Содержание

Колонка редактора

Александр Иванюк
выпускающий редактор

Венец эволюции

Все мы когда-то были начинающими компьютерными пользователями: запоминали консольные команды, методом проб и ошибок осваивали оконные интерфейсы, учились пользоваться программными пакетами и необходимыми утилитами. У кого-то этот этап занимает больше времени, у кого-то меньше, но рано или поздно мы можем сказать: да, теперь я вправе считать себя продвинутым компьютерным пользователем. Дальше можно развиваться в сторону освоения различным платформ — Mac, альтернативных Microsoft операционных систем, например Linux или Lindows. Но, пожалуй, венцом этой компьютерной эволюции будет навык заставить несколько компьютеров, объединенных в сеть, слаженно работать вместе, постигнув тем самым умение, называемое администрированием. Впрочем, стать человеком, перед которым обычные пользователи благоговеют в любой организации, где работа связана с компьютерами, не так уж сложно. Особенно если мы говорим об администрировании операционных систем семейства Windows, которые всегда отличались дружественным интерфейсом и простотой освоения.

Читая этот спецвыпуск, посвященный новейшей сетевой ОС от Microsoft — Windows Server 2003, вы сами убедитесь в этом. Ведь установка системы, настройка многочисленных сервисов, служб и серверов совсем не сложна, особенно если раньше вы работали с Windows 2000 или XP. Единственное, на что придется обратить большее внимание, — это вопросы безопасности. При этом не стоит верить распространенному среди матерых системных администраторов мнению, что на основе Windows нельзя создать надежной сетевой структуры. Попробуйте сами — и вы убедитесь, что это далеко не так.

Содержание

CHIP CO SPECIAL #11

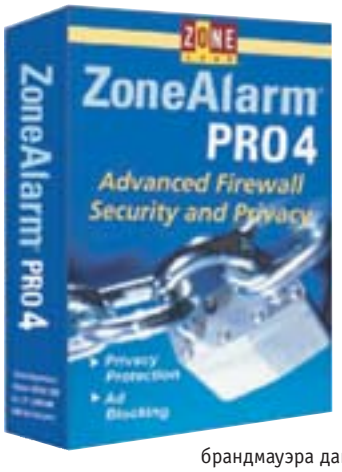
602Pro LAN Suite 2003

Данный программный пакет предоставляет различные сетевые сервисы и средства их администрирования и журналирования, защищает компьютер от хакеров, спама и вирусов. Это комплексное решение наверняка будет привлекательно для локальных сетей небольших предприятий вследствие небольшой совокупной цены владения. С помощью этой программы можно установить защищенный от несанкционированного доступа с почтовый сервер. Доступ к нему может осуществляться как через стандартные POP-клиенты, так и через веб-интерфейс. Установка включенного в дистрибутив факс-сервера даст возможность всем пользователям сети принимать и отправлять факсы. С помощью кэширующего прокси-сервера пользователи смогут более эффективно использовать доступ в Интернет. Для него можно задать правила IP-фильтрации и закрыть трафик для некоторых узлов сети. Если у вас возникнет потребность в небольшой информационной страничке о компании, полезным окажется встроенный веб-сервер. Легкий в настройке он поддерживает программные интерфейсы FastCGI, CGI и IDAPI, виртуальный хостинг и защиту информации по протоколу SSL.

Условия распространения: trialware **Язык интерфейса:** английский **Сайт производителя:** www.software602.com

ZoneAlarm Pro 4.5

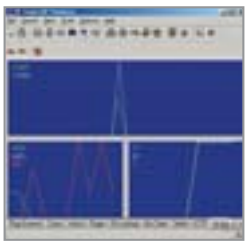
Недремлющие хакеры сканируют сеть в поисках лазеек на компьютер, чтобы получить личную и финансовую информацию. Даже официальные веб-сайты используют методы шпионажа, такие как cookies, которые отслеживают вашу личность и предпочтения в просмотре страниц. А если вы подключены к локальной сети, то угроза вторжения и несанкционированного доступа к информации возрастает многократно. В таких условиях не обойтись без программного щита от атак извне — firewall. Одна из наиболее популярных программ этого класса — ZoneAlarm. Надо отметить, что по сравнению со многими аналогичными программами от других производителей с большинством настроек ZoneAlarm легко разобраться. После первого запуска wizard проведет вас через процедуру установки наиболее важных параметров, посвященных сетевой безопасности. Помимо обычных функций брандмауэра данная программа также может сканировать почтовые сообщения на предмет наличия в них вредоносного кода, вырезать баннеры с веб-страниц и предотвращать отправку в Интернет конфиденциальной информации.



Условия распространения: trialware **Язык интерфейса:** английский **Сайт производителя:** www.zonelabs.com

IP Tools 2.20

Набор утилит, без которых не обойдется ни один администратор сети. Каждая из них предоставляет информацию о локальной системе, сетевых подключениях, включенных сервисах и открытых портах на удаленных компьютерах, регистрационных данных доменов и о многом другом. Также имеется Telnet-клиент.



Условия распространения: trialware **Язык интерфейса:** английский **Сайт производителя:** www.ks-soft.net

Software Update Services

Причиной взлома компьютерных сетей часто является невнимательность или лень системного администратора, не установившего вовремя критические заплатки и обновления на сервере. Однако обновления выпускаются чуть ли не ежедневно, а видимых из Интернета серверов или компьютеров в локальной сети предприятия может быть несколько. В связи с этим поддержка защиты на должном уровне превращается в рутинную и обременительную работу. Автоматизировать этот процесс призван новый инструмент от Microsoft — Software Update Services (SUS). Этот пакет позволяет администратору быстро установить важнейшие обновления на серверах, работающих под управлением Windows Server 2000 и 2003, а также на рабочих станциях с Windows 2000 Professional или Windows XP Professional. Работа с SUS выглядит так: после синхронизации с серверами Microsoft Windows Update администратор выбирает, какие обновления будут доступны пользователям. Затем компьютеры локальной сети, на которых установлен клиент Automatic Updates, по расписанию получают эти обновления.

Условия распространения: freeware **Язык интерфейса:** английский **Сайт производителя:** www.microsoft.com

Win 2003 Optimize Tool 1.44

Несмотря на то что операционная система Windows Server 2003 предназначена прежде всего для использования в качестве сервера, многие пользователи ставят ее и на обычные компьютеры. Однако ряд мультимедийных возможностей и привычных настроек интерфейса по умолчанию заблокирован. Большинство этих настроек можно сделать вручную и превратить Windows в подобие операционной системы для рабочих станций.

