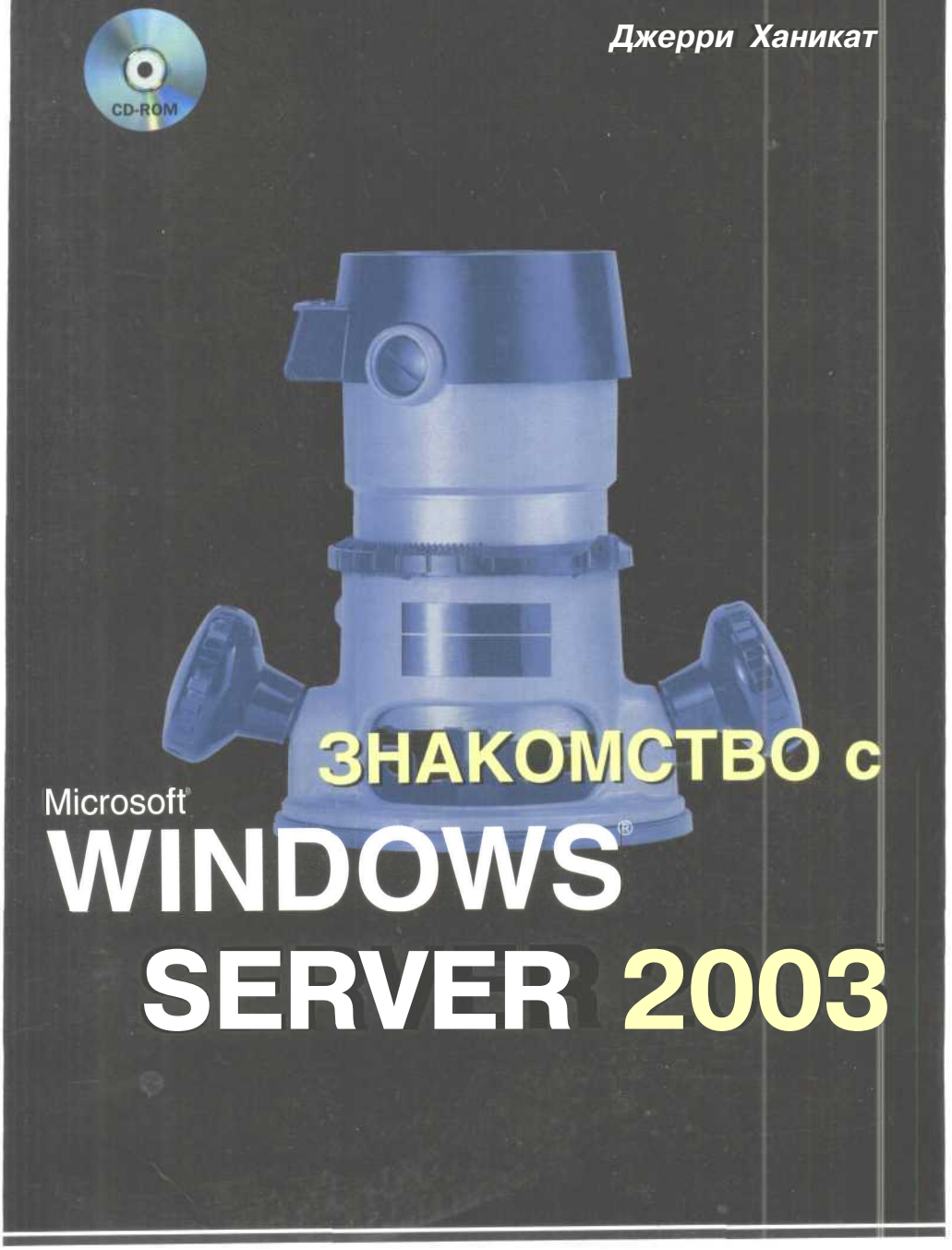
Джерри Ханикат



ЗНАКОМСТВО с Microsoft® WINDOWS® SERVER 2003

РУССКАЯ РЕДАКЦИЯ

Microsoft®

Jerry Honeycutt

INTRODUCING Microsoft® WINDOWS® SERVER 2003

Microsoft Press

Джерри Ханикат

ЗНАКОМСТВО с Microsoft WINDOWS® SERVER 2003

Москва 2003

РУССКАЯ РЕДАКЦИЯ

УДК 004.45
ББК 32.973.26-018.2
Х19

Ханикат Дж.

Х19 Знакомство с Microsoft Windows Server 2003 /Пер. с англ. — М.: Издательско-торговый дом «Русская Редакция», 2003. — 464 с.: ил.

ISBN 5-7502-0237-2

Из этого официального руководства вы узнаете о новинках и улучшениях в мощной сетевой операционной системе Microsoft Windows Server 2003, в том числе об усовершенствованных технологиях Web-сервисов и компонентов, безопасности, сетевой поддержке, службе каталогов Active Directory, Microsoft Internet Information Services, поддержке IPv6 и многом другом. Вы получите всю информацию, необходимую для планирования внедрения Microsoft Windows Server 2003 как в случае перехода с Microsoft Windows NT Server, так и Windows 2000 Server.

Книга состоит из 18 глав и предметного указателя. Компакт-диск, прилагаемый к книге, содержит 360-дневную ознакомительную версию (RC2) Microsoft Windows Server 2003.

УДК 004.45
ББК 32.973.26-018.2

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

ISBN 0-7356-1570-5 (англ.)
ISBN 5-7502-0237-2

Оглавление

Благодарности

Мне хотелось бы поблагодарить всех, кто помог в создании этой книги. Мартин Делре был выпускающим редактором. Валери Вули, редактор проекта, отвечала за общее управление процессом. Она проделала серьезную работу, заставляя меня укладываться в сроки. Благодарности заслуживают и многие другие люди. Прежде всего, технический редактор Дэйл Мэйджи мл., чья поддержка сделала книгу исключительно аккуратной. Редактор Шон Пэк добился того, что она стала читаемой,

Важно отметить авторов материалов, на основе которых создавалась эта книга. Это ребята из Microsoft, написавшие рекламные материалы по Microsoft Windows Server 2003, которые вы можете найти по адресу *http://www.microsoft.com/windows.netserver*. Вот эти люди: Марк Аггар, Перри Антон, Мэри Элис Калвин. Джозеф Дэвис, Брайан Дюи, Джейсон Гудмен, Тод Хэдрик, Джон Кайзер, Дженна Миллер Капчински, Дэвид Мартин, Азиф Мойнуддин, Маной Найар, Нэнси Нарроуэй, Даниэл Куэва, Джексон Шоу, Бил Стэплз, Энди Старк, Дэвид Зэнк и Этан Золлер.

Содержимое компакт-диска

На компакт-диске записана 360-дневная ознакомительная предварительная версия (RC2) Microsoft Windows Server 2003.

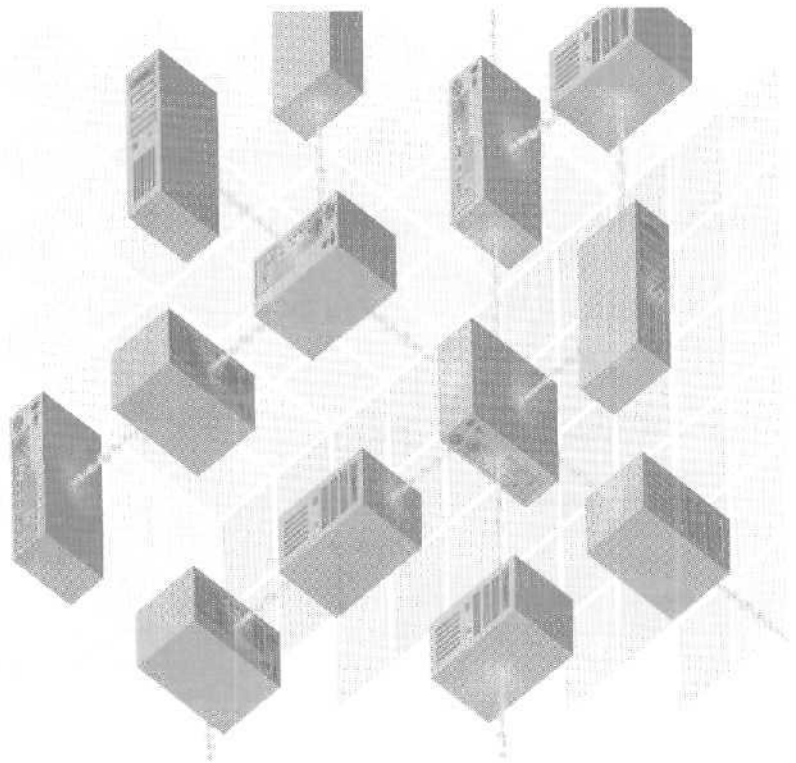
- Требования к оборудованию приведены в конце книги.
- Для работы с книгой дополнительное ПО не требуется.
- Компакт-диск предназначен лишь для ознакомительных целей.
- Windows Server 2003 пока находится в стадии предварительной реализации, и полная поддержка системы не осуществляется.

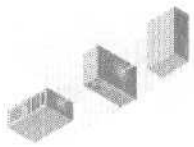
Предупреждение 360-дневная ознакомительная версия, поставляемая с этой книгой, не является законченным коммерческим продуктом и предоставляется лишь для ознакомительных целей. Microsoft Press не обеспечивает поддержки компакт-диска.

Дополнительные сведения о поддержке см. на Web-сайте Microsoft Press Technical Support (*http://www.microsoft.com/mspress/support*).Вы можете также написать по электронной почте: *tkinput@microsoft.com* или отправить письмо по адресу: Microsoft Press, Attn: Microsoft Press Technical Support, One Microsoft Way, Redmond, WA 98052-6399.

ЧАСТЬ I

ОБЗОР





ГЛАВА

1

Семейство операционных систем

Эта глава знакомит с семейством операционных систем Microsoft Windows Server 2003. Описываются различные выпуски (edition) ОС и требования каждого к аппаратным средствам. Задача этой главы — помочь вам в выборе выпуска Windows Server 2003 в соответствии с вашими потребностями. Кроме того, данная глава является путеводителем по другим главам книги,

Знакомство с семейством

Семейство Windows Server 2003 включает следующие выпуски.

- **Windows Server 2003, Standard Edition** Надежная сетевая ОС, позволяющая быстро создавать решения на ее основе. Это отличный выбор для малых предприятий и подразделений крупных компаний. Standard Edition предоставляет средства совместного использования файлов и принтеров, обеспечивает безопасное подключение к Интернету, а также поддерживает централизованное развертывание настольных приложений. Подробнее см. ниже раздел «Standard Edition».
- **Windows Server 2003, Enterprise Edition** ОС общего назначения для предприятий любых размеров. Эта идеальная платформа для приложений, Web-сервисов и инфраструктуры обеспечивает высокую надежность, производительность и средства масштаба предприятия. Enterprise Edition — полнофункциональная серверная ОС — поддерживает до 8 про-

цессоров, предоставляет такие средства масштаба предприятия, как 8-узловой кластер, и способна использовать до 32 Гб оперативной памяти. Она доступна на компьютерах на основе процессоров Intel Itanium и скоро будет доступна на 64-битных платформах, поддерживающих 8 процессоров и 64 Гб памяти. Подробнее см. ниже раздел «Enterprise Edition».

- Windows Server 2003, Datacenter Edition Предназначена для особо важных приложений, предъявляющих высочайшие требования к масштабируемости и готовности (availability). Microsoft полагает, что Datacenter Edition — это наиболее мощная и функциональная серверная ОС из когда-либо создававшихся компанией. Она поддерживает до 32 процессоров и до 64 Гб оперативной памяти. В качестве стандартных средств в нее включена поддержка 8-узловых кластеров и средств распределения нагрузки (load-balancing). Скоро она будет доступна на 64-битных платформах с поддержкой до 32 процессоров и до 128 Гб памяти, Подробнее см. раздел «Datacenter Edition» этой главы.
- Windows Server 2003, Web Edition Новый член семейства серверных ОС Windows. Microsoft предоставляет Web Edition для создания и развертывания Web-приложений, Web-страниц и Web-сервисов XML. В основном этот выпуск ОС предназначен для работы в качестве Web-сервера Internet Information Services (IIS) 6.0 и является платформой для быстрой разработки и развертывания Web-сервисов XML и приложений, использующих технологию ASP.NET, которая является ключевым компонентом .NET Framework. Подробнее см. ниже раздел «Web Edition».

Standard Edition

На верхнем уровне Windows Server 2003, Standard Edition поддерживает:

- симметричные 4-процессорные системы;
- 4 ГБ памяти;
- такие сетевые средства, как Internet Authentication Service (IAS), Network Bridge и Internet Connection Sharing (1CS).

В Standard Edition включены следующие средства.

- **Internet Information Services** IIS 6.0 — это Web-сервер для Windows Server 2003, позволяющий легко обеспечить обмен информацией между партнерами, клиентами и сотрудниками по интрасети, Интернегу или экстрасети. Модернизированная архитектура IIS 6.0 удовлетворяет самым высоким требованиям в области надежности, универсальности и управляемости.
- **Средства зашиты IIS** По умолчанию во время установки параметры защиты IIS 6.0 настраиваются так. чтобы гарантировать работу только необходимых служб. Это нововведение снижает начальный риск, связанный с зашитой. IIS Security Lockdown Wizard позволяет администраторам включать/отключать функциональные возможности сервера.
- **Средства каталога** Служба Microsoft Active Directory — центральный компонент платформы Windows — обеспечивает управление сетевой средой.
- **Управление модернизацией** Auto Update обеспечивает возможность систематическою получения исправлений и «заплат» системы защиты ОС. Момент установки этих обновлений определяет администратор.
- **Брандмауэр для Интернета** Встроенный брандмауэр Internet Connection Firewall защищает соединения с Интернетом лучше, чем раньше. Интеграция брандмауэра в ОС снижает объем капиталовложений. необходимых для подключения к Интернету.
- **Удаленный доступ** Права пользователей, подключающихся по телефонным линиям, могут быть ограничены административной политикой. Им может быть запрещен доступ к сети до тех пор, пока не будет проверено, что на их компьютерах установлено требуемое администратором ПО, например, последние версии антивирусных программ.
- **Поддержка серверных аппаратных средств** Верификаторы драйверов проверяют новые драйверы устройств, помогая обеспечить бесперебойную работу сервера.
- **Верификация приложений** Приложения, исполняющиеся под Windows Server 2003, позволяет проверить инструмент Application Verifier. Данная утилита выявляет дефекты структур управления памятью и проблемы совместимости.

- **Файловые службы** Производительность файловой системы Windows Server 2003 повышена по сравнению с Microsoft Windows NT Server 4.0 и Windows 2000 Server.
- **Техническая поддержка** Средства технической поддержки дают пользователям возможность отправлять в Microsoft электронные сообщения о возникающих проблемах, общаться с инженерами технической поддержки, а также управлять процессом решения проблем.
- **Отслеживание системных событий** Новое средство слежения за остановками сервера (shutdown tracker), позволяющее администраторам точно учитывать время работы сервера, записывает в файл журнала события Windows, связанные с остановками сервера.
- **Мастер Configure Your Server** Позволяет настроить сервер для выполнения различных ролей, таких как файловый сервер, сервер печати, сервер удаленного доступа и др., гарантируя правильную первоначальную установку и настройку компонентов.
- **Мастер Manage Your Server** Предоставляет удобный интерфейс повседневного управления сервером, облегчая выполнение таких операций, как заведение новых пользователей и создание общих сетевых каталогов.
- **Удаленное администрирование сервера** Remote Desktop for Administration (ранее Terminal Services в режиме Remote Administration) позволяет администраторам управлять сервером практически с любого компьютера в сети. Remote Desktop for Administration предназначен специально для управления сервером.
- **Удаленная поддержка** Remote Assistance позволяет администраторам управлять удаленным пользовательским компьютером. При обращении удаленного пользователя к администратору или в службу поддержки Remote Assistance предоставляет последним удобный способ подключения к удаленному компьютеру с компьютера, работающего под управлением Microsoft Windows XP или любого выпуска Windows Server 2003. После подключения к удаленному компьютеру персонал службы поддержки может видеть экран удаленного компьютера и обмениваться с удаленным пользователем текстовыми сообщениями в реальном времени.

С позволения пользователя удаленного компьютера персонал службы поддержки может получить доступ к мыши и клавиатуре удаленного компьютера.

- **Теневое копирование** Позволяет фиксировать версии файлов сетевых каталогов в заданные моменты времени. Администраторы могут просматривать прошлое содержимое сетевого каталога. Конечные пользователи могут восстанавливать случайно удаленные файлы и папки к сетевых каталогах без вмешательства системного администратора.
- **Terminal Server** Terminal Server позволяет пользователю, работающему на более старых устройствах, получать доступ к программам, исполняющимся на сервере. Так, пользователь может работать с виртуальным рабочим столом Windows XP Professional и Windows-приложениями, используя аппаратные средства, которые сами не способны исполнять эти программы. Данная возможность предоставляется Terminal Server как для клиентских устройств на основе Windows, так и для устройств на основе других ОС.
- **Сервер Web-приложений** Windows Server 2003 — это полноценный сервер Web-приложений. Он интегрирует .NET Framework с базовыми ресурсами сервера, что облегчает разработку, развертывание и администрирование приложений и Web-сервисов XML. .NET Framework предоставляет полностью управляемую и защищенную среду исполнения приложений, упрощенную разработку и развертывание, а также полную интеграцию с разнообразными языками программирования.
- **Windows Media Services** Обеспечивают распространение потокового аудио и видео по корпоративной интрасети или Интернету.
- **Поддержка беспроводных ЛВС** Данная возможность предоставляет улучшенную с точки зрения безопасности и производительности поддержку беспроводных локальных вычислительных сетей (ЛВС), в том числе автоматическое управление ключами, аутентификацию пользователей и авторизацию перед доступом к ЛВС. Windows Server 2003. Standard Edition значительно упрощает развертывание и эксплуатацию беспроводных служб.

Enterprise Edition

Windows Server 2003, Enterprise Edition предназначается для средних и крупных предприятий. Эту ОС Microsoft рекомендует для серверов, на которых исполняются сетевые приложения, приложения электронных сообщений, системы обслуживания клиентов, базы данных и Web-сайты электронной коммерции. По степени надежности, производительности и набору системных средств Enterprise Edition превосходит любые из предшествующих версий Windows. Скоро Enterprise Edition будет доступа в 32- и 64-битном вариантах. Она содержит все средства, включенные в Standard Edition, а кроме того, поддержку высокопроизводительных серверов и возможность построения кластеров серверов, выдерживающих большие нагрузки. На верхнем уровне Windows Server 2003 Enterprise Edition поддерживает:

- симметричные 8-процессорные системы;
- 8-узловые кластеры;
- 32 Гб памяти в 32-битном варианте и 64 Гб — в 64-битном.

Windows Server 2003, Enterprise Edition может масштабироваться и вверх, и вширь. Во-первых, производительность и возможности сервера можно увеличить, установив дополнительные процессоры и память. Такой подход называется *масштабированием вверх* (scaling up). Расширенная SMP-поддержка в Enterprise Edition позволяет задействовать многопроцессорные серверы. Данная ОС также поддерживает расширенные возможности управления памятью, что позволяет наращивать память серверы до 8 Гб. Enterprise Edition также позволяет объединять сервера в кластер с равномерным распределением нагрузки, т. е. реализовать *масштабирование вширь* (scaling out). Windows Server 2003, Enterprise Edition — самая надежная серверная ОС масштаба предприятия из всех, когда-либо создававшихся Microsoft. Расширения включают усовершенствования ключевых технологий, впервые представленных в Windows 2000 Server, таких как Network Load Balancing (NLB), кластеры серверов и служба каталогов Microsoft Active Directory.

Enterprise Edition поддерживает 64-битные вычисления на сертифицированных аппаратных платформах, что позволяет ускорить работу приложений, требующих больших ресурсов

процессора и памяти. Сюда входит поддержка процессоров Itanium и Itanium 2 компании Intel.

Помимо возможностей Standard Edition, Enterprise Edition включает ряд средств, повышающих готовность, масштабируемость и надежность. (Эти средства также включены в Windows Server 2003, Datacenter Edition.)

- **Служба кластеров** Кластеры серверов обеспечивают высокую степень готовности и отказоустойчивости для приложений баз данных, совместного использования файлов и данных в интрасети, электронных сообщений и приложений. Служба кластеров в Windows Server 2003, Enterprise Edition и Datacenter Edition поддерживает кластеры размером до 8 узлов. Это повышает возможности по добавлению и удалению аппаратных средств в географически распределенных кластерных средах, а также степень масштабируемости приложений. Enterprise Edition позволяет применять разные конфигурации кластеров, в частности, однокластерные конфигурации с выделенной памятью, множественные кластеры в сети хранилищ (storage area network) и распределенные кластеры.
- **64-битная поддержка** Windows Server 2003, Enterprise Edition доступен в 32-битном варианте, но скоро будет доступен и в 64-битном. 64-битный вариант будет оптимизирован для решения задач, требующих больших ресурсов памяти и процессора, таких как САПР, профессиональная графика, большие СУБД и научные расчеты. 64-битный вариант поддерживает процессоры Intel Itanium и Itanium 2.
- **Многопроцессорная поддержка** Windows Server 2003 масштабируется от 1- до 32-процессорных систем. Windows Server 2003, Enterprise Edition поддерживает до 8 процессоров, тогда как Windows Server 2003, Datacenter Edition — до 32.
- **Поддержка Metadirectory Services** Microsoft Metadirectory Services (MMS) облегчает интеграцию информации из различных каталогов, баз данных и файлов в Active Directory. MMS предоставляет организации единое представление идентификационной информации, обеспечивает интеграцию бизнес-процессов с MMS и облегчает синхронизацию этой информации внутри организации.

- «Горячее» добавление памяти «Горячая» установка памяти позволяет устанавливать в компьютер новую память и делать ее доступной ОС и приложениям как часть обычной памяти. При этом перезагружать компьютер не требуется, и система не простаивает. В настоящий момент эта возможность будет работать только на серверах с аппаратной поддержкой добавления памяти во время работы. Установка памяти в такие серверы будет приводить к автоматическому запуску средств Hot-Add Memory.
- Поддержка NUMA BIOS компьютера может создавать таблицу Static Resource Affinity Table, описывающую NUMA-топологию системы (NUMA, Non-Uniform Memory Access — доступ к неоднородной памяти). Windows Server 2003, Enterprise Edition использует эту таблицу для управления приложениями, установки стандартных параметров привязки, планирования потоков и распределения памяти. Кроме того, информация о топологии доступна приложениям посредством набора интерфейсов программирования NUMA.
- Terminal Services Session Directory Это средство распределения нагрузки, позволяющее легко восстанавливать разорванный сеанс с фермой серверов, на которой работают средства Terminal Services. Session Directory совместима со службой распределения нагрузки Windows Server 2003 и поддерживается продуктами распределения нагрузки других компаний.

Windows Server 2003, Enterprise Edition обеспечивает развертывание приложений с высокой надежностью и масштабируемостью на стандартных аппаратных средствах. Распространенными примерами приложений, для которых подойдет Enterprise Edition, являются серверы баз данных, обработка электронных сообщений, файл-серверы и серверы печати. Enterprise Edition — отличный выбор для приложений постоянной готовности. Эта ОС позволит растущей организации обеспечить непрерывную работу важных приложений с одновременным их масштабированием вверх и вширь в соответствии с возрастающими требованиями.

Datacenter Edition

Windows Server 2003, Datacenler Edition предназначен для случаев, предъявляющих самые высокие требования к масштабируемости, готовности и надежности. На его основе можно реализовать критически важные приложения для БД, планировать ресурсы предприятия, обрабатывать большие объемы транзакций в реальном времени и консолидировать серверы. Datacenter Edition скоро будет доступен в 32- и 64-битном вариантах. Этот выпуск, включающий все возможности Windows Server 2003 Enterprise Edition, поддерживает бо́льшее число процессоров и бо́льшие объемы памяти. Windows Server 2003, Datacenter Edition доступен только посредством программы Windows Datacenter Program, являющейся интеграцией предложений аппаратных средств, ПО и услуг по сопровождению со стороны Microsoft и сертифицированных поставщиков аппаратных средств. На верхнем уровне Windows Server 2003, Datacenter Edition поддерживает:

- симметричные 32-процессорные системы;
- 8-узловые кластеры;
- 64 ГБ памяти в 32-битном варианте; 128 ГБ — в 64-битном.

Программа Windows Datacenter Program создана Microsoft для предоставления пользователям списка серверов, тщательно протестированных и доказавших свою высокую надежность. Windows Datacenter Program позволяет минимизировать время простоя ваших приложений. Только Microsoft сертифицирует производителей аппаратных средств, которые для получения разрешения на лицензирование и поддержку Windows Server 2003, Datacenter Edition успешно прошли строгие тесты. Уникальность Datacenter Edition в том, что данная ОС доступна только уже установленной на компьютеры сертифицированных производителей. — это ПО нельзя приобрести отдельно. Windows Datacenter Program обеспечивает следующие преимущества:

- единое место для обращения за поддержкой, предоставляемой объединенной командой, состоящей из персонала Microsoft и независимых производителей оборудования;
- строгие тесты и квалификационные испытания аппаратных и программных средств, гарантирующие их оптимальную совместную работу;

- координацию управления сопровождением и модернизацией аппаратных и программных средств;
- твердые гарантии надежности на основе новых требований MCSC (Microsoft Certified Support Center), разработанных для этой программы.

В отличие от закрытых систем, предлагаемых некоторыми компаниями, Windows Server 2003, Datacenter Edition поставляется большим числом производителей, продающих системы высокого уровня на основе процессоров Intel, способные исполнять имеющиеся в организации приложения. Пользователи могут выбрать поставщика, соответствующего их конкретным требованиям. В Windows Datacenter Program включены процесс сертификации, а также Datacenter Hardware Compatibility List, расширяющий и усиливающий текущие требования Microsoft к совместимости аппаратных средств. Эта программа обеспечивает совместное тестирование всех компонентов сервера в условиях больших нагрузок и гарантирует отсутствие программных или аппаратных конфликтов между компонентами,

Windows Hardware Quality Labs (WHQL) должна гарантировать, что аппаратные и программные средства независимых производителей будут качественными и успешно взаимодействующими с продуктами и технологиями Microsoft. Продукты независимых производителей должны пройти тест Hardware Compatibility и получить логотип «Designed for Windows». Наличие данного логотипа на аппаратном или программном продукте говорит о том, что такой продукт соответствует стандартам Microsoft на совместимость с ОС Windows. Аппаратные средства, предназначенные для использования с Windows Server 2003, Datacenter Edition должны быть спроектированы в соответствии с Hardware Design Guide.

Пользователи серверов, проверенных Windows Dalacenter Program, знают, что они получают законченную конфигурацию, в которой все аппаратные средства и программные компоненты на уровне ядра прошли строгое тестирование. Windows Server 2003, Datacenter Edition может продаваться только независимыми производителями, обязавшимися выполнять это дополнительное тестирование и настройку конфигурации. Тесты, которые должны провести независимые производители, позволяют гарантировать успешную работу следующих компонентов на серверах с Windows Server 2003, Datacenter Edition:

- все аппаратные компоненты;
- все драйверы аппаратных средств;
- все ПО уровня ядра, включая антивирусное ПО, управление дисками и лентами, ПО резервного копирования и другое ПО подобного рода.

Персонал Joint Support Queue for Windows Server 2003, Datacenter Edition состоит из сотрудников Microsoft и независимых производителей, что гарантирует тесное взаимодействие поставщика аппаратных средств и Microsoft. В результате создается единая точка для обращения за поддержкой критически важных приложений. Datacenter Joint Support Queue имеет доступ ко всем аппаратным конфигурациям из Datacenter Hardware Compatibility List и к исходному коду Windows Server 2003, Datacenter Edition, что позволяет быстро находить причины проблем и пути их решения.

Помимо средств, включенных в Windows Server 2003, Standard Edition и Enterprise Edition, Windows Server 2003, Datacenter Edition предоставляет следующие дополнительные возможное™.

- **Расширенное пространство физической памяти** На 32-битных Intel-платформах Windows Server 2003, Datacenter Edition поддерживает Physical Address Extension (PAE), что расширяет доступный объем физической памяти до 64 ГБ. На 64-битных Intel-платформах поддерживаемый объем памяти увеличен до архитектурного ограничения в 16 терабайтов,
- **Поддержка Intel Hyper-Threading** Технология Hyper-Threading позволяет одному физическому процессору исполнять несколько потоков команд одновременно,
- **Windows Sockets: непосредственный доступ к** SAN Данное средство позволяет приложениям Windows Sockets, использующим протокол TCP/IP (Transmission Control Protocol/ Internet Protocol), получить преимущества производительности сетей хранилищ (SAN — storage area networks) без изменений в коде приложений. Основной компонент этой технологии — многоуровневый компонент доступа Windows Sockets Server 2003, эмулирующий TCP/IP поверх компонентов доступа к SAN.

Windows Server 2003, Datacenter Edition имеет гораздо более высокие надежность, масштабируемость и управляемость

в сравнении с Windows 2000 Datacenter Server и способен поддерживать критические нагрузки в центрах данных масштаба предприятия. Отличает Datacenter Edition от других ОС семейства Windows Server 2003 тесное содружество независимых производителей аппаратных и программных средств. Эти компании гарантируют партнерство с пользователями на протяжении всего времени жизни своих систем, что выделяет Windows Server 2003, Datacenter Edition среди существующих платформ.

Web Edition

Windows Server 2003, Web Edition, предназначенный для создания и развертывания Web-приложений, Web-страниц и Web-сервисов XML, является специализированным решением для Интернет-провайдеров, разработчиков приложений и всех, кто хочет задействовать только функциональность, связанную с Web. Web Edition использует последние улучшения в IIS 6.0, Microsoft ASP.NET и Microsoft .NET Framework. (Подробнее об IIS 6.0 см. главу 8.) Этот выпуск будет доступен только по каналам для избранных партнеров и не поступит в продажу. Подробную информацию поставщики услуг могут получить на Web-сайте Microsoft Service Providers по адресу *http://www.microsoft.com/serviceproviders*.На верхнем уровне Web Edition поддерживает:

- симметричные двухпроцессорные системы;
- **2 ГБ памяти;**
- средства разработки и развертывания Web-приложений, включая ASP.NET и .NET Framework, интегрированные в ОС.

Как и все члены семейства Windows Server 2003, Web Edition построена на основе промышленных стандартов, что позволяет организациям расширять существующие приложения и быстро создавать новые. Разработчики могут собирать приложения прямо на сервере приложений, используя Web-сервисы XML и управляемый код, и исполнять их на любой платформе для Web-приложений.

Windows Server 2003, Web Edition предназначен для использования именно в качестве Web-сервера. Хотя компьютеры с Web Edition могут быть членами домена Active Directory, по-

следний не может быть установлен на компьютере с Web Edition. Таким образом, в одиночку Web Edition не годится для реализации таких средств управления, как Group Policy, Software Restriction Policies, Remote Installation Services (RIS), Microsoft Metadirectory Services, Internet Authentication Service (IAS) и т. д. Нельзя устанавливать и службы Universal Description, Discovery, and Integration (UDDI), являющиеся важным элементом обеспечения поиска и использования Web-сервисов XML. Недоступны также возможности масштабирования, предназначенные для систем масштаба предприятия.

Windows Server 2003, Web Edition реализует средства Web-инфраструктуры следующего поколения для серверных ОС Windows. Интернет-провайдеры и другие компании, которым требуется только Web-функциональность, получают преимущества от этой недорогой, простой в установке и администрировании ОС. Благодаря интеграции с ASP.NET и .NET Framework. Web Edition позволяет разработчикам быстро создавать и развертывать Web-сервисы XML и приложения.

При необходимости использования средств масштаба предприятия или более сложных возможностей администрирования. таких как Microsoft Active Directory, следует рассмотреть возможность покупки одного из более мощных выпусков Windows Server 2003: Standard Edition. Enterprise Edition или Datacenter Edition. Все средства Windows Server 2003, Web Edition, в том числе IIS 6.0 и Microsoft ASP.NET. поддерживаются и остальными членами семейства Windows Server 2003.

Сравнение возможностей

Табл. 1-1 позволяет сравнить возможности, доступные в различных выпусках Windows Server 2003. В таблице использованы следующие обозначения;

- ● — возможность включена;
- ◒ — возможность включена частично;
- C ○ — возможность не включена.

Табл. 1-1. Сравнение возможностей

Возможность	Standard	Enterprise	Datacenter	Web
.NET Application Services				
.NET Framework	●	●	●	●
Internet Information Services (IIS) 6.0	●	●	●	●
ASP.NET	●	●	●	●
Службы UDDI масштаба предприятия	●	●	●	○
Кластерные технологии				
Network Load Balancing	●	●	●	●
Кластерная служба	○	●	●	○
Коммуникационные и сетевые службы				
Поддержка Virtual Private Network (VPN)	●	●	●	◒
Internet Authentication Service (IAS)	A	●	●	○
Сетевой мост (bridge)	flp	●	●	○
Internet Connection Sharing (ICS)	●	●	○	◒
IPv6	●	●	●	◒
Службы каталогов				
Active Directory	●	●	●	●
Поддержка Metadirectory Services (MMS)	○	●	●	○
Файл-сервер и сервер печати				
Distributed File System (DFS)	●	●	●	●
Encrypting File System (EFS)	A	●	●	●
Восстановление теневых копий	●	●	●	●
Сменные и удаленные носители	яр	●	●	○
Факс-службы	●	●	●	○
Службы для Macintosh	●	●	●	○

(см. след. стр.)

Табл. 1-1. Сравнение возможностей *(продолжение)*

Возможность	Standard	Enterprise	Datacenter	Web
Службы администрирования				
IntelliMirror	●	●	●	●
Resultant Set of Policy (RSoP)	●	●	●	●
Командная строка для Windows Management Instrumentation (WMI)	●	●	●	●
Удаленная установка ОС	●	●	●	●
Remote Installation Services (RIS)	●	●	●	○
Мультимедийные службы				
Windows Media Services	●	●	●	○
Масштабируемость				
64-битная поддержка для компьютеров на основе Intel Itanium	○	●	●	○
Горячее добавление памяти	○	●	●	○
Non-Uniform Memory Access (NUMA)	○	●	●	○
Datacenter Program	○	○	●	○
Службы защиты				
Internet Connection Firewall	●	●	○	○
Инфраструктура открытых ключей, службы сертификатов и смарт-карт	◒	●	●	◒
Terminal Services				
Remote Desktop for Administration	●	●	●	●
Terminal Server	●	●	●	◒
Terminal Server Session Directory	○	●	●	○

.NET Framework, ASP.NET и Windows Media Services не поддерживаются в 64-битных вариантах Windows Server 2003. Кроме того, «горячее» добавление памяти и NUMA могут быть недоступны из-за отсутствия аппаратной поддержки.

Соответствие требованиям

В табл. 1-2 описаны требования Windows Server 2003 к аппаратным средствам.

Табл. 1-2. Требования к аппаратным средствам

Требование	Standard	Enterprise	Datacenter	Web
Минимальная скорость процессора	133 МГц	133 МГц для компьютеров на основе x86 733 МГц для компьютеров на основе Itanium	400 МГц для компьютеров на основе x86 733 МГц для компьютеров на основе Itanium	133 МГц
Рекомендуемая скорость процессора	550 МГц	733 МГц	733 МГц	550 МГц
Минимальный объем оперативной памяти	128 МБ	128 МБ	512 МБ	128 МБ
Рекомендуемый минимальный объем оперативной памяти	256 МБ	256 МБ	1 ГБ	256 МБ
Максимальный объем оперативной памяти	4 ГБ	32 ГБ для компьютеров на основе x86 64 ГБ для компьютеров на основе Itanium	64 ГБ для компьютеров на основе x86 128 ГБ для компьютеров на основе Itanium	2 ГБ
Поддержка многопроцессорных систем	1 или 2	до 8	минимум 8 максимум 32	1 или 2
Объем дискового пространства для установки	1,5 ГБ	1.5 ГБ для компьютеров на основе x86 2.0 ГБ для компьютеров на основе Itanium	1.5 ГБ для компьютеров на основе x86 2.0 ГБ для компьютеров на основе Itanium	1.5 ГБ

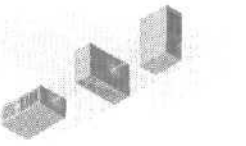
64-битные варианты Windows Server 2003, Enterprise Edition и Windows Server 2003, Datacenter Edition совместимы только с системами на основе 64-битных процессоров Intel Itanium. Они не могут быть установлены на 32-битные компьютеры.

Дополнительные сведения

Дополнительную информацию см. по следующим адресам:

- домашняя страница Windows Server 2003 — http://www.microsoft.com/windowsserver2003/;
- обзор продукта — http://www.microsoft.com/windowsserver2003/evaluation/overview/;
- аппаратные требования — http://www.microsoft.com/windowsserver2003/evaluation/sysreqs/systemrequirements.mspx.

ГЛАВА
2



Оценка характеристик Windows Server 2003

Эта глава начинается с описания преимуществ Microsoft Windows Server 2003. При ее разработке Microsoft особое внимание уделила надежности, производительности, способности к взаимодействию и экономической выгоде.

В разделе «Преимущества Windows Server 2003» описаны средства ОС, которые делают ее подходящей для крупных организаций. Два последних раздела посвящены причинам, по которым вам следует рассмотреть возможность перехода *на* Windows Server 2003. В заключение описаны средства, позволяющие объективно оценить Windows Server 2003 и рассчитать потенциальные прибыли от перехода на эту ОС.

Преимущества Windows Server 2003

Windows Server 2003 обладает преимуществами по сравнению с Windows 2000 Server в следующих четырех областях.

- Надежность Windows Server 2003 — самая быстрая, самая надежная и наиболее защищенная из всех серверных ОС Windows, когда-либо выпущенных Microsoft. Windows Server 2003 предоставляет интегрированную инфраструктуру, помогающую гарантировать безопасность вашей информации. Надежность, готовность и масштабируемость этой ОС позволяют вам реализовать сетевую инфраструктуру, соответствующую потребностям ваших пользователей.

- **Продуктивность** Windows Server 2003 предоставляет инструменты для развертывания, управления и использования сетевой инфраструктуры предприятия. Они позволяют спроектировать и развернуть сеть, соответствующую требованиям вашей организации. ОС предоставляет средства реализации административной политики, автоматизации задач и упрощения процесса модернизации, которые помогут вам в администрировании сети. Кроме того, средства ОС помогают снизить расходы на сопровождение, позволяя пользователям выполнять большее число задач самостоятельно.
- **Взаимодействие** Windows Server 2003 поможет организовать инфраструктуру прикладных задач, обеспечив лучшее взаимодействие между сотрудниками, партнерами, системами и клиентами. Для этого ОС предоставляет интегрированные Web-сервер и сервер медийных потоков, которые позволяют легко, быстро и безопасно создавать динамичные Web-сайты для интрасети и Интернета. ОС также включает интегрированный сервер приложений, обеспечивающий легкость разработки, развертывания и управления Web-сервисами XML.
- **Экономическая выгода** Windows Server 2003 в сочетании с продуктами и услугами, предоставляемыми партнерами Microsoft в области аппаратных и программных средств, обеспечивает повышение эффективности вложений в инфраструктуру. Для оптимизации конфигурации серверов новая ОС поможет консолидировать их с возможностями нового оборудования, программ и методологий.

Надежность

Надежность была важнейшей целью при разработке Windows Server 2003- В новой ОС получил свое развитие ряд технологий, появившихся в Windows 2000 Server: поддержка смарт-карт, Plug and Play, регулирование использования сетевых ресурсов (bandwith throttling). Новые технологии, такие как общеязыковая исполняющая среда (CLR — common language runtime), усиливают средства защиты и помогают оградить сети от влияния вредоносных или плохо написанных программ. Кроме того, улучшения в Internet Information Services (IIS) 6.0, инфраструктуре открытых ключей (PKI — public key infrastructure) и Ker-

beros упрощают обеспечение безопасности Windows Server 2003. Более эффективная синхронизация, репликация и кэширование регистрационных параметров пользователей в филиальных контроллерах доменов обеспечивает более быструю и качественную работу службы Microsoft Active Directory в ненадежных глобальных сетях.

Ключевые средства обеспечения надежности таковы.

- Готовность Благодаря расширенной поддержке кластеров Windows Server 2003 предоставляет большие возможности по поддержанию постоянной готовности. Поддержка кластеров стала абсолютной необходимостью для организаций, использующих критически важные приложения, в том числе для электронной коммерции, так как кластеры заметно повышают готовность, масштабируемость и управляемость. Установка и настройка кластеров в Windows Server 2003 существенно упрощена по сравнению с предыдущими версиями Windows: сетевые средства обеспечивают большие возможности по переключению при сбоях (failover) и сокращают простои.

  Windows Server 2003 поддерживает кластеры размером до 8 узлов. Если один из узлов становится недоступен из-за сбоя или при проведении регламентных работ, он сразу замещается другим узлом — данный процесс называется переключением при сбое (failover). Windows Server 2003 также поддерживает балансирование сетевой загрузки (NLB), распределяя трафик протокола TP между узлами кластера.
- Масштабируемость Windows Server 2003 обеспечивает масштабируемость путем масштабирования вверх, реализованного поддержкой симметричных многопроцессорных систем. и масштабирования вширь, реализованного поддержкой кластеров. Внутренние тесты Microsoft показали, что по сравнению с Windows 2000 Server, новая ОС обеспечивает более чем 140%-ое повышение производительности файловой системы и значительный прирост производительности других компонентов, включая Active Directory, Web-сервер, Terminal Server и сетевые службы. Windows Server 2003 масштабируется от 1- до 32-процессорных систем. Она поддерживает и 32-, и 64-битные процессоры.

- **Безопасность** Современные организации перешли от традиционных локальных вычислительных сетей (ЛВС) к более сложным сочетаниям интрасетей, экстрасетей и Интернет-сайтов. В итоге чрезвычайно важным стало обеспечение безопасности. Microsoft тщательно исследовала ОС семейства Windows Server 2003 с целью выявления возможных мест сбоев и уязвимых точек.

  Windows Server 2003 предоставляет ряд новых важных средств обеспечения безопасности, включая следующие.

  - CLR Этот ключевой элемент Windows Server 2003 позволяет уменьшить число сбоев и «дыр» в защите, вызываемых распространенными ошибками программирования. Кроме того, CLR проверяет, что приложение может работать без ошибок и обеспечивает проверку прав доступа, гарантируя, что программа выполняет только разрешенные действия.
  - **Internet Information Services 6.0** Для повышения защищенности Web-сервера при начальной установке IIS 6.0 по умолчанию устанавливается в минимальном режиме (locked down). Среди продвинутых средств защиты в IIS 6.0 — выбор службы шифрования, улучшенная дайджест-аутентификация и настраиваемое управление правами доступа процессов. IIS 6.0 также обладает рядом других новых средств защиты, позволяющих безопасно вести бизнес в Интернете.

Продуктивность

Один из важнейших приоритетов Windows Server 2003 — продуктивность — обеспечивается с помощью расширенных возможностей управления системой. Ориентированный на задачи интерфейс Windows Server 2003 облегчает поиск средств решения распространенных задач, Улучшения в Microsoft Management Console (MMC) и Active Directory повышают производительность и облегчают администрирование.

Среди новых средств управления и администрирования отметим переименование доменов, сквозное управление доменами и лесами, а также Resultant Set of Policy (RSoP). Расширенные компоненты доступа и утилиты командной строки Windows Management Instrumentation (WMI) дают администраторам возможность более тонкого управления серверами.

Ключевые средства обеспечения продуктивности таковы.

- **Службы файлов и печати** Эффективное управление ресурсами файлов и печатью и обеспечение к ним постоянного доступа пользователей с учетом назначенных прав является основой любой информационной системы. Растущее число пользователей, расположенных как локально, так и в удаленных подразделениях и даже в компаниях-партнерах, увеличивает нагрузку на сетевых администраторов. Windows Server 2003 предоставляет интеллектуальные службы файлов и печати, обладающие повышенными производительностью и функциональными возможностями,
- **Active Directory** Active Directory хранит информацию об объектах в сети и обеспечивает ее логическую иерархию. Active Directory в Windows Server 2003 обладает повышенной производительностью и масштабируемостью. Она также обеспечивает большую гибкость в проектировании, развертывании и управлении каталогом организации,
- **Средства сопровождения** Windows Server 2003 предоставляет новые средства автоматизации сопровождения, включая Microsoft Software Update Services (SUS) и мастер настройки сервера, что помогает автоматизировать развертывание. Новая Group Policy Management Console (GPMC) облегчает управление групповой политикой. Утилиты командной строки позволяют администраторам выполнять большинство задач из командной консоли. На момент выпуска Windows Server 2003 предоставление GPMC планировалось в виле отдельного компонента.
- **Управление хранением данных** Windows Server 2003 позволяет упростить и повысить надежность управления и сопровождения дисков и томов, резервного копирования и восстановления данных, а также подключение к сети хранилищ.
- **Terminal** Services Построены на основе Windows 2000 Terminal Services в режиме сервера приложений. Terminal Services обеспечивают доступ к Windows-приложенями или к самому пользовательскому интерфейсу Windows практически с любого вычислительного устройства, включая те, на которые Windows не может быть установлена.

Windows Server 2003 упрощает управление хранением и резервным копированием данных, снижая требования к систем-

ным администраторам. Среди новых и улучшенных файловых служб, которые сделали это возможным, — Volume Shadow Copy, обеспечивающая создание резервных копий содержимого сетевых каталогов на заданные моменты времени. Преимущества этой уникальной технологии доступны и пользователям, которые теперь могут прямо со своего Windows-компьютера восстанавливать старые версии файлов или удаленные файлы с помощью средства Shadow Copy Restore. Кроме того, новые возможности управления файлами и печатью обеспечивает технология совместного использования удаленных документов Web-Based Distributed Authoring and Versioning (WebDAV). Расширения Distributed File System (DFS) и Encrypting File System (EFS) также повышают гибкость средств совместного использования и хранения файлов.

Взаимодействие

Windows Server 2003 позволяет обеспечить поддержку соединения с центральной системой пользователей, находящихся в любом месте и работающих на любых устройствах. Microsoft значительно улучшила сетевые средства Windows Server 2003, включая поддержку Internet Protocol version 6 (IPv6), Point-to-Point Protocol over Ethernet (PPoE) и Internet Protocol Security (IPSec) при использовании Network Address Translation (NAT).

Улучшения в области средств взаимодействия таковы.

- Web-сервисы XML IIS 6.0 — важный компонент семейства Windows Server 2003. Архитектурные улучшения IIS включают новую модель процессов, повышающую надежность, масштабируемость и производительность. По умолчанию IIS устанавливается в минимальном режиме. Это повышает безопасность, так как системный администратор включает/отключает возможности в соответствии с требованиями приложения. Поддержка редактирования метабазы XML расширяет возможности управления.
- Сети и коммуникации Сотрудники должны иметь возможность подключения к сети из любой точки и с любого устройства. Партнерам и поставщикам требуется эффективно взаимодействовать с ключевыми ресурсами. Улучшения и новые средства поддержки сети в Windows Server 2003 повышают универсальность, управляемость, надежность и безопасность сетевой инфраструктуры,

- Службы Enterprise **UDDI** Windows Server 2003 включает службы Enterprise UDDI — динамическую и гибкую инфраструктуру для Web-сервисов XML. Этот стандарт позволяет компаниям использовать собственный внутренний сервис UDDI в интра- или экстрассти. Разработчики могут быстро находить и повторно использовать имеющиеся в организации Web-сервисы. Системные администраторы могут управлять и каталогизировать программируемые ресурсы своих сетей. Службы Enterprise UDDI позволяют создавать и использовать более интеллектуальные и надежные приложения.
- Windows Media Services Windows Server 2003 включает наиболее мощные на сегодняшний день службы передачи медийных потоков. Эти службы являются частью следующей версии платформы Microsoft Windows Media, которая также включает новые версии Windows Media Player, Windows Media Encoder, аудио/видео кодеков и Windows Media Software Development Kit.

Встроенная поддержка Microsoft .NET и XML, делает Windows Server 2003 идеальной платформой для разработки, распространения и размещения Web-сервисов XML, созданных на основе .NET. Microsoft .NET интегрирована в ОС семейства Windows Server 2003. Это обеспечивает беспрецедентный уровень интеграции программ с использованием Web-сервисов XML: дискретные приложения — строительные блоки, соединенные друг с другом, а также и с другими, большими приложениями по Интернету. Внедренная в продукты, составляющие платформу Microsoft, .NET обеспечивает быстрое и надежное создание, развертывание, эксплуатацию и использование защищенных и взаимосвязанных решений через Web-сервисы XML.

Платформа Microsoft предоставляет набор инструментов разработки, клиентских приложений, Web-сервисов XML и серверов. Web-сервисы XML предоставляют повторно используемые компоненты, построенные на основе промышленных стандартов, которые могут обращаться к другим приложениям независимо от того, как те были созданы, какая ОС или платформа нужна для их исполнения и какие устройства требуются для доступа к ним. С помощью Web-сервисов XML разработчики могут интегрировать приложения внутри предприятий или за пределами корпоративных сетей с партнерами и клиентами.

Возможность взаимодействия на федеративном уровне и более эффективные сервисы «бизнес — бизнес» и «бизнес — потребитель» потенциально способно заметно увеличить прибыли.

Экономическая выгода

Высокая надежность Windows Server 2003 позволяет управлять расходами, снижая время ремонтных работ и регламентных простоев. Windows Server 2003 может гибко масштабироваться вверх и вширь в зависимости от текущих потребностей.

Инструменты администрирования и настройки Windows Server 2003 упрощают развертывание и управление. Совместимость с существующими приложениями и продуктами независимых производителей означает, что вложения в инфраструктуру не будут потеряны.

Переход с Windows NT Server

Ниже описаны основные новые возможности и улучшения, на которые следует обратить внимания организациям, рассматривающим переход на новую ОС с Microsoft Windows NT Server 4.0.

- **Active Directory** Служба каталогов Microsoft Active Directory упрощает администрирование сложных сетевых каталогов и облегчает пользователям поиск ресурсов даже в очень больших сетях. Эта масштабируемая служба с самого начала строилась на основе стандартных технологий Интернета и полностью интегрирована на уровне ОС в Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition и Windows Server 2003, Datacenter Edition. Windows Server 2003 предоставляет массу улучшений, направленных на упрощение работы с Active Directory, и новые возможности: доверительные отношения между лесами, возможность переименования доменов, а также деактивизации атрибутов и классов схемы для изменения их определений.
- **Групповая политика: Group Policy Management Console** Администраторы могут применять групповую политику для определения параметров и разрешенных действий для пользователей и компьютеров. Групповая политика в отличие от локальной позволяет установить правила для всего узла, домена или организационного подразделения в Active Directory. Администрирование на основе политики облегчает

выполнение модернизации систем, установки приложений, управления профилями пользователей, а также блокировку рабочих станций. Планируемая в качестве подключаемого (add-in) компонента Windows Server 2003, GPMC предоставляет новый каркас для управления групповой политикой.

- **Производительность сервера** Внутренние тесты Windows Server 2003 показали, что производительность файл-сервера и Web-сервера возросла по сравнению с Windows NT Server 4.0 вдвое. Степень прироста производительности в конкретных условиях может быть иной из-за особенностей сети и компьютера, но Microsoft уверена, что улучшенная производительность Windows Server 2003 поможет ускорить работу сетевых решений.
- **Volume Shadow Copy Restore** Являясь частью службы Volume Shadow Copy, данное средство позволяет администраторам, не прерывая обслуживания, создавать моментальные копии важных данных, а затем задействовать их для восстановления или архивирования. Пользователи могут получить архивированные версии своих документов, хранящиеся на сервере невидимыми.
- **Internet Information Services 6.0 и Microsoft .NET Framework** IIS 6.0 — это полноценный Web-сервер, поддерживающий Web-приложения и Web-сервисы XML. Переработанная архитектура с новой отказоустойчивой моделью процессов заметно повышает надежность Web-сайтов и приложений. Теперь IIS может изолировать отдельное Web-приложение или несколько сайтов внутри самостоятельного процесса (пула приложений), взаимодействующего напрямую с ядром ОС. Это повышает производительность и возможности приложений и в то же время предоставляет больше пространства на серверах, что снижает требования к аппаратным средствам. Самостоятельные пулы приложений не позволяют приложению или сайту разрушить Web-сервисы XML или другие приложения на сервере. IIS также предоставляет средства мониторинга для обнаружения сбоев Web-приложения, а также для восстановления после таких сбоев и их предотвращения. Microsoft ASP.NET в Windows Server 2003 использует новую модель процессов IIS. Новые возможности контроля состояния приложений и обнаружения сбоев

доступны также и существующим приложениям для IIS 4.0 и 5.0, большинство из которых не потребует модификаций.

.NET Framework предоставляет модель программирования для построения, развертывания и исполнения Web-приложений и Web-сервисов XML на этой очень стабильной платформе. Она предоставляет продуктивную, основанную на стандартах многоязычную среду для интеграции прежних приложений с приложениями и сервисами следующего поколения, а также возможность быстрого решения проблем развертывания и работы приложений масштаба Интернета. Существующие приложения можно легко преобразовать в Web-сервисы XML, а UNIX-приложения — интегрировать или даже перенести в новое решение.

- **Terminal** Services Позволяют администраторам обеспечить доступ к Windows-приложениям или самому пользовательскому интерфейсу Windows с любого вычислительного устройства, включая те, на которых Windows исполняться не может. Когда пользователи работают с приложением через Terminal Services, приложение исполняется на сервере, а по сети передается только информация, связанная с клавиатурой, мышью и дисплеем. Пользователь видит только свою отдельную сессию, которая управляется серверной ОС прозрачно и остается независимой от сеансов других клиентов.

  Remote Desktop for Administration построен на основе Windows 2000 Terminal Services в режиме удаленного администрирования, Помимо двух виртуальных сеансов, поддерживаемых Windows 2000 Terminal Services в этом режиме, администратор может удаленно подключиться к реальной консоли сервера. Terminal Services могут повысить возможности развертывания программ в масштабах предприятия.
- Кластеры (до 8 узлов) Данная служба, доступная только в Windows Server 2003, Enterprise Edition и Datacenter Edition, обеспечивает высокую готовность и масштабируемость для критически важных приложений, таких как БД, системы электронных сообщений, а также файл-серверы и серверы печати. Кластеризация реализуется путем обеспечения постоянной связи между несколькими серверами (узлами). Узел кластера, ставший недоступным из-за сбоя или при проведении регламентных работ, сразу замещается другим узлом — данный процесс называется переключением при

сбое. Пользователи, работавшие с отключенным узлом, продолжают работать, даже не подозревая о том, что теперь сервис им предоставляется другим компьютером. И Windows Server 2003, Enterprise Edition, и Windows Server 2003, Datacenter Edition поддерживают кластеры до 8 узлов,

- **Интегрированная поддержка PKI с использованием Kerberos версии 5** Certificate Services и инструменты управления сертификатами позволяют организациям создавать свои инфраструктуры открытых ключей (PKI — public key infrastructure). Применяя PKI, администраторы могут реализовывать технологии на основе стандартов, такие как вход в систему по смарт-картам, аутентификация клиентов (посредством Secure Sockets Layer и Transport Layer Security), защищенная электронная почта, цифровая подпись и защищенное соединение по протоколу IP (IPSec). Certificate Services позволяет администраторам создавать и управлять центрами выпуска сертификатов (certification authorities), которые выдают и отзывают сертификаты X.509 V3. Это значит, что организации могут не зависеть от коммерческих служб аутентификации клиентов. хотя и они могут быть интегрированы с инфраструктурой открытых ключей организации.

  Kerberos версии 5 — это надежный стандартный сетевой протокол аутентификации, благодаря которому быстрый процесс однократного ввода параметров входа в систему обеспечивает пользователям доступ к ресурсам предприятия и другим средам, поддерживающим этот протокол. Поддержка Kerberos версии 5 дает и другие преимущества, такие как взаимная аутентификация (когда и клиент, и сервер аутентифицируют друг друга) и делегированная аутентификация (идентификационные параметры пользователя передаются по цепочки служб).

- **Управление из командной строки** Windows Server 2003 предоставляет расширенную инфраструктуру командной строки, позволяющую выполнять большинство административных задач, не применяя графического интерфейса. Особенно важна возможность выполнения широкого диапазона задач путем доступа к хранилищу информации, поддерживаемому Windows Management Instrumentation (WMI). Средство WMI с командной строкой (WMIC) предоставляет простой интерфейс командной строки, взаимодействую-

щий с командными процессорами (shell) и утилитами и легко расширяемый с помощью сценариев или других приложений администрирования. Возможности командной строки Windows Server 2003 в сочетании с готовыми сценариями соперничают с мощными средствами других ОС, часто имеющих большую стоимость владения. Администраторы, привыкшие управлять системами UNIX или Linux через командную строку, могут использовать ее в Windows Server 2003.

- **Интеллектуальные файловые службы: Encrypting File System, Distributed File System и File Replication Service** EFS дает пользователю возможность шифрования/дешифрования файлов для защиты их от несанкционированного просмотра лицами, получившими физический доступ к этим данным. Шифрование прозрачно: пользователи работают с зашифрованными файлами и каталогами так же, как и с обычными. Если пользователь EFS — то же лицо, что зашифровало файл или каталог, система автоматически дешифрует их при повторном обращении.

  DFS упрощает задачу управления совместно используемыми дисковыми ресурсами в сети. Администраторы могут назначать сетевым устройствам логические имена, не заставляя пользователей знать фактическое имя каждого сервера, к которому им может потребоваться доступ. FRS является шагом вперед в сравнении со средством репликации каталогов Windows NT Server 4.0. Так, FRS поддерживает многостороннюю (multimaster) репликацию файлов в заданный каталог между выбранными серверами. Кроме того, FRS используется DFS для автоматической синхронизации содержимого между заданными репликами, а также Active Directory — для автоматической синхронизации информации между контроллерами доменов.

Переход с Windows 2000 Server

Windows Server 2003 интегрирует мощную среду приложений для разработки инновационных Web-сервисов XML и улучшенных приложений, которая существенно повышает эффективность процесса. Организациям, планирующим переход на новую ОС с Microsoft Windows 2000 Server, надо обратить внимание на следующие возможности и улучшения.

- **Улучшения в Active Directory** Active Directory упрощает администрирование сложных сетевых каталогов и поиск ресурсов даже в самых больших сетях. Эта служба каталогов масштаба предприятия изначально строилась на основе стандартных технологий Интернета и полностью интегрирована на уровне ОС в Windows Server 2003, Standard Edition, Windows Server 2003, Enterprise Edition и Datacenter Edition. Windows Server 2003 предоставляет массу улучшений, направленных на упрощение работы с Active Directory, и новые возможности, включая доверительные отношения между лесами, переименование доменов и деактивизацию атрибутов и классов схемы для изменения их определений,
- **Group Policy Management Console** Посредством групповой политики администраторы могут разрешать действия пользователям и компьютерам. Групповая политику в отличие от локальной позволяет установить правила для всего узла, домена или организационного подразделения в Active Directory. Администрирование на основе политики облегчает модернизацию систем, установку приложений, управление профилями пользователей и блокировку рабочих станций. Планируемая в качестве подключаемого (add-in) компонента Windows Server 2003. GPMC предоставляет новую модель управления групповой политикой. GPMC упрощает применение групповой политики.
- Resultant Set **of Policy** RSoP предоставляется в виде набора оснасток (snap-in) Microsoft Management Console (MMC) и позволяет администраторам анализировать текущий набор правил политики в двух режимах: режим регистрации и режим планирования. В режиме регистрации администраторы могут просмотреть результат применения политики к определенному объекту. Режим планирования позволяет узнать, что получится в результате применения политики к определенному объекту, прежде чем внести соответствующее изменения в групповую политику.
- **Volume Shadow Copy Restore** Являясь частью службы Volume Shadow Copy, позволяет администраторам, не прерывая обслуживания, создавать моментальные копии важных данных, а затем задействовать их для восстановления или архивирования. Пользователи могут получить архивированные

версии своих документов, хранящиеся на сервере невидимыми.

- **Internet Information Services 6.0** Это полноценный Web-сервер, поддерживающий Web-приложения и Web-сервисы XML. Полностью переработанная архитектура с новой отказоустойчивой моделью процессов повышает надежность Web-сайтов и приложений. Теперь IIS может изолировать отдельное Web-приложение или несколько сайтов внутри самостоятельного процесса (пула приложений), взаимодействующего напрямую с ядром ОС. Это повышает производительность приложений и в то же время предоставляет больше пространства на серверах, что снижает требования к аппаратным средствам. Самостоятельные пулы приложений не позволяют приложению или сайту разрушить Web-сервисы XML или другие приложения на сервере. IIS также предоставляет средства мониторинга для обнаружения сбоев Web-приложения, а также для восстановления после таких сбоев и их предотвращения. Microsoft ASP.NET в Windows Server 2003 использует новую модель процессов IIS. Новые возможности контроля состояния приложений и обнаружения сбоев доступны также и существующим приложениям для Internet Information Server 4.0 и IIS 5.0. большинство из которых не потребует модификаций.
- **Интегрированная .NET Framework** Microsoft .NET Framework — это модель программирования взаимодействующих программных средств Microsoft .NET для построения, развертывания и исполнения Web-приложений, интеллектуальных клиентских приложений, а также Web-сервисов XML, которые предоставляют программный доступ к своим возможностям по сети по стандартным протоколам, таким как SOAP, XML и HTTP. .NET Framework предоставляет производительную, основанную на стандартах среду для интеграции прежних приложений с сервисами следующего поколения, возможность быстрого решения проблем развертывания и работы приложений масштаба Интернета. Благодаря полной интеграции .NET Framework в ОС Windows Server 2003 разработчикам не нужно писать инфраструктурный код. .NET Framework берет на себя детали интеграции и управления, что упрощает программы и повышает совместимость.

- **Управление из командной строки** Windows Server 2003 предоставляет расширенную инфраструктуру командной строки, которая позволяет выполнять большинство административных операций, не вызывая графического интерфейса. Особенно важна возможность выполнения широкого диапазона задач через хранилище информации, поддерживаемое Windows Management Instrumentation (WMI). Средство командной строки WMI (WMIC) предоставляет простой интерфейс командной строки, который взаимодействует с существующими командными процессорами (shell) и утилитами, а также легко расширяется с помощью сценариев или других приложений администрирования. Богатые функциональные возможности командной строки Windows Server 2003 в сочетании с готовыми сценариями соперничают со средствами других ОС, часто имеющих большую стоимость владения. Администраторы, привыкшие управлять через командную строку системами UNIX или Linux, могут использовать ее в Windows Server 2003.
- **Кластеры (до 8 узлов)** Данная служба, доступная только в Windows Server 2003, Enterprise Edition и Windows Server 2003, Datacenter Edition, обеспечивает высокую готовность и масштабируемость для критических приложений, таких как базы данных, системы электронных сообщений, а также файл-серверы и серверы печати. Кластеризация реализуется путем обеспечения постоянной связи между несколькими серверами (узлами). Если один из узлов кластера становится недоступен из-за сбоя или при проведении регламентных работ, его сразу замещает другой узел — данный процесс называется переключением при сбое. Пользователи, работавшие с отключенным узлом, продолжают работать, даже не подозревая, что теперь сервис им предоставляет другой компьютер. И Windows Server 2003, Enterprise Edition и Datacenter Edition поддерживают кластеры до 8 узлов.
- **Защищенные беспроводные ЛВС (802.1X)** Благодаря поддержке 802.1X в Windows Server 2003 возможен переход на модель безопасности, гарантирующую аутентификацию и шифрование любого физического доступа. Точки доступа или переключатели 802.1X позволяют гарантировать, что подключиться к защищенной сети и обмениваться с ней пакетами смогут только те системы, которым это разрешено. Так

как 802.1X предоставляет динамическое определение ключа, шифрование в беспроводных сетях 802.1X усовершенствовано с целью устранения многих проблем в Wired Equivalent Privacy (WEP), используемом сетями IEEE 802.11. 802.1X позволяет повысить защищенность и производительность беспроводных ЛВС, включая автоматическое управление ключами, аутентификацию пользователей и авторизацию перед доступом к ЛВС. Обеспечивается также управление доступом к сетям Ethernet при использовании проводного Ethernet в общественных местах.

- **Emergency Management Services: «сервер без головы»** Поддержка «сервера без головы» (headless server) позволяет администраторам устанавливать и управлять компьютером без монитора, видеоадаптера, клавиатуры и мыши. Emergency Management Services — это новое средство, позволяющее администратору выполнять удаленное управление и восстановление, когда сервер недоступен по сети или с помощью других стандартных механизмов и инструментов удаленного администрирования.

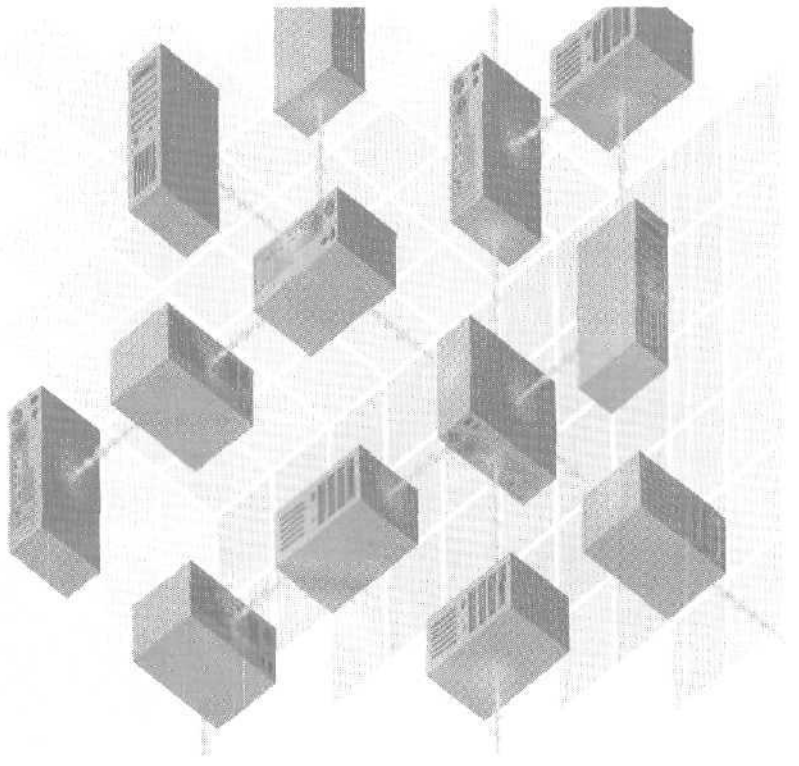
Дополнительные сведения

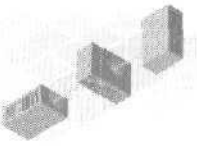
Дополнительную информацию см. по следующим адресам;

- Домашняя страница Windows Server 2003 —http://www.micro - soft.com/ windowsserver2003/;
- What's New in Windows Server 2003 — http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/;
- Характеристики Windows Server 2003 — http://www.microsoft.com/windowsserver2003/evaluation/features/;
- Feature Highlights Sorter http://www.microsoft.com/windowsserver2003/evaluation/features/featuresorter.aspx;
- Business Value of Microsoft Solutions — http://www.microsoft.com/business/solutions/value/valuehome.asp.

ЧАСТЬ II

НОВЫЕ ВОЗМОЖНОСТИ





ГЛАВА
3

Active Directory

Центральный компонент платформы Windows — служба каталогов Microsoft Active Directory -- предоставляет средства управления объектами и взаимосвязями сетевой среды,

Используя в качестве основы ОС Microsoft Windows 2000, Windows Server 2003 улучшает управляемость, упрощает миграцию и развертывание Active Directory. Кроме того, Active Directory в Windows Server 2003 — это наилучший выбор для разработки приложений, использующих службу сетевых каталогов.

Active Directory усовершенствована с целью сокращения совокупной стоимости владения. Новые возможности и расширения на всех уровнях продукта направлены на универсализацию, упрощение администрирования, повышение надежности и снижение затрат.

Основы Active Directory

Active Directory — это служба каталогов для семейства ОС Windows Server 2003. (Active Directory не может работать на Windows Server 2003, Web Edition, однако может управлять компьютером, на котором установлен этот выпуск ОС.)

Active Directory хранит данные об объектах в сети и обеспечивает удобные средства для поиска и использования этих сведений. В качестве основы для логической, иерархической организации информации каталога Active Directory использует структурированное хранилище данных.

Хранилище данных сетевого каталога

Хранилище данных сетевого каталога часто называют просто *каталогом* (directory). Этот каталог содержит сведения о таких объектах, как пользователи, группы, компьютеры, домены, подразделения и правила политики безопасности. Доступ к этой информации может быть предоставлен пользователям и администраторам.

Каталог хранится на серверах, известных как *контроллеры домена,* и доступен сетевым приложениям и службам. Домен может иметь несколько контроллеров. На каждом контроллере располагается изменяемая копия каталога домена, в котором он находится. Изменения каталога на одном из котроллеров реплицируются на другие контроллеры домена, дерева доменов или леса. Репликация каталога и наличие на каждом из контроллеров его копии, доступной для записи, позволяет гарантировать постоянный доступ к каталогу пользователям и администраторам по всему домену.

Данные каталога хранятся на контроллере домена в файле Ntds.dit. Рекомендуется располагать этот файл на дисковом разделе NTFS. Некоторые данные хранятся в файле БД каталога. другие же (такие как сценарии регистрации или правила групповой политики) находятся в реплицируемой файловой системе. Между контроллерами домена выполняется репликация трех категорий данных каталога.

- **Данные домена** Это сведения об объектах внутри домена. Обычно именно их имеют в виду, когда говорят об информации каталога: адресах электронной почты. атрибутах пользователей и компьютеров, а также сетевых ресурсах, представляющих интерес для администраторов и пользователей, Так, при создании нового пользователя в данных домена сохраняется объект его учетной записи. При изменении объекта каталога организации, таком как создание объекта, удаление объекта или изменение его атрибутов, информация об изменении сохраняется в данных домена.
- **Данные конфигурации** Описывают топологию каталога и содержат список всех доменов, деревьев, лесов, а также расположение котроллеров домена и глобальных каталогов (ГК).
- **Данные схемы** Схема — это формальное определение всех объектов и атрибутов, которые могут быть помещены в ка-

талог. Windows Server 2003 предоставляет стандартную схему, определяющую ряд типов, таких как учетные записи пользователей и компьютеров, группы, домены, подразделения и правила политики безопасности. Администраторы и программисты могут расширять схему, определяя новые типы объектов или добавляя новые атрибуты к существующим объектам. Объекты схемы защищены списками управления доступом (access control lists, ACL) гарантирующими, что схему могут изменить только пользователи с соответствующими правами.

Active Directory и безопасность

Средства безопасности интегрированы в Active Directory посредством аутентификации при входе пользователя в систему и контроля доступа к объектам каталога. Единая регистрация в сети позволяет администраторам управлять данными и структурой каталога из любого ее места, а пользователи с соответствующими правами могут получить доступ к любым ресурсам,

Active Directory предоставляет защищенное хранилище учетных записей пользователей и информации о группах за счет контроля доступа к объектам и учетным записям. Так как в Active Directory хранятся не только регистрационные данные пользователя, но и информация об управлении доступом, то пользователь, зарегистрировавшийся в сети, получает как аутентификацию, так и авторизацию доступа к системным ресурсам. Так, при входе пользователя в сеть система безопасности аутентифицирует его с помощью информации, хранящейся в Active Directory. Затем, при попытке пользователя получить доступ к сетевой службе, эта система проверяет свойства, определенные в списке избирательного управления доступом (discretionary access control list — DACL) этой службы.

Поскольку Active Directory позволяет создавать группы пользователей, администраторы могут управлять правами доступа более эффективно. Например, изменив свойства файла, можно разрешить его чтение всем пользователям группы. В этом случае доступ к объектам в Active Directory определяется на основании членства в группе.

Схема Active Directory

Схема Active Directory — это набор определений, задающих виды объектов, а также типы информации об этих объектах, которые могут быть помещены в Active Directory, Так как эти определения также представляют собой объекты, то управлять объектами схемы Active Directory можно так же, как и остальными объектами каталога. В схеме имеются определения двух типов: атрибуты и классы.

Атрибуты и классы (которые также называют объектами схемы или метаданными) можно описать так.

- Классы Классы, или *классы объектов*, описывают допустимые объекты каталога. Каждый класс является набором атрибутов. При создании объекта в атрибуты помещается информация, описывающая объект. Так, класс *User* состоит из массы атрибутов, включая *Network Address* (сетевой адрес), *Home Directory* (домашний каталог) и т. д. Каждый объект Active Directory является экземпляром некоторого класса объектов.
- Атрибуты Атрибуты определяются отдельно от классов. Каждый атрибут определяется только раз и относиться ко многим классам. Так, атрибут *Description,* используемый многими классами, определен в схеме только раз для обеспечения согласованности.

Атрибуты описывают объекты. Каждый атрибут имеет собственное определение, описывающее тип информации, которая может быть задана для данного атрибута. Каждый атрибут в схеме задается классом *AttributeSchema*, определяющим информацию, которую должно содержать любое определение атрибута. Список атрибутов, применимых к объекту, определятся классом, экземпляром которого этот объект является, а также всеми суперклассами класса этого объекта. Атрибуты определяются однажды, но могут быть использованы многократно. Это обеспечивает согласованность между всеми классами, использующими данный атрибут.

- Многозначные атрибуты Атрибуты могут быть однозначными или многозначными. Возможность задания нескольких значений для экземпляра атрибута указывается в опре-

делении этого атрибута в схеме. Экземпляр однозначного атрибута может быть либо пустым, либо содержать единственное значение. Экземпляр многозначного атрибута может быть либо пустым, либо содержать одно или несколько значений. Каждое значение многозначного атрибута должно быть уникальным.

- Индексированные атрибуты Индексы применяются к атрибутам, а не к классам. Индексация атрибута позволяет быстрее находить объекты с данным атрибутом. Если атрибут помечен как индексированный, в индекс добавляются все экземпляры данного атрибута, а не только относящиеся к определенному классу. Введение новых индексированных атрибутов может повлиять на время репликации Active Directory, доступную память и размер БД. Так как размеры БД увеличиваются, время ее репликации возрастает.

  Многозначные атрибуты также могут быть индексированными. Индексирование многозначных атрибутов увеличивает размер Active Directory и время создания объекта существеннее, чем при индексировании однозначных атрибутов. При выборе атрибутов для индексации надо убедиться, что они будут часто использоваться, и задать соотношение между накладными расходами и производительностью.

  Поиск индексированного атрибута схемы может также производиться по контейнеру, в котором хранится данный атрибут, а не по всей БД Active Directory. Это ускоряет поиск и сокращает необходимый для этого объем ресурсов.

Опытные разработчики и сетевые администраторы могут расширять схему динамически путем определения новых классов и новых атрибутов для существующих классов. Содержимым схемы управляет контроллер домена, играющий роль хозяина схемных операций (schema operations master). Копия схемы реплицируется на все контроллеры домена внутри леса. Применение этой общей схемы гарантирует целостность и согласованность данных по всему лесу. Расширить схему также позволяет оснастка Active Directory Schema. Чтобы модифицировать схему, нужно быть членом группы Schema Administrators (либо иметь права на модификацию схемы, выданные вам администратором) и установить оснастку Active Directory Schema на

компьютер — мастер схемных операций. При внесении изменений в схему следует учитывать, что:

- **расширения схемы являются глобальными:** расширяя схему, вы расширяете ее для всего леса, так как любые изменения схемы реплицируются на каждый контроллер каждого домена в лесу;
- **системные классы схемы не могут быть изменены:** нельзя модифицировать стандартные системные классы схемы Active Directory, однако приложения, модифицирующие схему, могут добавить нестандартные системные классы, изменять которые вы можете;
- **расширения схемы могут быть изменены:** некоторые свойства атрибутов или классов могут быть изменены после их создания; новый класс или атрибут, добавленный к схеме, может быть деактивизирован, но не удален, однако вы можете пометить определения как недействительные и заново использовать идентификаторы объектов (OTD) или отображаемые имена, что позволит изменить определение схемы.

Подробнее об изменении схемы ем. Microsoft Windows Resource Kits по адресу *http://www.microsoft.com/reskit*Active Directory не поддерживает удаление объектов схемы; однако объекты могут быть помечены как деактивизированные, что позволяет получить эффект аналогичный удалению.

Глобальный каталог

Глобальный каталог (ГК) — это контроллер домена, на котором хранятся копии всех объектов Active Directory в лесу. В ГК также хранятся те атрибуты каждого объекта, по которым чаще всего выполняется поиск. ГК содержит полную копию всех объектов каталога для домена, в котором он находится, и частичную копию всех объектов из всех других доменов леса, что позволяет выполнять эффективный поиск без лишних обращений к контроллерам доменов.

ГК создается автоматически на первом контроллере домена в лесу. Вы можете активизировать функциональность ГК на других контроллерах домена или переместить его на другой контроллер домена. ГК выполняет следующие функции.

- Поиск объектов ГК обеспечивает поиск информации Active Directory по всем доменам леса независимо от расположения данных. Поиск в лесу выполняется с максимальной скоростью и минимальным сетевым трафиком. Когда вы запускаете поиск человека или принтера из меню Пуск или выбираете опцию Entire Directory в запросе, вы выполняете поиск в ГК. Введенный поисковый запрос направляется в стандартный порт ГК и отсылается в ГК для выполнения.
- **Аутентификация идентификаторов пользователей** ГК служит для поиска идентификатора пользователя, когда выполняющий аутентификацию контроллер домена не имеет регистрационной записи данного пользователя. Так, если учетная запись расположена в *examplel.microsoft.com,* а пользователь пытается войти в систему под именем *user1@example1.microsoft.com* на компьютере, расположенном в *example2.microsoft.com*, контроллер домена *example2.microsoft.com* не сможет найти учетную запись и обратится для завершения процесса входа пользователя в систему к серверу ГК.
- **Поддержка информации о членстве в универсальных группах в многодоменной среде** В отличие от членства в глобальных группах, информация о котором хранится в каждом домене, информация о членстве в универсальных группах хранится только в ГК. Например, когда член универсальной группы входит в домен, работающий на стандартном функциональном уровне домена Windows 2000 или более высоком, ГК предоставляет информацию о членстве пользователя в универсальных группах. Если ГК недоступен при входе в домен, исполняемый ОС Windows 2000 или более старшей, компьютер задействует кэшированную информацию, если этот пользователь уже входил в данный домен ранее. Если же он никогда раньше не входил в этот домен, он сможет войти только на локальный компьютер.

Примечание Члены группы Domain Administrators могут входить в сеть, даже когда ГК недоступен.

Поиск информации в Active Directory

Active Directory предназначена для обработки запросов поиска объектов каталога со стороны пользователей и программ.

Администраторы и пользователи могут искать и находить информацию в каталоге посредством команды Найти в меню Пуск. Клиентские программы могут получить доступ к данным в Active Directory посредством Active Directory Services Interface (ADSI).

Одним из основных преимуществ Active Directory является хранение разнообразной информации о сетевых объектах. Помещаемая в Active Directory информация о пользователях, компьютерах, файлах и принтерах доступна пользователям сети. Доступ к информации управляется правами доступа.

При исполнении разного рода сетевых задач требуется взаимодействие с другими пользователями или подключение к сетевым ресурсам. При этом нужно отыскать соответствующие имена или адреса. С этой точки зрения Active Directory функционирует как общая адресная книга предприятия. Так, вы можете найти пользователя по имени, фамилии, адресу электронной почты, расположению в офисе или другим свойствам его учетной записи . Поиск оптимизирован с помощью ГК.

Диалоговые окна Advanced Find в оснастке Active Directory Users And Computers позволяют администраторам повысить эффективность выполнения задач управления, а также легко настраивать отображение и фильтрацию данных, выбираемых из каталога. Кроме того, администраторы могут быстро и с минимальным использованием сетевых ресурсов добавлять объекты к группам, применяя для поиска вероятных членов группы запросы, а не просмотр.

Репликация Active Directory

Репликация каталога обеспечивает гарантированный постоянный доступ к данным, отказоустойчивость, равномерное распределение нагрузки и повышение производительности. Active Directory использует многостороннюю (multimaster) репликацию, что позволяет изменять каталог не на единственном первичном котроллере, но на любом контроллере домена. Многосторонняя модель обладает большей отказоустойчивостью, так как при наличии нескольких контроллеров домена репликация продолжается, даже если один из них не работает. Контроллер домена хранит и реплицирует следующие виды информации.

- **Информация схемы** Определяет объекты, которые могут быть созданы в Active Directory, а также атрибуты, которые

эти объекты могут иметь. Данная информация является общей для всех доменов леса. Данные схемы реплицируются на все контроллеры доменов леса.

- **Информация конфигурации** Описывает логическую структуру сети и содержит такую информацию, как структура доменов и топология репликации. Эта информация является общей для всех доменов леса. Данные конфигурации реплицируются на все контроллеры доменов леса.
- **Информация домена** Описывает все объекты домена. Эти данные являются специфичными для домена и не распространяются в другие домены. С целью сквозного поиска информации по дереву или лесу доменов подмножество свойств всех объектов всех доменов хранится в ГК. Данные домена реплицируются на все контроллеры этого домена.
- **Информация приложений** Информация, хранящаяся в прикладном разделе каталога, предназначена для случаев, когда репликация необязательна в глобальном масштабе. Данные приложений могут явно перенаправлены на указанные администратором контроллеры домена внутри леса во избежание лишнего трафика репликации, либо для них может быть задана репликация на все контроллеры внутри домена.

Сайты повышают эффективность репликации Active Directory. Информация схемы и конфигурации реплицируется по всему лесу, а домена — по всем контроллерам внутри домена и частично — в ГК. Сократив объем репликации, вы сократите нагрузку на сеть. Контроллеры доменов используют сайты и управление репликацией (replication change control) для оптимизации репликации:

- периодически оценивая используемые соединения, Active Directory выбирает наиболее эффективные сетевые соединения;
- для обеспечения отказоустойчивости Active Directory использует для репликации изменений несколько маршрутов;
- накладные расходы на репликацию сокращаются за счет того, что реплицируется только измененная информация.

Если при развертывании сети не были организованы сайты, обмен данными между контроллерами доменов и клиентами может быть хаотичным. Сайты повышают эффективность сети. Active Directory реплицирует информацию внутри сайта

чаще, чем между сайтами. Таким образом, контроллеры домена, связь между которыми имеет наилучшие параметры и которым с наибольшей вероятностью потребуется соответствующая информация из Active Directory, получают реплики в первую очередь. Контроллеры доменов в других сайтах получают все изменения Active Directory, но не так часто, что снижает загрузку сети. Дополнительно она снижается за счет сжатия данных при репликации между сайтами. Для повышения эффективности обновления выполняются, только когда в каталог добавляется новая информация либо когда изменяется текущая информация каталога.

Постоянное распространение изменений каталога на все другие контроллеры домена приводит к загрузке сети. Репликация оптимизируется вручную или автоматически — с помощью Active Directory Knowledge Consistency Checker (KCC) на основании информации, задаваемой вами с помощью административного инструмента Active Directory Sites And Services. KCC отвечает за настройку и поддержание топологии репликации Active Directory. В частности, KCC определяет, когда будет выполняться репликация, а также набор серверов, с которыми будет обмениваться данными данный сервер.

Клиенты Active Directory

При установке клиента Active Directory многие возможности Active Directory, доступные в Windows 2000 Professional или Microsoft Windows XP Professional, становятся доступными на компьютерах с Windows 95/98/NT 4.

- **Поддержка сайтов** Вы можете входить в сеть через контроллер домена, расположенный ближе всего к данной рабочей станции.
- **Active Directory Services Interface** Вы можете управлять Active Directory, применяя сценарии. ADSI также предоставляет стандартный API доступа к Active Directory для программистов.
- **Отказоустойчивый клиент Distributed File System (DFS)** Вы можете работать с Windows 2000 и серверами, на которых хранятся общие каталоги файловой системы Windows .NET DFS, указанные в Active Directory.

- **Аутентификация NTLM версии 2** Вы можете задействовать усовершенствованные средства аутентификации Windows NT Challenge/Response Authentication (NTLM) версии 2. Подробнее об активизации NTLM версии 2 см. статью Q239869 «How to Enable NTLM 2 Authentication» в Microsoft Knowledge Base по адресу *http://support.microsoft.com/*.
- **Страницы свойств Active Directory Windows Address Book (WAB)** Вы сможете изменять такие свойства, как номер телефона или адрес, на страницах свойств объекта «пользователь».
- **Поиск в Active Directory** Из меню Пуск вы сможете выполнять поиск принтеров и людей в доменах Windows 2000 Server или Windows .NET. О регистрации принтеров в Active Directory см. статью Q234619 «Publishing a Printer in Windows Active Directory» в Microsoft Knowledge Base по адресу *http://support.microsoft.com/*.

Windows 2000 Professional и Windows XP Professional предоставляют возможности, не поддерживаемые клиентом Active Directory для Windows 95/98/NT 4, включая Kerberos версии *5.* поддержку групповой политики и технологии IntelliMirror, а также имена пользователей для служб (service principal name) или взаимную аутентификацию. Чтобы задействовать эти дополнительные возможности, нужно перейти на Windows 2000 Professional/XP Professional. Подробнее см. следующие ресурсы:

- переход на Windows 2000 — http://www.microsoft.com/ windows2000/professional/howtobuy/upgrading/;
- Windows XP Professional Upgrade Center — http://www.microsoft. com/windowsxp/pro/howtobuy/upgrading/;
- страница клиента Active Directory — http://www.microsoft.com/ windows-2000/server/evaluation/news/bulletins/adextension.asp.

Интеграция и продуктивность

Интерфейсы Active Directory (как программные, так и пользовательские) усовершенствованы с целью повышения эффективности администрирования и возможностей интеграции.

Управление Active Directory

Ряд новых средств, в том числе улучшения в оснастках Microsoft Management Console (MMC) и диалоге выбора объектов (object picker), упрощают работу с Active Directory. Компоненты расширения MMC позволяют администрировать наборы объектов. Например, администраторы теперь смогут делать следующее.

- **Выбирать и редактировать свойства нескольких объектов одновременно.**
- **Сохранять запросы** к Active Directory для использования в будущем; результаты могут быть экспортированы в формат XML.
- **Быстро выбирать объекты, используя усовершенствованный компонент выбора объектов** (object **picker).** Переработка этого компонента позволила повысить удобство работы и эффективность поиска объекта в большом каталоге, а также реализовать более гибкие запросы. Он применяется в большом количестве мест пользовательского интерфейса и доступен для сторонних разработчиков.

Дополнительные средства повышения продуктивности

Дополнительные средства повышения продуктивности работы с Active Directory включают следующие.

- **Изменения интерфейса редактирования ACL** Этот интерфейс улучшен с целью повышения удобства работы и отображения унаследованных прав доступа в противоположность правам доступа, назначенным непосредственно на данный объект.
- **Новые возможности расширения** Администратор, работающий с программным или аппаратным продуктом независимого производителя, применяющего Active Directory, получает расширенные возможности управления и может добавить к группе любой класс объектов.
- **Объекты-пользователи из других каталогов, поддерживающих протокол LDAP (Lightweight Directory** Access **Protocol)** Объекты-пользователи, определенные в LDAP-каталогах, применяющих класс *inetOrgPerson* согласно спецификации RFC 2798 (например, разработанные Novell и Netscape), могут определяться через пользовательский интерфейс Active Direc-

tory. Тот же интерфейс, что работает с объектами-пользователями Active Directory, будет работать с объектами *inetOrgPerson*. Теперь любой пользователь или приложение легко могут работать с классом *inetOrgPerson*.

- **Интеграция Passport (с помощью US)** Passport-аутентификация теперь поддерживается IIS 6.0, что позволяет отображать объекты-пользователи на их Passport-идентификацию (если она есть). IIS 6.0 устанавливает для HTTP-запросов от таких пользователей маркер доступа, создаваемый Local Security Authority (LSA). Пользователи Интернета, имеющие Passport, теперь могут использовать его для доступа к ресурсам так же, как если бы они использовали свои учетные данные из Active Directory.
- **Использование Terminal** Server с **ADSI** Свойства пользователя Terminal Server можно установить путем исполнения сценария с применением Active Directory Services Interface (ADSI). Возможность задавать свойства пользователя не только вручную через интерфейс Active Directory, но и из сценария облегчает реализацию массированных или программируемых изменений посредством ADSI.
- **Свойства WMI для мониторинга репликации и доверительных отношений** Классы Windows Management Instrumentation (WMI) могут выполнять мониторинг успешности репликации информации Active Directory между контроллерами домена. Так как многие компоненты Windows 2000, в том числе репликация Active Directory, используют междоменные доверительные отношения, это средство обеспечивает верификацию корректного функционирования доверительных отношений. Теперь через WMI можно легко уведомлять администраторов и обслуживающий персонал о проблемах репликации.
- **Списки рассылки MSMQ** В Message Queuing (MSMQ) добавлена поддержка отправки сообщений в списки рассылки (distribution lists), которые хранятся в Active Directory. Пользователи MSMQ могут легко управлять списками рассылки средствами Active Directory.

Производительность и масштабируемость

В механизмы репликации и синхронизации данных Active Directory в Windows Server 2003 внесены существенные изменения.

Поддержка филиалов

Обычно в многофилиальной компании сеть состоит из массы удаленных офисов, каждый из которых имеет свои контроллеры домена, но соединен с центральным офисом медленным каналом. В Windows Server 2003 процесс входа пользователя в систему из периферийного офиса усовершенствован, так как теперь доступ к центральному серверу ГК не требуется всякий раз, когда пользователь входит в сеть. Теперь организациям не нужно развертывать сервер ГК в периферийных офисах с ненадежной сетью.

Вместо того чтобы при всякой регистрации сервера на контроллере домена обращаться к ГК, контроллер домена кэширует информацию о членстве в глобальных группах для тех пользователей, которые ранее подключались к системе с этого сайта или с внешних серверов ГК, когда сеть была доступна. Теперь таким пользователям разрешается вход в систему, причем контроллеру домена пет нужды в этот момент обращаться к серверу ГК, что снижает число обращений по медленным или ненадежным сетям. Кроме того, это улучшение повышает надежность, позволяя обрабатывать вход пользователя в систему, когда ГК недоступен.

Другие улучшения производительности

Ниже перечислены дополнительные улучшения производительности Active Directory.

- **Отключение сжатия данных при репликации между сайтами** **Сжатие данных при репликации между контроллерами** домена, располагающимися на разных сайтах, можно отключить. Это позволяет повысить производительность, снизив загрузку процессора на контроллерах домена.
- **Поддержка кластеризованных виртуальных серверов** Теперь определен объект-компьютер для кластеризованных серверов. Приложения, поддерживающие кластеры и Active

Directory, могут связывать свою настроечную информацию со стандартным объектом,

- **Параллельные LDAP-привязки** На одном соединении допускается установление нескольких LPAP-привязок с целью аутентификации пользователей. Включив эту возможность, разработчики приложения могут повысить производительность LPAP-привязок и аутентификационных запросов к Active Directory.
- **Защита от перегрузок контроллеров домена** Это средство предотвращает перегрузку первого контроллера домена Active Directory, вводимого в домен, который уже содержит большое число членов с обновленной Windows 2000 и Windows Server 2003.

  Домен Windows NT Server 4 содержит клиентские и серверные компьютеры, на которых установлены Windows 2000 и Windows Server 2003. При обновлении первичного контроллера домена путем установки Windows 2000 Service Pack 2 (SP2) или Windows Server 2003 он может быть настроен на эмуляцию поведения контроллера домена Windows NT 4. Члены домена с Windows 2000 Server 2003 не будут отличать обновленные контроллеры домена от контроллеров домена Windows NT 4.

  Члены домена, на которых установлена Windows 2000 SP2/Server 2003, можно настроить так, чтобы сообщать контроллерам домена с Windows 2000 SP2/Server 2003 о необходимости отключать при работе с ними эмуляцию Windows NT 4.
- **Настройка репликации ГК** В доменах Windows Server 2003 с репликацией ГК состояние синхронизации ГК сохраняется, а не сбрасывается, что снижает объем данных генерируемых в результате Partial Attribute Set (PAS), благодаря тому, что пересылаются только добавленные атрибуты. В результате достигается эффект уменьшения объема трафика репликации и более эффективные PAS-обновления.
- **Усовершенствования репликации членства в группах** Когда лес доменов переводится в режим Windows Server 2003 Forest Native Mode, информация о членстве в группах начинает храниться и реплицироваться для отдельных членов, а не в виде единого куска для всей группы. В итоге снижается загрузка сети и процессора во время репликации, а также прак-

тически исчезает вероятность потери данных при одновременных обновлениях.

- **Поддержка в LDAP задания времени жизни (Time to Live,** TTL) **для динамических записей** В Active Directory могут храниться динамические записи. Для таких записей задается значение TTL. Пользователь может изменить его, продлив таким образом время жизни записи. LDAP API для языка C был расширен с включением поддержки этой новой возможности. Разработчики приложений теперь могут помешать в Active Directory информацию, которая не должна сохраняться длительное время, но автоматически удаляться Active Directory по истечении TTL,
- **Поддержка развертывания 64-битных приложений** Новые параметры групповой политики в Application Deployment Editor (ADE) позволяют указать, должны ли 32-битные приложения устанавливаться на 64-битные клиенты. Групповая политика позволяет гарантированно устанавливать на 64-битные клиенты только соответствующие приложения.

Администрирование и управление конфигурацией

Windows Server 2003 расширяет возможности эффективной настройки и управления Active Directory даже в очень больших сетях с большим числом лесов, доменов и сайтов.

Новые мастера установки

Новый мастер Configure Your Server облегчает установку Active Directory и предлагает предопределенные параметры для конкретных серверных ролей, что помогает администраторам стандартизовать параметры начального развертывания серверов. В процессе установки сервера администраторы могут разрешить пользователям завершить установку дополнительных компонентов, выбранных ими при установке Windows. Мастер Configure Your Server позволяет;

- установить первый сервер в сети с автоматической настройкой DHCP, DNS и Active Directory, используя базовые начальные параметры;
- помочь пользователям в настройке других серверов сети, указав на средства, необходимые им для установки файл-сер-

вера, сервера печати, Web и медиа-сервера, сервера приложений, сервера удаленного доступа (RAS) и маршрутизации или сервера управления IP-адресами.

Администраторы могут задействовать это средство для восстановления при сбоях, репликации серверной конфигурации на несколько компьютеров, завершения установки, настройки ролей сервера или конфигурирования первого или первичного сервера сети.