Данная программа автоматизирует этот процесс и снабжает подсказками по каждой из настроек. Так, например, можно отключить надоедающий при каждой перезагрузке ввод Ctrl+Alt+Del и Shutdown Event Tracker. Также из этой утилиты можно узнать о совместимых с ОС антивирусах, firewall и других типах программ или установить стандартные игры Windows (для этого потребуется диск Windows XP).

Условия распространения: freeware
Язык интерфейса: английский
Сайт производителя: www.hot.ee/salasource

Avant Browser 8.02

Строго говоря, Avant Browser не браузер, а надстройка над Internet Explorer, предоставляющая множество удобных и полезных возможностей. Для людей, экономящих трафик, полезными будут кнопки быстрого отключения/включения картинок, флэш-анимации и всплывающих окон. Вообще чувствуется, что разработчики уделили много внимания удобству интерфейса. Например, удерживая правую клавишу мыши и нажав левую, вы переместитесь на предыдущую веб-страницу. Нажатие клавиш в обратной последовательности приведет вас к следующей странице. Программа работает в многооконном режиме и открывает новые страницы во вкладках. Доступен русский интерфейс и разнообразные скины. При установке программа попросит заполнить форму с личной информацией и оптимистично заверит вас, что это последняя форма, которую приходится заполнять вручную, так как браузер включает в себя AI RoboForm — менеджер паролей и заполнения форм. Этот модуль сохраняет используемые вами при веб-серфинге пароли и шифрует их. Также он заполняет формы, автоматически нажимает кнопки «Login/Send», генерирует пароли.

Условия распространения: freeware **Интерфейс:** русский **Сайт производителя:** www.avantbrowser.com

Friendly Chat 4.5.6

Программа для организации чата в локальной сети. Не требует выделенного сервера. Имеет встроенный IRC-клиент, автоответчик, звуковые сигналы, доску объявлений, записную книжку, журналы, возможность посылать приватные сообщения и многое другое. Также доступно большое количество настроек интерфейса. Интересной и полезной функцией программы является создание дистрибутива чата со своими специфическими настройками. Такой дистрибутив можно затем передать другим пользователям локальной сети, что сэкономит время на ее конфигурировании.

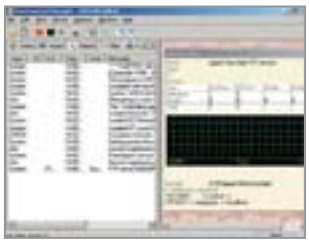
Условия распространения: freeware
Язык интерфейса: английский **Сайт производителя:** www.kilievich.com/rus/fchat

VisualRoute 8.0a

С помощью этой программы легко узнать маршрут, по которому TCP-пакеты проходят от вас до пункта назначения. На карте мира можно увидеть, в какой стране расположен хостинг того или иного веб-сайта. Программа встраивается в Internet Explorer, и произвести traceroute можно всего лишь одним кликом мыши. Помимо этого программа отображает регистрационные доменные данные, полученные от службы WhoIs. Встроенная утилита eMailTracker отслеживает путь прохождения e-mail сообщений до провайдера почтовой службы.

Условия распространения: trialware
Язык интерфейса: английский
Сайт производителя: www.visualware.com

War FTP Daemon 1.82



Развиваемая с 1996 года и по сей день, эта программа по праву является одним из наиболее популярных FTP-серверов. Она обладает очень высокой скоростью работы и мало загружает систему. Основная утилита, которой пользуется администратор для обслуживания сервера, — это War Daemon Manager. В ее главном окне предоставлена информация об активных подключениях, запущенных серверах, пользователях и файлах, выложенных на FTP. Кроме того, есть удобный User Manager. Он позволяет администратору редактировать свойства и права доступа пользователей. Программу довольно легко установить и настроить. Ваш FTP в простейшей конфигурации будет работать уже через пять минут после инсталляции. Если необходимо решить более сложную задачу, то для искушенных пользователей War FTP предоставляет огромное количество настроек по авторизации, журналированию и повышению производительности сервера.

Условия распространения: freeware
Язык интерфейса: английский
Сайт производителя: www.jgaa.com

Администрирование:

ServersCheck SE, Remote Desktop Connection, Resource Kit Tools, Servers Alive 4.0.1376, VisualRoute 8.0a, Web Application Stress 1.1, Angry IP scanner 2.20, CommTraffic 2.02, Application Compatibility Toolkit 3.0, Administration Tools Pack v. 3790, IP Tools 2.20, Aida32

Безопасность:

ZoneAlarm Pro 4.5, Norton Internet Security 2004, Tiny Personal Firewall 5.0, Armor2net Personal Firewall 3.12, 602Pro LAN Suite 2003, Kerio WinRoute Firewall 5, Eset NOD32, F-Secure Anti-Virus 5.41, F-Secure Policy Manager, F-Prot Antivirus 3.14, TrendMicro Server Protect 5.5, Access Manager 1.3, Digital Identity 1.0.18, Zero Footprint Crypt 3.0,

Сервисы:

Software Update Services, War FTP Daemon 1.82, MySQL 4.0.17 for Win32, Encrypted FTP 3.1.4.84, Apache 2.0.48, Xitami 2.4d10, Copernic 2.01

Мессенджеры:

Friendly Chat 4.5.6, mIRC 6.12, ICQ Pro 2003b, Bersirc 1.40, Intranet Chat 1.20, Miranda 0.3.2

Бонус:

Win 2003 Optimize Tool 1.44, Tune Up Utilities 2003, Your Uninstaller! 2003, Tweak UI, Acronis PartitionExpert 2003, Style XP, MyIE2 0.9.12, Opera 7.23, Avant Browser 8.02, AceFTP 3.01.0, WinHT Track Website Copier 3.30, Java Runtime Enviroment 1.4.2, IZArc 3.4.1.5, ZipGenius 5, PicoZip 2.8, MakePDF for Word 5.0, Visio Viewer 2003, Advanced Effect Maker Freeware Edition 1.0, Hexplorer 2.17, IsoBuster 1.5, Asterisk Key, Winamp 5.01, Blaze Media Pro 5.0

Обновления:

Набор обновлений, DirectX 9.0b, MSXML 4.0

Драйверы:

NVIDIA, ATI, Iomega

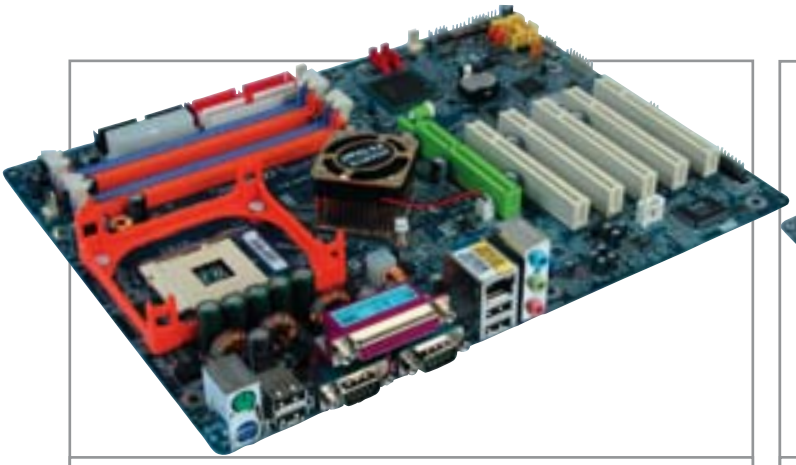
Организация локальной сети

Соединяй и властвуй

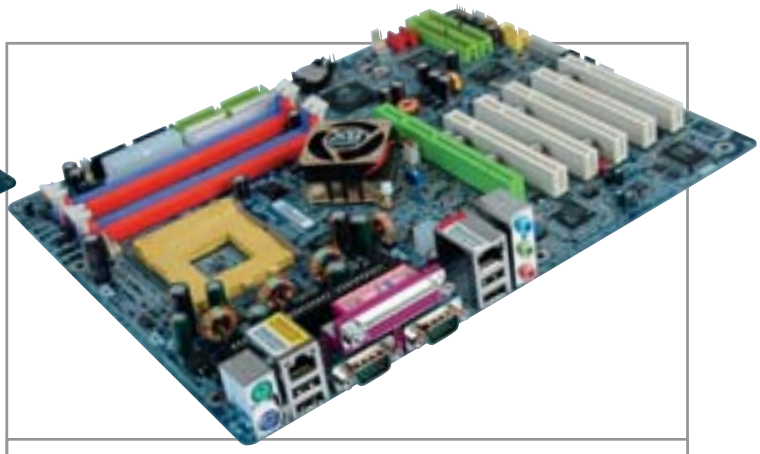
Сейчас, в век информации, становятся все более актуальными проблемы, связанные с желанием простых пользователей иметь доступ к различным сетевым информационным ресурсам. Все в большем количестве районов Москвы (и не только) появляются локальные сети, объединяющие дома и целые улицы.

Что нужно сделать, если возникла необходимость построить в офисе или подъезде локальную сеть, запустить веб-сервер? Если вам надо предоставить в общее пользование большое количество файлов, принтеров, обеспечить надлежащую защиту как от вторжения извне, так и от некорректных действий пользователей, и многое другое? Решение большинства этих задач ложится на плечи серверных ОС, различных вариантов которых сейчас существует достаточно много. Но сегодня мы будем говорить о Microsoft Windows Server 2003. Попробуем разобраться в том, что нужно для работы этой системы, и определим оправданность ее использования в различных ситуациях.

В качестве серверной ОС Windows Server 2003 выбрана нами по нескольким причинам. Во-первых, это самая свежая и совре- »



Для сервера начального уровня подойдет плата, построенная с использованием чипсета Intel 865PE



Если сервер оснащен процессором AMD, стоит обратить внимание на платы с чипсетом NVidia nForce 2

менная ОС, что уже само по себе вызывает к ней повышенный интерес. Во-вторых, основной ее конкурент Linux сложнее в настройке и использовании, что совсем не говорит о большей надежности и производительности таких систем. В качестве примера можно привести следующие данные — результаты независимого сравнительного тестирования Windows NT 4.0, Red Hat Enterprise Linux ES 2.1 и WS 2003 показали преимущество последней в производительности на 50-100%. Впечатляющий результат. Не менее красиво выглядит пример и с Лондонской биржей, где под управлением w2k3 работают тысячи терминалов и при этом запаздывание отображения информации на каждом из них не превышает одной секунды.

История развития

Семейство Windows Server 2003 — это дальнейшее развитие платформы Windows Server 2000. Но, впервые посмотрев на интерфейс новой системы, невольно ловишь себя на том, что где-то это уже видел. И действительно, почти полное сходство с Windows XP (особенно если в XP отключить стили отображения). Конечно, не стоит забывать о том, что в серверной ОС присутствует большое количество специализированных служб, и о том, что после выхода Windows XP регулярно выпускались различные исправления к этой системе (таким образом, только что установленная w2k3 надежнее и устойчивей, чем такая же XP, в идеале, конечно). Разработчики попытались скрестить удобство и надежность Windows XP с весьма успешной, но «тяжелой» серверной платформой w2k. Надо сказать, что это почти получилось, и человеку, имеющему опыт работы с w2k (а лучше с XP), будет довольно легко освоиться с новой ОС. Хотя, конечно, есть некоторые отличия и новые технологии.

Windows Server 2003 выпускается в четырех версиях, которые построены с использованием одного центрального ядра, но предназначены для выполнения различных задач. Подробное описание каждой из них можно найти в следующей статье.

Мы же в качестве примера будем рассматривать версию Standard Edition как наиболее удобную и рациональную в случае управления небольшими сетями.

Выбор конфигурации

По данным самой Microsoft, для запуска системы (минимально необходимая конфигурация) на базе Server 2003 достаточно Pentium (или аналогичный процессор от AMD) 133 МГц и 128 Мбайт оперативной памяти. Конечно, это больше похоже на теорию, так как на практике вы, может, и запустите систему на таком аппаратном обеспечении, но добиться от нее чего-либо толкового не удастся. Более правдоподобно выглядят рекомендуемые характеристики: Pentium 550 МГц и 256 Мбайт ОЗУ. Приведенные данные справедливы для Standard и Web Edition и платформ на базе x86-совместимых процессоров. Для всех версий потребуется от 1,5 до 2 Гбайт дискового пространства. Стоит помнить, что в большинстве случаев для нормальной работы необходимо «умножить» рекомендуемые требования на два. Таким образом, для запуска и полноценной работы среднестатистического сервера w2k3 необходим компьютер на базе процессора Pentium от 1 ГГц с 512 Мбайт памяти и от 4 Гбайт дискового пространства. Это не так уж много на сегодняшний день и не сильно отличается от требований, предъявляемых Windows 2000 Server.

Перед тем как начать установку новой системы, следует убедиться в том, что аппаратная часть компьютера совместима с новой ОС. Узнать о совместимости с Windows Server 2003 различных устройств можно из Hardware Compatibility List (HCL), который расположен на сайте Microsoft.