Другие усовершенствования в области администрирования

В области администрирования Active Directory также имеются другие усовершенствования.

- **Автоматическое создание зон DNS** Зоны и серверы Domain Name System (DNS) в ОС семейства Windows Server 2003 могут быть созданы и настроены автоматически. Они создаются в сети для размещения новой зоны. Это может существенно ускорить настройку каждого сервера DNS.
- **Усовершенствованный генератор топологии межсайтовой репликации** Средство Inter-Site Topology Generator (ISTG) использует теперь улучшенные алгоритмы, масштабируемые для поддержки лесов с большим числом сайтов, чем в Windows 2000. Так как все контроллеры доменов в лесу, исполняющие роли ISTG, должны договориться между собой о топологии межсайтовой репликации, новые алгоритмы не применяются, пока лес не переведен в режим Windows Server 2003 Forest Native Mode. Новые алгоритмы ISTG обеспечивают повышение производительности репликации между лесами.
- **Усовершенствования настройки DNS** Данное средство упрощает отладку и выдачу информации о неверной конфигурации DNS и помогает правильно настраивать инфраструктуру DNS, необходимую для работы Active Directory.

Один из примеров преимуществ нового средства — продвижение контроллера домена в существующем лесу, когда Active Directory Installation Wizard связывается с существующим контроллером домена для обновления каталога и репликации нужной его части. Если мастер не нашел контроллер домена из-за неверной настройки DNS или из-за того, что контроллер доме-

на недоступен, мастер анализирует причины ошибки и выдает информацию о ней, а также рекомендации по ее устранению.

Чтобы контроллер домена можно было отыскать в сети, он должен зарегистрировать в DNS записи поиска контроллера домена (domain controller locator). Мастер Active Directory Installation проверяет правильность настройки инфраструктуры DNS, чтобы позволить новому контроллеру домена динамически обновить свои записи в DNS. Если проверка обнаруживает неверную конфигурацию инфраструктуры DNS, пользователю выдается информация об этом с рекомендациями по исправлению ошибок.

- **Установка реплик из резервных копий** Вместо репликации полной копии БД Active Directory по сети. данная возможность позволяет администратору указать в качестве источника начальной репликации файлы, созданные при резервном копировании существующего контроллера домена или сервера ГК. Файлы резервной копии, созданные с помощью любой утилиты резервного копирования, поддерживающей Active Directory, можно перенести на вновь создаваемый контроллер домена, применяя такие носители, как магнитная лента, CD, DVD, или копируя файлы по сети,
- **Расширения инструментов миграции** Инструмент Active Directory Migration Tool (ADMT) в Windows Server 2003 усовершенствован и предоставляет следующие возможности.
  - D **Миграция паролей** ADMT версии 2 обеспечивает миграцию паролей из доменов Windows NT 4 в домены Windows 2000/Server 2003, а также из доменов Windows 2000 в домены Windows Server 2003.
  - □ **Новый интерфейс для сценариев** Позволяет выполнять миграцию пользователей, групп и компьютеров; теперь ADMT поддерживает COM-интерфейсы, и им можно управлять с помощью любого языка, в том числе Microsoft Visual Basic Scripting Edition (VBScript), Microsoft Visual Basic и Microsoft Visual C++.
  - □ **Поддержка командной строки** **Все** задачи, которые могут быть выполнены сценариями, вы вправе исполнять прямо из командной строки или с помощью командных файлов.

- **Усовершенствования в трансляции параметров защиты** Трансляция параметров защиты, например, повторное применение ресурсов в ACL, усовершенствована так, что исходный домен может быть лишен полномочий (decommissioned) при трансляции защиты; теперь ADMT позволяет задать файл преобразований, используемый в качестве входной информации для трансляции; ADMT версии 2 упрощает переход на Active Directory и предоставляет дополнительные возможности для автоматизации процесса.

- **Прикладные разделы** каталога Active Directory поддерживает создание контекста имен или раздела нового типа — *прикладного раздела* (application partition). Такой контекст имен может содержать иерархию объектов любого типа, кроме участников безопасности (security principal) (пользователей, групп и компьютеров), и для него может быть настроена репликация в любые контроллеры доменов леса, а не только внутри текущего домена.

  Это средство обеспечивает размещение в Active Directory динамических данных без существенного снижения производительности сети благодаря возможности управления границами репликации и размещением реплик.

- **Хранение интегрированных зон DNS в прикладных разделах** Зоны DNS могут храниться и реплицироваться прикладными разделами Active Directory. Хранение данных DNS в прикладных разделах позволяет сократить количество объектов, хранимых в ГК. Кроме того, при этом данные зоны DNS реплицируются только на котроллеры доменов, указанные для этою раздела. По умолчанию прикладные разделы для DNS содержат только те контроллеры доменов, на которых установлены серверы DNS. Кроме того, хранение зоны DNS в прикладном разделе позволяет реплицировать эту зону на серверы DNS, установленные па котроллерах других доменов леса Active Directory. Интеграция зон DNS в прикладные разделы позволяет ограничить репликацию этой информации и снизить требования к пропускной способности сети.

- **Усовершенствования элемента управления DirSync** В Active Directory усовершенствована поддержка DirSync — элемента управления LDAP — для выборки из каталога измененной

информации. DirSync может выполнять проверки, аналогичные тем, что производятся при обычных LDAP-поисках.

- **Уровни функциональности** Аналогично основному режиму домена в Windows 2000 данное средство предоставляет механизм версий, используя который, компоненты ядра Active Directory могут определять возможности, доступные каждому контроллеру в домене и в лесу- Оно применяется также для предотвращения включения контроллеров доменов, на которых установлены версии ОС, предшествующие Windows Server 2003, в лес, для которого установлен режим «только Windows Server 2003».
- **Деактивизация классов и атрибутов схемы** Усовершенствования в Active Directory позволяют деактивизировать определения атрибутов и классов схемы Active Directory. Атрибуты и классы могут быть определены заново. если в первоначальном определении содержалась ошибка.

  Деактивизация позволяет замешать определения уже добавленного в схему атрибута или класса, если при задании значения неизменяемого свойства имела место ошибка. Поскольку эта операция обратима, администратор вправе отменить случайную деактивизацию без побочных эффектов.
- **Переименование доменов** Данное средство поддерживает изменение имен DNS и NetBIOS существующих доменов леса. гарантируя, что новый лес будет по-прежнему *правильно сформирован* (well formed). Идентификация переименованного домена осуществляется посредством глобально уникального идентификатора (GUID), а идентификатор зашиты домена (SID) не меняется. При переименовании домена членство компьютеров в нем не нарушается.

  Это средство не позволяет изменить корневого домена леса. Хотя последний может быть переименован, другой домен не может быть указан в качестве нового корня.

  Переименование домена потребует прерывания нормальной работы и перезагрузки всех контроллеров доменов. Кроме того, переименование домена требует двукратной перезагрузки каждого члена переименованного домена. Это средство официально поддерживается как способ переименования домена, однако его нельзя рассматривать в качестве регулярно выполняемой операции.

- **Обновление версии леса и ломенов** В Active Directory введены усовершенствования в области безопасности и поддержки приложений. Прежде чем в существующем лесу или домене можно будет обновить первый контроллер домена, на котором установлена ОС Windows Server 2003, данный лес или домены должны быть к этому подготовлены. Для обновления леса и доменов предназначена новая утилита Adprep. Она не требуется при обновлении с Windows NT 4 или при первой установке Active Directory на серверах с ОС Windows Server 2003.
- **Мониторинг репликации и доверительных отношений** Администраторы получают возможность мониторинга успешности репликации информации Active Directory между контроллерами доменов. Поскольку многие компоненты Windows .NET, такие как репликация Active Directory, используют междоменные доверительные отношения, данное средство также предоставляет метод верификации корректного функционирования доверительных отношений.

Управление групповой политикой

Microsoft Group Policy Management Console (GPMC) — новое решение для управления групповой политикой (Group Policy) — позволяет снизить расходы на управление сетью. В состав GPMC входит новая оснастка Microsoft Management Console (MMC) и набор интерфейсов управления групповой политикой, доступный из сценариев. На момент выхода Windows Server 2003 GPMC предполагается поставлять в качестве отдельного компонента. GPMC предназначена для решения следующих задач.

- Упрощение управления групповой политикой за счет сосредоточения всех основных параметров управления в одном месте. GPMC можно рассматривать как единый центр управления групповой политикой.
- Реализация основных требований пользователей к развертыванию групповой политики путем предоставления:
  - a пользовательского интерфейса, значительно облегчающего работу с групповой политикой;
  - D резервного копирования и восстановления объектов групповой политики (group policy object — GPO);

D поддержки для GPO операции импорта/экспорта и копирования/вставки, а также фильтров Windows Management Instrumentation (WMI);

а упрощенного управления аспектами безопасности, связанными с групповой политикой;

D вывода параметров настройки GPO в формате HTML:

□ вывода в формате HTML данных Group Policy Results и Group Policy Modeling (ранее известных как Resultant Set of Policy);

П выполнение из сценариев операций над GPO, доступных из этого средства, но не доступ из сценариев к самим GPO,

До GPMC администраторы использовали для управления групповой политикой несколько инструментов. GPMC интегрирует эти инструменты в единую, унифицированную консоль и расширяет их возможности.

Управление доменами

GPMC позволяет управлять доменами как Windows 2000, так и Windows Server 2003 с установленной Active Directory. В обоих случаях на компьютере администратора, где исполняется этот инструмент, должна быть установлена одна из следующих ОС:

- Windows Server 2003;
- Windows XP Professional с Service Pack 1 (SP1) плюс дополнительный post-SP1 hot fix, а также Microsoft .NET Framework.

Другие усовершенствования групповой политики

Дополнительные улучшения поддержки групповой политики в Active Directory таковы.

- Контейнеры для новых пользователей и компьютеров Windows Server 2003 содержит инструмент автоматического направления новых объектов (пользователей и компьютеров) в заданные организационные подразделения (ОП), где к ним может быть применена групповая политика.

  Это позволяет избежать ситуации, в которой новые объекты остаются в стандартных контейнерах на корневом уровне домена. Такие контейнеры не предназначены для хранения связей групповой политики, и клиенты не могут считы-

вать и применять глобальную политику из этих контейнеров, В итоге многим клиентам, использующим такие контейнеры, приходится устанавливать правила на уровне домена, а это не всегда удобно.

Взамен Microsoft рекомендует создать логическую иерархию ОП для хранения вновь создаваемых объектов. Задать альтернативные значения по умолчанию для трех старых API: *NetUserAdd*,*NetGroupAdd*, и *NetJoinDomain* — администраторы могут новыми инструментами из Resource Kit: RedirUsr и ReDirComp. Это позволяет использовать по умолчанию подходящие ОП и применить групповую политику непосредственно к ним.

- **Результирующая групповая политика** Результирующая групповая политика (Group Policy Results) позволяет администраторам определять и анализировать текущие правила политики, применяемые к целевому объекту. Администраторы могут просматривать текущие правила политики на клиентских компьютерах. Ранее результирующая групповая политика была известна как режим регистрации в Resultant Set of Policy.
- **Моделирование групповой политики (Group Policy Modeling)** Позволяет задавать сценарии «что, если» и просматривать для них параметры правил политики, приложений и зашиты. Администратор может провести серию тестов с целью установить, что произойдет с пользователем или группой пользователей, если они будут перемешены в другое место, лругую группу защиты или даже на другой компьютер. В состав получаемой информации входит то, какие правила политики будут применены и какие файлы будут автоматически загружены в результате будет сделаного изменения.

Новые параметры политики

Windows Server 2003 включает более 150 новых параметров политики, которые позволяют настраивать и управлять поведением ОС для групп пользователей. Новые параметры влияют на такие аспекты поведения, как сообщения об ошибках, Terminal Server, диалог настройки сетевых параметров, DNS, запросы на вход в сеть, групповые политики и «блуждающие» профили (roaming profiles).

- **Web-представление административных шаблонов** Расширяет оснастку Group Policy Administrative Template, позволяя просматривать подробные сведения о параметрах политики. При выборе некоторого параметра политики информация о его поведении и возможности применения отображается в Web-представлении пользовательского интерфейса управления административными шаблонами. Эти данные также имеются на вкладке Expand страницы свойств каждого параметра политики.
- **Управление DNS-клиентом** Администраторы могут использовать групповую политику для настройки параметров DNS-клиента на Windows Server 2003. Это упрощает конфигурирование членов домена при изменении таких параметров клиентов DNS, как включение/отключение динамической регистрации клиентами записей в DNS, применение подстановки (devolution) суффикса первичного DNS при разрешении имен и заполнение списков поиска суффиксов DNS.
- **Перенаправление для папки Мои Документы** Позволяет перевести пользователей со старой модели домашних каталогов на модель Мои Документы, сохраняя совместимость с текущей средой домашних каталогов.
- **Полная установка заданных пользователем приложений в момент входа в сеть** Инструмент Application Deployment Editor предоставляет новую возможность, позволяющую выполнять полную установку определенных пользователей приложений в момент входа в сеть, а не по требованию. Администраторы могут гарантировать автоматическую установку нужного ПО на компьютеры пользователей.
- **Netlogon** Позволяет применять групповую политику для настройки параметров Netlogon лля компьютеров с Windows Server 2003. Это упрощает конфигурирование членов домена при таких значениях параметров Netlogon, как включение/отключение динамической регистрации контроллерами домена своих записей поиска в DNS, периодичность обновления таких записей и ряд других часто используемых параметров Netlogon.
- **Параметры настройки сетевых соединений** Доступ пользователей к интерфейсу настройки параметров сети в Windows Server 2003 можно ограничить путем групповой политики.

- **Политика распределенной обработки сообщений** Инфраструктура обработки событий WMI модернизирована для работы в распределенной среле. В состав расширений входят компоненты конфигурирования подписки, фильтрации, коррелирования, агрегирования и транспортировки событий WMI. Независимый производитель ПО может путем добавления пользовательского интерфейса и определения типа правил политики реализовать мониторинг функционирования, регистрацию событий, уведомления, автовосстановление и биллинг.
- **Отключение Credential Manager** Этот новый инструмент облегчает управление регистрационными записями пользователей. Групповая политика позволяет отключить Credential Manager.
- **Поддержка URL при развертывании программных средств** Предоставляет средства указания URL поддержки для пакета. Пользователь может для приложений, отображаемых в диалоге Добавить/Удалить Программы, выбрать Support Information URL и отобразить Web-страницу поддержки. Это позволяет сократить число обращений в группу технической поддержки.
- **Фильтрация WMI** Windows Management Instrumentation (WMI) генерирует для заданного компьютера большой объем данных, таких как список аппаратных и программных средств. параметры и конфигурационная информация. В качестве источников данных WMI использует реестр, драйверы, файловую систему, Active Directory, Simple Network Management Protocol (SNMP), службу Windows Installer, язык SQL, сетевую подсистему и Exchange Server. WMI Filtering в Windows Server 2003 позволяет динамически определять, применять ли GPO на основании запроса к данным WMI. Эти запросы (называемые также WMI-фильтрами) определяют, какие пользователи и компьютеры получают параметры политики, указанные в GPO. Данная функциональность позволяет автоматически определять цели групповой политики на основании свойств локального компьютера.

  Например, может существовать GPO, назначающий Office XP пользователям в некотором ОП. Однако администратор не уверен, все ли компьютеры этого ОП имеют достаточ-

ный объем дискового пространства для установки данного ПО. В этом случае для GPO можно задать WMI-фильтр, который назначает Office XP только тем пользователям, на компьютерах которых имеется более 400 МБ свободного места на жестком диске.

- **Terminal Server** Групповая политика позволяет задать правила пользования Terminal Server, в частности, принудительную установку средств перенаправления, парольного доступа и фона экрана.

Усовершенствования в области безопасности

Поддержка Active Directory в Windows Server 2003 была расширена средствами безопасности, облегчающими управление множественными лесами и междоменными доверительными отношениями. Кроме того, новый Credential Manager предоставляет безопасное хранилище учетных записей пользователей и сертификатов X.509.

Доверительные отношения между лесами

Доверительные отношения между лесами (forest trust) облегчают управление безопасностью между лесами и позволяет доверяющему лесу вводить ограничения на имена участников безопасности, аутентификацию которых он доверяет другим лесам. Вот их основные свойства:

- все домены одного леса (транзитивно) могут доверять всем доменам другого леса посредством единственной доверительной связи между корневыми доменами двух лесов;
- они нетранзитивны на уровне леса между тремя и более лесами; если лес A доверяет лесу B и лес B доверяет лесу C, то это не создает доверительных отношений между лесами A и C;
- они могут быть одно- и двусторонними;
- новый мастер упрощает создание всех типов доверительных отношений, в особенности отношений между лесами;
- новая страница свойств позволяет управлять доверительными пространствами имен (trusted namespace), связанными с доверительными отношениями между лесами;

- доверительные пространства имен служат для перенаправления запросов аутентификации и авторизации участников защиты, чьи учетные записи управляются лесом, для которого установлено доверие;
- публикуемые лесом пространства имен доменов, идентификаторов пользователей (user principal name, UPN), идентификаторов служб (service principal name, SPN) и безопасности (security identifier, SID) автоматически собираются при создании доверительных отношений между лесами и обновляются через пользовательский интерфейс Active Directory Domains And Trust;
- доверие для публикуемых лесом пространств имен оказывается по правилу «первый пришел, первым обслужен», пока они не вступают в конфликт с доверительными пространствами имен из существующих доверительных отношений между лесами;
- перекрытие доверительных пространств имен предотвращается автоматически; администраторы могут вручную отключать отдельные доверительные пространства имен,

Другие усовершенствования в области безопасности

Дополнительные усовершенствования в области безопасности Active Directory включают следующие.

- **Межлесная аутентификация** Обеспечивает безопасный доступ к ресурсам, когда учетная запись пользователя расположена в одном лесу, а учетная запись компьютера -- в другом. Эта возможность обеспечивает пользователям безопасный доступ к ресурсам в другом лесу с применением Kerberos или NTLM, сохраняя при этом преимущества однократного входа в сеть и простоты администрирования единой записи пользователя и пароля, хранящихся в домашнем лесу пользователя. Межлесная аутентификация включает такие возможности.
  - **Разрешение имен** Если Kerberos или NTLM не могут разрешить имя участника безопасности с помощью локального контроллера домена, выполняется обращение к ГК. Если имя не может быть разрешено ГК, вызывается новая функция межлесного сопоставления имен. Эта функция сопоставления имен сравнивает имя участника бе-

зопасности с именами в доверительных пространствах имен всех лесов, которым доверяет данный лес. При нахождении совпадения возвращается имя леса, используемое в качестве адреса перенаправления (routing hint).

- D **Перенаправление запросов** Kerberos и NTLM используют адреса перенаправления для передачи запросов аутентификации по доверительным отношениям из исходного домена в вероятный целевой домен, Для Kerberos центры распределения ключей (Key Distribution Center, KDC) генерируют ссылки на путь доверительных отношений. и клиент следует им, используя стандартные алгоритмы Kerberos. Для NTML контроллеры домена отправляют запрос по защищенным каналам вдоль пути доверительных отношений, применяя сквозную (pass-through) аутентификацию.
- D **Поддерживаемая аутентификация** В состав поддерживаемых методов аутентификации входят Kerberos и сетевая регистрация NTLM при удаленном доступе к серверу в другом лесу, Kerberos и интерактивная регистрация NTLM при физической регистрации вне домашнего леса пользователя, а также Kerberos-делегирование для многоуровневых приложений в другом лесу. Полностью поддерживаются параметры регистрации UPN.

■ **Межлесная авторизация** Позволяет администраторам легко выбирать пользователей и группы из доверительных лесов для включения в локальные группы или ACL. Данное средство поддерживает целостность границы безопасности леса, в то же время обеспечивая доверительные отношения между лесами. Она позволяет доверяющему лесу ограничить список допустимых идентификаторов защиты (SID) при обращении пользователей из доверяемых лесов к защищенным ресурсам.

- P **Членство в группах и управление ACL** В диалог выбора объектов введена поддержка выбора имен пользователей и групп из доверяемого леса. Имена должны быть введены полностью вручную. Перечисление и поиск по шаблону не поддерживаются.
- а **Трансляция «имя — SID»** Диалоги выбора объектов и редактирования ACL используют системные API для по-

мещения SID в записи членства в группе и ACL и для трансляяии их обратно в дружественные имена для отображения. API трансляции «имя — SID» расширены для использования адресов межлесного перенаправления и применяют защищенные каналы NTLM между контроллерами доменов в пути доверительных отношений для разрешения имен участников защиты или SID из доверяемых лесов.

- **Фильтрация SID** При передаче авторизационных данных от корневого домена доверяемого леса корневому домену доверяющего леса происходит фильтрация SID. Доверяющий лес принимает только SID для доменов, управление которыми он доверяет другому лесу. Все остальные SID автоматически отвергаются. Фильтрация SID автоматически реализуется для аутентификации Kerberos и NTLM, а также для трансляции «имя — SID».

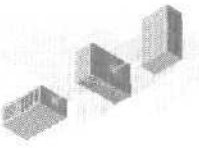
- **Усовершенствованная кросс-сертификация** Расширена путем добавления возможности кросс-сертификации на уровне отделов и на глобальном уровне. Например, теперь WinLogon способен запрашивать кросс-сертификаты и загружать их в «enterprise trust/enterprise store». По мере построения цепочки будут загружены все кросс-сертификаты,
- **IAS и межлесная аутентификация** При работе лесов Active Directory в межлесном режиме с двусторонними доверительными отношениями сервер Internet Authentication Service/Remote Authentication Dial-In User Service (IAS/RADIUS) может аутентифицировать пользователя в другом лесу. Это позволяет администраторам легко интегрировать новые леса с существующими сервисами IAS/RADIUS в их лесу.
- **Управление учетными записями** Средство Credential Manager предоставляет защищенное хранилище учетных записей пользователей, включая пароли и сертификаты X.509. Это позволяет реализовать согласованное поведение единой регистрации в сети для всех пользователей, включая «блуждающих». Например, при первом обращении пользователя к приложению сопровождения бизнеса из сети своей компании потребуется аутентификация, и пользователю будет предложено ввести свои учетные параметры. После их ввода пользователь связывается с запросившим их приложением.

При последующих обращениях к этому приложению регистрационные параметры пользователя подставляются автоматически, не требуя от него их повторного ввода.

Дополнительные сведения

Дополнительные сведения см. по следующим адресам:

- домашняя страница Microsoft Windows 2000 Active Directory — *http:// www.microsoft.con/ad/*;
- управление сетью предприятия с помощью Group Policy Management Console -- *http://www.microsoft.com/windows-server2003/gpmc/*;
- обзор Windows DNS — *http://www.microsoft.com/windows2000/techinfo/howitworks/communications/nameadrmgmt/dnsover.asp*.



ГЛАВА
4

Средства администрирования

Более легкая в развертывании, настройке и использовании, Windows Server 2003 предоставляет централизованные, настраиваемые средства администрирования, обеспечивающие снижение совокупной стоимости владения.

Microsoft Windows Server 2003 Resource Kit, выход которого ожидается в 2003 г. в издательстве Microsoft Press, предоставит подробное руководство по выполнению конкретных задач в самых разных областях. Help And Support Center в меню Пуск обеспечивает доступ к документации, а также к ссылкам на статьи и информацию об обновлениях.

Эта глава содержит обзор средств администрирования Windows Server 2003.

Управление конфигурацией

Пользователям нужна надежная рабочая среда, и Windows Server 2003 предоставляет средство управления изменениями и конфигурацией, позволяющее создать более управляемую инфраструктуру. Особенно важно это при совместной работе сотрудников над проектами в сетях больших предприятий, когда методы достижения целей существенно изменяются. Распределенный офис заменяет традиционную модель корпоративной сети с настольными компьютерами или терминалами в качестве рабочих мест.

В распределенном офисе пользователям требуется унифицированная, надежная среда, в том числе хорошо настроенная ОС, последние версии приложений и постоянный доступ к данным независимо от места подключения. ИТ-отдел должен эффективно удовлетворять потребности пользователей корпоративной сети. При этом нужно быстро реагировать на такие факторы, как:

- новые ОС и приложения;
- обновления ОС и приложений;
- новое оборудования;
- изменения конфигурации;
- новые требования бизнеса;
- новые пользователи;
- вопросы безопасности.

Управление этими изменениями можно рассматривать как бесконечный никл (рис. 4-1). Наличие средств управления изменениями и конфигурацией поможет вам:

- снизить совокупную стоимость владения путем сокращения:
  - D времени простоя и потерь на восстановление после сбоев;
  - П трудозатрат, связанных с неэффективной установкой и настройкой клиентских компьютеров;
  - □ потерь данных из-за аппаратных сбоев;
- повысить продуктивность путем:
  - п обеспечения постоянного доступа к данным, даже в отсутствие доступа к сетевым ресурсам;
  - D удаленной установки и удаленного обновления приложений;
  - п обеспечения пользователям доступа к их приложениям, данным и параметрам независимо от места их входа в сеть.

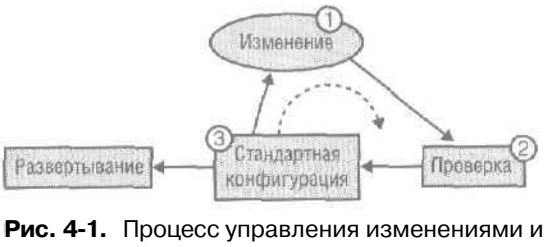


Рис. 4-1. Процесс управления изменениями и конфигурацией

Примечание Средство Software Installation, предоставляемое групповой политикой, подходит для простых схем развертывания ПО. В тех же случаях, когда при установке программ требуются работа по расписанию, инвентаризация и отчетность, а также поддержка установки по глобальным сетям, Microsoft рекомендует Systems Management Server 2.0 (SMS). Подробности см. на сайте этого продукта *http://www.microsoft.com/smsmgmt/*.

Управление безопасностью

При разработке ОС семейства Windows Server 2003 ставилась задача упростить как управление безопасностью, так и защиту сети от внешних угроз. Правила политики ограничения использования программ (software restriction) защищают вычислительную среду предприятия от ненадежного кода, позволяя указывать программы, которым разрешено работать. Администраторам также предоставляется новая инфраструктура получения и централизованного управления обновлениями ПО.

Шаблоны безопасности

Шаблоны безопасности (security templates) позволяют определить политику безопасности для сети. Являясь единой точкой, где могут быть определены все аспекты безопасности системы. шаблоны безопасности не вносят новых параметров защиты; они просто собирают все существующие атрибуты безопасности в одно место для упрощения администрирования. Импорт шаблона безопасности в объект групповой политики (Group Policy object, GPO) облегчает администрирование домена, позволяя сразу настроить безопасность для домена или ОП. Шаблоны безопасности позволяют задать:

- политику учетных записей;
- политику паролей;
- политику блокировку учетных записей;
- политику Kerberos;
- локальную политику;
- политику аудита;
- управление правами пользователя:

- параметры безопасности;
- параметры системных журналов: Application, System и Security;
- ограниченные группы; членство в группах, важных с точки зрения безопасности;
- параметры запуска и права доступа системных служб;
- права доступа к разделам реестра;
- права доступа к папкам и каталогам.

Шаблоны хранятся в виде текстового файла .inf. Это позволяет легко копировать, импортировать или экспортировать все или некоторые атрибуты шаблона. Кроме IP Security (IPSec) и политики открытых ключей, все атрибуты безопасности могут храниться в одном шаблоне безопасности. В Windows Server 2003/XP есть набор стандартных шаблонов, реализующих различные уровни безопасности и предназначенных для:

- повторной установки параметров по умолчанию;
- реализации среды с высокой степенью защиты;
- реализации менее защищенной, но более совместимой среды;
- защиты корня системы.

Вы можете создать новый шаблон безопасности либо использовать стандартные. Так, шаблон «Setup security.inf» позволяет задать значения параметров безопасности по умолчанию; он создается в процессе установки ОС на каждом компьютере и должен применяться локально. Прежде чем изменять параметры безопасности, проверьте действие измененных параметров в тестовой среде.

Политика ограничения использования программ

По мере все большего распространения Интернета и электронной почты новые программы проникают на компьютеры пользователей самыми разными путями. Пользователи должны постоянно принимать решения о запуске неизвестных программ. Вирусы вроде троянских программ часто нарочно выдают себя за другое ПО, чтобы заставить их запустить.

Политика ограничения использования программ (software restriction policies) позволяет защитить вычислительную среду от кода, не заслуживающего доверия, путем явного задания программ, которым разрешено исполняться. Вы можете задать для GPO по умолчанию уровень безопасности *без ограничений*

(unrestricted) или *запрещено* (disallowed), чтобы разрешить/запретить исполнение программ по умолчанию. Далее можно задать правила, изменяющие стандартный уровень безопасности для конкретных программ, Так, если уровнем по умолчанию является «запрещено», можно задать правила, разрешающие выполняться определенным программам.

Политика ограничения использования программ включает уровень безопасности по умолчанию и все правила, заданные для GPO. Эту политику можно применить ко всему домену, к локальным компьютерам или отдельным пользователям. Она предоставляет разные способы идентификации программ, а также основанную на политике инфраструктуру, принудительно реализующую решения об исполнении той или иной программы. Пользователи же при запуске программ должны следовать правилам, определеным администраторами.

Политика ограничения использования программ позволяет:

- управлять возможностью программ исполняться на вашем компьютере; например, если вас беспокоит возможность получения вирусов по электронной почте, можно запретить запуск файлов определенных типов из каталога вложений программы электронной почты;
- разрешить запускать только определенные файлы на многопользовательских компьютерах; например, запретить доступ к любым программам, кроме необходимых для работы;
- определять, кто имеет право добавлять производителей программ в список доверенных производителей (trusted publishers) на вашем компьютере;
- задавать, влияет ли политика ограничения использования программ на всех или только на некоторых пользователей компьютера;
- запрещать исполнение любых выбранных файлов на локальном компьютере, в ОП, сайте или домене; например, если известно, что система заражена определенным вирусом, можно предотвратить открытие компьютером файла, содержащего вирус.

Примечание Политика ограничения использования программ не заменяет антивирусного ПО.

Windows Update

Миллионы пользователей каждую неделю с помощью Windows Update устанавливают на свои системы последние обновления продукта. Windows Update позволяет подключиться к *http://www.windowsupdate.com,* где компьютер пользователя исследуется на предмет обновлений, в том числе на необходимость установки критических обновлений, обеспечивающих безопасность и защищенность системы. Windows Update также расширяет эти возможности посредством уведомлений о критических обновлениях (Critical Update Notification) и автоматического обновления (Automatic Updates),

Windows Update предоставляет следующие возможности.

- **Сайт Microsoft Windows Update Services Catalog** Администраторы могут загрузить «заплаты» и драйверы для распространения через SMS или другое аналогичное средство. Подробнее см. *http:// windowsupdate.microsoft.com/catalog/.*
- **Сайт Windows Update Consumer** Предназначенный в основном для непрофессионалов или пользователей слабо администрируемых сетей, этот сайт доставляет обновления на компьютеры, обращающиеся к нему. Это средство можно контролировать или отключить средствами групповой политики. Подробнее см. *http://windowsupdate.microsoft.com/.*
- **Auto Update** Администраторы могут автоматически загружать и устанавливать такие обновления, как «заплаты» безопасности, исправления серьезных ошибок и новые драйверы в отсутствие установленного драйвера для устройства. Auto Update помогает администраторам управлять развертыванием и установкой критических обновлений программ, а также объединяет несколько перезагрузок компьютера в одну. Будучи совместимым с внутрикорпоративными серверами обновлений программ, Auto Update предоставляет большую степень контроля за обновлениями. Автоматические обновления могут выполняться автоматически по Интернету или администрироваться на месте.
- **Dynamic Update** Служит для исправления проблем установки, например, при необходимости использования новых драйверов, которых нет на компакт-диске.
- **Драйверы устройств** Windows Server 2003 помогает администраторам предоставлять пользователям последние сер-

тифицированные драйверы через Web-сайты и обеспечивает интеграцию с диспетчером устройств и сервисами Plug and Play.

Software Update Services

Так как многие корпорации не желают, чтобы их компьютеры или пользователи получали из внешних источников предварительно не протестированные обновления, Microsoft предоставляет версию Windows Update для установки по эту сторону корпоративного брандмауэра. Microsoft Software Update Services (SUS) позволяет устанавливать на внутренний сервер с ОС Windows 2000/Server 2003 службу, которая будет загружать на этот сервер из Интернета все критические обновления по мере их появления на сайте Windows Update. Администраторы также могут получать уведомления о новых критических обновлениях по электронной почте.

SUS, поставляемый в настоящее время как расширение (add-on) для Windows 2000 Server, позволяет администраторам быстро развертывать наиболее критические обновления на своих серверах, а также настольных компьютерах с Windows 200C Professional/XP Professional. SUS предоставляет следующие компоненты.

- **Microsoft Software Update Services** Это серверный компонент, устанавливаемый на компьютер с Windows 2000 Server/Server 2003 по эту сторону корпоративного брандмауэра. Он синхронизируется с сайтом Windows Update для получения всех критических обновлений для Windows 2000/XP. Синхронизация может быть автоматической или выполняться администратором. Вы может протестировать полученные обновления в своей среде и решить, какие из них заслуживают установки.
- **Клиент автоматических обновлений** Это клиентский компонент для установки па все серверы с ОС Windows 2000/Server 2003, а также на компьютеры с Windows 2000 Professional/XP Professional. Он позволяет серверам и рабочим станциям подключаться к серверу, на котором установлен SUS, и получать с него обновления. Вы можете управлять тем, к какому серверу должен подключаться тот или иной клиент, а также составлять расписание установки клиентом

критических обновлений: вручную либо средствами групповой политики и Active Directory.

- **Поэтапное развертывание** Для этого SUS устанавливается на несколько серверов. Один из серверов может быть расположен в тестовой лаборатории, где обновления распространяются первоначально. Если установка обновлений тестовыми клиентами прошла успешно, вы можете настроить на публикацию обновлений и другие серверы SUS. Таким образом, можно гарантировать, что изменения не вызовут проблем в стандартной ОС рабочих станций.
- **Межсерверная синхронизация** Для доставки обновлений максимально близко к рабочим станциям и серверам может потребоваться несколько серверов SUS. В этом случае SUS позволяет указать вместо Windows Update другой сервер SUS, что дает возможность распространения критических обновлений внутри сети корпорации.

Основной задачей SUS является максимально быстрая доставка критических обновлений Windows 2000/XP/Server 2003 в корпоративную сеть. Многие компании для обеспечения безопасности своих систем используют электронные средства распространения программ, такие как Systems Management Server (SMS), обеспечивающие полное управление ПО, включая решение проблем, связанных с защитой и вирусами.

Подробнее о Software Update Services см. сайт *http://www.microsoft.com/windows2000/windows-update/sus/*.

Усовершенствования в IntelliMirror

Технологии администрирования IntelliMirror — это набор мощных средств управления изменениями и конфигурацией. IntelliMirror сочетает преимущества централизации с производительностью и гибкостью распределенных вычислений. IntelliMirror гарантирует, что данные, программы и личные параметры пользователей остаются доступными при перемещении последних на другие компьютеры и что эти параметры сохраняются, когда компьютеры подключены к сети. Кроме того, администраторы могут применять средства удаленной установки (Remote Installation Services — RIS) для удаленной установки ОС. Многие средства IntelliMirror используют групповую политику, кото-

рая в свою очередь требует Active Directory. Поддержка Active Directory имеется в Microsoft Windows 2000 Server/Server 2003.

Большинство средств IntelliMirror, имеющихся в Windows XP/ Server 2003, доступно и в Windows 2000. Вы можете применять IntelliMirror в сетях, где работает одна из или все эти ОС. Но усовершенствования, добавленные в Windows XP/Server 2003. обеспечивают повышенную гибкость администрирования компьютеров и учетных записей пользователей в сети.

Благодаря интеллектуальному управлению информацией, параметрами и программами, средства IntelliMirror повышают степень доступности пользовательских данных, личных параметров и вычислительной среды вообще. На основании правил политики IntelliMirror может развертывать, восстанавливать и заменять пользовательские данные, программы и личные параметры в средах на основе Windows 2000/Server 2003. Фактически IntelliMirror обеспечивает следование за пользователем его личной вычислительной среды. Пользователи получают немедленный доступ ко всей своей информации и ПО независимо от того, на каком компьютере они работают и подключены ли они к сети, с гарантией надежного хранения и доступности их данных.

IntelliMirror дает администратору возможность один раз установить правила политики и быть уверенным в том, что они будут применяться без его дальнейшего вмешательства. Ядром IntelliMirror являются следующие средства.

- **Управление политикой** Вы можете настроить параметры групповой политики, которые затем будут гарантированно применены к заданным компьютерам и пользователям. Например, можно настроить политику паролей для компьютеров, после чего Windows применит эти правила, не требуя перезагрузки компьютера или повторного входа пользователя в систему.
- **Управление пользовательскими данными** Служит для управления файлами, документами, электронными таблицами и другой информацией, создаваемой и используемой людьми в процессе своей работы. Путем перенаправления стандартных пользовательских папок, таких как папка Мои Документы, в сетевую папку и обеспечения доступа к этой пап-

ке в автономном режиме, пользователям может быть обеспечен доступ к их данным из любого места сети или вне ее.

- **Управление пользовательскими параметрами** Служит для централизованной настройки вычислительной среды для групп пользователей или для компьютеров. В случае сбоя компьютера пользовательские параметры можно легко восстановить. В состав пользовательских параметров входят как личные предпочтения, так и централизованно определяемые параметры интерфейса ОС и приложений. Параметры могут включать в себя выбор языка, вид «рабочего стола» и пр. Доступ к параметрам данного пользователя может быть обеспечен ему независимо от места входа в сеть.
- **Установка и сопровождение программ** Служит для установки, настройки, исправления проблем или удаления приложений, сервисных пакетов и обновлений ОС. Вы можете назначить или опубликовать программу для конкретных пользователей или компьютеров. Назначение приложений пользователю обеспечивает его доступ к ним независимо от места его входа в сеть. Назначение приложений компьютеру делает их доступными всем пользователям этого компьютера. Это полезно для приложений, необходимых всем пользователям, таких как антивирусные программы. При назначении приложения пользователю вы можете выбрать его полную установку при входе пользователя в систему или по требованию — когда пользователь вызовет приложение или его часть. Если приложение настроено на установку по требованию, для пользователя оно выглядит установленным, однако фактически оно не устанавливается, пока пользователь в первый раз не обратится к нему. Это позволяет ускорить развертывание конфигураций рабочих станций для большого числа пользователей, многие из которых не применяют все доступные возможности той или иной программы. С другой стороны, вариант полной установки, доступный в Windows Server 2003, полезен для групп пользователей, скажем, часто ездящих в командировки, которым может потребоваться полная установка нужных приложений перед поездкой. Приложения, опубликованные администратором, пользователь может установить на свой компьютер, выбрав инструмент Добавить/Удалить Программы из Панели управления.

Приложения следуют за пользователями или компьютерами, что гарантирует доступность приложений на любом компьютере, на котором работает данный пользователь.

Средства IntelliMirror могут применяться по отдельности или совместно в зависимости от конкретных требований организации. Вы также можете ограничить места, откуда будут доступны данные и параметры пользователя.

Средства IntelliMirror разработаны так. чтобы предоставить преимущества с одновременным снижением затрат на администрирование системы. Большая часть средств IntelliMirror позволяет обеспечить продуктивную работу пользователей и вместе с тем централизованное администрирование, снизив объем административного вмешательства, а значит, и затраты на него. Централизованное управление, обеспечиваемое IntelliMirror, позволяет организациям с меньшими затратами реализовать управление изменениями и конфигурацией, так как вся организация может рассматриваться и управляться посредством единого представления в Active Directory.

Управление политикой

Group Policy Management Console (GPMC), планируемая как бесплатное расширение к Windows Server 2003, предоставит новую архитектуру управления групповой политикой. GPMC упростит применение групповой политики, что позволит эффективнее использовать Active Directory. Так, GPMC обеспечивает резервное копирование и восстановление GPO, импорт/экспорт и копирование GPO, генерацию отчетов о параметрах GPO и данных Resultant Set of Policy (RSoP), применение шаблонов для управления конфигурацией, а также управление всеми операциями GPMC из сценариев. Кроме того, GPMC позволяет управлять политикой множества доменов и сайтов внутри данного леса, предоставляя для этого упрощенный пользовательский интерфейс с поддержкой технологии drag-and-drop. А если леса связаны доверительными отношениями, вы сможете с одной консоли управлять групповой политикой в нескольких лесах. GPMC может управлять групповой политикой в доменах Windows 2000/.NET.

Хотя объекты групповой политики могут быть связаны только с сайтами, доменами или ОП внутри данного леса, доверитель-

ные отношения между лесами в Windows .NET Server позволяют реализовать ряд новых сценариев групповой политики, Так, пользователь из леса А может войти на компьютер из леса В, имеющего собственные правила политики. Альтернативно параметры GPO могут ссылаться на серверы других лесов, например, на точки распространения ПО. Эти сценарии поддерживаются групповой политикой в Windows Server 2003.

Инструмент RSoP позволяет просмотреть эффект применения групповой политики к пользователю или компьютеру. RSoP служит для планирования и управления групповой политикой, а также исправления проблем в ее настройке. RSoP — это инфраструктура и инструмент, реализованный в виде оснастки MMC, позволяющий определять и анализировать текущие правила политики в режиме регистрации и режиме планирования. Первый позволяет определить текущие результаты применения политики к заданной цели, второй — посмотреть возможные результаты изменений групповой политики до реального внесения изменений.

RSoP использует способность WMI собирать данные из разных источников. Инструмент, работающий в среде MMC, поддерживает расширения оснастки для отображения результатов в зависимости от целевого объекта. Мастер установления цели задает границы действия инструмента RSoP. Этот мастер проведет администратора по всем этапам создания подходящего целевого объекта, генерации данных RSoP и запуска инструмента RSoP для использования этих данных.

WMI генерирует для целевого компьютера большой объем информации, такой как список аппаратных и программных средств и параметры конфигурации. В качестве источников данных WMI использует реестр, драйверы, файловую систему, Active Directory, Simple Network Management Protocol (SNMP), службу Windows Installer, язык SQL, сетевую подсистему и Exchange Server. WMI Filtering в Windows Server 2003 позволяет вам динамически определять, применять ли GPO на основании запроса к данным WM1. Эти запросы (называемые также WMI-фильтрами) определяют, какие пользователи и компьютеры получают параметры политики, указанные в GPO. Данная функциональность позволяет автоматически определять цели групповой политики на основании свойств локального

компьютера. Ниже перечислены примеры свойств, на основании которых можно создавать WMI-фильтры:

- **службы:** компьютеры, на которых активизирована поддержка протокола DHCP (Dynamic Host Configuration Protocol);
- **реестр:** компьютеры, на которых заполнен указанный раздел реестра;
- **аппаратные средства:** компьютеры с процессором Pentium III;
- **программные средства:** компьютеры, на которых установлена Visual Studio .NET;
- **аппаратная конфигурация:** компьютеры с сетевыми платами, использующими 3-й уровень прерываний;
- **программная конфигурация:** компьютеры с активизированной групповой рассылкой (multicasting);
- **зависимости:** компьютеры, на которых установлены службы, зависимые от службы SNA (systems network architecture);
- **команда Ping:** компьютеры, для которых передача эхо-пакетов командной ping на заданный сервер занимает менее 100 миллисекунд.

Интеграция в редактор объектов групповой политики Web-режима отображения облегчает понимание, управление и опенку текущих параметров политики. Щелчок правила политики отображает текст, описывающий его назначение и ОС, которые его поддерживают, скажем, только Windows XP или Windows 2000. Это позволяет быстро просматривать параметры и легко определять пути достижения той или иной цели политики. В ОС семейства Windows Server 2003 поясняющий текст был расширен путем включения описания для таких категорий политики, как меню Пуск и Панель задач.

Windows Server 2003 включает более 160 новых правил политики, управляющих поведением таких компонентов, как;

- Terminal Server;
- совместимость приложений;
- поддержка сети, в том числе SNMP, качество обслуживания (QoS), брандмауэры и доступ по коммутируемой линии;
- регистрацию в DNS;
- «блуждающие» профили пользователей и групповая политика;

- Панель управления;
- Windows Media Player.

Ключевое слово *supported,* включенное в файл административного шаблона (.adm) для каждого правила политики, позволяет выяснять, какие из них поддерживаются Windows 2000, определенным сервисным пакетом или Windows Server 2003. Администраторы и пользователи могут выполнять поиск правил политики на основании этих ключевых слов и отображать только те, что поддерживаются определенной версией ОС. Поясняющий текст к каждому правилу начинается с указания версии **ОС,** поддерживающей его.

Управление пользовательскими данными

Обеспечение постоянного доступа к данным — важнейшая задача. Средства IntelliMirror для управления пользовательскими данными позволяют гарантировать доступ пользователей к своей информации с любого компьютера сети как в оперативном, так и в автономном режиме. Вы можете создавать централизованные резервные копии пользовательских данных, что позволит легко заменять неисправные компьютеры.

Пользователи могут получать доступ к своим данным с любого компьютера корпоративной сети, на котором установлена Windows 2000 Professional (или более новая ОС). Данные пользователя следуют за ним, так как хранятся в выделенных для этой цели местах сети. Список доступных данных и папок можно настроить вручную или через групповую политику. Кроме того, если пользователь автономно работает с ресурсами, обычно хранящимися в сети, любые изменения будут синхронизированы, когда он подключится к сети снова.

Средства управления пользовательскими данными позволяют гарантировать их постоянную доступность:

- администраторы могут лучше защитить пользовательские данные, перенаправляя или копируя локальные данные в общий сетевой каталог, что обеспечивает возможность централизованного резервного копирования под контролем администратора; это позволяет гарантировать реализацию корпоративных правил, таких как копирование всех важных данных на серверы;

- администраторы могут гарантировать, что как на локальном компьютере, так и на сервере находятся наиболее актуальные версии пользовательских данных; так как локальное кэширование позволяет работать с данными на локальном компьютере, даже когда он отключен от сети, то данные всегда доступны пользователю, в том числе и при работе в автономном режиме;
- данные могут следовать за человеком при его переходе на другой компьютер сети; это повышает удобство работы, так как человек может получить доступ к своим данным с любого компьютера в сети.

Примечание Групповая политика позволяет перенаправить папку пользователя Мои Документы в его домашний каталог. Это облегчает переход пользователей от старой модели домашних каталогов к модели «Мои Документы», сохраняя совместимость с текущей средой домашних каталогов.

Для реализации управления пользовательскими данными могут использоваться все или часть из следующих технологий:

- Active Directory;
- групповая политика;
- RSoP;
- «блуждающие» профили пользователей;
- перенаправление папок:
- автономные файлы;
- диспетчер синхронизации;
- Distributed File System (DFS);
- Encrypting File System (EFS);
- квоты дискового пространства.

Управление пользовательскими параметрами

Средства управления пользовательскими параметрами IntelliMirror позволяют администраторам централизованно определять параметры среды для групп пользователей и компьютеров, чтобы пользователи автоматически получали нужную конфигурацию. Кроме того, администраторы могут восстанавливать

пользовательские параметры при сбоях компьютера, а также обеспечить следование параметров пользовательского интерфейса за человеком при его переходе на другой компьютер. Вы можете:

- уменьшить число обращений к персоналу поддержки путем предоставления заранее сконфигурированных сред для рабочих станций пользователя;
- сэкономить время и затраты при замене компьютеров;
- повысить эффективность работы пользователей, автоматически предоставляя им их параметры рабочего стола независимо от их текущего места работы.

Вы можете управлять профилем пользователя, т. е. параметрами рабочего стола, безопасности, языка, приложений и сценариев (запускаемых при включении/выключении компьютера и при начале/завершении сеанса работы пользователя). Эта информация хранится на каждом локальном компьютере для всех пользователей, которые с ним работали. Вы также можете перенаправить стандартные пользовательские папки на сетевой диск. Это позволяет поддерживать единый профиль пользователя независимо от того, с какого компьютера он входит в сеть.

Профиль пользователя, как и его данные, могут следовать за ним на другие компьютеры сети. Параметры групповой политики позволяют управлять окружением пользователя, а также предоставлять ему или нет права на настройку этого окружения. Эти параметры могут быть назначены для пользователей и для компьютеров. Обладая соответствующими правами, пользователи часто меняют стиль и параметры своей среды в соответствии с потребностями и привычками. Параметры содержат три основных типа информации: пользовательская и административная информация, временная информация и данные, специфичные для локального компьютера. Обычно временные и локальные данные не должны следовать за пользователем; их перемещение может привести к лишним накладным расходам, а различия между компьютерами — к невозможности обращения к ней. Если применяются «блуждающие» профили пользователя, групповая политика гарантирует, что будет сохраняться только жизненно важные пользовательские и административные параметры, тогда как временные и локаль-

ные параметры будут динамически генерироваться заново при необходимости. Это снижает объем информации, хранимой и перемещаемой по сети, в то же время обеспечивая пользователям схожую рабочую среду на любом компьютере сети,

Для реализации управления пользовательскими параметрами используются:

- Active Directory;
- групповая политика;
- автономные файлы;
- диспетчер синхронизации;
- DFS;
- перенаправление папок;
- «блуждающие» профили пользователей.

Примечание Windows Server 2003 поддерживает ряд новых правил политики, позволяющих обеспечить гибкое конфигурирование профилей пользователей, в том числе их отключение на определенных компьютерах и создание неизменяемых профилей.

Управление программами

С обеспечением пользователей ПО связан ряд проблем:

- пользователям нужны разные приложения, поэтому в больших организациях поддерживаются сотни, а то и тысячи приложений, и администраторы должны обеспечить их эффективную доставку и установку;
- с течением времени программные продукты эволюционируют: появляются новые приложения и новые версии старых приложений, нужно устанавливать и расширения, такие как новые пользовательские шаблоны или сервисные пакеты;
- при переходе на новые должности пользователям становятся нужны новые приложения, а надобность в старых отпадает; пользователь также может перейти на компьютер, расположенный в другом месте, и там ему потребуется «его» ПО.

Производительность пользователя растет, когда ему доступны все нужные ему программы. Администратору важно обеспечивать удаление приложений, которые более не используются или

устарели. ИТ-отделу приходится определять момент, когда прекратить поддержку ненужного ПО. Иногда лучше удалить устаревшее приложение, чем бороться с проблемами совместимости. Многие организации стремятся автоматизировать управление приложениями для больших групп или даже для всех рабочих станций одновременно.

Средства IntelliMirror для установки и сопровождения приложений позволяют устанавливать ПО при старте компьютера, входе пользователя в систему или по требованию. Вы также можете применять эти средства для обновления установленных приложений, удаления ненужных приложений и развертывания сервисных пакетов и обновлений ОС. Можно гарантировать невозможность установки пользователем ПО с локального носителя вроде компакт- или гибкого диска. IntelliMirror также предоставляет решения в следующих ситуациях:

- если пользователь случайно стер файлы приложения, оно восстановит себя;
- при переходе пользователя на другой компьютер его программы всегда будут ему доступны;
- если пользователь пытается открыть документ, связанный с приложением, не установленным на локальный компьютер, приложение автоматически установится и откроет документ.

Групповая политика позволяет задать параметры установки ПО, определяющие, какие приложения подлежат установке, обновлению или удалению с компьютера. Правила политики установки программ могут быть применены к группам пользователей или компьютеров. Имеется два метода установки приложений на компьютеры пользователей — назначение (assigning) и публикация (publishing),

- Назначение Групповая политика позволяет назначать приложения пользователю или компьютеру. При назначении приложения компьютеру оно будет автоматически установлено при его следующей загрузке. При использовании групповой политики для назначения приложения пользователю администратор может выбрать установку по требованию (при первой попытке вызова приложения) либо полную установку (при следующем входе пользователя в систему).

- **По требованию** Если приложение устанавливается по требованию, то на пользовательском компьютере настраивается ярлык в меню Пуск, а в реестре создаются соответствующие связи с типами файлов. С точки зрения пользователя все выглядит так, как если бы приложение уже было установлено. Однако оно не устанавливается полностью, пока оно не потребуется пользователю. При попытке запуска приложения или открытия связанного с ним файла Windows Installer проверяет наличие файлов и параметров, необходимых для корректной работы приложения. Если их нет, Windows Installer получает и устанавливает их из заранее заданной точки распространения. После установки приложение запускается.
- **Полная установка** Этот режим удобен для некоторых пользователей, например, часто выезжающих в командировки. В этом режиме приложения пользователя устанавливаются при его входе в систему.

  Режим назначения приложений обеспечивает их доступность независимо от действий пользователя; так, если пользователь удалит приложение, оно будет автоматически установлено заново по первому требованию.

- **Публикация** При публикации приложение появляется в диалоге Добавить/Удалить программы в Панели управления. Пользователи могут установить опубликованное приложение. Установка также может быть настроена на автоматическое выполнение при попытке открыть файл, для работы с которым служит опубликованное приложение. Публикация применяется, когда приложение не является абсолютно необходимым пользователю для его работы.

  Полностью преимущества публикации можно задействовать, только когда все публикуемые приложения разработаны с учетом установки с помощью Windows Installer. Хотя вы можете публиковать приложения, не поддерживающие Windows Installer, применяя файлы .zap, при этом не удастся задействовать описанные далее преимущества повышенных привилегий и, конечно, сам Windows Installer.

Примечание Текстовый файл .zap, содержит указатель на дистрибутив программы и позволяет отображать данное приложение в диалоге Добавить/Удалить программы.

Развертывание программ посредством групповой политики требует от приложений использования службы Windows Installer, которая, помимо возможности установки приложений, обеспечивает целостность приложений при случайном повреждении локальных файлов. Например, если пользователь пытается работать с копией Microsoft Word, в которой недостает некоторых файлов, Windows Installer автоматически установит их заново из источника установки (installation point) при следующей попытке запуска приложения. Кроме того, поддерживающие Windows Installer приложения при использовании для их развертывания групповой политики могут устанавливаться с повышенными привилегиями, т. е, пользователям не нужно быть администраторами на своих компьютерах, чтобы устанавливать ПО, определенное для них администратором сети. Восстановление приложения работает по тому же алгоритму, что и установка по требованию. Всякий раз при запуске приложения, поддерживающего Windows Installer, последний проверяет наличие необходимых файлов; если это потребуется, файлы и параметры будут восстановлены автоматически.

Windows Server 2003 предоставляет и другие усовершенствования в области развертывания программных продуктов.

- **Полная установка приложений, назначенных пользователю при его входе в систему** Средство установки программ доступное в разделе Software Settings оснастки Group Policy Object Editor модернизировано и включает новую опцию полной установки. Она позволяет устанавливать назначенные пользователю приложения целиком при его входе в систему, а не по требованию. Режим полной установки полезен группам пользователей, часто выезжающим в командировки, которым перед отъездом может потребоваться полная установка всех нужных приложений.
- **Поддержка 64-битных программ** Новые параметры установки программ в групповой политике позволяют указать, следует ли устанавливать 32-битные приложения на 64-битные компьютеры. Тот же уровень функциональности, что и для ОС Windows Server 2003, может быть предоставлен и для клиентов с Windows 2000. Данная возможность полезна тогда, когда администратор планирует установку 32-битного пакета Windows Installer для группы пользователей с 64-битными

компьютерами. Зная, что 32-битный пакет работает корректно на 64-битных компьютерах, администратор выбирает новую опцию «Make 32-bit x86 Windows Installer Application Available To IA64 Machines» в диалоге Group Policy Software Installation для установки данного пакета всем пользователям.

Для реализации установки и сопровождения программных средств используются некоторые или все из следующих технологий Windows:

- Active Directory;
- групповая политика;
- Windows Installer;
- инструмент Добавить/Удалить программы;
- DFS;
- служба репликации файлов (File Replication Service, **FRS).**

Настройка нового компьютера

Когда пользователю требуется новый компьютер, администраторам необходимо:

- быстро дать пользователю возможность вернуться к своей непосредственной работе;
- сократить частоту и продолжительность вызовов ИТ-персонала или даже вовсе устранить эти вызовы.

Удаленная установка (Remote Installation) позволяет улучшить эти показатели. Вся процедура основана на политике и может быть выполнена без поддержки на рабочем месте пользователя. Remote Installation можно применять для первой установки Windows на все клиентские компьютеры, поддерживающие Pre-Boot execution Environment (PXE). Для установки ОС и основных приложений администратору не нужно лично идти к новому компьютеру. Вы можете реализовать настроенный в соответствии с вашими потребностями, полностью автоматизированный процесс установки из удаленного источника. После включения компьютера пользователь нажимает F12 для запуска процесса установки ОС. Затем компьютер загружается с сетевого сервера, поддерживающего RIS. После входа пользователя в систему RIS может служить для установки:

- сетевого эквивалента дистрибутивного компакт-диска Windows;

- образа ОС (RIPrep-образа), который может включать предварительно сконфигурированные приложения, такие как текстовые процессоры или электронная почта.

Для реализации удаленной установки используются:

- Active Directory;
- групповая политика;
- DNS;
- DHCP;
- RIS.

Утилиты командной строки

Автоматизировать регулярно выполняемые действия позволяют более 60 новых утилит командной строки, в том числе для управления ключевыми компонентами, такими как серверы печати, Internet Information Services (IIS) 6.0 и Active Directory, Преимущества, предоставляемые этими утилитами, таковы.

- **Готовность к использованию** Предоставляются готовые решения, для использования которых не нужен или нужен лишь небольшой объем дополнительного кодирования. Все утилиты имеют стандартный унифицированный синтаксис, легко доступную из командной строки подсказку (по ключу /?), а также подробную справочную информацию в виде файла HTML-подсказки ntcmds.chm (доступен из пункта меню Help and Support Center).
- **Поддержка удаленного администрирования** Все новые утилиты поддерживают работу с удаленными серверами с помощью параметра /5, позволяющего задать имя удаленной машины (например, /5 *MyServer*), и работают в среде Telnet и Terminal Services. Это обеспечивает все возможности удаленного администрирования из командной строки.
- Сценарии Из командной строки можно запускать командные файлы иди сценарии для реализации специализированных административных операций и автоматизации часто выполняемых действий.

Командный процессор

Командный процессор — это отдельная программа, обеспечивающая взаимодействие пользователя с ОС. Неграфический ин-

терфейс командного процессора предоставляет среду исполнения консольных приложений и утилит. Командный процессор исполняет программы и отображает выводимые ими результаты на экране в символьном режиме, что во многом похоже на командный процессор MS-DOS — Command.com. Windows Server 2003 использует в качестве командного процессора интерпретатор команд Cmd.exe, который загружает приложения и организует передачу потоков информации между ними, транслируя пользовательский ввод в форму, понятную ОС.

Усовершенствования командного процессора повышают эффективность администрирования. Так, вы можете:

- использовать командный процессор для исполнения командных файлов (сценариев), автоматизирующих рутинные операции; например, сценарии позволяют автоматизировать управление пользовательскими учетными записями или выполнение ночного резервного копирования;
- использовать CScript — версию Windows Script Host для командной строки, позволяющую исполнять в среде командного процессора более сложные сценарии;
- повысить эффективность выполнения операций, применяя вместо пользовательского интерфейса командные файлы; в командных файлах можно использовать все команды, допустимые в командной строке;
- настраивать режим просмотра содержимого окна командной строки для повышения уровня контроля за ходом исполнения программ.

Утилиты командной строки

Ниже приведен список новых и обновленных утилит **командной строки в ОС** Windows Server 2003:

- **adprep** подготавливает домены и леса Windows 2000 при переходе на Windows Server 2003, Standard Edition, Enterprise Edition или Datacenter Edition;
- **bootcfg** позволяет конфигурировать, просматривать или изменять параметры файла Boot.ini;
- **choice** предлагает пользователю сделать выбор, отображая строку подсказки и приостанавливая выполнение до тех пор, пока пользователь не выберет один из предлагаемых вариантов;

- **clip** перенаправляет информацию, выводимую в окно командной строки, в системный буфер обмена;
- cmdkey создает, отображает и удаляет сохраненные имена пользователей и пароли;
- **defrag** выполняет дефрагментацию файлов загрузчика, файлов данных и папок на локальных томах;
- **diskpart** управляет дисками, разделами или томами;
- **driverquery** позволяет вывести список драйверов и их параметров;
- **dsadd** добавляет в Active Directory компьютер, контакт, группу, организационное подразделение или пользователя;
- **dsget** отображает выбранные атрибуты компьютера, контакта, группы, организационного подразделения, сервера или пользователя из Active Directory;
- **dsmod** изменяет существующий в Active Directory компьютер, контакт, группу, ОП или пользователя;
- **dsmove** перемещает выбранный объект в другое место Active Directory (если такое перемещение можно выполнить средствами одного контроллера домена) и переименовывает объект без перемещения по дереву Active Directory;
- **dsquery** позволяет выполнять в Active Directory поиск компьютеров, групп, ОП, серверов или пользователей по заданному условию;
- **dsrm** удаляет из Active Directory объект заданного типа или произвольный объект;
- **eventcreate** позволяет администратору записать собственное событие в заданный системный журнал событий;
- **eventquery** выводит события и их параметры из одного или нескольких системных журналов;
- **eventtriggers** отображает и конфигурирует триггеры событий на локальном или удаленном компьютере;
- **forfiles** выбирает файлы из каталога или дерева каталогов для пакетной обработки;
- **freedisk** проверяет наличие свободного пространства на диске перед выполнением установки файлов;
- **fsutil** позволяет управлять точками перенаправления (reparse point) и разреженными файлами; размонтировать или расширять тома;

- **getmac** выводит информацию о MAC-адресе (media access control) и список сетевых протоколов;
- **gettype** устанавливает системную переменную среды *%ERRORLEVEL%* в значение, связанное с заданной информацией об ОС Windows;
- **gpresult** отображает параметры групповой политики и результаты применения политики (RSoP) для пользователя или компьютера;
- **helpctr** запускает Help and Support Center;
- **inuse** замещает заблокированные файлы ОС;
- **iisback** создает и управляет резервными копиями конфигурации IIS (метабазой и схемой) для удаленного или локального компьютера;
- **iiscnfg** импортирует/экспортирует все или части конфигурации IIS на локальном или удаленном компьютере;
- **iisftp** создает, удаляет и выводит список FTP-сайтов на серверах под управлением IIS 6.0, а также позволяет запускать, останавливать, приостанавливать и возобновлять работу FTP-сайтов;
- **iisftpdr** создает и удаляет виртуальные каталоги FTP-сайтов на серверах под управлением IIS версии 6.0 или более поздней;
- **iisvdir** создает и удаляет виртуальные каталоги Web-сайтов на серверах под управлением IIS версии 6.0 или более поздней;
- **iisweb** создает, удаляет и выводит список Web-сайтов на серверах под управлением IIS 6.0, позволяет также запускать, останавливать, приостанавливать и возобновлять работу Web-сайтов;
- **logman** позволяет управлять и планировать сбор данных счетчиков производительности и журнала событий трассировки (event trace log) на локальном или удаленном компьютере;
- **nlb** заменяет wlbs.exe для настройки и управления работой средств распределения загрузки сети;
- **nlbmgr** конфигурирует и управляет кластерами распределения загрузки сети и всеми кластерными серверами с одного компьютера;
- **openfiles** выводит информацию об открытых файлах и позволяет отключать их;

- **pagefileconfig** отображает и настраивает параметры системного файла страниц виртуальной памяти;
- **perfmon** позволяет открыть консоль производительности, настраиваемую с помощью файлов параметров Performance Monitor версии для Windows NT 4.0;
- **prncnfg** конфигурирует или отображает информацию о принтере;
- **prndrvr** добавляет, удаляет и выводит список драйверов принтеров на локальном или удаленном сервере печати;
- **prnjobs** приостанавливает, возобновляет, отменяет и выводит список заданий на печать;
- **prnmngr** добавляет, удаляет и выводит список локальных или подключенных сетевых принтеров, а также позволяет установить принтер по умолчанию и отобразить информацию о нем;
- **prnport** создает, удаляет и выводит список стандартных портов печати TCP/IP, а также позволяет отобразить и изменить их конфигурацию;
- **prnqctl** печатает тестовую страницу, приостанавливает или возобновляет работу принтера, а также очищает очередь печати;
- **relog** извлекает значения счетчиков производительности из журналов производительности с преобразованием в другие форматы, такие как текст, разделенный табуляциями или запятыми, двоичный или SQL;
- rss активизирует Remote Storage для расширения дискового пространства сервера;
- sc получает и устанавливает параметры служб. Тестирует и отлаживает программы-службы;
- **schtasks** позволяет запланировать исполнение команд и программ периодически или в заданное время; добавляет и удаляет задачи из расписания, запускает и останавливает задачи по требованию, а также позволяет отобразить расписание и изменить параметры указанных в нем задач;
- **setx** устанавливает локальные или системные переменные среды, не требуя программирования или написания сценариев;
- **shutdown** выполняет останов или перезагрузку локального или удаленного компьютера;

- **systeminfo** позволяет получить базовую информацию о конфигурации компьютера;
- **takeown** позволяет администратору восстановить доступ к файлу, назначив себя его владельцем;
- taskkill завершает одну или несколько задач или процессов;
- tasklist отображает список приложений и служб, а также идентификаторы процессов, выполняющихся в данный момент на локальном или удаленном компьютере;
- timeout приостанавливает работу командного процессора на заданное число секунд;
- **tracerpt** обрабатывает журналы событий трассировки или трассировки данные, полученные в реальном времени от специальных аппаратных устройств, и позволяет генерировать отчеты анализа трассировки и файлы в формате CSV (текст, разделенный запятыми);
- **tsecimp** импортирует информацию из XML-файла в файл защиты сервера TAP1 (tsec.ini);
- **typeperf** выводит данные счетчика производительности в окно командной строки или в файл журнала поддерживаемого формата;
- **waitfor** использует сигналы для синхронизации работы нескольких компьютеров в сети;
- **where** находит и отображает все файлы, соответствующие заданному параметру;
- **whoami** возвращает имя домена или компьютера, имя пользователя, имена групп, идентификатор пользователя, задействованный при входе в систему, а также привилегии текущего пользователя;
- **WMIC** упрощает использование WMI и управление компьютерами с его помощью.

Командная строка WMI

Утилита командной строки WMI (WMIC — WMI Command Line) предоставляет для WMI простой интерфейс командной строки. WMIC служит для управления Windows-компьютерами. WMIC взаимодействует с другими командными процессорами и утилитами командной строки и может быть легко расшире-

аппаратура компьютера, подключенного к сети, отыскивает сетевой RIS-сервер и запрашивает установку новой копии ОС, сконфигурированной надлежащим образом для данного пользователя и компьютера.

Миграция пользовательского состояния

Инструмент USMT (User State Migration Tool) упрощает миграцию файлов и параметров большого числа пользователей в условиях крупных организаций. USMT позволяет настраивать нужные параметры, например реестр, с точностью, присущей утилитам командной строки.

USMT предназначен только для администраторов. Кроме того, для работы USMT клиентский компьютер должен быть подключен к контроллеру домена Windows 2000 Server или более новой версии. USMT предоставляет улучшения в следующих областях:

- затраты на технических специалистов отдела сопровождения;
- затраты времени сотрудников на настройку пользовательского интерфейса ОС;
- затраты времени сотрудников на поиск пропавших рабочих файлов;
- обращения сотрудников в отдел сопровождения при настройке пользовательского интерфейса ОС;
- освоение сотрудниками новой ОС;
- удовлетворение нужд сотрудников в результате миграции.

USMT состоит из двух исполняемых файлов (ScanState.exe и LoadState.exe) и четырех файлов с информацией о правилах миграции (Migapp.inf, Migsys.inf. Miguser.inf и Sysfiles.inf). ScanState.exe выполняет сбор пользовательских данных и параметров на основании информации, содержащейся в Migapp.inf, Migsys.inf, Miguser.inf и Sysfiles.inf. Собранные данные LoadState.exe помещает на компьютер, где установлена свежая (необновлснная) копия Windows XP Professional. USMT работает под управлением набора файлов .inf, которые могут быть модернизированы администраторами или независимыми производителями оборудования. При использовании USMT для автоматизации миграции администраторам практически в любых случаях потребуется изменить файлы .inf, чтобы они лучше

соответствовали особенностям конкретной среды. Для описания дополнительных правил миграции могут быть созданы дополнительные файлы .inf. Без изменения установок по умолчанию USMT переносит следующие компоненты:

- параметры Internet Explorer;
- параметры и хранилище Outlook Express;
- параметры и хранилище Outlook;
- параметры асинхронных коммуникаций;
- параметры телефонии и модемов;
- параметры для лиц с ограниченными физическими возможностями;
- классический «рабочий стол»;
- выбор хранителя экрана;
- шрифты;
- параметры папок;
- параметры панели задач;
- параметры мыши и клавиатуры;
- параметры звука;
- параметры национальных особенностей;
- параметры Office;
- сетевые диски и принтеры;
- папку Desktop;
- папку Мои Документы;
- папку Мои Картинки;
- папку Избранное;
- папку Cookies;
- стандартные типы файлов Office.

Информацию, собираемую ScanState.exe, легко модифицировать. Эту утилиту можно настроить на обработку/игнорирование файлов, папок, записей или подразделов реестра.

Windows Installer

Windows Installer позволяет упростить настройку параметров установки, обновления и модернизации программ, как и устранение проблем конфигурации. Windows Installer управляет общими ресурсами, гарантирует применение согласованных правил проверки версий файлов, а также выполняет диагнос-

тику и восстановление приложений в процессе их работы, что дает большую экономию при управлении приложениями.

До Windows Installer для установки ПО использовались различные технологии, каждая из которых характеризовалась уникальным набором правил установки для каждого приложения. Иногда при установке ПО случались ошибки. Например, предыдущая версия некоторого файла могла быть установлена поверх его новой версии. Применение большого числа технологий установки приложений делает сложным точный подсчет ссылок на компоненты, совместно используемые разными приложениями на данном компьютере. В результате установка или удаление одного приложения могли повлиять на работу других.

При использовании Windows Installer все правила установки реализуются ОС. Чтобы следовать этим правилам и избежать проблем, описанных выше, приложению достаточно лишь описать себя в пакете Windows Installer. Далее установка каждого приложения выполняется Windows Installer, что позволит предотвратить или свести к минимуму распространенные проблемы установки.

Windows Server 2003 предоставляет новые возможности, повышающие безопасность информации, а также удобство использования и администрирования Windows Installer.

- **64-битная поддержка** Windows Installer в 64-битных версиях Windows Server 2003, Enterprise Edition и Datacenter Edition реализован как настоящая 64-битный служба. Он выполняет установку как 32-, так и 64-битных приложений. 64-битные приложения помещаются в особым образом помеченные пакеты 64-битного Windows Installer, которые делают возможной установку как 32-, так и 64-битных компонентов.
- **Политика ограничения использования программ** Политика ограничения использования программ позволяет защитить сеть от подозрительного ПО путем указания приложений, которым разрешено исполняться. Для идентификации приложения система может использовать хэш-правило, правила сертификата, пути или зоны Интернета.

Пакеты, «заплатки» и трансформации Windows Installer подчиняются политике ограничения использования программ. Уровнями, определяющими возможности пользователей запускать

то или иное ПО, являются неограниченный и ограниченный. В частности, Windows Installer исполняет только такие пакеты, для которых установлен неограниченный уровень. Если в процесс установки вовлечены «заплатки» или трансформации, то для успеха установки для них также должен быть задан неограниченный уровень.

Если в соответствии с политикой ограничения использования программ для пакета задан ограниченный уровень, Windows Installer сообщает об ошибке. Кроме того, Windows Installer помещает запись в журнал событий приложений.

Система применяет политику ограничения использования программ, когда приложение впервые устанавливается, когда к нему применяется новая «заплата» или когда Windows Installer нужно восстановить в кэше установочный пакет для приложения. Вы можете применить правила ограничения использования программ ко всем пакетам Windows Installer для администраторов и других пользователей.

Удаленное администрирование

Архитектура Windows Server 2003 включает дополнительные возможности удаленного управления, такие как Remote Desktop for Administration (часть Terminal Services), Microsoft Management Console (MMC), Active Directory Services Interface (ADSI), служба Telnet и WMI. Указанные средства могут быть объединены в две большие группы: встроенные инструменты ОС Windows Server 2003, такие как Active Directory, групповая политика, диспетчер событий, службы и др.; другая же группа связана с удаленным подключением к компьютерам через оснастку Remote Desktop и соединение Remote Desktop.

Компьютеры с Windows Server 2003 могут работать в среде «с погашенными огнями». В такой среде сервер может управляться удаленного без локальных операций, т. е. без использования на сервере клавиатуры, мыши, видеоплаты и монитора. Администратор может управлять и наблюдать за состоянием многих серверов из одного места, диагностируя и устраняя большинство проблем. За исключением установки или замены оборудования вы сможете выполнять все административные действия удаленно из любого места сети.

Сторонние средства администрирования

Независимые производители ПО предоставляют массу инструментов удаленного администрирования. Так, может оказаться полезным инструмент управления событиями, собирающий большие объемы событий из нескольких систем. Среди других инструментов — средства мониторинга производительности и планирования расширений, уведомляющие администратора о необходимости установки дополнительных аппаратных средств, а также средства мониторинга безопасности.

Remote Desktop for Administration

Remote Desktop for Administration (ранее известный как Terminal Services в режиме Remote Administration) предоставляет удаленный доступ к «рабочему столу» компьютеров, на которых установлена любая из ОС Windows Server 2003, позволяя вам администрировать свой сервер практически с любого компьютера в сети. Удаленное администрирование серверов с помощью Remote Desktop for Administration возможно с любого компьютера, на котором установлен одна из ОС семейства Windows Server 2003. Более простой вариант Remote Desktop доступен для Windows **XP** Professional.

Remote Desktop for Administration может значительно удешевить администрирование. Построенный на основе технологии Terminal Services, Remote Desktop for Administration предназначен специально для управления серверами. Он не поддерживает средства совместного использования приложений, многопользовательские возможности и исполнение процессов по расписанию, реализованные компонентом Terminal Server (ранее известным как Terminal Services в режиме Application Server). В результате Remote Desktop for Administration можно применять на сильно загруженном сервере, не создавая существенной дополнительной нагрузки на процессор. Это делает Remote Desktop for Administration удобным и эффективным сервисом удаленного администрирования.

Remote Desktop for Administration не требует от вас покупки отдельных лицензий для клиентских компьютеров, с которых осуществляется доступ к серверу. Нет надобности и в установке Terminal Server Licensing. Вы также можете выполнять все административные действия для ОС Windows Server 2003

с компьютеров с более ранними версиями Windows, установив на них Remote Desktop Connection.

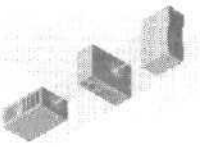
Дополнительные сведения

Дополнительные сведения см. по следующим адресам:

- Новинки Management Services — http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/mgmtsrvcs.mspx;
- Windows 2000 Management Services — http://www.microsoft.com/windows2000/technologies/management/;
- Using SMS 2.0 to Deploy Windows XP и Windows .NET Server — http://www.microsoft.com/smserver/techinfo/deployment/20/deployosapps/deploywinxp.asp;
- Application Deployment Using Microsoft Management Technologies — http://www.microsoft.com/windows2000/techinfo/howitworks/management/apdplymgt.asp;
- Web-сайт Microsoft Management — http://www.microsoft.com/management/;
- Web-сайт Software Update Services — http://www.microsoft.com/windows2000/windowsupdate/sus/.

ГЛАВА

5



Безопасность

Понятие сети предприятия включает не только локальные вычислительные сети (ЛВС), но и сочетания интрасетей, экстрасетей и сайтов Интернета; в результате безопасность системы стала важной как никогда. Windows Server 2003 содержит улучшения в традиционных средствах обеспечения безопасности, имевшихся в Microsoft Windows 2000 Server, и массу новых средств.

Microsoft сделала концепцию защищенных информационных систем (Trustworthy Computing) ключевой для всех своих продуктов. Концепция защищенных информационных систем — это модель разработки устройств на основе компьютеров и ПО. которые будут столь же безопасными и надежными, как бытовые приборы. Хотя сегодня платформы, реализующей концепцию защищенных информационных систем, не существует, Windows Server 2003 является важным шагом на пути претворения этой мечты в реальность.

Общеязыковая исполняющая среда (common language runtime, CLR) — это механизм исполнения программ, являющийся ключевым элементом Windows Server 2003, который повышает надежность среды для безопасных вычислений. CLR позволяет сократить число «дыр» в защите, вызываемых распространенными ошибками программирования. CLR проверяет приложения на наличие ошибок, а также проверяет права доступа, гарантируя тем самым, что программа выполняет только допустимые операции. Для этого выясняется, откуда данная программа была скачана или установлена, была ли она изменена после постановки на нее цифровой подписи и т. д.

В Microsoft просмотрели каждую строку кода ОС Windows Server 2003 в части своей общей программы с целью выявления мест возможных сбоев и слабых мест.

В этой главе обсуждаются инструменты и процессы, предоставляющие важные преимущества в области обеспечения безопасности: аутентификация, управление доступом, политика безопасности, аудит, Active Directory, защита локальных и сетевых данных, инфраструктура открытых ключей (public key infrastructure, PKI) и доверительные отношения,

Преимущества в области безопасности

Windows Server 2003 предоставляет более надежную и экономически выгодную платформу для ведения бизнеса, чем предыдущие версии Windows.

- **Снижение расходов** Обеспечивается за счет упрощения средств администрирования защиты, таких как списки управления доступом, Credential Manager и PKI.
- **Открытые стандарты** Протокол ШЕЕ 802.1X позволяет обеспечить безопасность беспроводных ЛВС от угроз подслушивания извне. Подробнее о других поддерживаемых стандартах см. RFC 3280, 2797, 2527 и 2459, а также криптографические стандарты открытых ключей (public key cryptography standards, PKCS) 1, 5, 8, 10 и 12.
- **Защита для портативных компьютеров и других устройств** Средства обеспечения безопасности, такие как файловая система с шифрованием (Encrypting File System, EFS), службы сертификатов и автоматическая регистрация по смарт-картам, позволяют обеспечить защиту для широкого диапазона устройств. EFS — это базовая технология шифрования и дешифрования файлов на томах NTFS. Открыть защищенный файл и работать с ним может только тот, кто его зашифровал. Службы сертификатов — это часть ядра ОС, благодаря которой предприятие может действовать как самостоятельный центр сертификации (certification authority, CA), выпускать цифровые сертификаты и работать с ними. Автоматическое использование сертификатов и средства автоподписки на сертификаты обеспечивают улучшенную защиту для пользователей сетей масштаба предприятия,

добавляя еще один слой аутентификации, позволяющий упростить реализацию защиты.

Аутентификация

Аутентификация позволяет выяснить, действительно ли человек или иной объект является тем, за кого себя выдает. При этом подтверждается источник и целостность информации, например, проверяется цифровая подпись или идентифицируется пользователь или компьютер.

Аутентификация является фундаментальным аспектом безопасности системы. Средства аутентификации в Windows Server 2003 обеспечивают единый вход в сеть для доступа ко всем ресурсам. Единый вход в сеть дает возможность пользователю, один раз войдя в домен по одному паролю или смарт-карте, аутентифицировать себя для любого компьютера в этом домене.

Типы аутентификации

Для идентификации пользователя может быть использовано несколько стандартных типов аутентификации. ОС семейства Windows Server 2003 поддерживают:

- **Kerberos** V5 служит для интерактивного входа в систему по паролю или смарт-карте; это также стандартный метод сетевой аутентификации для служб;
- **Secure Sockets Layer/Transport Layer Security** (SSL/TLS) применяется, когда пользователь пытается обратиться к защищенному Web-серверу;
- **NTLM** применяется, когда клиент или сервер используют одну из предыдущих версий Windows;
- **дайджест-аутентификацию** по данному протоколу параметры входа в систему пересылаются по сети как MD5-хэш или дайджест сообщения;
- **Passport** это служба аутентификации пользователя, обеспечивающая единую точку входа в сеть.

Защита Internet Information Services

При использовании Internet Information Services (IIS) аутентификация критически важна для обеспечения защиты. IIS 6.0 —

это полноценный Web-сервер, являющийся основой для Microsoft .NET Framework и существующих Web-приложений и Web-сервисов. IIS 6.0 оптимизирован для работы как серверная среда Web-приложений и Web-сервисов. В него был включен ряд возможностей, улучшающих безопасность, надежность, администрирование и производительность.

IIS позволяет изолировать отдельное Web-приложение или несколько Web-сайтов в независимый процесс, взаимодействующий с ядром напрямую. Независимые процессы предотвращают повреждение одним приложением или сайтом других Web-приложений сервера. IIS также предоставляет средства мониторинга для обнаружения, устранения и предотвращения сбоев Web-приложений.

IIS — это надежная платформа, предоставляющая инструменты и средства, которые обеспечивают простоту управления защищенным сервером. О средствах защиты в IIS 6.0 см. главу 8.

Интерактивный вход в систему

При интерактивном входе пользователя в систему выполняется его идентификация для локального компьютера или учетной записи в Active Directory. Подробнее о безопасности в Active Directory см. главу 3.

Сетевая аутентификация

Сетевая аутентификация удостоверяет личность пользователя для любой сетевой службы, к которой он пытается обратиться. Для поддержки аутентификации этого типа система безопасности включает следующие механизмы:

- Kerberos V5;
- сертификаты с открытыми ключами;
- Secure Sockets Layer/Transport Layer Security (SSL/TLS) Digest;
- NTLM (для совместимости с Windows NT 4.0),

Единый вход в сеть

Единый вход в сеть дает пользователям доступ к ресурсам сети без необходимости снова и снова вводить свои регистрационные данные. В Windows Server 2003 пользователям для доступа к сетевым ресурсам нужна лишь однократная аутентификация; последующие аутентификации для пользователя прозрачны.

Двухфакторная аутентификация

Средства аутентификации в Windows Server 2003 включают также двухфакторную аутентификацию, такую как применение смарт-карт. Смарт-карты — это устойчивый к подделкам и переносимый способ реализации защиты для таких задач, как аутентификация клиентов, вход в домен Windows Server 2003, цифровая подпись и защита электронной почты. Поддержка криптографических смарт-карт — ключевое средство инфраструктуры открытых ключей (PKI), интегрированной Microsoft в Windows XP/Server 2003. Смарт-карты предоставляют:

- устойчивое к подделкам хранилище для защиты закрытых ключей и другой персональной информации;
- изоляцию операций, включающихаутентификацию, обработку цифровых подписей и обмен ключами, от других частей компьютера; такие операции выполняются на смарт-карте;
- переносимость идентификационных данных и другой личной информации между компьютерами на работе, дома или в дороге.

При входе в сеть по смарт-карте для аутентификации пользователя в домене применяется идентификация на основе криптографии и доказательство собственности (proof of possession), Например, если злодей раздобыл пароль пользователя, он может выдать себя в сети за него, просто введя этот пароль. Многие люди выбирают легко запоминающиеся пароли, что делает их слабо защищенными от атак.

В случае смарт-карт нашему злодею, чтобы выдать себя за другого, потребуется получить как смарт-карту, так и личный идентификационный номер (PIN). Очевидно, что данная комбинация более устойчива к атакам, так как для подмены личности пользователя потребуется дополнительная информация. Дополнительным преимуществом является блокировка смарт-карты после небольшого числа неудачных последовательных попыток ввода PIN-кода, что крайне затрудняет словарную атаку на смарт-карту. (При этом PIN, кроме цифр, может содержать и другие символы.) Кроме того, смарт-карты устойчивы к необнаруживаемым атакам, так как злодею потребуется завладеть смарт-картой, что вряд ли останется незамеченным для пользователя.

Чтобы войти в домен по смарт-карте, пользователю не нужно нажимать Ctrl+Alt+Del. Он просто вставляет смарт-карту в считыватель, и компьютер предлагает ввести PIN-код вместо имени пользователя и пароля,

Управление доступом на основе объектов

Администраторы могут управлять доступом к ресурсам или объектам сети. Для этого с объектами, хранящимися в Active Directory, связываются дескрипторы защиты. В дескрипторе защиты перечислены пользователи и группы, имеющие доступ к данному объекту, а также предоставленные им права. Также дескриптор защиты задает аудит событий, связанных с доступом к объекту. Примеры объектов включают в себя пользователей, компьютеры и организационные подразделения (ОП). Управляя свойствами объектов, администраторы могут устанавливать права доступа, назначать владельца и осуществлять мониторинг доступа.

Администраторы могут контролировать не только доступ к конкретному объекту, но и доступ к его атрибутам. Настроив дескриптор защиты объекта, можно дать пользователю доступ только к части информации, скажем, к именам и телефонам сотрудников, но не к их домашним адресам. Для защиты компьютера и его ресурсов необходимо учитывать, какими правами будут обладать пользователи:

- можно защитить компьютер или несколько компьютеров, предоставив пользователям/группам определенные права;
- можно защитить объект, такой как файл или папку, назначив права, разрешающие пользователям/группам выполнять заданные действия с этим объектом.

Концепции управления доступом

Права доступа определяют действия, которые пользователь/группа могут выполнять над объектом или его свойством. Так, группе Finance можно предоставить права Read (Чтение) и Write (Запись) для файла Payroll.dat. Права доступа существуют для любых защищенных объектов, таких как файлы, объекты Active Directory или объекты реестра. Права доступа можно дать любому пользователю, группе или компьютеру. (Хорошей практикой является выделение прав доступа группам.) Права до-

ступа для объекта зависят от типа объекта. Например, права доступа к файлу отличаются от прав доступа к разделу реестра. Права доступа к объектам могут быть выданы:

- группам, пользователям и особым субъектам (special identities) домена;
- группам и пользователям любых доменов, которому доверяет данный домен;
- локальным группам и пользователям компьютера, на котором находится объект.

Устанавливая права доступа, вы задаете уровень доступа для групп и пользователей. Так, вы можете разрешить одному пользователю читать содержимое файла, другому — изменять его, а остальным — запретить к нему доступ. Можно задать права доступа к принтерам, чтобы лишь некоторые пользователи могли изменять конфигурацию принтера, а остальные — только печатать. Чтобы изменить права доступа к объекту, нужно запустить подходящий инструмент и изменить свойства этого объекта. Так, чтобы изменить права доступа к файлу, можно запустить Проводник Windows, щелкнуть имя файла правой кнопкой и затем — Свойства. Далее вы сможете изменить права доступа к файлу на вкладке Security.

При создании объекта ему назначается владелец. По умолчанию владельцем является создатель объекта. Независимо от текущих прав доступа к объекту его владелец всегда может их изменить.

Наследование облегчает администраторам выдачу и управление правами доступа. Это свойство обеспечивает автоматическое наследование объектами внутри контейнера всех наследуемых прав доступа к контейнеру. Так, при создании файла в папке он наследует права доступа, определенные для нее. Наследуются только те права доступа, что помечены как наследуемые.

Действующие права доступа

Вкладка Effective Permissions (рис. 5-1) — новая возможность в Windows Server 2003 — позволяет просмотреть все права доступа участника безопасности к данному объекту, включая права доступа, связанные с членством в группах.

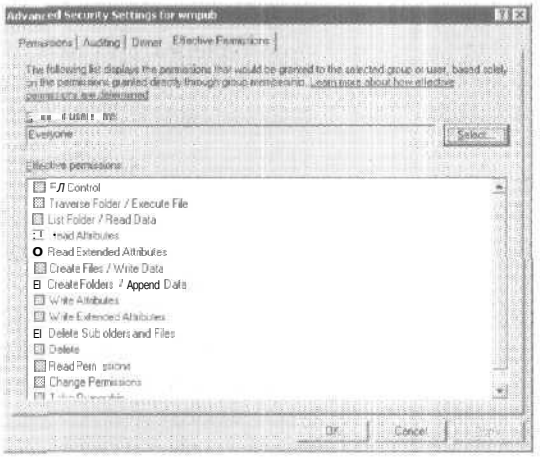


Рис. 5-1. Вкладка Effective Permissions

Для просмотра действующих прав доступа для пользователя или группы:

1. на вкладке Effective Permissions щелкните кнопку Select, чтобы открыть диалог Select User Or Group;
2. в поле Name введите имя интересующего вас встроенного участника безопасности, группы или пользователя;
3. можно также щелкнуть кнопку Object Types и затем выбрать Built-in Security Principals, Groups или Users;
4. щелкните OK.

Примечание Если участник безопасности является сетевым, вы можете щелкнуть Locations и выбрать цель, либо можно ввести имя домена с именем группы, например reskit\users. Важно указывать корректные типы объектов и места для поиска. В противном случае будет выдано сообщение об ошибке и предложение уточнить параметры поиска.

Права пользователей

Права пользователей предоставляют привилегии и права на вход в систему пользователям и группам сети.

Аудит объектов

Доступ пользователей к объектам можно подвергать аудиту, а сгенерированные в результате аудита события просмотреть в журнале Security с помощью Event Viewer.

Политика безопасности

На своем локальном компьютере или на нескольких компьютерах вы можете управлять политиками паролей, блокировки учетных записей, Kerberos, аудитом, правами пользователей и др.

Для создания общесистемной политики служат шаблоны безопасности, вызываемые из оснастки Security Configuration and Analysis. Вы также вправе редактировать правила политики локального компьютера, ОП или домена.

Security Configuration Manager

Позволяет создавать, применять и редактировать параметры защиты вашего локального компьютера, ОП или домена. Вот средства Security Configuration Manager:

- **шаблоны безопасности** позволяют определить политику безопасности в виде шаблона; такие шаблоны могут быть применены к групповой политике или к локальному компьютеру;
- **расширение параметров безопасности для групповой политики** позволяет редактировать отдельные параметры безопасности домена, сайта или ОП;
- **локальная политика безопасности** позволяет редактировать параметры безопасности локального компьютера;
- **команды Secedit** позволяют автоматически настроить безопасность из командной строки.

Оснастка Security Configuration and Analysis

Эта оснастка Microsoft Management Console (MMC) служит для анализа и настройки безопасности локального компьютера.

Анализ безопасности

Состояние ОС и приложений компьютера постоянно изменяется. Например, для разрешения административных или сетевых проблем может потребоваться временно изменить уровни

безопасности. Однако затем такое изменение часто забывают отменить.

Регулярный анализ позволяет администратору в рамках программы управления рисками предприятия отслеживать и гарантировать адекватный уровень безопасности для каждого компьютера. Администратор может выполнять тонкую настройку уровней защиты и обнаруживать изъяны в защите.

Оснастка Security Configuration and Analysis позволяет быстро просмотреть результаты анализа безопасности. Наряду с текущими характеристиками безопасности системы она предоставляет рекомендации и использует визуальные метки или ремарки для выделения областей, текущие характеристики которых не соответствуют требуемому уровню зашиты. Данная оснастка позволяет также устранять несоответствия, выявленные в результате анализа.

Настройка безопасности

Security Configuration and Analysis позволяет непосредственно настроить безопасность локального компьютера. Благодаря поддержке персональных баз данных, вы можете импортировать шаблоны безопасности, созданные с помощью Security Templates, и применить их к локальному компьютеру. Это приводит к немедленной настройке системы в соответствии с уровнями безопасности, определенными шаблоном.

Аудит

Аудит предоставляет способ выявления потенциальных проблем безопасности, помогает гарантировать учет действий пользователей и предоставляет доказательство фактов нарушения защиты. Для эффективного ведения аудита нужно установить политику аудита. При этом вы должны определить категории событий. объекты и виды доступа, подлежащие аудиту.

Установление стратегии

В основе вашей политики должна лежать некая стратегия. Например, вам может быть интересно, имел ли место доступ к системе или ее данным, или же вас может интересовать обнаружение незаконных попыток вмешательства в ОС,

Что обычно подлежит аудиту

Чаще всего аудит устанавливается для таких событий:

- начало и завершение сеанса работы пользователя с системой;
- управление учетными записями пользователей и группами;
- доступ к объектам, таким как файлы и папки.

Реализация политики аудита

При реализации политики аудита следуйте таким правилам.

- Разработайте стратегию аудита. Определите, что должно подлежать аудиту.
- Выберите только те категории аудита, которые соответствуют вашей стратегии, но не более того.
- Выберите подходящие размеры и правила сохранения для журнала безопасности. Для просмотра журнала безопасности и его параметров служит Event Viewer (рис. 5-2).
- Если вы решили вести аудит доступа к службе каталога или к объектам, то ваша стратегия должна определять тип объектов, подлежащих контролю. Определите минимум обращений, которые должны подлежать аудиту согласно вашей стратегии. Не ведите аудит большего числа объектов или видов обращений, чем нужно: слишком широкий диапазон событий может вызвать очень быстрое заполнение журналов защиты на постоянно загруженном компьютере.
- Реализуйте свою политику в системе. На отдельной машине это делается инструментом Local Security Policy, а в домене — через групповую политику.
- Регулярно просматривайте журналы безопасности. В аудите нет смысла, если вы не просматриваете журналы. Помочь вам в анализе журналов безопасности может система сбора журнала событий.
- По мере необходимости вносите коррективы в свою политику. Это может включать в себя добавление/удаление объектов/видов доступа, подлежащих аудиту, а также включение/отключение категорий аудита. В результате просмотра журналов вы можете прийти к выводу, что собрали информации больше или меньше, чем планировалось.

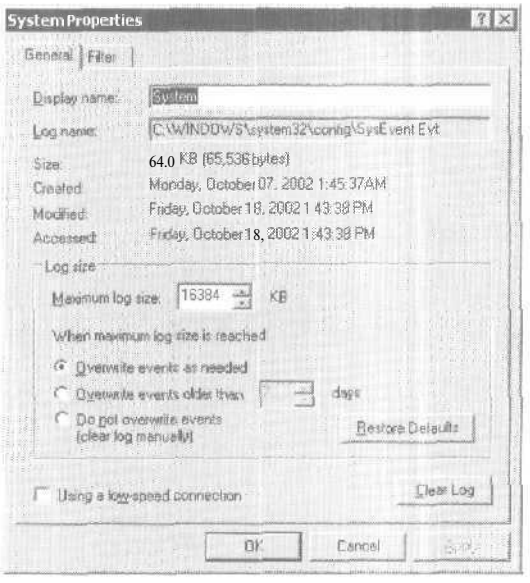


Рис. 5-2. Размер и правила сохранения журнала событий легко настраивать

Active Directory и безопасность

Служба Active Directory позволяет администраторам эффективно управлять аутентификацией и правами доступа пользователей. О безопасности и Active Directory см. главу 3.