В качестве примера можно привести конфигурацию компьютера для использования в качестве контроллера домена, файл-сервера и сервера печати (так же можно запустить на нем шлюз доступа в Интернет). Помня о правиле «умножить на два», будьте готовы к тому, что вам понадобится 512 и более Мбайт оперативной памяти. Точный ее объем зависит от конкретных задач и количества пользователей в сети. Например, на сеть, которая состоит из 25 машин, где сервер используется как контроллер домена, шлюз и файл-сервер (возможно и как сервер печати), 512 Мбайт будет вполне достаточно. Если вы предполагаете использовать сервер терминалов, то памяти понадобится больше. Объем жесткого диска не так важен — все зависит от количества информации, которую вы будете хранить на сервере.

Особое внимание стоит уделить выбору материнской платы и корпуса. При выборе корпуса следует обратить внимание на качество системы охлаждения и надежность блока питания, так как сервер, в отличие от рабочей станции, практически никогда не выключается и работает гораздо большее количество времени. Стоит обратить внимание на продукцию ASUS или ThermalTake. Более дешевые, но надежные корпуса делает компания Inwin. Часто на материнских платах присутствуют встроенный сетевой контроллер и Serial ATA или просто IDE RAID-контроллер и сетевой адаптер. Этим можно выгодно вос-

Так выглядит высокопроизводительный корпоративный сервер для больших локальных сетей

Коммуникационный шкаф крупной сети всегда опутан огромным количеством проводов

пользоваться. Использование RAID-массива в случае с сервером более чем оправдано. Как уже говорилось, сервер работает больше, чем все остальные компьютеры в сети, и нагрузка на дисковую подсистему достаточно велика, что увеличивает вероятность выхода жестких дисков из строя. И как следствие этого — остановка сервера, а возможно, и потеря данных. RAID-массив и существует для того, чтобы избегать подобных неприятностей; самый простой вариант его использования — так называемое зеркалирование. Этот режим работы представляет собой систему из нескольких жестких дисков, информация на которых дублируется. И в случае поломки одного из HDD, входящего в такой массив, всю необходимую информацию можно прочитать с другого. Есть еще одна хитрость, связанная с жесткими дисками. Рекомендуется использовать для установки системы и ПО один диск или раздел, а для хранения данных другой. Так вы убережете себя от проблем, связанных с переустановкой системы, или в случае серьезных неполадок в ее работе, когда возникает вопрос: «А куда же быстро сохранить такой объем информации?»

Так как сервер практически никогда не выключается, следует особое внимание уделить блоку питания

Однако, как показывает практика, интегрированные на материнскую плату RAID-контроллеры чаще всего работают неустойчиво. Именно поэтому можно порекомендовать использовать на сервере дополнительные RAID-контроллеры (как правило, PCI-платы). Среди них хорошо подойдут для сервера начального уровня модели, построенные на базе чипов Promise PDC 20376 и HighPoint HPT374.

А что же материнские платы? Для создания неплохого сервера начального уровня практически идеально подойдут материнские платы, построенные на базе чипсетов Intel 875P или 865PE. Не стоит использовать более дорогие серверные платы в домашних условиях. Это не оправдает затраченных денег. Но в том случае, если ваша сеть нуждается в сервере высокого уровня, лучше всего присмотреться к платам на чипсетах Intel E7501 и Intel E7505.

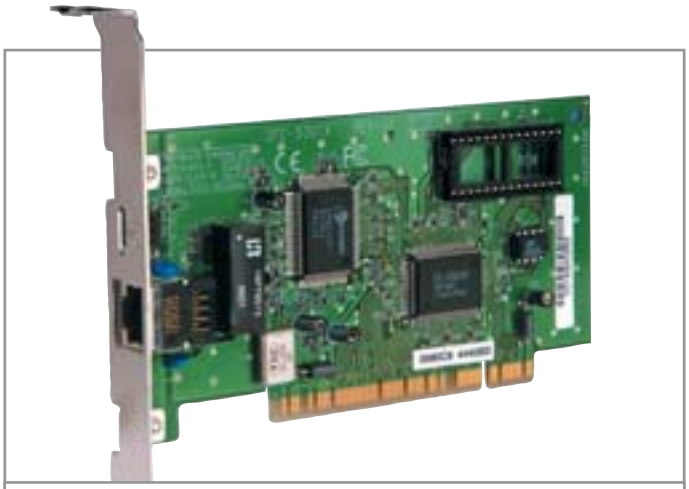
О продукции компании AMD тоже нельзя сказать ничего плохого. Windows Server 2003 будет прекрасно работать на этой платформе. В качестве материнских плат для процессоров AMD имеет смысл использовать построенные на базе чипсета NVidia nForce 2. Речь, естественно, идет о 32-разрядных процессорах. Хотя сейчас доступны и решения на базе 64-битных Athlon 64 и Opteron. При использовании 64-разрядных процессоров понадобится плата на чипсете NVidia nForce 3.

Есть еще один важный компонент будущего системного блока — память. Очень часто нестабильная работа системы вызвана именно некачественной памятью. При покупке комплектующих необходимо обращать особое внимание на их качество. Помните, что для сервера главное — надежность и стабильность в работе, поэтому выбирайте продукцию от известных и проверенных производителей.

С другой стороны, в бизнес-системах, офисах и везде, где требования к стабильности и надежности более высоки, нежели в домашних условиях, вполне логично будет приобрести готовый сервер от известного производителя. Дело в том, что такие компьютеры изначально ориентированы на подобные задачи. С большой вероятностью можно сказать, что они будут работать долго и надежно. К тому же вы получаете полноценную техническую поддержку от производителя, что приятно. Самому собрать сервер из комплектующих, описанных выше, тоже можно, но оправдано только в том случае, если вы хорошо знаете, чего хотите, и не можете найти подходящую готовую конфигурацию. При этом стоит осознавать, что стоимость такой системы не будет сильно отличаться от готовой, а протестировать и подобрать все аппаратные составляющие так, как это делают крупные производители, будет достаточно сложно.

Сетевое оборудование

Попробуем схематично представить себе процесс установки небольшой локальной сети под управлением сервера на базе Windows Server 2003 с выходом в Интернет в условиях подъезда. Предположим, что в подъезде имеется пять компьютеров. А так же договоримся, что будем строить сеть на базе проводной технологии Ethernet по классической схеме «звезда». Вам понадобятся сетевые карты, сетевой коммутатор (switch) или концентратор (hub), определенное количество кабеля типа витой пары (лучше пятой категории) и коннекторы RJ-45. На один из компьютеров, который выполняет роль сервера и под-



Сетевые карты DFE-530TX производства компании D-Link, можно использовать в сетях любого размера и типа

Для увеличения количества портов можно использовать хабы. Например, 8-портовый хаб D-Link DES-1008D

» ключен к Интернету, нужно установить ОС Windows Server 2003. На нем должны присутствовать две сетевых карты, одна из которых будет обращена к локальной сети, а другая к провайдеру, предоставляющему доступ в Интернет. Естественно, что в зависимости от типа подключения к нему вместо сетевой карты может быть использовано другое сетевое устройство (xDSL, обыкновенный модем и проч.). Если же сервер не будет являться роутером, то есть нет необходимости в предоставлении доступа как самому серверу, так и его клиентам в Интернет, то второй сетевой интерфейс не понадобится вообще.

Из имеющихся в продаже сетевых карт можно выбрать любые от таких производителей, как D-Link или 3Com. Например, DFE-530TX от D-Link — €10 или серия 3Com 90x по цене от €12 до 25. Последние несколько дороже, но обладают большим количеством поддерживаемых технологий. В качестве коммутатора или концентратора можно использовать любые подходящие по количеству портов и скорости связи от тех же производителей. Если вам нужно большее количество портов, чем может предоставить одно устройство, вы можете соединить несколько свичей или хабов вместе. В последнем случае скорость передачи данных будет сильно падать при росте количества хабов. Стоит обратить внимание на такие марки, как Surecom и Compex, для небольших сетей это очень неплохое решение за скромные деньги. Например, простой неуправляемый свич на 24 порта от компании Surecom (EP-824DX) вы сможете купить меньше чем за €90. А этого уже хватит на небольшой офис. Если количество компьютеров в офисе больше 24, можно использовать хабы для отдельных групп пользователей. Подойдут и небольшие свичи от той же Surecom — EP-808SX 10/100 Мбит, восемь портов, стоимостью около €20.

Свич Surecom EP-808SX 10/100 Мбит

Выбор между коммутатором и концентратором зависит от ваших финансовых возможностей и желания получить определенный результат. Задача хаба — принять пакет и размножить его по всем портам, далее рабочие станции сами разберутся, кому и что предназначалось. Свич работает по-другому. Он принимает пакет и направляет его в тот порт, к которому подключен получатель. Таким образом, при использовании свича, вы получите большую пропускную способность и меньшую загруженность сети, чем в случае с хабом, а так же сможете с меньшими потерями проводить расширение вашей сети. Но и обойдется это немного дороже.

Как видно из приведенного примера, создать небольшую LAN с выходом в Интернет не так сложно. А учитывая возможности и простоту настройки w2k3, задача становится еще более простой.

Виды клиентов

Но сеть — это не только сервер, провода и другое пассивное или активное оборудование. В ней так же присутствуют рабочие станции. Идеальным клиентом для Windows Server 2003 является Windows XP. Но не исключена возможность использования этой системы и в смешанных гетерогенных сетях, где есть компьютеры с разными ОС. С этим сервером могут работать Macintosh, Linux и более старые версии самой Windows. Для работы с Macintosh в систему встроена поддержка протокола Apple Talk. А в том случае, если среди клиентов w2k3 присутствуют такие, которые работают на ОС Linux, необходимо развернуть на них систему SAMBA, которая позволит взаимодействовать между собой двум этим ОС. Используя же в качестве клиентов Windows 9x или Windows Millennium, вы лишитесь полноценной поддержки доменов. При использовании сервера терминалов, в качестве рабочих станций можно выбрать тонкие клиенты или маломощные компьютеры с установленной Windows 98. В последнем варианте на клиентскую машину необходимо установить клиент сервера терминалов, загрузочные дискеты которого можно сделать на сервере. Часто для работы тонких клиентов на сервер нужно установить фирменное ПО, обеспечивающее поддержку терминального режима. Все зависит от ваших целей, имеющегося оборудования и средств. Иначе говоря, Windows Server 2003 является вполне универсальной серверной ОС.

Заключение

В общем, новая разработка Microsoft получилась весьма и весьма удачной. В результате скрещивания пользовательской Windows XP и серверной w2k появилась удобная в использовании и надежная система. Windows Server 2003 достаточно проста в освоении, в чем сильно помогает ее дружественный и интуитивно понятный интерфейс.

■ ■ ■ Алексей Агеев

Новая серверная ОС

Флагман от Microsoft

В апреле 2003 года фирма Microsoft выпустила новую версию серверной операционной системы — Windows Server 2003. После выхода в свет Windows XP, которая являлась системой для рабочих станций, появление новой серверной ОС, конечно же, ожидалось.

Новое — это хорошо переделанное старое!

Судя по всему в разработку Windows Server 2003 Microsoft вложила колоссальные деньги и еще более колоссальные усилия. По первым впечатлениям продукт получился действительно выдающийся. Понятно и желание Microsoft всеми силами продвигать его на рынок. После выхода новой операционной системы, получившей название Windows Server 2003, в Москве почти любой желающий бесплатно мог получить ознакомительную версию этого программного продукта со сроком действия 180 или 360 дней. Более того, в некоторых интернет-магазинах ознакомительная версия Windows Server 2003 продавалась и продается всего за 1 доллар! Распространялся ли хоть один продукт от Microsoft подобным образом? Естественно, столь активно продвигаемая система не могла не привлечь нашего внимания. Поэтому нам хотелось бы поговорить о том, что же представляет собой этот флагманский (по выражению Ольги Дергуновой, главы представительства фирмы Microsoft в России) продукт.

Данная ОС является не новой разработкой, а результатом развития предыдущих серверных операционных систем. Это следует из того, что в пресс-релизах и документах Microsoft используются слова «enhanced» и «improved», а отнюдь не «new». В некоторых своих документах Microsoft откровенно заявляет, что Windows Advanced Server, Limited Edition являлся одной из «пристрелочных» версий Windows Server 2003.

И это хорошо потому, что любая новая, написанная с нуля программа всегда изобилует различного рода ошибками, недодел- »

» ками, несоответствиями. В данном случае мы получили продукт, уже прошедший проверку боем и не кишащий ошибками.

Windows Server 2003 явилась первой операционной системой, составной частью которой является платформа .NET Framework. До этого при желании поработать в .NET ее приходилось устанавливать либо как отдельный продукт, либо как часть другого продукта, например Visual Studio .NET. К чему это приводило? Любой программист, написавший рассчитанную на работу в .NET программу, должен был с ней распространять и .NET Framework. Теперь о том, что вместе с программой надо поставлять еще и платформу, можно забыть.