Active Directory предоставляет защищенное хранилище пользовательских учетных записей и информации групп путем контроля доступа к объектам и регистрационной информации пользователей. Так как в Active Directory хранятся не только учетные данные пользователя, но и сведения о правах доступа, то после входа в сеть пользователь получает как аутентификацию, так и авторизацию для доступа к системным ресурсам. Например, при входе пользователя в сеть система безопасности аутентифицирует его, применяя информацию из Active Directory. Затем, когда пользователь пытается обратиться к сетевой службе, система проверяет информацию, заданную в списке избирательного управления доступом (discretionary access control list — DACL) для этой службы.

Так как Active Directory позволяет создавать группы пользователей, то администраторы могут эффективнее управлять безопасностью системы. Например, изменив свойства файла, администратор может разрешить чтение данного файла всем пользователям группы. Так что доступ к объектам в Active Directory можно задавать на основе членства в группах.

Защита данных

Хранимые (на постоянном или сменном носителе) данные можно защитить, применяя файловую систему с шифрованием (Encrypting File System, EFS) и цифровые подписи.

Encrypting File System

При использовании EFS данные сохраняются на диске зашифрованными. Для шифрования локальных данных NTFS EFS применяет алгоритм с открытым ключом. После того как пользователь зашифровал файл, он автоматически шифруется при каждом сохранении на диске. После того как пользователь отключил шифрование для файла, последний всегда записывается на диск незашифрованным. EFS предоставляет следующие возможности:

- пользователи могут шифровать свои файлы при сохранении на диске — нужно лишь установить флажок в диалоге Advanced Attributes файла (доступен через диалоговое окно свойств файла) (рис. 5-3);
- доступ к зашифрованным файлам происходит быстро и легко — при обращении к данным на диске они представляются пользователям в своем оригинальном виде;
- данные шифруются автоматически и прозрачно для пользователя;
- пользователи могут отменить шифрование файла, очистив поле Encrypt Contents в диалоговом окне Advanced Attributes свойств файла;
- администраторы могут восстановить данные, зашифрованные другим пользователем, — это гарантирует возможность доступа к данным, если зашифровавший их пользователь более недоступен или утратил свой закрытый ключ.

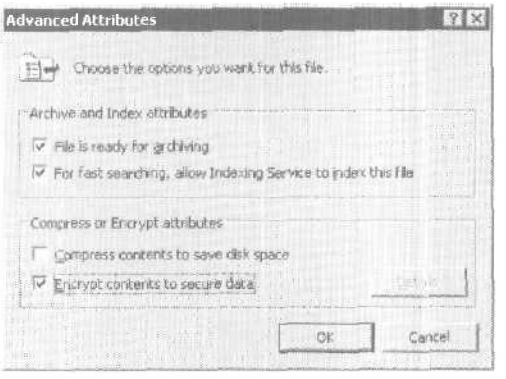


Рис. 5-3. Для шифрования нужно лишь установить флажок в поле Encrypt Contents

Примечание EFS шифрует данные только при записи на диск. Для шифрования данных, передаваемых по сети TCP/IP, имеется два дополнительных средства: Internet Protocol security (IPSec) и шифрование PPTP.

Настройка EFS по умолчанию не требует действий со стороны администратора — пользователи могут шифровать свои файлы сразу же. EFS генерирует для пользователя пару ключей шифрования, если они не были сгенерированы раньше. В качестве алгоритма шифрования применяется либо расширенный DES (extended Data Encryption Standard, DESX), либо TripleDES (3DES). Службы шифрования доступны из проводника Windows. Пользователи также могут зашифровать файл или папку с помощью утилиты командной строки *cipher*. Чтобы получить более подробную информацию об этой утилите, введите в командной строке «**cipher** /?». Пользователи шифруют файл или папку путем установки свойства шифрования для файлов и папок аналогично установке любого другого атрибута, такого как «только для чтения», «сжатый» или «скрытый». Если пользователь зашифровал папку, то все файлы и вложенные папки, добавляемые в зашифрованную папку, шифруются автоматически. Рекомендуется задавать шифрование на уровне папок. Сжатые файлы и папки не могут быть одновременно и зашифрованными. Если пользователь помечает сжа-

тый файл или папку для шифрования, то файл или папка будут распакованы. Кроме того, папки, помеченные для шифрования, на самом деле не шифруются. Шифруются только файлы внутри такой папки, а также файлы, создаваемые в ней или перемещаемые в нее. Расшифрованный файл остается таковым, пока вы не зашифруете его снова. Автоматическое восстановление атрибута шифрования для файла не выполняется. даже если он находится в каталоге, помеченном как зашифрованный.

Восстановление данных (data recovery) — это процесс дешифрования данных без закрытого ключа пользователя, зашифровавшего файл. Вам может понадобиться восстановить данные, применив агент восстановления (recovery agent), если пользователь уволился из компании, утратил свой закрытый ключ либо по запросу компетентных органов. Для восстановления файла агент восстановления:

- создает резервную копию зашифрованного файла;
- перемещает созданную копию в защищенную систему;
- импортирует в эту систему свой сертификат восстановления и закрытый ключ;
- восстанавливает резервные копии файлов;
- дешифрует файлы с помощью Проводника Windows или команды EFS *cipher.*

Оснастка Group Policy позволяет определить политику восстановления данных для серверов — членов домена, автономных серверов и членов рабочей группы. Вы можете либо запросить восстановление раскрытия либо экспортировать и импортировать ваши сертификаты раскрытия. Управление политикой восстановления данных можно возложить на особого администратора. Хотя число лип, имеющих право на восстановление зашифрованных данных, надо ограничить, предоставление права выступать в качестве агентов восстановления нескольким администраторам обеспечит дополнительные возможности для восстановления данных.

Цифровая подпись

Предоставляет доказательство того, что данные не были изменены после подписания, а также подтверждает личность человека или иного агента, подписавшего данные. Это позволяет реализовать критически важные для безопасных электронных

транзакций свойства целостности и невозможности отказа от обязательств.

Цифровую подпись обычно используют, когда данные распространяются открытым текстом, т. е. незашифрованными. При этом, хотя само сообщение может и не требовать шифрования, надо гарантировать, что оно не было изменено или отправлено самозванцем, так как в среде распределенных вычислений открытый текст вполне может быть прочитан и изменен в сети кем угодно.

CAPICOM

Windows Server 2003 включает поддержку CAPICOM 2.0. Данная поддержка позволяет разработчикам приложений посредством простого COM-интерфейса использовать средства CryptoAPI для работы с сертификатами и криптографией. Эта возможность позволяет разработчикам включить в приложения поддержку цифровой подписи и шифрования. Так как в ее основе лежит COM, то воспользоваться CAPICOM можно из разных сред, в том числе Visual C#, Visual Basic .NET, Visual Basic, Visual Basic Scripting Edition, JScript и др.

CAPICOM позволяет:

- формировать цифровую подпись и проверять произвольные данные с помощью смарт-карты или программного ключа;
- формировать цифровую подпись и выполнять проверку исполняемых файлов с использованием технологии Authenticode;
- генерировать хэш-значения для произвольных данных;
- графически отображать выбор сертификата и подробную информацию о нем;
- управлять и выполнять поиск в хранилищах сертификатов CryptoAPI;
- шифровать и дешифровать данные с помощью пароля или открытых ключей и сертификатов.

Защита сетевых данных

Сетевые данные внутри сайта (локальная сеть и подсети) защищены протоколом аутентификации. Для повышения уровня защиты можно применять шифрование сетевых данных внутри сайта. IPSec позволяет зашифровать все сетевые коммуникации для конкретных клиентов или для всех клиентов

домена. Данные, поступающие извне и отправляемые за пределы сайта (через интрасети, экстрасети или шлюз Интернета) помогут защитить следующие службы.

- **Internet Protocol Security** (IPSec) представляет собой набор служб защиты на основе криптографии, а также протоколы защиты.
- **Routing and Remote Access** конфигурирует протоколы удаленного доступа и маршрутизацию.
- **Internet Authentication Service** (IAS) предоставляет защиту и аутентификацию пользователям, подключающимся по телефонной линии.

Internet Protocol Security

IPSec — это набор, использующих криптографию служб защиты и протоколов безопасности. Так как он не требует изменений в приложениях или протоколах, его легко применять в существующих сетях.

IPSec предоставляет аутентификацию на уровне компьютера и шифрование данных для виртуальных частных сетей (virtual private network, VPN), использующих протокол туннелирования слоя 2 (Layer 2 Tunneling Protocol, L2TP). Ваш компьютер и VPN-сервер, поддерживающий L2TP, применяют IPSec для обмена начальной информацией, прежде чем будет установлено соединение L2TP. В процессе этого обмена обеспечивается безопасность паролей и данных. L2TP использует стандартные протоколы на базе PPP, такие как Extensible Authentication Protocol (EAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), MS-CHAP версии 2, CHAP, Shiva Password Authentication Protocol (SPAP) и Password Authentication Protocol (PAP) для IPSec.

Шифрование определяется ассоциацией безопасности Security Association (SA) IPSec. Ассоциация безопасности — это комбинация целевого адреса, протокола безопасности и уникального идентификатора SPI (Security Parameters Index). Среди поддерживаемых протоколов шифрования:

- стандарт DES (Data Encryption Standard), использующий 56-битный ключ;
- стандарт 3DES (Triple **DES),** использующий три 56-битных ключа и предназначенный для систем с повышенными требованиями к безопасности.

Маршрутизация и удаленный доступ

Служба Routing and Remote Access для ОС Windows Server 2003 — это полноценный программный маршрутизатор (router) и открытая платформа маршрутизации и межсетевого взаимодействия. Она предоставляет услуги маршрутизации для локальных и глобальных вычислительных сетей или по Интернету с использованием соединений VPN.

Преимуществом службы Routing and Remote Access является интеграция с ОС. Служба предоставляет ряд средств, позволяющих снизить затраты, и работает с разными аппаратными платформами и сотнями сетевых адаптеров. Данная служба может расширяться посредством API, который позволяет разработчикам создавать новые сетевые решения, а новым производителям аппаратных средств — участвовать в растущем бизнесе открытых сетей.

Служба IAS

Internet Authentication Service (IAS) в Standard Edition, Enterprise Edition и Datacenter Edition — это реализация сервера и прокси RADIUS (Remote Authentication Dial-In User Service) фирмой Microsoft:

- в качестве сервера RADIUS IAS выполняет централизованную аутентификацию соединений, авторизацию и учет пользователей для разных видов сетевого доступа, включая беспроводной, аутентифицирующий переключатель (authenticating switch), удаленный доступ по телефонным линиям и соединения VPN;
- в качестве прокси RADIUS IAS пересылает сообщения аутентификации и учета пользователей другим RADIUS-серверам; RADIUS — это стандарт IETF (Internet Engineering Task Force).

Инфраструктура открытых ключей

В эпоху всеобщего обмена информацией сеть предприятия может состоять из интрасетей, сайтов Интернета и экстрасетей — все они потенциально подвержены доступу нежелательных лиц. Возможны попытки мониторинга или изменения таких информационных потоков, как электронная почта, транзакции электронной коммерции и пересылаемые файлы. Ваша

организация может нанимать работников, о которых ничего не известно, но которым все же нужно предоставить доступ к части информационных ресурсов. Если для доступа к разным защищенным системам пользователям требуется множество паролей, то это может заставить их выбирать простые или одинаковые пароли, чтобы их было легче запомнить- Эти пароли не только легко вскрыть — они сразу дают им доступ к множеству защищенных систем и данных.

Как точно идентифицировать человека, обращающегося к информации, и на основе этой идентификации контролировать, к какой информации его можно допустить? Как управлять идентификационными параметрами пользователей в корпоративной сети? Ответы на эти вопросы может дать правильно спланированная инфраструктура открытых ключей (public key infrastructure, PKI) — система цифровых сертификатов, центров сертификации и других регистрационных агентств (registration authorities, RA), которые, применяя криптографию на основе открытых ключей, проверяют и удостоверяют подлинность участников электронной транзакции.

Организация может принять решение о развертывании PKI с помощью Windows по ряду причин.

- **Надежная защита** Вы можете обеспечить надежную аутентификацию при помощи смарт-карт. IPSec позволяет поддерживать конфиденциальность и целостность данных, передаваемых по сетям общего пользования, а EPS — защиту конфиденциальности хранимых данных,
- **Упрощенное администрирование** Организация может выпускать сертификаты и в сочетании с другими технологиями отказаться от паролей. Вы можете отзывать сертификаты и публиковать списки отзыва сертификатов (certificate revocation list, CRL). Сертификаты можно использовать для масштабирования доверительных отношений на всю корпоративную сеть. Вы также можете задействовать преимущества интеграции служб сертификатов с Active Directory и политикой. Можно также связывать сертификаты с пользовательскими учетными записями.
- **Дополнительные возможности PKI** Вы можете безопасно обмениваться файлами и данными по сетям общего пользования, таким как Интернет. Вы можете реализовать зашi-

щенную электронную почту, применяя S/MIME (Secure Multipurpose Internet Mail Extensions) и защищенные Web-соединения с помощью SSL (Secure Sockets Layer) или TLS (Transport Layer Security). Также можно усилить защиту беспроводных сетей.

В следующих разделах описываются возможности Windows Server 2003, которые помогут вам в реализации PKI.

Сертификаты

Сертификат — это цифровой документ, выпущенный некоторым агентством и подтверждающий подлинность его владельца. Сертификат связывает открытый ключ с личностью человека, компьютера или службы, имеющих соответствующий закрытый ключ. Сертификаты используются различными основанными на открытых ключах службами безопасности и приложениями, обеспечивающими аутентификацию, целостность данных и безопасные коммуникации.

Стандартный формат сертификата, используемый Windows, — это X.509v3. Сертификат X.509v3 содержит сведения о том, кому он выдан, о самом сертификате и необязательную информацию о центре, выпустившем его. Информация о субъекте может содержать имя, открытый ключ и алгоритм открытого ключа. Субъектом сертификата является тот, кому он выдан. Центр сертификации — это тот, кто выпустил и подписал сертификат.

Пользователи могут управлять сертификатами из оснастки MMC для сертификатов (рис. 5-4). Для автоматизации управления своими сертификатами пользователи могут разрешить для себя автоподписку на сертификаты.

Сертификаты можно применять для аутентификации пользователей Web-сайтов, аутентификации Web-сервера, защищенной электронной почты (S/MIME), IPSec, TLS и подписи кода программ (code signing). Сертификаты также выпускаются одним CA для другого с целью установления иерархии сертификации. Обычно сертификаты содержат;

- значение открытого ключа субъекта;
- сведения об идентификаторе субъекта, например, имя или адрес электронной почты;
- срок действия;

- информацию об идентификаторе эмитента сертификата;
- цифровую подпись эмитента сертификата, которая подтверждает достоверность связи между открытым ключом субъекта и его идентификатором,

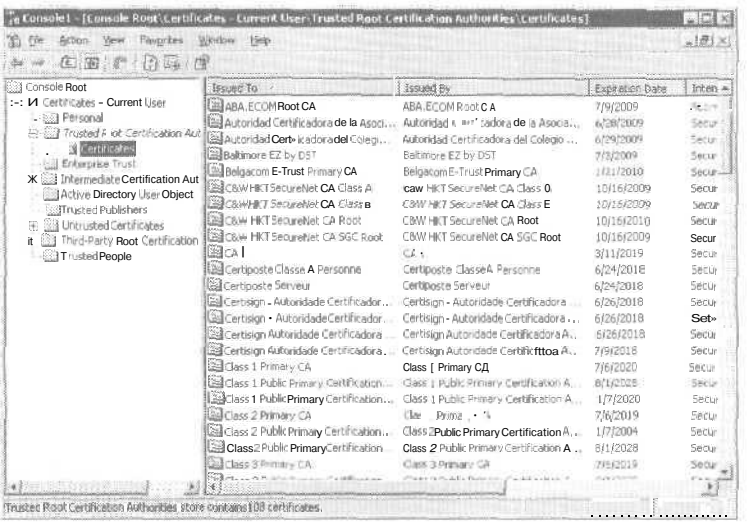


Рис. 5-4. Для управления сертификатами служит Microsoft Management Console

Сертификат действует только в течение указанного в нем срока; каждый сертификат содержит даты начала и окончания срока действия. По истечении срока действия сертификата субъект, им обладающий, должен запросить новый сертификат.

Сертификат может быть отозван эмитентом в тех случаях, когда надо отменить связь, подтверждаемую сертификатом. Эмитент поддерживает список отзыва сертификатов, к которому могут обращаться программы, проверяющие действительность сертификатов.

Одно из основных преимуществ сертификатов в том, что теперь серверам не нужно хранить пароли своих пользователей — достаточно установить доверительные отношения с выпускающим сертификаты. Если, например, Web-сервер определяет выпускающего сертификаты как корневой доверенный центр (trusted root authority), то тем самым доверяет правилам, которые использует этот центр для установления связей в выпус-

каемых им сертификатах. Фактически сервер доверяет центру сертификации проверку личности субъекта сертификата. Сервер определяет центр в качестве корневого доверенного центра, помещая сертификат этого центра, подписанного самим центром и содержащим его открытый ключ, в хранилище сертификатов корневых доверенных центров на компьютере-сервере. Промежуточные или подчиненные центры сертификации являются доверенными, только если к ним существует действительный сертификационный путь от корневого доверенного центра.

Службы сертификации

Службы сертификации (Certificate Services) — это компонент ОС Windows Server 2003, используемый для создания и управления CA. Задача CA — установление личности владельца сертификатов и ее подтверждение. CA также отзывает недействительные сертификаты и публикует CRL для использования при проверке сертификатов.

В простейшей архитектуре PKI имеется единственный корневой CA. На практике, однако, при использовании PKI будут устанавливаться несколько CA, организованных в иерархии сертификации. Для управления сервисами сертификации служит соответствующая оснастка MMC.

Шаблоны сертификатов

Сертификаты, выпускаемые CA, основываются на информации. переданной в запросе на сертификат, и параметрах, содержащихся в шаблоне сертификата. Шаблон сертификата — это набор параметров и правил, применяемых при обработке запросов на выдачу сертификата. Для каждого типа сертификата, выпускаемого CA предприятия, должен быть создан шаблон сертификата,

Шаблоны сертификатов в CA Windows Server 2003, Enterprise Edition и Datacenter Edition являются настраиваемыми и хранятся в Active Directory, доступные для использования всеми CA леса. Таким образом, администратор может выбрать один или несколько стандартных шаблонов, устанавливаемых вместе с сервисами сертификации, либо создать шаблоны, настроенные для определенных задач или ролей.

Автоподписка на сертификаты

Автоподписка (autoenrollment) позволяет настраивать автоматическую подписку на сертификаты, получение выпущенных сертификатов и обновление устаревших сертификатов субъектами без каких-либо действий со стороны самих субъектов. При этом субъект не должен ничего знать об операциях с сертификатами, если только шаблон сертификата не настроен на взаимодействие с субъектом или такого взаимодействия требует компонент шифрования (cryptographic service provider, CSP), скажем, в случае CSP для смарт-карт. Это значительно упрощает работу пользователей при применении сертификатов и минимизирует объем работы администратора. Для активизации автоподписки администраторы могут применить шаблоны сертификатов и настройки CA,

Web-страницы подписки

Web-страницы подписки (Web enrollment pages) — это отдельный компонент служб сертификации. Они устанавливаются по умолчанию, если при установке CA была разрешена отправка запросов на сертификаты через Web-браузер.

Кроме того, Web-страницы CA могут быть установлены на серверах с ОС Windows, на которых не установлен CA. В этом случае Web-страницы служат для перенаправления запросов на сертификаты центру сертификации, к которому почему-либо вы не хотите предоставлять прямого доступа.

Если для доступа к CA вы захотите создать свои Web-страницы, то Web-страницы, поставляемые вместе с Windows Server 2003, можно использовать как образец. О настройке служб сертификации и CA Web-страниц см. Microsoft Platform Software Development Kit.

Поддержка смарт-карт

Windows поддерживает вход в систему по сертификатам на смарт-картах, а также применение смарт-карт для хранения сертификатов и закрытых ключей. Смарт-карты можно использовать для Web-аутентификации, защищенной электронной почты, беспроводных сетей и других операций, применяющих криптографию на основе открытых ключей.

Политика открытых ключей

Средствами групповой политики можно автоматически распространять сертификаты субъектам, устанавливать общие доверенные центры сертификации и управлять политикой раскрытия данных для EFS.

Доверительные отношения

ОС семейства Windows Server 2003 поддерживают доверительные отношения между доменами и между лесами. Доверительные отношения между доменами дают пользователю возможность аутентификации для доступа к ресурсам в другом домене. При установке доверительного отношения между доменами надо принимать во внимание направление доверия (trust direction).

Направление доверия

Тип и направление доверительного отношения существенно влияют на путь доверия (trust path) — последовательность доверительных отношений, по которой должен проследовать междоменный запрос на аутентификацию.

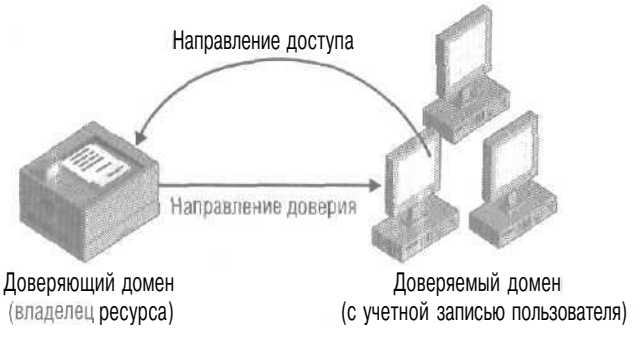


Рис. 5-5. Пути доверия и направления доверительных отношений

Прежде чем пользователь получит доступ к ресурсу в другом домене, система безопасности на контроллерах домена с Windows Server 2003 должна определить, имеет ли доверяющий домен (домен, содержащий ресурс, к которому пользователь пытается получить доступ) отношения доверия с доверяемым доменом (домен входа пользователя в сеть). Для этого систе-

ма безопасности вычисляет путь доверия между контроллерами доверяющего и доверяемого доменов. Стрелки на путях доверия, показанных на рис. 5-5, отражают направление доверия.

В каждое отношение доверия входят только два домена: доверяющий и доверяемый.

Типы доверительных отношений

Взаимодействие между доменами осуществляется посредством доверительных отношений. Доверительные отношения — это каналы аутентификации, наличие которых необходимо для доступа пользователей одного домена к ресурсам другого.

- **Односторонние доверительные отношения** Это однонаправленный канал аутентификации между двумя доменами. Такие отношения между доменами A и B означают, что пользователи домена A могут получить доступ к ресурсам домена B. Однако пользователи из домена B не могут получить доступ к ресурсам домена A. Односторонние доверительные отношения могут быть транзитивными или нетранзитивными:
  - транзитивные доверительные отношения проходят через группу доменов, такую как дерево доменов, и формируют связь между некоторым доменом и всеми доменами, которые ему доверяют; скажем, если домен A доверяет домену B, а B доверяет домену C, то A доверяет C; транзитивные отношения могут быть одно- или двусторонними и необходимы для аутентификации на базе Kerberos и репликации Active Directory;
  - нетранзитивные доверительные отношения ограничены двумя доменами; например, хотя домен A доверяет домену B, а домен B доверяет домену C, доверительные отношения между A и C отсутствуют; нетранзитивные отношения могут быть одно- или двусторонними.
- **Двусторонние доверительные отношения** Все доверительные отношения между доменами в лесу Windows .NET являются двусторонними и транзитивными. При создании нового дочернего домена между ним и его родительским доменом автоматически устанавливаются двусторонние транзитивные доверительные отношения. В двусторонних доверительных отношениях домен A доверяет домену B, а B

доверяет А. Это значит, что запросы на аутентификацию могут передаваться между этими доменами в обоих направлениях. Двусторонние доверительные отношения могут быть как транзитивными, так и нетранзитивными.

Доверительные отношения

Домен Windows .NET может устанавливать одно- или двусторонние доверительные отношения с:

- доменами Windows .NET в том же лесу;
- доменами Windows .NET в другом лесу;
- доменами Windows NT 4.0;
- областями (realm) Kerberos V5.

Доверительные отношения между лесами

В Windows Server 2003 администратор может создать доверительные отношения между лесами для расширения двусторонней транзитивности за пределы данного леса. Иначе говоря, доверительные отношения между лесами позволяют связать два леса Windows Server 2003 для формирования двусторонних транзитивных доверительных отношений между всеми доменами в обоих лесах. Доверительные отношения между лесами предоставляют следующие возможности.

- Упрощение управления ресурсами в двух лесах Windows Server 2003. Доверительные отношения между лесами сокращают число внешних доверительных отношений, необходимых для совместного использования ресурсов с другим лесом.
- Обеспечение двусторонних доверительных отношений между всеми доменами обоих лесов.
- Расширение сферы действия аутентификации пользователя. Аутентифицированное имя пользователя может применяться в обоих лесах.
- Большая доверительность данных авторизации. Для повышения доверительности данных авторизации, передаваемых между лесами, могут применяться и Kerberos, и **NTLM.**
- Гибкость администрирования. Совместная работа нескольких администраторов может быть разделена между административными единицами масштаба леса.

- Изоляция репликации Active Directory внутри каждого леса. Изменения схемы, конфигурации и добавление в лес новых доменов оказывают повсеместное воздействие только внутри данного леса, но не влияют на доверяющий ему лес.

Доверительные отношения могут быть созданы только между двумя лесами и, таким образом, не будут неявно распространяться на третий лес. Отсюда, если доверительные отношения созданы между лесами Forestl и Forest2, а также между лесами Forest2 и Forest3, то неявных доверительных отношений между лесами Forestl и Forest3 не возникнет.

Примечание В Windows 2000. если пользователям из одного леса нужен доступ к ресурсам другого, администратор мог создать внешние доверительные отношения между двумя доменами. Внешние доверительные отношения являются односторонними и нетранзитивными и, таким образом, позволяют расширять пути доверия на другие домены только путем явной настройки.

Дополнительные сведения

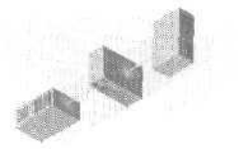
Дополнительные сведения см. по следующим адресам:

- новые возможности Internet Information Services 6.0 — http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/iis.mspx;
- Windows 2000 Security Services — http://www.microsoft.com/windows2000/technologies/security/;
- новые возможности Security for Windows XP — http://www.microsoft.com/windowsxp/pro/techinfo/planning/security/whatsnew/;
- расширения PKI в Windows XP Professional and Windows .NET Server — http://www.microsoft.com/windowsxp/pro/techinfo/planning/pkiwinxp/;
- защита и восстановление данных в Windows XP — http://www.microsoft.com/windowsxp/pro/techinfo/administration/recovery/;
- защита портативных компьютеров с помощью Windows XP Professional — http://www.microsoft.com/windowsxp/pro/techinfo/administration/mobile/;

- Wireless 802.11 Security в Windows XP -- http://www.microsoft.com/WindowsXP/pro/techinfo/administration/wirelesssecurity/;
- Institute of Electrical and Electronics Engineers — http://www.ieee.org/.

ГЛАВА

6



Коммуникации

Данная глава представляет техническое описание усовершенствований сетевых и коммуникационных средств в ОС семейства Windows Server 2003. Вы узнаете, какие преимущества сможете извлечь из улучшений средств подключения к сети, изменений в протоколах и расширенной поддержке сетевых устройств. Так, у мобильных пользователей появились новые возможности подключения к сети, такие как безопасный доступ в Интернет по беспроводным или Ethernet-соединениям. Теперь подключиться к сети можно через сотовый телефон, имеющий инфракрасный порт.

Windows Server 2003 позволяет администраторам управлять сетевой инфраструктурой, конфигурируя безопасный доступ к беспроводной ЛВС, с помощью правил групповой политики, а также создавая профиль диспетчера подключений (Connection Manager), позволяющий мобильным пользователям выбирать оптимальный VPN-сервер в зависимости от текущего местоположения.

Упрощенная установка, настройка и развертывание

Ниже описаны расширения, упрощающие установку, настройку и развертывание Windows Server 2003:

- средства сетевой диагностики;
- распознавание характеристик сети;
- расширенная поддержка беспроводных ЛВС;

- расширения службы маршрутизации и удаленного доступа;
- расширения диспетчера подключений.

Средства сетевой диагностики

В Windows Server 2003 были добавлены средства, облегчающие диагностику сетевых проблем.

- **Web-страница Network Diagnostics** Вызывается из раздела Tools в Help and Support или из раздела подробной информации в инструментах поиска неисправностей и настройки сети. Эта Web-страница позволяет получать информацию о локальном компьютере и сети, к которой он подключен. Страница также предоставляет доступ к различным тестам, выявляющим причины сетевых проблем.
- **Команды Netsh Diag** Новая вспомогательная DLL Netsh предоставляет команды для контекста Netsh Diag, позволяющие получать расширенную диагностическую информацию о сети и выполнять диагностические операции из командной строки. Для запуска диагностических команд Netsh введите в командной строке **netsh -c diag**.
- **Пункт меню Repair для сетевых подключений** Иногда состояние сетевого подключения может быть таким, что работа с сетью невозможна, однако конфигурацию можно восстановить путем выполнения набора стандартных процедур, таких как обновление параметров IP-адреса или регистрации имени в DNS, В контекстном меню каждого сетевого подключения есть пункт Repair, позволяющий избежать выполнения подобных процедур вручную. Выбор этого пункта вызывает выполнение последовательности шагов, которые позволяют устранить проблему конфигурации и гарантированно не приведут к более серьезным проблемам.
- **Вкладка Support для сетевых подключений** Диалоговое окно Status для каждого сетевого подключения из папки Network Connections теперь содержит вкладку Support, отображающую сведения о параметрах TCP/IP. Кнопка Repair на вкладке эквивалентна одноименному пункту контекстного меню сетевого подключения.
- **Вкладка Networking в диспетчере задач** Отображает в реальном времени текущие показатели производительности каждого сетевого адаптера компьютера (рис. 6-1).

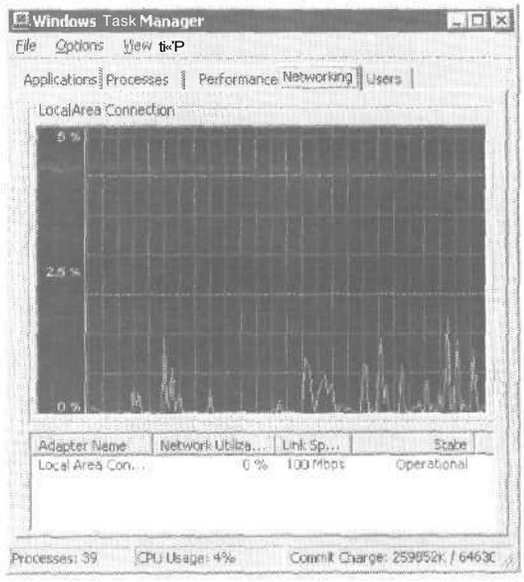


Рис. 6-1. Вкладка Networking в Task Manager появилась в Microsoft Windows XP и Windows Server 2003

- **Обновленная утилита командной строки для сетевой диагностики Netdiag.exe** Содержится на компакт-диске Windows Server 2003. Это расширенная версия Netdiag.exe из Microsoft Windows 2000 Resource Kit. Для установки вспомогательных утилит запустите файл Support.msi из папки Support/Tools на компакт-диске с дистрибутивом Windows Server 2003.
- **Пункт меню для включения журнала удаленного доступа** В диалоговое окно Remote Access Preferences, вызываемое из папки Network Connections, добавлена новая вкладка Diagnostics, позволяющая на уровне всего компьютера включать, просматривать и очищать журнал регистрации для подключений удаленного доступа. Чтобы вывести диалоговое окно Remote Access Preferences, выберите Remote Access Preferences из меню Advanced в папке Network Connections.

Распознавание характеристик сети

Распознавание положения в сети (network location awareness) позволяет компьютеру с Windows Server 2003 получать сведения о сети, к которой он подключен. Это дает возможность

автоматически настраивать стек сетевых протоколов для данного места в сети. Доступ к этой информации возможен также из Windows Socket API, что позволяет приложениям получать информацию о текущей сети или уведомления об изменении этой информации.

Распознавание характеристик сети также позволяет компонентам ОС семейства Windows Server 2003 предоставлять соответствующие сервисы. Так, новые параметры групповой политики для включения/отключения Internet Connection Sharing (ICS), Internet Connection Firewall (ICF) и Network Bridge учитывают характеристики сети; они применимы к компьютеру, только когда он подключен к сети, для которой эти параметры были заданы. Так, если портативный компьютер получает правило групповой политики, отключающее эти средства, когда он подключен к корпоративной сети, то при работе этого компьютера в домашней сети данные правила не применяются, и указанные средства могут быть использованы.

Расширенная поддержка беспроводных ЛВС

Ряд средств и расширений Windows Server 2003 упрощает развертывание беспроводных сетей, включая автоматическое управление ключами, а также аутентификацию и авторизацию пользователя перед доступом к ЛВС.

- **Расширенная безопасность Ethernet и беспроводных сетей (поддержка IEEE 802.1X)** Ранее для беспроводных сетей не было простого и безопасного решения развертывания с системой управления ключами. Microsoft и несколько поставщиков оборудования беспроводных ЛВС и ПК совместно с IEEE разработали стандарт ШЕЕ 802.1X управления доступом к сети на базе портов, который может быть использован как для Ethernet, так и для беспроводных ЛВС. Microsoft реализовала поддержку ШЕЕ 802.1X в Windows XP и работает *с* поставщиками оборудования беспроводных сетей для реализации поддержки стандарта в их точках доступа.
- **Беспроводные сети без необходимости настройки** Адаптер беспроводной сети Windows Server 2003 позволяет выбирать для настройки соединений нужную сеть без участия пользователя. Параметры для конкретной беспроводной сети могут быть сохранены и затем использованы автоматически при

следующем доступе к этой сети. Если ни одна из известных сетей недоступна, Windows Server 2003 может настроить адаптер беспроводной сети на специальный режим.

- **Поддержка «блуждающих» пользователей** Windows 2000 содержит расширения, позволяющие определять наличие сети и действовать соответствующим образом. Теперь эти возможности улучшены для обеспечения поддержки непостоянной природы беспроводных сетей. Среди новых средств в Windows Server 2003 — обновление конфигурации DHCP при новом подключении, повтор аутентификации при необходимости и выбор из нескольких вариантов конфигурации в зависимости от сети, к которой подключен компьютер,
- **Оснастка Wireless Monitor** Новая оснастка Wireless Monitor позволяет просматривать конфигурацию точки доступа или клиента беспроводной сети, а также отображать статистическую информацию.
- **Аутентификация с помощью пароля для защищенных беспроводных соединений** Windows Server 2003 поддерживает протокол PEAP (Protected Extensible Authentication Protocol) для соединений с беспроводными сетями. С помощью PEAP для защищенной аутентификации беспроводных соединений можно применять аутентификацию на основе пароля. Перед выполнением аутентификации PEAP создает шифрованный канал. Таким образом, обмен данными при аутентификации на основе пароля защищен от словарных атак в автономном режиме (offline dictionary attacks). Протокол MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocol version 2) теперь доступен как один из типов аутентификации EAP. PEAP с MS-CHAP v2 позволяет получить безопасную аутентификацию при беспроводном доступе без развертывания инфраструктуры сертификатов, известной также как инфраструктура открытых ключей (PKI), и без необходимости установки сертификатов на каждый беспроводной клиент. Сервер RADIUS (Remote Authentication Dial-In User Service) в Windows Server 2003, известный как Internet Authentication Service (IAS), расширен для поддержки PEAP.
- **Правила групповой политики для беспроводных** сетей Новое расширение групповой политики Wireless Network (IEEE

802.11) Policies позволяет задавать параметры беспроводной сети как часть групповой политики для компьютера. В параметры беспроводной сети входят список предпочитаемых сетей, параметры Wired Equivalent Privacy (WEP) и параметры IEEE 802.1X. Значение этих параметров рассылаются членам доменов, что облегчает развертывание конкретной конфигурации беспроводных соединений на клиентских компьютерах. Политика для беспроводных сетей настраивается из оснастки Group Policy в узле Computer Configuration/Windows Settings/Security Settings/Wireless Network (IEEE 802.11) Policies.

- **Неаутентифицированный** доступ к беспроводной ЛВС Как клиент беспроводной сети, так и IAS в Windows Server 2003 поддерживают беспроводные сетевые подключения без аутентификации. В этом случае протокол EAP-TLS (Extensible Authentication Protocol with Transport Level Security) служит для односторонней аутентификации сертификата IAS-сервера, а беспроводной клиент не передает имени и регистрационных параметров пользователя. Чтобы разрешить неаутентифицированный доступ для беспроводных клиентов, выберите Authenticate As Guest When User Or Computer Information Is Available на вкладке Authentication в диалоговом окне свойств беспроводного соединения в папке Network Connections. Чтобы разрешить неаутентифицированный доступ к серверу IAS, надо активизировать гостевую учетную запись и настроить политику удаленного доступа так, чтобы разрешить неаутентифицированный доступ для соединений EAP-TLS с использованием группы, содержащей гостевую учетную запись. Политика удаленного доступа может также задавать ID виртуальной ЛВС, соответствующий временному сетевому сегменту для неаутентифицированных пользователей.

  Благодаря этим расширениям возможны следующие сценарии:

  - мобильный пользователь, находясь в аэропорту, может получить безопасный доступ в Интернет по беспроводной или Ethernet-сети;
  - администратор может использовать эти расширения для настройки безопасного доступа к беспроводной сети; он

может также задать обязательное применение сертификатов, распространяемых средствами автоподписки и авторизации по правилам политики удаленного доступа, используемым **IAS;**

- администратор может настраивать аутентифицированный и авторизованный доступ к обычным ЛВС Ethernet без шифрования данных.

Расширения службы маршрутизации и удаленного доступа

В Windows Server 2003 включены следующие расширения службы маршрутизации и удаленного доступа (Routing and Remote Access).

- **Расширения оснастки и мастера установки** Мастер установки службы маршрутизации и удаленного доступа модифицирован так, чтобы упростить первоначальную настройку службы (рис. 6-2). Изменения в оснастке Routing And Remote Access упрощают конфигурирование параметров сервера после начальной установки.
- **Усовершенствованная настройка свойств EAP-TLS** Диалоговое окно Smart Card Or Other Certificate Properties теперь позволяет конфигурировать несколько серверов RADIUS и корневых центров сертификации. Это обеспечивает прозрачность работы с несколькими обычными или беспроводными сетями или большими сетями с несколькими серверами RADIUS. Чтобы вызвать это диалоговое окно, выберите Smart Card Or Other Certificate на вкладке Authentication в окне свойств соединения ЛВС, доступного в палке Network Connections, а затем — Properties.
- **Прокси разрешения имен для NetBIOS поверх TCP/IP** Новый прокси NetBIOS, встроенный в службу маршрутизации и удаленного доступа поверх **TCP/IP** (NetBT), позволяет клиентам удаленного доступа подключаться к сети, состоящей из одной или нескольких подсетей с единственным маршрутизатором (компьютер удаленного доступа с одной из ОС семейства Windows Server 2003), выполнять разрешение имен без использования DNS (Domain Name System) или сервера WINS (Windows Internet Name Service). Малые предприятия, таким образом, могут настроить удаленный доступ или VPN-сервер так, чтобы сотрудники могли работать дома,

При использовании прокси NetBT для разрешения имен подключающихся удаленно клиентов не требуется установка в сети малого предприятия сервера DNS или WINS,

- **Интеграция мастера Manage Your Server и службы маршрутизации и удаленного доступа** Данное средство предоставляет интегрированный способ настройки компонента NAT/Basic Firewall службы маршрутизации и удаленного доступа с использованием мастера Manage Your Server. Он поможет настроить сервер Windows .NET и компонент NAT/Basic Firewall во время единой процедуры установки.

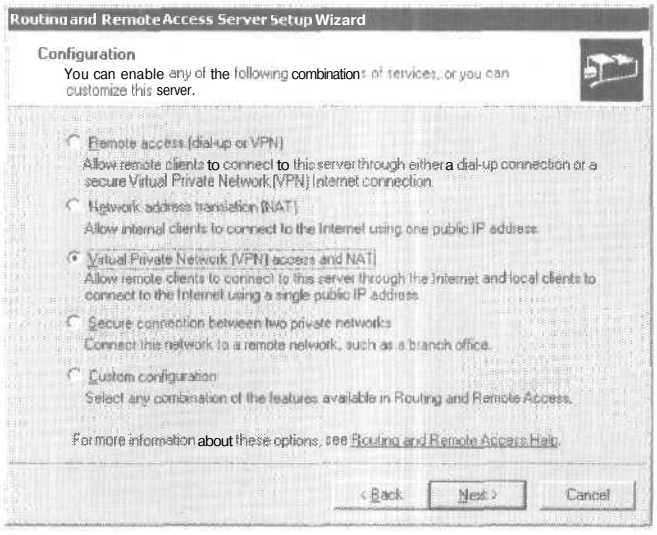


Рис. 6-2. Мастер установки службы удаленного доступа и маршрутизации значительно облегчает настройку разных типов удаленного доступа

- **Использование внутреннего интерфейса службы маршрутизации и удаленного доступа как закрытого интерфейса NAT** Компьютер с Windows 2000 Server, обеспечивающий удаленный доступ к закрытой интрасети и выступающий в качестве транслятора сетевого адреса NAT (Network Address Translator) для доступа к Интернету, не может обеспечить выход в Интернет подключенных к нему клиентов удаленного доступа. В Windows Server 2003 можно добавить внутренний (Internal) интерфейс в качестве закрытого интерфейса

к компоненту NAT службы маршрутизации и удаленного доступа, Это позволяет обеспечить выход в Интернет клиентам удаленного доступа.

- **Соединения по требованию (demand-dial) теперь могут использовать PPPoE** Данное средство позволяет использовать протокол PPPoE (Point-to-Point Protocol over Ethernet) для соединений, устанавливаемых по требованию. Соединения по требованию нужны службе маршрутизации и удаленного доступа для установления связи «точка — точка» при необходимости пересылки пакетов между двумя ЛВС. Для этого надо установить отметку в поле Connect Using PPP Over Ethernet (PPPoE) диалогового окна Connection Type мастера Demand-Dial Interface. Используя PPPoE для соединений по требованию, малое предприятие может задействовать компонент NAT/Basic Firewall службы маршрутизации и удаленного доступа и широкополосное соединение для подключения своего офиса к Интернету.
- **Усовершенствование поведения по умолчанию интерфейсов Internal и интерфейса Интернета** Дабы предотвратить проблемы при разрешении имени VPN-сервера и доступе к исполняющимся на нем службам, служба маршрутизации и удаленного доступа по умолчанию отключает динамическую регистрацию в DNS для интерфейса Internal, а для интерфейса, определенного в мастере Routing And Remote Access Server Setup как интерфейс Интернета, еще и NetBT.
- **Ограничение числа VPN-соединений для Windows Server 2003, Web Edition** Для указанного выпуска ОС число разрешенных соединений (на основе PPTP либо на основе L2TP) VPN равно 1. Это ограничение аналогично тому, что установлено для Windows XP Professional и Windows XP Home Edition. Для поддержки нескольких соединений VPN требуется Windows Server 2003 Standard Edition, Enterprise Edition или Datacenter Edition.
- **Интеграция NAT и брандмауэра** В компонент NAT/Basic Firewall службы маршрутизации и удаленного доступа добавлена поддержка базового брандмауэра (basic firewall) с той же технологией, что используется средством Internet Connection Firewall в Windows XP. Это позволяет защитить открытый интерфейс компьютера, на котором установлена

одна из ОС семейства Windows Server 2003, использующего NAT для доступа в Интернет. NAT позволяет защитить компьютеры внутренней сети, так как NAT-компьютер не пересылает из Интернета данные, не запрошенные клиентом из внутренней сети. Однако сам NAT-компьютер может быть уязвим для атак. При использовании базового брандмауэра для открытого интерфейса NAT-компьютера все получаемые из Интернега пакеты, не запрошенные этим компьютером (либо для себя, либо для клиентов в закрытой сети), удаляются. Для активизации этой возможности служит вкладка NAT/Basic Firewall в диалоге свойств закрытого интерфейса, для которого выбран компонент маршрутизации NAT/Basic Firewall.

- Прохождение **L2TP/IPSec** через NAT В Windows 2000 трафик Internet Key Exchange (IKE) и Encapsulating Security Payload (ESP) не мог проходить через NAT, так как NAT транслирует IP-адреса или порты пакетов, что нарушает безопасность пакетов. Это значит, что вы не можете создавать подключения L2TP,/IPSec через NAT и для подключений VPN должны использовать Point-to-Point Tunneling Protocol (PPTP). Семейство Windows Server 2003 поддерживает User Datagram Protocol (UDP), инкапсулирующий пакеты Internet Protocol security (IPSec) и позволяющий трафику IKE и ESP проходить через NAT. Это позволяет устанавливать подключения L2TP/IPSec между компьютерами, работающими под Windows XP/2000 Professional, и серверами под управлением Windows Server 2003, через одну или несколько систем NAT.
- Поддержка NLB для трафика **L2TP/IPSec** В Windows 2000 служба Network Load Balancing (NLB) не способна управлять ассоциациями безопасности IPSec (SA) среди нескольких серверов. Если сервер в кластере становится недоступным, управляемые этим кластером SA теряют родителя, и в конце концов срок их действия истекает. Это значит, что вы не могли кластеризовать серверы L2TP/IPSec VPN. Вы могли использовать циклическое назначение DNS (DNS round robin) для распределения нагрузки между несколькими серверами L2TP/IPSec VPN, но такой подход не обеспечивает отказоустойчивости. В семействе Windows Server 2003 служба NLB была усовершенствована, чтобы предоставлять поддержку

кластеризации для ассоциаций безопасности TPSec. Это значит, что можно создать кластер серверов L2TP/IPSec VPN и служба NLB будет обеспечивать как распределение нагрузки, так и отказоустойчивость для трафика L2TP/IPSec. Эта функция предоставляется только 32- и 64-разрядными версиями Enterprise Edition и Dalacenter Edition.

- **Конфигурирование ключей предварительной общей аутентификации для подключений L2TP/TPSec** Windows Server 2003 поддерживает в качестве методов аутентификации при установке ассоциаций безопасности IP Security (IPSec) для подключений L2TP как сертификаты компьютеров, так и ключи предварительной общей аутентификации (preshared key). Ключи предварительной общей аутентификации представляют собой текстовые строки, конфигурируемые на клиенте и на сервере VPN. Ключи предварительной общей аутентификации — довольно слабый метод аутентификации, поэтому применять их рекомендуется только при развертывании PKI, чтобы получить сертификаты компьютеров, или когда клиенты VPN требуют ключей предварительной общей аутентификации. Вы можете разрешить применение ключей предварительной общей аутентификации для подключений L2TP и задать ключ предварительной общей аутентификации на вкладке Security окна свойств сервера в оснастке Routing And Remote Access.

  Клиенты удаленного доступа VPN Windows XP и семейства Windows Server 2003 также поддерживают ключи предварительной общей аутентификации. Вы можете разрешить применение ключей предварительной общей аутентификации и задать ключ предварительной общей аутентификации из параметров TPSec на вкладке Security диалогового окна свойств подключения VPN в окне Network Connections. Ключи предварительной общей аутентификации также поддерживаются в Windows Server 2003 для VPN-подключений «маршрутизатор — маршрутизатор». Вы можете разрешить применение ключей предварительной общей аутентификации и задать ключ предварительной общей аутентификации для интерфейса соединений по требованию из параметров IPSec на вкладке Security свойств интерфейса соединений по требованию в оснастке Routing And Remote Access.

Усовершенствования диспетчера подключений

В семействе Windows Server 2003 были сделаны следующие усовершенствования диспетчера подключений (Connection Manager) и набора инструментов администратора диспетчера подключений (Connection Manager Administrator Kit).

- **Избранное диспетчера подключений** Функция Connection Manager Favorites позволяет устранить необходимость повторной настройки параметров диспетчера подключений пользователем при переключении между стандартными местами доступа к сети. Эта особенность предусматривает способ сохранения и легкого доступа к параметрам и применяется в следующем сценарии: пользователь часто перемещается между офисами компании и бизнес-партнеров. Для каждого из местоположений он задает параметры диспетчера подключений, в том числе ближайший телефонный номер для доступа, код области и правила дозвона и присваивает набору параметров уникальное имя. После этого он может выбирать один из сохраненных наборов параметров, чтобы быстро установить сетевое подключение из каждого местоположения.
- **Автоматическая настройка прокси** Функция автоматической настройки прокси (Automatic Proxy Configuration) позволяет создать профиль диспетчера подключений, гарантирующий, что во время подключения к корпоративной сети компьютер пользователя будет иметь соответствующий доступ к внутренним и внешним ресурсам. Данная функция требует применения Internet Explorer версии 4.0 или выше. Например, параметры домашнего компьютера сотрудника могут быть настроены на просмотр Интернета без любых параметров прокси. Такая конфигурация может вызвать проблемы при подключении к корпоративной сети. Администратор может создать профиль диспетчера подключений, устанавливающий нужные параметры прокси при подключении пользователя к корпоративной сети.
- **Файл журнала на стороне клиента** Эта особенность позволяет включить ведение журнала для быстрого и точного решения проблем диспетчера подключений. Так, пользователь может столкнуться с проблемами, устанавливая подключение к сети, применяющее предоставленный администра-

тором профиль диспетчера подключений. На компьютере клиента формируется файл журнала, который пользователь может переслать администратору для ускорения обнаружения и устранения проблемы.

- **Поддержка для выбора сервера VPN** Набор инструментов администратора диспетчера подключений (Connection Manager Administration Kit), поставляемый с Windows Server 2003, позволяет создать профиль диспетчера подключений, обеспечивающий пользователю возможность выбора сервера VPN, через который он подключается к корпоративной сети. Это обеспечивает связь VPN в таких сценариях:
  - офисы компании расположены по всему миру, и во многих из них есть серверы VPN; администратор может создать профиль диспетчера подключений, позволяющий мобильным пользователям выбирать сервер VPN, который лучше всего соответствует их потребностям на момент установки подключения;
  - корпоративный сервер VPN выключается для обслуживания; в это время пользователи могут выбрать для установки подключения другой сервер VPN.
- **Мастер Connection Manager Administration Kit** (CMAK) Набор инструментов администратора диспетчера подключений CMAK включает улучшенные диалоговые окна и возможность производить расширенную настройку перед созданием профилей пользователей. Улучшения упрощают процесс построения пакетов настраиваемых клиентских подключений и уменьшают потребность редактирования файлов .cms или .cmp для расширенной настройки. Большое число процедур настройки конфигурируется из мастера CMAK, в том числе процедуры настройки, разработанные специально для подключений VPN. Так, администратор может создать единственный профиль, чтобы разместить параметры системы безопасности для разных типов клиентских ОС, или настраивать профиль, чтобы задействовать возможности удаленного доступа к серверу вроде обратного вызова и служб терминалов.
- **Настройка ключей предварительной общей аутентификации** Позволяет администратору создать с помощью CMAK профиль диспетчера подключений, содержащий ключ пред-

варительной общей аутентификации сервера VPN для аутентификации при подключениях L2TP/IPSec.

- **Управление маршрутизацией подключений VPN для одновременного доступа к внутренней сети и Интернету** До Windows XP и семейства Windows Server 2003 клиент Microsoft VPN автоматически создавал маршрутизацию по умолчанию, отправлявшую весь трафик через туннель VPN. Хотя это позволяло клиенту VPN получить доступ к внутренней сети организации, доступ к ресурсам Интернета был возможен. только пока подключение VPN активно и если доступ к Интернету разрешен через VPN-подключение к сети организации. Новый диспетчер подключений, поддерживаемый Windows XP/Server 2003, учитывает описанный ниже вариант.

  Когда установлено подключение VPN, маршрутизация по умолчанию не изменяется. Вместо этого в таблицу маршрутизации клиента VPN добавляются указанные маршруты для местоположений во внутренней сети. Это обеспечивает одновременный доступ к ресурсам внутренней сети (по заданным маршрутам) и Интернета (по маршруту, заданному по умолчанию) без направления трафика Интернета через внутреннюю сеть организации. Connection Manager Administration Kit позволяет конфигурировать маршруты как часть профиля диспетчера подключений, предоставляемого пользователям VPN. Можно задать и URL, который содержит текущий набор маршрутов для внутренней сети организации или дополнительные маршруты, помимо указанных в профиле.

Усовершенствования подключения к Интернету

Ниже описаны усовершенствования подключения к Интернету в семействе Windows Server 2003:

- брандмауэр подключения к Интернету (Internet Connection Firewall);
- расширения сетевых подключений.

Брандмауэр подключения к Интернету

Когда компьютер подключен к Интернету или другим способом связан с внешним миром, появляется угроза несанкционированного доступа к компьютеру и его данным. Является ли

устройство, подключающееся к внешней сети, изолированным компьютером или шлюзом для другой сети. (например, когда применяется функция Internet Connection Sharing), брандмауэр может защитить домашнюю сеть от небезопасного сетевого трафика, в то же время пропуская соответствующий правилам сетевой трафик.

Брандмауэр подключения к Интернету (Internet Connection Firewall, ICF) позволяет защитить компьютеры и домашние сети. При запуске мастера новых подключений (New Connection Wizard) ICF автоматически разрешается для модемных и широкополосных подключений, при этом для брандмауэра задаются параметры по умолчанию, подходящие для большинства сетей. Применение брандмауэра для подключения также можно разрешить/запретить вручную через папку Network Connections.

ICF контролирует устанавливаемые с внутренней стороны брандмауэра подключения, чтобы определить трафик, который можно пропустить из внешней сети. По умолчанию прохождение трафика из внешней сети запрещено. Когда вы размещаете службы или программы (такие как Web-сервер) за брандмауэром, параметры ICF изменяются в соответствии с вашими потребностями. ICF может применяться для защиты удаленного подключения, когда устанавливается прямое соединение с поставщиком услуг Интернета, или для защиты подключения к ЛВС, когда соединение устанавливается через цифровую абонентскую линию или кабельный модем.

Данная возможность предоставляется только в 32-разрядных выпусках Standard Edition, Enterprise Edition и Web Edition.

Расширения сетевых подключений

Сетевые подключения в семействе Windows Server 2003 усовершенствованы.

- **Измененная групповая политика для сетевых и** модемных **подключений** Вы можете через групповую политику задать компоненты сетевой функциональности определенным пользователям с компьютерами под управлением Windows XP Professional/Server 2003. Эту особенность можно использовать в следующих сценариях.
  - Администратор может включить пользователя в группу Network Configuration Operators, чьи члены имеют доступ

к свойствам TCP/IP для подключений LAN и могут конфигурировать собственные IP-адреса.

- Если учетная запись входит в группу Administrators локального компьютера, пользователь может разрешать и настраивать ICS, ICF, Network Bridge и свойства сетевых подключений. Разрешение или перенастройка этих возможностей может повредить сетевым подключениям. Рассматриваемая особенность позволяет администратору задать политику, блокирующую настройку данных параметров даже для локальных администраторов.

- **Клиент Point-to-Point Protocol over Ethernet для широкополосных подключений к Интернету** Вы можете создавать подключения, использующие протокол Point-to-Point Protocol over Ethernet (PPPoE). Применение PPPoE и широкополосных подключений к Интернету, таких как DSL или кабельные модемы, позволяет пользователям получать индивидуальный аутентифицированный доступ к высокоскоростным сетям данных. В предыдущих версиях Windows пользователям требовалось устанавливать отдельное ПО, предоставляемое ISP. Теперь эта поддержка встроена в ОС. Клиент PPPoE позволяет использовать следующие сценарии,

  - Домашний пользователь имеет широкополосное подключение, требующее регистрацию PPPoE для подключения к Интернету. Встроенный клиент PPPoE и мастер новых подключений (New Connection Wizard) позволяют создать полностью интегрированное подключение к Интернету.
  - Администратор может сделать доступ к внутренней сети более безопасным, применив PPPoE для аутентификации доступа из областей в их офисах, таких как комнаты конференций.

  Наличие этой встроенной возможности предоставляет дополнительные рычаги для других функций вроде ICS (использование вашего широкополосного подключения совместно с другими компьютерами) и ICF (для защиты подключения PPPoE от атак из Интернета). Подключение PPPoE можно выбрать из Internet Explorer и других компонентов и приложений Windows.

Дополнительные возможности сетевого доступа

Ниже описаны расширения сетевого доступа, сделанные в семействе Windows Server 2003:

- сетевой мост (Network Bridge);
- удаленный доступ с использованием связки ключей диспетчера учетных записей (Remote Access Using Credential Manager Key Ring);
- управление учетными записями удаленного доступа для всех пользователей;
- поддержка протокола Internet Protocol over IEEE 1394 (IP/1394).

Сетевой мост

При построении сети для дома или малого офиса некоторые сетевые среды хорошо работают в одной части сети, но не подходят для другой. Например, некоторые компьютеры могут располагаться рядом с телефонными розетками, что позволяет соединять сетевые устройства через телефонную линию. Другие компьютеры могут быть расположены вдалеке от телефонных розеток, что потребует применения беспроводных сетевых подключений. Семейство Windows Server 2003 поддерживает работу с разными сетевыми средами, включая Ethernet, телефонные линии, беспроводные сети ШЕЕ 802.11b и IEEE 1394. Набор компьютеров, способных соединяться, используя определенную сетевую технологию, образует сегмент локальной сети.

Традиционно соединение различных сегментов LAN с применением TCP/IP требовало конфигурирование многочисленных адресов подсетей и маршрутизаторов для соединения различных сетевых сред. Сетевой мост позволяет компьютеру под управлением Windows Server 2003 соединить несколько сетевых сегментов в подсеть. Соединение нескольких сегментов LAN на компьютере моста сводится к выбору нескольких сетевых подключений в папке Network Connections: щелкнув правой кнопкой значок подключения, выберите пункт Bridge Connections контекстного меню.

В результате использования сетевого моста получается сетевая конфигурация, состоящая из легко настраиваемой под-

сети, соединяющей все сетевые среды. Компьютер моста определяет и управляет информацией о том, какие компьютеры в какой сегмент LAN подключены, и перенаправляет пакеты между соответствующими сегментами LAN.

Удаленный доступ с использованием связки ключей диспетчера учетных записей

В семейство Windows Server 2003 включена возможность формирования связки ключей диспетчера учетных записей (Credential Manager Key Ring), позволяющая управлять связкой ключей. содержащей набор учетных записей, которые могут применяться в системе. Это позволяет одновременно обращаться к нескольким сетям (с разными учетными записями, определяемыми именем пользователя и паролем) без необходимости постоянно повторно вводить данные учетной записи в ответ на приглашение системы. Информация о сетевом ресурсе, к которому вы подключаетесь (вроде имени сервера и имени домена), служит для выбора соответствующей учетной записи из связки ключей. Удаленный доступ участвует в связке ключей, добавляя по умолчанию временную учетную запись после успешной установки модемного или VPN-подключения. Эта учетная запись содержит имя пользователя и пароль, применяемые при установке подключения, так как зачастую эта же учетная запись разрешает доступ к сети. Это делает подключение к удаленной сети и доступ к ресурсам как локальной так и удаленной сетей, незаметными для пользователя,

Управление учетными записями удаленного доступа для всех пользователей

Функция управления учетными записями службы удаленного доступа для всех пользователей позволяет создавать подключение с набором учетных записей, имя и пароль которого будут доступны всем пользователям данного компьютера. Так, если на домашнем компьютере пользователя есть сетевое подключение к местному провайдеру Интернета, пользователь может из мастера новых подключений (New Connection Wizard) указать, что данное подключение является подключением для всех пользователей и сохранить учетную запись для всех пользователей. В этом случае другие члены семьи могут применять это

подключение, и им не надо помнить имя пользователя или пароль для подключений к ISP.

Поддержка протокола Internet Protocol over IEEE 1394 (IP/1394)

В Windows Server 2003 включена поддержка передачи и приема пакетов TCP/IP поверх сетевой среды IEEE 1394, последовательной шины, поддерживающей скорости передачи от 100 до 400 Мб/сек. IEEE 1394 обычно применяется для подключения аудио- и видеооборудования. Поддержка IEEE 1394 также включает специальную обработку кадров IEEE 1394 для сетевого моста. Подробнее см. документ RFC 2734. Подключения IEEE 1394 определяются и конфигурируются автоматически.

Изменения протоколов

В Windows Server 2003 были внесены изменения в сетевые протоколы, описываемые ниже:

- изменения и улучшения TCP/IP;
- стек протоколов IPv6;
- обработка Web-трафика в режиме ядра;
- усовершенствования качества обслуживания (Quality of Service).

Изменения и улучшения TCP/IP

В реализацию протокола TCP/IP для семейства Windows Server 2003 внесены такие изменения.

- **TCP/IP не может быть удален** TCP/IP устанавливается по умолчанию и не может быть удален. Одним из этапов диагностики неправильных параметров TCP/IP было удаление и повторная установка TCP/IP. В Windows Server 2003 вместо этого можно применить новую команду Netsh для сброса параметров TCP/IP в состояние по умолчанию. Подробнее см. ниже раздел «Команда Netsh для сброса TCP/IP в состояние по умолчанию».
- **Автоматическая альтернативная конфигурация для нескольких сетевых подключений** Позволяет вручную настроить статические параметры TCP/IP, задаваемые, когда компьютер является клиентом Dynamic Host Configuration Protocol

(DHCP), а сервер DHCP не найден при запуске компьютера. Для компьютеров под управлением Windows 2000/98/Me в случае, когда компьютер, настроенный как клиент DHCP, не может найти DHCP-сервер, служба Automatic Private IP Addressing (APIPA) назначает уникальный адрес из пространства адресов 169.254.0.0.16. Хотя APIPA позволяет запустить TCP/IP, она не назначает адрес шлюза по умолчанию, IP-адрес сервера службы доменных имен (DNS) или другие параметры, необходимые для связи во внутренней сети или в Интернете. Альтернативная конфигурация применяется, когда компьютер подключен к нескольким сетям, в одной из которых нет DHCP-сервера, а конфигурирование адресации APIPA нежелательно.

Например, пользователь работает на переносном компьютере в офисе и дома. В офисе параметры TCP/IP назначаются DHCP-сервером. Дома же DHCP-сервера нет, и компьютер автоматически использует альтернативную конфигурацию, обеспечивающую простой доступ к домашней сети и к Интернету. При наличии альтернативной конфигурации вам не надо вручную изменять параметры TCP/IP, когда компьютер перемещается между офисом и домашней сетью.

Вы можете настроить параметры альтернативной конфигурации TCP/IP на вкладке Alternate Configuration окна свойств протокола Internet Protocol (TCP/IP), доступного из окна свойств подключения LAN в папке Network Connections.

- **Команда Netsh для сброса TCP/IP в состояние по умолчанию** Позволяет сбросить параметры TCP/IP в состояние по умолчанию. Для этого в командной строке надо набрать **netsh interface ip reset.**
- **Новый параметр утилиты Netstat для отображения владельцев портов TCP** Позволяет отобразить активные подключения TCP вместе с идентификаторами процессов (PID) для каждого подключения. По значению PID на вкладке Процессы (Processes) Диспетчера задач (Windows Task Manager) можно найти соответствующее приложение. По умолчанию Диспетчер задач не отображает PID. Чтобы Диспетчер задач отображал PID, выберите в меню View пункт Select Columns, щелкните в списке столбцов PID (Process Identifier), а затем — кнопку OK.

- **IGMP версии 3** Позволяет создавать группы получателей широковещательных сообщений в зависимости от источника. Хосты могут запросить получение широковещательного трафика только из указанных источников либо из всех источников, кроме указанных.

  Информация об источнике предотвращает передачу широковещательного трафика через маршрутизатор в подсеть, не имеющую узлов, слушающих источник широковещательного трафика. Поддержка IGMPv3 включена по умолчанию и не требует настройки.
- **Автоопределение приоритетов маршрутизации на основе скорости интерфейса** Позволяет протоколу TCP/IP автоматически определять приоритеты маршрутизации для взятых из конфигурации TCP/IP маршрутов на основании скорости соответствующих интерфейсов. Так, маршруты, полученные из конфигурации TCP/IP для сетевого адаптера 10-Mbps Ethernet, имеют приоритет маршрутизации, равный 30, а маршруты, полученные из конфигурации TCP/IP для сетевого адаптера 100-Mbps Ethernet, — 20.

  Это полезно, если несколько интерфейсов с разными скоростями настроены на один шлюз по умолчанию. Самый быстрый интерфейс имеет самый низкий приоритет маршрутизации для заданного по умолчанию маршрута и служит для быстрой передачи трафика шлюзу. Если у нескольких интерфейсов одинаковая максимальная скорость, передавать трафик будет первый в списке привязки. Автоматическое определение приоритета интерфейса разрешается по умолчанию флажком Automatic metric на вкладке IP Settings и когда вы вручную настраиваете шлюз по умолчанию в диалоге Advanced TCP/IP Settings из окна свойств протокола Internet Protocol (TCP/IP) из подключения в папке Network Connections.
- **TCP получает размер окна, определяемый локальным сетевым адаптером** Размер окна определяет максимальное количество байт, которое может быть передано без требования подтверждения. Для низкоскоростных модемных сетевых подключений размер окна примерно равен размеру очереди на сервере удаленного доступа. Когда очередь заполнена TCP-сегментами одного TCP-подключения, новое TCP-подключение не может быть установлено, пока не от-

правлены эти пакеты. Алгоритм медленного запуска TCP для новых подключений делает ситуацию еще хуже. Рассматриваемая возможность позволяет планировщику пакетов качества обслуживания (QoS) на компьютере с ICS регулировать объявленный размер окна для соответствия скорости модемного сетевого подключения. Это сокращает очередь на сервере удаленного доступа и улучшает работу новых подключений.

В домашней сети все компьютеры обычно объединены высокоскоростной ЛВС, а доступ к Интернету осуществляется через компьютер с ICS. Компьютер с ICS подключается к Интернету через модем. Когда один из компьютеров пересылает большой файл, на других может снизиться скорость доступа к Интернету (например, при использовании Web-браузера). Благодаря рассматриваемой возможности скорость отклика новых TCP-подключений к Интернету уменьшается. Когда используется ICS, данная функция включена по умолчанию и не требует настройки.

Стек протоколов IPv6

В семейство Windows Server 2003 включен стек протоколов IPv6, возможности которого таковы.

- Поддержка Windows Sockets Поддержка новых функций Windows Sockets *getaddrinfo* и *getnameinfo* включена для разрешения «имя — адрес» и «адрес — имя» в приложениях Windows Sockets согласно документу RFC 2553. Применение этих функций вместо *getaddrbyname* и *gethostbyname* позволяет сделать приложения Windows Sockets независимыми от версии IP (IPv4 или IPv6), запущенной на компьютере.
- **Туннелирование** 6to4 Туннелирование 6to4 представляет собой технику, описанную в документе RFC 3056. Соответствующий компонент протокола IPv6 для семейства Windows Server 2003 обеспечивает автоматическое Туннелирование и связь IPv6 между узлами IPv6/IPv4 в локальной сети IPv4. Хосты 6to4 используют адреса IPv6, полученные из открытых адресов IPv4. С помощью техники 6to4 сайты и хосты IPv6 могут применять для коммуникаций адреса на основе 6to4 и Интернет IPv4 без необходимости получать глобаль-

ный префикс адреса IPv6 от ISP и IPv6-подключения к Интернету,

- **Intrasite Automatic Tunnel Addressing Protocol (ISATAP)** Механизм назначения адреса и автоматического туннелирования позволяет узлам IPv6/IPv4 в инфраструктуре сайта IPv4 использовать IPv6 для связи друг с другом, с узлами сетей, поддерживающих IPv6, к пределах сайта или в Интернете IPv6.
- **PortProxy** Облегчает связь между узлами или приложениями, которые не могут быть соединены с помощью общих протоколов уровня Интернета (IPv4 или IPv6). PortProxy обеспечивает прокси для трафика TCP в следующих вариантах подключений: IPv4 к IPv4, IPv4 к IPv6, IPv6 к IPv6 и IPv6 к IPv4. Для совместного существования и миграции IPv6/IPv4 PortProxy позволяет использовать следующие сценарии:
  - □ узел только с IPv4 может получить доступ к узлу только с IPv6;
  - п узел только с IPv6 может получить доступ к узлу только с IPv4;
  - п узел IPv6 может получить доступ к службе IPv4. запущенной на узле IPv6/IPv4.

  Последний сценарий позволяет компьютерам под управлением Windows Server 2003 с запущенным протоколом IPv6 использовать IPv6 для доступа к Web-страницам, расположенным на компьютерах под управлением Windows 2000 Server и Internet Information Services (IIS). Windows 2000 IIS не поддерживает IPv6, поэтому единственный способ получить доступ к нему — использовать IPv4. Когда на компьютере Windows Server 2003 настроен PorlProxy, входящие Web-запросы IPv6 преобразуются посредником и передаются серверу Windows 2000 IIS, позволяя серверу IIS связываться через посредника с Web-браузерами IPv6.

  Служба PortProxy настраивается командой **netsh interface portproxy add|set|delete v4tov4|v4tov6|v6tov4| v6tov6**.
- **Префиксы сайтов в объявлениях маршрутизатора** Публикуемые при связи префиксы могут быть настроены с длиной префикса сайта. Вы можете ввести команду **netsh interface ipv6 add|set route**. чтобы включить длину префикса сайта с префиксом адреса,

Когда параметры информации префикса задают получение префикса сайта, создается запись в таблице префиксов сайтов. Просмотреть эту таблицу позволяет команда **netsh interface ipv6 siteprefixes.** Таблица префиксов сайтов применяется, чтобы удалить не соответствующие местным сайтам адреса из возвращенных функцией Windows Sockets *getaddrinfo.*

- **Поддержка DNS** Обработка для записей узлов системы доменных имен (DNS) IPv6 (известных как записи ресурсов AAAA, или «четыре-А»), определенная в документе RFC 1886 «Расширения DNS для поддержки IP версии 6», и для динамической регистрации записей AAAA поддерживается клиентом DNS в Windows Server 2003 и службой DNS Server в Windows Server 2003/ 2000. Поддерживается прохождение трафика DNS как поверх IPv6, так и поверх IPv4.
- **Поддержка IPSec** Поддерживается обработка для Authentication Header (AH) с использованием хэша Message Digest 5 (MD5) и для Encapsulating Security Payload (ESP) с использованием заголовка NULL ESP и хэша MD5. Отсутствует поддержка шифрации данных ESP или протокола IKE. Политики безопасности IPSec, ассоциации безопасности и ключи шифрации должны быть настроены вручную с помощью утилиты Ipsec6.exe.
- **Поддержка компонентов ОС и приложений** Компоненты системы и приложения, поставляемые с Windows Server 2003, включая Internet Explorer, клиент Telnet (Telnet.exe), клиент FTP (Ftp.exe), IIS 6.0, службы файлов и печати (службы сервера и рабочей станции), Windows Media Services и Network Monitor поддерживают использование IPv6.
- **Поддержка RPC** Функции RPC служат для отправки вызовов прикладных функций в удаленную систему через сеть. Компоненты RPC в Windows Server 2003 разрешают применять IPv6. Компоненты RPC были изменены с целью использования модифицированного Windows Sockets, обеспечивающего работу RPC как поверх IPv4, так и поверх IPv6.
- **Поддержка IP Helper API** Internet Protocol Helper — это API, помогающий в администрировании сетевой конфигурации локального компьютера. IP Helper позволяет определять и изменять сетевую конфигурацию локального ком-

пьютера из программы. IP Helper также предоставляет механизмы оповещения, гарантирующие, что приложение будет уведомлено при изменении определенных параметров сетевой конфигурации локального компьютера. IP Helper в Windows Server 2003 усовершенствован с целью обеспечить получение информации для IPv6 и его компонентов.

- **Поддержка статической маршрутизации** Компьютер под управлением Windows Server 2003 может работать как статический маршрутизатор IPv6, перенаправляющий пакеты IPv6 между интерфейсами на основе таблицы маршрутизации IPv6. Статическая маршрутизация настраивается командой **netsh interface ipv6 add route.** Для службы маршрутизации и удаленного доступа протоколы маршрутизации IPv6 не предоставляются.

  Компьютер с Windows Server 2003 может посылать объявления маршрутизатора. Содержимое объявлений маршрутизатора автоматически получается из маршрутов, опубликованных в таблице маршрутизации. Неопубликованные маршруты могут служить для маршрутизации, но не посылаются в объявлениях маршрутизатора. Объявления маршрутизатора всегда содержат параметры, хранящие адрес канального уровня источника и максимальный размер передаваемого блока данных (MTU). Значение параметра MTU берется из значения MTU интерфейса отправителя для текущего соединения. Вы можете изменить это значение командой netsh **interface ipv6 set interface.** Компьютер под управлением Windows Server 2003 может объявить себя маршрутизатором по умолчанию (используя объявление маршрутизатора со сроком жизни маршрутизатора, отличным от 0), только если заданный по умолчанию маршрут настроен для публикации.

Обработка Web-трафика в режиме ядра

HTTP.sys — это реализация протокола Hypertext Transfer Protocol (HTTP), работающая в режиме ядра как на стороне сервера, так и на стороне клиента. Это сделано для масштабируемой, эффективной реализации HTTP, позволяющей применять истинный асинхронный ввод-вывод Win32, включая возможность привязки завершения запроса и ответа к закрытию порта. **API** пользовательского режима для клиентской стороны предостав-

ляется через такие API, как WinHTTP и .NET Framework Classes. На стороне сервера HTTP.sys предоставляется Windows Server 2003 и используется через IIS 6.O. Полная версия HTTP.sys. включающая и клиентскую и серверную части, будет поставляться со следующими версиями Windows.

Усовершенствования качества обслуживания (Quality of Service)

Когда домашняя сеть подключается к корпоративной или другой сети через медленное соединение, такое как телефонная линия, скорость трафика может снизиться.

Если получающий данные клиент расположен в относительно быстрой сети (например 100-Mbps Ethernet) за блоком ICS и сервер, с которым клиент устанавливает связь, расположен в быстрой сети за блоком удаленного доступа, возникают ошибки. В этом сценарии получателю на основании скорости подключения выделяется окно большого размера. Отправитель начинает посылать данные с низкой скоростью, но, поскольку пакеты не теряются, отправитель увеличивает их размер почти до полного размера окна.

Это может влиять на производительность других TCP-подключений, проходящих по той же сети, так как их пакеты попадают в потенциально большую очередь. Если пакет теряется, повторно передается полный размер окна, еше больше нагружая соединение. Решение в том, чтобы иметь на краю сети компьютер ICS, устанавливающий размер окна получателя в меньшее значение, которое отменяет спецификацию получателя и соответствует медленному соединению. Это не будет неблагоприятно влиять на трафик, поскольку размер окна устанавливается так, как если бы получатель был подключен напрямую к медленному соединению. Такую настройку окна выполняет планировщик пакетов QoS, запускаемый на компьютере ICS.

Информацию о QoS см. на Web-сайте Windows 2000 Networking and Communications Services по адресу: *http:// www.microsoft.com/windows2000/technologies/communications/.*

Улучшенная поддержка сетевых устройств

Ниже вы узнаете о таких улучшениях поддержки сетевых устройств, как;

- инкапсуляция постоянных виртуальных каналов;
- **NDIS** 5.1 и Remote **NDIS;**
- улучшенная поддержка сетевых сред;
- CardBus Wake on LAN;
- усовершенствованные драйверы устройств;
- Wake on LAN: усовершенствованный выбор события пробуждения;
- драйвер модема IrCOMM для IrDA.

Инкапсуляция постоянных виртуальных каналов

В Windows Server 2003 включена реализация RFC 2684, чтобы упростить для поставщиков реализацию DSL. Реализация включает промежуточный драйвер NDIS, подобный интерфейсу Ethernet, но использующий для передачи кадров Ethernet (или TCPДР) постоянные виртуальные каналы и асинхронный режим передачи DSL (ATM). В Windows Server 2003 с драйвером минипорта ATM для устройств DSL развертывание DSL может использовать следующие конфигурации драйверов:

- TCP/IP поверх PPP поверх ATM (PPPoA) с использованием драйвера минипорта DSL ATM, предоставляемого поставщиком;
- TCP/IP поверх RFC 2684 (четыре типа инкапсуляции) с использованием драйвера минипорта DSL ATM, предоставляемого поставщиком;
- TCPДР поверх PPPoE поверх RFC 2684 (четыре типа инкапсуляции) с использованием драйвера минипорта DSL ATM, предоставляемого поставщиком;

Кроме того, в интерфейс RFC 2684 Ethernet может быть добавлена аутентификация 802.1X. Разнообразные варианты охватывают потребности большей части вариантов развертывания DSL. Дополнительные сведения см. в документе RFC 2684.

NDIS 5.1 и Remote NDIS

Сетевые карты и их драйверы делают физическую сеть доступной ОС, поэтому в Windows Server 2003 усовершенствованы соответствующие протоколы.

- **Plug and Play и уведомления о событиях системы питания** Позволяет уведомлять драйвер минипорта сетевой карты о событиях системы электропитания или Plug and Play. Это обеспечивает более устойчивую работу системы при возникновении данных событий.
- **Поддержка отправки запроса о завершении** Позволяет сетевым протоколам избегать длительного ожидания сетевых пакетов путем отправки запроса о завершении.
- **Увеличение емкости статистики (64-разрядный счетчик статистики)** Обеспечивает получение точной сетевой статистики даже для высокоскоростных сетевых сред.
- **Улучшенная производительность** Увеличена скорость передачи данных по критическим сетевым путям за счет исключения ненужного дублирования пакетов.
- **Изменения Wake on LAN** Теперь включение от сетевого адаптера можно задать только при получении специальных пакетов (вместо задаваемых протоколом шаблонов пакетов). Эта возможность настраивается на вкладке Power Management окна свойств сетевого адаптера.
- **Прочие изменения** Дополнительные изменения учитывают пожелания разработчиков драйверов и улучшают целостность драйверов.

Remote NDIS, включенный в семейство Windows Server 2003. разрешает поддержку сетевых устройств, подключаемых через USB, без установки драйверов сторонних производителей. Microsoft предоставляет драйверы, необходимые для связи с сетевыми устройствами. Это обеспечивает более простую установку и уменьшает возможность отказа системы из-за плохо построенного или непроверенного драйвера.

Об NDIS 5.1 и Remote NDIS см. в DDK семейства Windows Server 2003 и на Web-страницах:

- http://www.microsoft.com/hwdev/tech/network/NDIS51.htm;
- http://www.microsoft.com/hwdev/tech/network/rmNDIS.htm,

Улучшенная поддержка сетевых сред

В Windows Server 2003 добавлена поддержка новых сетевых устройств. В частности, включена поддержка многих новых устройств для домашних сетей. Поддерживаются новые устройства HomePNA (телефонные линии). В Windows Server 2003 поддерживается большинство сетевых устройств, подключаемых через USB; некоторые из них используют Remote NDIS, что исключает необходимость установки дополнительных драйверов. Улучшена поддержка беспроводных устройств 802.11. Многие из этих устройств поддерживают беспроводную нулевую конфигурацию и возможности роуминга Windows Server 2003. Расширена и поддержка модемов для включения в список оборудования программируемых модемов.

CardBus Wake on LAN

Позволяет выводить компьютер из состояния ожидания по сигналу от карты CardBus. Администратор может использовать эту возможность для управления группами серверов.

Усовершенствованные драйверы устройств

Добавлено несколько возможностей в драйверы сетевых устройств, обычно используемых для домашних сетей, и удалены устаревшие унаследованные драйверы. Улучшено качество сетевых драйверов. Категории драйверов перечислены ниже.

- **Драйверы локальных сетей** Включают сетевые карты 10/100, ШЕЕ 802.11 и Home Phoneline Networking Alliance (HomePNA).
- **Широкополосные** Включают кабельные модемы, асимметричные цифровые абонентские линии (ADSL) и цифровые сети с комплексными услугами (ISDN).
- **Модемы** Включают модемы, основанные на драйверах и модемы 56-Kbps V.90.

Домашний пользователь, обновляющий компьютер до Windows Server 2003, обнаружит, что его сетевые устройства поддерживаются новой ОС.

Wake on LAN: усовершенствованный выбор события пробуждения

Функция Wake on LAN (WOL), появившаяся в Windows 2000, представляет собой аппаратную возможность сетевых карт с поддержкой WOL, позволяющую сетевой карте управлять включением электропитания компьютера при получении сетевых пакетов, соответствующих определенному шаблону:

- WOL допускается для всех пакетов, соответствующих образцу события пробуждения;
- WOL допускается только для специальных пакетов, вызывающих событие пробуждения;
- WOL полностью отключен,

Новые возможности позволяют использовать следующие сценарии.

- Для экономии энергии пользователь хочет перевести компьютер в спящий режим с малым энергопотреблением. Он также хочет, чтобы компьютер выходил из спящего режима, если другой компьютер в сети обращается к службам, расположенным на его компьютере, или для выполнения операций управления данным компьютером.
- Администратор хочет управлять WOL на компьютерах и полностью разрешает функционирование WOL.

Драйвер модема IrCOMM для IrDA

Драйвер модема IrCOMM позволяет применять в качестве модема сотовые телефоны с инфракрасным портом. Когда сотовый телефон располагается в зоне видимости инфракрасного порта, обнаруживается новое устройство и устанавливается соответствующий драйвер (или стандартный драйвер, если модель не определена). После этого мобильный телефон можно использовать как обычный модем для установки сетевых подключений.

Данный драйвер позволяет применить следующий сценарий: пользователь хочет получить доступ в Интернет по мобильному телефону с инфракрасным портом и поддержкой протокола IrCOMM. Переносной компьютер опознает мобильный телефон, включает его в список устройств и устанавливает в качестве модема. Теперь пользователь может устанавливать

модемное подключение к Интернету так же. как и при использовании встроенного модема.

Возможность предоставляется только в системах Enterprise Edition и Web Edition.

Поддержка новых сетевых служб

Ниже описаны улучшения поддержки сетевых служб в семействе Windows Server 2003.

- провайдеры служб TAPI 3.1 и TAPI;
- клиентский API Real Time Communication;
- **DHCP;**
- **DNS;**
- WINS;
- IPSec.

TAPI 3.1 и TAPI Service Providers

Предыдущие версии Windows поставлялись с ранними версиями Telephony API (TAPI), наиболее поздней версией является TAPI 3.0, поставляемая с Windows 2000. TAPI позволяет создавать приложения, предоставляющие пользователям услуги телефонной связи.

В Windows XP/Server 2003 входит TAPI 3.1. который поддерживает модель COM и предоставляет программисту набор COM-объектов. Это позволяет для написания телефонных приложений применять любую среду программирования или язык сценариев с поддержкой COM. В Windows Server 2003 включены провайдеры служб TAPI (TSP), предоставляющие функциональные возможности для IP-телефонии на базе H.323 и широковещательных видео- и аудиоконференций в сетях TCP/IP. Это расширение провайдеров TSP из предыдущих версий Windows. H.323 TSP и провайдеры медиа-служб (MSP) поддерживают H.323 версии 2. TAPI 3.1 предоставляет также следующие возможности.

- **Файловые терминалы** Позволяют приложениям записывать потоковые данные (такие как речь или видео) в файл и воспроизводить записанные данные обратно в поток.

- **Подключаемые терминалы** Позволяют сторонним фирмам добавлять новые объекты терминалов, которые может использовать любой MSP.
- **TSP для USB-телефонов** Позволяет приложению управлять USB-телефоном и использовать его как конечное устройство для потоковых данных.
- **Автообнаружение серверов TAPI** Позволяет клиентам обнаруживать доступные в сети телефонные серверы,

Для H.323 были реализованы дополнительные службы (обеспечивающие более богатые возможности контроля звонков):

- служба задержки вызовов (рекомендация ITU-T H.450-2);
- служба передачи вызовов (рекомендация ITU-T H.450-2);
- служба отклонения вызовов (рекомендация ITU-T H.450-3);
- служба удержания и возобновления вызовов (рекомендация ITU-T H.450-5).

Клиентский API Real Time Communication

Клиентский API Real Time Communication (RTC) обеспечивает коммуникационную платформу следующего поколения, основанную на протоколе Session Initiation Protocol (SIP). SIP предоставляет протокол для установки стандартного сеанса с использованием адреса электронной почты без необходимости знать местоположение вызывающего; поэтому коммуникация становится более эффективной. RTC обеспечивает быстрое развертывание Интернет-приложений, расширенных вспомогательными приложениями, такими как приложения для передачи голоса, видео и данных.

Windows Server 2003 включает клиентский API RTC с такими возможностями, как управление списком друзей, обнаружение активности пользователя, создание сеансов мгновенной передачи сообщений, а так же видео- и аудиосеансы между двумя клиентами, телефонные звонки на любой телефонный номер, совместный доступ к приложениям и сеансы дискуссий, Клиентский APIs включает защищенное туннелирование на сервер SIP по протоколу Secure Sockets Layer (SSL), цифровую и базовую аутентификации и логику NAT для разрешения сеансов подключений в реальном времени через NAT с поддержкой Universal Plug and Play (UPNP). Качество аудио и видео улучшено.

- **Подавление акустического эха** Для голосовых звонков не требуются гарнитуры, а встроенное подавление эха обеспечивает высококачественную связь.
- **Контроль качества** Новый алгоритм динамически изменяет параметры аудио и видео на основе обнаруживаемых изменений состояния сети,
- **Прямая коррекция ошибок** Прямая коррекция ошибок (FEC) служит для компенсации потери пакетов, вызванной загруженностью сети.
- **Динамически изменяемый буфер** Динамически изменяемый буфер позволяет устранить искажения полученного аудиосигнала, вызываемые неравномерной задержкой между получаемыми пакетами.

Клиентский API RTC позволяет использовать следующие сценарии.

- Разработчик игр использует возможности клиентского RTC API для добавления в новые игры списков друзей, мгновенных сообщений и аудио/видео. Пользователи во время игры могут отправлять сообщения, разговаривать и видеть друг друга.
- Администратор пишет небольшое приложение, которое оповестит всех пользователей о выключении сервера электронной почты для техобслуживания.
- ISV, создающий приложения для управления бюджетом и платежными ведомостями, создает элемент управления ActiveX, использующий клиентский RTC API. Он встраивает его в Web-страницы сервера, чтобы администраторы отделов могли просматривать доступные им платежные ведомости, задавать вопросы о бюджете через систему мгновенных сообщений или голосовую связь и совместно анализировать статьи бюджета, используя общий доступ к приложениям.

Этой возможности пег в 32-разрядной версии Web Edition.

DHCP

В Windows Server 2003 были сделаны следующие усовершенствования службы Dynamic Host Configuration Protocol (DHCP).

- **Архивация и восстановление БД DHCP** Оснастка DHCP теперь предоставляет новые пункты меню для архивации и

восстановления базы данных DHCP. Когда пользователь щелкает один из этих пунктов меню, открывается окно браузера, предлагающее выбрать местоположение или создать новую папку. Администратор может использовать эту возможность для архивации и восстановления на серверах, работающих под управлением Windows Server 2003. Данная возможность отсутствует в Web Edition.

- **Параметры бесклассового статического маршрута** Клиент DHCP может запросить этот параметр, чтобы получить список маршрутов, добавляемых к его таблице маршрутизации. Это соглашение позволяет клиентам удаленного доступа и клиентам VPN выполнять параллельное туннелирование при подключении к удаленной сети. Это также дает возможность клиентам локальной сети получать дополнительную информацию маршрутизации. Так, администратор может разрешить клиентам параллельное туннелирование через подключение VPN и Интернет. Благодаря этому трафик для Интернета не будет проходить через подключение VPN, и в то же время пользователь может обращаться к закрытым ресурсам сети своей организации.
- **Перемещение БД DHCP посредством Netsh** Обеспечивает простой перенос базы данных DHCP с одного сервера на другой, если для импорта применяется Netsh. Благодаря этому устраняется необходимость ручного конфигурирования, такого как редактирование реестра и повторное задание областей действия. Команда Netsh применяется для локальной настройки серверов и маршрутизаторов и может использовать файлы сценариев, автоматизирующие задачи конфигурирования, Данная возможность может использоваться в следующих случаях:
  - □ администратор получил уведомление об ошибке на диске DHCP-сервера и решает переместить службу DHCP до полного отказа диска;
  - D администратору нужно разделить функции DHCP-сервера; при этом он может использовать рассматриваемую возможность, чтобы переместить часть базы данных DHCP на другой компьютер или компьютеры.
- **Удаление аренды DHCP командой Netsh** Новая команда **netsh dhcp server scope** *scopeaddress* **delete lease** позволяет

удалить аренду DHCP из интерфейса командной строки, вместо того чтобы использовать оснастку DHCP. Это упрощает управление DHCP-сервером через интерфейс командной строки или с помощью сценариев.

DNS

В семействе Windows Server 2003 были сделаны следующие улучшения службы DNS.

- **Сохранение зон DNS в прикладном разделе Active Directory** Обеспечивает хранение и репликацию зон системы доменных имен (DNS) сохраненных в прикладном разделе службы Active Directory. Хранение данных DNS в прикладном разделе уменьшает количество объектов, хранимых в глобальном каталоге. Кроме того, при этом данные зоны DNS реплицируются только на подмножество контроллеров домена, определенное в прикладной области. По умолчанию прикладной раздел для DNS содержит только контроллер домена, на котором запущен DNS-сервер. Кроме того, хранение данных зоны DNS в прикладном разделе позволяет реплицировать зону DNS на DNS-серверы, запущенные на контроллерах домена в других доменах леса Active Directory. Администратору это хранить зону DNS в прикладном разделе. Это рекомендуется, если интегрированная с Active Directory зона DNS размещена на DNS-сервере под управлением Windows Server 2003.
- **Базовая совместимость с расширениями безопасности DNS** DNS-сервер под управлением Windows Server 2003 обеспечивает базовую совместимость с протоколом расширений безопасности DNS стандарта Internet Engineering Task Force (IETF) согласно документу RFC 2535. Сервер DNS может хранить записи типов (KEY, SIG и NXT), определенные в стандарте IETF и включать эти записи в ответ на запрос согласно документу RFC 2535. Сервер не обеспечивает полной совместимости и не выполняет криптографических операций, описанных в RFC 2535 (генерация записей KEY/SIG, подпись сообщений и проверка подписи). Однако сервер может сохранять и использовать стандартные записи KEY и SIG, генерируемые ПО сторонних производителей. Администратор может использовать DNS-сервер с Windows Ser-

ver 2003 как вторичный сервер для подписанной зоны, первичная копия которой хранится на сервере с полной поддержкой DNS Security Extensions (в RFC 2535).

- **Процедура подключения к домену усовершенствована для обнаружения неправильно настроенных DNS** Упрощает отладку, сообщает о неправильной конфигурации DNS и помогает настроить инфраструктуру DNS, чтобы разрешить подключение компьютера к домену. Когда компьютер, пытающийся подключиться к домену Active Directory, не может обнаружить контроллер домена из-за неправильной конфигурации DNS или недоступности контроллеров домена, выполняется настройка инфраструктуры DNS. В результате генерируется отчет, объясняющий причину отказа и предлагающий способ решения проблемы. Если инфраструктура DNS настроена верно и позволяет компьютеру подключиться к домену, администратор не будет замечать наличия данной функции. Если инфраструктура DNS настроена не так и не дает компьютеру обнаружить контроллер домена и войти в домен, функция привлечет внимание администратора, если он попытается присоединить компьютер к домену.
- **Управление клиентами DNS с помощью групповой политики** Позволяет настраивать параметры клиента DNS на компьютере с Windows Server 2003 с помощью групповой политики. Это упрощает настройку членов домена, таких как разрешение/запрещение динамической регистрации записей DNS клиентом, передача первичного суффикса DNS при разрешении имен и список поиска популярных суффиксов DNS. Кроме упрощения администрирования, поддержка групповой политики для списка поиска суффиксов DNS — важная особенность, необходимая при переходе к среде без NetBIOS. Администратор может использовать групповую политику для настройки клиентов DNS,
- **Зоны-заглушки и условная пересылка** Служат для контроля маршрутизации DNS-трафика в сети. Зона-заглушка позволяет DNS-серверу знать имена и адреса серверов, авторитетных для полной копии зоны, без необходимости хранить на сервере полную копию зоны или посылать запрос корневому серверу DNS. DNS-сервер с Windows 2000 может быть настроен для пересылки запросов DNS только одному на-

бору DNS-серверов. Условная пересылка обеспечивает лучшую степень детализации, поддерживая пересылку, зависимую от имени. Так, DNS-сервер можно настроить для:

- пересылки запросов для имен, заканчивающихся usa.microsoft.com, на первый набор DNS-серверов;
- пересылки запросов для имен, заканчивающихся europe.microsoft.com, на второй набор DNS-серверов;
- пересылки всех остальных запросов на третий набор DNS-серверов.

Администраторы могут использовать эту возможность для контроля за маршрутизацией трафика DNS в своих сетях.

- **Поддержка протокола EDNSO** Протокол EDNS0, определенный в документе RFC 2671, позволяет DNS-серверу принимать и передавать сообщения UDP, информационная часть которых превышает 512 октетов. Эта возможность пригодится администратору, когда ответы DNS, такие как запрос записи ресурса местоположения службы (SRV), используемый для обнаружения контроллера домена Active Directory, превышают 512 октетов. До Windows Server 2003 эти ответы требовали дополнительного цикла, включающего установку и завершение сеанса TCP. Благодаря использованию протокола EDNSO, в Windows Server 2003 большинство таких запросов выполняется за один цикл UDP и не требует установки и прекращения сеанса TCP,
- **Дополнительные расширения** Служба DNS-сервера в Windows Server 2003 поддерживает дополнительные расширения:
  - **поддержка кольцевого буфера для всех типов записей ресурсов (RR):** по умолчанию DNS-еервер производит циклическую ротацию для всех типов RR;
  - **расширенный журнал отладки:** параметры расширенного журнала отладки DNS-сервера помогут при диагностике неисправностей DNS;
  - **автоматическая запись ресурса сервера имен:** DNS-сервер теперь может автоматически управлять регистрацией записи ресурса сервера имен (NS) на основании сервера и зоны.

WINS

Служба Windows Internet Name Service (WINS) улучшена,

- **Фильтрация записей** Улучшенная фильтрация и новые функции поиска помогают обнаружить записи, показывая только те, что соответствуют заданным критериям. Эти функции особенно удобны при анализе очень больших баз данных WINS. Вы можете использовать несколько критериев для выполнения расширенного поиска записей в БД WINS. Эти расширенные возможности фильтрации позволяют комбинировать фильтры для получения настраиваемых и точных результатов запроса. Доступные фильтры включают владельца записи, тип записи, имя NetBIOS и IP-адрес с или без маски подсети. Поскольку результаты запросов можно кэшировать в памяти локального компьютера, производительность последовательных запросов растет, а сетевой трафик сокращается.
- **Принятие партнеров репликации** Можно определить список, управляющий источником поступающих записей имен в процессе репликации между серверами WINS. В дополнение к блокировке записей имен из указанных партнеров репликации вы также можете принимать записи имен только от определенных серверов WINS, исключая записи имен серверов, не указанных в списке.

IAS

Улучшения службы IAS перечислены в следующем списке. IAS недоступна в версии Web Edition.

- **Поддержка аутентификации JEEE 802.1x для защиты беспроводных и локальных сетей** Служба IAS усовершенствована, чтобы разрешать аутентификацию и авторизацию пользователей и компьютеров, подключенных к точкам беспроводного доступа ШЕЕ 802.11b и коммутаторам Ethernet с применением аутентификации IEEE 802.1X. Условие политики удаленного доступа NAS-Port-Type теперь позволяет выбирать тип беспроводных и Ethernet-подключений.

  Для защиты беспроводных или Ethernet-подключении можно применять сертификаты либо парольную защиту с аутентификацией Protected EAP (PEAP) и MS-CHAP v2. EAP-TLS использует сертификаты для аутентификации учет-

ных записей и предоставления ключей шифрации. EAP-TLS требует наличия инфраструктуры для выпуска сертификатов как на сервере IAS, так и на беспроводном или Ethernet-клиенте. С PEAP и MS-CHAP v2 вы можете безопасно применять аутентификацию на основе пароля, поскольку MS-CHAP v2 для обмена данными аутентификации создает шифрованный канал TLS, что предотвращает словарные атаки на пароль пользователя в автономном режиме. Обмен данными аутентификации PEAP также выполняется с ключом шифрации. PEAP с MS-CHAP v2 требуют установки сертификатов только на сервере IAS.

PEAP позволяет возобновлять сеанс TLS, созданный при начальной аутентификации PEAP. Эта возможность PEAP, известная как *быстрое восстановление подключения* (fast reconnection), заставляет последующие аутентификации на базе TLS выполняться очень быстро, так как большинство сообщений полной аутентификации PEAP не передается. Быстрое восстановление подключения PEAP минимизирует время подключения и аутентификации и не требует, чтобы пользователь повторно передавал данные учетной записи, такие как имя и пароль. Например, для беспроводных клиентов, перемешающихся от одного беспроводного протокола к другому, переключение выполняется незаметно, и не запрашиваются учетные данные для аутентификации.

Чтобы выбрать PEAP с MS-CHAP v2 на сервере IAS, в оснастке Internet Authentication Service щелкните EAP Methods на вкладке Authentication профиля свойств политики удаленного доступа, в диалоговом окне Select EAP Providers щелкните Protected Extensible Authentication Protocol (PEAP) и либо отредактируйте свойства, либо переместите их из списка типов EAP.

- Время сеанса отражает ограничения учетной записи IAS теперь корректно вычисляет время сеанса для подключения, основываясь на времени действия учетной записи компьютера/пользователя и разрешенных для регистрации часах. Например, ограничения учетной записи пользователя разрешают регистрацию с 9:00 до 17:00 с понедельника по пятницу. Если подключение с этой учетной записью было установлено в 16:00 в пятницу, IAS автоматически вычис-

лит, что максимальное время сеанса для подключения равно 1 часу и отправит максимальное время сеанса как атрибут RADIUS на сервер доступа.

- IAS и **аутентификация** между лесами Если леса Active Directory находятся в перекрестном режиме с двусторонним доверием, IAS может аутентифицировать учетную запись пользователя в другом лесу. Администратору эта возможность позволяет выполнить аутентификацию и авторизацию учетных записей в другом лесу Active Directory с двусторонним доверием, работающим в перекрестном режиме.
- IAS как **прокси** RADIUS Позволяет IAS пересылать аутентификацию RADIUS и сообщения учета между сервером доступа и сервером RADIUS. Функциональные возможности включают;
  - D гибкую, управляемую правилами пересылку;
  - D балансировку нагрузки и отказоустойчивость нескольких серверов RADIUS и балансировку нагрузки запросов RADIUS;
  - п возможность заставить клиента использовать обязательный туннель с/без аутентификации пользователя;
  - □ выборочную пересылку запросов аутентификации и учета на разные серверы RADIUS.

  Рассматриваемая возможность может использоваться в следующих сценариях.
  - D Администратор может создать прокси RADIUS на базе IAS, расположенный в одном домене, для аутентификации и авторизации пользователей в другом домене, не имеющем доверительных отношений, имеющем одностороннее доверие либо расположенном в другом лесу.
  - □ ISP, предлагающий модемную связь, VPN или беспроводные службы для корпорации, может пересылать запросы аутентификации и учета на корпоративный сервер RADIUS.
  - П Администратор может установить прокси IAS в сетевом периметре. Запросы могут пересылаться прокси IAS у ISP на сервер IAS в сети организации.
  - п Администратор может использовать IAS в сети, подключенной к партнерской сети, для пересылки аутентифи-

кации пользователей из другой компании их БД учетных записей пользователей.

- **Ведение журнала RADIUS в базе данных SQL** IAS можно настроить для отправки журнальной информации для запросов учета, аутентификации и периодической статистики на SQL-сервер. Это позволяет администраторам применять SQL-запросы для просмотра истории и данных реального времени о попытках подключений, использовавших для аутентификации RADIUS. Для настройки этой возможности выберите в качестве метода ведения журнала SQL Server в папке Remote Access Logging оснастки Internet Authentication Service.
- **Неаутентифицированный доступ EAP-TLS** Неаутентифицированный доступ EAP-TLS позволяет разрешать гостевой доступ беспроводным или коммутируемым клиентам, не имеющим установленных сертификатов. Если сетевой клиент не предоставляет данные учетной записи, IAS определяет, разрешен ли неаутентифицированный доступ в политике удаленного доступа, соответствующей устанавливаемому подключению. EAP-TLS поддерживает одностороннюю авторизацию или неаутентифицированный доступ, когда клиент не передает данные учетной записи.

  Эта возможность применяется в следующих сценариях.

  - Администратор может позволить беспроводным или коммутируемым клиентам, не имеющим сертификатов, подключаться к ограниченной виртуальной локальной сети (VLAN) для начальной загрузки параметров.
  - Администратор может предоставить посетителям или партнерам доступ к Интернету через корпоративную сеть. Это достигается предоставлением им доступа к VLAN или с помощью IP-фильтра, разрешающего прохождение Интернет-трафика.
  - D Беспроводной ISP может разрешить доступ потенциальным подписчикам. Они могут получить доступ к VLAN с локальной информацией. После того как пользователь оформит подписку на доступ к Интернету, клиент сможет подключаться к Интернету.
- **Параметры клиента RADIUS поддерживают диапазон IP-адресов** Чтобы упростить администрирование клиентов

RADIUS, когда несколько точек беспроводного доступа находятся в пределах одной подсети или в пределах одного адресного пространства IP, IAS позволяет указать для клиента RADIUS диапазон IP-адресов.

Диапазон адресов для клиента RADIUS записывается в виде *w.x.y.z/p*, где *w.x.y.z* — адресный префикс в десятичной нотации, а *p* — длина префикса (количество старших бит, определяющих префикс). Такая форма также известна как нотация бесклассовой междоменной маршрутизации (CIDR). Например, можно записать 192.168.21.0/24. При преобразовании длины префикса в маску подсети *p* обозначает количество старших бит, которые в маске подсети должны быть установлены в 1.

Используя эту возможность, администратор может упростить управление точками беспроводного доступа.

- **Усовершенствования выбора метода аутентификации EAP** Позволяет при настройке политик удаленного доступа выбрать несколько типов EAP. Это дает возможность IAS договариваться с клиентом о методе аутентификации EAP. Администратор может задействовать эту возможность, когда удаленные сетевые клиенты используют разные методы аутентификации EAP, и настроить сервер для разрешения выбранного списка методов аутентификации EAP.
- **Проверка идентификатора объекта для пользовательских сертификатов и смарт-карт** Чтобы требовать заданные типы пользовательских сертификатов для заданных типов подключений, IAS поддерживает спецификацию политики выпуска индивидуальных сертификатов с идентификаторами объектов (OID), которые должны быть включены в сертификат доступа клиента как часть параметров профиля политики удаленного доступа. Так, если администратор хочет гарантировать, что подключения удаленного доступа VPN будут использовать сертификаты смарт-карт, а не локально установленные пользовательские сертификаты, он настраивает соответствующую политику удаленного доступа для требования присутствия идентификатора объекта политики выпуска сертификатов Smart Card Logon (1.3.6.1.4.1.311.20.2.2) в сертификате, предоставляемом удаленным клиентом VPN. Вы можете настроить список идентификаторов объектов,

которые должны присутствовать в пользовательском сертификате, используя атрибут Allow Certificates With These OIDs на вкладке Advanced окна свойств профиля политики удаленного доступа. По умолчанию определенные идентификаторы объектов не требуются.

- **Балансировка нагрузки на прокси RADIUS** Обеспечивает балансировку нагрузки аутентификации между несколькими серверами RADIUS, когда IAS используется как прокси RADIUS. Это обеспечивает масштабирование и обработку отказов. Прокси IAS RADIUS выполняет динамическую балансировку нагрузки запросов подключений и учета между несколькими серверами RADIUS и увеличивает скорость работы большого числа клиентов RADIUS и количество аутентификаций в секунду. Кроме того, прокси RADIUS можно настроить, чтобы отдавать предпочтение каким-либо серверам RADIUS. Сервер RADIUS с меньшим приоритетом не будет использоваться, пока доступны серверы с более высоким.

  Данная возможность позволяет использовать следующие сценарии:

  D администратор может масштабировать беспроводные, VPN или модемные аутентификации, чтобы обрабатывать большее число запросов на подключение, используя несколько серверов RADIUS;

  D администратор может гарантировать, что сбой запроса на подключение будет обработан ближайшим доступным сервером RADIUS, и настроить серверы RADIUS на удаленном сайте как резервные.

- **Поддержка для игнорирования свойств модемного подключения в учетной записи** Вы можете задать атрибуты RADIUS профиля свойств политики удаленного доступа так, чтобы игнорировались свойства модемного подключения в учетной записи. Свойства модемного подключения в учетной записи включают:

  □ разрешения удаленного доступа;

  □ идентификатор звонящего;

  п параметры обратного вызова;

  п статический IP-адрес;

  п статические маршруты.

Чтобы поддерживать многочисленные типы подключений, для которых IAS предоставляет аутентификацию и авторизацию, может потребоваться запрещение обработки свойств модемного подключения в учетной записи. Это требуется сделать для поддержки сценариев, в которых не нужны некоторые свойства модемного подключения. Например, свойства, задающие идентификатор звонящего, обратный вызов, статический IP-адрес и статические маршруты, разработаны для клиентов, подключающихся через модем к серверу сетевого доступа (NAS). Эти параметры не предназначены для точек беспроводного доступа (AP). Беспроводные AP, получающие эти параметры в сообщении RADIUS от сервера IAS, возможно, не смогут обработать их, что приведет к отключению беспроводного клиента. Когда IAS предоставляет аутентификацию и авторизацию для пользователей, которым нужна модемная связь и беспроводной доступ к сети, свойства модемного подключения должны быть настроены либо для модемных подключений (с установкой свойств модемного подключения), либо для беспроводных подключений (без указания свойств модемного подключения).

IAS позволяет разрешить обработку свойств модемного подключения для учетных записей пользователя в одних сценариях (например, модемный доступ) и запретить обработку свойств модемного доступа для учетной записи пользователя в других сценариях (таких как беспроводной доступ и аутентифицируемых коммутируемых подключений): установите атрибут Ignore-User-Dialin-Properties на вкладке Advanced параметров профиля политики удаленного доступа. Ниже описано действие различных значений атрибута Ignore-User-Dialin-Properties.

- Чтобы разрешить обработку свойств модемного доступа учетной записи, удалите атрибут Ignore-User-Dialin-Properties или присвойте ему *False*. Это делается, например, для политики доступа, разработанной для модемных подключений. Дополнительной настройки не требуется.
- Чтобы запретить обработку свойств модемного подключения учетной записи, присвойте *True* атрибуту Ignore-User-Dialin-Properties. Это делается, например, для политики удаленного доступа, разрабатываемой для беспро-

водных подключений или аутентифицируемых коммутируемых подключений. Когда свойства модемного подключения учетной записи игнорируются, разрешения удаленного доступа определяются на основе разрешений удаленного доступа для политики удаленного доступа.

Этот атрибут также позволяет управлять сетевым доступом через группы и разрешения удаленного доступа политики удаленного доступа. Если присвоить *True* атрибуту Ignore-User-Dialin-Properties, разрешения удаленного доступа учетной записи пользователя игнорируются. Недостатки такого применения атрибута Ignore-User-Dialin-Properties заключаются в невозможности задействовать дополнительные свойства модемного подключения, такие как идентификатор звонящего, обратный вызов, статический IP-адрес и статические маршруты для подключений, соответствующих политике удаленного доступа.

- **Поддержка аутентификации компьютера** Active Directory и IAS поддерживают аутентификацию учетных записей компьютера с применением стандартных методов аутентификации пользователя. Это позволяет компьютеру и его учетным записям быть аутентифицированными для доступа беспроводных и коммутируемых клиентов.
- **Поддержка условия Authentication Type политики удаленного доступа** Вы можете создать политику удаленного доступа, использующую условие Authentication Type. Это новое условие позволяет задать ограничения для подключения, основанные на протоколах или методах аутентификации, используемых для подтверждения прав доступа клиента,
- **Усовершенствованный TAS SDK** Windows .NET Platform Software Development Kit (SDK) включает два небольших сетевых SDK: IAS SDK и EAP SDK. IAS SDK может применяться для возврата на сервер доступа дополнительных атрибутов, помимо возвращаемых IAS, контроля количества сетевых сеансов пользователя, импорта данных использования и аудита прямо в БД с поддержкой Open Database Connectivity (ODBC), создания нестандартных модулей авторизации и создания нестандартных модулей аутентификации (не EAP). EAP SDK позволяет создавать типы EAP. Разработчики могут использовать усовершенствованный IAS SDK

для модификации или удаления атрибутов RADIUS и для преобразований Access-Rejects в Access-Accepts, ISV или системные интеграторы (VAR) могут применять эту возможность при создании расширенных решений с IAS. Администраторы могут использовать данную возможность при создании нестандартных решений для IAS.

- **API, доступный из сценариев для конфигурации IAS** Вызывает (в IAS Platform SDK) API, доступный из сценариев, позволяющий конфигурировать IAS. ISV могут применять эту возможность для предоставления дополнительных служб на вершине инфраструктуры IAS, а администраторы — для интеграции IAS с их собственными службами инфраструктуры управления.
- **Усовершенствованная конфигурация EAP для политики удаленного доступа** В Windows 2000 для политики удаленного доступа можно было выбрать только один тип EAP, а значит, все подключения, соответствующие условиям политики должны использовать единый тип EAP для политики удаленного доступа. Кроме того, конфигурация типа EAP была глобальной для всех политик удаленного доступа. Эти ограничения могут вызвать проблемы, если требуется индивидуальная настройка типов EAP для каждой политики или если вы хотите выбрать несколько типов EAP для разных типов сетевых подключений или для групп пользователей. В Windows Server 2003 эти ограничения устранены. Так, можно выбрать разные сертификаты компьютера для аутентификации EAP-TLS для беспроводных и для VPN-подключений, или можно выбрать несколько типов EAP для беспроводных подключений, гак как одни беспроводные клиенты используют аутентификацию EAP-TLS, а другие — PEAP с MS-CHAP v2.
- **Разделение аутентификации и авторизации для прокси IAS** Компонент прокси IAS в семействе Windows Server 2003 поддерживает раздельную аутентификацию и авторизацию запросов подключений с сервера доступа. Прокси IAS может пересылать данные учетной записи пользователя внешнему серверу RADIUS для аутентификации и выполнения его собственной авторизации с применением учетной записи пользователя в домене Active Directory и локальной на-

стройки параметров политики удаленного доступа. Благодаря этому можно задействовать альтернативные БД аутентификации пользователей, но авторизацию подключения и ограничения будет определять локальный администратор.

Эта возможность позволяет использовать следующие сценарии.

- Посетителю сети можно предоставить доступ к гостевой LAN посредством аутентификации по данным учетной записи посетителя и авторизации подключения по учетной записи пользователя в домене Active Directory для недоверенных пользователей и политики удаленного доступа, настроенной прокси IAS. Данные учетной записи посетителя могут быть данными учетной записи пользователя в сети организации посетителя.
- Открытые беспроводные сети могут использовать альтернативные БД пользователей для аутентификации беспроводного доступа и авторизации регистрации с учетной записью локального пользователя в домене Active Directory.

Новая возможность настраивается с помощью параметра Remote-RADIUS-to-Windows-User-Mapping в дополнительных свойствах политики запроса подключений.

IPSec

В семействе Windows Server 2003 были сделаны следующие улучшения службы IPSec.

- **Новая оснастка IP Security Monitor** Обеспечивает тонкую настройку параметров политики IPSec. Она заменяет утилиту Ipsecmon.exe из Windows 2000. Политика IPSec включает набор политик основного режима, набор политик быстрою режима, набор фильтров основного режима, связанных с набором политик основного режима, и набора фильтров быстрого режима (для транспортного и туннельного режимов), связанных с набором политик быстрого режима. Активное состояние защиты включает активные ассоциации безопасности для главного и быстрого режимов и статистическую информацию о защищенном IPSec-трафике. Администраторы могут использовать новую оснастку для улучшенного контроля и диагностики IPSec.

- **Интерфейс командной строки Netsh** Позволяет статически/динамически настраивать параметры основного режима IPSec, параметры быстрого режима, правила и параметры конфигурации. Для входа в контекст Netsh ipsec введите в командной строке **netsh -c ipsec.** Контекст Netsh ipsec заменяет утилиту Ipsecpol.exe из Windows 2000 Server Resource Kits. Администраторы могут использовать эту возможность в сценариях для автоматизации настройки IPSec.
- **Интеграция безопасности IP и балансировки сетевой нагрузки** Позволяет группе серверов применять балансировку сетевой нагрузки (NLB) с целью предоставить VPN-службы высокой доступности на основе JPSec. Это также поддерживается низкоуровневыми клиентами L2TP/IPSec. Эта возможность обеспечивает более быструю обработку отказов IPSec. Администраторы могут применять данную возможность для интеграции NLB и VPN-служб на базе IPSec для создания более безопасных и надежных сетевых служб. Поскольку протокол IKE автоматически определяет службу NLB, дополнительной настройки не требуется. Данная возможность имеется только в версиях Enterprise Edition и Datacenter Edition,
- **Поддержка IPSec для RSoP** Для расширения возможностей диагностики и развертывания IPSec теперь поддерживает расширения для оснастки Resultant Set Of Policy (RSoP). RSoP — это дополнение к групповой политике, которое можно применять для просмотра существующих назначений политик IPSec и моделировать планируемые назначения политик IPSec для компьютеров/пользователей. Для просмотра существующих назначений политик, вы должны выполнить запрос режима регистрации RSoP. Для моделирования планируемых назначений политик IPSec выполните запрос режима планирования RSoP.

  Запросы режима регистрации полезны при диагностике проблем, вызываемых старшинством политик IPSec. В результате запроса режима регистрации отображаются все политики IPSec, назначенные клиенту IPSec. и старшинство каждой. Запросы режима планирования полезны для планирования развертывания, та как позволяют моделировать настройку политик IPSec. При этом вы можете оценить воздействие значений параметров и определить оптимальные

до их внедрения. Выполнив запрос режима регистрации RSoP или запрос режима планирования RSoP, можно просматривать детальные параметры (правила фильтрации, действия фильтров, методы аутентификации, конечные точки туннелей и типы подключений, заданные при создании политики IPSec) для применяемой политики IPSec.

- **Прохождение IPSec через** NAT Позволяет трафику, защищенному IKE и ESP, проходить через NAT. **IKE** автоматически определяет наличие NAT и использует инкапсуляцию User Datagram Protocol-Encapsulating Security Payload (UDP-ESP), чтобы позволить защищенному ESP трафику IPSec проходить через NAT. Поддержка прохождения IPSec через NAT в семействе Windows Server 2003 описана в черновиках документов, озаглавленных «UDP Encapsulation of IPsec Packets» (draft-ietf-ipsec-udp-encaps-02.txt) и «Negotiation of NAT-Traversal in the IKE» (draft-ietf-ipsec-nat-t-ike-02.txt).

  Благодаря этой поддержке корпоративные служащие могут использовать L2TP/IPSec при подключении к частным сетям, таким как домашняя сеть. Эта возможность обеспечивает более общую транспортировку IPSec ESP и режим ассоциаций безопасности поверх NAT. Администратор может использовать эту возможность для настройки туннеля IPSec «шлюз — шлюз» между двумя компьютерами под управлением Windows Server 2003 и службы маршрутизации и удаленного доступа, когда один или оба расположены за NAT, Допускаются и IPSec-подключения «сервер — сервер», например, когда сервер сетевого периметра подключается через NAT к серверу внутренней сети.

- **Аппаратное ускорение преобразования сетевых адресов** IPSec теперь поддерживает аппаратное ускорение NAT для обычного ESP-трафика. Эта возможность поддерживает такие сценарии:
  - администратор может использовать эту возможность для масштабирования L2TP/IPSec и нормальных IPSec-подключений, когда используется IPSec поверх NAT;
  - независимые поставщики аппаратуры (IHV) могут использовать эти функциональные возможности при построении новых карт или обновлении старого встроенного ПО для включения новых возможностей.

Интерфейс аппаратного ускорения IPSec документирован в Windows DDK как часть TCP/IP Task Offload.

- **Политика фильтров IPSec разрешает логические адреса для локальной конфигурации IP** Оснастка IP Security Policies позволяет теперь настраивать поля адреса источника или адреса приемника, интерпретируемые локальной службой политик IPSec как адреса DHCP-, DNS- и WINS-сервера и шлюза по умолчанию. Поэтому политика IPSec может автоматически обеспечивать изменение параметров IP сервера, используя либо DHCP, либо статическую конфигурацию IP. Компьютеры с Windows 2000/XP, игнорируют это расширение политики IPSec.
- **Отображение сертификатов на учетную запись компьютера в Active Directory обеспечивает контроль доступа** Оснастка IP Security Policies теперь позволяет настроить отображение сертификатов компьютера на учетную запись компьютера в лесу Active Directory. Это дает те же преимущества, что и отображение сертификатов Schannel, используемое IIS и другими службами с поддержкой PKI. После отображения сертификатов на учетную запись компьютера в домене, контроль доступа может осуществляться с помощью прав сетевой регистрации Access This Computer From Network и Deny Access To This Computer From Network. Сетевой администратор может теперь ограничить доступ к компьютеру с Windows Server 2003, используя IPSec, чтобы разрешить доступ только компьютерам определенного домена, компьютерам, имеющим определенные сертификаты, заданной группе компьютеров и даже единственному компьютеру. Компьютеры с Windows 2000/XP игнорируют это расширение политики IPSec.
- **Более сильная группа Diffie-Hellman для IKE** IPSec теперь поддерживает обмен 2048-разрядными ключами Diffie-Hellman, обеспечивая поддержку черновика документа «More MODP Diffie-Hellman groups for IKE». Полученный в результате закрытый ключ является более сильным. Оснастка IP Security Policies позволяет настроить параметры новой группы Diffie-Hellman как для локальной, так и для доменной политики IPSec. Компьютеры с Windows 2000/XP игнорируют эти параметры.

- **Лучшая защита от атак на службу для IKE** IKE в Windows Server 2003 модифицирована для лучшего отражения атак на службы с вовлечением трафика IKE. Наиболее общий вариант атаки — пачки пакетов с неправильной информацией, отправляемые на UDP-порт 500. IKE пытается подтверждать правильность пакетов, пока их не станет слишком много, после чего начинает отбрасывать пакеты. Когда частота поступления пакетов спадает до нормального уровня, IKE быстро начинает снова контролировать правильность пакетов IKE. Наиболее трудной для предотвращения атакой является отправка злоумышленником корректных сообщений инициирования IKE либо с указанием неправильного IP-адреса иеточника, либо просто быстрая отправка из источника с корректным IP-адресом. Этот вид атак аналогичен атакам TCP Synchronize (SYN) против серверов TCP/IP. При использовании новой зашиты получатель IKE отвечает на начальное корректное сообщение IKE другим сообщением IKE, содержащим специальное значение в поле Responder Cookie. Если инициатор не посылает следующего сообщения IKE с правильным значением свойства Responder Cookie, обмен IKE игнорируется. Когда инициатором IKE является Windows Server 2003, повторная инициация проходит должным образом. Модуль IPSec IKE не управляет состояниями обмена IKE, пока не получен ответ, содержащий правильно установленное значение поля Responder Cookie. Это обеспечивает взаимодействие с компьютерами под управлением Windows 2000/XP и реализациями IPSec сторонних фирм и увеличивает шансы успешного обмена данными с законными инициаторами, даже когда отправитель подвергается ограниченной атаке. Это остается возможным для отправителя IKE, перегруженного большим количеством легитимных пакетов IKE. Отправитель IKE ответит настолько быстро, насколько возможно, по завершении атаки.

Другие новые возможности

Ниже рассмотрено несколько других новых сетевых возможностей Windows Server 2003:

- изменения Winsock API;
- Windows Sockets Direct для сетей хранения данных;

- удаление унаследованных сетевых протоколов;
- удаление устаревших протоколов RPC;
- утилиты с интерфейсом командной строки;
- сильная аутентификация в службах для Macintosh.

Изменения Winsock API

В Windows Sockets API были внесены следующие изменения.

- **Удалена поддержка для AF_NETBIOS (только в 64-разрядной версии)** AF_NETBIOS не поддерживается в 64-разрядной версии Enterprise Edition и Datacenter Edition. В качестве альтернативы приложения должны использовать TCP или UDP. Функциональность сохранена для поддержки 32-разрядных приложений сторонних производителей.
- **ConnectEx/TransmitPackets и TCP/IP** Следующие две функции представляют расширение Microsoft для спецификации Windows Sockets 2.
  - Функция Windows Sockets *ConnectEx* устанавливает подключение к другому сокету приложения и может после установки подключения передать блок данных.
  - Функция Windows Sockets *TransmitPackets* передает данные из памяти или из файла через подключение сокетов (либо дейтаграммы, либо поток). Диспетчер кэша ОС служит для получения данных из файла и блокировки памяти на минимально требуемое для передачи время. Это обеспечивает высокую производительность и эффективность передачи данных из файла или из памяти через сокеты.

Windows Sockets Direct для сетей хранения данных

В Windows Server 2003 повышена производительность Windows Sockets Direct (WSD) для сетей хранения данных (SAN). WSD позволяет приложениям Windows Sockets, написанным для SOCK_STREAM, напрямую задействовать производительность SAN. Фундаментальный компонент этой технологии — коммутатор WinSock, эмулирующий семантику TCP/IP поверх «родных» компонентов доступа служб SAN. В Windows 2000 Server поддержка WSD доступна только для Windows 2000 Advanced Server и Datacenter Server. В Windows Server 2003 поддержка

WSD включена во все выпуски. Подробнее о Windows Sockets API см. Microsoft Platform SDK.

Удаление унаследованных сетевых протоколов

Удалены следующие унаследованные сетевые протоколы:

- Data Link Control (DLC);
- NetBIOS Extended User Interface (NetBEUI).

Следующие унаследованные сетевые протоколы удалены из 64-разрядной версии ОС:

- Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) и связанные с IPX службы;
- Infrared Data Association (IrDA);
- Open Shortest Path First (OSPF).

Удаление устаревших протоколов RPC

Следующие **унаследованные** протоколы RPC **были заменены TCP:**

- Remote Procedure Call (RPC) поверх NetBEUI;
- RPC поверх NetBIOS поверх TCP/IP (NetBT);
- RPC поверх NetBIOS поверх IPX (NBIPX);
- RPC поверх SPX (только в 64-разрядной версии);
- RPC поверх AppleTalk (только в 64-разрядной версии).

Следующие унаследованные протоколы были заменены UDP:

- RPC поверх IPX;
- RPC поверх Message Queuing (MSMQ).

Утилиты с интерфейсом командной строки

Новые утилиты с интерфейсом командной строки упрощают управление и администрирование компьютера. Включен новый и измененный справочный файл командной строки, документирующий оболочку Cmd.exe и каждую утилиту. Некоторые утилиты перечислены ниже.

- Bootcfg.exe служит для просмотра и установки свойств (таких как включение/выключение режима отладки) файла boot.ini на локальном или удаленном сервере (недоступно в 64-разрядной версии).

- **DriverQuery.exe** служит для просмотра списка загруженных в данный момент драйверов и используемой ими памяти.
- **Dsadd.exe** создает экземпляр объекта указанного типа в Active Directory.
- **Dsget.exe** служит для получения или просмотра выбранных свойств существующих объектов в Active Directory, когда местоположение просматриваемого объекта известно.
- **Dsmod.exe** служит для изменения выбранного атрибута существующего объекта в Active Directory.
- **Dsmove.exe** перемещает объект из его текущего местоположения в новое в пределах того же самого контекста или для переименования объекта в Active Directory.
- **Dsquery.exe** служит для поиска в Active Directory объектов по заданным критериям.
- **Dsrm.exe** удаляет объект или целое поддерево под объектом в Active Directory.
- **Eventcreate.exe** записывает определяемое пользователем событие в какой-нибудь из журналов событий.
- **Eventquery.vbs** служит для задания типа событий, извлекаемых из журнала событий. Выбранные события могут быть выведены на экран или записаны в файл.
- **Eventtriggers.exe** запускает процесс на основании возникновения события, записываемого в журнал,
- **Gpresult.exe** позволяет получить результирующий набор политик (RSoP) и список политик, примененных к компьютеру.
- **Сценарии IIS** (IISWeb.vbs, IISVdir.vbs и т. д.) предоставляют утилиты с интерфейсом командной строки для конфигурирования и управления сервером, выполняющим TIS и приложения Active Server Pages (ASP).
- **Netsh.exe** служит для конфигурирования сети; в этот мощный инструмент добавлены базовые средства диагностики сети, предоставляемые ранее утилитой NetDiag.exe.
- **Openfiles.exe** служит для просмотра списка подключенных пользователей и файлов, открытых ими на компьютере.
- **Pagefileconfig.vbs** позволяет получить текущий размер файла подкачки или установить новый размер файла подкачки.

- Сценарии печати (prncnfg.vbs, prnjobs.vbs и т. д.) служат для управления службами печати, драйверами принтеров и очередями заданий печати.
- Reg.exe служит для просмотра, создания и редактирования разделов реестра.
- SC.exe служит для запуска/остановки/управления службами Win32.
- Schtasks.exe служит для просмотра/установки/редактирования списка задач, запускаемых по расписанию при помощи службы планировщика заданий Win32.
- Systeminfo.exe служит для просмотра основных свойств машины (таких как тип процессора и объем памяти).
- Taskkill.exe служит для выгрузки/остановки запущенного процесса.
- Tasklist.exe служит для просмотра списка всех запущенных процессов и их PID.
- Tsecimp.exe служит для импорта свойств и прав доступа учетной записи пользователя Telephony Application Programming Interface (TAPI).

Администраторы могут использовать утилиты с интерфейсом командной строки из сценариев Visual Basic или пакетных файлов для автоматизации объемных или часто выполняемых задач администрирования сервера. Это позволяет избегать одноразовых операций, которые часто недоступны через утилиты с графическим интерфейсом пользователя, и сокращает затраты на администрирование.

Сильная аутентификация в службах для Macintosh

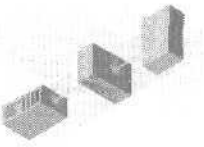
На компьютерах с запущенными службами для Macintosh (SFM) и использующих модуль аутентификации пользователя Microsoft (MSUAM) в интерфейсе MSUAM доступен новый флажок Require Strong Authentication (NTLMv2), установленный по умолчанию. Выбор этого параметра позволяет аутентифицировать пользователя только на сервере, поддерживающем NTLMv2. Это исключает Windows NT 4.0 и старые серверы, не способные выполнять аутентификацию с использованием NTLMv2. Чтобы разрешить аутентификацию для старых серверов, пользователь должен снять флажок Require Strong Authentication (NTLMv2).

Дополнительные сведения

Дополнительные сведения см. по следующим адресам:

- обзор семейства Windows Server 2003 — http://www.microsoft.com/windowsserver2003/evaluation/overview/;
- новое в сетевых и коммуникационных возможностях — http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/networking.mspx;
- Web-сайт Microsoft Windows~IPv6 — http://www.microsoft.com/ipv6/;
- Web-сайт Microsoft Windows–Wi-Fi — http://www.microsoft.com/wifi/;
- Web-сайт Microsoft Windows-VPN — http://www.microsoft.com/vpn/;
- Web-сайт MicrosoftWindows–IAS — http://www.microsoft.com/win-dows2000/technologies/communications/ias/;
- Web-сайт Microsoft Windows–IPSec — http://www.microsoft.com/win-dows2000/technologies/communications/ipsec/.

ГЛАВА
7



Службы терминалов

Службы терминалов (Terminal Services) Microsoft Windows Server 2003 расширяют функциональность служб терминалов Windows 2000 и включают клиентские функции и поддержку протоколов, добавленные в Windows XP. Службы терминалов позволяют работать с Windows-приложениями и рабочим столом Windows практически на любом компьютере, включая даже те, что работают не под Windows.

Службы терминалов Windows Server 2003 упрощают развертывание, управление и работу ПО в масштабе предприятия. Когда пользователь запускает приложение на сервере терминалов (доступном через службы терминалов), оно выполняется на сервере, а по сети передаются только команды от клавиатуры и мыши, а также отображаемые на экране данные. Каждый пользователь видит только свой сеанс, управляемый ОС сервера и независимый от сеансов других клиентов.

Преимущества служб терминалов

Службы терминалов Windows Server 2003 предоставляют следующие преимущества,

- **Быстрое, централизованное развертывание приложений** Сервер терминалов — удачное решение для быстрого развертывания Windows-приложений, особенно часто обновляемых, нерегулярно используемых или сложных в обслуживании. Когда управление приложением осуществляется на сервере терминалов, а не на каждом из устройств, админи-

стратор может гарантировать, что пользователи будут запускать последнюю версию приложения,

- **Доступ к данным через соединения с низкой пропускной способностью** Применение служб терминалов для запуска приложений через соединения с ограниченной пропускной способностью, такие как модемное или совместно используемое соединение глобальной сети (WAN), эффективнее для удаленного доступа и управления большими объемами информации, так как вместо самих данных пересылается представление данных на экране.
- **Windows везде** Сервер терминалов повышает производительность, обеспечивая доступ пользователей к приложениям с любых устройств, включая аппаратуру с низкой производительностью и рабочим столом, отличным от предоставляемого Windows. Поскольку сервер терминалов позволяет применять Windows везде, вы можете получить дополнительные вычислительные возможности, работая с такими переносными устройствами, как Pocket PC.

Клиентские возможности

Новые клиентские возможности обеспечивают улучшенное управление серверами терминалов и компьютерами, работающими под Windows Server 2003.

Улучшенный интерфейс пользователя

Большинство новых функций значительно улучшает интерфейс пользователя на стороне клиента.

- **Подключение удаленного рабочего стола (Remote Desktop Connection, RDC)** Улучшенный клиент служб терминалов RDC служит для подключения к удаленному рабочему столу в компьютерах с Windows XP Professional и может применяться для подключения к предыдущим версиям служб терминалов, в том числе Microsoft Windows NT 4.0 Terminal Server Edition и Windows 2000. Чтобы использовать RDC, достаточно просто ввести имя удаленного компьютера и выбрать Connect (рис. 7-1).
- **Переключение между удаленным сеансом и рабочим столом** По умолчанию удаленный сеанс запускается в полно-

экранном режиме с высококачественным цветом. Панель Connection Bar, расположенная в верхней части экрана сеанса RDC, позволяет переключаться между удаленным сеансом и рабочим столом локального компьютера.

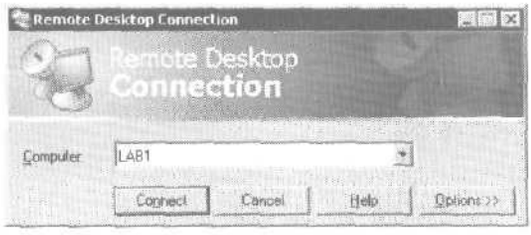


Рис. 7-1. Подключение к удаленному компьютеру посредством Remote Desktop Connection

- **Настройка удаленного подключения** На вкладках окна свойств можно задать режимы дисплея, перенаправляемые локальные ресурсы и программы, запускаемые при подключении.
- **Оптимизация производительности для подключений с низкой пропускной способностью** Вы можете выбрать скорость подключения и отключить ненужные компоненты удаленного сеанса, например, темы, кэширование растровых изображений и анимацию. Для настройки служит вкладка Experience диалогового окна Remote Desktop Connection (рис. 7-2).
- **Нет отдельного диспетчера подключений (Connection** Manager) Connection Manager более не нужен, так как ею функциональность расширена и интегрирована в RDC. Это позволяет пользователям и администраторам сохранять и открывать файлы с параметрами подключений, которые могут задаваться локально или для других пользователей. Сохраняемый пароль надежно шифруется и может быть расшифрован только на том компьютере, на котором был сохранен.
- **Автоматическое восстановление подключения** Чтобы улучшить защиту от сетевых сбоев (особенно в беспроводных и модемных средах), RDC пытается восстановить соединение с сервером, когда обрыв сетевого соединения вызывает завершение сеанса.
- **Перенаправление клиентских ресурсов** Remote Desktop Connection поддерживает широкий диапазон типов перена-

правления данных. По соображениям безопасности любой из них может быть отключен на клиенте или на сервере. При запросе перенаправления данных файловой системы, портов или смарт-карт выводится предупреждение системы безопасности; пользователь может прервать подключение или запретить перенаправление,

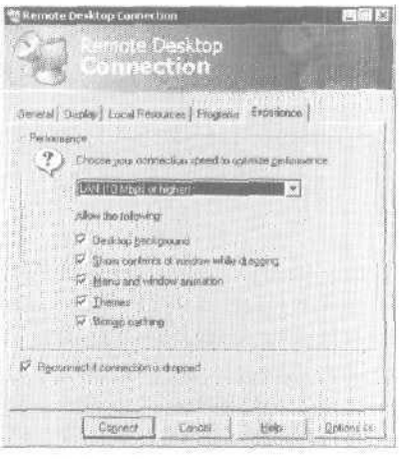


Рис. 7-2. Вы можете настроить параметры подключения с учетом доступной полосы пропускания

Возможности перенаправления клиентских ресурсов

Если в приведенном списке не указано иное, возможности перенаправления клиентских ресурсов доступны только для клиентов, подключенных к компьютерам с Windows Server 2003/XP Professional. Новые возможности может использовать любой клиентский компьютер с работающей службой Remote Desktop Connection.

- **Файловые системы** Клиентские диски, в том числе сетевые, подключаются в сеансе сервера. Это дает пользователям возможность открывать/сохранять файлы на дисках их собственного компьютера в дополнение к открытию/сохранению файлов на сервере.
- **Порты** Последовательные порты клиентского компьютера могут управляться с сервера. Это позволяет выполняюще-

муся на сервере ПО получить доступ к оборудованию, подключенному к клиентскому компьютеру.

- Принтеры Все установленные на клиентском компьютере принтеры, включая сетевые, доступны серверу. В Windows 2000 Terminal Services перенаправление работало только для принтеров, подключенных непосредственно к компьютеру. Перенаправляемым принтерам даются простые и понятные имена. Например, пользователь может видеть *printername on printserver (from clientname) in session 9.* В Windows 2000 это имя выглядело бы так: *_printserver_printername/clientname/ Session 9.* Перенаправление принтеров также работает при подключении к серверам с Windows 2000.
- Аудиоданные Звуки, такие как уведомления об ошибках или о получении электронной почты, перенаправляются клиенту.
- Смарт-карты Смарт-карта, содержащая учетную запись для регистрации пользователя Windows, может предоставить эти данные для регистрации пользователя при удаленном подключении к Windows Server 2003. Чтобы задействовать эту возможность, на клиентском компьютере должна быть установлена ОС, способная первой распознать смарт-карту: Windows 2000/XP/CE .NET.
- Клавиши Windows Комбинации клавиш, такие как Alt+Tab и Ctrl+Esc, по умолчанию пересылаются через удаленное подключение. Комбинацию Ctrl+Alt+Del из соображений безопасности всегда обрабатывает клиентский компьютер. Эти комбинации работают так же, когда клиент подключен к серверу терминалов с Windows 2000, но только если компьютер клиента работает под управлением ОС семейства Windows NT. Для клиентских компьютеров с Windows 95/98 эта возможность недоступна.
- Часовые пояса Клиентский компьютер с RDC может предоставить серверу данные о часовом поясе, или пользователь может вручную указать свой часовой пояс. Это позволяет администратору применять один сервер для нескольких клиентов, расположенных в разных часовых поясах. Это полезно и для приложений, поддерживающих такие функции, как календарь. По умолчанию эта возможность отключена, так как она зависит от правильности настройки параметров часового пояса на клиентском компьютере.

- **Виртуальные каналы** По виртуальным **каналам** (Virtual Channels) могут передаваться **различные типы данных между клиентским компьютером и** сервером. Эта **возможность** доступна **в Windows Server** 2003/2000 **Server. О виртуальных каналах** см. на сайте MSDN *http://msdn.microsoft.com/*.

Варианты развертывания клиентского ПО

Служба Remote Desktop Connection встроена в Windows XP/Server 2003. Установить RDC на клиентском компьютере, где этой службы нет, можно одним из следующих способов.

- Используйте инструменты, такие как Microsoft Systems Management Server или Windows 2000 Group Policy для публикации/назначения RDC на базе Windows Installer.
- Создайте совместно используемый клиентский дистрибутив на Windows Server 2003. (Этот вариант годиться и для Windows 2000 Server.)
- Установите RDC с компакт-диска Windows XP/Server 2003. Для этого выберите пункт Perform Additional Tasks в меню, появляющемся при автозагрузке с компакт-диска. (Устанавливать ОС при этом не требуется.)
- Загрузите RDC с Web-сайта http://www.microsoft.com/windowsxp/remotedesktop.

Примечание Remote Desktop Web Connection — это улучшенный, безопасный для сценариев элемент ActiveX/COM-объект. Его могут использовать провайдеры приложений (ASP) и организации, желающие развернуть Web-страницысовстроеннымиWeb-приложениями,применяющими компоненты Win32. Кроме того, версия RDC для Windows CE включена в Windows CE .NET Platform Builder, что позволяет включать ее в свои устройства разработчикам аппаратуры, работающей под управлением Windows CE.

Новые возможности сервера

Ряд новых возможностей сервера обеспечивает улучшенное управление службами терминалов и Windows Server 2003.

Улучшенное управление сервером

Большинство из перечисленных далее возможностей упрощает управление сервером независимо от того, установлены ли службы терминалов.

- Удаленный рабочий стол для администрирования Удаленный рабочий стол для администрирования (Remote Desktop for Administration) построен на основе режима удаленного администрирования в службах терминалов Windows 2000. В дополнение к двум виртуальным сеансам, доступным в режиме удаленного администрирования служб терминалов Windows 2000, администратор может устанавливать подключение к реальной консоли сервера. Инструменты, не работавшие раньше в удаленном сеансе, поскольку взаимодействовали с «сеансом 0», теперь работают удаленно.

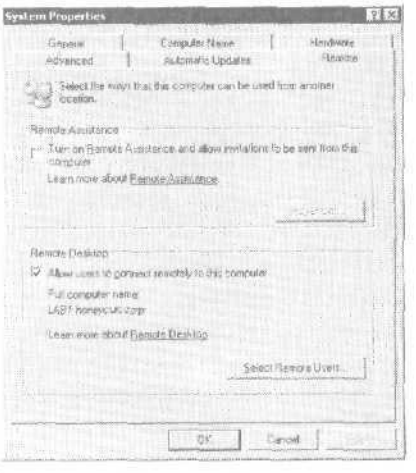


Рис. 7-3. Удаленный рабочий стол устанавливается по умолчанию и легко включается на вкладке Remote панели System Properties

- Подключение к консоли Подключиться к консоли можно:
  - □ из оснастки Remote Desktop консоли Microsoft Management Console (MMC);
  - D запустив программу Remote Desktop Connection (mstsc.exe) с параметром командной строки */console;*
  - □ создав страницу Remote Desktop Web Connection с установленным свойством *ConnectToServerConsole.*

- **Активизация удаленного рабочего стола и служб терминалов** В отличие от Windows 2000 Server, в котором компоненты служб терминалов работали в двух режимах, Windows Server 2003 разделяет функции в независимые настраиваемые компоненты. Удаленный рабочий стол для администрирования включается на вкладке Remote панели управления System (рис. 7-3). Службы терминалов включаются путем добавления компонента Terminal Server из раздела Windows Components мастера Add/Remove Programs.

Дополнительные возможности управления

Перечисленные ниже возможности облегчают управление службами терминалов в Windows Server 2003.

- **Групповая политика** Позволяет управлять свойствами служб терминалов. При этом можно одновременно настраивать группу серверов, включая параметры для новых возможностей, такие как путь к профилю служб терминалов для каждого компьютера и запрещение отображения обоев рабочего стола при работе через удаленное подключение.
- **Провайдер Windows Management Interface (WMI)** Позволяет настроить параметры служб терминалов с помощью сценариев. Множество псевдонимов WMI предоставляет простой интерфейс для часто используемых задач WMI.
- **Active Directory Service Interfaces** Провайдер Active Directory Services Interface (ADSI) обеспечивает программный доступ к личным параметрам профиля пользователя служб терминалов, таким как домашний каталог, разрешения удаленного помощника (Remote Assistance) и т. д.
- **Управление принтерами** В управление принтерами были внесены улучшения:
  - □ улучшен алгоритм поиска подходящего драйвера принтера в случае неполного совпадения;
  - а когда не удается выбрать нужный драйвер, параметр Trusted Driver Path позволяет указать другие стандартные драйверы принтера, которые вы разрешите использовать вашим серверам терминалов;
  - D поток данных принтера сжимается, чтобы повысить производительность медленных соединений между клиентом и сервером.

- **Диспетчер служб терминалов** Усовершенствованный диспетчер служб терминалов (Terminal Services Manager) упрощает управление большими массивами серверов, сокращая автоматический поиск серверов. Это позволяет обращаться к выбранным серверам по имени и создавать список часто используемых серверов.
- **Диспетчер лицензий сервера терминалов** Диспетчер лицензий сервера терминалов (Terminal Server License Manager) улучшен с целью сделать более простой активизацию сервера лицензий на сервере терминалов и назначение лицензий.
- **Односеансовая политика** Позволяет ограничить пользователей одним сеансом независимо от того, является ли он активным, даже в рамках серверной фермы.
- **Сообщения об ошибках на клиентах** Более 40 новых сообщений об ошибках на клиентах упрощают диагностику проблем клиентских подключений.

Усиленная безопасность

Модель доступа сервера терминалов теперь боле соответствует парадигме управления серверами Windows.

- **Группы пользователей удаленного рабочего стола** Вместо того чтобы добавлять пользователей в список программы Terminal Services Connection Configuration (TSCC), вы просто делаете их членами группы Remote Desktop Users (RDU). Например, чтобы разрешить доступ к серверу терминалов любому пользователю, можно добавить группу Everyone в группу RDU. Применение реальных групп пользователей Windows NT означает также, что для контроля доступа к серверам терминалов в группах серверов может применяться групповая политика. Чтобы назначать индивидуальные разрешения для сетевой карты в серверах с несколькими сетевыми картами, администратор может продолжать использовать TSCC.
- **Редактор политик безопасности** Права пользователей служб терминалов могут назначаться индивидуальным пользователям или группам с помощью редактора политик безопасности (Security Policy Editor). Это позволяет дать пользователям возможность регистрации на сервере терминалов, не делая их членами группы Remote Desktop Users.

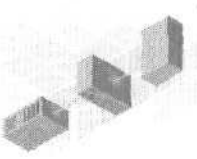
- **128-разрядное шифрование** По умолчанию подключения к серверам терминалов защищаются 128-разрядным симметричным шифрованием по алгоритму RC4, если для клиента разрешено 128-разрядное шифрование. (Шифрование RDC является 128-разрядным по умолчанию.) Возможно подключение клиентов предыдущих версий, применяющих шифрование с меньшим числом разрядов, если не указано, что разрешено подключение клиентов только с сильным шифрованием.
- **Политики ограниченного использования программ** Позволяют администраторам применять групповую политику для упрощения блокировки серверов терминалов (и других компьютеров с Windows Server 2003) посредством разрешения запуска определенных программ только указанным пользователям. Эта встроенная возможность Windows заменяет утилиту AppSec (Application Security) из предыдущих версий служб терминалов.
- **Каталог сеансов** Серверы терминалов можно организовать в фермы, что позволяет кластерам с балансировкой нагрузки компьютеров выглядеть с точки зрения пользователей единой отказоустойчивой службой. Каталог сеансов служб терминалов позволяет пользователям повторно соединяться с определенным разъединенным сеансом в пределах фермы, а не быть перенаправленными при подключении на наименее загруженный сервер. Служба каталога сеансов может задействовать службу балансировки нагрузки в Windows или программы балансировки нагрузки от сторонних производителей и службы, которые могут выполняться на любом компьютере с Windows Server 2003. Компьютеры, составляющие ферму серверов терминалов, должны работать под управлением Windows Server 2003 Enterprise Edition.

Дополнительные сведения

Дополнительные сведения см. по следующим адресам:

- **«Что нового в** службах **терминалов?» —** *http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/terminalserver.mspx*;

- обзор семейства Windows .NET Server — *http://www.microsoft.com/windowsserver2003/evaluation/overview/*;
- описание возможностей Windows .NET Server — *http://www.microsoft.com/windowsserver2003/evaluation/feature/*;
- обзор «.NET» в семействе Windows .NET Server - - *http://www.microsoft.com//windows.netserver/evaluation/overview/dotnet/dotnet.mspx*;
- применение политики ограниченного использования программ для зашиты от неавторизованного ПО — *http://www.microsoft.com/windowsxp/pro/techinfo/administration/restrictionpolicies/*;
- тонкий клиент в Windows — *http://www.microsoft.com/windows/powered/thinclients/*;
- развертывание приложений с использованием технологий Microsoft Management Technologies — *http://www.microsoft.com/windows2000/techinfo/howitworks/management/apdplymgt.asp*.



ГЛАВА

8

Internet Information Services

Администраторам и разработчикам Web-приложений необходима быстрая, надежная, масштабируемая и защищенная Web-платформа. IIS 6.0 и Microsoft Windows Server 2003 предоставляют много новых возможностей для управления сервером Web-приложений, обеспечения высокой производительности и масштабируемости, доступности и надежности, а также безопасности. По пожеланиям пользователей архитектура **IIS** усовершенствована.

В этой главе рассказывается о следующем поколении функций Web-инфраструктуры, предоставляемых Windows Server 2003. Рассматриваются также новые возможности, доступные при развертывании IIS 6.0, в частности, архитектура IIS, новые функции управления и защиты, меры, предпринятые для повышения производительности и др.

Роль Web Application Server

Web application server (сервер Web-приложений) — новая роль сервера, реализованная в семействе ОС Windows Server 2003, — объединяет некоторые ключевые серверные технологии в отдельную сущность — *сервер приложений* (application server). Вот эти технологии:

- IIS;
- **ASP.NET;**
- **ASP;**
- COM +;

- Microsoft **Data** Engine (MSDE);
- Microsoft Message Queuing (MSMQ).

В результате такого объединения у администраторов и разработчиков Web-приложений появилась возможность размещать динамическое содержимое, например приложения ASP.NET под управлением БД, не устанавливая на сервере дополнительное ПО.

В Windows Server 2003 сконфигурировать сервер приложений позволяют следующие утилиты.

- **Configure Your** Server (CYS) Эта отправная точка для конфигурирования ролей Windows Server 2003 теперь включает новую роль Web application server, которая заменяет роль Web server. Управлять установленной ролью можно из приложения Manage Your Server, в котором будет присутствовать новая запись сервера приложений.
- **Add/Remove Components** Сервер приложений доступен как необязательный компонент верхнего уровня в приложении Add/Remove Components. Это новый способ установки ПО, относящегося к серверу приложений (IIS, ASP.NET, COM+ и MSMQ), и настройки компонентов такого ПО, Конфигурируя сервер приложений средствами Windows Add/Remove Components, вы точнее определите список устанавливаемых компонентов ПО.

Новая архитектура обработки запросов

Код Web-узлов и приложений становится все сложнее. Нестандартные приложения и Web-узлы вполне могут включать несовершенный код. В связи с этим управляющие процессы должны активно контролировать исполняющую среду, автоматически выявляя утечки памяти, нарушения прав доступа и другие ошибки. При этом базовая архитектура должна обеспечить отказоустойчивость, активно перезапуская или повторно используя процессы по мере необходимости и продолжая ставить запросы в очередь, чтобы не нарушать работу конечных пользователей.

Для реализации этой устойчивой и активно управляемой исполняющей среды ITS 6.0 предоставляет управление очередью запросов на уровне ядра — новую среду изоляции приложений с активным управлением процессами, называемую также режимом изоляции рабочего процесса. В архитектуре IIS 5.0

в качестве основного процесса Web-сервера выступал единственный процесс, Inetinfo.exe, передававший поступавшие ему запросы для обработки приложениям, выполняющимся вне процесса (dllhost.exe). IIS 6.0 делится на два новых компонента, использующих новый драйвер режима ядра, что позволяет IIS разделить основной код Web-сервера и код обработки приложений. Вот эти компоненты:

- **HTTP.sys** — HTTP-слушатель, работающий в режима ядра;
- **WWW Service Administration and Monitoring** — диспетчер конфигурации и процессов, работающий в пользовательском режиме.

Обработку всех операций Web-приложений, включая загрузку фильтров и расширений ISAPI, а также проверку подлинности и авторизацию, осуществляет новая DLL службы WWW. Эта DLL загружается в один или несколько управляющих процессов, которые называются *рабочими* и обслуживают запросы на выделение пулов приложений в HTTP.sys. Имя исполнимого файла рабочего процесса — w3wp.exe. О взаимодействии рабочих процессов с IIS 6.0 см. ниже раздел «Режим изоляции рабочего процесса». *Пул приложений* соответствует одной очереди запросов в HTTP.sys и одному или нескольким рабочим процессам. Пул приложений может обслуживать запросы к одному или нескольким уникальным Web-приложениям. Приложения сопоставляются с пулами на основе своих URL. Возможна одновременная работа нескольких пулов приложений. О пулах приложений см. ниже раздел «Режим изоляции рабочего процесса».

Примечание На сервере с 8 процессорами предварительное тестирование показало более чем 100%-ый рост производительности в сравнении с предыдущими версиями IIS. Это следствие реализации новой архитектуры обработки запросов и усовершенствований в области масштабируемости в сервере Web-приложений.

HTTP.sys

В IIS 6.0 HTTP.sys прослушивает запросы и помещает их в соответствующие очереди. Каждая очередь запросов соответ-

ствует одному пулу приложений. В HTTP.sys не выполняется код, созданный программистами сторонних фирм, и поэтому ошибки в коде пользовательского режима, обычно влияющие на состояние службы WWW, на HTTP.sys не сказываются.

Если почему-либо инфраструктура обработки запросов пользовательского режима прекратит существование, HTTP.sys продолжит принимать запросы и помещать их в очередь при условии, что служба WWW запущена и выполняется. HTTP.sys будет принимать запросы и помещать их в соответствующую очередь, пока не закончатся очереди, не останется места в очередях или не будет остановлена служба WWW.

Обнаружив аварийно завершившийся рабочий процесс, в пуле приложений которого имеются ожидающие обслуживания запросы, служба WWW запускает новый рабочий процесс. Таким образом, хотя временная остановка обработки запросов пользовательского режима и возможна, пользователь ее не заметит, поскольку запросы все так же принимаются и ставятся в очередь,

Компонент WWW Service Administration

Еще одна ключевая особенность новой архитектуры IIS 6.0 — функциональность WWW Service Administration and Monitoring. Этот компонент — основная часть службы WWW. где, как и в HTTP.sys, находятся критические службы IIS 6.0 и никогда не загружается код сторонних фирм,

WWW Service Administration and Monitoring отвечает за конфигурирование и управление процессами. В период инициализации диспетчер процесса запросов из состава службы WWW считывает данные метабазы и инициализирует таблицу маршрутизации пространства имен HTTP.sys. внося в нее по одной записи для каждого приложения. Каждая запись включает сведения, на основе которых URL, сопоставленные с пулами приложений, маршрутизируются в конкретные пулы.

Эти действия по предварительной регистрации сообщают HTTP.sys о пуле приложений, реагирующем на запросы в данной части пространства имен, и о том, что HTTP.sys может при необходимости указать системе запустить рабочий процесс. Предварительная регистрация полностью завершается до того, как HTTP.sys сможет передавать запросы процессам. По мере добавления пулов приложений и новых приложений служба

WWW конфигурирует HTTP.sys для приема запросов на новые URL, создает для новых пулов приложений новые очереди запросов и задает параметры маршрутизации новых URL.

В качестве диспетчера процесса запросов WWW Service Administration and Monitoring определяет время жизни рабочих процессов, обрабатывающих запросы, включая:

- время запуска рабочего процесса;
- время повторного использования рабочего процесса:
- время перезапуска рабочего процесса, если тот больше не может обрабатывать запросы (блокируется).

Режим изоляции рабочего процесса

В IIS 6.0 реализован режим изоляции рабочего процесса, при котором весь код приложений выполняется в изолированной среде, но без падения производительности, имевшего место в предыдущих версиях IIS. HTTP-запросы передаются в очередь подходящего пула приложений: рабочие процессы пользовательского режима, обслуживающие пул приложений, выбирают запросы прямо от HTTP.sys, исключая тем самым ненужные циклы, возникающие при передаче запроса приложению, выполняющемуся вне процесса, и обратно.

В IIS 6.0 понятия приложений, выполняющихся в процессе, больше не существует: HTTP-службы периода выполнения приложений, например поддержка расширений ISAPI, доступны в любом пуле приложений. Такая архитектура исключает негативное влияние некорректно работающего Web-приложения или Web-узла на функционирование других Web-приложений (но не Web-узлов), обслуживаемых другими рабочими процессами на данном сервере. Теперь можно выгружать компоненты, выполняющиеся в процессе, не останавливая работу всей службы WWW. Можно временно приостанавливать управляющий рабочий процесс, не затрагивая другие рабочие процессы. Кроме того, дополнительное преимущество дает возможность подключать прочие службы ОС, доступные на уровне процессора (например, регулирование уровня загруженности процессора), для отдельных пулов приложений. Архитектура Windows также переработана для поддержки еще большего числа параллельных процессов.

Режим изоляции рабочих процессов IIS 6.0 предназначен для того, чтобы администраторы могли помещать разные Web-приложения и Web-узлы в разные пулы приложений. Так, на сервере подразделений приложение Web-HR может находиться в одном пуле приложений, а Web-Finance — в другом; поставщик услуг Интернета может поместить узлы CustomerX.com и CustomerY.com в разные пулы приложений.

Режим изоляции рабочего процесса исключает останов приложения или узла из-за сбоев в работе другого приложения/узла. Кроме того, разнеся приложения и узлы по разным рабочим процессам, вы упрощаете ряд административных задач, в частности, перевод приложения/узла в рабочий или автономный режим (независимо от прочих выполняющихся в системе приложений), замену используемого приложением компонента, мониторинг счетчиков приложения и регулирование ресурсов, к которым обращается приложение.

Пулы приложений

Пул приложений — это набор Web-приложений, совместно использующих один или несколько рабочих процессов. Все пулы приложений отделены друг от друга границами процесса. На приложение, передаваемое в один пул приложений, не влияют другие пулы, и в период обслуживания текущим пулом передача приложения в другой пул невозможна. В период работы сервера приложения можно легко сопоставить с другим пулом. В HTTP.sys пулы приложений представлены очередью запросов, из которой рабочие процессы пользовательского режима, обслуживающие пул, могут получать запросы.

Усовершенствования изоляции

Режим изоляции рабочего процесса усовершенствован.

- Надежность Реализованная архитектура исключает негативное влияние одних Web-приложений и Web-узлов, обслуживаемых в режиме изоляции рабочего процесса IIS 6.0, на другие Web-приложения, Web-узлы и на сервер в целом.
- Отсутствие перезагрузок Пользователю не нужно перезагружать сервер или полностью останавливать работу службы WWW. Обычные операции вроде обновления содержимого или компонентов, отладки Web-приложений и работы

с Web-приложениями, вызывающие сбои, не должны сказываться на обслуживании других узлов и приложений, выполняемых на сервере.

- **Саморегулирование** IIS 6.0 поддерживает автоматический перезапуск приложений, аварийно завершивших работу, и периодический перезапуск некорректно работающих приложений, приложений, вызывающих утечки памяти, и приложений с кодом, вызывающим сбои.
- **Масштабируемость** IIS 6.0 поддерживает масштабирование в соответствии с потребностями поставщиков услуг Интернета, у которых на одном сервере могут размещаться тысячи узлов. IIS 6.0 также поддерживает *Web-сады* (Web gardens), в которых каждый рабочий процесс из группы равноправных рабочих процессов на сервере получает лишь часть запросов, обычно обслуживаемых одним рабочим процессом. Это обеспечивает улучшенную многопроцессорную масштабируемость.
- **Жесткое понятие приложения** IIS 6.0 поддерживает приложения как единицу администрирования. Это включает активизацию изоляции приложений, регулирование ресурсов, а также масштабирование на основе приложения.

Web-сервер становится более надежным и всегда доступным, даже если в результате действий приложения его управляющий процесс аварийно завершится. Режим изоляции рабочего процесса развивает концепцию изоляции приложений, появившуюся в IIS 4.О. Приложения можно полностью изолировать друг от друга, чтобы ошибка одного приложения не сказывалась на работе другого приложения в другом процессе. Кроме того, режим изоляции рабочего процесса IIS 6.0 обеспечивает усовершенствованную изоляцию, не вызывая падения производительности. Запросы к приложению выбираются не процессом пользовательского режима из ядра, а напрямую из ядра; затем они соответственно передаются другому процессу пользовательского режима.

Повышенная надежность

Вот компоненты **режима изоляции рабочего процесса,** повышающие его **надежность, не снижая производительности,**

- **Четкое разделение пользовательского кода и сервера** Весь пользовательский код обрабатывают рабочие процессы, полностью изолированные от основного Web-сервера. Это совершенствует архитектуру TIS 5.0 в том плане, что программисты могут и зачастую загружают ISAPI на основном Web-сервере как выполняющееся в процессе приложение. Если ISAPI, загруженное в рабочем процессе, откажет или вызовет нарушение доступа, будет завершен только рабочий процесс, в котором выполняется ISAP1. Тем временем служба WWW создает новый рабочий процесс для замены отказавшего. На другие рабочие процессы это не влияет.
- **Множество пулов приложений** В **IIS** 5.0 приложения можно группировать для выполнения вне процесса, но только в одном пуле приложений — DLLHOST.EXE. Когда IIS 6.0 функционирует в режиме изоляции рабочего процесса, администраторы могут создавать множество пулов приложений с разными конфигурациями.
- **Улучшенная поддержка распределителей нагрузки** С пулами приложений в IIS появилось четкое физическое деление приложений — настолько четкое, что можно параллельно выполнять сотни и тысячи узлов и приложений на одном Windows-сервере. При такой конфигурации важно, чтобы одно проблемное приложение не влияло на другие. Желательно также автоматическое взаимодействие с распределителями нагрузки и коммутаторами, позволяющее перенаправлять только трафик проблемного приложения и дающая серверу возможность принимать запросы к нормально работающим приложениям. Допустим, сервер обрабатывает запросы к приложениям А и Б. Если Б отказывает столь часто, что IIS решает автоматически завершить его работу (см. пункт по быстрой защите против отказов), серверу нужна возможность получать запросы к приложению А. В IIS 6.0 реализована модель расширения, которая в случае обнаружения службой WWW отказа конкретного приложения запускает события и команды. Такая возможность позволяет сконфигурировать распределители нагрузки и коммутаторы для автоматического прекращения маршрутизации трафика проблемных приложений и продолжения маршрутизации трафика нормально работающих программ.

- **Web-сады** Режим изоляции рабочего процесса IIS 6.0 также позволяет сконфигурировать несколько рабочих процессов для обслуживания запросов к одному пулу приложений. По умолчанию у каждого пула есть только один рабочий процесс. И все же пул можно сконфигурировать так, чтобы запросы к нему обрабатывались группой равноправных рабочих процессов. Такая конфигурация называется Web-садом, поскольку она аналогична Web-ферме и отличается лишь тем, что размещается на олном сервере. HTTP.sys распределяет запросы между набором рабочих процессов из группы путем сопоставления очереди входящих запросов к пулу приложений *с* очередью *запросов на запросы* из каждого набора процессов в Web-саду. Преимущество Web-садов в том, что если один рабочий процесс остановится (зависнет ядро сценариев), другие процессы смогут принимать и обслуживать запросы.
- **Мониторинг состояния** Служба WWW ведет мониторинг состояния рабочих процессов, периодически опрашивая последние и определяя, не заблокированы ли они. Если рабочий процесс заблокирован, служба WWW завершает его и создает взамен новый рабочий процесс. Более того, служба WWW поддерживает канал связи с каждым рабочим процессом и быстро узнает об отказах процессов, выявляя разрывы каналов.
- **Привязка к процессору** Чтобы задействовать преимущества частого попадания в кэш (первого или второго уровня) процессора, рабочие процессы можно привязать к конкретному процессору.
- **Сопоставление узлов и приложений с пулами приложений** В IIS 6.0, как и в IIS 5.0, приложения — это пространства имен, для которых в метабазе определено свойство *AppIsolated*. По умолчанию узлы считаются простым приложением — таким, *в* котором в качестве приложения сконфигурировано корневое пространство имен (/). Пул приложений можно сконфигурировать для обслуживания чего угодно: от одного Web-приложения до сотен приложений и узлов. Чтобы сопоставить приложение с пулом приложений, нужно указать в метабазе, в какой пул должно передаваться это приложение.

- **Запуск по требованию** Пулы приложений предоставляют преимущества: например, запуск по требованию процессов, обслуживающих группу пространства имен, когда на сервер поступает первый запрос на URL из этой части пространства имен. Такой запуск, а также управление жизненным циклом рабочих процессов осуществляет диспетчер приложений IIS 6.0 (из состава службы WWW).
- **Допустимое время простоя** Пул приложений можно сконфигурировать так, чтобы при простое в течение определенного времени рабочие процессы указывали системе завершить их. Это делается для освобождения неиспользуемых ресурсов. При необходимости для пула приложений запускаются дополнительные рабочие процессы.
- **Быстрая защита против отказов** При аварийном завершении рабочий процесс разрывает канал связи со службой WWW. Та выявляет такой разрыв и принимает соответствующие меры, обычно включающие занесение информации о событии в журнал и перезапуск рабочего процесса. IIS 6.0 можно сконфигурировать так, чтобы при многократных отказах пул приложений автоматически отключался. Это называется *защитой против частых отказов* (rapid-fail protection). Защита от частых отказов переводит пул приложений в необслуживаемый режим, и на все запросы к данной части пространства имен, включая запросы, уже стоящие в очереди этого пула. HTTP.sys возвращает сообщение «503-Service Unavailable» (503 — Служба недоступна). Кроме того, администратор может явно перевести группу пространства имен в необслуживаемый режим, скажем, при переводе приложения в автономный режим из-за серьезной ошибки в нем. Для этого пул приложений нужно остановить средствами диспетчера IIS Manager или с помощью сценария.
- **Многократное использование рабочих процессов** На сегодня у многих организаций имеются проблемы с Web-приложениями, вызывающими утечки памяти. В связи с этим администраторам приходится перезагружать или перезапускать Web-серверы. Б предыдущих версиях IIS перезапуск Web-узла без остановки работы всего Web-сервера был невозможен.

Перезапуск рабочих процессов

Режим изоляции рабочего процесса можно сконфигурировать для периодического перезапуска рабочих процессов в пуле приложений с целью управления приложениями, вызывающими ошибки. Перезапуск возможен на основе таких критериев:

- прошедшее время;
- число обработанных запросов;
- по расписанию в течение 24 часов;
- запрос о состоянии, на который должен ответить процесс (см. в списке выше пункт по мониторингу состояния);
- использование виртуальной памяти;
- использование физической памяти;
- по требованию.

При перезапуске рабочего процесса служба WWW указывает существующему рабочему процессу завершить работу и дает ему время на обслуживает оставшихся запросов. Одновременно служба WWW создает заменяющий рабочий процесс для той же группы пространства имен, который запускается перед остановкой старого процесса, — такой подход исключает перерывы в обслуживании. Старый процесс остается на связи с HTTP.sys для обработки невыполненных запросов и завершается обычным образом или принудительно, если не завершится сам по истечении заданного периода времени.

Режим изоляции IIS 5.0

В IIS 6.0 реализовали режим изоляции рабочего процесса. Хотя данный режим обеспечивает повышенную изоляцию, надежность, доступность и производительность Web-серверам, некоторые приложения не могут работать в такой среде из-за проблем совместимости, например наследования состояния сеансов в процессе или если приложение написано в виде фильтра для чтения неструктурированных данных. В связи с этим у IIS 6.0 для обеспечения совместимости есть возможность переключаться на другую модель процессов — режим изоляции IIS 5.O.

Режим изоляции IIS 6.0 функционирует аналогично TIS 5.0, Фактически все выше режима ядра, называемое пользовательским режимом, работает так же, как и IIS 5.O. Благодаря наличию тех же основных процессов пользовательского режима, что

и в IIS 5.0, режим изоляции IIS 5.0 — это способ запуска IIS 6.0, обеспечивающий пользователям наибольшую совместимость. Применяются те же методы изоляции приложений (низкий, средний и высокий), и Inetinfo.exe по-прежнему является основным процессом, через которых проходят все запросы.

Кроме того, HTTP.sys предоставляет режиму изоляции IIS 5.0 те же преимущества, что и режиму изоляции рабочего процесса: управление очередью запросов на уровне ядра и кэширование на уровне ядра. IIS 6.0 изменяет порядок взаимодействия службы WWW и HTTP.sys.

Примечание Все прочие службы из состава Inetinfo, например FTP и SMTP, работают так же, как и в IIS 5.0, и точно так же входят в состав Inetinfo. Только служба WWW сконфигурирована для получения запросов от HTTP.sys.

Новые функции безопасности

Продумать все варианты атак и заранее устранить все уязвимые места невозможно. Однако в действиях хакеров усматривается некоторая закономерность. Вследствие этого для обеспечения повышенной безопасности IIS в TIS 6.0 реализован ряд превентивных мер. Кроме того, сделаны усовершенствования, упрощающие блокировку узла, поиск и установку программных заплат для системы безопасности.

Заблокированный сервер

IIS поставляется в заблокированном состоянии, в котором обслуживается только статичное содержимое (.htm-, .jpg-, .bmp- и аналогичные файлы), обеспечивая дополнительную защиту. IIS предоставляет несколько уровней безопасности.

- **По умолчанию IIS не устанавливается вместе с Windows Server 2003** Цель системы безопасности — понизить степень уязвимости вашей системы, и поэтому администратор должен выбрать и вручную установить IIS,
- **IIS устанавливается в заблокированном состоянии** Установка IIS по умолчанию предоставляет лишь минимальную функциональность. Обслуживаются только статичные фай-

лы, и всю прочую функииопальность администратор должен включать вручную.

- **Отключение при обновлении** Случайно установленные серверы IIS при обновлении Windows Server 2003 будут отключены.
- **Отключение IIS средствами оснастки Group Policy** В Windows Server 2003 администраторы домена могут запретить пользователям устанавливать IIS на компьютеры.
- **Запуск в контесте учетной записи с ограниченными привилегиями** Рабочие процессы IIS выполняются в контексте учетной записи с ограниченными привилегиями. Это значительно снижает риск потенциальных атак.
- **Безопасная ASP** Все встроенные функции всегда выполняются в контексте учетной записи с ограниченными привилегиями (анонимный пользователь).
- **Заретистрированные расширения файлов** TIS обслуживает только файлы с зарегистрированными расширениями и отбрасывает запросы на незарегистрированные расширения файлов.
- **Web-пользователям недоступны утилиты командной строки** Зачастую злоумышленники используют преимущества утилит командной строки, выполняемых на Web-сервере. В IIS 6.0 Web-сервер не может выполнять такие утилиты,
- **Содержимое защищено от записи** Получив доступ к серверу, злоумышленник нередко пытается изменить оформление Web-злов. Если анонимным Web-пользователям запрещено перезаписывать Web-содержимое, таких атак становится меньше.
- **Ограничения и время ожидания В IIS** 6.0 используются безопасные и действенные параметры по умолчанию. Это уменьшает число атак, так как раньше ограничения и время ожидания были слишком велики.
- **Ограничения на закачку данных** Администратор может ограничить объем данных, закачиваемых на сервер.
- **Защита от переполнения буфера** При переполнении буфера рабочий процесс аварийно завершает выполнение программы.
- **Проверка файлов** Прежде чем передать запрос обработчику (расширению ISAPI), основной сервер проверяет наличие запрошенного содержимого.

Чтобы уменьшить уязвимую область Web-сервера, IIS 6.0 в варианте установки по умолчанию обслуживает только статичное содержимое. Администратор должен вручную активизировать программную функциональность, предоставляемую API-интерфейсами IIS (ISAPI) или интерфейсами CGI (Common Gateway Interfaces). ISAPI и CGI расширяют возможности Web-страниц и поэтому называются здесь расширениями Web-службы. Например, чтобы использовать Active Server Pages в данной версии 1IS, нужно активизировать библиотеку ISAPI asp.dll в качестве нового расширения Web- службы.

Узел Web Service Extension позволяет администраторам Web-узлов включать/отключать функциональность IIS на основе, исходя из потребностей организации. Таким образом, чтобы дополнительная функциональность, скажем, Active Server Pages или серверные расширения FrontPage, работала, как вам надо, ее нужно предварительно активизировать. IIS 6.0 предоставляет программные и графические интерфейсы, а также интерфейсы командной строки для активизации расширений Web-сервиса.

Идентификатор рабочего процесса

К Web-серверам, на которых выполняется масса приложений и узлов, предъявляются дополнительные требования. Если поставщик услуг Интернета размещает на одном сервере узлы двух компаний (последние могут быть и конкурентами), гарантировать изоляцию обоих приложений друг от друга он не может. Более того, поставщик услуг Интернета должен убедиться, что злонамеренный администратор одного приложения не сможет обращаться к данным другого.

IIS 6.0 предоставляет уровень полной изоляции при помощи конфигурируемого идентификатора рабочего процесса. Вместе с другими средствами изоляции, например, регулированием полосы пропускания и использования процессора, а также повторным использованием процессов на основе доступного объема памяти, IIS 6.0 предоставляет среду, позволяющую размешать на одном Web-сервере даже наиболее жестко конкурирующие приложения. Точно так же IIS 6.0 предоставляет и среду, позволяющую выполнять на одном Web-сервере множество приложений с полной изоляцией последних.

IIS выполняется в контексте учетной записи NetworkService

Рабочий процесс выполняется в контексте новой учетной записи NetworkService, обладающей весьма ограниченными привилегиями. Выполнение в контексте такой записи — один из важнейших принципов безопасности. Вероятность использования уязвимых мест системы безопасности очень низка, если рабочий процесс обладает в базовой системе ограниченным набором прав.

Усовершенствования SSL

В IIS 6.0 реализовано три основных усовершенствования протокола Secure Sockets Layer (SSL).

- **Производительность** IIS 5.0 предоставляет самую быструю программную реализацию SSL на рынке, и вследствие этого 50% всех Web-узлов, использующих данный протокол, работают под управлением IIS. IIS 6.0 предоставляет еще более быструю реализацию этого протокола. Microsoft модернизировала и сконфигурировала базовую реализацию SSL для обеспечения повышенной производительности и масштабируемости.
- **Объект Remotable Certification Object** В IIS 5.0 администраторы не могут удаленно управлять сертификатами SSL, поскольку хранилище сертификатов *поставщика услуг шифрования* (cryptographic service provider, CSP) не поддерживает удаленного взаимодействия. Клиенты управляют сотнями и тысячами серверов IIS с использованием сертификатов SSL, и поэтому им нужна возможность удаленной работы с такими сертификатами,
- **Возможность выбора поставщика услуг шифрования** При использовании протокола SSL производительность заметно падает, так как процессору приходится интенсивно заниматься шифрованием. Существуют специальные аппаратные платы, снимающие с процессора нагрузку по шифрованию. Они подключают к системе собственный поставщик Crypto API (CAPI). IIS 6.0 упрощает выбор стороннего поставщика.

Если проверка подлинности дает ответ на вопрос «Кто вы?», авторизация отвечает на вопрос «Каковы ваши права?». Таким образом, авторизация позволяет/запрещает пользователю выполнять те или иные операции. IIS 6.0 поддерживает механизм

проверки подлинности Passport, интегрированный в Windows Server 2003. IIS 6.0 расширяет применение новой инфраструктуры авторизации, реализованной в Windows Server 2003. Кроме того, для управления доступом Web-приложения могут совместно использовать авторизацию URL и диспетчер Authorization Manager. В Windows Server 2003 добавлена принудительная, делегированная авторизация, предоставляющая администраторам домена возможность разрешать делегирование только определенным машинам и службам.

Интегрированный механизм Passport

IIS 6.0 поддерживает проверку подлинности Passport, интегрированную в Windows Server 2003, что обеспечивает проверку подлинности средствами Passport на основном Web-сервере и использует интерфейсы Passport версии 2, предоставляемые стандартными компонентами Passport. К услугам администратора клиентская база Passport (свыше 150 000 000 записей), избавляющая его от таких проблем управления учетными записями, как окончание срока действия пароля и повторная инициализация.

Когда результаты проверки подлинности средствами Passport будут заверены, пользователя механизма Windows Server 2003 Passport можно сопоставить с пользователем Active Directory путем идентификации Windows Server 2003 Passport (если такое сопоставление существует). Local Security Authority (LSA) создает для пользователя маркер, который затем задается IIS для HTTP-запроса.

Разработчики приложений и администраторы Web-узлов могут применять данную модель безопасности для проверки подлинности на основе пользователей Active Directory. Кроме того, данные реквизиты позволяет передавать новая функция Constrained Delegation, поддерживаемая в Windows Server 2003.

Авторизация URL

Для принятия решений авторизации сегодня применяются списки контроля доступа (access control list, ACL). Однако модель ACL ориентирована преимущественно на объекты (файлы, папки) и пытается соответствовать требованиям диспетчера ресурсов — файловой системы NTFS, Однако большинство

современных Web-приложений — это бизнес-приложения, ориентированные не на объекты, а на выполнение конкретных задач. Если приложение должно предоставить модель управления доступом на основе операций или задач, ему потребуется создать собственную такую модель. Реализованная в Windows Server 2003 новая инфраструктура авторизации обеспечивает соответствие потребностям таких бизнес-приложений.

IIS 6.0 расширяет применение этой инфраструктуры, предоставляя предварительную авторизацию для конкретных URL. Кроме того, Web-приложения могут совместно использовать авторизацию URL и диспетчер Authorization Manager для централизованного (на основе единого хранилища политик) управления доступом к URL, подвергающих Web-приложение риску, а также для управления специфичными для приложения задачами и операциями. Размещение политик в едином хранилище позволяет централизованно управлять доступом к URL и функциям приложений, используя при этом преимущества групп приложений уровня хранилища и программируемых бизнес-правил.

Делегированная аутентификация

Делегирование — это предоставление серверному приложению разрешения выступать в сети в качестве пользователя. Как пример можно привести Web-сервис в корпоративной интрасети, который в качестве клиента собирает данные с разных серверов предприятия и затем, обобщив их, выводит конечному пользователю по протоколу HTTP.

В Windows Server 2003 реализовано принудительное делегирование, дающее администраторам домена возможность разрешать делегирование только определенным компьютерам и службам. Вот некоторые советы по делегированию.

- Делегирование не должно позволять серверу подключаться от имени клиента к ресурсам домена или леса. Должны допускаться только подключения к определенным службам (например, к серверной БД SQL Server или удаленному хранилищу данных). Иначе недобросовестный администратор сервера или приложения может подменить клиента и от его имени пройти проверку подлинности для подключения к ресурсам домена.

- В ходе делегирования клиент не должен предоставлять свои регистрационные реквизиты серверу. Получив их. недобросовестный администратор сервера или приложения сможет использовать их во всем домене и не только для подключения к серверному хранилищу данных.

Принудительная, делегированная проверка подлинности — это рекомендуемая архитектура разработки приложений в среде Windows, поскольку можно задействовать высокоуровневые протоколы, например, Remote Procedure Call (RPC) и Distributed Component Object Model (DCOM). Они позволяют незаметно переносить контекст пользователя с сервера на сервер и подменять этот контекст. Кроме того, эти протоколы позволяют применять контекст пользователя в качестве этого самого пользователя при проверке подлинности, осуществляемой различными объектами по правилам авторизации, определяемым данными о группах домена и о локальных группах, а также независимыми ACL, сопоставленными ресурсам сервера.

Новые средства управления

Стандартный современный Web-узел Интернета размещается не на одном, а на нескольких Web-серверах — *Web-фермах* (Web farms). Web-ферма — это кластер серверов, предоставляющих содержимое, бизнес-логику и службы. По мере того как организации предоставляют все больше приложений через Web, растет и число узлов интрасетей, в частности узлов, предоставляющих торговые приложения с поддержкой Web.

Кроме того, с распространением удаленного администрирования растет потребность в совершенствовании доступа к API и поддержки прямого конфигурирования. В свете изменений, произошедших в Интернете и интрасетях в последние годы, управление Web-узлом перестало представлять собой управление одним или несколькими Web-серверами и стало интегрированным и сложным процессом.

В IIS 6.0 реализованы новые функции, которые расширяют возможности управления, предоставляемые администраторам Web-узлов на основе **IIS.** IIS 6.0 включает заменяющий метабазу уровень хранения данных (хранилище конфигурации), который позволяет напрямую редактировать конфигурацию метабазы в текстовом режиме, обеспечивая возможность вос-

становления измененной информации. Более того, поддержка WMI и работы с командной строкой позволяют администрировать Web-узлы средствами IIS Manager.

XML-метабаза

Метабаза — это иерархичное хранилище используемых IIS конфигурационных параметров, предоставляющее обширную функциональность, например, наследование, управление типами данных, уведомление об изменениях и систему безопасности. В IIS 4.0 и 5.0 конфигурация метабазы хранилась в двоичном файле закрытого формата, и считать или изменить ее было непросто. В IIS 6.0 этот файл, называвшийся MetaBase.bin, заменен текстовыми файлами формата XML. Вот краткий обзор XML-метабазы.

- Преимущества текстовых файлов метабазы формата XML:
  - улучшенные возможности резервного копирования и восстановления на неисправных компьютерах;
  - усовершенствованное устранение проблем и восстановление метабазы при нарушении целостности данных;
  - возможность прямой модификации стандартными средствами редактирования текста;
  - возможность экспорта/импорта конфигурации приложения в указанное пользователем место;
  - повышенная производительность и масштабируемость.
- Новая XML-метабаза позволяет администраторам напрямую считывать и редактировать конфигурационные параметры, не используя сценарии или код для администрирования Web-сервера. XML-метабаза значительно упрощает:
  - диагностику вероятного нарушения целостности данных метабазы;
  - расширение имеющейся схемы метабазы средствами XML;
  - просмотр и редактирование текущей конфигурации метабазы прямо в файле метабазы с обеспечением 100%-ой совместимости с существующими открытыми API-интерфейсами метабаз и интерфейсом Active Directory Services Interface (ADSI).
- Новая XML-метабаза повышает производительность и масштабируемость. Имеющаяся двоичная метабаза без проблем обновится до XML-метабазы. Новая XML-метабаза:

- D занимает столько же или меньше места на диске;
- □ обеспечивает более высокую скорость считывания данных при запуске Web-сервера, чем двоичная метабаза IIS 5.0;
- □ обеспечивает такую же производительность записи, как и двоичная метабаза IIS 5.O.

• Новая XML-метабаза решает проблемы управления следующими способами:

- П прямое редактирование и устранение проблем конфигурации метабазы с обеспечением повышенной надежности;
- П применение утилит, допускающих форматирование текста, например windiff, систем управления версиями, а также средств редактирования;
- П откат конфигурации;
- Р журналы с номерами версий, включающие копии метабазы для всех изменений;
- □ клонирование конфигурации Web-узлов и приложений;
- □ резервное копирование и восстановление, не привязанное к серверу.

По-прежнему поддерживаются схема ADSI и расширение схем. Удобная для чтения и редактирования схема поддерживает ADSI и еще больше повышает читабельность и удобство редактирования текстового формата. В метабазу добавлена новая конфигурация IIS 6.0, доступная ADSI, чтобы к новым функциям можно было обращаться, используя имеющиеся сценарии и средства.

- **Автоматическое управление версиями и ведение журнала** Журнал метабазы позволяет автоматически отслеживать записываемые на диск изменения метабазы. При записи метабазы на диск IIS задает новому файлу MetaBase.xml имя, представляющее номер версии, и сохраняет копию файла в папке журнала. Каждому файлу журнала задается уникальный номер версии, который можно использовать для отката или восстановления метабазы. По умолчанию ведение журнала метабазы включено.
- **Редактирование в процессе работы** IIS 6.0 позволяет администратору редактировать файл MetaBase.xml, когда IIS запущен. Для изменения конфигурации можно открыть Meta-

Base.xml, например в Блокноте, и ввести новые конфигурационные параметры нового узла или виртуального каталога или отредактировать имеющуюся конфигурацию.

- **Импорт и экспорт конфигурации** В **IIS** 6.0 реализовано два новых метода Admin Base Object (ABO): *Export* и *Import*. Они позволяют импортировать и экспортировать между серверами конфигурацию с узла любого уровня. Важные данные защищаются пользовательским паролем, аналогичным применяемому в новой утилите архивации/восстановления. Кроме того, данные методы доступны пользователям ADSI и WMI через IIS Manager. Методы *Export* и *Import* позволяют:
  - □ экспортировать один узел или все дерево в XML-файл с любого уровня метабазы;
  - п при необходимости экспортировать унаследованную конфигурацию;
  - а импортировать из XML-файла один узел или все дерево;
  - D защитить важные данные паролем;
  - а выполнить в процессе импорта сведение импортируемой и текущей конфигурации.
- **Резервные копии, не привязанные к серверу** **В** IIS 6.0 есть новый API-интерфейс Admin Base Object (ABO), позволяющий архивировать и восстанавливать метабазу с использованием пароля. Это позволяет создавать резервные копии, не привязанные к серверу.

  Ключ сеанса шифруется с помощью вводимого пользователем пароля и не привязан к ключу машины. Архивируя метабазу, ОС шифрует ключ сеанса с помощью указанного пользователем пароля. При восстановлении ОС с помощью пароля расшифровывает ключ сеанса и затем повторно зашифровывает его, используя текущий ключ машины.

  Новый метод восстановления позволяет восстанавливать и резервные копии, сделанные старым способом, и придерживается такого же подхода, какой использовался старым методом при невозможности расшифровки ключа сеанса. WMI и ADSI поддерживают эти методы. Существующее приложение для архивации/восстановления БД также использует новый метод резервного копирования/восстановления.

WMI-поставщик IIS

В Windows 2000 были реализованы новые средства получения доступа к важной информации, например, счетчикам производительности и системной конфигурации, — Windows Management Instrumentation (WMI). С целью использования таких возможностей WMI, как поддержка запросов и сопоставление объектов, для IIS 6.0 создан WMI-поставщик, предоставляющий множество интерфейсов программирования, позволяющих более точно и гибко администрировать Wcb-сервср. WMI-поставщик IIS предоставляет функциональность, аналогичную средствам ADSI-поставшика **IIS** для редактирования метабазы.

Назначение WMI-поставщика IIS — реализовать удобство управления IIS на уровне, функционально аналогичном уровню, обеспечиваемому ADSI-поставщиком IIS, а также реализовать поддержку расширяемой схемы. В частности, для этого требуется WMI-схема, конгруэнтная схеме метабазы IIS. И хотя в отношении соответствующих объектных моделей и моделей данных, используемых в ADSI WMI, схемы могут различаться, обе предоставляют одинаковую функциональность. Иначе говоря, *сценарий* для выполнения задачи средствами модели ADSI можно написать и с использованием модели WMI. Сценарии внесут в метабазу одинаковые изменения. Точно так же все расширения схемы, осуществляемые через ADSI, автоматически отражаются в поставщике WMI. Если средствами ADSI сделано изменение схемы, они передаются WMI-поставщику IIS,

Администрирование из командной строки

IIS 6.0 копирует в папку Windows\System32 поддерживаемые сценарии, позволяющих администрировать Web-сервер на основе IIS 6.O. Эти сценарии, написанные на Visual Basic, получают/задают значения конфигурационных параметров в метабазе с помощью WMI-поставщика IIS. Данные сценарии предназначены для выполнения большинства распространенных задач, с которыми сталкивается Web-администратор, из командной строки, не выводя пользовательский интерфейс. Вот список предоставляемых IIS 6.0 административных сценариев командной строки и выполняемых ими задач:

- **Iisweb.vbs** создание/удаление/запуск/останов/генерирование списка Web-узлов;

- **Iisftp.vbs** создание/удаление/запуск/останов/генерирование списка FTP-узлов;
- **Iisvdir.vbs** создание/удаление виртуальных каталогов, а также вывод списка виртуальных каталогов указанного корня;
- **Iisftpdr.vbs** создание/удаление/вывод списка виртуальных каталогов в указанном корне;
- **Iisconfg.vbs** экспорт/импорт конфигурации IIS в XML-файл;
- **Iisback.vbs** резервное копирование и восстановление конфигурации IIS;
- **Iisapp.vbs** вывод списка идентификаторов процессов и пулов приложений для рабочих процессов, выполняющихся в данный момент;
- **Iisext.vbs** конфигурирование расширений службы WWW.

Администрирование через Web

Утилита Remote Administration (HTML) Tool позволяет удаленно администрировать IIS через Интернет или интрасеть с помощью Web-браузера.

Новые функции, повышающие производительность

Новое поколение приложений предъявляет более высокие требования к производительности и масштабируемости Web-серверов. Повышение скорости обработки HTTP-запросов и увеличение числа приложений и узлов, обслуживаемых одним сервером означает, что для размещения узла понадобится меньше серверов.

Совет При определенной рабочей нагрузке предварительное тестирование показывает на сервере с 8 процессорами 100%-ый и более прирост производительности.

В Windows Server 2003 реализован новый драйвер режима ядра, HTTP.sys, для анализа и кэширования HTTP-пакетов. HTTP сконфигурирован для повышения пропускной способности Web-сервера и рассчитан на недопущение перехода процессора в пользовательский режим, когда система считает, что содержимое можно обработать в самом ядре. Это важно для

пользователей IIS, так как IIS 6.0 основан на HTTP.sys. Если в обработке запроса должен участвовать компонент пользовательского режима, HTTP.sys передает запрос соответствующему рабочему процессу пользовательского режима. Другие процессы пользовательского режима в выборе этого процесса не участвуют.

IIS 6.0 более тесно взаимодействует со средой обработки. Компоненты IIS пользовательского режима и режима ядра написаны так, чтобы учитывать особенности процессоров. На многопроцессорных системах это повышает степень масштабируемости сервера. Кроме того, администраторы могут привязать рабочую нагрузку, генерируемую конкретными приложениями или узлами, к конкретным процессорным подсистемам. Это значит, что приложения могут создавать виртуальные бункеры обработки приложений в одном образе ОС (рис. 8-1).

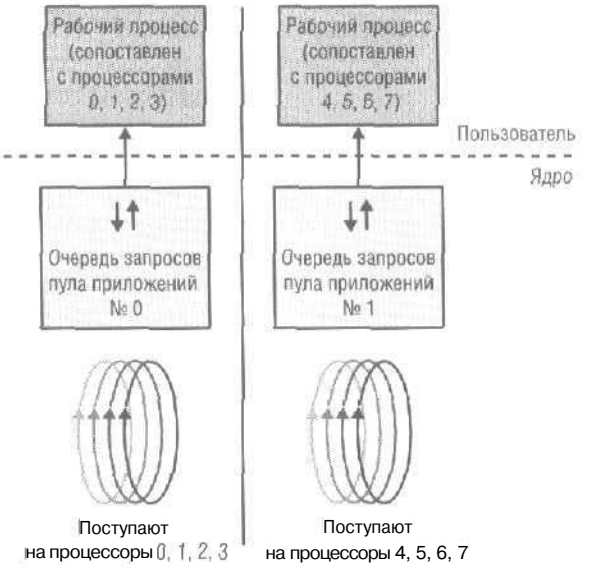


Рис. 8-1. Виртуальные бункеры обработки запросов в IIS 6.0

Новый драйвер режима ядра

Новый драйвер **режима ядра, HTTP.sys, —** единый **центр,** обслуживающий **все поступающие (серверные) HTTP-запросы. Это**

обеспечивает серверным приложениям, работающим по HTTP, эффективную и высокоскоростную связь. Драйвер выполняется поверх TCP/IP и получает от комбинаций «IP-адрес/порт», которые он сконфигурирован прослушивать, все запросы на подключение. HTTP.sys также осуществляет общее управление соединениями, регулирует полосу пропускания и ведет журнал Web-сервера.

Примечание В ходе предварительного тестирования было высказано предположение, что по сравнению с IIS 5.0 пропускная способность для статичного содержимого возрастет на 200%, а для кэшированных ответов — на 165%.

Политика кэширования

В IIS 6.0 реализован эвристический механизм для определения кэшируемого «набора первой необходимости» приложения или набора узлов. То, что некоторый объект поддерживает помещение в кэш, не значит, что есть смысл туда его помещать, так как управление этим объектом и размещение его в памяти связаны с определенными затратами. Поэтому IIS 6.0 с помощью нового эвристического механизма определяет необходимость кэширования, основываясь на распределении поступающих к узлу запросов. Это означает повышение масштабируемости Web-узла, так как ресурсы сервера используются оптимально и обеспечивается приемлемый уровень производительности при частых запросах.

Кроме того, в IIS 6.0 имеется эвристический механизм для мониторинга общего состояния сервера и приема на основе получаемых данных решений о повышении/снижении параллелизма. Так, при выполнении связанных с процессором запросов запуск параллельных заданий — не всегда лучшее решение.