Нельзя не заметить и поразительную нетребовательность систем семейства Windows Server 2003 к ресурсам, что хорошо видно из табл. 1.

Что нового подарит нам Microsoft?

Итак, какие же новшества были привнесены в Windows Server 2003 по сравнению с Windows 2000 и какие возможности были улучшены?

Системные приложения

.NET Framework

Эта платформа полностью меняет представления о выполнении программ в Windows. Теперь каждая программа, созданная для работы в .NET, является управляемой, то есть ответственность за ее правильное и безопасное исполнение несет непосредственно платформа, а точнее, одна из ее составных частей CLR (Common Language Runtime, общая языковая среда исполнения).

Компилятор преобразует программу в так называемое промежуточное представление (IL — Intermediate Language, промежуточный язык). CLR в некотором смысле является интерпретатором этого языка. Перед запуском программного кода Common Language Runtime проверяет, может ли данный код выполняться без ошибок, подходят ли текущие разрешения безопасности для того, чтобы выполнять этот код, и не производит ли он каких-либо запрещенных действий.

Интересно, что любая управляемая программа может содержать в себя цифровую подпись разработчика. Естественно, если подписанная программа будет каким-то образом изменена, то исполняющая среда не »

Версии Windows Server 2003

Не один, а целое семейство

Операционная система Windows Server 2003 представляет собой не один продукт, а целое семейство таковых. Назначение каждого из них очевидно и соответствует названию.

▸ **Windows Server 2003 Web Edition** предназначена для построения и хостинга веб-приложений, веб-страниц и веб-сервисов. Она является самой дешевой и будет интересна в первую очередь сервис-провайдерам и разработчикам интернет-приложений. Версия вобрала в себя все лучшее, что есть в Internet Information Services 6.0, Microsoft ASP .NET и Microsoft .NET Framework. Потолком для Web Edition является 2-процессорный сервер с 2 Гбайт оперативной памяти. Хотя компьютеры под управлением Windows Server 2003 Web Edition могут быть членами домена Active Directory, в данной системе нельзя запускать этот сервис. Следовательно, Windows Server 2003 Web Edition не может использоваться для выполнения функций управления, таких как групповая политика, политики ограничения запуска программ, службы удаленной установки, службы Microsoft Metadirectory Services (MMS), служба Internet Authentication Service (IAS) и т. д.

▸ **Windows Server 2003 Standard Edition** предназначена для работы в небольших организациях и обеспечивает подключение к Интернету и доступ каждого сотрудника к файлам и принтерам. Сервер содержит все необходимые средства для организации взаимодействия сотрудников. Он обеспечивает высокий уровень надежности, безопасности, позволяет при необходимости наращивать ресурсы сети. Standard Edition может работать на 4-процессорном сервере с 4 Гбайт оперативной памяти. Возможно, выбор именно этой версии станет оптимальным для большинства российских сетей.

▸ **Windows Server 2003 Enterprise Edition** разрабатывалась с прицелом на использование в сфере среднего и крупного бизнеса. Эта версия выпущена как в 32-разрядном, так и в 64-разрядном варианте. Она может работать на 8-процессорном сервере и поддерживает адресацию до 32 Гбайт оперативной памяти, а также 8-узловую кластеризацию. К стандартному варианту в версии Enterprise добавлены несколько новых возможностей. К ним относятся, например, поддержка MMS и NUMA, а также реализация функции Hot Add Memory, которая позволяет добавлять в сервер модули памяти без остановки и даже без перезагрузки последнего (в настоящее время эта функция может быть использована только в серверах с аппаратной поддержкой добавления памяти во время работы).

▸ **Windows Server 2003 Datacenter Edition** предназначена для работы с крупными базами данных. Она работает на машинах минимум с восемью процессорами и поддерживает до 32 процессоров, а также допускает восьмиузловую кластеризацию. При использовании обычных процессоров x86 она обеспечивает адресацию до 64 Гбайт памяти. На 64-разрядных платформах предел поддерживаемой памяти составляет 16 Тбайт.

Табл. 1. Требования к системам, на базе которых будут работать ОС семейства Windows Server 2003

	Web-edition	Standard Edition	Enterprise Edition	Datacenter Edition
Минимальная частота процессора, МГц	133	133	133 (733 для Itanium)	400 (733 для Itanium)
Рекомендованная частота процессора, МГц	550	550	733	733
Минимальный размер RAM, Мбайт	128	128	128	512
Рекомендованный размер RAM, Мбайт	256	256	256	1024
Необходимое дисковое пространство, Гбайт	1,5	1,5	1,5 (2 для Itanium)	1,5 (2 для Itanium)

» позволит ее запустить. Это значительно затрудняет возможность для вирусописателя или злоумышленника каким-то образом внедрить в исполняемый файл свой код. Тем самым увеличивается и безопасность системы.

Неоднородный доступ к памяти

С увеличением тактовой частоты процессоров, приводящим к росту нагрузки на архитектуру процессорной шины, проблемы масштабируемости решаются путем реализации нескольких процессорных шин. Это приводит к созданию архитектуры, состоящей из процессоров и ячеек памяти, организованных в более компактные подсистемы, называемые узлами. Скорость доступа процессора к памяти в других узлах ниже, чем в том же узле. В результате создается эффект неоднородного доступа к памяти (Non-Uniform Memory Access, NUMA) в масштабах системы.

Низкие скорости доступа к отдельным узлам могут привести к падению быстродействия приложений. ОС пытается ограничить снижение быстродействия за счет назначения всех потоков процесса процессорам одного узла и выделения памяти по запросу в пределах того же узла, где находится этот процессор. Кроме того, в поставку включен программный интерфейс (API), который позволяет приложениям получать сведения об архитектуре NUMA.

Режимы совместимости

Новый режим обеспечивает совместимость со многими распространенными приложениями без необходимости дополнительной настройки. Режим совместимости позволяет использовать среду, соответствующую по поведению Windows 95, Windows 98, Windows NT 4.0 или Windows 2000. Эти режимы устраняют некоторые из наиболее распространенных проблем, мешающих нормальной работе старых приложений. Если после переноса в работе приложения возникли проблемы, можно воспользоваться одним из режимов совместимости — в большинстве случаев проблемы исчезнут.