Web-сады

Web-сад — это пул приложений, в котором передаваемые ему запросы обрабатывают несколько процессов. В многопроцессорной системе рабочие процессы в Web-саду можно связать с определенной группой процессоров. Используя Web-сады, Web-приложения повышают свой уровень масштабируемости,

так как программная блокировка в одном процессе не мешает обработке остальных запросов, передаваемых приложению. Если Web-сад включает четыре процесса, блокировка конкретной программы помешает обработке примерно четверть запросов.

Кэш ASP-шаблонов

В IIS 5.0, прежде чем ASP-код будет выполнен, ядро ASP компилирует ASP-файл в ASP-шаблон. Такие шаблоны хранятся в памяти процесса. Если узел включает массу ASP-страниц, из памяти удаляются наиболее старые шаблоны, чтобы освободить место для новых. В ITS 6.0 удаляемые шаблоны сохраняются на диске. Если один из этих ASP-файлов будет запрошен снова, ядро ASP загружает шаблон, вместо того чтобы загружать файл и тратить время процессора на повторную его компиляцию.

Примечание В ходе предварительного тестирования было высказано предположение о 50%-ом повышении пропускной способности вследствие записи удаляемых из кэша шаблонов на диск.

Поддержка ОЗУ большого объема

Если требуется большой объем кэшированных данных, ITS 6.0, установленный на системе с процессором x86, можно сконфигурировать для кэширования до 64 Гб информации.

Масштабируемость узлов

В IIS 6.0 усовершенствован **способ использования внутренних** ресурсов. **IIS** 6.0 **выделяет** системные ресурсы по мере того, **как HTTP-запросы запрашивают их, а не** осуществляет предварительное выделение ресурсов **в период инициализации. В результате этого можно:**

- на одном IIS 6.0-сервере разместить гораздо больше узлов;
- параллельно выполнять больше рабочих процессов;
- быстрее запускать/завершать работу сервера, на котором размещены Web-узлы.

Предварительное тестирование показывает, что под управлением IIS 6.0 может выполняться на порядок больше группо-

вых приложений, чем под управлением IIS 5.O. В IIS 6.0 можно сконфигурировать тысячи изолированных приложений, которые будут выполняться в собственном контексте безопасности, конкретное число зависит от системных ресурсов. Если приложения сконфигурированы для выполнения в совместном пуле приложений, на одном сервере под управлением IIS 6.0 их можно легко разместить десятки тысяч.

Примечание Предварительное тестирование показало, что запуск 20 000 узлов на сервере с 2 процессорами требует менее 2 минут,

В новой архитектуре IIS 6.0 есть еще одно усовершенствование масштабируемости: IIS может прослушивать запросы множества узлов, не запуская рабочих процессов (см. выше раздел «Новая архитектура обработки запросов»). Совместное применение данной функции запуска по запросу и намеренного перевода рабочих процессов в режим простоя означает, что Web-сервер, на котором размещается множество узлов, можно масштабировать и дальше. Это обусловлено тем, что IIS 6.0 подстраивает использование ресурсов под действительно активные узлы. Кроме того, IIS 6.0 динамически удаляет из кэша элементы, связанные с неактивными узлами.

Новые возможности программирования

ITS 6.0 продолжает развивать модель программирования ISAPI и предоставляет такие новые возможности, как:

- интеграция ASF.NET и IIS;
- внутреннее перенаправление (функция *ExecuteURL* и глобальные перехватчики);
- передача буферов и описателей (функция *VectorSend*);
- кэширование динамического содержимого;
- реализованная в ISAPI поддержка нестандартных ошибок;
- многократное использование рабочего процесса;
- усовершенствованная поддержка Unicode в ISAPI;
- службы COM+ **в ASP.**

ASP.NET

Интегрируя ASP.NET и IIS, Windows Server 2003 расширяет возможности разработчиков. Основанные на TIS 6.0 усовершенствования платформы предоставляют разработчикам высокий уровень функциональности, например, быструю разработку приложений и широкий выбор языков программирования. Усовершенствованная интеграция модели процессов в IIS 6.0 расширяет возможности применения ASP.NET и .NET Framework. Кроме того, IIS 6.0 предоставляет поддержку новейших Web-стандартов, включая **XML,** SOAP и IPv6.

Функция ExecuteURL

Функция поддержки сервера *HSE_REQ_EXEC_URL*позволяет расширению ISAPI легко перенаправить запрос на другой URL. Эта функция — ответ на потребность разработчиков расширений ISAPI объединять запросы в цепочку,

Функция *ExecuteURL* предоставляет функциональность для замены практически всех фильтров чтения неструктурированных данных. Самая распространенная причина для создания фильтра чтения неструктурированных данных — необходимость просмотреть или изменить тело запроса до того, как оно будет обработано конечным URL. В настоящий момент единственный способ просмотреть тело запроса (если вы не являетесь конечным URL) — задействовать уведомления о чтении неструктурированных данных. К сожалению. создать реализующий это фильтр ISAPI, чрезвычайно трудно, а в некоторых конфигурациях и невозможно,

С другой стороны, расширения ISAPI предоставляют функциональность для простого получения и управления телом запроса. *ExecuteURL* позволяет расширению ISAPI обработать тело запроса и передать его дочернему запросу, что соответствует потребностям практически всех разработчиков фильтров для чтения неструктурированных данных.

Глобальные перехватчики

Функция *ExecuteURL* позволяет IIS 6.0 реализовать перехватчики запросов ISAPI, способные перехватывать, изменять, перенаправлять или отклонять все входящие HTTP-запросы к конкретному пространству URL.

- IIS 5.0 уже поддерживает одно расширение ISAPI, перехватывающее все запросы с использованием карты сценария, состоящей из одного символа шаблона (*). Сконфигурировать это расширение можно на вкладке Application mappings диалогового окна свойств приложения.
- В IIS 6.0 концепция карты сценария, состоящей из одного символа шаблона (*), расширена и позволяет выполнять глобальные перехватчики многократно.

Ранее прием всех запросов к конкретному URL можно было реализовать только с помощью фильтров ISAPI. Однако с последними связаны определенные проблемы. Они действуют глобально, на уровне Web-узла. Они не могут обрабатывать длительные операции (например, запросы к БД), не «подвешивая» пул потоков IIS. Они не могут обращаться к телу запроса. Будучи расширениями ISAPJ, у глобальных перехватчиков нет ограничений, накладываемых на фильтры ISAPI, и совместно с функцией *ExecuteURL* они предоставляют функциональность, позволяющую заменить практически все фильтры чтения неструктурированных данных.

Функция VectorSend

Сегодня при наличии множества буферов, формирующих ответ, у разработчиков ISAPI есть только два варианта; многократно вызывать функцию *WriteClient* или объединить ответ в один большой буфер.

- Первый способ создает узкое место производительности, поскольку для каждого буфера один раз осуществляется переход в режим ядра.
- Второй способ также негативно влияет на производительность и требует дополнительной памяти.

Решение этой проблемы — *VectorSend* в IIS 6.0. Реализованная как серверная функция поддержки для ISAPI, *VectorSend* позволяет разработчикам создать список пересылаемых буферов и описателей файлов с указанием их порядка и затем передать его IIS 6.0 для генерации конечного ответа. HTTP.sys компилирует в ядре все буферы и описатели файлов в один буфер ответа, а затем пересылает его. При этом ISAPI не нужно создавать буфер или вызывать *WriteClient*.

Кэширование динамического содержимого

Еще одна новая функция — реализация кэша режима ядра, предназначенного для хранения динамического содержимого, Ее преимущество в том, что многие клиенты программно создают неизменяемое содержимое.

В предыдущих версиях IIS для каждого динамического запроса приходилось осуществлять переход из режима ядра в пользовательский режим, а также генерировать ответы. Исключив такой переход и реализовав выборку кэшированного содержимого из кэша режима ядра, Microsoft обеспечила заметный прирост производительности.

Функция ReportUnhealthy

Новая функция поддержки сервера — *HSE_REQ_REPORT_UNHEALTHY*— позволяет расширению TSAPI обратиться к рабочему процессу 1IS 6.0 и сообщить, что данный процесс нужно использовать повторно. Разработчикам эта новая функция позволяет сообщать о необходимости повторного использования процесса, если приложение ISAPI начинает нестабильно работать или почему-либо переходит в неизвестное состояние.

Примечание Чтобы IIS мог повторно использовать процесс после того, как ISAPI вызовет функцию HSE REQ_REPORT_UNHEALTHY, надо включить мониторинг состояния.

Вызывая *HSE_REQ_REPORT_UNHEALTHY* разработчик может также передать строку с указанием причины, по которой ISAPI вызывает данную функцию. Эта строка добавляется к записи о событии, заносимой рабочим процессом в журнал событий Application.

Нестандартные ошибки

Разработчикам, использующим ISAPI, больше не требуется генерировать собственные сообщения об ошибках. Вместо этого они могут задействовать встроенную в IIS поддержку нестандартных ошибок, представленную новой функцией поддержки сервера *HSE_REQ_SEND_CUSTOM_ERROR*.

ISAPI-интерфейс Unicode

Структура протокола HTTP не рассчитана на поддержку Unicode, и поэтому IIS 5.0 вынуждает разработчика прибегать к системным кодовым страницам. При использовании URL в кодировке UTF-8 становится возможным применять Unicode. ITS 6.0 представляет клиентам серверные переменные в кодировке Unicode и включает две новых функции поддержки сервера, позволяющие разработчикам получать Unicode-представление URL.

Службы COM+ в ASP-приложениях

В IIS 4.0 и 5.0 ASP-приложения могут использовать службы COM+. Для этого нужно сконфигурировать в хранилище конфигурации COM+ объект Web Application Manager (WAM), соответствующий приложению, для применения набора служб. Это обусловлено тем, что службы COM+ разрабатывались для совместного использования с COM-компонентами. В IIS 6.0 команды TIS и COM+ отделили службы COM+ от компонентов и предоставили ASP-приложениям возможность задействовать набор служб COM+.

К службам COM+, доступным в Windows 2000, добавлена служба *Fusion,* поддерживаемая в ASP. Она позволяет ASP-приложению задействовать конкретную версию системной DLL периода выполнения или классического COM-компонента. *Fusion* позволяет разработчику приложения указать конкретные версии системных библиотек периода выполнения и классических COM-компонентов, применяемых в приложении. После загрузки и запуска приложение получит именно эти версии библиотек и компонентов, Раньше приложениям приходилось обращаться к той версии системной библиотеки периода выполнения, которая была установлена в системе. В случае установки новых версий библиотеки с несколько измененной функциональностью вынужденное использование имеющейся версии могло создавать проблемы.

Вот дополнительные усовершенствования COM+.

- Разделы COM+ позволяют администратору определить разную конфигурацию одного и того же COM+-приложения для разных пользователей. Конфигурация включает в

себя информацию о безопасности и управлении версиями. Подробнее о разделах COM+ см. документацию COM+.

- Система слежения COM+, когда она включена, позволяет администраторам наблюдать, какой код и когда выполняется в контексте ASP-сеанса. Эти сведения весьма полезны при отладке ASP-приложений. Подробнее о системе слежения COM+ см. документацию COM+.
- ASP при помощи COM+ позволяет разработчикам определять, какая модель управления потоками используется при выполнении страниц приложения. По умолчанию применяется модель Single Threaded Apartment. И все же приложение, использующее объекты *с* поддержкой добавления в пул, можно выполнять с применением модели Multi-Threaded Apartment.

Усовершенствования платформы

В IIS 6.0 реализованы некоторые общие усовершенствования платформы, которые делают IIS все более привлекательной платформой для Web-приложений.

Поддержка 64-битных платформ

Код всех ОС семейства Windows Server 2003 работает на 32- и 64-битных платформах. Клиенты, которым необходимы приложения с повышенной степенью масштабируемости, могут воспользоваться ОС, которая выполняется и поддерживается обеими этими платформами.

Поддержка протокола IPv6.Q

Протокол Интернета версии 6.0 (IPv6.0) предназначен для обмена информацией по Интернету. В Windows Server 2003 реализован готовый для использования в производственной среде стек IPv6.0. На серверах, где данный стек установлен, ITS 6.0 автоматически поддерживает обработку HTTP-запросов, поступающих по протоколу IPv6.0.

Усовершенствованное управление сжатием

В перегруженной сети ответы протоколов рекомендуется сжимать. В IIS 5.0 за такое сжатие отвечал фильтр ISAPI, рабо-

тавший только на уровне сервера. IIS 6.0 позволяет конфигурировать параметры сжатия более точно — на уровне файлов.

Механизм Quality of service

Механизм Quality of service (QoS, качество обслуживания) гарантирует, что конкретные компоненты Web-сервера или обслуживаемое данным сервером содержимое не займут все ресурсы сервера, скажем, память и процессор. Данный механизм позволяет администратору управлять ресурсами, используемым конкретными узлами, пулами приложений, службой WWW в целом и т. д. Кроме того, QoS гарантирует службам, узлам и выполняющимся в системе приложениям определенный уровень обслуживания, ограничивая ресурсы, к которым обращаются конкретные Web-узлы и приложения или вообще служба WWW. В IIS 6.0 механизм QoS включает следующие компоненты;

- ограничение числа соединений;
- тайм-ауты соединений;
- управление размером очереди пула приложений;
- регулирование полосы пропускания;
- учет процессов;
- утилизация памяти.

Усовершенствованное ведение журнала

В IIS 6.0 усовершенствовано ведение журнала.

- **Ведение журнала в кодировке UTF-8** Поддержка кодировок Unicode и UTF-8 позволяет IIS 6.0 вести файлы журнала не только в формате ASCII (или локальной кодовой страницы), но и в формате UTF-8.
- **Двоичный формат ведения журнала** Позволяет нескольким узлам записывать данные в один файл журнала в двоичном представлении и без форматирования. Новый формат обеспечивает более высокую производительность, чем существующие текстовые форматы — World Wide Web Consortium (W3C), IIS и National Center for Supercomputing Applications (NCSA), поскольку данные не надо форматировать.

  Кроме того, двоичный формат обеспечивает преимущества в плане масштабируемости, так как уменьшается число буферов файлов журнала, необходимых при ведении жур-

налов для десятков тысяч узлов. Затем с помощью специальных утилит можно обрабатывать файл журнала и извлекать нужные записи. Для обработки двоичных файлов журнала можно даже написать собственные утилиты, поскольку формат файла и записей журнала будет скоро опубликован.

IIS 6.0 также может регистрировать коды состояния HTTP в журнале формата W3C или двоичного формата. Коды состояния полезны при отладке и устранении проблем, поскольку для ошибок определенного типа IIS возвращает определенные коды состояния. Так, если нельзя обработать запрос, поскольку нужное приложение отключено (например, на чистых установках по умолчанию не отключен ASP), система вернет клиенту стандартный код ошибки 404. На самом же деле IIS генерирует код 404.2, регистрируемый в файлах журнала формата W3C и двоичного формата.

Протокол FTP

Клиенты провайдеров Интернета и прикладных служб обычно загружают Web-содержимое по протоколу FTP. так как он широко распространен. IIS 6.0 позволяет изолировать действия пользователя областью отдельного каталога, тем самым предотвращая просмотр или перезапись Web-содержимого посторонними лицами. Выделенный пользователю каталог верхнего уровня отображается как корневой каталог службы FTP, что ограничивает доступ и не дает пользователям перемещаться вверх по дереву каталогов. В пределах собственного узла пользователь может создавать, изменять и удалять папки/файлы. Реализация FTP распределяется между произвольным числом клиентских и серверных систем, что повышает надежность и доступность. Службу FTP легко масштабировать, добавляя виртуальные каталоги и серверы и не затрагивая при этом конечных пользователей.

Для PASV FTP серверу нужно открыть порт данных, с которым клиент установит второе соединение. Оно обособлено от обычного соединения через порт 21, используемый управляющим каналом FTP. В IIS 6.0 можно конфигурировать диапазон портов, применяемых для PASV-соединений. Это позволяет понизить степень уязвимости FTP-серверов под управле-

нием IIS 6.0, так как администраторы теперь могут управлять диапазоном портов, к которым возможно подключение из Интернета.

Усовершенствованное управление программными заплатами

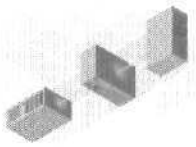
В Windows Server 2003 усовершенствовано управление программнымизаплатами.

- **При установке программных заплат работа служб не прерывается** В архитектуре 1IS 6.0 реализовано многократное использование рабочего процесса, т. е. администратор может легко установить большинство «горячих» исправлений IIS и большинство новых DLL рабочего процесса, не останавливая работу служб.
- **Auto Update** Средство Auto Update версии 1.0 позволяет:
  - а извещать о наличии заплаты, когда та становится доступна;
  - □ загружать программную заплату;
  - а установить программную заплату в соответствии с расписанием, определенным администратором.
- **Корпоративная редакция сервера Windows Update** Многие ИТ-отделы не позволяют пользователям устанавливать программные заплаты для системы безопасности и другие пакеты Windows Update, пока они не пройдут тестирование в стандартной рабочей среде. Теперь Windows Update предоставляет возможность проводить для программных заплат тесты проверки качества. Протестированную заплату можно разместить на защищенном брандмауэром корпоративном сервере Windows Update, с которого все находящиеся за этим же брандмауэром пользователи смогут ее установить.
- **DLL-библиотеки без ресурсов** В новом семействе ОС Windows ресурсы для локализации и фактическая реализация разделены. Это позволяет Microsoft быстро выпускать исправления на 30 языках.

Дополнительные сведения

Дополнительные сведения см. по следующим адрксам:

- новые возможности Internet Information Services 6.0 — *http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/iis.mspx*;
- новые возможности Security - *http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/security.mspx*;
- технический обзор Security — *http://www.microsoft.com/windowsserver2003/techinfo/overview/security.mspx*;
- обзор «.NET» в семействе ОС Windows .NET Server — *http://www.microsoft.com/windowsserver2003/evaluation/overview/dotnet/dotnet.mspx*;
- Web-сервисы и службы приложений Windows 2000 — *http://www.microsoft.com/windows2000/technologies/web/*.



ГЛАВА
9

Службы приложений

Семейство Windows Server 2003 обладает всеми качествами, которые традиционно относят к сильным сторонам Windows: безопасностью, управляемостью, надежностью, доступностью и масштабируемостью. Внесенные в Windows Server 2003 усовершенствования дают целый ряд преимуществ при разработке приложений, снижая их совокупную стоимость владения (total cost of ownership, TCO) и повышал производительность:

- **упрошенная интеграция и возможности взаимодействия** позволяют легко устанавливать соединения с системами партнеров и клиентов, защищать и расширять инфраструктуру, а также создавать динамические приложения;
- **повышение производительности труда разработчика** обеспечивает более быстрый выпуск ПО на рынок и внедрение ускоренных и упрощенных циклов разработки;
- **улучшенная корпоративная функциональность** гарантирует удовлетворение потребностей клиентов при минимальной TCO решений, а также высокую производительность труда при минимальных затратах кадровых ресурсов.

Эта глава посвящена возможностям служб приложений Windows Server 2003.

Упрошенная интеграция и возможности взаимодействия

Составляя основу .NET-технологий, Windows Server 2003 предоставляет окружение для приложений, которое позволяет

создавать, развертывать и исполнять Web-сервисы XML. Благодаря интегрированной поддержке Web-сервисов XML приложениямдоступныпреимуществаслабосвязанныхвычислений с обменом данными через Интернет.

- **Встроенная поддержка Web-сервисов XML** Windows Server 2003 предлагает встроенную поддержку стандартов, на которых базируются Web-сервисы XML: SOAP, Universal Description, Discovery and Integration (UDDI) и Web Services Description Language (WSDL).
- **Enterprise UDDI** Windows Server 2003 включает службы Enterprise UDDI — динамическую и гибкую инфраструктуру Web-сервисов XML. Эти службы позволяют компаниям организовывать внутренние UDDI-репозитарии, доступные из экстра- и интрасетей. В таком репозитарии разработчики смогут найти любые Web-сервисы, доступные в сети организации, что способствует их повторному использованию. ИТ-администраторы смогут каталогизировать программируемые сетевые ресурсы и управлять ими. UDDI-службы дают организациям возможность создавать и развертывать более интеллектуальные и надежные приложения.
- **Поддержка служб** Тесная интеграция Web-сервисов XML с Windows Server 2003 открывает доступ к их возможностям таким службам, как COM+ и Microsoft Message Queuing (MSMQ). Пометив один флажок, администраторы смогут разрешить приложениям COM+ вызывать Web-сервисы XML через XML/SOAP; MSMQ сможет взаимодействовать с SOAP и XML в «родном» формате, обеспечивая взаимодействие слабосвязанных приложений с широким спектром систем,
- **Инфраструктура федерации (federation infrastructure)** Web-сервисы XML формируют архитектурную основу для интеграции приложений, а фундаментальная задача инфраструктуры федерации — обеспечение взаимодействия серверов и служб через границы областей, в которых действуют доверительные отношения.

Повышение производительности труда разработчика

Прикладное окружение Windows Server 2003 способствует повышению эффективности работы программиста.

- **Инфраструктура .NET Framework** включает CLR и унифицированный набор библиотек классов, таких как Windows Forms, Microsoft ADO.NET и Microsoft ASP.NET.

  .NET Framework предоставляет полностью управляемую, защищенную среду приложений, упрощающую создание и развертывание программ и бесшовно интегрируемую с разными языками программирования. Интеграция .NET Framework со средой разработки приложений Windows Server 2003 избавила программистов от написания сопрягающего кода, позволив сосредоточиться на бизнес-задачах.

  Инфраструктура .NET Framework, поддерживаемая большинством ОС семейства Windows (Windows XP/2000 Server/Professional/98/Me/NT 4), позволяет создавать Web-приложения с применением ASP.NET и других технологий, а также облегчает проектирование и реализацию приложений, над которыми идет работа в настоящее время. Низкоуровневые механизмы .NET Framework обеспечивают межъязыковое взаимодействие, что позволяет расширять программы, написанные на одном языке, с помощью компонентов, созданных с применением других языков, посредством межъязыкового наследования, отладки и обработки ошибок.

  Windows Server 2003 предоставляет самый богатый набор служб среди существующих платформ разработки, включая всеобъемлющие возможности доступа к данным, встроенные средства обеспечения безопасности, интерактивные пользовательские интерфейсы, продуманную объектную модель, мониторы обработки транзакций и службы очередей мирового класса.
- **ASP.NET: простое создание Web-сервисов** Поддержка Web-сервисов **XML** в **ASP.NET** позволяет сосредоточиться на создании бизнес-логики, а обеспечение доступности этих сервисов через SOAP и другие открытые протоколы инфраструктура ASP.NET берет на себя.
- **Изоляция кода от информационного наполнения** в инфраструктуре .NET Framework позволяет плодотворно сотрудничать разработчикам и авторам содержимого.
- **Встроенные инструменты** Visual Studio .NET позволяют создавать Web-приложения и Web-сервисы XML, поддерживающие несколько языков программирования.

- **Возможность многократного использования кода** обеспечивается простой в освоении интеллектуальной архитектурой ASP.NET.
- **Автоматическое управление памятью** обеспечивается тем, что .NET Framework работает внутри CLR — окружения, использующего сбор мусора, который освобождает приложение, построенное с применением .NET-объектов, от явного уничтожения таких объектов, что снижает частоту распространенных ошибок программирования.
- **Серверные Web-элементы управления** повышают продуктивность, инкапсулируя сложные операции внутри серверных компонентов. Это позволяет разработчикам создавать масштабируемые Web-приложения, способные обслуживать множество пользователей. Web-элементы управления компилируются и работают на сервере, что обеспечивает им максимальную производительность, поддержку наследования и дальнейшее расширение их возможностей.

Улучшенная корпоративная функциональность

Приложения, созданные в среде Windows Server 2003, характеризуются меньшим временем реакции и более высокой доступностью по сравнению с приложениями из прежних версий Windows. Теперь для управления окружением требуется меньше людей, что снижает TCO и повышает производительность, а также повышает масштабируемость, надежность и устойчивость защиты приложений. Windows Server 2003 также освобождает ИТ-администраторов от рутинных задач, облегчая развертывание и управление приложениями.

- **ASP.NET: интеграция с Internet Information Services (IIS) 6.0** ASP.NET интегрирована с моделью процессов IIS 6.0 и способна исполнять несколько приложений в одном процессе. Таким образом, приложения ASP.NET могут быть изолированы и напрямую взаимодействовать со слушателем HTTP, работающим в режиме ядра. Это снижает издержки на обслуживание процессов и позволяет приложениям ASP.NET использовать службы кэширования файлов режима ядра.
- **ASP.NET: дополнительные возможности при компиляции** Механизм компиляции в .NET Framework заменяет интерпретируемые страницы компилируемыми. Поддерживается

как предварительная компиляция, так и компиляция на лету (по запросу). ASP.NET использует более совершенную модель потоков, поддерживающую асинхронный ввод-вывод, повышающую масштабируемость и производительность приложений. Это позволяет избежать преобразования серверного кода перед его исполнением, экономя серверные ресурсы и увеличивая масштабируемость и производительность сервера.

- **ASP.NET: интеллектуальное кэширование** Модель программирования ASP.NET поддерживает функции API кэша, позволяющие активизировать службы кэширования, таким образом повышая производительность. В кэш вывода (output cache) записываются полностью сформированные, а в кэш фрагментов (fragment cache) — частично сформированные страницы. Кроме того, поддерживаются классы, позволяющие приложениям, HTTP-модулям и обработчикам запросов записывать в кэш любые объекты по мере необходимости.
- **Сбор мусора** Сборщик мусора, встроенный в CLR, обеспечивает эффективное управление памятью, оптимизированное для Web-сервера, и устраняет проблемы, связанные с фрагментацией кучи, применяя классическую модель выделения-освобождения памяти.

Повышенная масштабируемость и надежность

Разработчикам будут полезны возможности, обеспечивающие высокую масштабирумость и надежность прикладного окружения.

- **Поддержка асинхронных операций** В .NET Framework тесно интегрированы две технологии асинхронного взаимодействия, обеспечивающие масштабируемость и надежность: SOAP и MSMQ. Они позволяют создавать устойчивые приложения, способные работать в автономном режиме.
- **Сохранение состояния сеансов в Web-фермах** Механизмы сохранения состояния сеансов, поддерживающие Web-фермы, сохраняют сеансовые сведения о состоянии во внешнем по отношению к Web-приложению процессе, делая их устойчивыми к краху приложения и доступными другим компьютерам Web-фермы.
- **Отказоустойчивые процессы IIS 6.0** Архитектура IIS 6.0 предоставляет дополнительные возможности по изоляции

приложений. Администраторы вправе создавать пулы приложений и изолировать с их помощью приложения, распределяя их по разным пулам. Поддержка автоматического мониторинга и рециклизации пулов приложений обеспечивает доступность приложений.

- **ADO.NET** Использует временные подключения и интеллектуальную обработку данных о состоянии. При обмене XML-сообщениями между приложениями и источником данных в ADO.NET соединение открывается и закрывается по мере надобности. В результате приложения, использующие ADO.NET, лучше масштабируются, а ADO.NET работает через любые виды сетевого транспорта.

Эффективное развертывание и управление

Ряд инструментов, и улучшенных (службы Windows Installer), и новых (например Fusion), обеспечивает развертывание приложений в автоматическом режиме. Fusion поддерживает управление версиями DLL, позволяя одновременно использовать несколько версий одной библиотеки. Другой компонент Fusion — декларация (manifest) — позволяет получить точный список DLL, необходимых приложению. Декларации Fusion можно включать в Windows Installer как средство описания библиотек, нужных приложению. Это позволяет сосуществовать приложениям, требующим разные версии одних и тех же библиотек, повышая надежность приложений после развертывания.

Дополнительные инструменты ускоряют развертывание и увеличивают его точность с помощью Xcopy и редактирования параметров US «на лету».

Windows Management Instrumentation (WMI) и новые инструменты из Visual Studio .NET позволяют за считанные часы сделать то, что раньше занимало несколько дней. Надежность приложений также повышается путем применения инструментов командной строки, бесплатно загружаемых из Интернета. Теперь легко генерировать события и определять переменные в приложениях и сервисах.

Безопасность от и до

Система безопасности Windows Server 2003 построена наверху единой модели защиты, основанной на Active Directory. Усовершенствования и новшества системы безопасности в Windows Server 2003 делают ее менее уязвимой и увеличивают возможности механизмов аутентификации и авторизации Windows посредством новой архитектуры защиты приложений. Смена протокола (protocol transition) в дополнение к любому методу аутентификации, используемого внешним Web-сервером (front-end Web server), позволяет выполнять встроенную аутентификацию Kerberos.

Встроенная поддержка службы .NET Passport обеспечивает аутентификацию и авторизацию любых клиентов или потребителей, формируя фундамент для новых возможностей по консолидации серверов. Если внешний сервер доверяет службе Passport, то для проверки подлинности пользователя с его входа в систему можно применять паспорт .NET. Удостоверения .NET Passport также можно сверять со сведениями о клиентах, хранимыми в Active Directory.

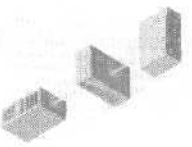
Дополнительные сведения

Дополнительную информацию к этой главе см. по адресам:

- Developing Applications for Windows Server 2003 — http://www.microsoft.com/windowsserver2003/developers/;
- Windows 2000 Web and Application Services — http://www.microsoft.com/windows2000/technologies/web/;
- Introducing the «.NET» in the Windows Server 2003 Family - http://www.microsoft.com/windowsserver2003/evaluation/overview/dotnet/dotnet.mspx.

ГЛАВА

10



Службы Windows Media

Службы Windows Media 9 (Windows Media Services 9 Series) — это серверный компонент платформы Windows Media 9, который вместе с Windows Media Encoder и Windows Media Player обеспечивает доставку аудио- и видеоданных клиентам через Интернет и интрасети. Клиентами могут быть компьютеры и иные устройства, воспроизводящие полученные данные через программу-проигрыватель вроде Windows Media Player. В роли клиентов могут выступать и другие компьютеры, на которых работают службы Windows Media (такие компьютеры называются *серверами Windows Media),* Эти компьютеры выполняют функции прокси-серверов, кэшируют данные и обеспечивают распространение мультимедийного содержимого. Клиентами также могут быть пользовательские приложения, разработанные с применением пакета Windows Media SDK.

Windows Media Services способны передавать потоки данных, формируемых в реальном времени (live stream), и данных, хранимых на сервере, таких как оцифрованные видео- и аудиоданные. Для трансляции мультимедийных потоков, формируемых в реальном времени (в режиме «прямого эфира») потребуется сконфигурировать пункт публикации широковещанием (broadcast publishing point) и подключить к нему программу (вроде Windows Media Encoder), сжимающую потоковые данные в реальном времени и преобразующую их в один из поддерживаемых сервером форматов. Для потоковой передачи пригодны и файлы, заранее созданные с помощью Windows Media Encoder, Microsoft Producer для PowerPoint 2002, Windows Movie

Maker, Windows Media Player либо кодирующей программы от стороннего производителя. Такие потоки транслируют через пункты публикации по запросу (on-demand publishing points). Примеры пунктов публикации обоих типов предоставляются по умолчанию.

В этой главе вы познакомитесь со службами Windows Media 9, имеющимися в Windows Server 2003, с Fast Streaming, динамической доставкой содержимого и др.

Fast Streaming

Fast Streaming, компонент Windows Media Services, базируется на новейших технологиях и способен доставлять потоковые аудио- и видеоданные через сети различных типов, включая ненадежные. Преимущества Fast Streaming обеспечивают:

- Fast Start;
- Fast Cache;
- Fast Recovery;
- Fast Reconnect,

Fast Start

Обеспечивает немедленный запуск воспроизведения без задержки из-за заполнения буфера, при этом характер воспроизведения данных не имеет значения: пользователь может просматривать длительный непрерывный фрагмент, либо переключаться между запрошенными им клипами или широковещательными каналами.

Перед воспроизведением Windows Media Player должен записать часть данных в буфер. При передаче потока данных клиенту, использующему Windows Media Player для Windows XP или более высокой версии, Fast Start записывает первую порцию данных прямо в буфер проигрывателя. При этом данные передаются с большей скоростью, чем нужно для воспроизведения. Это позволяет клиенту быстрее принять данные. Когда начинается воспроизведение, широковещательные и запрошенные потоки продолжат доставку данных в буфер со скоростью, обусловленной форматом записи.

Fast Start обеспечивает более высокое качество воспроизведения, позволяя клиентам «прокручивать» запись вперед и назад без задержек, вызванных обновлением буфера. Проиг-

рыватели, подключаемые к сети через широкополосные каналы, начинают воспроизведение еще быстрее, приближаясь по времени реакции к теле- и радиотрансляциям. При проигрывании мультимедийного содержимого с сервера по серверному списку воспроизведения (server-side playlist) переход между элементами списка происходит плавно, без длительных пауз. Буферизация защищает проигрыватель от ошибок воспроизведения, возникающих из-за потери пакетов и других проблем в сети,

Fast Cache

Обеспечивает непрерывное воспроизведение путем передачи потока данных прямо в кэш Windows Media Player на предельной скорости, возможной в данной сети. Это снижает вероятность перебоев воспроизведения из-за проблем с сетью.

Так, Fast Cache позволяет серверу передавать поток с битрейтом в 128 Кбит/с на скорости 700 Кбит/с, а Windows Media Player воспроизводит этот поток с обычной скоростью (128 Кбит/с). Так что клиент может поместить в буфер гораздо больше данных перед началом воспроизведения, что позволяет справиться с колебаниями пропускной способности сетевого канала без ощутимых последствий для качества воспроизведения любого вида содержимого — как широковещательного, так и предоставленного по требованию. Это удобно, когда:

- ширина доступной клиенту полосы пропускания больше необходимой для воспроизведения текущего типа содержимого (скажем, если клиент подключается через кабельный модем, DSL-подключение или корпоративную интрасеть);
- сетевое подключение неустойчиво или характеризуется большой задержкой, как в беспроводных сетях;
- решающее значение имеет качество воспроизведения (например, в случае платных видеоканалов).

Fast Recovery

Совместно с технологией Forward Error Correction (FEC) Fast Recovery передает клиентам, подключенным через беспроводные каналы, избыточные пакеты. Это позволяет избежать потери данных при разрыве связи в момент передачи. FEC позволяет Windows Media Player восстанавливать потерянные или

поврежденные пакеты, не запрашивая у сервера Windows Media их повторной передачи.

В окружении, подверженном большим задержкам, скажем, в сетях на основе спутниковых и других беспроводных каналов, эти технологии заметно повышают эффективность приема данных. Объем информации, необходимой для исправления ошибок и передаваемой с каждым фрагментом данных, легко задать через интерфейс Windows Media Services.

Fast Reconnect

Автоматически восстанавливает соединения (как широковещательные, так и установленные по запросу), разорванные при передаче данных от проигрывателя к серверу или обратно, обеспечивая непрерывное воспроизведение.

Если клиент был подключен к пункту публикации по запросу, воспроизведение продолжится с момента, на котором соединение прервалось, восстановив синхронизацию с потоком. Если воспроизводились видеоданные, клиент попытается найти кадр, на котором остановилось воспроизведение (в индексированных данных нужный кадр найти проще). Если же клиент был подключен к широковещательной точке публикации, он продолжит прием с текущего места, при этом в воспроизведении возможны перебои.

Fast Reconnect доступен клиентам, подключающимся по любому из протоколов, поддерживаемых по умолчанию: Microsoft Media Server (MMS), Hypertext Transfer Protocol (HTTP) и Real Time Streaming Protocol (RTSP). Клиенты могут применять Fast Reconnect как при приеме широковещательных потоковых передач, так и данных, предоставляемых по запросу.

Динамическая доставка содержимого

Службы Windows Media 9 позволяют управлять распространением содержимого, используя серверные списки воспроизведения и механизмы демонстрации рекламных материалов. Это гарантирует своевременную доставку содержимого по назначению и позволяет объединять серверы при помощи новейших протоколов и механизмов кэширования/замещения.

Серверные списки воспроизведения

Серверные списки воспроизведения в Windows Media основаны на стандарте Synchronized Multimedia Integration Language (SMIL) 2.0. Это устойчивый к ошибкам механизм упорядочивания содержимого, предназначенного для воспроизведения на ПК и портативных устройствах. И широковещательные пункты публикации, и пункты публикации по запросу позволяют контролировать серверные списки воспроизведения. В такой список можно включать как готовые материалы, так и данные, формируемые в реальном времени (live content), и доставлять их путем одно- или многоадресной передачи.

Службы Windows Media в полном объеме поддерживают управление списками воспроизведения посредством бизнес-правил и корпоративной политики, а также совместимы с правилами Recording Industry Association Association of America (RIAA) и Digital Millennium Copyright Act (DMCA).

Возможности серверных списков воспроизведения таковы;

- потоковая передача содержимого на устройства, не поддерживающие серверные списки воспроизведения, такие как карманные компьютеры и телеприставки;
- вставка в трансляции рекламы, информации от спонсора и элементов стилевого оформления сайта;
- прерывание передач для рекламы или экстренных сообщений;
- динамическая демонстрация рекламы при каждом проходе по списку воспроизведения с помощью сценариев ASP и CGI;
- переключение между хранимыми и оперативно формируемыми потоками без перебоев воспроизведения на стороне клиента;
- динамическая смена и сохранение списков воспроизведения, а также генерация их «на лету» на основе профиля или личных параметров пользователя;
- потоковая передача содержимого, сгенерированного такими источниками, как Windows Media Encoder и не только;
- создание вложенных списков воспроизведения.

Отображение рекламы

Потоковая передача рекламной информации — прекрасный способ повышения рентабельности Web-сайта. Службы Windows

Media способны интегрироваться с серверами рекламы сторонних компаний, что позволяет им:

- произвольно размещать рекламные материалы в списке воспроизведения;
- динамически изменять состав рекламных материалов в зависимости от страны, региональных стандартов, демографических и иных особенностей целевой аудитории;
- персонифицировать рекламу при помощи данных, полученных из cookie-файлов и собранных иными способами;
- накладывать рекламные материалы на трансляцию согласно требованиям, предъявляемым организацией American Federation of Television and Radio Artists (AFTRA);
- вести учет демонстрации рекламных материалов (регистрировать, сколько раз был проигран тот или иной рекламный ролик в течение данной передачи, сколько пользователей просмотрело или прослушало его целиком и т. д.).

Своевременная доставка содержимого

Чтобы гарантировать своевременную доставку содержимого по назначению, службы Windows Media поддерживают:

- новый способ кэширования/замещения, упрощающий разработку решений на основе этой технологии, а также управление встроенными политиками кэширования/замещения и расширение их возможностей; кэширование/замещение позволяет рационально использовать сетевые каналы, снижать задержку в сети и нагрузку на серверы-трансляторы Windows Media;
- улучшенную поддержку протоколов, таких как RTSP и HTTP, для межсерверного взаимодействия; к новым протоколам и стандартам, поддерживаемым Windows Media, относятся RTSP, HTTP 1.1, Internet Group Management Protocol (IGMP) 6 и IP версии 6;
- гибкое распределение нагрузки между серверами с использованием UDP/TCP;
- взаимодействие с Windows Media Services 4.1 для потоковой передачи данных в смешанном окружении.

Корпоративные возможности

Службы Windows Media никогда не были более масштабируемыми, надежными и защищенными, чем в версии 9. Следующие особенности позволяют службам Windows Media обеспечивать потоковую передачу содержимого в сетях крупнейших предприятий и медиа-корпораций.

- **Встроенная защита** В Windows Media Services встроены средства защиты промышленного класса. Встроенные механизмы аутентификации и авторизации обеспечивают защиту данных при их передаче от программы-кодировщика на сервер и с сервера клиенту. Поддерживается и HTTP Digest и системы управления правами доступа к данным, обеспечивающие их безопасность при передаче по каналам связи и хранении на клиентской стороне.
- **Наблюдение в реальном времени** При наблюдении за производительностью сервера с помощью Windows Performance Monitor и консоли Simple Network Management Protocol (SNMP) доступны 72 счетчика производительности, устанавливаемых автоматически.
- **Администрирование** К вашим услугам три инструмента, позволяющих администрировать Windows Media Server практически в любом окружении:
  - оснастка Windows Media Services для консоли Microsoft Management Console (MMC) с новым полнофункциональным интерфейсом, полностью перестроенным для оптимизации решения административных задач и новыми мастерами, облегчающими исполнение типовых действий поадминистрированию;
  - Windows Media Services Administrator для Web с интерфейсом на основе HTML 3.2 предоставляет беспрецедентную возможность удаленного администрирования Windows Media Services, а также для администрирования этих служб через брандмауэр и сетевые каналы с низкой пропускной способностью;
  - возможность администрирования сервера Windows Media посредством сценариев, исполняемых в командной строке.

Расширяемая платформа

Windows Media Services -- это открытая платформа, поддерживающая более 500 свойств и около 60 интерфейсов, доступных разработчикам. Эту богатую функциональность можно применять для программного конфигурирования сервера Windows Media, наблюдения за ним и подключенными к нему клиентами, а также для получения доступа к любым статистическим данным, собранным при мониторинге.

Функциональность сервера Windows Media можно расширить при помощи подключаемых модулей (как готовых, так и собственных). Пакет Windows Media Services SDK теперь поддерживает интерфейсы, позволяющие создавать подключаемые модули с разнообразной функциональностью:

- модули аутентификации;
- модули кэширования/замещения;
- модули протоколов управления;
- компоненты записи данных:
- источники данных;
- модули авторизации и уведомления о событиях;
- модули ведения журналов;
- анализаторы медиа-данных;
- анализаторы списков воспроизведения.

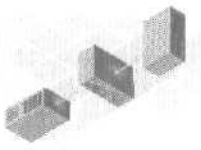
Новый расширенный пакет Windows Media Services SDK в полном объеме поддерживает вышеперечисленные интерфейсы, свойства и методы, а также допускает их использование в сценариях. Разработчики могут писать приложения на C, Visual C++, Visual C#, Visual Basic, Visual Basic Scripting Edition (VBScript), Microsoft Jscript и других языках сценариев,

Дополнительные сведения

Дополнительную информацию к этой главе см. по адресам:

- Introducing the Windows Server 2003 Family — http://www.microsoft.com/windowsserver2003/evaluation/overview/f_amily.mspx;
- Windows Media 9 Series — http://www.microsoft.com/windows/windowsmedia/;

- Upgrading to Windows Media Services 9 Series — http://www.microsoft.com/windows/windowsmedia/9series/server.asp;
- Compare the Editions of Windows Server 2003 — http://www.microsoft.com/windowsserver2003/evaluation/features/compareeditions.mspx;
- Introducing the «.NET» in the Windows Server 2003 Family - http://www.microsoft.com/windowsserver2003/evaluation/overview/dotnet/dotnet.mspx;
- Windows 2000 Streaming Media Services — http://www.microsoft.com/windows2000/technologies/other/default.asp#section2.



ГЛАВА

11

Файловые службы

Технологии ОС Windows Server позволяют снизить совокупную стоимость владения (total cost of ownership, TCO) решений и предоставляют надежные файловые службы для создания корпоративной вычислительной инфраструктуры. Усовершенствования файловых служб Windows Server 2003, ориентированы главным образом на удовлетворение потребностей организаций, использовавших файловые службы Windows NT Server 4.0. В этой главе обсуждаются улучшения Windows Server 2003, коснувшиеся файловых служб, а также основные инновации в инфраструктуре этих служб, новые возможности и усовершенствования в инструментах управления, снижающих затраты на поддержку файловых серверов.

Большинство улучшений файловых служб ОС семейства Windows Server 2003 сделано Microsoft по просьбам пользователей.

- **Службы инфраструктуры** Последние годы, пока новые приложения и топологии хранилищ (речь идет о *сетях хранения данных* — storage area networks, SAN) завоевывали популярность, шла борьба за то, чтобы заставить все компоненты подобных решений работать вместе. Стандартизированные службы инфраструктуры Windows Server 2003 упрощают разработку ключевых инструментов для управления сервером и файловыми службами.
- **Дополнительные удобства для конечного пользователя** Windows Server 2003, используемая совместно с Windows XP, позволяет напрямую обращаться к сетевым данным и фай-

лам, обеспечивая более стойкую защиту сетевого соединения с конечными пользователями, хранящими файлы на сетевых дисках (даже если пользователи не являются Windows XP-клиентами).

- **Меньшая суммарная стоимость владения** Достигается путем применения усовершенствованных инструментов управления, работающих через Web, и инструментов командной строки с расширенной функциональностью, поддерживающих управление локальными и удаленными файловыми серверами при помощи сценариев.

В этой главе вы узнаете об усовершенствованиях локальных хранилищ, службах виртуальных дисков, теневом копировании томов и др.

Улучшения файловых систем

В семействе ОС Windows Server 2003 файловая система усовершенствована.

- **Повышена надежность** Новые функции, такие как Automated System Recovery (ASR), упрощают восстановление ОС, резервное копирование файлов и обеспечивают максимальную доступность.
- **Повышена производительность труда** Улучшенная инфраструктура файловой системы облегчает защиту, хранение и доступ к файлам и критическим ресурсам. Это позволяет работникам в любой момент подучить доступ к нужным ресурсам или восстановить файлы без вмешательства отдела технической поддержки.
- **Улучшены возможности работы в сети** Функции совместной работы с удаленными документами расширяют возможности доступа к ресурсам одной или нескольких организаций.

Новые возможности файловых служб

В Windows Server 2003 усовершенствован ряд функций инфраструктуры файловой системы. Вот краткий список файловых служб, улучшенных или добавленных в Windows Server 2003,

- **Работа с удаленными документами (WebDAV)** Эта новинка обеспечивает доступ к корпоративным ресурсам через редиректор WebDAV, который позволяет клиентам обращаться

к файлам, хранимым в Web-репозитариях, вызывая функции файловой системы.

- **Automated System Recovery** (ASR) Это новшество позволяет за одну операцию восстановить ОС, ее состояние и конфигурацию оборудования после аварии.
- **Интерфейс командной строки** Инструменты командной строки позволяют решать большинство задач управления дисками, включая конфигурирование дисков и RAID, управление теневым копированием и настройку файловой системы.
- **Таблицы разделов на основе GUID** 64-разрядные версии Windows XP/Server 2003 (Enterprise и Datacenter) поддерживают новый способ организации разделов на диске — *таблицу разделов на основе GUID* (GUID partition table, GPT). В отличие от обычных дисков с разделами, основанных на *главной загрузочной записи* (master boot record, MBR), при использовании GPT данные, критичные для работы платформы, записываются не в сектора, расположенные вне разделов или в скрытые сектора, а в сами разделы. Диски с разделами на основе GPT содержат копии главной и резервной таблиц разделов, что тоже способствует сохранению целостности структуры данных раздела.
- **Высокопроизводительные инструменты для дефрагментации** Windows Defragmenter повышает доступность и производительность дисков, оптимизируя размещение файлов в томе. Дефрагментация выполняется быстрее и эффективнее, чем в Windows 2000. Поддерживается также *дефрагментация «на лету»* (online defragmentation) *главной таблицы файлов* (Master File Table, MFT) и дефрагментация томов NTFS с любым размером кластера.
- **Индексирование содержимого** На локальной машине и в сети обеспечивается простой, быстрый и безопасный поиск данных в разных форматах и на разных языках при помощи команды Search из меню Start или через HTML-страницы, доступные для просмотра через браузер.
- **Улучшенная распределенная файловая система (Distributed File System, DFS)** Позволяет создавать высокодоступные файловые службы с невысокой TCO. Используя DFS, можно объединять несколько физических файловых систем в одну логическую, упрощая тем самым работу с системой и повы-

шая ее производительность. DFS позволяет создать единый логический каталог, который включает несколько файловых серверов и сетевых дисков группы, подразделения или целой организации, благодаря чему пользователи смогут без труда находить файлы и папки, расположенные в любом месте сети. Служба каталогов Active Directory делает возможной публикацию разделяемых ресурсов DFS в виде объектов томов, администрирование которых можно делегировать другим уполномоченным лицам. Среди новых функций DFS – возможность выбора ближайшего сайта: на основе метрики сайта из Active Directory DFS рассчитывает маршрут от клиента до ближайшего файлового сервера с заданным путем. Кроме того, теперь можно размешать несколько корней DFS на одной системе, работающей под управлением Windows Server 2003.

- **Службы репликации файлов (File Replication Services, FRS)** Позволяют дополнительно снизить TCO, обеспечивая синхронизацию данных. FRS работает совместно с DFS, реплицируя хранимые ею данные в сетевые хранилища и автоматически синхронизируя реплики, расположенные на нескольких серверах, Топологию репликации можно настраивать при помоши оснастки DFS для консоли MMC (это новинка Windows Server 2003). Службы FRS также были дополнены возможностями сжатия сгенерированного репликацией трафика и сброса его излишков.
- **Шифрующая файловая система (Encrypting File System)** Расширяет возможности других средств управления доступом, формируя дополнительный уровень защиты данных. EFS работает прозрачно для пользователей (как встроенный сервис файловой системы), облегчая управление файловой системой и затрудняя атаки злоумышленникам,
- **Новые средства поддержки антивирусных программ** Устойчивая поддержка антивирусной защиты, имевшаяся в Windows Server, дополнена функциями ядра, повышающими производительность и надежность антивирусных программ от сторонних производителей. Теперь доступен пакет Windows Hardware Quality Lab (WHQL) для тестирования антивирусных программ, выполненных в виде драйверов фильтра файловой системы, и разработана процедура их сертификации.

- **Утилита CHKDSK** NTFS всегда была истинной файловой системой на основе журналов, поэтому прибегать к CHKDSK требовалось редко. Когда же необходима проверка диска утилитой CHKDSK (меньше 1% от общего числа непредвиденных отключений), она выполняется минимум вдвое быстрее, чем в Windows 2000.

Улучшенная инфраструктура файловой системы

Службы *виртуальных дисков* (Virtual Disk) и *теневого копирования томов* (Volume Shadow Copy) являются ключевыми элементами улучшенной инфраструктуры файловой системы в Windows Server 2003.

Служба виртуальных дисков

Служба виртуальных дисков (Virtual Disk service, VDS) предоставляет важный набор новых функций API, обеспечивающих управление собственно дисками.

В Windows 2000 каждый производитель оборудования для SAN предоставлял набор специализированных API для управления его оборудованием, что затрудняло разработку унифицированного ПО. В Windows Server 2003 эту проблему решает VDS, предоставляющая единый унифицированный интерфейс для управления дисками. Производители могут создать провайдер VDS, транслирующий вызовы универсального VDS API в соответствующие аппаратные команды. Уровень абстрагирования, формируемый VDS, обеспечивает пользователям Windows Server 2003 доступ к более устойчивым решениям.

Теперь при выборе оборудования можно не думать об управляющих приложениях. Новые приложения для управления дисками в Windows будут ориентированы на VDS, благодаря чему следующее поколение подобных программ будет способно управлять любым оборудованием, для которого есть провайдер VDS.

Microsoft реализовала провайдеры VDS для базовых и динамических дисков. Эти провайдеры расширяют функциональность базовых дисков, позволяя делать то, что раньше было возможно лишь с динамическими дисками, например, увеличивать размер тома «на лету» (рис. 11-1).

Рис. 11-1. Архитектура службы виртуальных дисков

Служба теневого копирования томов

Служба теневого копирования томов — это универсальная инфраструктура, позволяющая создавать «снимки» данных тома на определенный момент времени.

Самый яркий пример ее применения — приложение Shadow Copy Restore, а также приложения для резервного копирования. В Windows 2000 Server резервное копирование требовало остановки сервера либо заставляло мириться с такими побочными эффектами копирования «на лету», как несогласованность данных и невозможность копирования открытых файлов. В Windows Server 2003 данные можно копировать «на лету», не теряя их согласованности и не беспокоясь об открытых файлах.

Служба Volume Shadow Copy облегчает создание резервных копий «на лету», обеспечивая согласованность данных путем формализации связей между тремя ключевыми сущностями-участниками процесса управления данными. Вот эти сущности:

- **запрашивающие компоненты,** например, приложения для резервного копирования, управляющие работой запоминающих устройств;
- **записывающие компоненты** — это приложения, генерирующие данные;
- **провайдеры** — устройства или программы, способные создавать «снимки» дисков.

Схема взаимодействия этих компонентов — на рис. 11-2,

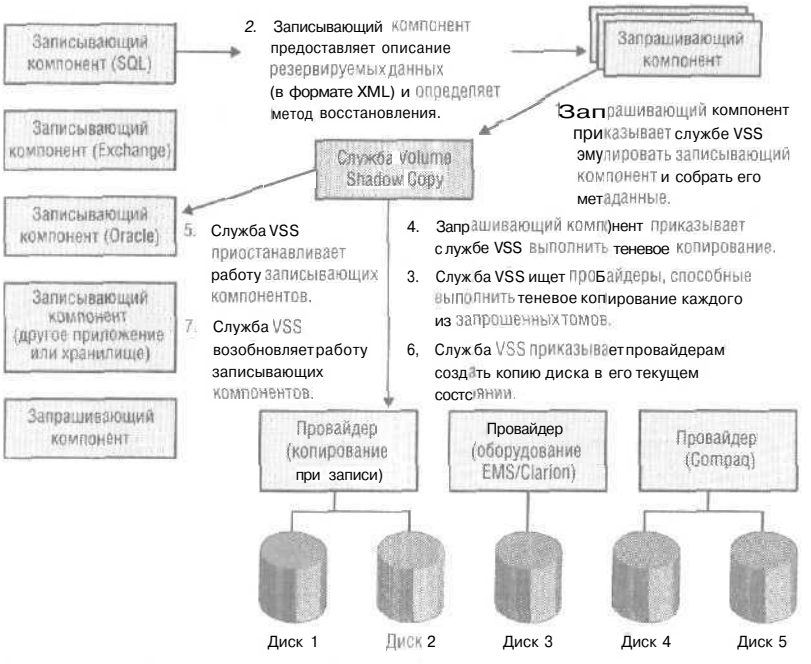


Рис. 11-2. Схема взаимодействия компонентов при теневом копировании томов

Примечание Встроенный провайдер теневого копирования Windows использует алгоритм *копирования при записи* (copy-on-write). Так, если в разделе хранится 3 Гб данных, теневое копирование Windows Server 2003 не создает копию для всех 3 Гб, а копирует порции данных тома по мере их изменений приложениями.

Распределенная файловая система

Ряд усовершенствований Windows Server 2003 касается *распределенной файловой системы* (Distributed File System, DFS) — мощного средства для управления объединенными файловыми серверами, которое предоставляет:

- **уровень сервиса (service layer),** изолирующий имена, которые клиенты используют для получения доступа к файлам через сеть, от имен серверов, на которых физически находятся эти файлы;
- **масштабируемость,** равномерно распределяя между серверами нагрузку, генерируемую клиентами;
- **надежность,** при аварии сервера направляя (прозрачно для клиента) поступающие запросы другому серверу; DFS автоматически синхронизирует реплики при помощи FRS;
- **корни и соединения DFS** — фундаментальные понятия DFS;
  - *корень DFS* (DFS root) — это сервер либо набор серверов, к которому клиенты обращаются в первую очередь, пытаясь получить доступ к файлу;
  - *соединение DFS* (DFS junction) — это ссылка от корня DFS на сервер или набор серверов (реплик), способных обработать пользовательский запрос.

В Windows Server 2003 теперь допускается размещение нескольких корней DFS на одном сервере. В Windows 2000 это невозможно, т. е. в кластере Windows 2000 должно быть не более одного корня DFS. Если при восстановлении после сбоя имеет место попытка разместить на одном узле кластера два корня DFS одновременно, ОС генерирует исключение. В Windows Server 2003 это ограничение снято, что позволяет повысить надежность корней DFS путем применения кластеров.

DFS в Windows Server 2003 управляется лучше благодаря делегированию администрирования. В Windows 2000 только администратор пространства имен DFS имел право управлять частями этого пространства имен. В крупных организациях, нуждавшихся в пространстве имен DFS, объединяющем все корпоративные ресурсы, это вызывало проблемы, так как в Windows 2000 было невозможно делегировать полномочия на управление частью пространства имен DFS администратору соответствующего подразделения.

В Windows Server 2003 можно передать права на администрирование определенной части пространства имен другому администратору.

В Windows Server 2003 улучшено и создание реплик, размещенных на нескольких сайтах. В Windows 2000 DFS отдает приоритет репликам, размешенным на сайте клиента. Если же подходящих реплик на этом сайте нет, DFS выберет для обработки запроса любую доступную реплику. Ясно, это не лучший алгоритм.

Допустим, у компании есть сайты в Редмонде, Вашингтоне, Кремниевой долине и Тасмании. Если реплика сайта, расположенная в Кремниевой долине, станет недоступной, DFS из Windows 2000 может отослать запрос сайту в Редмонде или в Тасмании с равной вероятностью. Windows Server 2003 в этом случае получит из Active Directory сведения о стоимости обработки запросов на разных сайтах и выберет на их основе удаленную реплику, способную удовлетворить клиентский запрос. В этом примере DFS, проанализировав данные из Active Directory, обнаружит, что обработка запроса тасманийским сайтом обойдется «дороже», чем сайтом из Редмонда, и направит запрос клиента из Кремниевой долины сайту в Редмонде.

Другие улучшения файловых служб

К перечисленным улучшениям файловых служб можно добавить:

- повышение пропускной способности Common Internet Fije System (CIFS), особенно в многопроцессорных системах;
- улучшение масштабируемости DFS (в частности, за счет снижения объема используемой памяти, а также ускорения запуска и настройки);
- более совершенные диагностические инструменты для FRS;
- улучшенные механизмы для управления дисковым пространством и полосой пропускания сетевого канала для FRS.

Дополнительные удобства для конечного пользователя

Утилита Shadow Copy Restore, а также улучшения Offline Files и редиректора WebDAV делают удобнее работу с системой,

Shadow Copy Restore

Экспериметнтально установлено, что треть всех случаев потери данных — результат ошибок человека. Новая функция Windows Server 2003 — теневое копирование — позволяет решить эту проблему.

Теневая копия содержит последнюю версию файла. Теневое копирование позволяет файловому серверу с Windows Server 2003 эффективно и прозрачно для пользователя хранить несколько версий каждого серверного файла. Просматривать последние версии файлов позволяет программа-надстройка (она есть на установочном компакт-диске Windows Server 2003), бесшовно интегрирующаяся с ПО клиентской машины.

Теневое копирование — низкозатратный способ восстановления файлов, потерянных в результате ошибок, возникших по недосмотру оператора, скажем, из-за неправильного редактирования, случайного повреждения или удаления.

Теневое копирование не заменит стандартных решений для резервного копирования (теневое копирование не защитит от потери данных из-за отказа носителя), но позволит реже восстанавливать данные с носителя на магнитной пленке.

Улучшения Offline Files

Windows Server 2003 и ряд изменений клиента на основе Windows XP позволили улучшить предоставление файлов. На стороне клиента это коснулось функции Offline Files, введенной в Windows 2000 и позволяющей кэшировать копии удаленных файлов и папок на локальных машинах.

Кэширование бывает двух типов: кэширование документов и кэширование программ. Общему сетевому файловому хранилищу тип кэширования назначает администратор сервера:

- если клиент кэширует документы, ОС берет копию документа с файлового сервера, если тот доступен, в противном случае Windows XP прозрачно для пользователя открывает копию документа из кэша;
- если клиент кэширует программы и файловый сервер доступен, Windows XP проверяет актуальность кэшированной версии программы; при положительном результате проверки Windows XP запускает копию программы из кэша; это

позволяет разгрузить файловый сервер, переложив на клиентскую ОС часть его работы, что повышает масштабируемость файлового сервера.

Есть и другие причины большей устойчивости улучшенной версии Offline Files из Windows XP/Server 2003 в сравнении с таковой из Windows 2000. Так, пользователи Windows XP могут кэшировать файлы из пространства имен DFS, что невозможно в Windows 2000. Кроме того, в Windows XP улучшена работа Offline Files с шифрующей файловой системой (EFS).

РедиректорWebDAV

Благодаря редиректору WebDAV на клиенте под управлением Windows XP стало удобнее работать с общими файлами.

Сегодня можно создавать в Web хранилища документов. Специализированные инструменты для публикации данных в Web используют протокол WebDAV для обновления документов, хранящиеся в таких репозитариях, В Windows XP подобные хранилища доступны любому приложению через редиректор WebDAV (WebDAV Redirector). Редиректор назначает серверу WebDAV букву диска, после чего имеюшиеся приложения смогут получать доступ к файлам этого сервера.

Меньшая стоимость владения

ИТ-специалистам, поддерживающим файловые серверы, требовалось снизить себестоимость предоставляемых сервисов. Это требование было выполнено благодаря следующим ключевым усовершенствованиям Windows Server 2003.

- **Web-интерфейс для администрирования сервера** Web-интерфейс в Windows Server 2003 позволяет администрировать файловые серверы через любой браузер. Через этот интерфейс можно управлять дисками, квотированием и совместным доступом.
- **Инструменты командной строки** В Windows Server 2003 имеются инструменты для управления локальным хранилищем, работающие в командной строке:
  - Diskpart.exe служит для управления разделами; позволяет создавать зеркальные, чередующиеся, расширенные и другие тома;

- Fsutil.exe управляет дополнительными функциями NTFS, такими как журнал USN, жесткие ссылки и квоты;
- Vssadmin.exe управляет службой Volume Shadow Copy.

- Автоматическое восстановление системы (Automated System Recovery, ASR) Служит для восстановления после аварий, вызванных как физическим уничтожением оборудования, так и его катастрофическими отказами.

В Windows 2000 восстановление после аварии занимало много времени и осуществлялось, как правило, вручную. Типичная процедура включала такие этапы:

1. приобретение нового оборудования;
2. установка базовой версии Windows;
3. ручная настройка оборудования хранилища с целью воссоздать состояние, в котором оно было до аварии:
4. установка ПО для восстановления;
5. восстановление параметров ОС:
6. восстановление параметров приложения;
7. восстановление данных приложений.

Задача ASR — быстро и в автоматическом режиме привести отказывающуюся загружаться машину в состояние, пригодное для запуска программы восстановления данных. ASR конфигурирует новое хранилище с параметрами, применявшимися до аварии, восстанавливает ОС, приложения и их конфигурацию. В отличие от длительного процесса ручного восстановления Windows 2000 или предыдущих версий этой ОС ASR позволяет администратору Windows Server 2003 быстро решать эту задачу. Процедура восстановления ОС с использованием ASR в Windows Server 2003 такова:

1. загрузитесь с компакт-диска Windows .NET Server и выберите в загрузочном меню пункт Automated System Recovery;
2. при необходимости вставьте носитель с резервной копией и заранее созданный гибкий диск ASR;
3. займитесь другими делами -- через некоторое время вы сможете вернуться к работоспособной машине с установленной ОС и правильно настроенными приложениями.

Перед началом процедуры надо подготовить носитель с резервной копией ОС -- он потребуется для ASR. Резервная

копия для ASR включает обычную копию системы плюс гибкий диск ASR с важными сведениями о конфигурации системы (например, числом и размером разделов) и способе восстановления этой копии.

Работу ASR обеспечивает небольшой загрузочный код, встроенный в программу установки Windows. Если во время загрузки с компакт-диска нажать F8 при выводе соответствующего приглашения, запустится загрузочная программа ASR. Код ASR из Windows Setup «умеет» читать с диска ASR данные, нужные для восстановления конфигурации хранилища. Далее специальная версия программы Windows Setup устанавливает ровно столько компонентов ОС, сколько необходимо для запуска программы восстановления, а затем ASR автоматически вызывает эту программу, а она восстанавливает все остальные данные с резервной копии ASR.

В Windows Server 2003 Microsoft включила полное решение ASR, которое можно без ограничений расширять системами резервного копирования от сторонних производителей.

Улучшенные дисковые утилиты

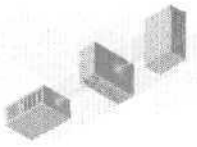
В Windows Server 2003 усовершенствованы ключевые утилиты.

- **CHKDSK** В Windows Server 2003 повышена производительность утилиты CHKDSK. появившейся в Windows 2000. Независимое тестирование, проведенное eTesting Labs, подтвердило, что CHKDSK из Windows Server 2003 на 90% быстрее аналогичной утилиты из Windows NT Server 4.0 при обработке томов, содержащих несколько миллионов файлов. Помимо повышения производительности, приоритетной задачей при создании NTFS было уменьшение числа случаев, требующих запуска CHKDSK. NTFS полностью основана на журналах, и в ней (как и в большинстве баз данных) применяется журнал с опережающей записью, обеспечивающий согласованность метаданных даже после краха системы, поэтому CHKDSK нужно запускать только после отказа оборудования или повреждения метаданных NTFS.
- **Disk Defragmenter** Microsoft повысила производительность механизма дефрагментации. В Windows Server 2003 утилита Disk Defragmenter способна дефргаментировать главную таблицу файлов (MFT) NTFS.

Дополнительные сведения

Дополнительную информацию к этой главе см. по адресам:

- What's New in File and Print Services for Windows Server 2003 — http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/fileandprint.mspx;
- Introducing the Windows Server 2003 Family — http://www.microsoft.com/windowsserver2003/evaluation/overview/family.mspx;
- Windows Server 2003 Family Technical Overviews — http://www.microsoft.com/windowsserver2003/techinfo/overview/;
- What's New in Storage Management — http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/storage.mspx;
- Windows 2000 File and Print Services — http://www.microsoft.com/windows2000/technologies/fileandprint/.



ГЛАВА
12

Службы печати

Одни из самых распространенных типов серверов — файловые серверы и серверы печати. В Windows Server 2003 усовершенствованы многие функции печати Windows 2000.

Преимущества новых служб печати

Преимущества усовершенствованных служб печати Windows Server 2003 таковы (табл. 12-1),

Табл. 12-1. Преимущества служб печати Windows Server 2003

Сфера усовершенствований	Преимущества
Надежность	Более высокая надежность благодаря управлению драйверами принтера
	Увеличенная производительность очереди печати на сильно загруженных серверах
	Лучшая масштабируемость и доступность приложений, критичных для бизнеса
	При установке драйвера принтера в кластер выполняется автоматическая репликация драйвера на все узлы кластера
Поддержка нового оборудования	Улучшенная поддержка оборудования (более 3800 устройств)
	Поддержка цветных принтеров класса High-end (поддержка PCL XL в мини-драйвере Unidrv)
	Поддержка USB 2.0

(см. след. стр.)

Табл. 12-1. Преимущества служб печати ... *(продолжение)*

Сфера усовершенствований	Преимущества
Управление	Улучшенная процедура настройки кластерного сервера печати
	Провайдер печати для Windows Management Instrumentation (WMI)
	Более защищенный сервис очереди печати
	Универсальная схема управления версиями драйверов принтеров
	Блокировка драйверов режима ядра (по умолчанию включена)
	Увеличенная производительность редиректора печати Terminal Server
Поддержка Интернета	Более защищенное управление печатью через Интернет (point-and-print)
Доступность	Автоматический перезапуск спулера
	Возможность настройки в соответствии с потребностями организации

Улучшения служб печати

В службах печати ОС семейства Windows Server 2003 сделано множество улучшений.

- **Интерфейс командной строки** Новые инструменты командной строки позволяют решать большинство задач печати. включая расширенное управление и настройку принтеров, диспетчеризацию заданий и очереди печати, а также управление портами и драйверами.
- **Поддержка кластерных серверов печати (только в редакциях Enterprise и Datacenter)** Эта новинка Windows Server 2003 повышает продуктивность, облегчая установку драйверов принтеров в кластерах. При установке драйвера принтера в виртуальный кластер, система автоматически реплицирует его на все узлы кластера.
- **64-разрядная поддержка печати** Еще одна новинка Windows Server 2003 — поддержка 64-разрядных драйверов и приложений. Технология *Point-and-print* (указал и напечатал),

применяемая для поддержки печати в клиент-серверных системах, обеспечивает взаимодействие 32- и 64-разрядных клиентов и серверов.

- **Поддержка широкого спектра оборудования** Windows Server 2003 поддерживает более 3800 принтеров.
- **Более высокая надежность** Серверы печати на основе Windows Server 2003 более надежны благодаря блокировке драйверов режима ядра. Это дает в руки администратора инструменты для тонкого управления установкой драйверов на сервере.
- **Улучшения Active Directory** Опубликовав принтер через службу каталогов Active Directory, вы предоставите пользователям возможность быстро найти принтер с заданными характеристиками (адресом, поддержкой цветной печати и скоростью) и подключиться к нему.
- **Повышение производительности** В Windows Server 2003 достигнута более высокая производительность по сравнению с Windows 2000 путем оптимизации работы спулера с файлами (операций дискового чтения-записи), ориентированной на поддержку больших заданий. Все это позволяет пользователям быстрее печатать нужные им документы.
- **Более совершенная технология Plug and Play** Windows Server 2003 повышает производительность труда, автоматически определяя новое оборудование и соответствующим образом изменяя конфигурацию сервера.
- **Упрошенное управление принтером** Теперь легко наблюдать за локальными и удаленными принтерами: System Monitor позволяет следить за счетчиками, отражающими, например, размер данных (в битах), отправленных на печать в секунду, число ошибок заданий и отпечатанных страниц,
- **Более высокая производительность при печати через сеть** Обновлен стандартный монитор портов — основной метод, применяемый Microsoft для быстрой и устойчивой к ошибкам печати на сетевых принтерах: повышена его производительность и расширен набор предоставляемых им сведений о состоянии устройств,

  Windows Server 2003 также поддерживает печать через беспроводные соединения по протоколу 802.1X или Bluetooth.

Кроме того, драйверы принтера автоматически загружаются при подключении клиентского компьютера к серверам печати — это упрощает печать через сеть и экономит время.

- **Более устойчивая защита** В Windows Server 2003 добавлены две групповые политики, повышающие безопасность окружения печати: первая запрещает подконтрольным ей клиентам подключаться к серверам печати, с которыми не установлены отношения доверия, а вторая запрещает спулеру соединяться с клиентами, если данный сервер не поддерживает службы печати.
- **Широкие возможности взаимодействия** Благодаря поддержке протоколов AppleTalk, LPR/LPD и IPX серверы печати Windows могут принимать задания от клиентов, работающих под управлением других ОС (Macintosh, UNIX. Linux и Novell), а Windows-клиенты способны использовать северы печати пол управлением ОС. отличных от Windows.

Управление службами печати

В Windows Server 2003 сделан ряд улучшений в сфере управления серверами печати.

- **Централизованная настройка принтеров** Администраторы могут определить конфигурацию принтера по умолчанию, которая сделает всевозможности принтера доступными для пользователей, не требуя от них знания параметров принтера. Параметры *duplex by default* (двусторонняя печать по умолчанию) обеспечивают экономичную печать,
- **Планирование и управление доступом к принтеру** Административные инструменты контролируют доступ к печатающим устройствам, приоритет заданий и распределение нагрузки. Например, администратор может создать два логических принтера на основе одного физического устройства. Первый принтер можно настроить для печати в течение всего дня. а второй — только вне часов пик. Сконфигурировав большие пакетные задания так, чтобы они отправлялись только на второй принтер (где они будут стоять в очереди, пока не придет время печати), можно избежать помех печати документов, необходимых остальным пользователям, которые создаются объемными заданиями.

- **Управление драйверами принтеров** Windows Server 2003 поддерживает блокировку сбойных драйверов (она имелась в Windows 2000), в том числе драйверов пользовательского режима. Новая политика Windows Server 2003 позволяет администратору управлять установкой драйверов режима ядра; по умолчанию она запрещена (*disallowed*).
- **Репликация драйверов** Поддерживаемая Windows технология «point-and-print» обеспечивает репликацию драйверов и параметров конфигурации на самые разные типы клиентов. Windows 2000/XP-клиенты поддерживают богатый набор средств для автоматического обновления параметров, драйверов и др.
- **Поддержка сценариев** Провайдер печати WMI для Windows Server 2003 предоставляет богатый набор функций для поддержки сценариев, позволяющий собирать сведения о принтерах, манипулировать ими, а также создавать новые и копировать (клонировать) имеющиеся принтеры со всеми параметрами на новые и имеющиеся серверы. Пакет Windows Server 2003 Resource Kit содержит дополнительную информацию о консоли Windows Management Instrumentation Command Line (WMIC), средствах поддержки и возможностях. WMIC - - это интерфейс командной строки для Windows Management Instrumentation. Поставляется шесть готовых сценариев для управления печатью из командной строки, которые позволяют;
  - D **Prnqctl** — приостановить/возобновить/удалить задания, а также напечатать пробную страницу;
  - □ **Prnport** — добавить/удалить порты tcpmon, а также вывести их список;
  - D **Prnmngr** — добавлять/удалять принтеры и соединения, а также вывести их список;
  - п **Prnjobs** — приостановить/возобновить/отменить задания и вывести их список;
  - п **Prndrvr** — добавлять/удалять драйверы принтеров, а также вывести их список;
  - п **Prncnfg** — задать конфигурацию принтера (возможность его совместного использования. адрес, имя и т. п.).
- **Поддержка оборудования** Windows Server 2003 поддерживает не только популярные модели, имевшиеся в Windows 95,

но и принтеры корпоративных моделей. В универсальный механизм печати Unidrv добавлена поддержка цвета PCL **XL,**

- **Поддержка кластеров** Помимо портов принтеров. Windows Server 2003 автоматически реплицирует драйверы принтеров из ресурсов спулера на все узлы кластера, что примерно на треть снижает усилия на развертывание. В Windows Server 2003 добавлены новые функции поддержки кластеров:
  - □ поддержка кластеров до 8 узлов;
  - П централизованное управление драйверами принтеров (теперь их достаточно установить однократно);
  - П «кворум» из большинства узлов кластера;
  - п снижены требования к свободному месту на общем диске (отпала потребность в «кворумном» разделе);
  - П теперь кластеры сервера печати и Terminal Services могут соседствовать на одних узлах.

  И все же кластерным серверам печати понадобится место на общем диске для хранения ресурсов спулера, такое хранилище нужно для любого виртуального сервера. О развертывании кластеров см. главу 13.
- **Простая установка** Стандартный монитор портов TCP/IP (SPM) упрощает установку портов для сетевых принтеров. SPM предоставляет подробные сведения о состоянии принтера — их можно получить через Web-интерфейс на любой клиентской машине, подключенной к Интернету- SPM также выводит более точные сообщения об ошибках (например. *paper out)* по сравнению со скудными описаниями, выводимыми другими мониторами портов, такими как LPR. Интерфейс WMI в Windows Server 2003 предоставляет мощные средства для удаленной установки и настройки принтеров с применением сценариев.
- **Интеграция с Active Directory** Пользователи смогут искать серверы печати и просматривать их ресурсы, чтобы выбрать подходящий принтер. Стандартные правила именования серверов и принтеров максимально упрощают этот процесс, Благодаря применению устоявшихся стандартов представления имен, описаний и адресов принтеров формируется высокодоступное и эффективно окружение печати.
- **Поиск принтеров** В Windows Server 2003 средства мониторинга адресов принтеров (были в Windows 2000) объеди-

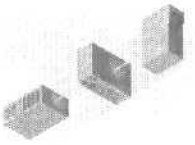
нены с Active Directory. Это даст пользователям возможность искать принтеры по стандартным названиям зданий, городов и другим критериям. Active Directory также позволит искать печатающие устройства с заданными характеристиками и возможностями, например, с поддержкой двусторонней и цветной печати, а также подходящей скоростью. Интеграция Active Directory и служб печати намного облегчит устранение неполадок отдельных принтеров и серверов.

Дополнительные сведения

Дополнительную информацию к этой главе см. по адресам;

- What's New in File and Print Services for Windows Server 2003 — http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/fileandprint.mspx;
- Windows 2000 File and Print Services — http://www.microsoft.com/windows2000/technologies/fileandprint/;
- What's New in Storage Management — http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/storage.mspx.

ГЛАВА
13



Службы кластеров

Кластерные серверы и кластеры с балансировкой сетевой нагрузки, разработанные для Windows NT Server 4.0. в Windows Server 2003 Enterprise и Datacenter существенно усовершенствованы и предоставляют три основных преимущества;

- **высокая доступность** достигается благодаря способности служб и приложений продолжать обслуживание клиентов, несмотря на отказы оборудования, сбои ПО и отключения для планового обслуживания;
- **лучшая масштабируемость** достигается расширением серверов путем наращивания числа процессоров (до 8 в Enterprise Edition, а в Datacenter Edition — до 32) и оперативной памяти (до 8 Гб в Enterprise Edition, в Datacenter Edition — до 64 Гб), а также объединения серверов в кластеры, образующие платформу для приложений;
- **удобное управление** возможно благодаря тому, что администраторы теперь могут управлять устройствами и ресурсами кластера как компонентами обычного компьютера.

Обзор кластерных технологий

Последние годы характеризуются ростом значения высокой доступности и масштабируемости для организаций, развертывающих ПО для электронной коммерции и бизнеса. ИТ-специалисты узнают из этой главы, как, используя кластерные решения в Windows Server 2003, создать эффективную вычислительную среду в масштабах предприятия.

Кластерные технологии Microsoft

В Windows 2000 удалось увеличить общее время работоспособности системы (ее доступность), уменьшить число отказов системы (повысить ее надежность) и облегчить добавление ресурсов и компьютеров с целью наращивания производительности (масштабируемости) — Windows Server 2003 поднимает эти характеристики на новый уровень. Стратегия кластеров в Windows 2000/Server 2003 характеризуется такими особенностями.

- **Балансировка нагрузки на сеть (Network Load Balancing. NLB),** доступная во всех версиях ОС семейства Windows Server 2003, равномерно распределяет входящий IP-трафик между узлами кластера, повышая доступность и масштабируемость Интернет-сервисов, таких как Web-сервисы, потоковая передача мультимедийных данных и службы терминалов (Terminal Services). Выполняя функции инфраструктуры, ответственной за балансировку нагрузки и предоставление данных управляющим приложениям, построенных на основе Windows Management Instrumentation (WMI), NLB бесшовно интегрируется в инфраструктуру Web-ферм.

  Балансировка нагрузки на компоненты обеспечивает динамическое распределение нагрузки на компоненты приложений среднего уровня, использующих COM+. Этот механизм равномерно распределяет нагрузку между компонентами COM+ на нескольких узлах, что повышает доступность и масштабируемость серверных приложений. Служба балансировки нагрузки на компоненты входит в пакет Application Center 2000.2
- **Кластерные серверы** (поддерживаются только в редакциях Enterprise Edition и Datacenter) обеспечивают высокую доступность и масштабируемость критичных для бизнеса приложений, таких как БД. системы обмена сообщениями и службы файлов и печати. Если один из узлов кластера почему-либо недоступен, его заменяет другой узел, который продолжает обслуживать конечных пользователей отказавшего узла. Этот процесс называется *восстановлением после сбоя* (failover). После восстановления кластерной службы пользователи продолжают работать с ней, не подозревая, что их. обслуживает уже другой сервер (узел). Windows

Server 2003 Enterprise/Datacenter поддерживает кластеры размером до 8 узлов.

Балансировка нагрузки на компоненты является частью обшей стратегии обеспечения доступности и масштабируемости приложений, развертываемых на платформе Windows, однако она не входит в состав Windows Server 2003. О балансировке нагрузки на компоненты см. документацию по Application Center 2000.

Защита от простоев

Кластерные технологии от Microsoft обеспечивают защиту от:

- отказов приложений и служб, влияющих на прикладное ПО и ключевые сервисы;
- отказов систем и оборудования, влияющих на аппаратные компоненты (процессоры, диски, память, сетевые адаптеры, источники и питания и др.);
- сбоев сайтов, вызванных природными бедствиями, отключениями электропитания и каналов связи;
- плановых простоев (связанных с обновлением прикладного ПО и ОС, установкой сервисных пакетов или «горячих» исправлений).

Назначение и требования

Кластерные технологии предназначены для решения определенных задач и спроектированы с учетом соответствующих требований:

- служба Network Load Balancing разработана для повышения масштабируемости и доступности клиентских Web-сервисов и пограничных серверов, таких как серверы VPN и брандмауэры;
- балансировка нагрузки на компоненты служит исключительно для повышения масштабируемости и доступности приложений среднего уровня;
- служба кластеров Windows (Windows Clustering) обеспечивает поддержку автоматического восстановления служб серверных БД, круглосуточно работающих служб, нуждающихся в сохранении состояния и иных данных (например служб печати).

Служба кластеров Windows

Усовершенствованные технологии Windows Clustering предоставляют дополнительные средства для поддержки широкого спектра кластерных серверов с различной топологией.

Общие улучшения

Общие улучшения службы кластеров Windows Server 2003 таковы.

- **Увеличенный размер кластера** Windows Server 2003 Enterprise/Datacenter поддерживает кластеры размером до 8 узлов (раньше предельный размер кластера составлял 2 и 4 узла соответственно), что обеспечивает большую гибкость кластерных решений, в частности, при развертывании приложений на кластерных серверах. Приложения, способные работать в виде нескольких экземпляров, получат в свое распоряжение больше узлов, на каждом из которых сможет работать экземпляр такого приложения. Кроме того, на одном кластерном сервере можно развертывать несколько приложений, при этом доступно больше возможностей по управлению заменой отключившихся узлов.
- **64-разрядная поддержка** 64-разрядные версии Windows Server 2003 поддерживают службу кластеров и обеспечивают работу приложений, требующих много памяти. Windows Server 2003 поддерживает до 4 Тб, тогда как Windows 2000 Datacenter Server — не более 64 Гб. Примером приложений, использующих это преимущество 64-разрядных версий Windows Server 2003, является SQL Server 2000 Enterprise Edition (64-разрядная версия), которая наряду с этим поддерживает кластеры. В совокупности эти возможности создают мощную платформу для приложений, требовательных к вычислительной мощности.
- **Высокая доступность службы каталогов Terminal Server** Достигается благодаря автоматическому восстановлению после сбоев.
- **Мастер установки кластера** Поддерживает применение универсальных сценариев для обеспечения высокой доступности приложений.

- **Кластеры** MNS **(majority node** set) В Windows Server 2003 можно создать необязательный кворумный ресурс, который не требует диска, подключенного к общей шине в качестве кворумного устройства. Эта функция предназначена для встраивания в крупные комплексные решения производителями оборудования, а не для самостоятельного развертывания конечными пользователями. Кластеры MNS применяются в следующих ситуациях.
  - **Географически рассредоточенные кластеры** Этот механизм предоставляет единый кворумный ресурс от Microsoft, который не зависит от внешних запоминающих устройств и обеспечивает поддержку кластеров, узлы которых рассредоточены по некоторой территории, а также кластеров, включающих несколько сайтов. Оборудование для таких кластеров следует выбирать из отдельного списка совместимых устройств (HCL).
  - **Высокодоступные устройства, не использующие разделяемые диски** Эти бюджетные устройства вместо разделяемых дисков используют для хранения данных портирование журнала (log shipping) или псевдодиск, а также репликацию и создание зеркальных копий файловой системы, чтобы сделать хранимые данные доступными всем узлам кластера.

В Windows Server 2003 нет механизма для создания зеркальных копий или репликации пользовательских данных на узлы кластера MNS. В принципе можно создать кластер вовсе без общего диска, но обеспечение высокой доступности и избыточности данных приложений зависит от типа приложения. Применение кластеров MNS сулит следующие выгоды.

- **Абстрагирование внешнего хранилища** Позволяет подсистеме хранения данных управлять репликацией данных на другие сайты, не беспокоясь об общем кворумном диске; при этом поддерживается концепция единого виртуального кластера,
- **Возможность отказаться от общих дисков** Иногда необходимо точное согласование работы кластера, но общие диски не требуются, например, в кластерах, где данные узлов синхронизируются приложением [как при пор-

тировании журнала базы данных (БД) и репликации мало изменяемых файлов] и где приложения вовсе не сохраняют данных, но применяют тесно связанное взаимодействие, сохраняя согласованное состояние в оперативной памяти.

- **Увеличенная избыточность** Если общий кворумный диск будет поврежден, то выйдет из строя весь кластер, в случае же кластеров MNS повреждение кворумного хранилища на одном из узлов не ведет к отключению кластера.

Установка кластера

В этой процедуре сделаны следующие улучшения.

- **Вариант установки по умолчанию** Файлы кластера размещаются на узлах при установке Windows Server 2003, и вам остается только настроить кластер при помощи Cluster Administrator или сценария и утилиты Cluster.exe. Кроме того, можно заранее установить кворумные ресурсы от сторонних производителей и подключить их в ходе настройки сервера, вместо того чтобы устанавливать их по отдельности. Для развертывания кластеров любых конфигураций применяются стандартные процедуры. Это упрощает администрирование (теперь для установки службы кластеров не нужен носитель с дистрибутивом) и устраняет необходимость перезагрузки после установки/удаления службы кластеров.
- **Предварительный анализ конфигурации** Программа установки проверяет аппаратную и программную конфигурацию с целью выявления потенциальных проблем при установке кластера. Перед созданием кластерного сервера она предоставляет полный отчет с описанием обнаруженных потенциальных проблем с конфигурацией. Это гарантирует выявление любых потенциально несовместимых компонентов до начала настройки сервера. Так, Services for Macintosh (SFM), NLB, динамические диски и применение DHCP для выделения адресов не поддерживаются службой кластеров.
- **Значения по умолчанию** При установке создается кластерный сервер, оптимально настроенный с применением значений по умолчанию и эвристических методов. Как правило, значения по умолчанию оптимальны для новых кластерных серверов. Программа установки кластерных серверов

собирает нужные данные (теперь она задает намного меньше вопросов, чем раньше) и принимает ряд решений относительно конфигурации кластерного сервера, ее задача — создать и запустить кластерный сервер с конфигурацией по умолчанию. В дальнейшем эту конфигурацию можно изменить, используя административные инструменты. Можно добавлять к кластеру несколько узлов одновременно, что ускоряет и упрощает создание кластерных серверов из нескольких узлов.

- **Расширяемая архитектура** Позволяет подключать к кластерному серверу системные компоненты и приложения. Так. можно установить приложение или группу приложений до подключения этого узла и добавить их во время установки кластера. Это позволяет приложениям оперативно подключать ресурсы для кластерного сервера или изменять их конфигурацию при установке, а не после нее,
- **Удаленное администрирование** Позволяет выполнять любые действия по созданию и настройке кластерных серверов удаленно. Со станции удаленного управления можно создавать новые кластеры и добавлять узлы к существующим. Все изменения, связанные с назначением дискам других букв и восстановлением ресурсов дисков после сбоев применяются к клиентским сеансам Terminal Server, что улучшает удаленное администрирование через Terminal Sewer.
- **Инструменты командной строки** Создание и настройку кластерных серверов можно выполнять с помощью сценариев и утилиты командной строки Cluster.exe,
- **Упрощенная установка** Раньше требовалось сначала вывести узел из кластера и *лишь потом* удалять службу кластеров. Удаление службы кластеров стало эффективнее, поскольку теперь для этого достаточно вывести узел из кластера при помощи Cluster Administrator или Cluster.exe. Если вызвать Cluster Administrator сложно, можно удалить узел, вызвав Cluster.exe с новым ключом командной строки,
- **Локальный кворумный ресурс** Если узел не подключен к разделяемому диску, он автоматически создает локальный кворумный ресурс. Такой ресурс можно создать и сразу после запуска службы кластера. Пользователь сможет без труда создать у себя на локальном компьютере кластер для тес-

тирования кластерных приложений или изучения службы кластеров. Тестовый кластер можно создать и без оборудования, указанного в списке Microsoft Cluster HCL. Локальный кворум поддерживается только для кластеров из одного узла, а оборудование, не указанное в Microsoft Cluster HCL. не поддерживается в рабочем окружении. Если выйдут из строя все диски, кластер сможет некоторое время работать без них (скажем, до замены дисков). Для этого надо вызывать Cluster.exe с параметром */fixquorum*,затем создать локальный ресурс и сделать его кворумным:

- для кластерного сервера печати следует выбрать папку спулера на локальном диске;
- для файлового сервера можно выбрать локальный диск. на котором прежде нужно восстановить данные из резервной копии.

- **Выбор кворумного ресурса** Теперь можно не выбирать кворумныи диск вручную — им автоматически становится диск наименьшего объема (но не меньше 50 Мб), отформатированный под NTFS, так что конечный пользователь может не беспокоиться о кворумном диске. При установке кластера или настройке кластера кворумныи ресурс можно будет переместить на другой диск.
- **Active Directory** Намного теснее стала интеграция службы кластеров и службы каталогов Active Directory, включая объекты виртуальных компьютеров, аутентификацию Kerberos, адреса по умолчанию для служб, таких как Microsoft Message Queuing (MSMQ), применяемые для публикации пунктов управления службами. Опубликовав виртуальный кластерный сервер как объект компьютера Active Directory, вы дадите пользователям возможность работать с виртуальным сервером как с обычным Windows 2000-сервером.

  Объект компьютера, представляющий виртуальный сервер в Windows Server 2003, нужен лишь для поддержки аутентификации Kerberos для служб, размещенных на виртуальном сервере, а службам, поддерживающим кластеры и Active Directory (таким как MSMQ) он нужен для публикации сведений о провайдере сервисов, специфичных для виртуального сервера, на котором они размещаются.

- **Аутентификация Kerberos** Обеспечивает аутентификацию пользователей на сервере без пересылки его пароля. Вместо пароля пользователь «предъявляет» билет на доступ к серверу. Этим аутентификация Kerberos отличается от аутентификации NTLM, которую использует служба кластеров Windows 2000: NTLM пересылает хешкод пароля через сеть. Kerberos также поддерживает взаимную аутентификацию клиента и сервера, а также позволяет делегировать аутентификацию другим машинам. Для применения аутентификации Kerberos на виртуальном сервере, работающем в смешанном режиме (например, на сервере, состоящем из узлов под управлением Windows 2000/Server 2003), требуется Windows 2000 Enterprise Server SP3 или выше, иначе будет применяться аутентификация NTLM.
- Публикация служб Теперь служба кластеров поддерживает Active Directory и способна интегрироваться с другими службами, публикующими сведения о себе в Active Directory. Например. MSMQ 2.0 публикует информацию об открытых очередях в Active Directory, что позволяет пользователю найти ближайшую очередь. В Windows Server 2003 эта возможность дополнена поддержкой публикации в Active Directory открытых очередей, работающих на кластерных серверах, причем интеграция с кластерным сервером не влияет на схему Active Directory.

Внимание! Хотя кластерный сервер сетевых имен публикует объект компьютера в Active Directory, не используйте этот объект для решения административных задач, таких как применение групповой политики.

Ресурсы

Следующие улучшения коснулись ресурсов кластерных серверов.

- Настройка принтера Надо лишь настроить ресурс спулера при помощи Cluster Administrator и подключиться к виртуальному серверу, чтобы настроить порты и очереди печати. Это существенное улучшение по сравнению с прежними версиями службы кластеров.

- **Настройка MSDTC (Microsoft Distributed Transaction Coordinator)** Службу MSDTC теперь достаточно настроить только раз, а потом можно реплицировать настройки на все узлы кластера. Раньше для создания кластерного сервера MSDTC утилиту Comclust.exe приходилось запускать на каждом узле. Теперь можно объявить службу MSDTC ресурсом и поместить ее в группу ресурсов — это позволит автоматически настроить эту службу на всех узлах кластера. Более того. после его добавления к кластеру нового узла служба MSDTC будет сконфигурирована на нем автоматически.
- **Поддержка сценариев** Приложения можно дополнить поддержкой кластерных серверов при помощи сценариев (написанных на Visual Basic Scripting Edition или JScript) и при этом обойтись без написания DLL ресурсов на C или Visual C++. Сценарии упрощают написание ресурсов специализированных подключаемых модулей для мониторинга и управления приложениями кластерного сервера. В сценариях поддерживаются свойства, специфичные для ресурса, позволяющие хранить в сценариях ресурсов глобальные параметры конфигурации, которые можно получать и манипулировать ими, как любым другим ресурсом. Сценарии также усовершенствовали наблюдение за «здоровьем» кластера. Можно взять за основу простой стандартный сценарий и добавить к нему код, проверяющий доступность нужного сервиса.
- **Триггеры MSMQ** Служба кластеров поддерживает улучшенный тип ресурса MSMQ, допускающий существование нескольких экземпляров очереди на одном кластере. Триггеры MSMQ обеспечивают в кластере одновременную работу нескольких очередей сообщений, что повышает производительность (при использовании кластеров MSMQ в конфигурации «активный — активный») и гибкость решения. В группе кластеров может быть только один ресурс MSMQ.

Работа с сетью

В новой версии службы кластеров усовершенствована работа с сетью.

- **Улучшено восстановление после сбоев сети** Служба кластеров теперь поддерживает более совершенные алгоритмы восстановления после полной потери внутренней связи («пуль-

са»). Теперь учитывается состояние открытых сетевых интерфейсов на всех узлах. Так, если в Windows 2000 на узле А, владеющем кворумным диском, выходят из строя все сетевые интерфейсы (например, открытые сетевые интерфейсы и «пульс»), этот узел сохранит контроль над кластером, даже если ни один узел не сможет связаться с ним, а у другого узла открытый интерфейс будет функционировать. Узлы кластеров Windows Server 2003 теперь учитывают состояние открытых интерфейсов при передаче управления внутри кластера.

- Media Sense Если разрывается соединение с сетью, стек TCP/IP не выгружается, как это происходит в Windows 2000 по умолчанию, и раздел реестра DisableDHCPMediaSense теперь можно не устанавливать. В Windows 2000 при разрыве сетевого канала стек TCP/IP выгружался, и, следовательно, все ресурсы, зависимые от IP-адресов, становились недоступными. Кроме того, после восстановления соединения с сетью ресурсам возвращались значения их сетевых ролей по умолчанию, например, client и private. Если технология Media Sense по умолчанию отключена, сетевые роли сохраняются, и все ресурсы, зависимые от IP-адресов, остаются доступными.
- **Многоадресные сообщения «пульса»** Теперь поддерживается обмен многоадресными сообщениями «пульса» между узлами кластера. Эта функция автоматически включается, если кластер достаточно велик и сетевая инфраструктура поддерживает многоадресную передачу между узлами кластера. Хотя параметры многоадресной передачи можно задать вручную, типичную конфигурацию можно выставить без административных действий или дополнительной настройки. Если многоадресная передача дает сбой, внутренняя связь возвращается в режим одноадресной передачи. Все внутренние сообщения подписываются и защищаются. Многоадресная передача снижает трафик во внутренней подсети кластера. Это особенно выгодно в кластерах, состоящих из двух и более узлов, а также в географически рассредоточенных кластерах.

Внешнее хранилище

Работа с внешними запоминающими устройствами также подверглась улучшению.

- **Изменение размеров дисков кластера** Размер дисков кластерного сервера можно изменять динамически либо инструментом командной строки DiskPart (если базовая инфраструктура хранилища поддерживает динамическое изменение логической единицы хранения). Увеличение размеров общих дисков динамически учитывается службой кластеров, что особенно удобно в сетях хранения данных (SAN), где это позволяет изменять размеры томов, не допуская их переполнения.
- **Точки монтирования томов** Поддерживаются теперь и для общих дисков (кроме кворумных). При восстановлении точки монтирования работают корректно, если они были правильно настроены. В Windows 2000 и выше точки монтирования являются каталогами, которые представляют собой постоянные ссылки на заданные тома. Так, можно сделать путь C:\Data ссылкой на дисковый том. Этот механизм позволяет подключать тома, не назначая им буквы диска, и тем самым преодолеть ограничение в 26 томов, обусловленное числом букв в алфавите. Например, без точек монтирования томов подключение тома с данными потребовало бы назначить ему букву диска G. Поддержка точек монтирования службой кластеров обеспечивает гибкость при манипулировании пространствами имен общих дисков. Каталог, содержащий точку монтирования, должен быть каталогом NTFS, поскольку его базовый механизм использует точки повторного разбора NTFS, зато монтируемый том может иметь любую файловую систему — FAT, FAT32, NTFS, CDFS или UDFS.
- **Кэширование на стороне клиента** (client-side caching, CSC) Поддерживается теперь и для разделяемых хранилищ файлов кластерных серверов, позволяя клиенту кэшировать файлы, полученные из общего хранилища кластерного сервера. Клиент работает с локальной копией данных, которая после закрытия файла используется для обновления данных серверного хранилища. Это позволяет скрыть от клиента отказы узлов кластерного сервера и восстановление службы общего хранилища файлов.

- **Распределенная файловая система** (DFS) Теперь поддерживает размещение нескольких изолированных корней файловой системы в кластере, независимое восстановление корней DFS и конфигурацию «активный — активный». DFS позволяет объединить несколько общих файловых хранилищ, расположенных на разных машинах, в единое пространство имен. Так, \\dfsroot\share1 и \\dfsroot\share2 могут быть в действительности созданы на основе \\server1\share1 и \\server2\share2. Применение усовершенствованной DFS с кластерами дает следующие преимущества.
  - **Поддержка нескольких изолированных корней DFS** Прежние версии допускали размещение только одного изолированного корня DFS в кластере, теперь же их может быть несколько, что дает больше гибкости при планировании пространства имен DFS. Например, можно разместить несколько корней DFS на одном или нескольких виртуальных серверах.
  - **Независимое восстановление корней DFS** Теперь можно отдельно управлять восстановлением каждого из корней DFS, что сокращает время восстановления.
  - **Поддержка конфигурации «активный — активный»** Теперь допускается наличие нескольких изолированных корней, работающих в активном режиме на разных узлах.
- **Шифрующая файловая система** (EFS) Windows Server 2003 поддерживает EFS для общих файловых хранилищ кластерных серверов. Это позволяет хранить файлы на дисках кластерных серверов в зашифрованном виде.
- **Сети хранения данных (storage area networks,** SAN) Кластеры оптимизированы для SAN и поддерживают сброс целевого устройства и общих шин хранилища.
  - **Сброс целевых устройств** ПО кластерных серверов теперь генерирует управляющий код при освобождении дисков в результате арбитража. Этот код позволяет драйверам адаптера главной шины (Host Bus Adapter, HBA), поддерживающим расширенный набор функций Windows Server 2003, вместо полного сброса шины выборочно выполнять сброс устройств SAN. Это снижает негативный эффект активности кластерного сервера на SAN.

- **Общая шина хранилища** Общие диски могут быть подключены к шине хранилища вместе с загрузочным диском и дисками со страничными файлами и диск для сброса файлов. Это позволяет построить кластер целиком на основе единой шины хранилища (или единой избыточной шины).

По умолчанию эта функция отключена из-за ограничений, накладываемых конфигурацией. Ее могут (и должны) активизировать только производители оборудования и специализированных решений, так как она *не является* функцией общего назначения, доступной конечным пользователям.

Эксплуатация

В эксплуатации службы кластеров усовершенствованы следующие аспекты.

- **Резервное копирование и восстановление** Теперь можно выполнять активное восстановление конфигурации только на локальный узел либо на все узлы кластера. Средства восстановления узлов также встроены в Automated System Recovery (ASR).
  - **Резервное копирование и восстановление** Улучшенная утилита Backup (NTBackup.exe) поддерживает бесшовное копирование и восстановление БД локального кластера, что позволяет восстанавливать конфигурацию на локальном узле либо на всех узлах кластера.
  - **Автоматическое восстановление системы (ASR)** Позволяет полностью восстановить кластер в самых разных ситуациях, скажем, при повреждении или потере системных файлов, полной переустановке ОС или при отказе оборудования, а также при повреждении БД кластера или изменении сигнатуры дисков (включая общие).
- **Поддержка связывания групп (group affinity)** Позволяет приложению описать себя как «приложение N + I». Это значит, что, если приложение активно на N узлах кластерного сервера, I резервных узлов останется для замены отказавших активных узлов. При отказе активного узла диспетчер восстановления попытается перевести приложение на резервный узел. При миграции приложений при восстановлении

после сбоев резервные узлы имеют приоритет перед активными узлами.

- **Вывод узлов из кластера** Теперь вывод узлов из кластерного сервера не требует перезагрузки для очистки состояния кластерного сервера. Перемещать узлы из одного кластера в другие тоже можно без перезагрузки. При катастрофическом отказе конфигурацию кластерного сервера можно очистить принудительно независимо от его состояния. Это обеспечивает повышенную доступность (исключение перезагрузки сокращает время простоя) и восстановление после катастрофических сбоев (при отказе узлов легко очистить состояние кластера).
- **Веерное обновление (rolling upgrade)** Позволяет поочередно отключать узлы кластера для обновления их ПО, тогда как остальные узлы продолжают работать под управлением прежней версии ПО. Веерное обновление поддерживается в Windows 2000/Server 2003. Однако этот метод не поддерживается для обновления кластеров Windows NT 4.0 до Windows Server 2003 — при этом придется отключить кластер на время обновления.
- **Изменение паролей** Windows Server 2003 позволяет изменять пароль доменной учетной записи службы кластеров, а также учетных записей этой службы на локальных узлах, не отключая кластера. Если несколько кластеров используют одну учетную запись, пароль для них можно изменить одновременно. В Windows NT 4.0/2000 для изменения пароля учетной записи службы кластеров требовалось остановить ее на всех узлах.
- **Удаление ресурсов** Выполняется через Cluster Administrator или Cluster.exe без их предварительного отключения — теперь служба кластеров отключает их автоматически;
- WMI поддерживается для:
  - **функций управления кластером и его ресурсами:** запуска, остановки и создания новых ресурсов и зависимостей и др.;
  - **управления сведениями о состоянии приложения и кластера:** WMI позволяет запрашивать состояние приложения и узлов кластера (работают ли они) и получать массу других сведений о статусе кластера;

- **D событий, связанных с изменением состояния кластера: это** позволяет приложениям подписываться на получение событий WMI, уведомляющих о сбое и перезапуске приложения, отказе узлов и других происшествиях;
- **управления** кластерными серверами как компонентами окружения WMI.

Техническая поддержка и устранение неполадок

Следующие улучшения были сделаны в сфере поддержки и устранения неполадок службы кластеров.

- **Коды причины отключения или сбоя** Позволяют получить сведения о причине отключения/сбоя приложения, а также автоматически перевести группу на определенный узел при сбое данного приложения либо одного из зависимых от него приложений.
- **Трассировка программ** Новая функция службы кластеров, *трассировка программ* (software tracing), позволяет собирать больше сведений, полезных для устранения неполадок кластеров. Она представляет новый метод отладки, благодаря которому Microsoft сможет отлаживать службу кластеров без загрузки проверочных версий ОС или DLL (символов),
- **Усовершенствования журналов кластеров**
  - **журнал установки** %SystemRoot%\system32\Logfiles\Cluster\ClCfgSrv.log, создаваемый при установке службы кластеров, содержит сведения, полезные для устранения неполадок;
  - **п уровни ошибок** (info, warn, err) позволяют легко выделить только те записи журнала, что требуют вмешательства, например, записи, отражающие ошибки (*err*);
  - **а отметка времени локального сервера** облегчает сравнение записей журнала событий с журналами кластера.
- **Журнал событий** Хранит записи о событиях, связанных с ошибками и успешной миграцией ресурса между узлами, поддерживает синтаксический анализ и поиск записей об успешной миграции (а не только о катастрофических отказах) при помощи управляющих инструментов.
- **Clusdiag** Этот инструмент из пакета Windows Server 2003 Resource Kit обеспечивает:

- **более удобное устранение неполадок:** Clusdiag облегчает чтение и сравнительный анализ журналов отдельных узлов кластера, а также устранение неполадок кластерных серверов;
- **проверку и тестирование:** пользователи смогут проводить нагрузочное тестирование серверов, запоминающих устройств и инфраструктуры кластеров; Clusdiag можно применять как средство проверки и тестирования кластера перед его сдачей в эксплуатацию.

- **Журнал утилиты CHKDSK** Служба кластера создает журнал CHKDSK каждый раз, когда эта утилита запускается для проверки общего диска. Это позволяет администратору выявлять проблемы и соответствующим образом на них реагировать.
- **Повреждение диска** При подозрении на повреждение диска служба кластеров записывает результаты, переданные ей **CHKDSK,** в журнал событий и создает журнал в каталоге %SystemRoot%\Cluster. Результаты регистрируются в журнале событий приложения. Cluster.log также ссылается на файл журнала (например, на %windir%\CLUSTER\CHKDSK_DISK2_SIGE9443789.LOG), куда записывается подробный вывод CHKDSK.

Новые возможности NLB

Среди усовершенствований кластерных технологий отметим разнообразные сценарии и топологии NLB.

Диспетчер NLB

Чтобы создать в Windows 2000 кластер, поддерживающий балансировку нагрузки на сеть (Network Load Balancing, NLB), пользователю приходилось настраивать все компьютеры кластера по отдельности. Новая утилита Network Load Balancing Manager (диспетчер сетевой нагрузки) позволяет:

- создавать новые кластеры с NLB и автоматически реплицировать параметры настройки и правила портов на все или на отдельные узлы кластера;
- добавлять и удалять узлы из кластеров с NLB;
- автоматически регистрировать IP-адрес кластера в **TCP/IP;**

- управлять существующими кластерами, просто подключаясь к ним либо загружая описание узлов из файла и сохраняя его в файл для дальнейшего использования;
- настраивать NLB для распределения нагрузки между Web-сайтами и приложениями, развернутыми на одном кластере с NLB (регистрировать все IP-адреса кластера в TCP/IP и управлять трафиком определенных приложений, работающих на заданном узле);
- диагностировать неправильно настроенные кластеры.

Виртуальные кластеры

В Windows 2000 пользователи настраивали балансировку нагрузки между Web-сайтами и приложениями, развернутыми на одном кластере с NLB, регистрируя их IP-адреса в TCP/IP на каждом из узлов кластера. Это было возможно, поскольку на каждом узле NLB балансирует трафик для всех IP-адресов, зарегистрированных в TCP/IP, кроме IP-адресов внутренней сети кластера. Вследствие этого в Windows 2000 действовали ограничения:

- правила портов, заданные для кластера, автоматически применялись ко всем Web-сайтам и приложениям, балансировку нагрузки на которые выполнял кластер;
- все узлы кластера должны были обрабатывать трафик, генерированный всеми Web-сайтами и приложениями, размещенными на нем;
- чтобы блокировать трафик, генерированный определенным приложением, размещенным на некотором узле, приходилось блокировать трафик всех приложений, размещенных на этом узле.

Новая функция — *виртуальные кластеры* (virtual clusters) — снимает эти ограничения, позволяя задавать для каждого IP-порта свои правила. Это дает возможность:

- определять правила для IP-адресов кластера, где каждый IP-адрес кластера представляет Web-сайт или приложение, развернутое на кластере с NLB; в Windows 2000 правила портов применялись ко всему узлу, а не к определенным IP-адресам этого узла;

- фильтровать входящий трафик определенного Web-сайта или приложения, размещенного на некотором узле кластера, что позволяет выборочно отключать приложения, размещенные на отдельных узлах для обновления, перезапуска и иных целей, не затрагивая другие приложения, обслуживаемые кластером NLB;
- задавать узел, который должен обслуживать входящий трафик определенного Web-сайта или приложения, при этом не обязательно, чтобы все узлы кластера обрабатывали трафик всех приложений, размещенных на этом кластере.

Поддержка нескольких сетевых плат

В Windows 2000 пользователи могли привязывать NLB лишь к одной сетевой плате, установленной в системе. В Windows Server 2003 можно привязывать NLB к нескольким сетевым платам, что позволяет:

- развертывать несколько кластеров с NLB на одних и тех же узлах, но в совершенно независимых сетях; это достигается путем привязки NLB к разным сетевым платам, установленным в одной системе;
- применять NLB для распределения нагрузки на сеть по разные стороны прокси или брандмауэра.

Двусторонняя привязка NLB

Поддержка нескольких сетевых плат сделала возможным сценарии, требующие балансировки нагрузки как во внутренней. так и во внешней сетях кластера с NLB. Предполагается, эта функция будет применяться в основном в кластерных серверах Internet Security and Acceleration (ISA), требующих балансировки нагрузки на прокси и брандмауэры. Чаще всего NLB будет применяться вместе с ISA в таких целях.

- Публикация данных в Web Кластерный сервер ISA обычно располагается между Интернетом и внешними Web-серверами. В этом сценарии NLB привязана только к внешнему сетевому интерфейсу сервера ISA, поэтому здесь нет необходимости в двусторонней привязке NLB,
- Публикация серверов Кластерный сервер ISA располагается между внешними Web-серверами и внутренними сер-

верами, которые нужно опубликовать. Здесь NLB привязан как к внешнему (соединенному с Web-серверами), так и к внутреннему интерфейсу (соединенному с публикуемыми серверами) каждого узла кластерного сервера ISA.

Второй сненарий сложнее: распределение нагрузки, генерируемой соединениями с Web-серверами, осуществляется на внешнем интерфейсе кластерного сервера ISA, после этого каждый сервер ISA передает свою часть трафика от Web-серверов к публикуемому внутреннему серверу. Служба NLB должна гарантировать передачу отклика публикуемого сервера только тому серверу JSA, что обрабатывал запрос Web-сервера, вызвавшего этот отклик. Это необходимо, так как только этот сервер ISA из всего кластера обладает контекстом безопасности данного сеанса. То есть NLB должна гарантировать, что отклик публикуемого сервера не будет подвергаться распределению на внутреннем интерфейсе кластерного сервера ISA, поскольку он также привязан к NLB кластера ISA.

Двусторонняя привязка обеспечивает парную работу экземпляров NLB, которые функционируют на одном узле для маршрутизации откликов публикуемых серверов через соответствующие узлы кластерного сервера ISA.

Ограничение лавинообразной передачи с помощью IGMP

Алгоритм NLB требует, чтобы каждый узел кластера с NLB «видел» все входящие пакеты, адресованные кластеру. Это достигается при помощи коммутатора, которому запрещают связывать MAC-адрес кластера с определенным своим портом. Однако у этого метода есть побочный эффект: в конце концов порты коммутатора блокируются лавинообразным трафиком из входящих пакетов, адресованных кластеру с NLB. Чтобы решить эту проблему, в Windows Server 2003 введена поддержка протокола IGMP (Internet Group Management Protocol).

IGMP ограничивает лавинообразную передачу, направляя адресованные NLB пакеты только к тому порту, к которому подключены серверы с NLB. Так что машины без NLB не «видят» трафик, предназначенный исключительно кластерному серверу с NLB, тогда как все машины кластера с NLB «видят» адресованный им трафик. Это позволяет выполнить требова-

ния алгоритма. Поддержку IGMP можно активизировать, только когда NLB работает в режиме многоадресной передачи.

Однако у этого режима есть свои недостатки, которые в деталях обсуждаются в соответствующих статьях базы знаний Microsoft, доступных на сайте Microsoft.com.

Коммутатор можно разгрузить, применив режим одноадресной передачи, лишенный недостатков режима многоадресной передачи. Для этого надо создать в коммутаторе VLAN и поместить кластерный сервер с NLB в отдельной VLAN.

Архитектура кластерного сервера

Кластерные серверы базируются на архитектуре кластера без разделения ресурсов. Эта модель описывает способ управления серверами кластера, локальными и общими устройствами и ресурсами кластера.

Кластеры без разделения ресурсов

В кластерах, построенных на основе модели без разделения ресурсов, каждый сервер владеет и управляет лишь своими локальными устройствами. Устройства, общие для кластера, например, дисковые массивы и сетевая среда, управляются серверами кластера по очереди, причем в каждый момент времени ими может управлять только один сервер.

Подобная модель облегчает управление дисковыми устройствами и стандартными приложениями. Она не требует специальных соединений или приложений, но позволяет кластерным серверам поддерживать стандартные приложения и дисковые ресурсы Windows Server 2003/2000.

Локальные запоминающие устройства и соединения с сетевой средой

Кластерные серверы используют стандартные драйверы локальных запоминающих устройств и сетевых соединений Windows Server 2003/2000 Server и поддерживают несколько видов сетевой среды для подключения внешних общих устройств, которые должны быть доступны всем серверам кластера.

Внешние запоминающие устройства, общие для кластера, должны поддерживать спецификацию SCSI и стандартные подключения через PCI и Fibre Channel, а также шину SCSI с не-

сколькими инициаторами. Устройства, подключенные через волоконно-оптические каналы, тоже являются устройствами SCSI. только они подключены через шину Fibre Channel, а не SCSI. Концептуально технология Fibre Channel инкапсулирует команды SCSI, поэтому кластерные серверы могут использовать поддерживаемые ими команды SCSI (Reserve/Release, **Bus** Reset), которые одинаково работают через стандартные и волоконно-оптические каналы,

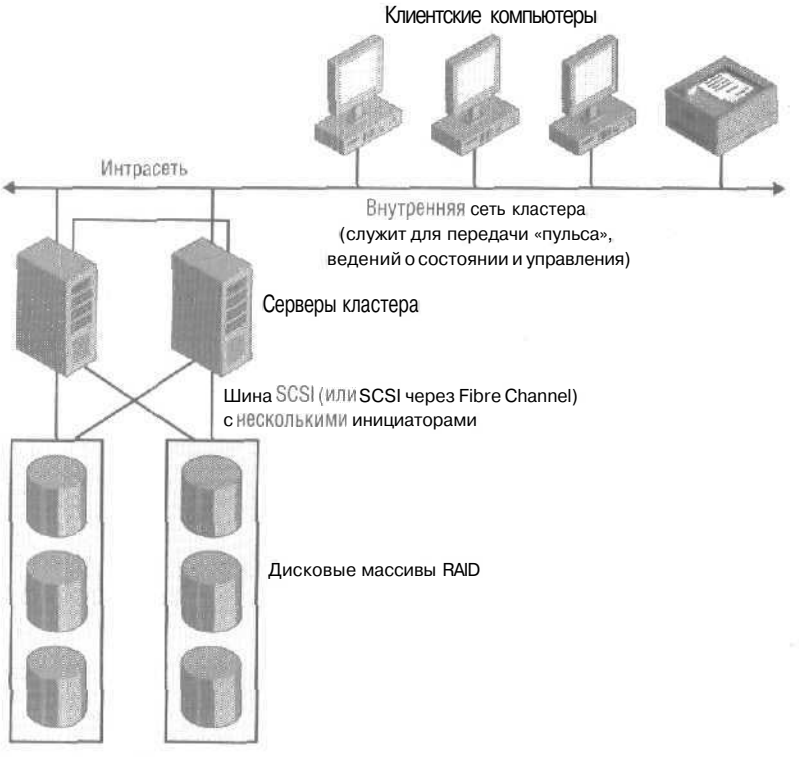


Рис. 13-1. Схема кластерного сервера из двух узлов, работающего под управлением Windows Server 2003, Enterprise Edition

На рис. 13-1 показаны компоненты кластерного сервера, состоящего из двух узлов. Узлами такого кластера могут быть серверы с Windows Server 2003, Enterprise Edition/2000 Enterprise Server. Через канал SCSI (либо SCSI через Fibre Channel) к

кластеру подключено внешнее общее запоминающее устройство.

Windows Server 2003 Datacenter Edition поддерживает кластеры размером 2-8 узлов и требует подключения устройств через Fibre Channel (рис. 13-2).

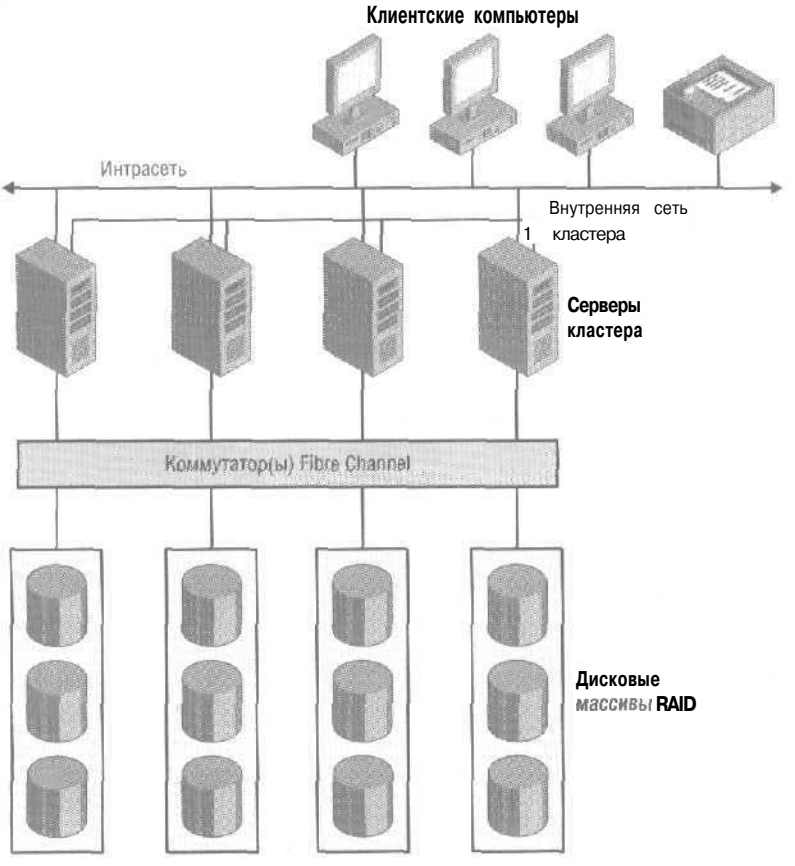


Рис. 13-2. Схема кластерного сервера из четырех узлов, работающего под управлением Windows Server 2003, Datacenter Edition

Виртуальные серверы

Одно из преимуществ кластерных серверов в том, что работающие на них приложения и службы можно опубликовать для пользователей и рабочих станций в виде виртуальных серверов с такими характеристиками,

- Физическая структура Для пользователей и клиентов подключение к приложению или службе, работающей как виртуальный кластерный сервер, не отличается от подключения к обычному физическому серверу. На самом деле соединение с виртуальным сервером может обслуживать любой из узлов кластера. Пользователь или клиентское приложение не знают, какой из узлов кластера обслуживает виртуальный сервер. Службы и приложения, не предназначенные для клиентов, можно не публиковать в виде виртуальных серверов. В кластере может быть несколько виртуальных серверов, представляющих различные приложения (рис. 13-3).

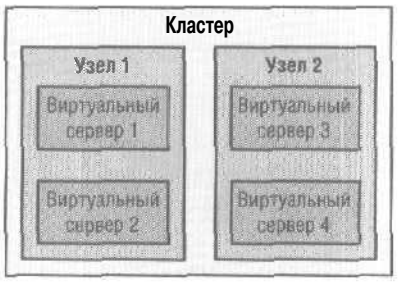


Рис. 13-3. Схема физической организации виртуальных серверов на кластерном сервере

На рис. 13-3 показан кластерный сервер из двух узлов с четырьмя виртуальными серверами, по два на каждом узле. Кластерный сервер управляет виртуальными серверами как группой ресурсов. В каждой группе ресурсов, представляющей виртуальный сервер, содержится два ресурса: IP-адрес и соответствующее ему сетевое имя.

- **Вид виртуального сервера со стороны клиента** Соединения с клиентами и клиентскими приложения осуществляются как сеансы, которые «знают» лишь IP-адрес виртуального сервера, опубликованный службой кластеров. Для клиента

это просто обычная пара из сетевого имени и IP-адреса, Кластерный сервер из двух узлов с виртуальными серверами (рис. 13-3) с точки зрения клиента показан на рис. 13-4: клиент «видит» только IP-адреса и имена виртуальных серверов, а не физические адреса узлов. Это позволяет кластерным серверам обеспечивать высокую доступность приложений, работающих как виртуальные серверы.

Рис. 13-4. Вид виртуальных серверов, размещенных на кластерном сервере, со стороны клиента

- **Отказ приложений и серверов** В случае отказа приложения или сервера служба кластеров перемешает всю группу ресурсов виртуального сервера на другой узел кластера. Для клиента отказ проявляется как сбой сеанса работы с приложением. При этом клиент пытается восстановить соединение с приложением так же. как он устанавливал исходное соединение. Эта попытка оканчивается успехом, так как в ходе восстановления после сбоя служба кластеров просто связывает IP-адрес виртуального сервера с физическим адресом одного из «выживших» узлов. Таким образом, клиенту не требуется физический адрес узла, на котором размешается приложение, чтобы восстановить соединение.

  Хотя этот метод обеспечивает высокую доступность приложений и служб, состояние сбойного сеанса теряется, если только приложение не хранит данных клиентских сеансов на диске, откуда их можно извлечь при восстановлении, Кластерные серверы обеспечивают высокую доступность, но не отказоустойчивость: это забота самого приложения, которое может достичь ее путем применения транзакций.

  Примером приложения, хранящего данные о клиентах и поддерживающего восстановление сеансов, может быть служба DHCP. IP-адреса, выделенные этой службой клиентам,

сохраняются в БД DHCP. При отказе ресурса DHCP-сервера, можно перевести БД DHCP на доступный узел кластера и перезапустить сервис DHCP-сервера, передав ему клиентские данные, извлеченные из БД DHCP.

Ресурсы

Ресурс представляет физический объект или экземпляр исполняемого кода: диск, IP-адрес, очередь MSMQ, объект COM и т. п. С точки зрения управления, ресурсы — это единицы, которые можно запускать и останавливать независимо друг от друга. С точки зрения службы кластеров, ресурс может находиться в одном из состояний:

- **Off line** — ресурс отключен/не обслуживается;
- **Started** — ресурс загружен в память, и диспетчер ресурсов может подключить его в любой момент;
- **On line** — ресурс корректно функционирует и способен обслуживать запросы;
- **Failed** — ресурс вышел из строя и не может быть перезапущен.

Ресурсы и зависимости

Как уже говорилось, приложение состоит из нескольких компонентов, представляющих его код и физические ресурсы. Между этими компонентами существуют различные связи. Так, нельзя подключить приложение, записывающее данные на диск, пока диск не станет доступным. Если же диск вышел из строя, то работа приложения не может продолжаться по определению — ведь ему нужно записывать данные на диск.

Зависимости отражают связи между ресурсами. На рис. 13-5 видно, что у ресурса SQL есть зависимость, определяющая порядок запуска: SQL зависит от ресурсов диска и сетевого имени. В свою очередь ресурс сетевого имени зависит от ресурса IP-адреса. Если пользователь попытается подключить ресурс SQL, когда отключены ресурсы IP-адреса и сетевого имени, а ресурс диска подключен, первым будет подключен ресурс IP-адреса, а затем ресурс сетевого имени и, наконец, ресурс SQL. Порядок запуска ресурсов, не связанных зависимостями (таких как сетевое имя и диск на рис. 13-5), не определен. Такие ресурсы могут запускаться одновременно.

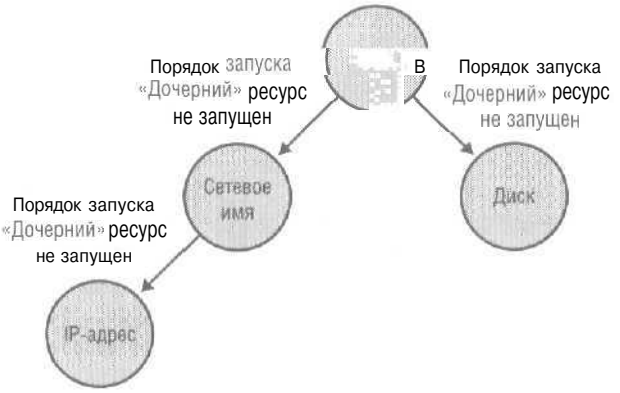


Рис. 13-5. Схема зависимостей между ресурсами

Набор ресурсов, управляемых и отслеживаемых как единое целое, называется группой ресурсов. При запуске группы запускаются все составляющие ее ресурсы с учетом определенного для них порядка запуска. При остановке останавливаются и все составляющие ее ресурсы. Зависимости между ресурсами не могут выходить за пределы группы. Иначе говоря, ресурсы, составляющие группу, представляют собой неделимую автономную единицу, которая может быть запущена/остановлена независимо от другой группы. В окружении кластера группа может располагаться только на одном узле. В кластерах, поддерживающих приложения с автоматическим восстановлением после сбоев, группа также является единицей восстановления (рис. 13-6).

Группа ресурсов — это логический набор ресурсов кластера. Обычно в группу объединяют логически связанные ресурсы, например, приложения с его устройствами и данными. Однако группа не может состоять только из ресурсов, предназначенных только для административных задач, таких как внутренний набор имен и IP-адресов виртуальных серверов. В каждый момент времени группа может принадлежать только одному узлу, и, напротив, составляющие одну группу ресурсы не могут принадлежать разным узлам,

С каждой группой ресурсов связана глобальная политика. которая задает предпочитаемый сервер для запуска этой группы, а также сервер, на который она мигрирует при отказе предпочитаемого узла. У каждой группы есть имя сетевой службы и адрес, необходимые для привязки сетевых клиентов к службам.

При отказе узла можно восстановить группу, переместив на доступный узел кластера.

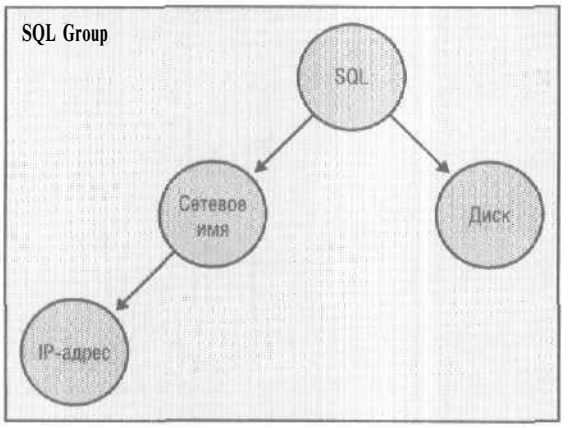


Рис. 13-6. Схема ресурсов, составляющих группу SQL Group

Любой ресурс группы может зависеть от других ресурсов. Зависимости — это связи между ресурсами, определяющие, какие ресурсы запустить в первую очередь, чтобы сделать их доступными, прежде чем будет запущен другой ресурс. Так, приложение БД может зависеть от доступности диска, IP-адреса и сетевого имени. которые требуются ему, чтобы запуститься и начать обслуживание других приложений и клиентов. Зависимости между ресурсами определяются через свойства группы ресурсов кластера и позволяют службе кластера управлять порядком подключения/отключения ресурсов. Область действия любой зависимости не может выходить за пределы группы, так как группы подключаются/отключаются независимо.

Политики миграции при сбоях

Миграция при сбое обеспечивает высокую доступность приложений, работающих в виде одного экземпляра, а также отдельных экземпляров разделенных приложений [высокодоступные приложения, работающие в одном экземпляре, и экземпляры общих приложений обозначают термином *пакет* (pack)]. Для кластера, состоящего из двух узлов, политика миграции тривиальна: при отказе одного из узлов остается лишь передать

его функции оставшемуся узлу. По мере роста кластера становятся возможными различные политики.

- **Миграция в паре** В большом кластере можно назначить каждому узлу с приложением резервный узел. При отказе первого узла его функции передаются резервному узлу. На рис. 13-7 пример показан пример кластера из четырех узлов с двумя приложениями (App1 и App2).

Рис. 13-7. Схема миграции двух приложений в кластере из четырех узлов

Эта конфигурация:

- □ подходит для кластеров, поддерживающих требовательные к ресурсам приложения, и гарантирует, что при отказе приложение мигрирует на другой узел;
- □ позволяет легко планировать производительность: производительность узлов пары определяется развернутым на них приложением (как для кластера из двух узлов с одним приложением);
- П позволяет легко прогнозировать влияние отказа узлов на доступность и производительность системы;
- П обеспечивает гибкость, сравнимую с таковой крупного кластера: при отключении резервного узла для технического обслуживания приложению автоматически назначается другой резервный узел (buddy), что может потребовать определения политики замены узлов (см. ниже);

- требует только половины мощности кластера;
- при отказе нескольких узлов требует вмешательства администратора.

Во всех версиях Windows кластерные серверы с парами узлов поддерживаются через список возможных владельцев, определяемый для каждого ресурса. В этом случае список ограничивают узлами, составляющих данную пару.

- Сервер для «горячей» замены Для снижения издержек, связанных с парной конфигурацией, можно объединить резервные узлы всех пар с образованием *сервера для «горячей» замены,* способного принимать на себя функции отказавших узлов (рис, 13-8).

Рис. 13-8. Кластер, использующий миграцию на сервер для «горячей» замены

Конфигурация, использующая сервер «горячей» замены:

- оптимальна для кластеров, поддерживающих требовательные к ресурсам приложения, такие как БД, и гарантирует, что при одиночном отказе на резервном узле будет не больше одного приложения;
- позволяет легко планировать производительность: размер узла определяется приложением, которое он будет обслу-

живать; производительность резервного узла должна быть максимальной среди всех узлов кластера;

- □ позволяет легко прогнозировать эффект отказа узлов на доступность и производительность системы;
- D оптимизирована для восстановления после сбоя одного узла;
- п плохо справляется с множественными отказами, что чревато проблемами в ситуации, когда резервный узел отключают на плановое обслуживание.

Служба кластеров Windows поддерживает резервные серверы, комбинируя списки возможных и предпочитаемых владельцев. Предпочитаемым узлом должен быть узел, на котором приложение работает по умолчанию, а возможными владельцами данного ресурса должны быть оба узла – предпочитаемый и резервный.

- Конфигурация N + I Сервер «горячей замены» хорошо работает в кластерах из четырех узлов с некоторыми конфигурациями, но плохо справляется с множественными отказами. Конфигурации типа N+I являются расширением концепции серверов горячей замены. При использовании такой конфигурации на *N* узлах размещаются приложения, а / узлов остаются в резерве (рис. 13-9).

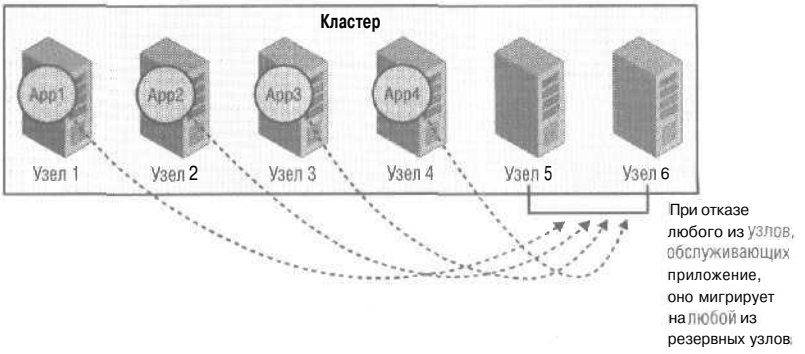


Рис. 13-9. Конфигурация кластера типа N+I

Конфигурация N+I:

- п **оптимальна для кластеров, поддерживающих** требовательные **к ресурсам приложения, такие** как **БД** и Microsoft

Exchange, и гарантирует, что при отказе экземпляр приложения мигрирует только на свободный резервный узел:

- позволяет легко планировать производительность: размер узла определяется приложением, которое он будет обслуживать;
- позволяет просто прогнозировать эффект отказа узлов на доступность и производительность системы;
- хорошо справляется с множественными отказами;
- плохо подходит для размещения разных приложений и оптимальна для кластеров, обслуживающих одно приложение.

В Windows Server 2003 служба Windows Clustering поддерживает кластеры типа N+I при помощи открытого свойства группы кластера *AntiAffinityClassName*. Это свойство содержит произвольную символьную строку. При отказе диспетчер перевода ресурсов проверяет свойство *AntiAffinityClassName* и, обнаружив, что оно не пусто, переходит к другому узлу.

Узел же, указанный в списке потенциальных владельцев данного ресурса, расположенный *вне* группы с идентичным значением свойства *AntiAffinityClassName* рассматривается как подходящий кандидат на замену отказавшего узла.

- Миграция по кругу (**failover** ring) Позволяет любому из узлов кластера обслуживать экземпляр приложения, при отказе приложение мигрирует с него на следующий узел кольца (рис. 13-10).

Конфигурация с миграцией по кругу:

- оптимальна для кластеров, поддерживающих несколько экземпляров небольших приложений, когда производительности узлов хватает для одновременного обслуживания нескольких экземпляров таких приложений;
- позволяет легко предсказать влияние отказа узла на производительность системы;
- позволяет легко спланировать производительность для восстановления после одиночного отказа;
- не всегда справляется с множественными отказами: если отказывает узел 1, узлу 2 придется обслуживать два экземпляра приложения, а узлу 3 и 4 — по одному, если же откажет и узел 2, то третьему придется обслуживать

три экземпляра приложения, тогда как на долю узла 4 по-прежнему останется один экземпляр;

- плохо подходит для приложений, требовательным к ресурсам, так как на одном (даже сильно загруженном) узле может оказаться несколько экземпляров приложения.

Конфигурация с миграцией по кругу поддерживается Windows Server 2003 посредством определения порядка миграции при отказе для данной группы ресурсов, применяя список предпочитаемых владельцев. Следует определить порядок узлов, затем создать список предпочитаемых узлов, в котором каждой группе будет назначен предпочитаемый узел, отличный от текущего.

Рис. 13-10. Схема кластера с миграцией по кругу

- Миграция на случайный узел В больших (и не очень) кластерах, обслуживающих несколько приложений, определить отдельные целевые узлы и политики миграции для каждого экземпляра приложения очень трудно, что чревато ошибками. Самое лучшее в таких случаях — разрешить миграцию на случайный узел, при этом согласно статистике дополнительная нагрузка, возникающая при отказах, будет равномерно распределяться между оставшимися узлами кластера.

Миграция **на случайный узел:**

- оптимальна для кластеров, поддерживающих несколько экземпляров небольших приложений, когда производительности узлов хватает для одновременного обслуживания нескольких экземпляров таких приложений;
- освобождает администратора от выбора узла, на который следует перевести приложение в случае отказа;
- если приложений или экземпляров общего приложения достаточно много, этот механизм в силу статистических закономерностей обеспечивает равномерное распределение дополнительной нагрузки, возникающей при отказах;
- хорошо справляется с множественными отказами;
- оптимальна для обслуживания нескольких приложений (нескольких экземпляров одного) на одном кластере;
- затрудняет планирование производительности, поскольку нет реальной гарантии равномерного распределения нагрузки;
- не позволяет легко предсказать влияние отказа узла на производительность;
- плохо подходит для обслуживания требовательных к ресурсам приложений, поскольку на одном узле, даже сильно загруженном, может оказаться несколько экземпляров приложения.

Служба Windows Clustering поддерживает случайный выбор целевого сервера для миграции при отказе узлов. Так выбирается целевой узел для каждой группы ресурсов, чей список предпочитаемых владельцев пуст.

- Специализированный порядок миграции Иногда при отказе приложение лучше перевести на известный узел, явно задав его в конфигурации приложения. Специализированный порядок миграции:
  - дает администратору полный контроль над тем, что происходит при отказе;
  - позволяет легко планировать производительность, так как события при отказе узлов предсказуемы;
  - затрудняет выбор оптимальной политики миграции, если кластер обслуживает несколько приложений;

- усложняет планирование миграции при множественных взаимообусловленных отказах,

Список предпочитаемых узлов

Служба кластеров Windows предоставляет полный контроль над порядком миграции через *список предпочитаемых узлов* (preferred node list) (табл. 13-1).

Табл. 13-1. Список предпочитаемых узлов

Содержимое списка	Если перемещение группы в раздел *Best Possible* инициирует администратор...	Если происходит отказ **узла** или группы...
Все узлы кластера	... группа мигрирует на доступный функционирующий узел кластера, расположенный в начале списка.	... группа мигрирует на следующий узел в списке.
Подмножество узлов кластера	... группа мигрирует на доступный функционирующий узел кластера, расположенный в начале списка. ... если ни один из узлов, указанных в списке, недоступен, группа мигрирует на случайный узел.	... группа мигрирует на следующий узел в списке. ... если узел, на котором размещалась группа, был последним в списке или отсутствовал в нем, группа мигрирует на случайный узел.
Список пуст	... группа мигрирует на случайный узел.	... группа мигрирует на случайный узел.

Архитектура NLB

Этот раздел посвящен описанию архитектуры службы Network Load Balancing (NLB) из Windows Server 2003. В нем рассматриваются:

- работа NLB;
- управление сведениями о состоянии приложения;
- **архитектура NLB;**
- доставка трафика в кластере;
- алгоритм балансировки нагрузки;

- **перекличка;**
- **удаленное** управление.

Работа NLB

Служба NLB обеспечивает масштабирование серверных программ, таких как Web-серверы, равномерно распределяя клиентские запросы между узлами кластера. При использовании NLB каждый входящий пакет IP передается всем узлам, но принимает его тот узел, который должен его обработать. Узлы кластера обрабатывают клиентские запросы одновременно, включая запросы, присланные одним клиентом. Так, если Web-браузер загружает страницу с несколькими изображениями, эти изображения могут быть предоставлены разными узлами кластера. Такой подход ускоряет обработку и ускоряет генерацию отклика.

Для каждого узла в NLB можно определить долю общей нагрузки (в %), которую он в состоянии обработать, либо задать равномерное распределение нагрузки по узлам. Серверы с NLB используют распределенный алгоритм, основанный на статистическом распределении нагрузки по узлам кластера согласно заявленному ими участию в обработке общей нагрузки. При таком методе балансировки нагрузка на узлы динамически изменяется по мере подключения/отключения узлов.

Колебания загруженности сервера (например, изменение утилизации процессора и памяти) на балансировку не влияют. В случае приложений, обслуживающих многочисленных клиентов и обрабатывающих сравнительно короткоживущие запросы (такие как Web-серверы), статистический алгоритм работает эффективно и обеспечивает равномерное распределение нагрузки и быстро реагирует на изменения состава кластера.

Кластерные серверы с NLB передают в сеть особые пакеты, адресованные другим узлам кластера («пульс»), и сами принимают подобные пакеты от других узлов (слушают их «пульс»). При отказе одного из серверов кластера остальные перераспределяют между собой дополнительную нагрузку, не прерывая обслуживание клиентов.

Соединения с отказавшим узлом разрываются, но Интернет-службы при этом остаются доступными. Как правило (например, в случае Web-сервера), клиентское ПО пытается автома-

тически восстановить прерванное подключение, в результате клиенты замечают лишь небольшую задержку отклика.

Управление состоянием приложений

Состоянием (state) приложений называют данные, которые серверное приложение поддерживает для своих клиентов. Если серверное приложение (скажем, Web-сервер) поддерживает состояние клиентского сеанса, включающего несколько TCP-соединений, важно направлять все эти соединения на один узел кластера. Пример такого состояния — корзина покупателя на сайте электронной коммерции и состояние SSL. NLB поддерживает масштабирование приложений, управляющих состоянием сеансов, которые включают несколько соединений.

Если установлен параметр привязки клиента NLB, служба балансировки направляет все TCP-соединения для этого клиента на один узел кластера. Это позволяет хранить состояние сеанса в памяти этого узла. Если во время сеанса произойдет сбой сети или отказ сервера, клиенту может потребоваться заново регистрироваться в системе, повторно пройти аутентификацию и восстановить состояние сеанса. При добавлении к кластеру нового узла часть трафика, генерированного клиентами, будет направлена новому узлу. Добавление узла отразится на обслуживании сеансов, но не на существующих TCP-соединениях.

Клиент-серверным приложениям, хранящим состояние клиента в форме, доступной любому узлу кластера (например, внедряя его в cookie-файлы или записывая в серверную БД), привязка клиентов к NLB не нужна.

NLB дополнительно облегчает поддержку состояния сеансов посредством необязательных параметров привязки клиентов. Эти параметры позволяют направлять все клиентские запросы, присланные с IP-адресов из одного диапазона класса C, на один и тот же узел кластера. Благодаря этому TCP-соединения клиентов, использующих несколько прокси-серверов, можно направлять на один узел кластера.

Применение нескольких прокси-серверов на сайте клиента имитирует ситуацию, когда клиентские запросы приходят из разных систем. Если адреса всех клиентских прокси-серверов находятся в одном диапазоне адресов класса C (такой диапа-

зон содержит 254 адреса), NLB обеспечивает обработку сеансов этих клиентов на одном узле кластера, сводя к минимуму влияние на распределение нагрузки между узлами кластера. Очень крупные клиентские сайты могут использовать прокси-серверы, чьи адреса расположены в разных диапазонах адресов класса C.

Помимо состояния сеансов, серверные приложения часто поддерживают сведения о состоянии в постоянном серверном хранилище; данные в этом хранилище обычно обновляются посредством клиентских транзакций. Пример — инвентарная база данных на сайте электронной коммерции.

NLB не предназначена для непосредственного обращения приложений, независимо обновляющих состояние клиентов, поскольку обновления, сделанные таким образом на одном из узлов кластера, не будут видимы на других узлах. Таким приложением, является, например, SQL Server (кроме случаев, когда его БД открыты только для чтения).

Для использования NLB должен поддерживаться одновременный доступ нескольких экземпляров приложения к общему серверу БД, который синхронизирует обновления. Так, Web-серверу ASP нужно записывать обновленные клиентские данные в общую серверную базу данных.

Подробный обзор архитектуры NLB

Для достижения максимальной пропускной способности и высокой доступности в NLB применяется полностью распределенная архитектура. В параллели с каждым узлом кластера работает несколько идентичных копий драйверов NLB.

Эти драйверы позволяют всем узлам кластера, расположенным в одной подсети, параллельно обрабатывать входящий трафик, направленный на основные IP-адреса кластера (в случае многосетевых узлов и на дополнительные IP-адреса). Для каждого узла драйвер NLB выполняет функцию фильтра, размещенного между драйвером сетевой платы и стеком TCP/IP, который позволяет узлу принимать лишь часть входящего трафика. Так осуществляется распределение входящих клиентских запросов и балансировка нагрузки на узлы кластера.

NLB работает как сетевой драйвер, расположенный в логической схеме ниже высокоуровневых прикладных протоколов, таких как HTTP и FTP. На рис. 13-11 показана схема реализа-

ции NLB в виде промежуточного драйвера сетевого стека Windows 2000. Такая архитектура выбрана для достижения следующих целей.

- **Максимальная пропускная способность** Достигается посредством применения подсетей с широковещательной передачей для доставки входящего сетевого трафика всем узлам кластера и исключения маршрутизации входящих пакетов отдельным узлам кластера. Поскольку фильтрация пакетов работает быстрее маршрутизации (которая требует получения, анализа и ретрансляции пакетов), NLB обеспечивает более высокую пропускную способность сети по сравнению с решениями на основе диспетчеров,

  По мере роста скорости сетей и северов пропорционально возрастает пропускная способность NLB. что исключает зависимость от аппаратной реализации маршрутизатора. Например, в гигабитных сетях NLB обеспечивает пропускную способность около 250 Мбит/с.

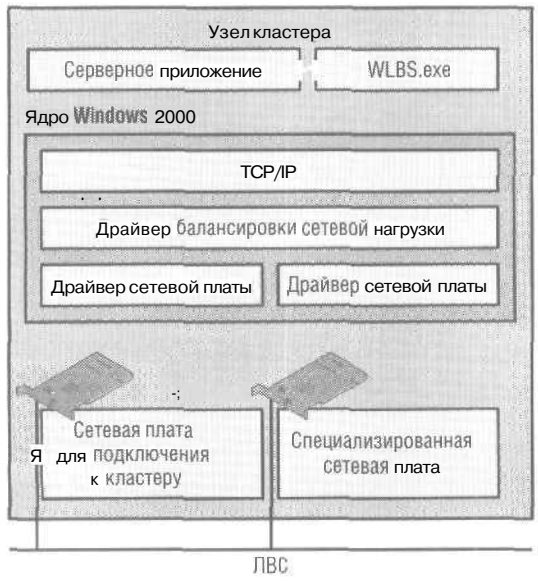


Рис. 13-11. Схема архитектуры NLB, реализованной в виде промежуточного драйвера между TCP/IP и драйвером сетевой платы

- **Высокая доступность** Достигается путем миграции по схеме (N–1) в кластере из N узлов. В отличие от NLB решения на основе диспетчеризации пакетов изначально уязвимы для одиночных отказов, что требует применения избыточности, которая обеспечивает только один вариант миграции при отказе. Такое решение менее устойчиво к сбоям, чем решение на основе полностью распределенной архитектуры.
- **Применение концентраторов и коммутаторов в подсетях** Архитектура NLB использует преимущества подсетей, построенных с применением концентраторов и коммутаторов с целью одновременной доставки сетевого трафика всем узлам кластера. Однако этот подход увеличивает нагрузку на коммутаторы, снижая их пропускную их портов.

  Для большинства специализированных приложений, таких как Web-сервисы и потоковая передача мультимедийных данных, это не имеет значения, так как в этих случаях входящий трафик составляет небольшую часть общего трафика. Но если со стороны клиента к коммутатору подключен канал, который значительно быстрее канала, подключенного со стороны сервера, входящий трафик может полностью блокировать порты на стороне сервера. Аналогичная проблема возникает, когда к одному коммутатору подключено несколько кластеров без размещения кластеров в отдельных виртуальных ЛВС.
- **Взаимодействие с** драйвером **NDIS** Получая пакеты, NLB (реализованная полностью на основе конвейеров) обрабатывает их, тогда как входящие пакеты доставляются TCP/IP, а драйвер NDIS (Network Driver Interface Specification) получает следующие пакеты. Это ускоряет общую обработку и сокращает задержку, поскольку, пока TCP/IP обрабатывает один пакет, драйвер NDIS уже получает следующий. Такая оптимизация также снижает издержки на координирование действий TCP/IP и драйвера NDIS и зачастую позволяет избежать копирования пакетов в память.

  NLB повышает пропускную способность при пересылке пакетов, сокращает задержку и накладные расходы, увеличивая число пакетов, которые TCP/IP может переслать за один вызов NDIS. Эти преимущества NLB обеспечивает при помощи пула буферов для пакетов и дескрипторов, координирующих совместные действия TCP/IP и драйвера NDIS.

Распределение трафика в кластере

NLB использует широковещательную передачу уровня 2 или многоадресную передачу для одновременной доставки входящего сетевого трафика всем узлам кластера. При работе в режиме одноадресной передачи (это режим по умолчанию) NLB модифицирует адрес станции (MAC-адрес) сетевой платы, к которой она привязана (она называется адаптером внутренней сети), назначая одинаковые MAC-адреса всем узлам кластера. Таким образом, все узлы кластера получают входящие пакеты и передают их драйверу NLB, который их и фильтрует.

Для обеспечения уникальности MAC-адрес образуется из основного IP-адреса кластера, указанного в диалоговом окне Network Load Balancing Properties. Если основной IP-адрес кластера — 1.2.3.4. то MAC-адрес для одноадресной передачи будет 02-BF-1-2-3-4. NLB автоматически модифицирует MAC-адрес адаптера внутренней сети кластера, устанавливая соответствующее значение реестра и перезагружая драйвер адаптера; перезагрузка ОС для этого не требуется.

Если узлы кластера подключены к коммутатору, а не к концентратору, то применение одинаковых MAC-адресов приведет к конфликту, так как коммутаторы второго уровня требуют уникальных MAC-адресов отправителя на всех своих портах. Чтобы избежать этого, NLB делает MAC-адреса исходящих пакетов уникальными. Скажем, MAC-адрес 02-BF-1-2-3-4 превращается в 02-*h*-1-2-3-4. где *h* — приоритет узла в кластере (его задают через диалоговое окно Network Load Balancing Properties). Такая методика не дает коммутатору определить *истинный* MAC-адрес кластера, поэтому адресованные кластеру входящие пакеты доставляются во все порты коммутатора. Если же узлы кластера подключены к концентратору, маскировку MAC-адреса отправителя, выполняемую NLB в режиме одноадресной передачи, можно отключить во избежание перегрузки вышестоящих коммутаторов. Для этого параметру реестра *MaskSrcMAC* надо задать 0. Проблема также решается путем применения вышестоящих коммутаторов третьего уровня,

У работы NLB в режиме одноадресной передачи есть побочный эффект — невозможность взаимодействия между узлами кластера через адаптеры внутренней сети. Поскольку исходящие пакеты, адресованные другим узлам кластера, имеют тот же MAC-адрес, что и их отправитель, они возвращают-

ся обратно сетевым стеком и никогда не попадут в сетевой канал. Это ограничение можно снять, установив на каждом узле кластера дополнительную сетевую плату. В такой конфигурации NLB привязана к сетевой плате, подключенной к внешней подсети, из которой поступают входящие клиентские запросы, а другой адаптер обычно подключают к внутренней (локальной) подсети — через нее взаимодействуют узлы кластера и сервер разделяемой БД. NLB использует адаптер внутренней сети для приема и передачи «пульса» и трафика, генерированного удаленным управлением. При работе в режиме одноадресной передачи NLB не влияет на взаимодействие узлов кластера, а также машин, которые не входят в состав кластера.

Трафик, проходящий через внутренний IP-адрес узла (адрес адаптера внутренней сети кластера), получают все узлы, так как им назначены одинаковые MAC-адреса. NLB никогда не распределяет трафик, проходящий через внутренние IP-адреса, сразу передавая его стеку TCP/IP узла-адресата. На других узлах кластера NLB считает этот трафик подлежащим балансировке (поскольку IP-адрес получателя не соответствует внутренним IP-адресам этих узлов) и передает его стеку TCP/IP, который его отбрасывает. Избыточный входящий трафик, нацеленный на внутренний IP-адрес, может вызвать помехи при работе NLB в одноадресном режиме, так как стек TCP/IP вынужден отбрасывать ненужные пакеты.

NLB поддерживает второй режим доставки входящего сетевого трафика всем узлам кластера — режим многоадресной передачи, при котором вместо модификации MAC-адреса сетевым платам кластера назначается групповой адрес второго уровня. Так, кластеру с главным IP-адресом 1.2.3.4 будет назначен групповой MAC-адрес 03-BF-1-2-3-4. Поскольку при этом у каждого узла остается уникальный адрес станции, режим многоадресной передачи устраняет потребность в установке второго сетевого адаптера для взаимодействия узлов кластера и позволяет избежать снижения производительности из-за применения внутреннего IP-адреса. Работа NLB в режиме одноадресной передачи вызывает лавинообразную передачу пакетов для одновременной доставки входящего трафика всем узлам кластера. При использовании NLB в режиме многоадресной передачи для доставки многоадресного трафика по умолчанию также применяется лавинообразная передача. Однако

NLB позволяет системному администратору ограничить лавинообразную передачу, создав на коммутаторе VLAN для портов, соответствующих узлам кластера. Это можно сделать, запрограммировав коммутатор вручную, либо применив протоколы IGMP и GMRP. Однако в текущей версии NLB нет автоматической поддержки этих протоколов.

В NLB реализован протокол Address Resolution Protocol (ARP), гарантирующий разрешение основного IP-адреса кластера и других виртуальных адресов на групповой MAC-адрес кластера (внутренний IP-адрес при этом разрешается на адрес станции адаптера внутренней сети кластера). Опыт показал, что текущие модели маршрутизаторов Cisco не принимают отклика ARP от кластера, разрешающего обычные IP-адреса в групповые MAC-адреса. Эту проблему можно решить, добавив к маршрутизатору статическую запись ARP для каждого виртуального IP-адреса. Групповой MAC-адрес кластера можно получить из окна свойств NLB или при помощи программы для удаленного управления WIbs.exe. В режиме одноадресной передачи (он включен по умолчанию) эта проблема не возникает, поскольку MAC-адрес кластера в этом случае на является групповым.

NLB управляет входящим IP-трафиком протоколов TCP, User Datagram Protocol (UDP) и Generic Routing Encapsulation (GRE как часть PPTP), нацеленным на определенные порты, игнорируя остальной трафик. NLB не фильтрует трафика ICMP, IGMP, ARP (кроме вышеописанных случаев) и других протоколов IP — этот трафик без изменений передается стеку протоколу TCP/IP на всех узлах кластера. В результате кластер может генерировать отклики для некоторых программ, использующих TCP/IP и ориентированных на соединения типа «точка -- точка» (таких как ping), если вызвать их с IP-адресом кластера. Устойчивость TCP/IP и его способность обрабатывать реплицированные дейтаграммы обеспечивает корректную работу других протоколов в окружении кластера. Эти программы могут использовать внутренние IP-адреса узлов кластера, чтобы избежать подобных проблем.

Алгоритм балансировки нагрузки

Для сопоставления входящих клиентских соединений с узлами кластера в NLB применяется полностью распределенный ал-

горитм фильтрации. Это обусловлено тем, что данный алгоритм позволяет узлам независимо и быстро принимать решения па балансировке даже при значительном числе клиентов при помощи частых, но небольших запросов вроде тех, что обрабатывают Web-серверы.

Когда клиентов мало или уровень генерируемой ими нагрузки на сервер сильно колеблется, эффективность алгоритма балансировки NLB снижается. Однако простота и скорость NLB позволяет достигать очень высокой производительности как при большом, так и при малом времени генерации отклика, а также при использовании разных клиент-серверных приложений.

NLB распределяет входящие клиентские запросы, направляя каждому узлу кластера определенную часть поступивших запросов. Долю нагрузки задают через окно Network Load Balancing Properties для каждого диапазона портов, через которые проходит трафик, подлежащий балансировке. Этот алгоритм не реагирует на изменения нагрузки на отдельные узлы кластера (например, на колебания утилизации процессора и памяти). Однако изменение состава кластеров влияет на сопоставление запросов и узлов, вызывая изменение доли нагрузки, обрабатываемой каждым узлом.

Анализируя полученный пакет, узлы кластера выполняют и ряд статистических расчетов, определяя, кто из них должен обработать этот пакет. Алгоритм балансировки использует рандомизирующую функцию, которая генерирует значение приоритета узла на основе его IP-адреса, номера порта и некоторых других сведений. Узел, получивший самый высокий приоритет, передает пакет вверх по сетевому стеку протоколу TCP/IP, а остальные узлы отбрасывают его. Правила распределения нагрузки остаются постоянными, пока не изменится состав кластера. Это гарантирует, что узел кластера, связанный с IP-адресом и портом, которые использовал данный клиент, не изменится. Однако эту связь нельзя определить заранее, поскольку рандомизирующая функция учитывает и текущий, и прежний состав кластера, чтобы свести к минимуму изменения правил распределения нагрузки. Если связывание клиентов активно, алгоритм балансировки предполагает, что IP-адреса и номера портов клиента статистически независимы, но при использовании серверного брандмауэра, замещающего IP-адреса клиентов одним IP-адресом, активизировано связыва-

ние клиентов. В этом случае все клиентские запросы будут обрабатываться только одним узлом, и балансировки нагрузки не будет. Если связывание клиентов не применяется, распределение клиентских портов внутри брандмауэра обычно обеспечивает хорошую балансировку нагрузки.

В общем случае качество балансировки определяется статистически и зависит от числа запрашивающих клиентов. Это аналогично бросанию игральной кости, где каждая грань соответствует узлу кластера, а каждый бросок — запросу. Распределение нагрузки улучшается с поступлением новых клиентских запросов как величина, обратная числу бросков кости с n гранями, которая с увеличением числа бросков стремится к $1/n$. Правило таково: если используется связывание клиентов, для равномерного распределения нагрузки их число должно быть существенно больше числа узлов кластера. В силу статистической природы изменения числа клиентов, возможны колебания распределения нагрузки во времени. Заметьте: стремление к идеально равномерному распределению нагрузки снижает производительность (в терминах пропускной способности и времени отклика) из-за издержек на измерение текущей нагрузки и соответствующую регулировку распределения. Следует сравнить снижение производительности с выгодой от максимальной утилизации ресурсов кластера (главным образом процессоров и памяти). В любом случае часть ресурсов кластера следует держать свободными на случай отказа одного из узлов. Максимально простой и устойчивый алгоритм балансировки, применяемый в NLB, обеспечивает наивысшую производительность и доступность.

Параметры связывания клиентов NLB реализованы путем модификации правил распределения нагрузки, генерированных статистически на основе входных данных. Если в диалоговом окне Network Load Balancing Properties задано связывание клиентов, номер порта клиента не учитывается при выборе узла для обработки запроса, поэтому все запросы от одного клиента всегда направляются на один узел кластера. Это правило действует бессрочно (как и в решениях, основанных на применении диспетчера), т. е. до изменения состава кластера. Если задано связывание одного адреса, алгоритм учитывает полный IP-адрес клиента, а если выбрано связывание группы адресов класса C, учитываются только первые три октета IP-адреса (его

старшие 24 разряда). Это гарантирует, что все клиенты с IP-адресами, различающимися лишь последним октетом, будут обслужены одним узлом кластера.

При выборе узла для обслуживания клиентов NLB не может непосредственно отслеживать границы сеансов (например, сеансов SSL), поскольку решения по балансировке принимаются при установке TCP-соединения, когда прикладные данные пакетов еще не получены. NLB также не видит границы потоков UDP, поскольку логические границы сеансов определяются приложением. Для сохранения сеансов служат параметры NLB, определяющие связывание клиентов. При отказе узла или при выводе его из кластера соединения с клиентами всегда разрываются. Если при перекличке (о ней чуть ниже) оказалось, что состав кластера изменился, клиенты, прежде подключенные к отказавшему узлу, перераспределяются между функционирующих узлами. Отказ не влияет на остальные сеансы, которые продолжают получать от кластера бесперебойное обслуживание. Таким образом, алгоритм балансировки NLB позволяет минимизировать негативное влияние сбоев на клиентов.

Подключение к кластеру нового узла инициирует перекличку, завершающуюся расчетом нового состава кластера. После переклички некоторая минимальная часть клиентов мигрирует на новый узел. Для каждого узла NLB отслеживает TCP-соединения; если, завершив одно соединение, мигрирующий клиент снова подключится к кластеру, его будет обслуживать уже другой узел. Новые потоки UDP в любом случае обслуживаются другими узлами. Это может вести к прекращению клиентских сеансов, включающих несколько соединений или потоков UDP. Поэтому для подключения новых узлов к кластеру надо выбирать моменты, когда их негативный эффект будет минимальным. Чтобы полностью решить эту проблему, данные о состоянии сеансов следует поддерживать с помощью серверного приложения, способного реконструировать их или получить с узла кластера. Например, эти данные можно записывать в серверную БД или в cookie-файлы на клиентские машины. Состояние сеансов SSL автоматически восстанавливается после повторной аутентификации клиента.

Потоки GRE, инкапсулированные внутри протокола PPTP (Point-to-Point Tunneling Protocol), — это особый вид сеансов, на которые не влияет подключение узлов к кластеру. Поскольку

поток GRE существует в течение времени жизни управляющего им TCP-соединения, NLB отслеживает его вместе с соответствующим управляющим соединением. Это защищает туннель PPTP от разрыва при добавлении узла к кластеру.

Перекличка

Узлы с NLB периодически обмениваются многоадресными или широковещательными сообщениями — «пульсом». Это позволяет узлам следить за состоянием кластера. При изменении состояния кластера (в результате отказа/отключения/подключения узла) NLB инициирует процесс *переклички* (convergence), во время которой узлы обмениваются сообщениями «пульса», чтобы определить новое состояние кластеров и выбрать узел с высшим приоритетом новым узлом по умолчанию. Когда узлы приходят к согласию и принимают новое состояние кластера, по завершении переклички они записывают изменения состава кластера в журнал событий Windows.

При перекличке узлы продолжают обработку входящего сетевого трафика как обычно (естественно, кроме отказавших узлов), перекличка не влияет на обработку запросов функционирующими узлами. Перекличка завершается, когда ни один узел не сообщает об изменения состава кластера в течение нескольких «ударов пульса» (периодов обмена сообщениями). Если к кластеру пытается подключиться узел с несоответствующими правилами портов или идентичным уровнем приоритета, перекличка продолжается. Это не дает неверно сконфигурированным узлам принимать участие в обработке трафика кластера. По завершении переклички доля трафика, которую обрабатывал отказавший узел, перераспределяется между оставшимися узлами. Если узел добавляется к кластеру, после переклички ему достается доля трафика, вычисленная при балансировке. Расширение кластера не влияет на его текущие операции и выполняется прозрачно как для Интернет-клиентов, так и для серверных программ. Однако оно может повлиять на клиентские сеансы, так как клиенты могут быть переданы другому узлу кластера в промежутках между подключениями (см. выше).

В режиме одноадресной передачи каждый узел кластера периодически передает широковещательные, а в режиме многоадресной передачи — многоадресные сообщения «пульса». Каждое такое сообщение занимает один кадр Ethernet и отме-

чается основным IP-адресом кластера, поскольку в одной подсети может быть несколько кластеров. Сообщениям «пульса» NLB присваивается шестнадцатеричный код типа передачи 886F. Период между передачей «пульса» по умолчанию составляет 1 секунду и определяется параметром реестра *MsgAlivePeriod*. При перекличке этот период уменьшается вдвое, чтобы скорее завершить перекличку. Даже в больших кластерах передача сообщений «пульса» почти не снижает пропускной способности сети (так, в кластере из 16 узлов трафик пульса составляет не более 24 Кб/с). NLB предполагает, что узел кластера работает нормально, если он в состоянии обмениваться «пульсом» с другими узлами. Если другие узлы в течение нескольких циклов не слышат «пульса» какого-либо узла, они начинают перекличку. По умолчанию число пропущенных сообщений «пульса», необходимое для начала переклички, — 5, но его можно изменить, задав в реестре параметр *NumAliveMsgs*.

Узел кластера начинает перекличку, если он получает «пульс» от нового узла или «пульс» сбивается с ритма (что свидетельствует о проблемах с распределением нагрузки). Если какой-то узел услышит «пульс» нового узла, он проверяет, не обрабатывал ли новый узел трафик, генерированный его клиентами. Такая проблема возникает при воссоединении ранее разделенной внутренней подсети кластера. Не исключено, что по результатам переклички новый узел оказался единственным в другой части подсети. Это возможно, если коммутатор вносит существенную задержку при подключении узла к подсети. Если узел кластера обнаруживает подобную проблему и определяет, что со времени последней переклички к другому узлу подключилось больше клиентов, он сразу прекращает обработку клиентского трафика в соответствующем диапазоне портов. Поскольку оба узла обменивались «пульсом», узел, к которому подключено больше клиентов, продолжает обработку трафика, а другой узел ждет конца переклички, после чего начинает обрабатывать свою порцию нагрузки. Такой эвристический алгоритм исключает потенциальные конфликты в распределении нагрузки при воссоединении подсети кластера, которая до этого была разделена. Это событие также регистрируется в журнале событий.

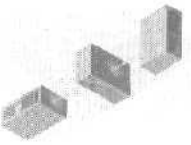
Удаленное управление

Механизм удаленного управления NLB использует протокол UDP и работает через порт 2504. Дейтаграммы удаленного управления направляются на основной IP-адрес кластера. Поскольку эти дейтаграммы обрабатывает драйвер NLB на всех узлах кластера, они должны маршрутизироваться во внутреннюю сеть кластера (а не в сеть, к которой подключен кластер). Команды удаленного управления, генерированные во внутренней сети кластера широковещательно транслируются в локальную подсеть. Это гарантирует их получение всеми узлами кластера, даже если тот работает в режиме одноадресной передачи.

Дополнительная информация

Дополнительные сведения к данной главе см. по адресам:

- What's New in Clustering Services — http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/clustering.mspx;
- Windows Server 2003 Product Overviews — http://www.microsoft.com/windowsserver2003/evaluation/overview/;
- Windows Server 2003 vFeatures guide — http://www.microsoft.com/windowsserver2003/evaluation/features/;
- Introducing the «.NET» in the Windows Server 2003 Family - http://www.microsoft.com/windowsserver2003/evaluation/overview/dotnet/dotnet.mspx;
- Windows 2000 Server — http://www.microsoft.com/windows2000/server/;
- Application Center 2000 — http://www.microsoft.com/applicationcenter/;
- Windows 2000 Clustering Technologies — http://www.microsoft.com/windows2000/technologies/clustering/;
- Increasing System Reliability and Availability with Windows 2000 — http://www.microsoft.com/windows2000/server/evaluation/business/relavail.asp;
- Hardware Compatibility List — http://www.microsoft.com/hcl/;
- Windows 2000 Server Family: Advanced Scalability — http://www.microsoft.com/windows2000/advancedserver/evaluation/business/overview/scalable/.



ГЛАВА

14

Многоязыковаяподдержка

Предприятие только тогда может считаться транснациональным, когда оно способно вести дела на многих языках, поддерживая языковые и культурные особенности любых регионов. Вашим пользователям, партнерам и потребителям нужен доступ к ресурсам на удобном для них языке независимо от того. где и на какой платформе они работают.

Microsoft потратила годы на обеспечение поддержки многоязыковых программ. В Windows 2000 Microsoft сделала важный шаг в переводе всех элементов ОС на международный стандарт Unicode, а также представила пакет многоязыкового пользовательского интерфейса (Multilingual User Interface, MUI). MUI позволяет пользователям изменять язык пользовательского интерфейса и приложений. В XP Microsoft обеспечила поддержку большего числа языков и регионов, при этом сделав MUI проще и гибче. В Windows Server 2003 Microsoft подняла эту технологию на новый уровень.

Одна из основных целей MUI — позволить как можно проще и с меньшими затратами внедрять многоязыковую поддержку. У Microsoft несколько технологий развертывания, включая Windows Installer, которые делают MUI одним из оптимальных способов обеспечения глобальной информатизации. MUI полностью поддерживается в Microsoft Office и других локализуемых Unicode-приложениях. Кроме того, функциональность MUI доступна разработчикам через API, что позволяет применять ее в приложениях любых компаний.

Задачи интернациональных корпораций

При решении задач поддержки интернациональных предприятий следует учитывать следующие моменты.

- **Учет региональных различий** В глобализованной экономике люди и организации должны общаться на разных языках, а значит, им нужны технологии, поддерживающие разные языки для общения с пользователями, потребителями и партнерами, им также нужно работать с разными валютами, форматами дат/времени, наборами символов и т. д, Б такой среде должны работать и пользовательские приложения, и серверы.
- **Поддержка локализованных приложений** Во многих компаниях применяется локализованное ПО: бизнес-приложения, инструменты для управления персоналом, аналитические или узкоспециализированные приложения и т. д. Для работы в условиях международного предприятия оно должно быть локализуемым, т. е. легко адаптируемым к глобальной среде без повторного написания. Однако компаниям нужно не только создавать приложения с многоязыковой поддержкой, но и стандартизовать их разработку,
- **Обеспечение поддержки пользователей, служб и рабочих станций на нескольких языках** В многонациональной среде исключительно важно поддерживать множество языков в одном офисе или подразделении. Один и тот же пользователь должен иметь доступ к ПО на разных языках. Дело усложняется, когда мобильные пользователи требуют доступ к системе на выбранном ими языке в разных офисах.
- **Управление развертыванием в различных регионах** Развертывать ПО в международной среде сложнее, чем в отдельном регионе. Надо учитывать все возможные комбинации языков и ОС независимо от того, развертывается ли серверное или настольное ПО. Проблема усложняется наличием разных видов валют, местных стандартов представления чисел, дат, времени и т. п.
- **Развертывание изменений и обновлений в разных странах** Поддержка исправлений, изменений и обновлений — важнейшая задача в условиях разрастания всемирной сети. Быстрое внедрение важнейших изменений имеет решающее

значение не только по причинам сетевой безопасности, на и как средство экономии. Сопровождение и регулярное обновление — важная задача ИТ-отделов. Эта нагрузка возрастает по мере увеличения числа поддерживаемых конфигураций, особенно в многоязыковой среде. Нужно учитывать все комбинации ОС, языков, региональных параметров, иметь для каждой комбинации сценарий обновления и план сопровождения. Надо учитывать и задержки во внедрении изменений для каждого языка. Временной промежуток между реализацией изменения или обновления для английской версии и локализованными может быть весьма значительным.

Поддержка многонационального предприятия

Windows Server 2003 вскоре будет доступен в локализованных вариантах, оптимизированных для конкретных стран. Англоязычная же версия Windows Server 2003 в паре с MUI позволит переключаться с языка на язык, поддерживая широкий спектр региональных особенностей.

Многоязыковый пользовательский интерфейс

MUI — это продукт Microsoft, позволяющий развертывать Windows в многоязыковой глобальной среде, не создавая отдельных локализованных вариантов установки. MUI позволяет выбирать нужный язык для элементов пользовательского интерфейса, включая меню Пуск, управляющие элементы программ и файлы справочной системы.

MUI работает «поверх» англоязычной версии ОС, а значит, специалисты по сопровождению не должны развертывать и поддерживать отдельных версий для каждого нужного языка. Вместо этого они стандартизуют процесс развертывания англоязычной версии ОС с MUI. MUI также поддерживает настольные приложения, включая Microsoft Office и серверные продукты вроде Microsoft SQL Server.

Варианты для многонациональных предприятий

Англоязычная версия Windows Server 2003 — лучший выбор для организаций, применяющих в основном английский язык и лишь иногда другой. Например, американская компания, имеющая представительство в Японии, ведет бизнес на англий-

ском, однако иногда бывает нужно читать электронную почту и документы, написанные по-японски. На японском нужно сопровождать и Web-сайт. Такую компанию вполне устроит англоязычная версия Windows Server 2003 в качестве сервера, а в качестве ОС для рабочих станций — Windows XP. Для просмотра документов и почты на японском языке можно использовать Microsoft Office XP.

MUI обеспечивает поддержку многих языков в англоязычной версии Windows Server 2003 и является лучшим решением для компаний, деятельность которых связана с разными языками. Представим себе компанию с офисами в разных странах. Пользователям нужны разные языки, а кое-где требуется поддержка нескольких языков. Единственный эффективный в финансовом отношении вариант в этом случае — создать стандартный вариант развертывания и применять его во всех регионах. Здесь и подойдет Windows Server 2003 с MUI. MUI — лучший выбор и в том случае, когда компания должна работать на двух или более языках в одном месте, особенно когда пользователям нужно регистрироваться на одном компьютере на разных языках. Возьмем американскую компанию с офисами в разных странах. В регионах пользователи будут работать как на английском, так и на местном языке. Задача решается развертыванием ОС и Office XP с MUI.

Microsoft будет поставлять версии Windows Server 2003, локализованные для конкретных регионов. Локализованные версии оптимизированы для работы с одним языком, отличным от английского, так что это не самое гибкое решение. Локализованная версия — оптимальный выбор для компаний, использующий единственный язык, если это не английский. Компания, расположенная в Японии и ведущая бизнес на японском языке, может использовать Windows Server 2003 на японском.

Усовершенствования многонациональной поддержки

В Windows Server 2003/XP Professional MUI усовершенствован.

- **Увеличено число регионов** Windows 2000 поддерживает множество языков, регионов и способов ввода текста. В Windows XP/Server 2003 добавлена поддержка еще 9 регионов, так что их общее число достигло 135.

- **Простота использования** Дизайн управляющей панели Regional And Language Options в Windows XP/Server 2003 усовершенствован так, что стало проще выполнять задачи, связанные с языками.
- **Проще получить справку** Компонент Multilanguage Document Consultant в Windows XP Help and Support Center помогает пользователям обнаруживать и решать проблемы с открытием, просмотром и редактированием многоязыковых документов.
- **Поддержка нескольких языков и письменностей** По умолчанию устанавливается один из трех языковых наборов, другие наборы устанавливаются по запросу. Набор Basic Language Collection поддерживает основные западно- и центральноевропейские языки. а Complex Script Collection поддерживает такие языки со сложным написанием символов, как арабский, иврит и др. Набор East Asian Collection поддерживает прочие азиатские языки.
- **Язык для программ, не поддерживающих Unicode** Windows XP Professional/Server 2003 позволяет указывать параметры языка для программ, не поддерживающих Unicode.

Многоязыковый пользовательский интерфейс

В Windows 2000 Professional Microsoft представила MUI — технологию, позволяющую сосуществовать нескольким локализованным интерфейсам. В Windows XP ее стало проще применять. Связанная с MUI технология Multilanguage User Interface for Office XP позволяет переключать пользовательский интерфейс в приложениях Office, расширяя редакторские возможности для многих языков. В Windows Server 2003 MUI поднята на новый уровень за счет усовершенствований в методологии развертывания, поддержке многоязыковых сеансов служб терминалов и т. д.

- **Поддержка Terminal Services** Terminal Services — технология Microsoft, позволяющая пользователям удаленно регистрироваться на центральном сервере и создавать виртуальные сеансы Windows, MUI для Windows Server 2003 поддерживает многоязыковые сеансы Terminal Services. Сервер с MUI и Windows Server 2003 позволяет пользователям регистрироваться и создавать терминальные сеансы на разных

языках на одном сервере служб терминалов. Раньше для этого требовалось несколько локализованных серверов терминалов. MUI снижает затраты на создание и поддержку терминальных сеансов в многоязыковой среде.

- **Улучшенные возможности развертывания** MUI для Windows Server 2003 поддерживает технологию Microsoft Windows Installer, применяемую для создания простых в управлении пакетов установки. MUI теперь проще развертывать, сопровождать и настраивать.

Поддерживаемые платформы и программы

Кроме Windows XP Professional/Server 2003, MUT поддерживает и другие платформы и приложения.

- **Office XP** Multilanguage User Interface for Office XP предлагает множество возможностей многоязыковой поддержки, в том числе переключение пользовательского интерфейса, средства проверки орфографии и редактирования для многих языков.
- **Windows CE** Разработчики могут использовать MUI API для создания локализованных приложений для мобильных устройств под управлением Windows CE,
- **SQL Server** Серверные продукты, поддерживающие Unicode, такие как SQL Server, могут работать под управлением Windows Server 2003 с MUI, обслуживая многоязыковые предприятия. Microsoft SQL Server обеспечивает поддержку нескольких языков и наборов символов. Подробнее см, документацию no SQL Server.
- **Унаследованные продукты** MUI для Windows Server 2003 использует технологии, аналогичные применяемым в MUI для Windows 2000 и MUI для Office 2000. При замене Windows 2000 Server на Windows Server 2003 необходимо обновить и MUT,

Чем вам может быть полезен MUI

Пакет MUI для Windows Server 2003 обеспечивает многоязыковую поддержку с приемлемыми затратами.

- **Учет региональных требований** MUI позволяет учесть региональные требования в разных отделениях предприятия.

Он поддерживает управление различными устройствами ввода, такими как клавиатуры для азиатских языков, позволяет менять язык большинства элементов пользовательского интерфейса, включая меню Пуск, диалоговые окна и справочную систему.

- **Поддержка многоязыковых рабочих столов** Windows XP с MUI — превосходный выбор для платформ с многоязыковым рабочим столом. При этом пользователи, регистрирующиеся на компьютере, могут работать с разными языками. Без MUI подобная функциональность потребовала бы конфигурации с различными вариантами загрузки системы. MUI можно настроить и для поддержки многоязыковых мобильных пользователей.
- **Развертывание односерверной конфигурации в разных регионах** Развернуть ПО в многонациональной среде довольно трудно. MUI для Microsoft Windows Server 2003 призван упростить этот процесс. Поскольку MUI базируется на англоязычной версии ОС, персоналу ИТ-отдела нужно развертывать и сопровождать лишь одну версию ОС.
- **Упрощенное сопровождение** На развертывание тратится лишь часть средств, уходящих на поддержку ПО. MUI снижает TCO для всего жизненного цикла программ. Требуется сопровождать и обновлять единственную версию ОС, а такие задачи, как развертывание программных заплат и обновлений упрощаются. Организациям, работающим с локализованными версиями ОС, приходится ждать, когда обновления появятся для программ с разными языками. Это значит, что применение MUI не только ускоряет процесс внедрения обновлений, но и делает среду более безопасной.
- **Поддержка нескольких языков для служб терминалов** Службы терминалов с МШ для Windows Server 2003 поддерживают одновременную работу пользователей на разных языках, что делает поддержку многоязыковой среды более эффективной, не требуя отдельного сервера для каждого языка.

Развертывание многоязыкового предприятия

Развертывание многоязыкового предприятия требует учесть следующее.

- **Региональные требования** Первый этап при развертывании ПО в международном масштабе — определение языковых потребностей для всех регионов функционирования предприятия. Нужно учесть и бизнес-приложения, требующие многоязыковой поддержки. Для каждого региона определите, какие языки, диалекты, валюты и форматы календарей нужно поддерживать. Обратите внимание и на то, нужны ли в регионах специальные устройства ввода.
- **Требования к аппаратуре** MUI использует устанавливаемые модули — *языковые пакеты*, которые поддерживают отдельные локализации. Эти пакеты требуют дополнительного места на жестких дисках. Для сложных языков, таких как иврит и арабский, требуется 100 Мб дискового пространства, а для дальневосточных языков — 230 Мб. Также нужно учесть потребность в альтернативных устройствах ввода.
- **Потребности мобильных пользователей** Пакет MUI для Microsoft Windows Server 2003 позволяет поддерживать работу мобильных пользователей на разных языках. Пакеты MUI должны быть установлены (или должны устанавливаться по требованию) на все машины, на которых работает пользователь.
- **Многоязыковое развертывание Microsoft Office XP** Microsoft Office XP готов к работе на разных языках, но развертывать его нужно одновременно с ОС. Microsoft предлагает инструменты, упрощающие развертывание Office. Существуют локализованные версии Microsoft Office XP. а также версия с Microsoft Office Multilingual User Interface Pack.

Примечание О развертывании Multilanguage Office XP см. раздел «Microsoft Office XP in a Multilingual Environment» на странице *http://www.microsoft.com/office/evaluation/indepth/mu ltilingual/*.

Настройка серверных платформ

Поскольку MUI поддерживает технологию Microsoft Windows Installer, для настройки и сопровождения серверов вы можете применять любые инструменты Microsoft, использующие Windows Installer. Для каждого поддерживаемого языка пакеты MUI содержатся в отдельных файлах .msi. Они могут быть установлены по отдельности двойным щелчком пакета или средством добавления и удаления программ на панели управления.

- **Установка из командной строки** MUI можно установить из командной строки, вызвав программу Msiexec. Можно указать массу опций, например, устанавливать ли пакет для текущего пользователя, для всех пользователей или для пользователя по умолчанию на данной машине. Если вы укажете пользователя по умолчанию, MUI будет доступен для всех пользователей, которые в дальнейшем будут создаваться на данной машине.
- **Установка, не требующая вмешательства** Windows Server 2003 с MUI поддерживает установку без вмешательства оператора. Это позволяет автоматизировать установку как при начальной установке Windows Server 2003, так и после нее. Поскольку MUI поставляется на нескольких компакт-дисках, вам потребуется создать сетевые совместно используемые каталоги, содержащие все языковые пакеты, а также файлы ответов для установки нужных конфигураций.

Настройка рабочих столов

При настройке рабочих столов пользователей в многоязыковой среде нужно учитывать несколько важных моментов.

- **Языковые параметры по умолчанию** Определив необходимые языковые параметры, вы можете применить их как параметры по умолчанию на своих настольных компьютерах. Когда параметры по умолчанию установлены, все пользователи, которые будут создаваться на компьютере, будут их наследовать. На пользователей, чьи регистрационные данные уже существуют, эти параметры не будут действовать. Параметры задаются либо интерактивно через пользовательский интерфейс, либо из файла ответов при установке без вмешательства оператора.

- **Групповая политика** Администратор может создать сценарии регистрации, включающие языковые параметры, в том числе язык по умолчанию и методы ввода.
- **Установка пакетов MUI по требованию** Администраторы могут определить конфигурацию пользователя и компьютера средствами групповой политики. Это позволит им устанавливать пакеты MUI на пользовательских компьютерах до того, как пользователи будут на них регистрироваться. Когда администратор устанавливает пакеты MUI для дальневосточных языков или языков со сложной письменностью, может возникнуть ошибка, если для этих языков еще не установлены языковые пакеты или в накопителе нет дистрибутива Windows Server 2003. Пакеты MUI в каталогах Active Directory всегда относятся к одному пользователю. Такой вариант установки не рекомендуется, поскольку, хотя задействовать пакет MUI смогут разные пользователи, удалить его сможет только установивший его.
- **Настройка локализованного содержимого** Вы можете настроить рабочие столы так, чтобы принимать локализованную информацию, скажем, новости или прогноз погоды из Интернета, интрасети или от экстранет-серверов. Для этого нужно установить соответствующие региональные параметры на панели Regional And Language Options.
- **Многоязыковая поддержка Microsoft Office XP** Существуют локализованные версии Office XP, а также версия на базе англоязычной версии с Office **XP** Multilingual User Interface Pack, поддерживающая редактирование на нескольких языках. Развертывая Microsoft Windows XP в многоязыковой среде, нужно учитывать, что одновременно нужно установить и Office XP. Microsoft предоставляет инструменты и технологии, облегчающие развертывание Office XP.

Многоязыковые приложения

Разработка локализуемых приложений может принести большую выгоду в многоязыковой среде. MUI предоставляет общедоступные API, которые можно применять для разработки полностью локализуемых приложений. Чтобы ваши приложения поддерживали разные языки и сложные письменности, создавая их, нужно учитывать следующие моменты.

- **Обеспечьте поддержку Unicode** Основной момент при разработке многоязыкового приложения — применение Unicode, международного стандарта, позволяющего использовать практически любые языки. Приложения, поддерживающие Unicode, могут отображать элементы пользовательского интерфейса на любом языке. Это делает вас независимым от кодовых страниц для поддержки разных языков. Приложение будет локализуемым только в том случае, если оно поддерживает Unicode.
- **Для каждого языка создавайте DLL ресурсов** MUI-приложения используют для хранения текстовых строк, применяемых в пользовательском интерфейсе, DLL ресурсов. Такой подход требует дополнительных трудозатрат в начальной фазе, но обеспечивает значительные преимущества в иелом. Этот метод позволяет не только менять пользовательский интерфейс, но и легко изменять приложения, добавляя поддержку новых языков без изменения основного исходного кода или других ресурсных DLL. Ваше приложение становитсяполностьюлокализуемым,

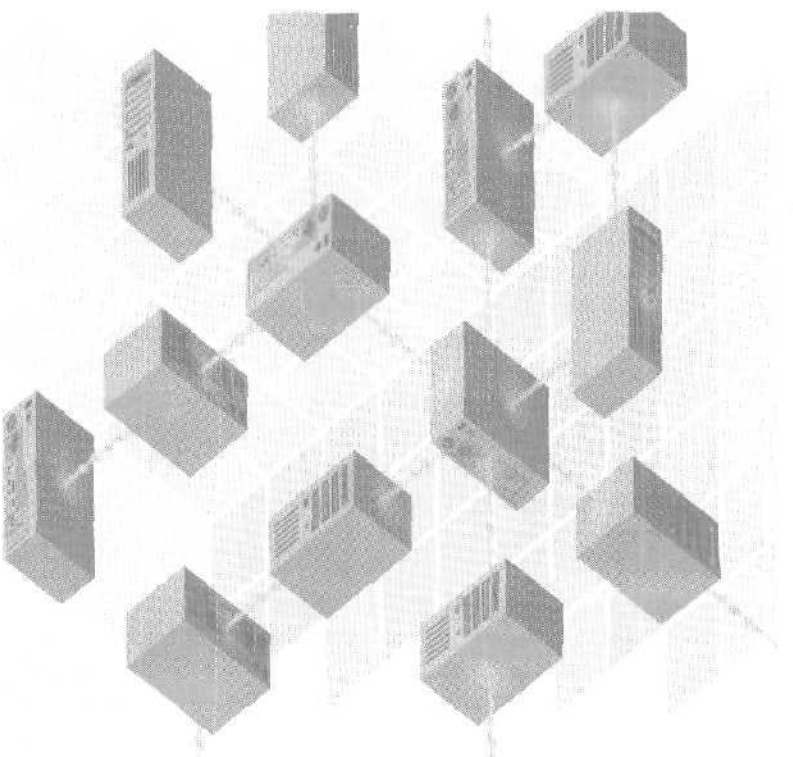
Дополнительные сведения

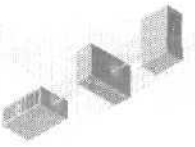
Дополнительные сведения см. по следующим адресам:

- многоязыковые возможности в Microsoft Windows XP Professional — http://www.microsoft.com/windowsxp/pro/techinfo/planning/multilingual/;
- Microsoft Office XP в многоязыковой среде —http://www.microsoft.com/office/evaluation/indepth/multilingual/;
- часто задаваемые вопросы по Windows XP и Windows 2000 MUI — http://www.microsoft.com/globaldev/FAQs/Multilang.asp;
- создание многоязыкового пользовательского интерфейса — http://www.microsoft.corn/globaldev/arlicles/muiapp.asp.

ЧАСТЬ III

НАЧАЛО РАБОТЫ





ГЛАВА
15

Развертывание Windows Server 2003

Эта глава поможет вам спланировать установку Windows Server 2003 в сетевой среде. Подробно об этом процессе см. «Microsoft Windows Server 2003 Deployment Kit» (Microsoft Press, 2003). В этой книге также описано создание множества доменов со структурированными связями. О ресурсах см. на Web-узле Microsoft (*http://www.microsoft.com/windows/reskits/*).

Изучив материал этой главы, вы сможете запустить программу установки Windows Server 2003 и работать с мастером Configure Your Server Wizard. Программа установки и этот мастер помогут настроить серверы сети. Подробнее о мастере Configure Your Server см. справочную систему Help and Support Center, интегрированную в Windows Server 2003. Чтобы открыть ее, по завершении установки раскройте меню Start и выберите Help And Support. Тематические разделы Help and Support см. также на Web-узле Microsoft *(http://www.microsoft.com/windows~server2003/)*.

Сравнение обновления и новой установки

Приведенное ниже сравнение обновления и новой установки поможет вам решить, устанавливать ли ОС «с чистого листа» (об обновлении см. главы 16 и 17). Обновление — это замена Windows NT 4.0 (с установленным сервисным пакетом версии 5 или более поздней) или Windows 2000 продуктом семейства ОС Windows Server 2003. В отличие от обновления установка

означает полное удаление имеющейся ОС или установку Windows Server 2003 на диск или раздел диска, на котором нет никакой ОС.

Доводы в пользу обновления

Вот доводы в пользу обновления.

- При обновлении упрощается конфигурирование, сохраняются имеющиеся пользователи, параметры, группы, права и разрешения.
- При обновлении не требуется переустанавливать файлы и приложения. Однако, как и при любом другом значительном изменении содержимого жесткого диска, рекомендуется создать резервную копию этого содержимого.
- Если вы собираетесь обновить ОС и затем использовать те же приложения, что и раньше, изучите информацию о приложениях в файле Relnotes.htm (папка \Docs установочного компакт-диска). О приложениях, совместимых с Windows Server 2003, см. на Web-узле Windows Catalog *(http://www.microsoft.com/windows/catalog/)*.

Доводы в пользу установки

Вот доводы в пользу установки с нуля.

- Если отформатировать жесткий диск и установить ОС с нуля, может возрасти эффективность работы диска. Кроме того, форматирование позволяет изменить размер или число разделов диска для более точного соответствия вашим требованиям.
- Если вы хотите настроить систему, например сервер, где важна высокая доступность, лучше установить на нем ОС с нуля. Это особенно полезно для серверов, ОС которых уже не раз обновлялась.
- На компьютере могут быть одновременно установлены Windows Server 2003 и другая ОС. Но в этом случае возникают проблемы совместимости файловых систем. Подробнее см. ниже раздел «Установка нескольких ОС».
- Чтобы установить Windows Server 2003 на компьютер, где ранее была установлена ОС, выпущенная до Windows 2000. помните следующее:

- Если диск сжат не средствами NTFS, устанавливать на него или обновлять имеющуюся на нем ОС до Windows Server 2003 не следует. Прежде чем запустить программу установки, восстановите исходный размер томов DriveSpace или DoubleSpace.
- Если вы создали средствами Windows NT 4.0 набор томов, зеркальных томов, чередующихся томов или чередующихся томов с четностью и хотите запустить на этом компьютере программу установки Windows Server 2003, вам потребуется предварительно подготовить набор дисков. Подробнее см. раздел «Использование зеркальных, чередующихся и обычных томов».

Системные требования

Убедитесь, что компьютеры, на которые вы устанавливаете Windows Server 2003, соответствуют следующим требованиям.

- Один или несколькопроцессоров с рекомендуемой минимальной тактовой частотой 550 МГц (минимально поддерживаемая тактовая частота — 133 МГц). Рекомендуется использовать процессоры семейств Intel Pentium/Celeron или AMD K6/Athlon/Duron или совместимые с ними. Подробнее о числе процессоров, поддерживаемых разными выпусками Windows Server 2003, см. главу 1.
- Минимальный рекомендуемый объем ОЗУ — 256 Мб (минимально поддерживаемый — 128 Мб). Подробнее о максимальном объеме ОЗУ, поддерживаемом разными выпусками Windows Server 2003, см. главу 1. Если на компьютере установлено более 4 Гб ОЗУ, изучите информацию о совместимости оборудования на Web-узле Windows Catalog *(http://www.microsoft.com/windows/catalog/)*.

Примечание Windows Server 2003, Enterprise Edition, выполняющейся на компьютерах с процессорами Itanium, нужен один или несколько процессоров с минимальной тактовой частотой 733 МГц и ОЗУ объемом не менее 1 Гб.

- Раздел жесткого диска или том с достаточным свободным объемом для установки. Чтобы обеспечить гибкость при

дальнейшей работе с ОС, рекомендуется выделить значительно больше места, чем минимально необходимо для запуска программы установки (~1,5-2 Гб для компьютеров с процессором семейства x86 и 3-4 Гб для компьютеров с процессором Itanium). В случае запуска программы установки по сети или с компакт-диска, а также при установке ОС на раздел с файловой системой FAT или FAT32 потребуется больше свободного места (рекомендованная файловая система — NTFS).