Сетевые возможности

Автонастройка для подключения к нескольким сетям

Данная возможность упрощает доступ к сетевым устройствам и Интернету. Она также позволяет пользователям мобильных компьютеров осуществлять доступ к офисной и домашней сети, не настраивая параметры TCP/IP вручную. Автонастройка обеспечивает применение альтернативной конфигурации TCP/IP, если сервер DHCP (Dynamic Host Configuration Protocol) не найден. Альтернативная конфигурация помогает в ситуациях, когда компьютер используется для работы в нескольких сетях, причем в одной их этих сетей сервер DHCP отсутствует, а автоматическое назначение частных IP-адресов нежелательно.

Передача голоса по протоколу IP

Получение удаленной помощи (Remote Assistance) по Интернету стало лучше благодаря подключению к Windows Messenger возможности передачи голоса по протоколу IP.

Поддержка ATM

Асинхронный режим передачи (Asynchronous Transfer Mode, ATM) — это высокоскоростной протокол, предназначенный для одновременной передачи по сети различных типов данных, таких как голос, изображение, видео и т. д.

Говоря более научным языком, это широкополосный метод ретрансляции ячеек, при котором данные передаются ячейками фиксированной длины (по 53 байта). Ячейки содержат 48 байтов: собственно передаваемые данные и 5 дополнительных байтов — заголовок ATM. Например, передавая 1000-байтный пакет, ATM разобьет его на 21 кадр и поместит каждый кадр в ячейку. В результате будет производиться передача стандартных, единообразных пакетов.

Сетевое оборудование может коммутировать, маршрутизировать и перемещать пакеты фиксированного размера быстрее, чем пакеты произвольной длинны. А ячейки стандартного размера позволяют более эффективно использовать буферы и сокращают время на свою обработку. Одинаковый размер ячеек, кроме того, позволяет упростить планирование необходимой полосы пропускания.

Теоретически пропускная способность ATM может достичь 1,2 Гбит в секунду. Однако в настоящее время скорость ATM ограничивается скоростью оптоволоконного кабеля, которая не превышает 622 Мбит/с.

Поддержка служб метакаталогов (Microsoft Metadirectory Services, MMS)

Общий смысл службы метакаталога состоит в построении БД, являющейся хранилищем информации об объектах любых служб каталогов, будь то Active Directory, Lotus Notes, Netscape iPlanet и т. д. MMS хранит и интегрирует информацию из множества каталогов в единую службу каталога для всей организации. Встроенные в MMS агенты управления выполняют функции посредника между службой какого-либо каталога и базой интегрированных метаданных. На первом этапе работы они обеспечивают импорт и преобразование информации для размещения их в метакаталоге, а после модификации — экспорт этих преобразованных данных обратно, в соответствующие службы каталогов.

Вся информация о ресурсах сети хранится в БД метакаталога в виде объектов, как и в службах каталогов. Каждый из объектов характеризуется набором свойств (атрибутов). Сами данные хранятся в виде конкретных значений этих атрибутов.

Подключение по протоколу PPPoE

Посредством протокола PPPoE (Point-to-Point Protocol over Ethernet) пользователи Ethernet-сети могут устанавливать соединение с Интернетом через широкополосную линию, такую как DSL, беспроводное устройство или кабельный модем. С помощью PPPoE пользователи локальной сети могут получать доступ к высокоскоростным сетям данных. Объединяя Ethernet и протокол PPP (Point-to-Point Protocol), протокол PPPoE обеспечивает эффективный способ созда- »

Улучшения в области надежности, сделанные в Windows Server 2003

» ния отдельных соединений с удаленным сервером для каждого пользователя. В Windows Server 2003 включен драйвер этого протокола.

Поддержка протокола IPv6

IPv6 — это набор стандартных протоколов сетевого уровня следующего поколения. IPv6 устраняет многие проблемы, которые присутствуют в текущей версии IP (IPv4) для ОС семейства Windows, в том числе проблемы, касающиеся нехватки адресов, безопасности, автонастройки, расширяемости и т. д.

Безопасность

Firewall (брандмауэр)

Брандмауэр подключения к Сети (Internet Connection Firewall, ICF) обеспечивает безопасную работу в Интернете и предназначен для использования в домашних условиях и на небольших предприятиях. Эта возможность доступна для применения в локальных сетях, при удаленном доступе к сети, в виртуальных частных сетях и при подключениях по протоколу PPPoE. Брандмауэр также предотвращает сканирование портов и ресурсов из внешних источников.

Поддержка протокола IPSec

IP Security — это комплект протоколов, касающихся вопросов шифрования, аутентификации и обеспечения защиты при транспортировке IP-пакетов; в его состав сейчас входят почти 20 предложений по стандартам и 18 RFC. Он позволяет обеспечивать защиту интрасетей, а также создавать безопасные решения на базе виртуальной частной сети для связи через Интернет. Технология IPSec была разработана группой IETF (Internet Engineering Task Force) и является стандартом шифрования трафика TCP/IP.

Наверное, это далеко не полный перечень того, что было добавлено в новую серверную операционную систему. Но даже такой список позволяет сказать, что внесенные изменения нельзя недооценивать.

Главное — надежность и безопасность

При знакомстве с технической документацией Windows Server 2003 в глаза бросаются две детали. Во-первых, Microsoft везде подчеркивает повышение надежности нового сервера. По заявлениям руководителей Microsoft, каждая строчка кода была просмотрена и все программы были неоднократно проверены на наличие ошибок.

Во-вторых, в выступлениях официальных лиц компании красной нитью проходит мысль о том, что безопасность нового сервера была увеличена. Например, Билл Вегте, вице-президент подразделения Windows Server Division корпорации Microsoft, заявил следующее: «При разработке Windows Server 2003 мы ставили во главу угла повышение безопасности системы. Безопасность является одной из главных забот пользователей, и новые функции, реализованные в этой версии, значительно облегчают создание защищенных систем. Windows Server 2003 представляет собой надежную безопасную платформу».

На конференции «Определяя будущее», организованной московским представительством фирмы Microsoft, прозвучало сообщение, что для проверки надежности и безопасности сервера Microsoft наняла несколько фирм, специализирующихся на тестировании устойчивости безопасности компьютерных систем. Все потенциально небезопасные алгоритмы были проанализированы и переработаны.

Более того, во время разработки Windows Server 2003 в соответствии с распоряжением Билла Гейтса обязательным чтением для сотрудников Microsoft стала книга Майкла Ховарда и Дэвида Лебланка «Защищенный код». Эти факты только подтверждают, что безопасности и надежности нового сервера во время разработки был отдан наивысший приоритет.