По завершении работы программы установки ОС будет занимать больше места, чем изначально требовалось программе установки, так как потребуется дополнительное дисковое пространство для файла подкачки, устанавливаемых необязательных компонентов и (на контроллерах домена) для учетных записей пользователей и прочих данных Active Directory. Размер файла подкачки обычно равен 1,5 объемам ОЗУ. Подробнее о файле подкачки, необязательных компонентах, учетных записях пользователей и информации, хранимой в Active Directory см. Help and Support Center: по завершении установки раскройте меню Start и выберите Help And Support.

- Монитор VGA с разрешением 640x480 или более высоким (рекомендуется монитор Super VGA с разрешением 800x600 или более высоким), клавиатура и (необязательно) мышь или другое координатное устройство,

  В качестве альтернативы для работы без монитора или клавиатуры можно использовать процессор удаленной диагностики и поддержки, разработанный для продуктов семейства Windows Server 2003. Подробнее см. раздел Web-узла Windows Catalog (*http://www.microsoft.com/windows/catalog/*) с информацией о совместимости оборудования.
- Для установки с компакт-диска — привод CD-ROM или DVD-ROM.
- Для установки по сети — одна или несколько сетевых плат и соответствующие кабели. Нужен также сервер, который предоставит доступ по сети к файлам программы установки.
- Соответствующее оборудование для необходимой вам функциональности. Так. если вы планируете поддерживать сетевые клиенты, серверы и клиенты должны быть оснащены

сетевыми платами и кабелями. Если вам требуется кластер серверов, все компоненты кластерного решения должны быть совместимы с Windows Server 2003. Подробнее об оборудовании см. раздел Web-узла Windows Catalog *(http://www.mwrosoft.com/windows/catalog/)* с информацией о совместимости оборудования.

Совместимость оборудования

Перед установкой сервера важно убедиться, что оборудование совместимо с Windows Server 2003. Для этого можно запустить с установочного компакт-диска утилиту предварительной проверки на совместимость или просмотреть информацию о совместимости оборудования на Web-узле Windows Catalog. Нужно также убедиться, что используются обновленные драйверы устройств и обновленная BIOS компьютера (у компьютеров с процессорами Itanium должен быть обновленный интерфейс Extensible Firmware Interface). Независимо от того, запускаете ли вы утилиту предварительной проверки на совместимость, программа установки в начале работы проверяет совместимость оборудования и ПО и при обнаружении каких-либо проблем выводит отчет.

Предварительная проверка на совместимость

С установочного компакт-диска можно запустить утилиту предварительной проверки оборудования и ПО. Начинать установку ОС для проведения проверки не требуется. Есть два способа запустить проверяющую утилиту.

- Вставьте установочный компакт-диск в привод CD-ROM и затем следуйте инструкциям на экране для проверки системы на совместимость. В начале проверки вам предложат загрузить новейшие файлы программы установки (с помощью средства Dynamic Update). При наличии подключения к Интернету рекомендуется загрузить эти файлы.
- Вставьте установочный компакт-диск в привод CD-ROM, откройте окно командной строки и наберите rf:\i386\winnt32 **/checkupgradeonly**, где *d* — буква привода CD-ROM.

Проверка драйверов и BIOS компьютера

Убедитесь, что у вас есть новейшие драйверы для оборудования и новейшая BIOS (для компьютеров с процессором семейства x86) или интерфейс Extensible Firmware Interface (для компьютеров с процессором Itanium). Получить их можно у производителя оборудования,

Проверка устройств, не поддерживающих Plug and Play

Windows Server 2003 поддерживает технологию Plug and Play (PnP). позволяющую ОС автоматически распознавать устройства (например, видеокарты и сетевые платы), исключать конфликты и не заставлять пользователя задавать параметры всех устройств вручную, Тем не менее, если у вас есть устройства, не поддерживающие PnP или вы уверены, что ваши PnP-устройства спроектированы не в точном соответствии со стандартами. можно избежать конфликтов конфигурации устройств.

Чтобы проверить устройства на компьютере с установленной ОС, получите средствами ОС список текущих параметров устройств, например, используемых адресов памяти и прерываний. Так, в Windows NT 4.0 просмотреть эти параметры можно из Панели управления (раскройте меню Start\Settings, выберите Control Panel и затем дважды щелкните нужный значок, например Network and Ports). Можно также просмотреть информацию BIOS компьютера. Для этого изучите информацию на экране при загрузке компьютера и нажмите указанную клавишу.

В начале работы программа установки также автоматически проверяет устройства. Самостоятельная проверка устройств, не поддерживающих PnP или реализованных не в точном соответствии со стандартами данной технологии, позволяет избежать следующих проблем.

- Если два или больше адаптеров используют одинаковые прерывания или адреса памяти, программа установки может оказаться бессильна устранить конфликт. Во избежание этого можно:
  - перед запуском программы установки удалить одну из плат и затем переустановить ее (об установке и конфигурировании адаптеров и прочих устройств см. Help and Support Center);

- перед запуском программы установки изменить прерывание и адреса памяти, используемые одним из адаптеров, сделав тем самым параметры каждого адаптера уникальными.

- Если адаптеры не реагируют обычным образом на попытки программы установки найти их, она может получить неточные или не поддающиеся расшифровке данные. В этом случае может потребоваться перед ее запуском удалить эти устройства и затем переустановить их. Об установке и конфигурировании адаптеров и прочих устройств см. Help and Support Center.

Если перед запуском программы установки вы решили проверить устройства, не поддерживающие PnP, необходимо собрать следующую информацию (табл. 15-1).

Табл. 15-1. Проверка конфигураций устройств

Устройство	**Что необходимо** зафиксировать
Видеокарта	Тип видеокарты и набора микросхем, а также число видеокарт
Сетевой адаптер	Прерывание, адрес ввода-вывода, канал DMA (если используется), тип разъема (например BNC или витая пара) и тип шины
SCSI-контроллер	Модель или набор микросхем адаптера, прерывание и тип шины
Мышь	Тип мыши и используемый порт (COM1, COM2, PS/2 или USB)
Порт ввода-вывода	Для каждого порта ввода-вывода — прерывание, адрес ввода-вывода, канал DMA (если используется)
Звуковая карта	Прерывание, адрес ввода-вывода и канал DMA
USB (Universal serial bus)	Подключенные устройства и концентраторы
Платы PC Card	Какие платы установлены и в какие разъемы
Plug and Play	Включена ли поддержка данной технологии в BIOS
Настройки BIOS	Версия и дата выпуска **BIOS**

(см. след. стр.)

Табл. 15-1. Проверка конфигураций устройств *(продолжение)*

Устройство	Что необходимо зафиксировать
Внешний модем	Какой **COM-порт** занимает (COM1, **COM2 и т. д.)**
Внутренний **модем**	Какой COM-порт занимает; для нестандартных конфигураций — прерывание и адрес ввода-вывода
Advanced Configuration and Power Interface (ACPI)	Включена ли поддержка данной технологии; параметры питания, текущие параметры
PCI	**Какие** PCI-адаптеры установлены и в какие **разъемы**

Драйверы устройств массовой памяти и процесс установки

Если ваш контроллер массовой памяти (например, контроллер SCSI, RAID или Fibre Channel) совместим с Windows Server 2003 и вы знаете, что выпущен отдельный драйвер для вашей ОС, получите этот драйвер. В самом начале установки в нижней части экрана появится сообщение с предложением нажать клавишу F6. Следуя инструкциям на экране, предоставьте драйвер программе установки, чтобы та могла обращаться к контроллеру массовой памяти.

Если вы не уверены в необходимости получать у производителя отдельный драйвер для вашего контроллера массовой памяти, попробуйте запустить программу установки. Если на установочном компакт-диске не записан драйвер для вашего контроллера и программе установки нужен драйвер от производителя, будет выведено сообщение о том, что дисковые устройства не найдены, иди будет выведен неполный список контроллеров. Получив нужный драйвер, перезапустите программу установки и, увидев соответствующее сообщение, нажмите F6.

Примечание Информацию по проблемам совместимости см, на Web-узле Windows Catalog по адресу *http://www.microsoft.com/windows/catalog/*.

Нестандартный файл уровня абстрагирования от оборудования

Если производитель вашего компьютера предоставляет нестандартный файл уровня абстрагирования от оборудования (hardware abstraction layer, HAL), перед запуском программы установки найдите дискету или другой носитель с этим файлом. В начале установки в нижней части экрана появится предложение нажать клавишу F6 — нажмите F5 (не F6), чтобы включить файл HAL в процесс установки. Нажав F5, следуйте инструкциям на экране.

ACPI BIOS компьютеров с процессорами семейства x86

На компьютерах с процессором семейства x86 BIOS — это набор ПО, с помощью которого ОС (или программа установки) взаимодействует с устройствами компьютера. ACPI — это современный стандарт работы BIOS. Windows Server 2003 поддерживает не только ACPI-совместимые версии BIOS, но и некоторые другие, использующие старую архитектуру Advanced Power Management (APM) и PnP.

Некоторые версии BIOS на основе ACPI не полностью совместимы с последним стандартом. Чем новее версия BIOS, тем выше гарантия ее совместимости. BIOS на основе ACPI, несовместимая со стандартом ACPI, может не обеспечивать взаимодействия ОС (или программы установки) с оборудованием. Если это так, программа установки останавливает работу и сообщает о необходимости обратиться к поставщику оборудования или предлагает пути решения проблемы.

Вот что еще надо знать о совместимости BIOS с ACPI:

- Чтобы узнать версию BIOS, перед запуском программы установки перезагрузите компьютер и изучите текст на экране. Особое внимание уделите фрагментам текста со словами *BIOS* или *ACPI BIOS*.
- Чтобы узнать версию BIOS ваших устройств, изучите их документацию и обратитесь к поставщику оборудования.

Получение новейших драйверов с помощью средства Dynamic Update

Если компьютер с запущенной программой установки подключен к Интернету, в процессе установки можно задействовать средство Dynamic Update и получить самые новые файлы программы установки, включая драйверы и другие файлы. Если в важные файлы программы установки вносятся изменения, они будут доступны через службу Dynamic Update Web-узла Windows Update. Некоторые из обновленных файлов заменяют старые (например, обновленный драйвер или файл программы установки), а некоторые — дополняют (например, если на момент записи установочного компакт-диска драйвера не было). При запуске программы установки рекомендуется использовать средство Dynamic Update.

Работать с Dynamic Update весьма удобно,

- Файлы в разделе Dynamic Update Web-узла Windows Update тщательно проверены. Этот раздел содержит только файлы, действительно необходимые для корректной работы программы установки. Файлы с незначительными обновлениями, не оказывающими сильного влияния на функционирование программы установки, не распространяются через Dynamic Update.
- Dynamic Update загружает только необходимые для вашего компьютера файлы и поэтому проводит краткую проверку оборудования системы. Какая-либо личная информация не собирается и не сохраняется. Единственная цель проверки — выбрать подходящие драйверы для оборудования системы. Это позволяет максимально ускорить загрузку файлов и гарантирует, что на диск будут записаны лишь необходимые драйверы.
- Dynamic Update можно использовать при предварительной проверке на совместимость или в процессе установки ОС, В любом случае вы получите самые новые файлы для запуска программы установки. Подробнее о проверке на совместимость см. выше раздел «Совместимость оборудования».
- Dynamic Update можно использовать при установке, не требующей вмешательства оператора. Подготовка к этому включает несколько этапов. Подробнее об использовании Dynamic Update при установке, не требующей вмешательства (так-

же называемой автоматической установкой), см. книги «Microsoft Windows XP Professional Resource Kit» или «Microsoft Windows Server 2003 Deployment Kit».

Web-узел Windows Update (*http://windowsupdate.microsoft.com/*) предоставляет массу обновлений, которые можно использовать по завершении установки ОС.

Важные файлы, которые нужно просмотреть

Прежде чем запустить программу установки, ознакомьтесь с файлом Relnotes.htm, записанным в папке \Docs установочного компакт-диска Windows Server 2003. Он содержит важную информацию по использованию оборудования, работе с сетью, приложениям и печати, Также изучите информацию о совместимости оборудования с Windows Server 2003. Подробнее см. выше раздел «Совместимость оборудования».

Вопросы при новой установке

Ниже описаны вопросы, которые вам потребуется решить при установке ОС с нуля.

- **Выбор вида лицензирования** Продукты семейства Windows Server 2003 поддерживают два вида лицензирования: *Per Device or Per User* и *Per Server.* В режиме Per Device or Per User для каждого компьютера, обращающегося к серверу Windows Server 2003, нужна отдельная клиентская лицензия доступа (Client Access License, CAL). В режиме Per Server отдельная CAL нужна для каждого параллельного подключения к серверу. Подробнее о лицензировании см. ниже раздел «Выбор режима лицензирования».
- **Выбор ОС при запуске компьютера** Можно настроить компьютер так, чтобы при запуске выводилось меню выбора ОС. Подробнее см. ниже раздел «Установка нескольких операционных систем».
- **Выбор файловой системы для установочного раздела** Для установочного раздела можно выбрать одну из трех файловых систем: NTFS, FAT или FAT32. Обычно настоятельно рекомендуется использовать NTFS. Это единственная система, которая поддерживает Active Directory, включающую важные функции типа доменов и безопасности на основе

доменов. Если же компьютер с процессором семейства x86 нужно настроить так, чтобы иногда можно было запускать Windows Server 2003, а иногда — Windows NT 4.0, на базовом диске вам потребуется раздел с файловой системой FAT или FAT32. Подробнее см. ниже раздел «Выбор файловой системы».

- **Выбор раздела или тома для установки ОС** При установке с нуля изучите дисковые разделы и тома дисков (при обновлении используются существующие разделы и тома). И разделы, и тома делят диск на одну или больше областей, которые можно форматировать для одной файловой системы. Зачастую разным разделам и томам соответствуют разные буквы дисков (например C и D). После запуска программы установки можно изменять конфигурацию диска за исключением форматирования или изменения размера раздела/тома, содержащего ОС. Подробнее о планировании разделов и томов для новой установки см. ниже раздел «Планирование разделов диска».
- **Порядок обработки IP-адресов и разрешения имен TCP/IP.** При использовании протокола TCP/IP надо решить, как обрабатывать IP-адреса и разрешение имен (преобразование IP-адресов в имена, понятные пользователям). Подробнее см. ниже раздел «Настройка параметров сети».

Выбор вида лицензирования

Windows Server 2003 поддерживает два вида лицензирования: Per Device or Per User и Per Server. В режиме Per Device or Per User для каждого компьютера, обращающегося к серверу Windows Server 2003, нужна отдельная CAL. Имея одну CAL, конкретный клиентский компьютер может подключаться к любому числу серверов, работающих под управлением Windows Server 2003. Это наиболее распространенный метод лицензирования для компаний, имеющих более одного сервера Windows Server 2003 (рис. 15-1).

В режиме Per Server отдельная CAL требуется для каждого параллельного подключения к серверу. Иначе говоря, сервер поддерживает только ограниченное число подключений. Например, если выбрать режим лицензирования клиентов Per Server с 5 лицензиями, сервер будет обрабатывать только 5 па-

раллельных подключений (если каждому клиенту необходимо одно подключение, это означает 5 параллельных клиентов). Клиентам, использующим подключения, какие-либо дополнительные лицензии не нужны. Режим лицензирования Per Server зачастую выбирают небольшие компании, имеющие только один сервер. Кроме того, данный режим полезен для серверов Интернета и удаленного доступа, когда у клиентского компьютера может не быть лицензии сетевого клиента на подключение к Windows Server 2003. Можно указать максимально допустимое число параллельных подключений и отбрасывать дополнительные запросы на вход в систему (рис. 15-2).

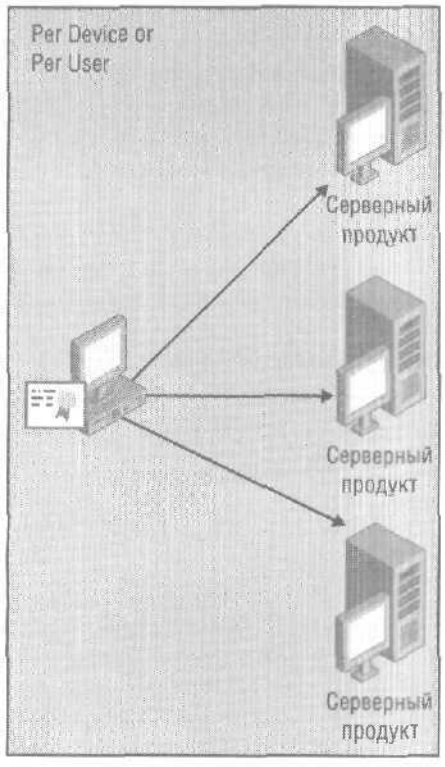


Рис. 15-1. Режим лицензирования Per Device or Per User

Если вы не знаете, какой режим вам нужен, выберите Per Server, так как у вас есть возможность однократно изменить

данный режим на Per Device or Per User без дополнительных затрат. Выбрав Per Server и завершив установку, просмотрите информацию о режимах лицензирования в Help and Support Center (раскройте меню Start и выберите Help and Support).

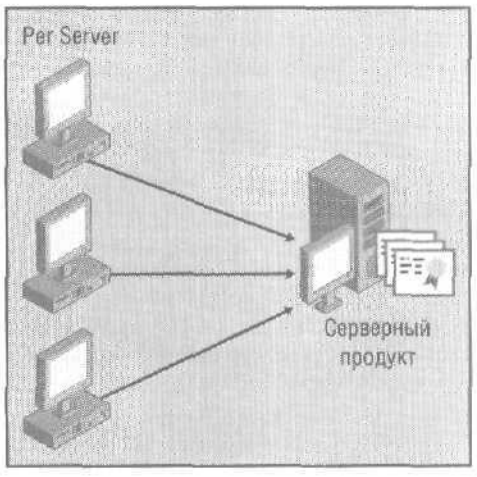


Рис. 15-2. Режим лицензирования Per Server

Установка нескольких операционных систем

На компьютере с подходящей конфигурацией диска (табл. 15-2) можно установить несколько ОС и затем при перезагрузке компьютера выбирать ОС для запуска.

Например, сервер с процессором семейства x86 можно настроить так, чтобы запускать преимущественно Windows Server 2003 и иногда, в целях поддержки старого приложения, Windows NT Server 4.0, И все же для этого вам потребуется выбрать определенную файловую систему и установить сервисный пакет версии 5 или более поздней (подробнее см. ниже разделы «Совместимость файловых систем» и «Выбор файловой системы»). При перезапуске компьютера в течение определенного времени будет отображаться меню выбора ОС для загрузки. (Можно указать ОС по умолчанию, которая будет запускаться, если при перезагрузке пользователь не выберет какую-то конкретную ОС),

В табл. 15-2 перечислены конфигурации диска, допускающие установку нескольких ОС.

Табл. 15-2. Требования к установке нескольких ОС

Конфигурация диска	Требования
Базовый диск (диски)	На базовый диск можно установить несколько ОС, включая Windows NT версии 4.0 и более ранних версий. Каждая ОС должна находиться на отдельном разделе или логическом диске накопителя. Раздел или логический диск — это секция диска, выступающая в качестве отдельной рабочей единицы. Зачастую разным разделам задают разные буквы дисков, например C и D.
Отдельный динамический диск	Возможна установка только одной ОС. Тем не менее, если вы средствами Windows 2000/XP преобразовали диск без разделов в динамический диск, перед установкой ОС его нужно преобразовать в базовый. Подробнее см. ниже.
Несколько динамических дисков	На каждом динамическом диске может размещаться одна установка Windows 2000/XP/Windows Server 2003. Запуск других ОС с динамического диска невозможен. Тем не менее, если вы средствами Windows 2000/XP преобразовали диск без разделов в динамический диск, перед установкой ОС его необходимо преобразовать в базовый.
Диск с главной загрузочной записью (Master Boot Record, MBR) на компьютере с процессором Itanium	На компьютерах с процессором Itanium запуск ОС с диска с MBR невозможен. Установка ОС возможна только на GPT-диск.
Диск с таблицей раздела GUID (GPT-диск) на компьютере с процессором Itanium	На GPT-дисках компьютеров с процессорами Itanium можно устанавливать одну или несколько ОС. Приведенные выше правила для базовых и динамических дисков также распространяются и на GPT-диски компьютеров с процессорами Itanium.

Примечание На компьютеры с процессорами Itanium можно устанавливать ОС Windows XP, 64-Bit Edition, 64-битную версию Windows Server 2003, Enterprise Edition, 64-битную версию Windows Server 2003, Datacenter Edition. Установка предыдущих ОС, скажем, Windows 2000, на такие компьютеры невозможна.

Если вы средствами Windows 2000/XP преобразовали диск без разделов в динамический диск, перед установкой ОС его надо преобразовать в базовый. При этом будут утеряны все данные, так что предварительно сделайте резервную копию. Затем средствами Windows 2000/XP можно сделать диск базовым или воспользоваться программой установки Windows Server 2003. Чтобы задействовать средства Windows 2000/XP, следуйте инструкциям справочной системы вашей ОС. Чтобы использовать программу установки Windows Server 2003, на этапе управления разделами найдите в списке разделов динамический диск и удалите его (при этом будут удалены данные на всех томах). Вам предложат подтвердить свои действия. Затем диск будет содержать только неразмеченную область, и с помощью программы установки вы сможете создать на нем новый раздел (базовый диск).

Причины для установки одной ОС

Сконфигурировав компьютер для возможности выбора ОС при запуске, вы получаете некоторое преимущество: можно использовать приложения, работающие только в конкретной ОС. Тем не менее лучше установить только одну ОС.

- Каждая ОС занимает ценное дисковое пространство,
- Возможны проблемы совместимости, например совместимости файловых систем. Подробнее см. ниже раздел «Совместимость файловых систем».
- На динамический диск можно установить только одну ОС. Кроме того, некоторые ОС не поддерживают динамические диски. Подробнее см. табл. 15-2.
- Теперь не требуется поддерживать несколько ОС как средство против проблем с запуском компьютера. Windows Server 2003 предоставляет вам разные варианты восстановления

системы. Так, в случае проблем с недавно установленным драйвером устройства можно выбрать безопасный режим работы, когда Windows Server 2003 перезапускается с парамтерами по умолчанию и минимальным набором драйверов.

Требования к установке нескольких ОС

Прежде чем решиться на установку нескольких ОС, изучите следующие ограничения.

- На компьютерах с MS-DOS и Windows Server 2003:
  - каждую ОС следует устанавливать на собственный раздел, а приложения, используемые в конкретной ОС — на один раздел с ней; если приложение используется в двух ОС, установите его на два раздела;
  - MS-DOS следует устанавливать на раздел базового диска с файловой системой FAT; если на системном разделе (это практически всегда первый раздел диска) MS-DOS не установлена, системный раздел также должен быть отформатирован в FAT;
  - Windows Server 2003 следует устанавливать последней, иначе могут быть перезаписаны важные файлы, необходимые для ее запуска;
  - возможна проблема совместимости файловых систем (см. ниже раздел «Совместимость файловых систем»).
- На компьютерах с Windows 98/Me/Server 2003:
  - каждую ОС следует устанавливать на собственный раздел, а приложения, используемые в конкретной ОС, — на один раздел с ней; если приложение используется в двух ОС, установите его на два раздела;
  - Windows 98/Me следует устанавливать на раздел базового диска с файловой системой FAT или FAT32; если на системном разделе (это практически всегда первый раздел диска) Windows 98/Me не установлена, системный раздел также должен быть отформатирован в FAT;
  - Windows Server 2003 следует устанавливать последней, иначе могут быть перезаписаны важные файлы, необходимые для ее запуска;
  - возможна проблема совместимости файловых систем (см. ниже раздел «Совместимость файловых систем»).

- О компьютерах с Windows NT 4.0 и Windows Server 2003 см, ниже разделы «Совместимость файловых систем» и «Мультизагрузка с Windows NT 4.0».
- На компьютерах с комбинацией из Windows Server 2003 и Windows 2000/XP, а также на компьютерах, содержащих несколько разделов с Windows Server 2003:
  - устанавливайте каждую ОС на собственный раздел или. в случае с динамическими дисками, на собственный диск, а приложения, используемые в конкретной ОС, — на один диск или раздел с ней; если приложение используется в двух ОС, установите его на два раздела/диска;
  - на разделах компьютеров с процессором семейства x86 можно устанавливать любые продукты из семейства Windows Server 2003; так, на одном разделе можно установить, Standard Edition, а на другом — Web Edition;
  - на компьютер с процессором Itanium можно установить Windows XP, 64-Bit Edition. 64-битные версии Windows Server 2003: Enterprise Edition и Datacenter Edition;
  - при установке Windows 2000 и Windows Server 2003 последнюю ОС следует устанавливать в последнюю очередь, иначе могут быть перезаписаны важные файлы, необходимые для запуска Windows Server 2003;
  - если компьютер включен в домен, для каждой установки используйте разные имена компьютеров; для каждой установки в домене применяется уникальный идентификатор безопасности (security identifier, SID), и поэтому имя компьютера во всех установках должно быть разным, даже если эти установки находятся на одном компьютере;
  - если вы собираетесь использовать шифрованную файловую систему (Encrypting File System, EFS), следует предпринять определенные меры для обеспечения доступности шифрованных файлов изо всех установок; подробнее см. ниже раздел «Шифрованная файловая система».

Совместимость файловых систем

На компьютерах с несколькими ОС при выборе файловой системы усложняются проблемы совместимости. Возможные файловые системы — NTFS, FAT и FAT32 (см. ниже раздел «Выбор файловой системы»).

Обычно рекомендуют NTFS: она наиболее эффективна и надежна и поддерживает важные функдии, включая Active Directory и безопасность на основе доменов. Если же вы используете NTFS и собираетесь устанавливать на компьютере несколько ОС, может возникнуть проблема совместимости, поскольку NTFS в Windows 2000/Server 2003 включает новые функции в дополнение к реализованным в Windows NT. В случае Windows 2000/Server 2003 файлы, использующие эти новые функции, будут полностью пригодны к работе. Однако зашифрованный файл будет нечитаем, если пользователь загрузит Windows NT Server 4.0, выпушенную до появления шифрования.

Примечание Если вы хотите установить на компьютере Windows NT и Windows Server 2003 и вам требуется раздел NTFS, вам подойдет лишь Windows NT 4.0 с установленным новейшим сервисным пакетом. Этот пакет максимизирует совместимость Windows NT 4.0 и Windows Server 2003 (если конкретнее, нужно установить сервисный пакет версии 5 или более поздней). И все же даже новейший сервисный пакет не предоставит доступа к файлам, использующим новые функции NTFS,

Использовать NTFS как единственную файловую систему на компьютере, содержащем и Windows Server 2003, и Windows NT, не рекомендуется. На таких компьютерах раздел FAT с Windows NT 4.0 гарантирует, что при запуске Windows NT 4.0 у компьютера будет доступ к нужным файлам. Кроме того, если на системном разделе (это практически всегда первый раздел диска) не установлена Windows NT, системный раздел рекомендуется отформатировать в файловой системе FAT.

Если настроить компьютер так, чтобы на разделе FAT была установлена Windows NT 3.51, а на разделе NTFS — Windows Server 2003, при загрузке Windows NT 3.51 раздела NTFS не будет видно. Если компьютер настроен именно так и раздел с Windows NT 3.51 не является системным (это практически всегда первый раздел диска), системный раздел надо также отформатировать в FAT.

Мультизагрузка с Windows NT 4.0

При установке на компьютер Windows NT 4.0 и Windows Server 2003 помните, что:

- если единственная задача — обеспечить гарантированную загрузку компьютера, настраивать его для выбора загружаемой ОС необязательно;
- использовать NTFS в качестве единственной файловой системы на компьютере с Windows Server 2003 и Windows NT не рекомендуется;
- убедитесь, что в Windows NT 4.0 установлен новейший сервисный пакет;
- устанавливайте каждую ОС на собственный раздел, а приложения, используемые в конкретной ОС, — на один раздел с ней; если приложение используется в двух ОС, установите его на два раздела;
- не устанавливайте Windows Server 2003 на сжатый диск, если тот сжат не средствами NTFS;
- устанавливать Windows Server 2003 нужно в последнюю очередь, иначе могут быть перезаписаны файлы, необходимые для ее запуска;
- если компьютер состоит в домене, используйте для каждой установки разные имена компьютеров.

Шифрованная файловая система

Если ваш сервер содержит комбинацию из Windows Server 2003 и Windows 2000/XP или включает несколько разделов с продуктами из семейства Windows Server 2003 и вы хотите использовать на нем EFS, нужно предпринять определенные меры, чтобы обеспечить чтение файлов из разных установок.

- Первый вариант — убедиться, что все установки относятся к одному домену и у их пользователя есть перемешаемый профиль.
- Второй вариант — экспортировать сертификат шифрования пользователя и сопоставленный ему закрытый ключ из одной установки и импортировать его в другие установки.

Подробнее о EFS, перемещаемых профилях пользователей, импорте/экспорте сертификатов см. Help and Support Center.

Выбор файловой системы

Установочный раздел можно отформатировать в одной из трех файловых систем: NTFS, FAT или FAT32. Обычно рекомендуется NTFS. Задействовать важные функции, например, Active Directory и безопасность на основе доменов, можно, только выбрав в качестве файловой системы NTFS.

Примечание На GPT-дисках (доступны только на компьютерах с процессорами Itanium) в качестве файловой системы установочного раздела рекомендуется NTFS. Если же на вашем компьютере с процессором Itanium есть небольшой раздел FAT емкостью 100 или более Мб. не удаляйте и не форматируйте его — он необходим для загрузки ОС.

В табл. 15-3 перечислены варианты установки ОС для компьютеров с процессорами семейства x86 (два последних варианта, в общем-то, редки), и для каждого из них приводятся советы по выбору файловой системы.

Табл. 15-3. Файловые системы для вариантов установки ОС

Вариант установки	Файловая система
В настоящий момент на компьютере используется NTFS (разделов FAT или FAT32 нет).	Продолжайте использовать NTFS, Дополнительной информации по файловым системам не требуется.
Компьютер с процессором x8б содержит один или несколько разделов FAT или FAT32 и только одну ОС; или на компьютере установлено несколько ОС, одна из которых Windows 2000/XP/Server 2003 и никаких других ОС.	Для компьютеров с процессором Itanium см. предыдущее замечание в этом разделе. Попробуйте отформатировать или преобразовать все разделы в NTFS.
На компьютере будет установлено несколько ОС, включая MS-DOS, Windows 95/98/Me.	Для разделов, к которым требуется обращаться из MS-DOS, Windows 95/98/Me, используйте FAT (в случае необходимости FAT32).
На компьютере будет установлено несколько ОС, включая Windows NT.	См. выше раздел «Совместимость файловых систем».

Форматирование или преобразование в NTFS

Если вы собираетесь установить Windows Server 2003 на имеющийся раздел FAT или FAT32 и хотели бы использовать NTFS, можно сделать следующее.

- Преобразовать раздел FAT или FAT32 в NTFS. При этом файлы останутся нетронутыми, хотя, возможно, у раздела будет более высокая степень фрагментации и более низкая производительность, чем у раздела, отформатированного в NTFS, Однако использовать NTFS выгодно независимо от того, был ли раздел отформатирован или преобразован в NTFS,

  При установке Windows Server 2003 на раздел FAT или FAT32 вам будет предложено преобразовать раздел в NTFS, Кроме того, преобразовать раздел FAT или FAT32 можно по завершении работы программы установки, используя утилиту Convert.exe, Чтобы получить дополнительную информацию о Convert.exe, по завершении работы программы установки наберите в командной строке **help** convert.
- Отформатировать раздел в NTFS. При этом удаляются все файлы раздела, но зато обеспечивается более высокая производительности и низкая фрагментация, чем в случае с преобразованным разделом.

Примечание Если на компьютере с процессором Itanium есть небольшой раздел FAT емкостью 100 или более Мб, не удаляйте и не форматируйте его — он необходим для загрузки ОС.

Если форматировать раздел в процессе установки, вам предложат на выбор NTFS или FAT. В табл. 15-4 описана взаимосвязь между размером раздела и файловой системой, предлагаемой при установке ОС.

Табл. 15-4. Форматирование разделов в процессе установки

Состояние раздела	Предлагаемая файловая система
Неотформатирован, размером меньше 2 Гб.	NTFS или FAT. Программа установки использует выбранную файловую систему.
Неотформатирован, размером от 2 до 32 Гб.	NTFS или FAT. При выборе FAT программа установки использует FAT32.

(см. след. стр.)

Табл. 15-4. Форматирование разделов ... *(продолжение)*

Состояние раздела	Предлагаемая файловая система
Неотформатирован, размером больше 32 Гб.	Только NTFS.
Ранее отформатированный в системе FAT32, размером больше 32 Гб. (Раздел, созданный средствами Windows 95/98/Me.)	Форматирования не требуется, хотя неформатированный раздел такого размера при форматировании в процессе установки или после нее для установки Windows Server 2003 будет использовать NTFS. Иначе говоря, имеющиеся разделы FAT32 такого размера поддерживаются Windows Server 2003.

При необходимости форматирования в процессе установки можно выполнить быстрое и полное форматирование.

- **Быстрое форматирование** На диске создается структура файловой системы без проверки целостности каждого сектора. Данный метод следует использовать для дисков, не содержащих поврежденных секторов и не имеющих проблем с файлами, которые, возможно, вызваны поврежденными секторами.
- **Полное форматирование** Выявляются и отслеживаются поврежденные сектора, чтобы их нельзя было использовать для хранения данных. Данный метод следует использовать для дисков, содержащих поврежденные сектора или имеющих проблемы с файлами, которые, возможно, вызваны поврежденными секторами.

Сравнение NTFS, FAT и FAT32

NTFS всегда была более мощной файловой системой, чем FAT и FAT32. В Windows 2000/XP/Server 2003 реализована новая версия NTFS, поддерживающая различные функции, включая службу Active Directory, необходимую для доменов, учетных записей и средств безопасности.

FAT и FAT32 аналогичны друг другу за исключением того, что FAT32 предназначена для дисков большего размера, чем FAT. Наиболее легко работает с дисками большого размера NTFS. Выбор файловой системы не влияет на доступ к файлам по сети. Так, использование NTFS на всех разделах сервера не сказывается на клиентах, подключающихся по сети к

общим папкам и файлам этого сервера, даже если клиенты работают под управлением Windows 98/NT. Ниже описаны размеры дисков и совместимость файловых систем с разными ОС.

- NTFS Компьютер с Windows 2000/XP/Server 2003 может обращаться к файлам на локальном разделе NTFS. Компьютер под управлением Windows NT 4.0 с установленным сервисным пакетом версии 5 или более поздней сможет обращаться лишь к некоторым из этих файлов. Прочие ОС не обеспечивают локального доступа. Рекомендуемый минимальный размер тома - ~10 Мб. Максимальные размеры тома и раздела начинаются с 2 Тб. Например, на динамическом диске, отформатированном с использованием стандартного размера файлового кластера (4 Кб), могут быть разделы размером 16 Тб минус 4 Кб. Максимальный размер файла потенциально равен 16 Тб минус 64 Кб, хотя файлы не могут быть больше тома или раздела, на котором они размещаются.
- FAT Обращаться к файлам на локальном разделе можно из MS-DOS, всех версий Windows, а также OS/2. Размер тома — от размера дискеты до 4 Гб. Максимальный размер файла — 2 Гб.
- FAT32 Обращаться к файлам локального раздела можно только из Windows 95 OSR2/98/Me/2000/XP/Server 2003. Windows Server 2003 позволяет считывать/записывать тома размером от 512 Мб до 2 Тб, а также форматировать тома размером до 32 Гб с использованием FAT32. Максимальный размер файла — 4 Гб.

Примечание На компьютерах с процессорами Itanium, включающих несколько дисков, можно выбирать не только файловую систему, но и тип раздела, определяющий порядок хранения информации. Есть два типа разделов. В разделах нового типа (используются только на компьютерах с процессорами Itanium) информация раздела хранится в GPT, в разделах старого типа — в MBR. Устанавливать Windows Server 2003 на компьютеры с процессорами Itanium следует на GPT-диск.

Возможности NTFS

Ниже описаны некоторые возможности NTFS.

- Усовершенствованная масштабируемость для больших дисков. Максимальный размер тома/раздела в NTFS гораздо больше, чем *в* FAT, и с ростом размера раздела производительность NTFS в отличие от FAT не падает.
- Служба Active Directory (и домены, ее составляющие). Active Directory упрощает просмотр и управление ресурсами сети. Домены позволяют точно конфигурировать параметры безопасности, не усложняя администрирование. Для контроллеров домена и службы Active Directory нужна NTFS.
- Средства сжатия, включая уплотнение и разуплотнение дисков, папок и отдельных файлов. Сжать файл и одновременно зашифровать его нельзя.
- Шифрование файлов, значительно повышающее безопасность. Зашифровать файл и одновременно сжать его нельзя.
- Разрешения, назначаемые отдельным файлам, а не только папкам.
- Служба Remote Storage, увеличивающая доступное дисковое пространство посредством повышения доступности съемных носителей, например лент.
- Ведение журнала дисковых операций, позволяющее NTFS быстро восстановить данные при сбоях питания и других системных проблемах.
- Разреженные файлы занимают лишь ограниченный объем дискового пространства. Имеется в виду, что NTFS выделяет дисковое пространство только тем частям файла, в которые производится запись.
- Дисковые квоты, позволяющие вести мониторинг и управлять объемом дискового пространства, выделяемого отдельным пользователям.

Это лишь часть возможностей NTFS, реализованных в Windows Server 2003. Подробнее о новых функциях см. главу 11.

Планирование разделов диска

Планировать дисковые разделы перед запуском программы установки следует, только если верны оба следующих утверждения.

- Вы устанавливаете систему с нуля, а не обновляете ее.
- Вы устанавливаете систему на базовый, а не на динамический диск. Базовые диски существовали до Windows 2000; большинство дисков — базовые. Динамические диски — это диски, бывшие базовыми и преобразованные средствами Windows 2000/XP/Server 2003 в динамические. Если вы собираетесь устанавливать ОС на динамический диск, изменить размеры разделов и томов в процессе установки нельзя, так что планировать эти размеры не нужно. В таком случае см. ниже раздел «Использование динамических дисков».

Создание разделов на диске — способ поделить его на отдельно функционирующие рабочие единицы. При создании разделов на базовом диске последний делится на одну или больше областей, которые можно форматировать с использованием файловой системы, например FAT или NTFS. Зачастую разным разделам задают разные буквы дисков (например C и D). На базовом диске может быть до четырех основных разделов или три основных и один дополнительный раздел (дополнительный раздел можно делить на логические диски, основной — нет).

Примечание Если вы собираетесь создавать или удалять разделы на диске, не забудьте создать резервную копию содержимого диска, поскольку в результате ваших действий будут удалены все данные.

Перед запуском программы установки для установки ОС с нуля определите размер установочного раздела. Специальной формулы для этой задачи нет. Основной принцип — выделить достаточно места для ОС, приложений и прочих файлов, которые будут храниться на установочном разделе. На компьютерах с процессором семейства x86 файлы для установки Windows Server 2003 занимают около 1,25-2 Гб, а на компьютерах с процессором Itanium — 3-4 Гб (см. выше раздел «Системные требования»). Рекомендуется выделять значительно больше пространства, чем минимально необходимо. Для больших установок не лишено смысла выделить на разделе 4-10 Гб или даже больше свободного места. Это позволит разместить на диске различные элементы, включая необязательные компонен-

ты, учетные записи пользователей, информацию Active Directory, журналы, сервисные пакеты, файл подкачки ОС и т. д.

При установке с нуля можно выбрать установочный раздел. Если указать раздел с другой ОС, вам предложат подтвердить ваш выбор.

В процессе установки создавайте только установочный раздел для Windows Server 2003. Для управления новыми и существующими дисками и томами по завершении установки служит утилита Disk Management. Она позволяет создавать новые разделы на основе неразмеченного дискового пространства, удалять/переименовывать/форматировать имеющиеся разделы, добавлять/удалять жесткие диски и преобразовывать базовые диски в динамические и обратно.

На компьютерах с процессорами Itanium, включающих несколько дисков, можно выбирать не только размер, но и тип раздела, определяющий порядок хранения информации. Есть два типа разделов. В разделах нового типа (применяются только на компьютерах с процессорами Itanium) данные раздела хранятся в GPT. В разделах старого типа информация хранится в MBR. На компьютерах с процессорами Itanium ОС Windows Server 2003 следует устанавливать на GPT-диск. GPT позволяет создавать больше разделов, тома большего размера, а также предоставляет другие преимущества. Подробнее о типах разделов на компьютерах с процессором Itanium см. справочную систему, а также книги «Server Management Guide» из комплекта ресурсов «Microsoft Windows Server 2003 Resource Kit».

Служба Remote Installation Services

Если вы собираетесь использовать на сервере службу Remote Installation Services для установки ОС на другие компьютеры, нужно создать для нее отдельный раздел NTFS. NTFS необходима функции Single Instance Store, которую предоставляет служба Remote Installation Services.

Новый раздел для службы Remote Installation Services следует создавать по завершении установки ОС; не забудьте оставить для него достаточно неразмеченного пространства (рекомендуется не менее 4 Гб). Как вариант, системный диск (но не диски кластера) можно сделать динамическим, чтобы задействовать пространство более гибко, чем на базовом диске.

Подробнее о службе Remote Installation Services и о вариантах создания дисков и разделов см. справочную систему.

Варианты создания разделов на диске

Изменять конфигурацию разделов диска средствами программы установки можно только при установке с нуля, но не при обновлении. Управлять разделами диска по завершении установки позволяет утилита Disk Management.

При установке с нуля программа установки изучает существующую конфигурацию жесткого диска и предоставляет следующие варианты.

- Если жесткий диск не разбит на разделы, можно создать установочный раздел для Windows Server 2003 и определить его размер.
- Если жесткий диск разбит на разделы, но содержит достаточно пространства, не входящего в разделы, можно создать на основе этого пространства установочный раздел для Windows Server 2003.
- Если на жестком диске есть раздел достаточного размера, можно установить на него Windows Server 2003 без предварительного форматирования раздела. В случае форматирования все данные раздела будут удалены. Если вы не будете форматировать раздел и установите Windows Server 2003 туда, где уже имеется ОС, та будет перезаписана, и вам потребуется переустановить все приложения, с которыми вы собираетесь работать в Windows Server 2003.
- Если на диске есть раздел, его можно удалить и создать неразмеченное пространство под установочный раздел для Windows Server 2003. При удалении раздела также удаляются все его данные.

Использование динамических дисков

Динамическим называется диск, основанный на новом типе хранилища, реализованном в Windows 2000. Если вы преобразовали диск в динамический и хотите установить на него ОС с нуля, помните следующее.

- Если вы средствами Windows 2000/XP преобразовали диск без разделов в динамический, перед установкой ОС его нужно

преобразовать в базовый. При этом будут утеряны все данные, так что предварительно сделайте резервную копию.

Сделать диск базовым можно средствами Windows 2000/XP, или можно использовать программу установки Windows Server 2003. О применении средств Windows 2000/XP см. справочную систему ОС. Чтобы задействовать программ) установки Windows Server 2003, на этапе управления разделами найдите в списке разделов динамический диск и удалите его (при этом будут удалены данные на всех томах). Вам предложат подтвердить свои действия. Затем диск будет содержать только неразмеченную область, и вы сможете с помощью программы установки создать на нем новый раздел (базовый диск).

- Если вы собираетесь повторно запустить программу установки на компьютере, где уже установлена Windows Server 2003 и где есть динамические диски, изучите ограничения на установку ОС на диски, преобразованные в динамические средствами Windows Server 2003. Подробнее см. соответствующие разделы в Help and Support Center.

Использование зеркальных, чередующихся и обычных томов

Средства управления дисками Windows NT 4.0 позволяют создавать наборы томов, зеркальные наборы, чередующиеся наборы и чередующиеся наборы с четностью, каждый со своими возможностями и ограничениями. Реализованная в Windows 2000 технология динамических дисков позволяет создавать такие же наборы и расширять дисковые тома без форматирования и изменения конфигурации разделов.

Такой переход от технологий Windows NT 4.0 означает, что перед запуском программы установки Windows Server 2003 нужно принять определенные решения. Наборы томов, зеркальные наборы, чередующиеся наборы и чередующиеся наборы с четностью, созданные средствами Windows NT 4.0, в Windows Server 2003 не поддерживаются, хотя Windows 2000 и предоставляет их ограниченную поддержку.

Если вы создали средствами Windows NT 4.0 набор томов, зеркальный набор, чередующийся набор или чередующийся набор с четностью и хотите установить на этом компьютере Windows Server 2003, вам потребуется следующее.

- **В случае с зеркальным набором — отменить зеркальное отражение** Если вы хотите установить Windows Server 2003 на компьютер, где имеется Windows NT 4.0 и зеркальный набор, создайте резервную копию данных и отмените зеркальное отражение. Прежде чем запустить программу установки Windows Server 2003, убедитесь, что установлен сервисный пакет версии 5 или более поздней.
- **В случае с набором томов, чередующимся набором или чередующимся набором с четностью — создать резервную копию данных и удалить набор** Если вы хотите установить Windows Server 2003 на компьютер с Windows NT 4.0 и набором томов, чередующимся набором или чередующимся с четностью, создайте резервную копию данных, а затем удалите набор (при этом будут удалены и данные). Прежде чем запустить программу установки Windows Server 2003, убедитесь, что установлен сервисный пакет версии 5 или более поздней. После запуска программы установки можно преобразовать диск в динамический, восстановить заархивированные данные и создать тома (см. раздел «Типы многодисковых томов на динамических дисках»). Подробнее о динамических дисках см. справочную систему.
- **Иисполь зовать утилиту Ftonline** Описанные выше методы рекомендуется применять при подготовке к запуску программы установки Windows Server 2003 на компьютере, включающем набор томов, зеркальный набор, чередующийся набор или чередующийся набор с четностью, созданный средствами Windows NT 4.0. Если вы не воспользовались данными методами и после запуска программы установки Windows Server 2003 вам нужно обратиться к одному из таких наборов, к вашим услугам Ftonline из пакета утилит Support Tools, поставляемого с Windows Server 2003. Подробнее см. соответствующие разделы справочной системы.

Типы многодисковых томов на динамических дисках

Описанные выше наборы дисков в Windows Server 2003 называются иначе, чем в Windows NT 4.0:

- набор томов — теперь перекрытый том на динамическом диске;
- зеркальный набор — зеркальный том на динамическом диске;

- чередующийся набор — чередующийся том на динамическом диске;
- чередующийся набор с четностью — том RAID-5 на динамическом диске.

Настройка параметров сети

Сетевой протокол TCP/IP предоставляет доступ в Интернет. Его использует большинство серверов, хотя на серверах можно устанавливать и дополнительные сетевые платы и соответствующие им протоколы. Программа установки и мастер Configure Your Server предназначены для простого конфигурирования TCPЯP и поддерживающих его служб.

Чтобы задействовать TCP/IP, убедитесь, что каждому серверу выделен IP-адрес — динамический, предоставляемый программно, или статический, который вы получили и задали компьютеру. Кроме того, надо дать пользователям удобные имена. Преобразование имен может осуществляться разными способами, преимущественно средствами DNS и WINS. Подробнее об этом см. ниже.

О TCP/IP, DHCP, DNS и WINS см. справочную систему и комплекты ресурсов, посвященные Windows Server 2003. Тематические разделы Help and Support см. по адресу *http://www.microsoft.com/windo wsserver2003/*.

IP-адресация

Для использования TCP/IP необходимо, чтобы каждому компьютеру был назначен IP-адрес. Есть два основных способа предоставить IP-адрес настраиваемому серверу,

- **Протокол DHCP** Чтобы предоставить IP-адреса компьютерам сети, можно установить один или несколько DHCP-серверов, динамически выделяющих IP-адреса другим машинам. Собственно DHCP-серверу должен быть назначен статический IP-адрес.

  Предоставлять DCHP и службы разрешения имен, DNS и WINS, могут один или несколько серверов. О службах разрешения имен см. ниже раздел «Разрешение имен».

  Если вы хотите запустить программу установки, не определившись с выбором DHCP-сервера и назначаемым ему статическим IP-адресом, щелкните в процессе установки в

диалоговом окне Networking Settings переключатель Typical Settings и настройте параметры сети позже. При этом, если в сети нет DHCP-сервера, программа установки задействует функцию автоматической закрытой IP-адресации (Automatic Private IP Addressing, APIPA). Сервер, использующий APIPA, может взаимодействовать только с применяющими APIPA компьютерами в этом же сегменте сети. Сервер, использующий APIPA, не может подключаться к Интернету (для просмотра страниц или электронной почты) и не может использоваться в DNS и службе Active Directory (она зависит от DNS).

Если вы определились с выбором DHCP-сервера, при его установке щелкните в диалоговом окне Networking Settings переключатель Custom settings и введите статический IP-адрес и прочие параметры сети. По завершении установки изучите информацию справочной системы и с помощью мастера Configure Your Server установите компонент DHCP и завершите конфигурирование DHCP-сервера.

- Статические IP-адреса Некоторым серверам в процессе установки или по ее окончании надо назначить статический IP-адрес и маску подсети. К таким относятся DHCP-, DNS- и WINS-серверы, а также серверы, предоставляющие пользователям доступ в Интернет. Рекомендуется также назначить статический IP-адрес и маску подсети всем контроллерам домена. Если на компьютере больше одного сетевого адаптера, им нужно назначить отдельные IP-адреса.

  Если вы хотите запустить программу установки, не определившись с назначаемым серверу статическим IP-адресом, щелкните в процессе установки в диалоговом окне Networking Settings переключатель Typical Settings и сконфигурируйте параметры сети позже. При этом, если в сети есть DHCP-сервер, программа установки получит IP-адрес от него. Если DHCP-сервера нет, программа установки воспользуется функцией APIPA (см. о ней выше).

  О статических IP-адресах, включая частные (выбираемые из определенных диапазонов адресов) и общедоступные (получаемые у поставщика услуг Интернета), см. справочную систему.

Разрешение имен

Сформировав план IP-адресации, нужно подумать, как осуществлять разрешение имен — сопоставление имени компьютера (имени, которое понятно пользователю и которое он может запомнить) с соответствующим IP-адресом. Это позволяет применять понятные имена, а не числовые IP-адреса, по которым серверы идентифицируют друг друга в сети TCP/IP. Есть две службы разрешения имен — DNS и WINS,

- DNS Эта иерархичная система имен служит для поиска компьютеров в Интернете и частных сетях TCP/IP. В большинстве установок нужен один или больше DNS-серверов. Служба DNS необходима для работы с Интернетом, электронной почтой и Active Directory. DNS зачастую играет роль службы разрешения имен в доменах, включающих клиенты под управлением Windows 2000/XP/Server 2003.

  При создании контроллера домена (или преобразовании сервера в контроллер домена) DNS устанавливается автоматически, если только Windows Server 2003 не определит, что в данном домене уже есть DNS-сервер. Кроме того, установить службу DNS позволяет мастер Configure Your Server или раздел Add/Remove Windows Components приложения Add Or Remove Programs, доступного в Control Panel.

  Чтобы установить на сервере DNS, назначьте ему статический IP-адрес и сконфигурируйте так, чтобы он использовал данный адрес для разрешения собственного имени. О назначении статического IP-адреса см. выше раздел «IP-адресация», о конфигурировании DNS — справочную систему.
- Windows Internet Naming Service Для поддержки клиентов под управлением Windows NT и более ранних ОС Microsoft вам, возможно, потребуется установить на одном или нескольких серверах домена службу WINS. Кроме того, WINS нужно установить, если она требуется вашим приложениям. Это можно сделать, используя мастер Configure Your Server или раздел Add/Remove Windows Components приложения Add Or Remove Programs, доступного в Control Panel.

  Если вы собираетесь установить на сервере службу WINS, назначьте ему статический IP-адрес. Подробнее см. выше раздел «IP-адресация», а о конфигурировании WINS — справочную систему.

Планирование серверов

Домены и служба каталогов Active Directory, частью которой они являются, предоставляют массу способов предоставления пользователям доступа к ресурсам, одновременно обеспечивая надежный мониторинг и безопасность. Об Active Directory см. главу 3.

В Windows Server 2003 серверы домена могут выполнять роли контроллера домена, содержащего сопоставляемые копии учетных записей и прочих данных Active Directory для данного домена, и рядового сервера, состоящего в домене и не содержащего копии данных Active Directory (сервер, включенный в рабочую группу, но не в домен, называется автономным). Можно изменять роль сервера с контроллера домена на рядовой сервер и обратно даже по завершении работы программы установки. И все же домен рекомендуется спланировать до запуска программы установки и изменять роли (и имена) серверов только при необходимости.

Несколько контроллеров домена обеспечивают лучшую поддержку пользователей, чем один контроллер. При наличии нескольких контроллеров у вас может быть несколько копий информации об учетных записях пользователей, а также прочих данных Active Directory; и все же важно регулярно архивировать данные, включая резервное копирование средствами Automated System Recovery, и знать методы восстановления контроллера домена. Кроме того, несколько контроллеров домена взаимодействуют для совместной реализации своих функций, например, проверки реквизитов при входе в систему.

Управляя доменами семейства Windows Server 2003, вы, возможно, захотите узнать о ролях хозяина операций. Это специальные роли, назначаемые одному или нескольким контроллерам домена Active Directory. Домены, выполняющие данные роли, осуществляют операции с одним хозяином (операции, одновременное выполнение которых в разных сегментах сети недопустимо). Так, идентификаторы безопасности для новых ресурсов (например, новых компьютеров) в целях обеспечения уникальности должны генерироваться одним контроллером домена.

Контроллеру домена, установленному первым, автоматически назначаются все роли хозяина операций. По завершении уста-

новки такое назначение можно изменить, однако обычно этого не требуется. Если на хозяине операций возникли проблемы или вы собираетесь снять с сервера данную роль, вам нужно знать о ролях хозяина операций как можно больше. О ролях хозяина операций, являющихся частью Active Directory, см. справочную систему Help and Support Center,

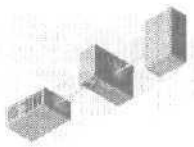
Дополнительные сведения

Дополнительные сведения см. по адресу:

- Руководство по развертыванию Microsoft Windows .NET Server — *http://www.microsoft.com/technet/prodtechnol/windows-netserver/evaluate/cpp/reskit/*.

ГЛАВА

16



Переход с Windows NT 4.0 Server

Microsoft Windows Server 2003 является значительным шагом вперед по сравнению с Microsoft Windows NT 4.0. Чтобы перейти на Microsoft Windows Server 2003 с семейства Windows NT 4.0 Server, не нужно устанавливать Windows 2000: достаточно установить Service Pack 5 или более позднюю версию.

Варианты обновления

Вы можете обновить до Windows Server 2003, Enterprise Edition:

- Windows NT Server 4.0 с Service Pack 5 или выше;
- Windows NT Server 4.0 Terminal Server Edition с Service Pack 5 или выше;
- Windows NT Server 4.0 Enterprise Edition с Service Pack 5 или выше.

Примечание Если версия установленной Windows NT меньше 4.0, вы не сможете напрямую обновить ОС до Enterprise Edition: сначала надо выполнить обновление до Windows NT 4.0 и установить Service Pack 5 или выше. Если у вас есть серверы или клиенты с Windows NT 3.51, вы должны выполнить установку или обновление до более новой ОС на всех этих компьютерах или прекратить их использование. Если у вас больше, чем один домен, этот шаг необходим для надежной проверки

правильности входа в систему. В остальных случаях этот шаг увеличит безопасность и сократит количество применяемых ОС, упростив тем самым управление и поиск неисправностей.

Потребность обновления может быть ясна даже при быстром взгляде на список предлагаемых усовершенствований.

- **Active Directory** Служба каталогов Active Directory включает улучшенные методы поиска и изменения местоположения или атрибутов объектов, утилиты с интерфейсом командной строки, прикладные разделы каталога, возможность добавлять контроллеры домена в существующие домены с использованием архивных носителей, универсальное кэширование членства в группах. Active Directory обеспечивает управление сетевыми средами масштаба предприятия.
- **Службы приложений** Усовершенствования Windows Server 2003 предоставляют много преимуществ разработчикам приложений, в том числе упрощение интеграции и взаимодействия, благодаря чему уменьшается общая стоимость владения (TCO) и повышается производительность.
- **Службы кластеризации** Установка в Windows Server 2003 проще и надежнее, чем в ранних версиях Windows, а улучшенные сетевые возможности обеспечивают защиту от сбоев.
- **Службы файлов и печати** Функция автоматического восстановления системы (ASR) упрощает восстановление системы, архивацию файлов и поддержку максимальной доступности. Улучшенная инфраструктура файловой системы упрощает использование, защиту и хранение файлов и других ресурсов. Необходимые ресурсы всегда доступны пользователям и могут быть легко восстановлены без помощи сотрудников службы поддержки.
- **Internet Information Services 6.0** В семействе Windows Server 2003 Microsoft полностью пересмотрела архитектуру службы IIS 6.0, чтобы учесть потребности клиентов крупных предприятий, поставщиков услуг Интернета (ISPs) и независимых поставщиков ПО (ISV).
- **Службы управления** Windows Server 2003 предоставляет централизованные, настраиваемые службы управления для

снижения TCO и упрощения развертывания, настройки и использования системы.

- **Организация сети и коммуникации** Улучшения и новые возможности сетевой организации в Windows Server 2003 расширяют универсальность, управляемость и надежность сетевых инфраструктур, базируясь на фундаменте, заложенном в Windows 2000 Server.
- **Безопасность** Функции безопасности Windows Server 2003 включают протокол ШЕЕ 802.1X (который упрощает защиту беспроводных ЛВС бизнес-окружения от прослушивания), шифрованную файловую систему (EFS), службы сертификатов и автоматическую регистрацию смарт-карт.
- **Управление устройствами хранения** Новые и улучшенные возможности управления устройствами хранения делают более простым и надежным управление дисками/томами. архивацию/восстановление данных и подключение к сетям хранения данных (SAN).
- **Сервер терминалов** Этот компонент Windows Server 2003 предоставляет более надежную, масштабируемую и управляемую компьютерную платформу на базе сервера. Это обеспечивает новые варианты развертывания приложений, более эффективный доступ к данным через подключения с низкой пропускной способностью.
- **Службы Windows Media Services** Этот серверный компонент технологии Windows Media Technologies предназначен для распространения цифрового медиа-контента через корпоративные сети и Интернет. В дополнение к традиционным службам цифрового распространения, таким как файловые и Web-службы, Windows Media предоставляют более надежные, масштабируемые, управляемые и экономичные решения для распространения потокового аудио и видео.

Windows Server 2003 также служит основанием для Microsoft .NET. Microsoft .NET разрешает беспрецедентный уровень интеграции ПО посредством использования Web-сервисов XML — небольших, дискретных, подобных строительным блокам приложений, соединяемых одно с другим (так же как и с другими, большими, приложениями) через Интернет.

Связанное с .NET ПО от Microsoft включает всестороннее семейство продуктов — клиентов для интеллектуальных уст-

ройств, служб, серверов и утилит, — поддерживающее XML и включающее промышленные стандарты Интернета. Разработка стала проще благодаря Microsoft Visual Studio .NET и Microsoft .NET Framework, которые не только изменили методы разработки приложений, но и сделали возможной разработку новых видов приложений.

Проверка системных требований

Прежде чем перейти к Windows Server 2003, надо убедиться, что обновляемый компьютер соответствует рекомендуемым системным требованиям и что все аппаратные компоненты совместимы с ОС. Если вы регулярно обновляли аппаратное обеспечение вашей системы Windows NT 4.0 Server, это не должно вызвать проблем. Но если ваш сервер работает на старом компьютере, вы можете рассмотреть вариант установки Windows Server 2003 на новый компьютер.

Системные требования

Самое существенное изменение — рекомендуемая скорость процессора. В то время как для Windows 2000 нужен процессор с тактовой частотой 133 МГц, Microsoft рекомендует процессор с тактовой частотой 550 МГц или более быстрый для Web Edition и Standard Edition и процессор с тактовой частотой 733 МГц или более быстрый для Enterprise Edition и Datacenter Edition. Требования к памяти и пространству на диске почти те же. О требованиях к оборудованию см. главу 1.

Дисковое пространство

Дисковое пространство и дисковые разделы — еще один фактор для принятия решения о том, что выполнить: обновление или чистую установку на новую систему. Например, если в данный момент сервер использует файловую систему FAT, в которой максимальный размер дискового раздела равен 2 Гб, вы не сможете выполнить обновление до Windows Server 2003, так как обновление требует более 2 Гб дискового пространства.

Если ваши серверы используют NTFS, в которой размер раздела может достигать 32 Гб, вы можете выполнить обновление до Windows Server 2003. Однако если вы хотите превысить предел в 32 Гб, потребуется установка с нуля.

Совместимость оборудования

Перед началом установки надо убедиться, что аппаратура совместима с Windows Server 2003. Вы можете сделать это, запустив программу проверки совместимости оборудования с установочного компакт-диска или проверив список совместимого оборудования, доступный на Web-сайте Microsoft. Выполните также проверку наличия обновленных версий драйверов устройств и обновлений системного BIOS (или для компьютеров на базе процессора Itanium обновленного Extensible Firmware Interface).

Если у вас есть контроллер устройств массовой памяти (такой как SCSI, RAID или адаптер Fibre Channel) для ваших жестких дисков, убедитесь, что он совместим с Windows Server 2003. щелкнув соответствующую ссылку в списке поддерживаемого оборудования.

Если ваш контроллер совместим с Windows Server 2003, но вы знаете, что изготовитель поставляет отдельный файл драйвера для использования с этими ОС, получите его (на дискете) до начала установки. В начале установки подсказка в нижней части экрана попросит вас нажать клавишу F6. Дальнейшие инструкции помогут предоставить файл драйвера, необходимый программе установки для доступа к контроллеру устройств хранения данных.

Если вы не уверены, нужен ли вам отдельный файл драйвера от производителя устройств массовой памяти, можно попытаться запустить программу установки. Если контроллер не поддерживается драйверами устройств, предоставленными на установочном компакт-диске, и нужен драйвер, предоставляемый производителем оборудования, программа установки остановится и сообщит о том, что дисковые устройства не обнаружены, либо отобразит неполный список контроллеров. Получив нужный драйвер, запустите заново программу установки и при появлении подсказки нажмите F6.

Независимо от того, выполнялась ли предварительная проверка совместимости оборудования, программа установки проверяет совместимость аппаратного и программного обеспечения и, обнаружив несовместимость, выводит отчет.

Service Pack 5 или более поздняя версия

Прежде чем обновлять Windows NT 4.0 до Windows Server 2003, надо установить Service Pack 5 или более позднюю версию. После этого можно выполнить прямое обновление до Windows Server 2003, не устанавливая Windows 2000. Если вы делаете чистую установку, Service Pack 5 не требуется.

Ресурсы совместимости

Полный список аппаратного и программного обеспечения, поддерживаемого ОС Windows, см. в каталоге Windows Catalog на Web-сайте Microsoft (*http:// www.microsoft.com/*).

Выбор между обновлением и новой установкой

При обновлении до Windows Server 2003 на вашем компьютере остается существующая Windows NT 4.0 (с Service Pack 5 или более поздней версии). Новая установка означает удаление предыдущей ОС или установку продукта семейства Windows .NET Server на диск без предыдущей версии ОС.

Доводы в пользу обновления

Для небольших организаций обновление обычно предпочтительнее новой установки. При обновлении упрощается настройка и сохраняются существующие пользователи, параметры, группы, права и разрешения. Кроме того, при обновлении не требуется повторная установка файлов и приложений. Не забудьте, однако, предварительно сделать резервную копию системы.

Дополнительные сведения см. в следующих источниках:

- обновление — тема «Operating Systems from Which You Can Upgrade» (раздел «Upgrading Compared with Installing» справочной системы Windows Server 2003);
- обновление в домене, включающем контроллеры домена под управлением Windows NT 4.0, — раздел «Upgrades in a Windows NT 4.0 Domain» в справочной системе.
- использование после обновления тех же приложений, что и раньше, — файл Relnotes.htm (папка \Docs на установочном компакт-диске); о совместимости приложений для продуктов семейства Windows Server 2003 — раздел совместимости ПО на Web-сайте Microsoft (*http://www.microsoft.com/*).

Доводы в пользу новой установки

Существуют серьезные доводы в пользу новой установки, особенно если речь идет о больших организациях. Если вы переформатируете жесткий диск и затем выполните новую установку. эффективность работы жесткого диска может возрасти. Кроме того, переформатирование позволяет изменить размеры или количество дисковых разделов.

Если вы хотите применять осторожное управление параметрами конфигурации, скажем, для сервера, которому требуется высокая доступность, вы можете предпочесть новую установку обновлению. Это особенно верно для серверов на которых в прошлом уже не раз обновлялась ОС.

Можно установить Enterprise Edition и позволить компьютеру иногда работать под управлением другой ОС. Однако тогда файловые системы могут вызвать проблемы.

Дополнительные сведения Об использовании нескольких ОС см. тему «Deciding Whether a Computer Will Contain More than One Operating System» в справочной системе Windows Server 2003.

Понимание ролей сервера

Сервер в домене может играть одну из двух ролей: рядового сервера или контроллера домена. Сервер, не входящий в домен является изолированным.

Рядовые серверы

Рядовой сервер — это компьютер, который:

- работает под управлением Windows NT 4.0 Server/2000 Server/ Server 2003;
- включен в домен;
- не является контроллером домена.

Рядовой сервер не регистрирует учетные записи и не участвует в репликации Active Directory или хранении информации политики безопасности домена. Он обычно работает как файловый сервер, сервер приложений, сервер БД, Web-сервер, сертификационный сервер, брандмауэр или сервер удаленного доступа.

Общими для всех рядовых серверов являются возможности, относящиеся к безопасности:

- рядовые серверы твердо придерживаются параметров групповой политики, определенных для сайта, домена или организационного подразделения;
- для ресурсов, доступных на рядовом сервере, существует контроль доступа;
- пользователям рядового сервера назначаются права пользователей;
- рядовой сервер хранит локальную БД учетных записей системы безопасности Security Accounts Manager (SAM).

Контроллеры домена

Контроллер домена:

- работает под управлением ОС Windows NT 4.0 Server/2000 Server/Server 2003;
- хранит доступную для записи и чтения копию БД домена;
- участвует в репликации с многими хозяевами;
- выполняет аутентификацию пользователей.

Контроллеры доменов хранят данные каталога и управляют связью между пользователями и доменами, в том числе процессом регистрации пользователей, аутентификацией и поиском в каталоге. Контроллеры домена синхронизируют данные каталога, применяя множественную репликацию, гарантируя соответствие информации по прошествии времени.

Active Directory поддерживает репликацию с множеством хозяев для данных каталога между всеми контроллерами домена в домене. Однако репликация с множеством хозяев не соответствует репликации некоторых данных каталога. В этом случае данные обрабатывает контроллер домена, называемый хозяином операций. В лесу Active Directory минимум пять различных ролей хозяина операций, которые могут быть назначены одному или нескольким контроллерам домена.

При изменении потребностей вычислительной среды может понадобиться изменение ролей сервера. Мастер Active Directory Installation Wizard позволяет повысить рядовой сервер до контроллера домена или понизить контроллер домена до рядового сервера.

Изолированные серверы

Изолированный сервер:

- работает под управлением Windows NT 4.0 Server/2000 Server/ Server 2003;
- не является членом домена.

Сервер, установленный как член рабочей группы, является изолированным и может использовать ресурсы совместно с другими компьютерами сети, но эти компьютеры не получат преимуществ, предоставляемых Active Directory. Подробнее см. справочную систему Windows Server 2003.

Active Directory

Служба каталогов Active Directory — это основная и неотделимая часть сетевой архитектуры Windows Server 2003, разработанная для распределенных сетевых сред. Она предоставляет единую точку для управления учетными записями пользователей Windows. клиентами, серверами и приложениями. Она также помогает объединить системы, не использующие Windows, с приложениями Windows и Windows-совместимыми устройствами,

Active Directory также позволяет улучшить защиту системы в Интернете, уменьшить общую стоимость вычислений, делая сетевую ОС Windows более управляемой, безопасной и коммуникабельной.

В качестве основы для иерархической организации данных Active Directory использует структурированное хранилище, также известное как каталог. Оно содержит информацию об объектах Active Directory. Объекты обычно представляют совместно используемые ресурсы, такие как серверы, тома и принтеры и учетные записи сетевых пользователей и компьютеров. Каталог хранится на контроллере домена и доступен для сетевых приложений или служб. Домен может иметь один или несколько контроллеров домена. Каждый контроллер домена имеет копию каталога для того домена, в который он входит.

Система безопасности объединена с Active Directory посредством аутентификации входа в систему и контроля доступа к объектам каталога. Используя единую сетевую регистрацию, администраторы могут управлять организацией и данными каталога по сети. Авторизованные сетевые пользователи полу-

чают доступ к ресурсам в любом месте сети. Администрирование на основе политик упрощает управление даже очень сложными сетями.

Служба каталогов Active Directory также включает следующее.

- Схема Active Directory Schema — это набор определений, описывающих виды объектов и типы информации об этих объектах, которые могут храниться в Active Directory. Сами определения хранятся как объекты, чтобы Active Directory могла управлять объектами схемы, используя те же операции управления, что и для управления остальными объектами каталога. Б схеме два типа определений: атрибуты и классы, которые называют объектами схемы или метаданными.
- **Глобальный** каталог **(ГК)** Содержит информацию о каждом объекте каталога. Это позволяет пользователям и администраторам искать информацию ГК независимо от того. какой домен в нем действительно содержит данные. ГК располагается на одном или нескольких контроллерах домена в лесу.
- **Механизм запросов и индексирования** Active Directory предоставляет пользователям и программам сведения об объектах каталога. Для поиска информации служит команда Search меню Start. Клиентские программы могут получить доступ к информации в Active Directory через интерфейс Active Directory Services Interface (ADSI).
- **Служба репликации** За исключением малых сетей данные каталога должны располагаться более чем в одном месте. Посредством автоматической репликации служба каталогов Active Directory управляет копиями, или репликами, данных каталога на каждом контроллере домена. Репликация Active Directory использует модель репликации с несколькими хозяевами. При репликации с несколькими хозяевами вы можете вносить изменения в каталог на любом контроллере домена, а не только на главном контроллером домена, и изменения будут реплицированы на все другие контроллеры домена.
- **Клиентское ПО** Компьютеры с Windows 95/98/NT 4.0 могут получить доступ ко многим возможностям Active Directory, доступным для Windows 2000 Professional/XP Professional, посредством запуска клиентского ПО Active Directory. Для

клиентских компьютеров, на которых не запущен клиент Active Directory, каталог выглядит точно так же, как каталог Windows NT.

Новые возможности Active Directory

Новые возможности Active Directory, доступные в Standard Edition, Enterprise Edition и Datacenter Edition, обеспечивают более эффективное администрирование Active Directory. Они делятся на те, что доступны на любом контроллере домена под управлением Windows Server 2003, и те, что доступны, только если все контроллеры домена в домене или лесу работают под управлением Windows Server 2003. Ниже приведены возможности Active Directory, разрешенные по умолчанию на любом контроллере домена под управлением Windows Server 2003.

- **Выбор нескольких пользовательских объектов** Одновременная модификация обших атрибутов для нескольких пользовательских объектов.
- Drag-and-drop Перемещение объектов Active Directory из контейнера в контейнер методом перетаскивания одного или нескольких объектов в новое место в иерархии домена. Объекты (один или несколько, включая другие объекты групп) можно добавлять к списку членства в группах, перетаскивая их на целевую группу.
- Поиск Можно осуществлять поиск без просмотра, сокращая тем самым сетевой траффик.
- Запись запросов Запись наиболее часто применяемых параметров поиска для их повторного использования в Active Directory Users and Computers.
- **Утилиты с интерфейсом командной строки для Active Directory Выполнение новых команд службы каталогов для сценариев** администрирования.
- Выборочное создание классов Создание экземпляров указанного класса, определенного в основной схеме леса Windows Server 2003. Вы можете создать экземпляры нескольких общих классов, включая страну или область, человека, *organizationalPerson*, *groupOfNames*, устройство и *certificationAuthority*.
- Класс *InetOrgPerson* Добавлен к основной схеме как участник безопасности, может использоваться так же, как класс

пользователей. Атрибут *userPassword* также может применяться для задания пароля учетной записи.

- **Прикладной раздел каталога** Настройка области действия репликации данных, относящихся к приложениям, среди контроллеров домена под управлением Standard Edition, Enterprise Edition и Datacenter Edition. Так, вы можете управлять репликацией данных зоны DNS, хранящихся в Active Directory, чтобы только указанные контроллеры домена в лесу участвовали в репликации зоны DNS.
- **Добавление контроллеров домена к существующему домену с использованием архивных носителей** Ускоряет данную операцию.
- **Универсальное кэширование членства в группах** Предотвращает необходимость поиска местоположения ГК в глобальной сети при регистрации, сохраняя универсальное членство пользователей в группе на выполняющих аутентификацию контроллерах домена,

Новые возможности Active Directory масштаба домена и леса функционируют, только если все контроллеры домена в домене или в лесу работают под управлением Windows Server 2003 и функциональность домена или леса установлена на Windows Server 2003. Ниже обобщены возможности Active Directory масштаба домена и леса, которые могут быть разрешены, если функциональный уровень домена или леса повышен до Windows .NET.

- **Утилита переименования контроллера домена** Переименование контроллеров домена без предварительного понижения их до рядовых серверов.
- **Переименование домена** Переименование любых доменов, работающих под управлением контроллеров домена с Windows Server 2003. Вы можете изменить имя NetBIOS или имя DNS любого потомка, родителя, корня дерева или корневого домена леса.
- **Доверие между лесами** Расширяет двустороннюю транзитивность области видимости одного леса на другой лес.
- **Реструктуризация леса** Перемещение существующих доменов на другое место в иерархии доменов.
- **Ненужные объекты схемы** Деактивизация неиспользуемых классов или атрибутов схемы.

- **Динамические вспомогательные классы** Динамическое привязывание вспомогательных классов к индивидуальным объектам, а не только к целым классам объектов. Вспомогательные классы, присоединяемые к экземплярам объектов, можно впоследствии удалить.
- **Настройка репликации ГК** Сохранение состояния синхронизации ГК, когда в результате административных действий частично расширяется набор атрибутов. Это минимизирует объем работы при частичном расширении набора атрибутов путем передачи только добавленных атрибутов.
- **Усовершенствования репликации** Репликация в сети индивидуальных членов группы, вместо того чтобы передавать целую группу как отдельную единицу репликации.

Совместимость с Windows NT 4.0

Служба каталогов Active Directory совместима с Windows NT 4.0 Server и поддерживает набор операций, осуществляемых контроллерами домена под управлением Windows NT 4.0/2000/ Server 2003. Это позволяет обновлять домены и компьютеры в нужном темпе,

Active Directory поддерживает протокол NTLM, используемый Windows NT. Это разрешает авторизацию пользователей и компьютеров из доменов Windows NT для регистрации и доступа к ресурсам в доменах Windows 2000/Server 2003. Для клиентов, работающих с Windows 95/98/NT без клиентского ПО Active Directory, домены Windows 2000/Server 2003 выглядят как домены Windows NT 4.0.

Переход к Active Directory может быть постепенным и выполняться без прекращения операций. При обновлении домена Windows NT сначала надо обновить главный контроллер домена. После этого обновлять рядовые серверы и рабочие станции можно в любое время.

Active Directory позволяет обновить любую модель домена Windows NT 4.0 и поддерживает как централизованную, так и децентрализованную модели доменов. Типичные модели доменов с одним или несколькими хозяевами легко обновить для леса Active Directory.

Обновление домена Windows NT

Мастер установки Active Directory упрощает обновление домена Windows NT до Windows Server 2003 Active Directory. Он устанавливает и настраивает контроллеры доменов, предоставляющие сетевым пользователям и компьютерам доступ к службе каталогов Active Directory. Мастер позволяет повысить любой рядовой сервер (кроме серверов с ограниченным лицензионным соглашением) до контроллера домена. При этом для нового контроллера домена определяется одна из ролей:

- новый лес (также новый домен);
- новый дочерний домен;
- новое дерево доменов в существующем лесу;
- дополнительный контроллер домена в существующем домене.

Обновление проходит в несколько этапов:

- планирование и внедрение пространства имен и инфраструктуры DNS;
- определение функциональности леса;
- обновление Windows NT 4.0 Server или более ранней версии на главном контроллере домена;
- обновление оставшихся резервных контроллеров домена;
- преобразование групп;
- завершение обновления домена;
- установка клиентов Active Directory на старых клиентских компьютерах.

Дополнительные сведения О мастере установки Active Directory см. справочную систему Windows Server 2003.

Планирование и внедрение пространства имен и инфраструктуры DNS

Пространства имен связаны с соглашениями о назначении имен, определяющими набор уникальных имен для сетевых ресурсов. К ним относится доменная система имен (DNS), иерархическая структура назначения имен, идентифицирующая каждый сетевой ресурс и его место в иерархии пространства имен и Windows-служба имен Интернета (WINS) — однородная структура назначения имен, идентифицирующая каждый сетевой ресурс с использованием единого, уникального имени.

DNS необходима для Active Directory. DNS — иерархическая распределенная БД — содержит отображение доменных имен DNS на разные типы данных, такие как IP-адреса. DNS позволяет использовать для определения местоположения компьютеров и служб понятные пользователю имена, а также получать другую информацию из БД.

При внедрении пространства имен рекомендуется сначала зарегистрировать уникальное родительское имя DNS, применяемое для поиска организации в Интернете, например microsoft.com. После того как выбрано имя родительского домена. можно комбинировать это имя с названием местоположения или организационного подразделения для формирования имен субдоменов, Если в дерево домена добавлен субдомен, скажем, itg.example.microsoft.com (для ресурсов, используемых ИТ-отделом), дополнительные имена субдоменов можно формировать, применяя это имя. Например, группа программистов, работающая в этом подразделении с электронным обменом данными, может иметь субдомен edi.itg.example.microsoft.com. Аналогично группа, обеспечивающая поддержку, может взять имя support.itg.example.microsoft.com.

Перед обновлением Windows NT 4.0 до службы Active Directory Windows Server 2003 убедитесь, что у вас разработаны пространства имен DNS и Active Directory и либо есть настроенный DNS-сервер, либо запланирована автоматическая установка DNS-сервера на контроллер домена с помощью мастера установки Active Directory.

Active Directory объединяется с DNS следующими способами.

- **Active Directory и DNS используют одну и ту же иерархическую структуру** Пространства имен для DNS и Active Directory имеют идентичную структуру, хотя внедряются поразному и предназначены для разных целей. Например, microsoft.com — это домен DNS и домен Active Directory.
- **Зоны DNS могут храниться в Active Directory** Если вы используете службу DNS Windows .NET Server, файлы первичной зоны могут храниться в Active Directory для их репликации на другие контроллеры домена Active Directory.
- **Active Directory использует DNS как поисковую службу для разрешения имен доменов Active Directory, сайтов и служб в IP-адреса** Для регистрации в домене Active Directory клиент Active Directory отправляет запрос указанному DNS-

серверу для получения IP-адреса службы Lightweight Directory Access Protocol (LDAP), запущенной на контроллере домена в указанном домене. Хотя Active Directory интегрирована с DNS и совместно использует одну и ту же структуру пространства имен, важно понимать различия между ними.

- DNS **является службой разрешения имен** Клиенты DNS отправляют запросы имен DNS указанному в их параметрах DNS-серверу. Тот принимает запрос имени и либо выполняет разрешение имени, используя локально хранящиеся файлы, либо консультируется с другим DNS-сервером. **DNS** не требует наличия Active Directory для работы.
- **Active Directory является службой каталогов** Active Directory предоставляет хранилище информации и службы, делающие эту информацию доступной пользователям и приложениям. Клиенты Active Directory отправляют запросы серверам Active Directory по протоколу LDAP. Для обнаружения сервера Active Directory клиент Active Directory отправляет запрос DNS. Active Directory требует для работы наличия DNS.

Дополнительные сведения О настройке DNS см. справочную систему Windows Server 2003.

Определение функциональных возможностей леса

Функциональные возможности леса определяют возможности Active Directory, которые будут разрешены в пределах данного леса. Каждый функциональный уровень леса имеет набор минимальных требований к версиям ОС, под управлением которых будут работать контроллеры домена в лесу. Так, функциональный уровень леса Windows .NET требует, чтобы все контроллеры домена работали под управлением Windows Server 2003.

Когда вы обновляете первый домен Windows NT, чтобы он стал первым доменом нового леса Windows Server 2003, рекомендуется (будет выведено сообщение) временно установить функциональный уровень леса на Windows .NET. Этот уровень включает все возможности, используемые в функциональном уровне леса Windows 2000, и еще два важных расширения возможностей Active Directory:

- улучшенные алгоритмы генерации в генераторе межсайтовой топологии;
- усовершенствованная репликация членства в группах,

Временный функциональный уровень леса Windows .NET, предлагаемый как параметр при обновлении первого домена Windows NT до нового леса, можно вручную настроить после обновления. Этот функциональный уровень поддерживается только контроллерами домена с Windows .NET/NT и не поддерживается контроллерами доменов с Windows 2000. Серверы Windows 2000 нельзя повысить до контроллера домена в лесу, для которого установлен временный функциональный уровень Windows .NET. О функциональных возможностях леса см. ниже в разделе «Расширение функционального уровня домена».

Обновление Windows NT 4.0 или более ранней версии на главном контроллере домена

Первым сервером под управлением Windows NT 4.0 или более ранней версии, который нужно обновить, является главный контроллер домена (PDC). В процессе обновления мастер установки Active Directory просит указать, осуществляется ли вхождение в имеющееся дерево или лес доменов либо начинается новое дерево или лес доменов. Выбрав вход в существующий домен, укажите ссылку на желаемый родительский домен,

Мастер установки Active Directory устанавливает необходимые компоненты контроллера домена, такие как ПО хранилища данных каталога и протокол аутентификации Kerberos V5. Сразу после установки Kerberos V5 запускаются служба аутентификации и служба предоставления билетов и, если это новый дочерний домен, устанавливаются транзитивные доверительные взаимоотношения с родительским доменом. В конечном счете контроллер домена из родительского домена копирует схему и конфигурационную информацию на контроллер нового дочернего домена. Существующие объекты Security Accounts Manager (SAM) копируются из реестра в новое хранилище данных. Эти объекты являются участниками системы безопасности.

Во время установки создаются объекты, содержащие учетные записи и группы из домена Windows NT. — Users, Computers и Builtin. Они отображаются как папки в Active Directory Users

And Computers. Учетные записи пользователей и предопределенные группы размещаются в папке Users, учетные записи компьютеров — в папке Computers, встроенные группы — в папке Builtin. Заметьте: это специальные контейнерные объекты, а не организационные подразделения. Их нельзя переместить, переименовать или удалить.

Существующие группы Windows NT 4.0 располагаются в разных папках в зависимости от природы группы. Встроенные локальные группы Windows NT 4.0 (такие как Administrators и Server Operators) помещаются в папку Builtin, глобальные группы Windows NT 4,0 (такие как Domain Admins) и любые созданные пользователем локальные и глобальные группы — в папке Users.

Обновленный PDC может синхронизировать изменения участников системы безопасности с оставшимися резервными контроллерами доменов (BDC) Windows NT 4.0. Он признается хозяином домена резервными серверами Windows NT Server 4.0.

Если контроллер домена под управлением Windows Server 2003 выключен или недоступен и в домене нет других контроллеров домена с Windows Server 2003, Windows NT BDC может быть повышен до PDC, чтобы выполнять роль отключенного контроллера домена с Windows Server 2003.

Обновленный контроллер домена является полнофункциональным членом леса. Новый домен добавляется в структуру сайтов и доменов, и все контроллеры доменов уведомляются о подключении к лесу нового домена.

Дополнительные сведения Подробности см. в справочной системе Windows Server 2003.

Обновление оставшихся резервных контроллеров домена

Как только вы обновили Windows NT 4.0 на PDC, можно обновлять все BDC. На время обновления можно удалить один BDC из сети, чтобы обеспечить наличие резервной копии. Данный BDC будет хранить защищенную копию текущей БД домена.

Если при обновлении возникнут проблемы, можно удалить все контроллеры домена с Windows .NET из производственной среды, вернуть в сеть BDC и сделать его новым PDC. Новый

PDC реплицирует свои данные в домене, что вернет домен в предыдущее состояние.

Единственный недостаток этого метода в том, что все изменения, сделанные после отключения защищенного BDC, теряются. Чтобы минимизировать потери, при обновлении можно периодически включать этот BDC и отключать его снова (когда домен находится в стабильном состоянии) для обновления безопасной копии каталога.

При обновлении доменов Windows NT 4.0 и более ранних только один контроллер под управлением Windows Server 2003 может создавать участников системы безопасности (пользователей, группы и учетные записи компьютеров). Этот контроллер домена настраивается как эмулятор PDC. Эмулятор PDC имитирует PDC Windows NT 4.0 и более ранних версий.

Дополнительные **сведения** О роли эмулятора PDC см. раздел «Operations Master Roles» справочной системы Windows Server 2003.

Преобразование групп

При обновлении главного контроллера домена с Windows NT 4.0 Server до сервера с Windows Server 2003 существующие группы Windows NT преобразуются:

- локальные группы Windows NT — в локальные группы домена на серверах с Windows Server 2003;
- глобальные группы Windows NT — в глобальные группы на серверах с Windows Server 2003.

Члены домена Windows NT могут продолжать отображать и полумать доступ к преобразованным группам. С точки зрения этих клиентов группы выглядят как локальные и глобальные группы Windows NT 4.0. Однако клиенты Windows NT не могут отображать членов групп или модифицировать их свойства, когда это членство нарушает правила групп Windows NT. Например, когда клиент Windows NT просматривает членов глобальной группы на сервере с Windows Server 2003, он не рассмагривает любые другие группы, являющиеся членами данной глобальной группы.

Преобразование групп и Microsoft Exchange

Microsoft Exchange позволяет организовывать адреса электронной почты в группы и списки рассылки. Когда сервер Exchange обновляется до Active Directory, списки рассылки Exchange преобразуются в группы рассылки с универсальной областью видимости. Администратор может преобразовать их в группы безопасности через Active Directory Users And Computers. Messaging Application Programming Interface (MAPI) разрешает компьютерам с предыдущими версиями клиентов Exchange просматривать преобразованные группы рассылки.

Использование преобразованных групп с серверами под управлением Windows Server 2003

Клиентские компьютеры, на которых не запущен клиент Active Directory, идентифицируют группы с глобальной областью видимости на сервере с Windows Server 2003 как имеюшие глобальную область видимости. При просмотре членов группы с универсальной областью видимости клиент Windows NT может обращаться только к тем членам группы, которые соответствуют правилам членства глобальных групп на серверах с Windows Server 2003.

В домене Windows Server 2003 с установленным функциональным уровнем домена Windows 2000 Native все контроллеры домена должны быть серверами Windows Server 2003. Однако домен может содержать рядовые серверы Windows NT Server 4.0, Эти серверы видят группы с универсальной областью видимости как имеюшие глобальную область видимости и могут назначать группам с универсальной областью видимости права и разрешения и размещать их в локальных группах.

В домене Windows Server 2003 утилиты администрирования. запускаемые на рядовых серверах Windows NT Server 4.0, не имеют доступа к локальным группам домена. Чтобы обойти это ограничение, используйте сервер Windows Server 2003 и пакет административных утилит Windows Server 2003 Administration Tools Pack. Эти утилиты позволяют отображать локальные группы домена и назначать им разрешения для ресурсов на серверах с Windows NT Server 4.0.

После того как все главные и резервные контроллеры домена с Windows NT 4.0 будут обновлены до Windows Server 2003 и если вы не планируете использовать контроллеры домена

Windows NT 4.0. можно повысить функциональный уровень домена с Windows 2000 Mixed до Windows 2000 Native. О повышении функционального уровня домена см. ниже раздел «Повышение функционального уровня домена».

При повышении функционального уровня домена до Windows 2000 Native происходит следующее.

- Контроллер домена более не поддерживает репликацию NTLM.
- Контроллер домена, эмулирующий хозяина операций PDC больше не синхронизирует данные с BDC Windows NT 4.0 и более ранних версий.
- Контроллеры домена с Windows NT 4.0 и более ранними версиями не могут быть добавлены к домену (вы можете добавлять контроллеры домена с Windows 2000/Server 2003).
- Пользователи и компьютеры, которые работают с предыдущими версиями Windows, получают преимущества от транзитивного доверия Active Directory и (при условии надлежащей авторизации) могут обращаться к ресурсам, расположенным в любом месте леса. Хотя предыдущие версии Windows не поддерживают Kerberos V5, обеспечиваемая контроллерами домена передача аутентификации позволяет пользователям и компьютерам быть аутентифицированными в любом домене леса. Благодаря этому пользователи и компьютеры могут обращаться к ресурсам, для которых они имеют соответствующие разрешения, в любом домене леса. Другой стороной усовершенствованного доступа к любым другим доменам в лесу, является то, что клиенты не будут знать об изменениях в домене.

Установка клиента Active Directory на старых компьютерах

Компьютеры с клиентским ПО Active Directory могут использовать возможности Active Directory, такие как аутентификация для доступа к ресурсам в дереве доменов или лесу и запросы к каталогу. По умолчанию клиентские компьютеры с Windows XP Professional/2000 Professional имеют встроенное клиентское ПО и могут нормально обращаться к Active Directory,

Однако компьютеры под управлением предыдущих версий Windows (Windows 98/95/NT) требуют установки клиента Active Directory, чтобы получить доступ к ресурсам Active Directory,

Без клиентского ПО предыдущие версии Windows могут получить доступ к домену только как к домену Windows NT 4.0 или более ранней версии, находя только те ресурсы, что доступны для домена Windows NT 4.0 с односторонним доверием.

Когда функциональный уровень домена установлен на Windows 2000 Mixed, контроллер домена предоставляет клиентам, которые используют предыдущие версии Windows, только те ресурсы домена, для которых ранее в Windows NT 4.0 было установлено явное доверие. Это создает последовательную среду, где предыдущие версии клиентов могут получать доступ только к ресурсам домена с явным доверием независимо от того, под управлением какой системы работает контроллер домена — Windows Server 2003 или Windows NT 4.0.

Повышение функционального уровня домена

Для домена можно задать три функциональных уровня: Windows 2000 Mixed (значение по умолчанию, домен включает контроллеры домена с Windows 2000/NT 4.0/Server 2003), Windows 2000 Native (включает контроллеры доменов с Windows 2000/Server 2003), и Windows Server 2003 (включает только контроллеры домена с Windows Server 2003).

Когда все контроллеры домена работают под Windows Server 2003, можно повысить функциональный уровень домена и леса до Windows Server 2003 открыв окно Active Directory Domains And Trusts, щелкнув правой кнопкой домен, для которого вы хотите повысить функциональный уровень, а затем — Raise Domain Functional Level.

После повышения функционального уровня домена нельзя добавить в домен контроллеры домена, работающие под управлением предыдущих версий ОС. Так, если вы повышаете функциональный уровень домена до Windows Server 2003, в него нельзя будет добавить контроллеры домена, работающие под Windows 2000 Server.

В табл. 16-1 перечислены возможности масштаба домена, разрешенные для соответствующих функциональных уровней.

Табл. 16-1. Возможности масштаба домена

Возможность домена	Windows 2000 Mixed	Windows 2000 Native	Windows Server 2003
Утилита переименования контроллера домена	Запрещено.	Запрещено.	Разрешено.
Обновление временных меток входа в систему	Запрещено.	Запрещено.	Разрешено.
Номера версий ключей Kerberos KDC	Запрещено.	Запрещено.	Разрешено.
Пароль пользователя для объекта *InetOrgPerson*	Запрещено.	Запрещено.	Разрешено.
Универсальные группы	Разрешено для групп рассылки.	Разрешено.	Разрешено.
	Запрещено для групп безопасности.	Допускается как для групп безопасности, так и для групп рассылки.	Допускается как для групп безопасности, так и для групп рассылки.
Вложение групп	Разрешено для групп рассылки.	Разрешено.	Разрешено.
	Запрещено для групп безопасности, исключая локальные группы безопасности домена, которые могут в качестве членов иметь глобальные группы.	Допускает полное вложение групп.	Допускает полное вложение групп.

(см. *след, стр.)*

Табл. 16-1. **Возможности масштаба домена** *(продолжение)*

Возможность домена	Windows 2000 Mixed	Windows 2000 Native	Windows Server 2003
Преобразование групп	Запрещено.	Разрешено.	**Разрешено.**
	Преобразование групп не разрешается.	Разрешено преобразование между группами безопасности и группами рассылки.	Разрешает преобразование между группами безопасности и группами рассылки.
История SID	Запрещено.	Разрешено.	Разрешено.
		Разрешает миграцию участников безопасности из одного домена в другой.	**Разрешает** миграцию **участников** безопасности из одного **домена в** другой.

Повышение функционального уровня леса

Функциональные возможности леса разрешены для всех доменов в лесу. Доступны два функциональных уровня леса: Windows 2000 (поддерживает контроллеры доменов с Windows NT 4/2000/ Server 2003) и Windows Server 2003 (поддерживает только контроллеры домена под Windows Server 2003). Если вы обновляете первый домен Windows NT, который станет первым доменом в новом лесу Windows Server 2003, можете выбрать дополнительный функциональный уровень леса (Windows .NET interim).

По умолчанию для леса устанавливается функциональный уровень Windows 2000. Вы можете повысить функциональный уровень леса до Windows Server 2003. После этого в него нельзя будет добавлять контроллеры домена, работающие под управлением ранних версий ОС.

Следующие возможности масштаба леса разрешены для соответствующих функциональных уровней (табл. 16-2).

Табл. 16-2. Возможности масштаба леса

Возможности леса	Windows 2000	Windows Server 2003
Настройка репликации ГК	Запрещено.	Разрешено.
Отключение объектов схемы	Запрещено.	Разрешено.
Доверие между лесами	Запрещено.	Разрешено.
Связанные значения репликации	Запрещено.	Разрешено-
Переименование доменов	Запрещено.	Разрешено.
Улучшенный алгоритм репликации	Запрещено.	Разрешено.
Динамические вспомогательные классы	Запрещено.	Разрешено.
Изменение класса объектов *InetOrgPerson*	Запрещено.	Разрешено.

Контроллеры домена

Обновление до Active Directory может быть постепенным и выполняться без прерывания операций. Если вы следуете рекомендациям по обновлению домена, отключать домен для обновления контроллеров домена, рядовых серверов или рабочих станций не потребуется.

В Active Directory доменом называется определяемый администратором набор объектов компьютеров, пользователей и групп. Эти объекты совместно используют общую БД каталога, политики безопасности и отношения безопасности с другими доменами. Лес -- это набор из одного или нескольких доменов Active Directory, совместно использующих одни и те же определения классов и атрибутов (схему), сайты и информацию репликации (конфигурацию) и возможности поиска в масштабе леса (ГК). Домены одного леса связаны двусторонними транзитивными доверительными взаимоотношениями.

При подготовке обновления домена, содержащего контроллеры домена с Windows 2000, рекомендуется применить Service Pack 2 или выше ко всем контроллерам домена с Windows 2000.

Перед обновлением ОС контроллера домена с Windows 200I3 до Windows Server 2003 или установкой Active Directory на первый контроллер домена под управлением Windows Server 2003 убедитесь, что ваш сервер, лес и домен подготовлены.

При обновлении контроллеров домена полезны две утилиты с интерфейсом командной строки.

- **Winnt32** Проверяет совместимость сервера с обновлением.
- Adprep Используйте на хозяине операций схемы для подготовки леса. Выполнение Adprep на хозяине схемы модифицирует схему, после чего она реплицируется на все другие контроллеры домена в лесу.

Вы не можете обновить контроллеры домена с Windows 2000 до Windows Server 2003 или добавить контроллеры домена с: Windows Server 2003 к доменам Windows 2000, пока не используете Adprep для подготовки леса и доменов в лесу.

Дополнительные сведения Об утилитах командной строки и об обновлении контроллеров домена см. в справочной системе Windows Server 2003.

Работа со службами удаленной установки

Все выпуски Windows Server 2003, кроме Web Edition, включают службы удаленной установки (RIS), обеспечивающие изменения и управление конфигурацией, также включенные в Windows 2000. RIS разрешает удаленно устанавливать ПО на кли-

ентские компьютеры. RIS позволяет установить ОС на удаленном клиентском компьютере с возможностью удаленной загрузки путем подключения компьютера к сети, запуска клиентского компьютера и регистрации под допустимой учетной записью пользователя.

Если в сети используется RIS с Windows NT 4.0 Server, сервер RIS должен быть первым компьютером, обновляемым до Windows Server 2003. Если этого не сделать, позднее вы не сможете использовать RIS из-за изменений в способах, которыми Active Directory выполняет аутентификацию. Обновление сервера RIS до Windows Server 2003 позволяет ему устанавливать соединение как с оставшимися контроллерами домена Windows NT 4.0, так и с контроллерами домена Windows Server 2003.

Ресурсы для развертывания

Для развертывания контроллеров домена с Windows Server 2003 рекомендуется применять Windows Server 2003 Deployment Kit, доступный в Интернете на Web-сайте Microsoft Windows Deployment and Resource Kits (*http://www.microsoft.com/windows/reskits/*).

Сетевой комплект развертывания включает описание вариантов и необходимую информацию для развертывания Windows Server 2003 Active Directory в сетях с контроллерами доменов под управлением Windows NT 4.0/2000. Если ваша сеть включает филиалы, обратитесь к разделу «Designing the Site Topology» в Microsoft Windows Server 2003 Deployment Kit (Microsoft Press, 2003). Это сетевое руководство поможет планировать развертывание Active Directory, когда сайты филиалов подключены через медленные сетевые соединения.

Переименование контроллеров домена

Переименование контроллеров домена с Windows Server 2003 обеспечивает:

- изменение структуры сети для организационных или деловых потребностей;
- более простое управление и административный контроль.

При переименовании контроллера домена нужно гарантировать, что для клиентов не будет перерыва в возможности обнаруживать переименованный контроллер домена и выпол-

нять аутентификацию на нем, кроме тех случаев, когда контроллер домена перезапускается,

Другое требование для переименования домена — установка функционального уровня домена в Windows Server 2003. Новое имя контроллера домена автоматически изменяется в DNS и Active Directory. Как только новое имя будет размножено в DNS и Active Directory, клиенты смогут обнаруживать переименованный контроллер домена и использовать его для аутентификации. Задержка репликации DNS и Active Directory может задержать возможность обнаружения переименованного контроллера домена клиентами и его использования для аутентификации. Длительность задержки зависит от параметров сети и топологии репликации в организации.

В течение задержки репликации клиенты не могут обращаться к недавно переименованному контроллеру домена. Это приемлемо для клиентов, пытающихся обнаружить конкретный контроллер домена и выполнить аутентификацию, так как другие контроллеры домена должны быть способны обработать запрос аутентификации.

Работа с доверием доменов

Все доверительные отношения в рамках леса Windows 2000/ Server 2003 являются транзитивными и двухсторонними. Поэтому оба домена автоматически доверяют друг другу. Это значит, что, если домен A доверяет домену B и домен B доверяет домену C, пользователи из домена C (которым назначены соответствующие разрешения) могут получить доступ к ресурсам домена A.

Протоколы доверия

Контроллеры доменов с Windows Server 2003 аутентифицируют пользователей и приложения, применяя один из двух протоколов: Kerberos V5 или NTLM. Kerberos V5 используется по умолчанию на компьютерах с Windows 2000/XP Professional/ Server 2003. Если какой-либо из вовлеченных в транзакцию компьютеров не поддерживает Kerberos V5, применяется протокол NTLM.

С протоколом Kerberos V5 клиент запрашивает у контроллера домена его учетной записи билет на сервер в доверенном ломене. Этот билет выпускается посредником, которому дове-

ряют и клиент, и сервер. Клиент предъявляет этот билет серверу в доверенном домене для аутентификации.

Когда клиент пробует получить доступ к ресурсам на сервере в другом домене, используя аутентификацию NTLM, сервер, содержащий ресурс, должен установить соединение с контроллером домена учетной записи клиента для проверки параметров учетной записи.

Объекты доверия доменов

Объекты доверия доменов (TDO) представляют каждое доверительное отношение в пределах отдельного домена. Каждый раз, когда устанавливается доверие, создается уникальный TDO и сохраняется (в контейнере System) в его домене. В TDO представляются такие атрибуты, как транзитивность доверия, его тип и имя партнерского домена.

TDO для доверия между лесами хранят дополнительные атрибуты, чтобы идентифицировать все доверенные пространства имен из партнерского леса: имена деревьев доменов, основные суффиксы имен пользователя, основные суффиксы имен служб и идентификаторы безопасности пространств имен.

Нетранзитивное доверие и Windows NT 4.0

Нетранзитивное доверие ограничено только двумя доменами, установившими доверительные отношения, и не распространяется на другие домены в лесу. Нетранзитивное доверие может быть одно- или двусторонним.

Нетранизитивное доверие — одностороннее по умолчанию, хотя вы можете установить и двусторонние отношения, создав два односторонних доверия. Нетранзитивное доверие — единственная возможная форма доверительных отношений между

- доменом Windows Server 2003 и доменом Windows NT;
- доменом Windows Server 2003 в одном лесу и доменом в другом лесу (которые не объединены доверием лесов).

Мастер New Trust Wizard позволяет вручную создать следующие нетранзитивные доверия,

- Внешнее доверие Нетранзитивное доверие между доменом Windows Server 2003 и доменом Windows NT/2000/Server 2003 в другом лесу. Когда вы обновляете домен Windows NT до Windows Server 2003, все существующие доверия Windows NT

остаются неизменными. Все доверительные отношения между доменами Windows Server 2003 и доменами Windows NT нетранзитивны.

- Доверие области Нетранзитивное доверие между доменом Active Directory и областью Kerberos V5.

Внешнее доверие и Windows NT 4.0

Вы можете создать внешнее доверие как форму одностороннего нетранзитивного отношении с доменами вне вашего леса. Внешнее доверие необходимо, когда пользователю нужен доступ к ресурсам в домене Windows NT 4.0 или в домене в отдельном лесу, не объединенном доверием лесов.

Когда установлено доверие между доменом в отдельном лесу и доменом вне его, участники системы безопасности из внешнего домена могут обращаться к ресурсам во внутреннем домене. Active Directory создает во внутреннем домене объект *внешнего участника безопасности* (foreign security principal) для представления каждого участника системы безопасности из доверенного внешнего домена. Эти внешние участники безопасности могут быть членами локальных групп внутреннего домена. Локальные группы домена могут включать членов из доменов вне леса.

Объекты каталога для внешних участников безопасности создаются Active Directory и не модифицируются вручную. Вы можете просмотреть объекты внешних участников безопасности из Active Directory Users And Computers, разрешив дополнительные возможности.

Дополнительные сведения О дополнительных возможностях см. раздел «To View Advanced Features» в справочной системе Windows Server 2003.

Для создания внешнего доверия надо иметь права Enterprise Admin или Domain Admin для домена в лесу Windows Server 2003 и Domain Admin — для домена вне леса. Каждому доверию назначается пароль, который должен быть известен администраторам обоих участвующих в отношении доменов,

В смешанных доменах Windows 2000 внешнее доверие всегда должно удаляться с контроллера домена Windows Server 2003, Внешнее доверие к доменам Windows NT 4.0/3.51 может быть

удален авторизованным администратором на контроллере домена Windows NT 4,0/3.51. Однако на контроллере домена Windows NT 4.0/3.51 может быть удалена только доверяемая сторона отношения. Доверительная сторона отношения (созданная в домене Windows Server 2003) не удаляется, и, хотя она больше не действует, доверие по прежнему отображается в Active Directory Domains And Trusts. Для полного удаления доверия нужно удалять доверие на контроллере домена Windows Server 2003 в доверяющем домене, Если внешнее доверие по ошибке удалено на контроллере домена Windows NT 4.0/3.51, его можно создать заново с любого контроллера домена Windows Server 2003 в доверяющем домене.

Выполнение некоторых задач Windows NT в Windows Server 2003

В табл. 16-3 перечислены общие задачи настройки Active Directory. Пользовательский интерфейс для выполнения этих задач в рассматриваемой версии Windows отличается от способа, применявшегося в Windows NT 4.0.

Табл. 16-3. Выполнение задач настройки Active Directory

Задача	В Windows NT 4.0 используется	В Windows Server 2003 используется
Установка контроллера домена	Windows Setup	Мастер установки Active Directory
Управление учетными записями пользователей	User Manager	Active Directory Users And Computers
Управление группами	User Manager	Active Directory Users And Computers
Управление учетными записями компьютеров	Server Manager	Active Directory Users And Computers
Добавление компьютера в домен	Server Manager	Active Directory Users And Computers
Создание или управление отношениями доверия	User Manager	Active Directory Domains And Trusts

(см. след. стр.)

Табл. 16-3. Выполнение задач настройки ... *(продолжение)*

Задача	В Windows NT 4.0 используется	В Windows Server 2003 используется
Управление политикой учетных записей	User Manager	Active Directory Users And Computers
Управление правами пользователей	User Manager	Active Directory Users And Computers
Управление политикой аудита	User Manager	Active Directory Users And Computers

Поддержка существующих приложений

На серверах Windows NT 4.0 и более ранних версий права доступа для чтения информации о пользователях и группах назначались анонимным пользователям, чтобы приложения, включая Microsoft BackOffice, SQL Server и приложения сторонних производителей, работали правильно.

В Windows 2000/Server 2003 члены группы Anonymous Logon имеют право на чтение этой информации, только когда данная группа добавлена в группу the Pre-Windows 2000 Compatible Access.

Мастер установки Active Directory позволяет добавить группу Anonymous Logon и группу безопасности Everyone в группу Pre-Windows 2000 Compatible Access — выберите параметр Permissions Compatible With Pre-Windows 2000 Server Operating Systems. Чтобы запретить членам группы Anonymous Logon чтение информации о пользователях и группах, выберите параметр Permissions Compatible Only With Windows Server 2003 Operating Systems.

Если группа безопасности Everyone уже включена в группу безопасности Pre-Windows 2000 Compatible Access (на что указывают параметры обратной совместимости), во время обновления контроллера домена с Windows 2000 до Windows Server 2003. группа безопасности Anonymous Logon будет добавлена в качестве члена к группе Pre-Windows 2000 Compatible Access.

Вы можете вручную переключаться между параметрами обратной совместимости и высокой безопасности объектов

Active Directory, добавляя группу безопасности Anonymous Logon в группу безопасности Pre-Windows 2000 Compatible Access с помощью Active Directory Users And Computers.

Если при обновлении контроллера домена выбран параметр Permissions Compatible Only With Windows Server 2003 Operating Systems и приложения работают некорректно, можно попытаться решить проблему, добавив специальную группу Everyone в группу безопасности Pre-Windows 2000 Compatible Access и перезапустив контроллеры домена. Выполнив обновление до приложений, совместимых с Windows Server 2003, верните более безопасную конфигурацию Windows Server 2003, удалив группу Everyone из группы безопасности Pre-Windows 2000 Compatible Access и перезапустив контроллеры домена в этом домене.

Работа с Active Directory

Следующие советы помогут вам в настройке и работе с Active Directory.

- Для усиления безопасности не регистрируйтесь на своем компьютере по учетной записи администратора. При этом для выполнения административных задач можно использовать окно Run As.

Дополнительные сведения Подробнее см. разделы «Why You Should Not Run Your Computer as an Administrator» и «Using Run As» справочной системы Windows Server 2003.

- Для лучшей защиты Active Directory следуйте рекомендациям безопасности:
  - □ переименуйте или отключите учетную запись Administrator (и учетную запись Guest) в каждом домене, чтобы предотвратить атаки на домен (см. раздел «User and Computer Accounts» центра справки и поддержки);
  - П обеспечьте физическую защиту всех контроллеров домена и разместите их в запертой комнате.
- Управление отношениями безопасности между двумя лесами упростит администрирование системы безопасности и аутентификацию между лесами.

- Чтобы обеспечить дополнительную защиту схемы Active Directory, удалите всех пользователей из группы Schema Admins и добавляйте пользователей в группу, только когда необходимо изменить схему. Сделав изменения, удалите пользователей из группы.
- Ограничьте доступ пользователей, групп и компьютеров к общим ресурсам; фильтруйте параметры групповой политики.
- По умолчанию весь трафик утилит администрирования Active Directory при передаче через сеть шифруется и подписывается. Не отключайте эту функцию.
- Некоторые права пользователей, назначаемые по умолчанию определенным группам, могут позволить членам этих групп получать дополнительные права в домене, в том числе права администратора. Поэтому организация должна одинаково доверять членам групп Enterprise Admins. Domain Admins, Account Operators, Server Operators, Print Operators и Backup Operators.
- Установите как сайт каждую географическую область, для которой нужен быстрый доступ к самой последней информации каталога.

Дополнительные сведения О безопасности Active Directory см. разделы «Security Overview for Active Directory» и «Securing Active Directory» справочной системы Windows .NET Server.

Устанавливая области, требующие немедленного доступа к обновленной информации Active Directory, как отдельные сайты, обеспечьте необходимые ресурсы.

Разместите минимум один контроллер домена в каждом сайте и создайте минимум один контроллер домена в каждом сайте ГК. Сайты, не имеющие собственных контроллеров домена и минимум одного ГК, зависят при получении информации каталога от других сайтов и менее эффективны, чем сайты, имеющие данные ресурсы.

Оставьте все мостовые связи сайтов и неограниченное расписание подключения связей сайтов. Объединение всех связей сайта увеличивает связи репликации между сайтами и предотвращает необходимость создания объединения связей сайта вручную. Оставив неограниченное расписание подключения

связей сайта, вы избежите конфликтов в расписании подключений, которые могут мешать репликации. По умолчанию все связи сайта объединены и расписания подключений связей сайта неограниченны.

Установите выделенный мостовой сервер, если вы применяете брандмауэр или хотите использовать компьютер для межсайтовой репликации. Мостовой сервер служит посредником для соединений с другими сайтами, расположенными за брандмауэром. Все сайты должны быть связаны минимум одной подсетью и минимум с одной связью сайта, или их нельзя будет использовать.

Регулярно архивируйте контроллеры домена, чтобы сохранить все отношения доверия в пределах этого домена.

Совместимость приложений

Проверка совместимости приложений с новой ОС — один из критически важных этапов тестирования и планирования фаз успешного развертывания.

Комплект утилит для проверки совместимости (ACT) содержит несколько инструментов, облегчающих управление этим процессом. ACT предоставляет утилиты для проверки приложений как в фазе разработки, так и во время развертывания. Он также содержит утилиты, позволяющие собрать данные о приложениях, установленных на каждом входящем в сеть компьютере с Windows, и о пакетах, необходимых для решения проблем совместимости каждого из этих компьютеров.

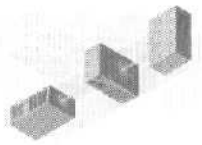
- **Анализатор** Собирает сведения о каждой из установленных в сети программ. Анализатор может служить для автоматизации составления списка используемого ПО.
- **Верификатор приложений** Помогает разработчикам при поиске проблем совместимости новых приложений. Также позволяет ИТ-профессионалам определять наличие общих проблем совместимости у определенного пакета ПО.
- **Администратор совместимости** Определяет исправления совместимости, необходимые для поддержки приложения в Windows. Утилита может упаковывать исправления в настраиваемую БД для передачи ее другим компьютерам в сети. О пакете ACT см. главу 18.

Дополнительные сведения

Дополнительные сведения см. по следующим адресам:

- использование Application Compatibility Toolkit — *http://www.microsoft.com/windowsserver2003/compatible/appcom-pat.mspx*;
- 10 основных причин для перехода организаций на Windows Server 2003 с Windows NT Server 4.0 — *http://www.microsoft.com/ windowsserver2003/evaluation/whyupgrade/top10nt.mspx*;
- 10 основных причин для перехода организаций с Windows 2000 Server — *http://www.microsoft.com/windowsserver2003/evaluation/ whyupgrade/top 10w2k.mspx*;
- руководство по развертыванию Microsoft Windows Server 2003 — *http:// www.microsoft.com/technet/prodtechnol/windowsnetserver/evaluate/ cpp/reskit/*.

ГЛАВА
17



Обновление с Windows 2000 Server

Обновив ОС с Microsoft Windows 2000 на один из продуктов Microsoft Windows Server 2003, вы сможете задействовать новые функции Windows Server 2003, не изменяя текущей конфигурации сети. Такое обновление осуществляется гораздо проще, чем с Windows NT 4.0 Server (см. главу 16). При переходе на Windows Server 2003 существующая структура службы каталогов остается прежней.

Вот некоторые функции, доступные после обновления до Windows Server 2003:

- усовершенствованная репликация членства в группах;
- прикладные разделы каталога;
- доверительные отношения между лесами;
- универсальное кэширование групп;
- усовершенствованный генератор топологии межсайтовой репликации.

Здесь обсуждаются проблемы, которые необходимо устранить перед переходом с Windows 2000 Server на Windows Server 2003. Кроме того, в этой главе используется материал книги «Microsoft Windows Server 2003 Deployment Kit» (Microsoft Press, 2003). Этот комплект ресурсов и утилиты, записанные на поставляемом с ним компакт-диске, беспенны для планирования и развертывания Windows Server 2003. Подробнее о нем см.: *http://www.microsoft.com/reskit/*.

Подготовка к обновлению

Если хоть один из контроллеров домена сети работает под управлением Windows NT 4.0, его нужно обновить до Windows Server 2003 (см. главу 16).

Чтобы успешно обновить домены Windows 2000 до Windows Server 2003, требуется знать функциональные уровни доменов и лесов Active Directory. Начать такое обновление можно одним из следующих способов;

- обновив имеющийся контроллер домена Windows 2000 до Windows Server 2003;
- установив с помощью мастера Active Directory Installation Wizard службу Active Directory на рядовом сервере Windows .NET.

Active Directory Preparation Tool

Подготовить домен Windows 2000 к обновлению до Windows Server 2003 позволяет Active Directory Preparation Tool (ADPrep.exe). После обновления вы сможете использовать преимущества прикладных разделов каталога. Запускают ADPrep.exe только из командной строки.

ADPrep.exe подготавливает лес и домен к обновлению Active Directory. ADPrep.exe записана на компакт-диске с ОС Microsoft Windows .NET Server и для подготовки леса и домена Active Directory копирует с этого диска или сетевого источника установки файлы 409.csv и dcpromo.csv.

ADPrep.exe сводит генерируемую ею новую информацию схемы с текущей схемой, сохраняя при этом в вашей среде сделанные ранее изменения. Прежде чем подготовить домен, выполнив команду *adprep* с ключом */domainprep,* нужно выполнить ту же команду в лесу с ключом */forestprep* и дождаться успешного завершения ее выполнения. Выполните *adprep* с ключом */forestprep* на мастере схемных операций. Во всех доменах, где планируется установить контроллер домена Windows .NET, перед обновлением первого из контроллеров домена или добавлением рядового сервера Windows .NET или автономного сервера в качестве дополнительного контроллера домена нужно выполнить на мастере операций инфраструктуры команду *adprep* с ключом */domainprep.* Чтобы подготовить лес и домен

Active Directory к обновлению до Windows Server 2003, программа ADPrep.exe делает следующее.

- Обновляет схему Active Directory.
- Обновляет дескрипторы безопасности по умолчанию.
- Модернизирует спецификаторы вывода.
- Настраивает списки управления доступом, определенные для объектов Active Directory и файлов общей папки Sysvol, предоставляя доступ контроллеру домена.

  Если в версиях Windows, предшествовавших Windows Server 2003, добавить идентификатор безопасности Everyone в список управления доступом или в группу, пользователи, прошедшие проверку подлинности, пользователи с гостевой учетной записью и все лица, подключившиеся к системе анонимно, получают доступ к ресурсам. В контроллерах домена Windows 2000 анонимный доступ также служит для управления рядом объектов и файлов Active Directory. В Windows Server 2003 идентификатор безопасности Everyone уже не предоставляет доступа анонимным пользователям, тем самым ограничивая доступ контроллеров домена к некоторым объектам. ADPrep.exe изменяет списки управления доступом этих объектов так, чтобы предоставить контроллерам домена доступ к ним.
- Создает новые объекты, используемые такими приложениями, как COM+, и инструментами управления Windows (Windows Management Instrumentation, WMI).
- Создает в Active Directory новые контейнеры, с помощью которых проверяется успешность подготовки.

При каждом запуске ADPrep.exe создает файл журнала, который содержит подробные сведения обо всех этапах подготовки леса. Все файлы журнала ADPrep находятся во вложенных папках каталога %SystemRoot%\system32\debug\adprep; им задается имя в виде даты и времени запуска ADPrep.

При обновлении контроллера домена Windows 2000 до Windows Server 2003 программа Winnt32.exe проверяет, готовы ли лес и домен. Если лес и домен, членом которого станет новый контроллер домена, не готовы, проверка завершается ошибкой и выводом сообщения о необходимости запуска ADPrep.exe. Обновить контроллеры домена Windows 2000 до Windows .NET без предварительного запуска ADPrep.exe нельзя.

Прикладные разделы каталога

Если в лесу имеется хоть один контроллер домена с Windows Server 2003, можно использовать прикладные разделы каталога, предназначенные для хранения данных, специфичных для приложений и не связанных с доменом, и позволяющие реплицировать эти данные в произвольный набор контроллеров домена (об этом см. главу 3).

В Windows Server 2003 прикладные разделы каталога могут применяться для хранения данных системы доменных имен (Domain Name System, DNS). Если установку Active Directory начал член группы Enterprise Admin, в процессе этой установки на всех имеющихся DNS-серверах автоматически создаются прикладные разделы каталога со специфичными для DNS данными. Если при создании прикладного раздела каталога в процессе установки Active Directory произойдет ошибка, служба DNS повторно попытается создать такой раздел, когда компьютер перезагрузится по завершении установки Active Directory. Создавать специфичные для DNS прикладные разделы каталога могут только члены группы Enterprise Admin.

В процессе установки Active Directory создаются два специфичных для DNS прикладных раздела каталога: раздел уровня леса под названием ForestDnsZones, а для каждого домена в лесу — раздел уровня домена под названием DomainDnsZones. Обновив в домене все контроллеры до Windows Server 2003, можно указать для всех имеющихся зон, интегрированных с Active Directory, область репликации, переместив зону в новый прикладной раздел каталога. Такое перемещение дает следующие преимущества.

- Службу DNS, интегрированную с Active Directory, можно использовать на уровне леса, так как прикладной раздел уровня леса допускает репликацию данных за пределы домена. Прибегать к обычному переносу зоны DNS для репликации файла с информацией о зоне на DNS-серверы, находящиеся за пределами домена, не требуется.
- Репликация уровня домена позволяет уменьшить сетевой трафик. Администратору достаточно указать контроллеры домена с работающей службой DNS, которые должны получить информацию о зоне DNS.

- Репликация уровня леса позволяет уменьшить сетевой трафик, так как данные **DNS** больше не реплицируются в глобальный каталог.

О хранении DNS-сведений в прикладных разделах каталога см. ниже раздел «Использование прикладных DNS-разделов каталога».

Возможные способы обновления

Чтобы узнать, можно ли обновить компьютеры до Windows Server 2003 или нужно устанавливать систему с нуля, надо определить, какие версии Windows 2000 есть в среде. В табл. 17-1 приведена информация о возможности непосредственного обновления компьютеров с Windows 2000 до Windows Server 2003.

Табл. 17-1. Возможные способы обновления до Windows Server 2003

Платформа	Обновление до Windows Server 2003 Standard Edition	Обновление до Windows Server 2003 Enterprise Edition	Обновление до Windows Server 2003 Datacenter Edition
Windows 2000 Professional	Невозможно	Невозможно	Невозможно
Windows 2000 Server	Возможно	Возможно	Невозможно
Windows 2000 AdvancedServer	Невозможно	Возможно	Невозможно
Windows 2000 DatacenterServer	Невозможно	Невозможно	Возможно

Требования к оборудованию

Изучите и запишите конфигурацию и версию ОС всех компьютеров, которые собираетесь обновлять. Затем определите, какие компьютеры можно обновить до Windows Server 2003, а какие следует снять с эксплуатации или оставить в качестве обычных рядовых серверов. Рекомендуемые минимальные требования к оборудованию рядового сервера под управлением Windows Server 2003 Standard Edition таковы:

- процессор с тактовой частотой не менее 550 МГц;
- ОЗУ объемом не менее 256 Мб;
- не менее 1,5 Гб дискового пространства.

На контроллерах домена выделите побольше дискового пространства для хранения файлов БД и журнала Active Directory. Следующие рекомендации помогут определить, сколько пространства выделить для установки Active Directory:

- на диске с шаблоном БД Active Directory NTDS.dit выделите такой объем свободного пространства, который составит 10% от размера имеющейся БД или минимум 250 Мб;
- на диске с файлами журнала транзакций Active Directory ESENT должно быть не менее 50 Мб свободного пространства.

Совет Для оптимальной производительности рекомендуется размещать БД Active Directory, файлы журнала Active Directory и ОС Windows .NET на отдельных физическихдисках.

Инструменты и журналы, используемые при тестировании

Важно разработать план тестирования всех этапов процесса обновления. До начала обновления проверьте состояние контроллеров домена и убедитесь, что они нормально функционируют. Проверяйте также их состояние и в процессе обновления, чтобы убедиться в корректной и согласованной работе репликации Active Directory. В табл. 17-2 перечислены инструменты и журналы, применяемые для проверки успешности процедур обновления.

Табл. 17-2. Инструменты и журналы, используемые в процессе тестирования

Инструмент/ Файл журнала	Описание	Размещение
Repadmin.exe	Контролирует согласованность репликации, а также ведет мониторинг пассивных и активных участников репликации. Отображает состояние репликации для пассивных участников репликации и разделов каталога.	Папка \Support\Tools компакт-диска с Windows Server 2003

(см. след. стр.)

Табл. 17-2. Инструменты и журналы... *(продолжение)*

Инструмент/ Файл журнала	Описание	Размещение
Dcdiag.exe	Определяет состояние контроллеров домена в лесу или на предприятии. Проверяет функциональность и возможность подключения к Active Directory. Возвращаемый результат проверки — «passed» (проверка прошла успешно) или «failed» (проверка завершилась ошибкой).	Папка \Support\Tools компакт-диска с Windows Server 2003
Netdiag.exe	Выявляет проблемы с сетью и подключением, выполняя ряд тестов для определения состояния и работоспособности сетевого клиента.	Папка \Support\Tools компакт-диска с Windows Server 2003
Nltest.exe	Запрашивает и проверяет статус доверенных серверов, а также позволяет принудительно выключать контроллеры домена,	Папка \Support\Tools компакт-диска с Windows Server 2003
Dnscmd.exe	Выявляет проблемы с регистрацией и зонами DNS, позволяя администратору просматривать свойства DNS-серверов, зон и записей о ресурсах.	**Папка** \Support\Tools компакт-диска с Windows Server 2003
Adprep log	Содержит подробный отчет о ходе процесса подготовки леса и домена.	Папка %SystemRoot%\ system32\debug\ adprep
DcpromoUI.log	Содержит подробный отчет о ходе установки Active Directory, включая информацию о репликации и службах, а также соответствующие сообщения об ошибках.	Папка %SystemRoot%\ debug
ADSIEdit.exe	Оснастка консоли MMC, выступающая в роли низкоуровневого редактора Active Directory и позволяющая просматривать/добавлять/удалять/перемещать в каталоге объекты и атрибуты.	**Папка \Support\Tools** компакт-диска с Windows Server 2003

Управление процессом обновления

Подготовив лес, реплицировав в его пределах все изменения, сделанные ADPrep.exe, и подготовив домены, можно начинать обновление. Ниже перечислены этапы обновления контроллеров домена Windows 2000 до Windows Server 2003. Подробнее об этих этапах — в последующих разделах.

1. Установка Active Directory на рядовом сервере.
2. Обновление первого домена до Windows Server 2003,
3. Обновление остальных доменов до Windows Server 2003.

Установка Active Directory на рядовом сервере

Установите Active Directory на рядовом сервере Windows Server 2003 с помощью мастера Active Directory Installation Wizard — рядовой сервер станет контроллером домена. Установить Active Directory можно на любом рядовом сервере Windows Server, соответствующем требованиям к оборудованию контроллера домена. Мастер Active Directory Installation Wizard:

- позволяет создать дополнительный контроллер домена и добавить его в имеющийся домен;
- конфигурирует локальный сервер для размещения службы каталогов;
- создает разделы каталога и определяет участников безопасности домена по умолчанию;
- позволяет установить или настроить DNS.

Запускают мастер Active Directory Installation Wizard из командной строки или с помощью мастера Configure Your Server Wizard члены группы Domain Admins. Установив Active Directory на рядовом сервере под управлением Windows .NET, дождитесь окончания репликации и синхронизации всех контроллеров домена с вашим сервером.

Дополнительные сведения Об установке и удалении Active Directory см. раздел «Installing and Removing Active Directory» книги «Directory Services Guide» из Microsoft Windows Server 2003 Resource Kit (или раздел «Installing and Removing Active Directory» Web-узла http://www.microsoft.com/reskit/).

Обновление первого домена

Дождавшись синхронизации нового контроллера домена Windows Server 2003 с остальными контроллерами, обновите контроллеры домена Windows 2000 до Windows Server 2003. Чтобы начать установку ОС на контроллере домена, вставьте диск с Windows Server 2003 в привод CD-ROM соответствующего компьютера или, если файлы Windows .NET доступны в сети, запустите Winnt32.exe.

Также возможна необслуживаемая установка Windows Server 2003. Инструкции по созданию файла ответов для установки Active Directory см. в файле Deploy.cab из папки Support\Tools компакт-диска с ОС Windows Server 2003. Найдите в файле Deploy.cab файл Ref.chm и откройте его. Затем раскройте в левой панели файл Unattend.txt и щелкните DCInstall.

Обновление остальных доменов

Обновив первый домен, обновите и остальные домены в лесу, Обновить можно все контроллеры домена с Windows 2000, которые соответствуют аппаратным требованиям к установке Windows Server 2003.

Помните: прежде чем обновить контроллер в другом домене, на компьютере, выполняющем в этом домене роль мастера инфраструктуры, нужно предварительно запустить *adprep* с ключом */domainprep*. Однократно выполните команду *adprep* с ключом */forestprep* в корневом домене леса и однократно — с ключом */domainprep* в каждом из доменов леса, где будет развернут контроллер домена Windows Server 2003.

Заключительные мероприятия

Обновив все контроллеры домена в лесу до Windows Server 2003, завершите обновление, повысив функциональные уровни леса и домена до Windows .NET, и разместите информацию DNS в новых прикладных разделах каталога.

Повышение функциональных уровней леса и домена

После того как вы обновите первый контроллер домена в лесу до Windows Server 2003, лес автоматически продолжает работать на уровне Windows 2000. Если все домены Windows 2000

работают в основном режиме, после обновления первого из контроллеров в домене до Windows Server 2003 домен автоматически начинает работать в основном режиме домена Windows 2000. Если все домены леса работают в основном режиме домена Windows 2000, после повышения уровня леса до Windows .NET уровень всех его доменов автоматически повышается до Windows .NET.

И все же, если в организации есть домен Windows 2000, работающий в смешанном режиме, после обновления первого домена он продолжит работать в смешанном режиме. При наличии в лесу доменов, работающих в смешанном режиме Windows 2000, перед повышением общего функционального уровня до Windows .NET нужно вручную повысить функциональный уровень таких доменов до основного режима Windows 2000. Повышать функциональный уровень леса могут члены группы Enterprise Admins, а домена — члены группы Domain Admins.

Допустим, организация с тремя доменами — корневым доменом леса и двумя региональными доменами — обновляет среду Windows 2000 до Windows Server 2003. Функциональный уровень леса в данной организации — Windows 2000. Функциональные уровни доменов:

- корневой домен леса: основной режим Windows 2000;
- региональный домен 1: основной режим Windows 2000;
- региональный домен 2: смешанный режим Windows 2000.

Перед повышением функционального уровня леса организации нужно повысить функциональный уровень второго регионального домена до основного режима Windows 2000. Администратор второго домена осуществляет такое повышение, и теперь все домены леса работают на стандартном функциональном уровне домена Windows 2000. Затем корпоративный администратор повышает функциональный уровень леса до Windows .NET. В результате, поскольку все домены леса работают на стандартном уровне домена Windows 2000, уровень всех доменов автоматически повышается до Windows .NET. Это позволяет организации использовать все функции и преимущества, предоставляемые лесом Windows .NET.

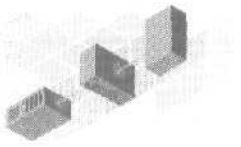
Использование прикладных DNS-разделов каталога

Используя прикладные разделы каталога для DNS-интегрированных зон, вы заметно уменьшаете объем сетевого трафика и размер данных, хранимых в глобальном каталоге. Обновив все контроллеры домена Windows 2000 до Windows Server 2003, переместите на всех DNS-серверах DNS-зоны. интегрированные с Active Directory, из раздела домена в новые прикладные DNS-разделы каталога. DNS-зоны, которые требуется реплицировать на все DNS-серверы леса, следует переместить в прикладной DNS-раздел уровня леса, ForestDnsZones. DNS-зоны, реплицируемые только на DNS-серверы домена, — в прикладной DNS-раздел уровня домена, DomainDnsZones.

Дополнительные сведения

Дополнительные сведения см. по адресу;

- руководство по развертыванию Microsoft Windows .NET Server — *http://www.microsoft.com/technet/prodtechnot/windows-netserver/evalu a te/cpp/reskit/.*



ГЛАВА
18

Тестирование приложений на совместимость

Перед развертыванием новой ОС необходимо многое предусмотреть. Если вы предполагаете переходить на Windows Server 2003/XP, возникает вопрос: будут ли эти ОС поддерживать ваши приложения? Поиск ответа на него составляет основную часть мероприятий по планированию и тестированию при развертывании новой системы.

Пакет Application Compatibility Toolkit (ACT) содержит ряд инструментов, облегчающих проведение этих мероприятий. Его можно загрузить с Web-сайта Microsoft *(http://www.microsoft.com/downloads/release.asp?releaseid=42071)*.ACT предоставляет инструменты для тестирования приложений на стадиях разработки и развертывания; эти инструменты также позволяют собрать сведения о приложениях со всех компьютеров сети, работающих под управлением Windows, и создать для них индивидуальные пакеты исправлений,

- **Analyzer** позволяет собрать сведения обо всех программах, установленных на компьютерах сети, применяется для инвентаризации программного обеспечения предприятия.
- **Application Verifier** выявляет проблемы с совместимостью новых приложений. С его помощью IT-специалисты смогут обнаруживать общие проблемы с совместимостью приложений, которые планируется внедрять.
- **Compatibility Administrator** определяет набор исправлений, необходимый для поддержки приложений в Windows. По-

зволяет создавать индивидуальные пакеты исправлений в виде пользовательских баз данных обеспечения совместимости, которые можно распространять по компьютерам сети.

В этой главе также рассказывается об инвентаризации приложений, тестировании па совместимость, создании исправлений, обеспечивающих совместимость, и их распространении. В завершение приводится список вопросов, составляющих содержание тестирования на совместимость. Подробности об инструментах, описанных в этой главе, см. по адресу *http://www.microsoft.com/windowsserver2003/compatible/appcompat.mspx*.

Инвентаризация приложений

Прежде чем приступать к тестированию приложений на совместимость, следует узнать, какие приложения применяются в организации. В организациях важность этих сведений часто недооценивают, уповая на наличие списка приложений, официально разрешенных к применению. Однако в такой список не входят ни приложения, установленные на время, например, для исполнения некоторых проектов, ни программы, официально не разрешенные, но неизбежно присутствующие на компьютерах сотрудников. Эти обстоятельства делают необходимость инвентаризации ПО очевидной.

Есть несколько подходов к инвентаризации ПО, но большинство специальных методов инвентаризации здесь не рассматривается. В настоящее время Microsoft предлагает два метода сбора сведений о программах: через Systems Management Server (SMS) и при помощи инструмента Analyzer из пакета Application Compatibility Toolkit.

Compatibility Analyzer позволяет собирать сведения о программной и аппаратной конфигурации компьютеров и записывать собранную информацию в журнал в формате XML. Далее Analyzer импортирует сведения из журналов в централизованную БД, откуда их затем можно извлечь и использовать для анализа совместимости приложений и составления отчетов. Compatibility Analyzer состоит из трех компонентов.

- **Collector** — этот первый компонент в порядке применения. Он представляет собой утилиту командной строки, которая. работая в фоновом режиме, не выводя сообщений и не мешая пользователю, собирает сведения обо всех приложени-

ях, установленных на компьютере. После этого она записывает собранные данные в файл журнала, расположенный в заданном каталоге (по умолчанию это рабочий стол на пользовательском компьютере, но можно выбрать и сетевой диск, выделенный для централизованного сбора информации).

- Merger (Merger.exe) объединяет файлы журналов в единую БД, по умолчанию база записывается в формате Microsoft Access (.MDB), доступен также формат SQL,
- Analyzer — инструмент с графическим интерфейсом, служит для просмотра собранных данных и генерации отчетов.

Сбор данных

Чтобы выполнить сбор сведений о приложениях с помощью Compatibility Analyzer, нужно скопировать на каждый компьютер, на котором надо провести инвентаризацию ПО, и запустить утилиту командной строки Collector.exe. При вызове этой утилиты можно задать параметры инвентаризации — пути для поиска приложений, выбрать сетевые или локальные диски, а также указать, нужно ли собирать сведения об оборудовании и куда следует записывать файлы журнала. Поддерживается инвентаризация следующих платформ:

- клиенты Windows 98;
- клиенты Windows Me;
- клиенты и серверы Windows NT 4.0;
- клиенты и серверы Windows 2000;
- клиенты Windows XP;
- серверы из семейства Windows Server 2003;
- смешанные домены, включающие клиенты под управлением Windows 98/Me/NT 4.0/2000/XP;
- смешанные домены, включающие серверы под управлением Windows NT 4.0/2000/Server 2003.

После запуска утилита для сбора данных определяет ОС клиента и загружает соответствующую поддержку. Например, в Windows 98/Me встроенной кодировкой является ANSI, поэтому в этих ОС Collector загрузит поддержку ANSI для записи данных в журнал, а в Windows NT/XP будет загружена поддержка Unicode.

Основная функция Compatibility Analyzer — сбор сведений о совместимости приложений с клиентских компьютеров. Все последующие этапы предполагают наличие данных, собранных минимум с одного клиентского компьютера, записанных в файл журнала. Утилиту Collector можно настраивать при помощи переключателей командной строки. Вот синтаксис ее вызова:

```
collector.exe [-o filename] [-f source] [-e department]
              [-n] [-d days] [-a] [-p profile]
```

-o *filename*	Задает путь для записи выходных данных Collector. По умолчанию это пользовательский рабочий стол.
• f*source*	Задает путь к файлу или каталогу для инвентаризации. Если этот параметр не задан, Collector будет собирать данные со всех дисков машины.
-e *department*	Указывает название подразделения, которое будет использоваться при обработке журналов. Эти данные позволяют разделить собранные сведения на категории, что удобно при консолидации журналов в дальнейшем.
-n	Запрещает собирать сведения с сетевых дисков (по умолчанию содержимое сетевых дисков также подвергается анализу).
-d *days*	Разрешает запускать Collector, только если с момента его последнего запуска прошло указанное этим параметром число дней. Если этот параметр не задан, Collector не запустится, если он запускался раньше на данной машине.
-a	Дополняет данные, собранные при обработке заданных дисков и каталогов, сведениями, полученными из оболочки и списка установленных программ.
-*p profile*	Заставляет Collector использовать заданный профиль (файл инициализации).

Представление данных

Компонент Compatibility Analyzer, ответственный за анализ собранных данных, работает на компьютере администратора, куда передаются все результаты. На администраторском компьютере можно анализировать сведения о совместимости и генерировать отчеты. Компонент анализа консолидирует инфор-

мацию журналов в БД, объединяя сведения об идентичных приложениях. Поддерживаются форматы БД ODBC SQL и Access.

Анализировать совместимость и генерировать отчеты можно на следующих платформах (необходим Internet Explorer 5.0 или выше):

- клиенты и серверы Windows NT 4.0;
- клиенты и серверы Windows 2000;
- клиенты Windows **XP;**
- серверы семейства Windows Server 2003.

Вот как применять Compatibility Analyzer.

1. Установите компонент анализа на компьютер администратора, где предполагается работать с отчетами.
2. Создайте БД для хранения анализируемой информации, это может быть база данных ODBC SQL или Access.
3. Настройте компонент, собирающий данные (Collector): задайте область инвентаризации и размещение журналов.
4. Скопируйте этот компонент на все компьютеры, подлежащие инвентаризации, и запустите его. Для его работы не требуется учетной записи администратора. Распространить его можно:
   - □ на гибких дисках;
   - □ на CD-ROM;
   - П с помощью сценариев входа в систему;
   - D при помощи групповой политики Active Directory;
   - П через гиперссылки в почтовых сообщениях;
   - П через сетевой диск;
   - □ через SMS.
5. Получите журналы и объедините собранные сведения в базе данных.
6. Проанализируйте содержимое базы данных.
7. Сгенерируйте и изучите отчет.

Отчет можно упорядочить по приложениям или по компьютерам, поддерживается также фильтрация и сортировка результатов. Упорядочив данные по компьютерам, можно увидеть все приложения, установленные на некотором компьютере, а если упорядочить отчет по приложениям, можно узнать, сколько экземпляров того или иного приложения установлено в сети.

При создании плана тестирования основное внимание необходимо уделить приложениям, установленным на большинстве компьютеров, а также несовместимым приложениям и приложениями, совместимость которых определить не удалось.

Тестирование на совместимость

После инвентаризации ПО и проверки инвентарных списков можно приступать к планированию тестирования. Типичный план тестирования при развертывании новой ОС должен включать ряд важных моментов. Например, нужно выяснить, будет ли приложение работать в новой ОС. В плане тестирования также описаны более сложные мероприятии по тестированию комбинаций программ, применяемых в организации,

Ниже описана стратегия тестирования приложений при развертывании Windows, а также дан обзор инструментов из пакета Application Compatibility Toolkit.

Перед развертыванием Windows необходимо протестировать все ПО, установленное на рабочих станциях и серверах. В организациях, где есть стандартный набор разрешенных приложений, решить эту задачу легче, чем там, где использование ПО не регламентировано. Выполнив инвентаризацию и определив приоритетные приложения, можно переходить к составлению плана тестирования.

В идеале перед развертыванием новой версии Windows нужно протестировать все приложения, используемые в организации. Однако далеко не каждый отдел автоматизации может позволить себе такую роскошь. Определив приоритетные приложения, можно рационально распределять средства, выделенные на тестирование. Каждому приложению следует присвоить приоритет согласно его значению для деятельности организации. Ясно, что приоритет приложения для рабочих станций, которое к тому же используется время от времени, будет намного ниже, чем у ключевого клиент-серверного ПО, на котором построена вся работа. Шкала приоритетов приложений может быть такой.

1. Критическое для бизнеса **приложение** Приложения этой категории жизненно необходимы для бизнеса, их простой неизбежно оборачиваются солидными потерями.

2. **Рабочие приложения** К этой категории относятся приложения, которые применяет большинство пользователей. Пример — Microsoft Word 2002. Кратковременные перебои в доступе к таким приложениям терпимы, но их основная функциональность должна оставаться доступной.
3. **Специализированные приложения** Эти приложения важны для ограниченного круга пользователей, деятельность организации в целом от них не зависит. Примером могут быть графические редакторы, в которых обрабатываются фотографии для маркетинговых материалов. При возникновении серьезных проблем с совместимостью таких приложений от них можно отказаться.
4. **Остальные приложения** К этой категории относится нестандартное ПО, которое пользователи устанавливают сами. Как правило, это ПО не имеет значения для работы организации, или это значение невелико. Проблемы с совместимостью этих приложений не отразятся на бизнесе.

Microsoft предоставляет документацию Application Test Framework, где перечислены требования, а также описаны процедуры подготовки и проведения испытаний для получения логотипа «Designed for Windows XP». Получение этого логотипа не является целью развертывания приложений, но в этой документации прекрасно описаны процедуры и параметры, которые необходимо протестировать, чтобы определить совместимость приложений с Windows.

Test Framework предполагает наличие у тестировщика следующих навыков:

- опыт тестирования ПО и создания планов тестирования;
- опыт тестирования Windows-приложений для рабочих станций;
- умение устанавливать и настраивать компьютерное оборудование;
- знание ОС Windows;
- умение устанавливать и настраивать Windows XP/Server 2003;
- опыт работы с тестирующими приложения и отладчиками ядра.

Сбор сведений о приложениях

Analyzer позволяет создать список приложений, используемых в организации. Однако этот список ничего не скажет о роли

программы в рабочем процессе организации. Чтобы получить эту информацию, необходимо проинтервьюировать следующие группы пользователей.

- **Руководство** Руководство верхнего уровня способно сообщить много полезного о ПО, применяемом в организации; не забудьте и про руководителей подразделений.
- **Сотрудники отдела автоматизации** Никто не скажет точнее, чем эти люди, какие приложения находятся в повседневном использовании.
- **Рядовые пользователи** Эту группу респондентов часто (и безосновательно) игнорируют. Попытайтесь собрать сведения у репрезентативных групп пользователей из разных отделов.

Вполне возможно, что приложения, попавшие в список установленных программ, в настоящее время не используются. При тестировании совместимости перед развертыванием новой ОС такие приложения можно смело отнести к низкоприоритетным. Этот момент и является причиной сбора сведений о приложениях, которые позволят определить приоритетные приложения. Проблемам с совместимостью отдельных редко используемых приложений и новой ОС можно уделять меньше внимания или вовсе игнорировать их. Шкала приоритетов приложений с точки зрения их востребованности может быть такой,

1. **Критичные для бизнеса** Это жизненно важные приложения, используемые в повседневной деятельности организации, например, ПО для электронной коммерции.
2. **Программы для повседневного использования** Это категория приложений, необходимых для работы большинству пользователей, однако кратковременный выход из строя этих приложений не является непреодолимым препятствием для организации как таковой.
3. **Редко используемые программы** Эту категорию можно разделить на две группы: в первую входят приложения, имеющие некоторое значение для бизнеса, а во вторую — приложения, которые пользователи просто любят ставить на свои компьютеры.

Применение Compatibility Administrator

Compatibility Administrator применяется в основном на завершающих этапах тестирования. Он не предназначен для автоматизации тестирования или выявления проблем с совместимостью, его миссия — поиск возможных решений проблем с совместимостью, выявленных в ходе тестирования.

Тестирование выявляет проблемные приложения среди ПО, используемого в организации или запланированного для внедрения, а Compatibility Administrator позволяет найти решение для этих проблем. Рассмотрим пример.

- **Приложение** MyApp16 — 16-разрядное Windows-приложение для регистрации звонков в службу работы с клиентами и отслеживания различных событий.
- **Роль в деятельности организации** Это приложение ежедневно используется в отделе по работе с клиентами для обработки входящих звонков, поэтому допустимы лишь кратковременные перебои в его работе.
- **Описание проблемы с совместимостью** MyApp16 разработано для Windows 3.1. Оно нормально работало в Windows 95, но в Windows XP Professional/Server 2003 не работает.

Первое, что можно посоветовать в такой ситуации, — перейти на новую, 32-разрядную версию приложения с близкой или идентичной функциональностью. Однако ассигнований, запланированных на развертывание ОС Windows XP Professional на всех рабочих станциях организации, мало, чтобы обновить это приложение вместе с ОС. Выход заключается в поиске средств, которые заставят приложение работать в Windows XP. Решить задачу способен Compatibility Administrator.

Создание исправлений, обеспечивающих совместимость

Независимые поставщики ПО (Independent software vendors, ISV) долгое время практиковали подход, в рамках которого приоритетной задачей был выпуск программ, максимально эффективно работающих на машинах заказчика. Стремясь к этой цели, они искали способы взаимодействия с ОС. В результате создавались приложения, высоко оптимизированные для работы в одной версии Windows, для которой они разрабатывались. Если

заказчик пытался запустить свое любимое приложение в новой версии Windows, возникали проблемы с совместимостью. Это особенно характерно при переходе на Windows XP, поскольку эта ОС построена на основе Windows NT/2000,

Большинство ISV разрабатывало приложения, ориентированные на домашних пользователей, т. е. приложения для Windows 95/98, а Windows NT/2000 считались ОС для предприятий. В Windows XP знакомые по Windows 95/98 задачи решаются иначе. Отчасти это результат появления в Windows XP новых возможностей, отчасти — более строгих правил, обусловленных наследием Windows NT.

Приложения, созданные для прежних версий Windows, в Windows XP могут работать некорректно. Это относится в основном к ПО, написанному для Windows 95/98, но иногда то же происходит и с приложениями для Windows NT/2000. Причины несовместимости могут быть следующими.

- Приложение отказывается работать из-за того, что Windows сообщает новый номер версии. Чаше всего эти приложения неплохо работают с новыми версиями Windows, если пользователю удается обойти проверку номера версии.
- Приложение вызывает старые версии функций Win32 API, возвращающие неожиданные значения на машинах с большой оперативной памятью и дисками большой емкости.
- Приложение не поддерживает новый формат данных Windows.
- Приложение не может найти каталоги, в которых размещаются пользовательские данные, например личные и временные файлы, из-за несоответствия путей и правил именования.

Обзор технологий обеспечения совместимости

В Windows XP/Server 2003 одной из приоритетных задач является обеспечение совместимости приложений. Пользовательский интерфейс этих ОС открывает доступ к средствам, которые позволяют в той или иной степени справиться с несовместимостью приложений, а также к мощным инструментам, предназначенным для разработчиков и администраторов. Все эти технологии основаны на данных о совместимости, полученных при анализе файлов локального компьютера, и соответствующей информации из глобальной БД обеспечения совместимости. Данные из базы позволяют уникально идентифицировать

приложения, для корректной работы которых требуется дополнительная поддержка со стороны ОС.

В зависимости от ситуации применяются средства обеспечения совместимости трех уровней.

- **Исправление, обеспечивающее совместимость** Этот уровень реализован посредством *исправлений* (shim) — небольших фрагментов кода, устраняющих определенное несоответствие в программе, которое вызывает ее несовместимость. Как правило, одно исправление устраняет только одну проблему с совместимостью.
- **Режим совместимости (compatibility mode)** Это набор исправлений, обычно применяемых одновременно. Примером может быть так называемый уровень совместимости с Windows 98, доступный через пользовательский интерфейс. Он представляет собой режим совместимости, т. е. включает в себя несколько исправлений, необходимых для поддержки большинства приложений, ориентированных на Windows 98.
- **AppHelp** Выводит сообщение при запуске приложения, у которого есть известные проблемы с совместимостью с ОС, но нет известного способа их решения. AppHelp выводит разные сообщения: от рекомендательных, уведомляющих о том, что программа не поддерживает некоторые функции ОС, до сообщений о невозможности запуска приложения. Блокировка запуска приложений и вывод соответствующих сообщений AppHelp имеют место только при запуске приложений, способных повредить ОС, например, утилиты обслуживания диска, не поддерживающей новую ОС. Часто сообщение AppHelp содержит ссылку на Web-сайт, где пользователь сможет найти дополнительные сведения или даже исправление.

Технологии исправлений, обеспечивающих совместимость с Windows XP/Server 2003, используют специальные базы данных.

- **MigDB.inf** Обеспечивает поддержку при переходе с Windows 95/98/Me. Содержит информацию, которая позволяет выявить приложения, несовместимые или требующие вмешательства пользователя при обновлении ОС. Программа установки выводит отчет об обновлении со списком проблемных приложений и сведениями о совместимости оборудова-

ния. Раньше эта база данных была в составе Windows 2000 Setup, а теперь после обновления добавлена в программу установки Windows XP/Server 2003.

- NTCompat.inf Содержит сведения того же типа, что и MigDB.inf, но используется при обновлении Windows NT 4.0/2000, также входит в программы установки Windows XP/Server 2003.
- SysMain.sdb Содержит данные для поиска несовместимых приложений и исправления, обеспечивающие совместимость: расположена в каталоге %windir%\AppPatch. Эта БД позволяет найти исправления для приложений, требующих особой поддержки для корректной работы в Windows XP/Server 2003.
- AppHelp.sdb Этот файл хранит только справочные сообщения, которые предлагают пользователю установить исправления и предлагают URL или другой источник, где можно найти исправления от сторонних производителей. Этот файл также располагается в каталоге %windir%\AppPatch.

Это главные файлы баз данных, на которых основаны технологии обеспечения совместимости приложений Windows XP и Server 2003. Сама ОС не содержит кода, проверяющего совместимость программ, кроме небольшой проверочной процедуры, которая приказывает ОС обратиться за сведениями о совместимости к соответствующим базам данных. Этот подход обеспечивает оптимальную поддержку для приложений, оказывая минимальное влияние на производительность ОС.

Создание исправлений, обеспечивающих совместимость

После того как нужные исправления найдены и проверены, можно воспользоваться Compatibility Administrator (рис. 18-1). чтобы создать пользовательскую базу данных исправлений, в которой будут средства поддержки для приложений, составляющих уровни совместимости, а также исправления, которые не входят в уровни совместимости.

Чтобы добавить исправление в пользовательскую БД, щелкните Database\Create New\Application Fix — программа попросит ввести отображаемое имя и имя файла программы, указать режим совместимости и выбрать исправления, которые нужно применять к этому приложению. В завершение программа

попросит выбрать несколько файлов целевого приложения, которые позволят найти его на клиентских компьютерах. Выберите идентифицирующие целевую программу файлы, расположенные в одном каталоге, — например, справочный файл, расположенный в одном каталоге с исполняемым файлом приложения. Попробуйте выбрать минимальное число файлов, уникально идентифицирующих целевое приложение.

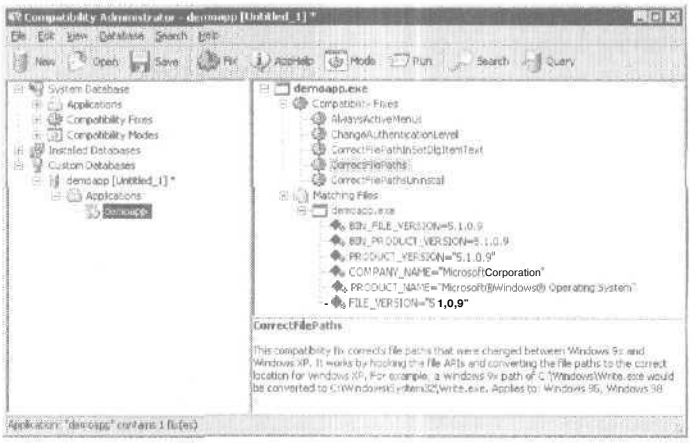


Рис. 18-1. Compatibility Administrator применяется для создания пользовательских БД исправлений для приложений, некорректно работающих в Windows XP и Server 2003

Технологии Windows XP/Server 2003, обеспечивающие совместимость приложений, не позволяют перепутать разные файлы с близкими или идентичными именами. ОС сравнивает файлы с использованием сведений из базы данных. Если вы создаете исправление для Setup.exe, но не хотите, чтобы оно применялось ко всем файлам с именем Setup.exe, следует выбрать дополнительные файлы, идентифицирующие целевое приложение, ОС собирает данные о специфических свойствах этих файлов, которые позволят ей найти именно то приложение, которое требует исправления (если оно есть на компьютере).

Распространение исправлений

Базы данных с исправлениями, обеспечивающими совместимость, переписанные на клиентские компьютеры, необходимо

установить. Все способы установки используют утилиту Compatibility Database Installer (Sdbinst.exe).

Установка на локальную систему

Проще всего установить базу данных локально при помощи Sdbinst.exe. Вот синтаксис вызова Sdbinst.exe:

```
sdbinst.exe [-?] [-q] [-u] [-g] [-n] database | {GUID} | name
```

-o*filename*	Задает путь для записи выходных данных Collector. По умолчанию это пользовательский рабочий стол.
-?	Выводит справку по команде sdbinst.exe.
-q	Запрещает вывод сообщений во время установки.
-и	Удаляет заданную базу данных (ее необходимо идентифицировать именем файла, GUID или внутренним именем).
-g	Задает GUID, идентифицирующий удаляемую базу данных.
-п*name*	Задает внутреннее имя базы данных (имя, назначенное ей Compatibility Administrator при создании).

Установка на удаленную систему

Установка файла базы данных обеспечения совместимости на удаленный компьютер требует по-особому вызывать Sdbinst.exe на удаленном компьютере. Обычно это делают при помощи сценария входа в систему или иных методов, например Remote Desktop Connection (RDC). Преимущество использования сценария в том, что он позволяет с помощью Active Directory выбрать пользовательские компьютеры, которым нужна БД обеспечения совместимости, и устанавливать эту базу только на них. Вот как установить БД на удаленный компьютер.

1. Создайте на сервере общую папку, доступную всем клиентам, которым нужна база данных обеспечения совместимости, и предоставьте разрешение на чтение этого каталога.
2. Отредактируйте сценарий входа в систему, назначенный некоторому уровню каталога Active Directory (сайту, домену или организационному подразделению), где требуется БД обеспечения совместимости. Добавьте в сценарий строку:

```
Sdbinst.exe \\имя_сервера\имя_ресурса\database.sdb -q
```

3. Проверьте, корректно ли сценарий выполняет установку.
4. Назначьте сценарий группе (сайту, домену или организационному подразделению), которой нужно установить БД. Если вы редактируете существующий сценарий, этот этап можно опустить.

Тестирование на совместимость во время развертывания

При развертывании Windows в крупной организации следует подумать о совместимости приложений, жизненно важных для нормального хода рабочего процесса.

Тестирование приложений на совместимость с ОС упрощает инструмент Application Verifier (AppVerifier). AppVerifier состоит из нескольких инструментов, специально разработанных для выявления наиболее распространенных проблем с совместимостью, в том числе связанных с ядром ОС. Эти компоненты также позволяют выявить несоответствия требованиям логотипа «Designed for Windows XP».

AppVerifier позволяет выявить ряд распространенных проблем с безопасностью, которые вызывают приложения, не совместимые с Windows, например, запись данных в неверные каталоги, где они уязвимы для вредоносного кода. Application Verifier не устраняет эти проблемы, но позволяет их обнаружить и исправить.

Применение Application Verifier

AppVerifier — это не средство автоматизации тестирования приложений. AppVerifier подключается к программе и выполняет свои тесты каждый раз, когда эта программа запускается. Его можно применять вместе с программами, автоматизирующими тестирование. AppVerifier подключает к исполняемому файлу тестируемой программы *заглушку* (stub) — небольшой фрагмент кода, позволяющий выполнять заданные тесты.

Чтобы протестировать приложение с помощью AppVerifier, необходимо выбрать файл тестируемой программы. Доступны следующие тесты.

- **Heap corruption detection** Выполняет обычную проверку кучи и помечает все области выделенной памяти контрольны-

ми страницами, которые позволяют обнаружить переполнение этой области.

- **Locks usage checking** Выявляет распространенные ошибки при установке и освобождении блокировок. Результаты теста выводятся в отдельном отладчике. Обнаружив ошибку, этот тест генерирует исключение «нарушение доступа» (access violation),
- **Invalid handle usage detection** Выявляет общие ошибки при использовании описателей. Обнаружив ошибку, этот тест также генерирует нарушение доступа.
- **Thread stack size checking** Запрещает увеличивать стек потока, что вызывает исключение «переполнение стека», если исходно выделенной под стек памяти оказывается недостаточно.
- **LogStartAndStop** Записывает в журнал некоторые сведения при запуске и завершении работы приложения, что облегчает чтение журналов при анализе результатов тестирования.
- **FilePaths** Ведет мониторинг попыток приложения получить путь к файлу. Позволяет определить, не использует ли программа пути, «зашитые» в код, или нестандартные способы сбора информации. Этот тест может вызвать крах приложения, если оно попытается некорректно получить путь к файлу.
- **HighVersionLie** В прошлом многие приложения создавались для работы только в одной версии Windows. Этот тест возвращает приложению в ответ на запрос версии ОС заведомо больший номер.
- **RegistryChecks** Ведет мониторинг использования реестра приложением, регистрируя все некорректные или опасные вызовы.

Выбрав нужный тест, щелкните Options, чтобы настроить его (рис. 18-2). Затем запустите приложение, щелкнув кнопку Run в AppVerifier. Попробуйте задействовать как можно больше функций программы, чтобы сгенерировать максимально полные данные для журналов AppVerifier. Закройте приложение и изучите журнал — для этого нужно щелкнуть View Logs.

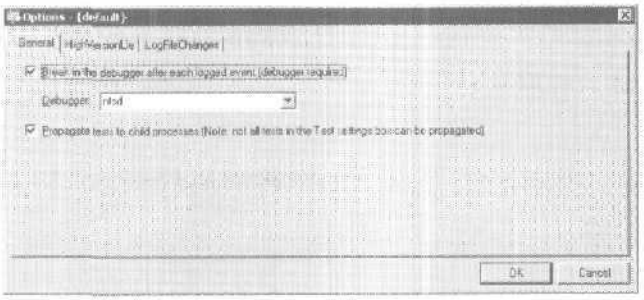


Рис. 18-2. Выберите тесты, которым вы хотите подвергнуть приложения

Параметры тестирования, заданные в AppVerifier для приложения, будут активизироваться при каждом его запуске и будут доступны, пока это приложение не будет удалено из списка приложений AppVerifier. Это позволяет многократно проводить тестирование с заданными параметрами при диагностике проблем.

Первые четыре теста AppVerifier (см. список выше) выявляют проблемы на уровне ядра, поэтому результаты этих тестов доступны только через отдельный отладчик ядра. Обнаружив ошибку в программе, эти тесты генерируют исключение «нарушение доступа», чтобы отладчик ядра подключился в месте возникновения ошибки. Если запустить AppVerifier без подключенного отладчика, ошибка, обнаруженная при тесте ядра, вызовет крах приложения.

Чтобы запустить приложение с отладчиком, выберите в AppVerifier нужные тесты, после чего можно запустить приложение с отладчиком, как описано в инструкции к отладчику. Например, для отладки приложения Myapp.exe с помощью NTSD (это системный отладчик Windows XP), вызовите командную строку и наберите **ntsd myapp.exe.**

С AppVerifier можно применять любые отладчики при условии, что тестировщик знает, как ими пользоваться,

Тестирование на соответствие требованиям логотипа «Designed for Windows»

Программа присвоения логотипа «Designed for Windows» позволяет отметить продукты, которые по результатам испытаний показали высокий уровень совместимости с Windows. Ряд

тестов Application Verifier связан с этой программой. При помощи этих тестов любой **ISV,** выдвигающий свой продукт на получение логотипа «Designed for Windows», может проверить его на соответствие предъявляемым требованиям. Эти тесты помечены номером после названия (рис. 18-3).

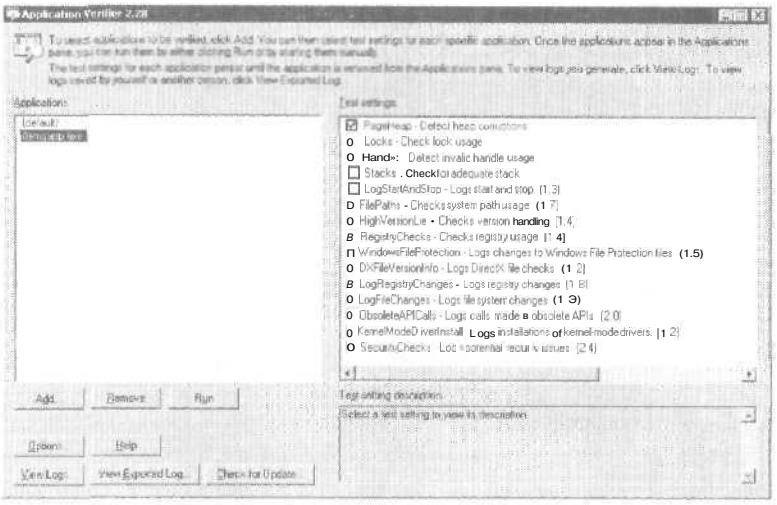


Рис. 18-3. Application Verifier тестирует приложения на соответствие требованиям логотипа «Designed for Windows»

Нумерация тестов в интерфейсе Application Verifier соответствует таковой в требованиях спецификации Designed for Windows XP Application Specification. Например, тест WindowsFileProtection (1.5) проверяет приложения на соответствие пятому требованию из первого раздела: «поддержка быстрого переключения пользователей и удаленного рабочего стола», поскольку корректное использование системных каталогов является одной из составляющих поддержки быстрого переключения пользователей в Windows XP и более высоких версиях Windows.

Application Verifier позволяет обнаружить примерно 90% ошибок, которые Microsoft выявляет в продуктах, не соответствующих требованиям логотипа «Designed for Windows». Сделав Application Verifier инструментом цикла разработки, вы уст-

раните большинство ошибок, которые могут помешать получить логотип. Кроме того, этот инструмент делает приложение более удобным для клиентов.

Требования к совместимым приложениям

Ниже описаны некоторые тесты из Windows XP Logo Test Framework, которые позволят оценить, насколько приложение соответствует предъявляемым требованиям. Если вы планируете выдвинуть свой продукт на получение логотипа «Designed for Windows», обратитесь на сайт *http://www.windowslogo.com/.*

- Остается ли приложение стабильным при тестировании основных функций?
- Сохраняет ли приложение стабильность при использовании мыши с более чем тремя кнопками?
- Сохраняет ли приложение свои временные файлы в пользовательской временной папке?
- Использует ли приложение для хранения временных файлов при установке только временную папку пользователя?
- Использует ли приложение для хранения временных файлов при тестировании его функциональности только временную папку пользователя?
- Не вызывают ли длинные имена файлов, папок и принтеров крах приложения или потерю данных?
- Сохраняет ли приложение стабильность, записывая файл в каталог User1 LFNPathl, вложенный в папку My Documents пользователя Userl?
- Сохраняет ли приложение стабильность при записи файла в каталог, заданный при помощи длинного пути Userl LFNPath2?
- Сохраняет ли приложение стабильность при записи файлов с длинными именами?
- Сохраняет ли приложение стабильность, открывая файл из каталога Userl LFNPathl, вложенного в папку My Documents пользователя Userl?
- Остается ли приложение стабильным при чтении файла из каталога, заданного при помощи длинного пути Userl LFNPath2?
- Сохраняет ли приложение стабильность при чтении файлов с длинным именем?

- Остается ли приложение стабильным при печати на принтере с длинным именем?
- Сохраняет ли приложение стабильность и способность выполнять основные функции на компьютере с двумя процессорами?
- Не происходит ли крах приложения при запуске в отсутствие используемых им устройств?
- Сохраняет ли приложение стабильность, если инициировать печать в отсутствие установленного принтера?
- Сохраняет ли приложение стабильность при попытке использования отсутствующего устройства?
- Способно ли приложение вернуть дисплей в исходный режим после того, как оно автоматически переключило его в 256-цветный режим?
- Все ли драйверы режима ядра проходят тестирование, когда Windows XP загружает их?
- Все ли драйверы режима ядра проходят тестирование функциональности, если активизированы стандартные тесты ядра?
- Все ли драйверы режима ядра проходят испытания дефицитом ресурсов?
- Все ли драйверы, используемые приложением, проверены в Windows Hardware Quality Labs (WHQL)?
- Выводится ли во время тестирования предупреждение об использовании неподписанных драйверов?
- Корректно ли выполняется установка приложений в текущей и будущих версиях Windows?
- Вся ли функциональность приложения способна пройти тестирование в текущей и будущих версиях Windows?
- Поддерживает ли приложение Fast User Switching?
- Поддерживает ли приложение Remote Desktop?
- Если приложение устанавливает нестандартную библиотеку графической идентификации и аутентификации (Graphical Identification and Authentication, GINA), поддерживает ли эта библиотека Remote Desktop?
- Все ли функции приложения проходят тестирование при использовании тем оформления Windows XP?

- Не вызывает ли переключение между приложениями с помощью Alt+Tab искажения вида приложения или потери данных?
- Не вызывает ли переключение между приложениями с помощью кнопки Пуск и панели инструментов искажения вида приложения или потери данных?
- Нормально ли отображаются окна системы безопасности Windows и диспетчера задач? Можно ли закрыть приложение или прервать его исполнение без потери данных?
- Выводятся ли сообщения Windows File Protection при установке приложения?
- Способно ли приложение к миграции из Windows 98 в Windows XP Home Edition?
- Способно ли приложение к миграции из Windows Me в Windows XP Home Edition?
- Способно ли приложение к миграции из Windows 98 в Windows XP Professional?
- Способно ли приложение к миграции из Windows Me в Windows XP Professional?
- Способно ли приложение к миграции из Windows NT 4.0 Workstation в Windows XP Professional?
- Способно ли приложение к миграции из Windows 2000 Professional в Windows XP Professional?
- Не заменяет ли приложение стандартные файлы старыми версиями?
- Помечены ли исполняемые файлы приложения номером версии, именем продукта и компании?
- Не требуется ли перезагрузка после установки приложения?
- Все ли тесты из Test Framework можно завершить без перезагрузки приложения?
- Предлагает ли приложение папку в каталоге C:\Program Files для установки по умолчанию?
- Устанавливает ли приложение обшие файлы в корректные каталоги?
- Добавляются ли при установке все необходимые элементы в системный реестр?

- Полностью ли удаляются файлы и элементы реестра при удалении приложения владельцем? Не удаляются ли при этом лишние элементы?
- Корректно ли выполняется удаление приложения из-под учетной записи User1?
- Можно ли установить приложение после его удаления?
- Предоставляет ли приложение возможность установки «для всех пользователей» по умолчанию или только при установке владельцем (Owner)?
- Предоставляет ли приложение возможность установки «для всех пользователей» по умолчанию или только при установке из-под учетной записи Userl?
- Запускается ли программа установки приложения через Autorun?
- Способна ли установочная программа приложения определить, что программа уже установлена, и не допустить повторной установки?
- Верный ли каталог предлагает приложение при попытке открыть файл, созданный пользователем Userl?
- Предлагает ли приложение верный каталог при попытке сохранить файл, созданный пользователем Userl?
- Предлагает ли приложение верный каталог при попытке открыть файл, созданный пользователем User2?
- Предлагает ли приложение верный каталог при попытке сохранить файл, созданный пользователем User2?
- Не превышает ли объем данных, которые приложение записывает в реестр для пользователя Userl, 128 Кб?
- Корректны ли каталоги, в которых приложение сохраняет сведения о конфигурации для пользователя Userl?
- Запрещает ли приложение пользователю Userl записывать файлы в системный каталог Windows?
- Запрещает ли приложение пользователю Userl модифицировать документы, принадлежащие пользователю User2?
- Запрещает ли приложение пользователю Userl модифицировать глобальные параметры?
- Разрешает ли приложение пользователю Userl повторить установку, если во время установки произошел сбой? Под-

держивает ли оно корректное удаление, если пользователь отказывается повторить установку?

Дополнительные сведения

Дополнительные сведения см. по адресам:

- Using the Application Compatibility Toolkit — http:// www.microsoft.com/windowsserver2003/compatible/appcom-pat.mspx;
- Windows Application Compatibility Toolkit download — http:// www.microsoft.com/downloads/release.asp?releaseid=42071.

Об авторе

Джерри Ханикат (Jerry Honeycutt) знакомит читателей с популярными технологиями, включая семейство продуктов Microsoft Windows, IP-сети и Интернет. Он достиг в этом успеха, однако предпочитает помогать компаниям в развертывании и управлении компьютерами.

Джерри написал 25 книг. Его последние творения — «Microsoft Windows XP Registry Guide» (Microsoft Press, 2002) и «Introducing Microsoft Windows 2000 Professional» (Microsoft Press, 1999). Большинство его книг продается в разных странах и переведено на разные языки.

Джерри также ведет рубрики в Microsoft Expert Zone, Web-сайте для поклонников Windows XP и участвует в создании многих страниц на Web-сайте Microsoft, включая Office XP и TechNet. Он часто публикуется на деловых сайтах, включая *Smart Business* и *CNET*. Джерри часто выступает на разных публичных мероприятиях, таких как COMDEX, Developer Days, Microsoft Exchange Conference и Microsoft Global Briefing, а также поддерживает конференции на Web-сайте Microsoft TechNet.

Однако Джерри не только пишет и выступает: он специализируется на внедрении и сопровождении настольных систем, в основном с использованием продуктов семейства Windows. Его опыт оценили такие организации, как Capital One, Travelers, IBM, Nielsen North America, IRM, Howard Systems International и NCR.

Джерри закончил Техасский университет в Далласе в 1992 г., получив степень бакалавра информатики. Он также учился в Техасском техническом университете в Лаббоке. В свободное время Джерри играет в гольф, занимается фотографией и путешествует. Он страстный коллекционер редких книг и фишек из казино. Живет Джерри во Фриско, под Далласом, в штате Техас.

Заглядывайте на Web-сайт Джерри: www.honeycutt.com и пишите ему по адресу jerry@honeycutt.com.

Системные требования

С этой книгой поставляется 360-дневная ознакомительная версия Microsoft Windows Server 2003 Standard Edition. В период написания этой книги ОС Windows Server 2003 была в стадии предварительной реализации (RC2), и полная поддержка этого продукта не осуществляется.

Информацию, которая поможет вам с поддержкой Windows Server 2003, вы найдете по адресу *http://www.microsoft.com/windows.server2003/support*.

Аппаратные требования RC2

Минимальные и рекомендуемые ресурсы, необходимые для работы Windows Server 2003, Standard Edition

Минимальная скорость процессора	133 МГц
Рекомендуемая скорость процессора	550 МГц
Минимальный объем ОЗУ	128 Мб
Рекомендуемый объем ОЗУ	256 Мб
Максимальный объем ОЗУ	4 Гб
Многопроцессорная поддержка	До 4
Дисковое пространство для установки	1.5 Гб

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ MICROSOFT

прилагаемый к книге компакт-диск

ЭТО ВАЖНО - ПРОЧИТАЙТЕ ВНИМАТЕЛЬНО. Настоящее лицензионное соглашение (далее «Соглашение») является юридическим документом, оно заключается между Вами (физическим или юридическим лицом) и Microsoft Corporation (далее «корпорация Microsoft») на указанный выше продукт Microsoft, который включает программное обеспечение и может включать сопутствующие мультимедийные и печатные материалы, а также электронную документацию (далее «Программный Продукт»). Любой компонент, входящий в Программный Продукт, который сопровождается отдельным Соглашением, подпадает пол действие именно того Соглашения, а не условий, изложенных ниже. Установка, копирование или иное использование данного Программного Продукта означает принятие Вами данного Соглашении. Если Вы не принимаете его условия, то не имеете права устанавливать, копировать или как-то иначе использовать этот Программный Продукт.

ЛИЦЕНЗИЯ НА ПРОГРАММНЫЙ ПРОДУКТ

Программный Продукт защищен законами Соединенных Штатив по авторскому праву и международными договорами по авторскому праву, а также другими законами и договорами ло правам на интеллектуальную собственность.

1. **ОБЪЕМ ЛИЦЕНЗИИ.** Настоящее **Соглашение дает Вам право:**
   - a) Программный **продукт**. Вы можете установить и использовать одну копию Программного Продукта на одном компьютере. Основной пользователь компьютера, на котором установлен данный Программный Продукт, может сделать только для себя вторую копию и использовать ее на портативном компьютере.
   - b) Хранение или **использование** в сети. Вы можете также скопировать или установить экземпляр Программного Продукта на устройстве хранения, например на сетевом сервере, исключительно для установки или запуска данного Программного Продукта на других компьютерах в своей внутренней сети, но тогда Вы должны приобрести лицензии на каждый такой компьютер. Лицензию на данный Программный продукт нельзя использовать совместно или одновременно на других компьютерах.
   - c) License Halt. Если Вы купили эту лицензию в составе Microsoft License Pak, можете сделать ряд дополнительных копий программного обеспечении, входящего в данный Программный Продукт, и использовать каждую копию так, как было описано выше. Кроме того, Вы получаете право сделать соответствующее число вторичных копий для портативного компьютера в целях, также оговоренных выше,
   - d) Примеры кода. Это относится исключительно к отдельным частям Программного Продукта, заявленным как примеры кода (далее «Примеры»), если таковые входят в состав Программного Продукта.
     - i) **Использование** и **модификация**. Microsoft дает Вам право использовать и модифицировать исходный код Примеров при условии соблюдения пункта (d)(iii) ниже. Вы не имеете права распространять в виде исходного кода ни Примеры, ни их модифицированную версию.
     - ii) Распространяемые файлы. При соблюдении пункта (d)(iii) Microsoft дает Вам право на свободное от отчислений копирование и распространение в виде объектного кола Примеров или их модифицированной версии, кроме тех частей (или их модифицированных версий), которые оговорены в файле Readme, относящемся к данному Программному Продукту, как не подлежащие распространению.
     - iii) **Требования к распространению** файлов. Вы можете распространять файлы, разрешенные *к распространению*, при условии, что: а) *распространяете* их в виде *объектного* кода *только* в сочетании со своим приложением и как его часть; б) не используете название, эмблему или товарные знаки Microsoft для продвижения своего приложения; в) включаете имеющуюся в Программном Продукте ссылку на авторские права в состав этикетки и заставки своего приложения; г) согласны освободить от ответственности и взять на себя защиту корпорации Microsoft от любых претензий или преследований по закону, включая судебные издержки, если таковые возникнут в результате использования или распространения Вашего приложения; и д) не допускаете дальнейшего распространения конечным пользователем своего приложения. По поводу отчислений и других условий лицензии применительно к иным видам использования или распространения распространяемых файлов обращайтесь в Microsoft.

2- ПРОЧИЕ ПРАВА И ОГРАНИЧЕНИЯ

- **Ограничения на реконструкцию, декомпиляцию и дизассемблирование.** Вы не имеете права реконструировать, декомпилировать или дизассемблировать данный Программный Продукт, кроме того случая, когда такая деятельность (только в той мере, которая необходима) явно разрешается соответствующим законом, несмотря на это ограничение.
- **Разделение компонентов.** Данный Программный Продукт лицензируется как единый продукт. Его компоненты нельзя отделять друг от друга для использования более чем на одном компьютере.
- **Аренда.** Данный Программный Продукт нельзя сдавать в прокат, передавать *по* временное пользование или уступать для использования в иных целях.
- **Услуги по технической** поддержке. Microsoft может (но не обязана) предоставить Вам услуги по технической поддержке данного Программною Продукта (далее «Услуги»). Предоставление Услуг регулируется соответствующими правилами и программами Microsoft, описанными в руководстве пользователя, электронной документации и/или других материалах, публикуемых Microsoft. Любой дополнительный программный код. предоставленный в рамках Услуг, следует считать частью данного Программною Продукта и подпадающим под действие настоящего Соглашения. Что касается технической информации, предоставляемой Вами корпорации Microsoft при использовании *ее* Услуг, то Microsoft может задействовать чту информацию и деловых целях, в том числе для технической поддержки продукта и разработки. Используя такую техническую информацию, Microsoft не будет ссылаться на [Sac.
- **Передача прав на программное обеспечение.** Вы можете безвозвратно уступить все права, регулируемые настоящим Соглашением, при условии, что не оставите себе никаких копий, передалите все составные части данного Программного Продукта (включая компоненты, мультимедийные и печатные материалы, любые обновления. Соглашение и сертификат подлинности, если таковой имеется) н принимающая сторона согласится с условиями настоящего Соглашения.
- **Прекращение действия Соглашения.** Без ущерба для любых других прав Microsoft может прекратить действие настоящего Соглашения. если Вы нарушите его условия. В этом случае Вы должны будете уничтожить все копии данного Программного Продукта вместе со всеми его компонентами.

3. АВТОРСКОЕ **ПРАВО.** Все авторские права и право собственности на Программный Продукт (в том числе любые изображения, фотографии, анимации, видео, аудио, музыку, текст. примеры кода, распространяемые файлы и апплеты, включенные в состав Программного Продукта) и любые его копии принадлежат корпорации Microsoft или ее поставщикам. Программный Продукт охраняется законодательством об авторских правах и положениями международных договоров. Таким образом, Вы должны обрашагься с данным Программным Продуктом, как с любым другим материалом, охраняемым авторскими правами, **с** тем **исключением**, что Вы можете установить Программный Продукт на один компьютер при условии, что храните оригинал исключительно как резервную или архивную копию. Копирование печатных материалов, поставляемых вместе с Программным Продуктом, запрещается.

ОГРАНИЧЕНИЕ ГАРАНТИИ

ДАННЫЙ ПРОГРАММНЫЙ ПРОДУКТ (ВКЛЮЧАЯ ИНСТРУКЦИИ ПО ЕГО ИСПОЛЬЗОВАНИЮ) ПРЕДОСТАВЛЯЕТСЯ БЕЗ КАКОЙ-ЛИБО ГАРАНТИИ. КОРПОРАЦИЯ MICROSOFT СНИМАЕТ С СЕБЯ ЛЮБУЮ ВОЗМОЖНУЮ ОТВЕТСТВЕННОСТЬ, В ТОМ ЧИСЛЕ ОТВЕТСТВЕННОСТЬ ЗА КОММЕРЧЕСКУЮ ЦЕННОСТЬ ИЛИ СООТВЕТСТВИЕ ОПРЕДЕЛЕННЫМ ЦЕЛЯМ. ВЕСЬ РИСК ПО ИСПОЛЬЗОВАНИЮ ИЛИ РАБОТЕ С ПРОГРАММНЫМ ПРОДУКТОМ ЛОЖИТСЯ НА ВАС.

НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ КОРПОРАЦИЯ MICROSOFT, ЕЕ РАЗРАБОТЧИКИ, А ТАКЖЕ ВСЕ, ЗАНЯТЫЕ В СОЗДАНИИ, ПРОИЗВОДСТВЕ И РАСПРОСТРАНЕНИИ ДАННОГО ПРОГРАММНОГО ПРОДУКТА. НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА КАКОЙ-ЛИБО УЩЕРБ (ВКЛЮЧАЯ ВСЕ, БЕЗ ИСКЛЮЧЕНИЯ, СЛУЧАИ УПУЩЕННОЙ ВЫГОДЫ, НАРУШЕНИЯ ХОЗЯЙСТВЕННОЙ ДЕЯТЕЛЬНОСТИ, ПОТЕРИ ИНФОРМАЦИИ ИЛИ ДРУГИХ УБЫТКОВ) ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ИЛИ НЕВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ДАННОГО ПРОГРАММНОГО ПРОДУКТА ИЛИ ДОКУМЕНТАЦИИ, ДАЖЕ ЕСЛИ КОРПОРАЦИЯ MICROSOFT БЫЛА ИЗВЕЩЕНА О ВОЗМОЖНОСТИ ТАКИХ ПОТЕРЬ, ТАК КАК В НЕКОТОРЫХ СТРАНАХ НЕ РАЗРЕШЕНО ИСКЛЮЧЕНИЕ ИЛИ ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ ЗА НЕПРЕДНАМЕРЕННЫЙ УЩЕРБ. УКАЗАННОЕ ОГРАНИЧЕНИЕ МОЖЕТ ВАС НЕ КОСНУТЬСЯ.

РАЗНОЕ

Настоящее Соглашение регулируется законодательством штата Вашингтон (США), кроме случаев (и лишь в той мере, насколько это необходимо) исключительной юрисдикции того государства, на территории которого используется Программный Продукт.

Если у Вас возникли какие-либо вопросы, касающиеся настоящего Соглашения, или если Вы желаете святься *с* Microsoft по любой другой причине, пожалуйста, обращайтесь в местное представительство Microsoft или пишите по адресу: Microsoft Sales Information Center, One Microsoft Way, Redmond, WA 98052-6399.

Ханикат **Джерри**

Знакомство с Microsoft Windows Server 2003

Переводчик *А. Е. Соловченко*

Технический редактор **Л.** *А. Панчук*

Компьютерная верстка *В. В, Хильченко*

Дизайнер обложки *Е. В, Козлова*

Оригинал-макет выполнен с использованием
издательской системы Adobe PageMaker 6.0

TypeMarket*FontLibrary*
легальный пользователь

ПОЛЬЗОВАТЕЛЬ Para(-)Type IN LEGAL USE

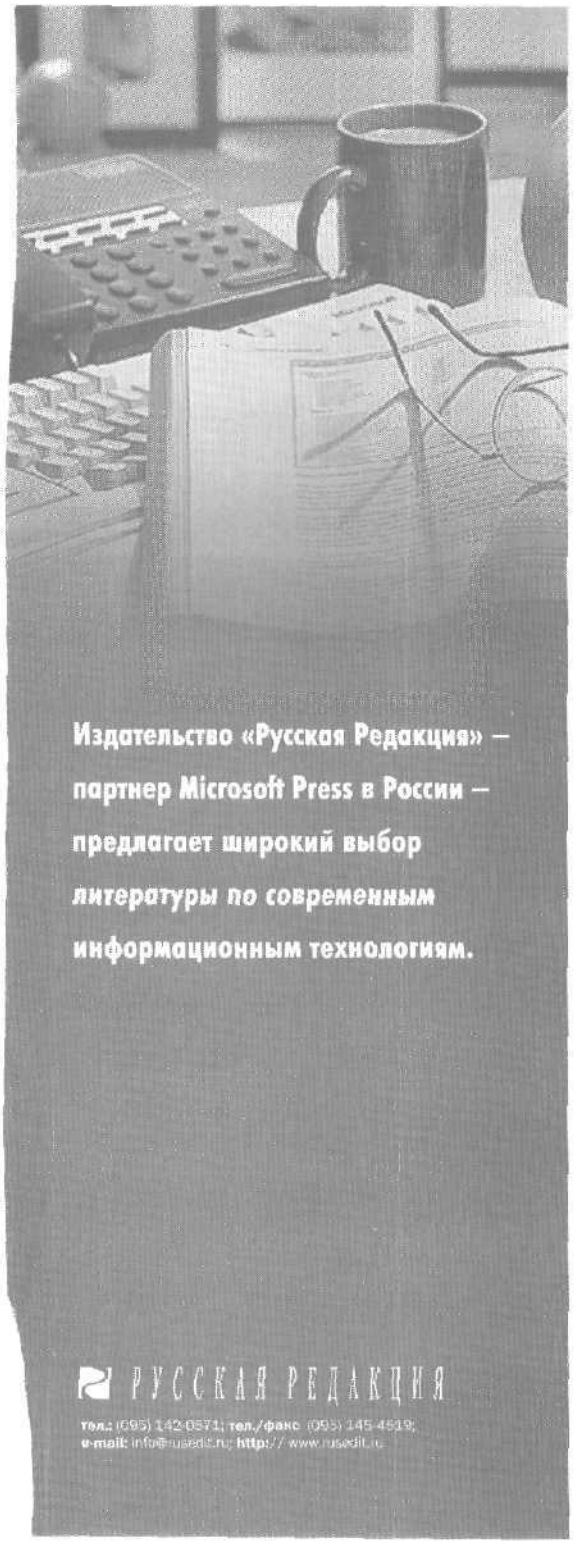
Главный **редактор** *А, И. Козлов*

Подготовлено к печати издательством «Русская Редакция»
121087, Москва, ул. Заречная, д.9
тел.: (095) 142-0571, тел./факс; (095) 145-4519
e-mail: info@rusedit.ru, http:// www.rusedit.ru

РУССКАЯ РЕДАКЦИЯ

Подписано в печать 23.04.03 г. Тираж 3000 экз.
Формат 60x90/16. Физ. п. л. 24

Отпечатано в ОАО «Типография «Новости»
107105. Москва, ул. Фр. Энгельса, 46



Издательство «Русская Редакция» — партнер Microsoft Press в России — предлагает широкий выбор *литературы по современным* информационным технологиям.

РУССКАЯ РЕДАКЦИЯ

тел.: (095) 142-6571; **тел./факс** (095) 145-4519;
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) 778-7369

«Библио-Глобус» ул. Мясницкая, 6, тел.: (095) 928-3567

«Московский дом книги» ул. Новый Арбат, 8. тег - (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) 229-6483

• ***в* Санкт-Петербурге:**

СПб Дом книги, Невский пр-т., 28 тел.: (812) 318-6402

СПб Дам 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** Дом **«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) 59-1200

• **в Великом Новгороде:**

«Наука и техника», ул БольшаяСанкт-Петербургская. 44, Дворец Молодежи, 2-й этаж

• **в Новосибирске:**

ООО **«Топ-книга»**, тел.: (3332) 36-1026

• **в Алматы (Казахстан):**

ЧП Болат Амреев, моб. тел : 8-327-908-28-57, (3272) 76-1404

• **в Киеве (Украина):**

ООО Издательство **«Ирина-Пресс»**, тел.: (+1038044) 269-0423

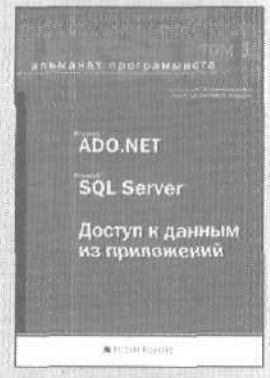
«Техническая книга на **Петровке»**, тел.: (+1038044) 268-5346

Альманах (*от араб. аль-манах — календарь*)
непериодический сборник, содержащий сведени
из различных областей общественной деятельности, обычн
с указанием литературных новинок, научных достижени
законодательных изменений и т.

большая *Советская Энциклопед*

Представляем тематический сборник

«АЛЬМАНАХ ПРОГРАММИСТА



Альманах программиста,
том 1: Microsoft ADO.NET,
Microsoft SQL Server,
доступ к данным
из приложений.
400 стр., апрель 2003 г.

Альманах программиста,
том 2: Microsoft ASP.NET,
Интернет-приложения.
400 стр., сентябрь 2003 г.

Это уникальное издание адресовано профессионалам в области современных информационных технологий. Каждый том представляет собой тематический сборник статей из журнала «MSDN Magazine» и Microsoft MSDN Library по наиболее актуальным и перспективным технологиям разработки программного обеспечения.

Планируется выпуск альманахов по базовым механизмам .NET Framework (модели защиты, отражение, удаленное взаимодействие, сервисы взаимодействия с неуправляемым кодом и т. д.), специфике языков программирования, поддерживающих .NET, отладке/тестированию и другим темам.

Если вас интересует специфическая тематика или определенные материалы из «MSDN Magazine» и MSDN Library, обращайтесь на сайт издательства *www.rusedit.ru* или по адресу ***almanah@rusedit.ru.***
Мы постараемся учесть ваши пожелания в будущих выпусках альманаха.

издательство компьютерной литературы

И РУССКАЯ РЕДАКЦИЯ

Продажа книг
оптом: тел.: (095) 142-0571, e-mail: sale@rusedit.ru;
интернет-магазин: http:// www.ITbook.ru, тел.: (095) 145-4519

Подробное и достоверное описание новых возможностей и усовершенствований в Microsoft Windows Server 2003

Microsoft Windows Server 2003 повышает эффективность, производительность и безопасность по сравнению с предыдущими версиями. Из этого официального руководства вы узнаете о новинках и улучшениях в этой мощной сетевой операционной системе, в том числе об усовершенствованных технологиях Web-сервисов и компонентов, безопасности, сетевой поддержке, службе каталогов Active Directory, Microsoft Internet Information Services, поддержке IPv6 и многом другом.

В книге рассматриваются следующие темы

- Знакомство с семейством Windows Server 2003: его возможности и требования
- Преимущества Windows Server 2003

Как начать работу

- Развертывание Windows Server 2003
- Переход с Windows NT Server
- Переход с Windows 2000 Server
- Тестирование совместимости приложений

Подробности о новых и улучшенных возможностях

- Служба Microsoft Active Directory
- Службы управления и консоль управления групповой политикой
- Службы, повышающие безопасность
- Сети и коммуникации
- Службы терминалов
- Internet Information Services
- Приложения и Web-сервисы XML
- Службы Microsoft Windows Media
- Файловые службы и управление хранилищами
- Службы печати
- Службы кластеризации
- Многоязыковая поддержка

Содержимое компакт-диска

- 360-дневная *ознакомительная версия Microsoft Windows Server 2003 Standard Edition Release Candidate 2*

Об авторе

Джерри *Ханикат* — популярный автор, написавший 25 книг, в том числе «Microsoft Windows XP Registry Guide» (Microsoft Press, 2002) и «Introducing Microsoft Windows 2000 Professional» (Microsoft Press, 1999). Он ведет рубрики в Microsoft Expert Zone (www.microsoft.com/windowsxp/expertzone/) и участвует в создании многих страниц на Web-сайте Microsoft, включая Office XP и TechNet. В свободное от писательского труда время он разъезжает по всему свету, помогая малым и большим предприятиям внедрять Windows XP и Office XP. Джерри часто выступает на разных публичных мероприятиях, таких как COMDEX, Developer Days и Microsoft Exchange Conferenc

ISBN 5-7502-0237-2

Web-узел издательства: www.rusedit.ru
Интернет-магазин: www.ITbook.ru