При разговоре о безопасности нового сервера нельзя не заметить, что после его инсталляции все работает по минимуму. Чтобы запустить тот или иной сервис, пользователю придется осознать, нужен ли ему этот сервис, и понять, каким образом он может быть запущен. Любой видимый из Интернета сервис представляет собой потенциальную брешь в защите. Зачем эти лазейки открывать заранее?

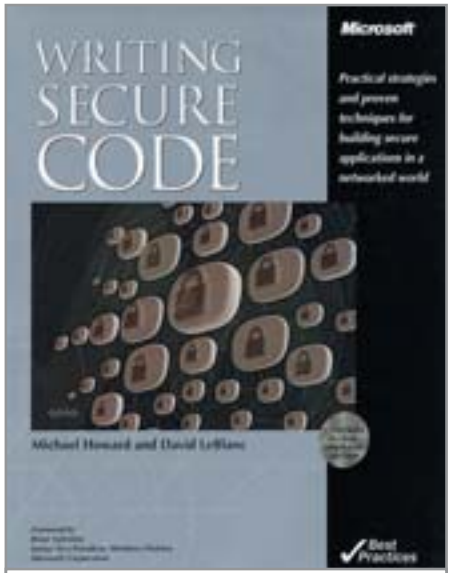
Билл Вегте, вице-президент подразделения Windows Server Division корпорации Microsoft

Итоги и выводы

Главный вывод из всего сказанного в том, что администратор любой сети, переходя на Windows Server 2003, получает ряд преимуществ. В их числе — повышенные надежность и безопасность сервера.

Кроме того, идеология нового сервера подразумевает высокую квалификацию администратора. Система, обеспечивающая профессиональный рост администраторов, является гарантией высокого уровня знаний. А что в наше время ценится дороже?

■ ■ ■ Павел Румянцев



Книга Майкла Ховарда и Дэвида Лебланка «Защищенный код»

Начало пути

Путеводитель

Для того чтобы работать с Windows Server 2003, его, разумеется, необходимо инсталлировать на свой компьютер. Естественно, нужен путеводитель, который расскажет нам об этапах установки новой операционной системы.

Windows Server 2003 можно инсталлировать с нуля, а можно сделать обновление той системы, которая уже установлена на компьютере. К сожалению, список операционных систем, обновление которых допускается, ограничен Windows NT Server 4.0 SP5 (включая Terminal Server Edition и Enterprise Edition) и Windows 2000 Server (включая Advanced Server). При обновлении с указанных систем обеспечивается перенос базы данных имен и паролей пользователей в устанавливаемую систему.

Мы рассмотрим установку с нуля. Инсталляция в качестве второй системы или поверх предыдущей отличается от нее только некоторыми мелочами, которые очевидны и не требуют подробного описания.

Первые шаги

Включите в BIOS загрузку с CD, вставьте компакт-диск с записанной на нем версией Windows Server 2003 и сядьте поудобнее. Ждать придется долго, процесс инсталляции будет длиться порядка сорока минут.

Если у вас в компьютере есть оборудование, требующее специальных драйверов, то в самом начале установки необходимо нажать F6, после чего система запросит диск с драйверами и загрузит их. А теперь давайте пройдем весь путь инсталляции по шагам.

Текстовый этап

Шаг 1. На данном этапе на диске ничего нет, минимально работающая система загружена с компакт-диска.

Сначала система запросит, принимаете ли вы лицензионное соглашение Microsoft. Если вы не примете его, то тогда установить новый сервер не удастся. Поэтому нажмите F8, иначе на этом установка системы будет прервана практически не начавшись.

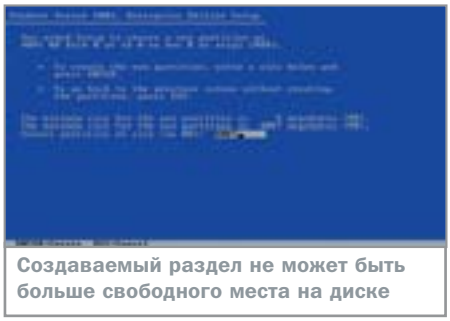
Другого выхода, кроме как нажать клавишу F8, у вас просто нет

Шаг 2. На этом шаге будут создаваться и при необходимости уничтожаться разделы жесткого диска. Поэтому нужно быть крайне внимательным — здесь выбор элемента «Удаление раздела» приводит к немедленному удалению. Никаких «Undo» на этом шаге нет, то есть вернуть удаленное не удастся.

Нужно создать как минимум один раздел на винчестере, нажав клавишу C (Create Partition, «Создать раздел»)

Шаг 3. Необходимо указать размер этого раздела. Мы рекомендуем разбить диск минимум на два раздела в целях повышения надежности.

Шаг 4. На этом шаге система задаст вопрос о том, какая файловая система будет размещена на разделе. Есть четыре варианта форматирования — FAT (Quick format), NTFS (Quick format), FAT и NTFS. Мы рекомендуем следует выбирать NTFS как наиболее надежную файловую систему.



Создаваемый раздел не может быть больше свободного места на диске

Быстрое форматирование создает таблицу разделов, не размечая весь диск и не проверяя его на плохие сектора. Если вы недавно проверяли винчестер на наличие плохих секторов или уверены в его исправности, смело выбирайте быстрое форматирование.

Оптимальный выбор способа форматирования — быстрое форматирование

Система отформатирует диск, скопирует файлы с компакт-диска на винчестер, произведет некоторые подготовительные действия и перезагрузит компьютер.

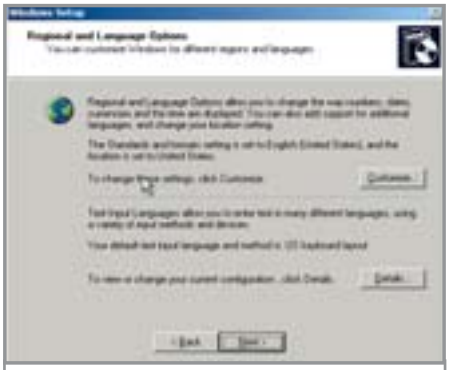
Программа установки начала форматирование раздела жесткого диска

После перезагрузки начнется второй, графический этап. Во время перезагрузки убедитесь, что система загружается именно с жесткого диска, это будет свидетельствовать о том, что вы все делаете правильно, а пер-вый этап программы установки отработал корректно. »

по инсталляции: 60+

Графический этап

Шаг 5. Итак, начался второй этап установки. Через несколько секунд на экране будет отображено диалоговое окно, в котором вы должны указать системе региональные и языковые параметры, в соответствии с которыми она будет формировать сообщения и отвечать на запросы. Нажав в этом окне кнопку «Customize», мы перейдем к следующему шагу.

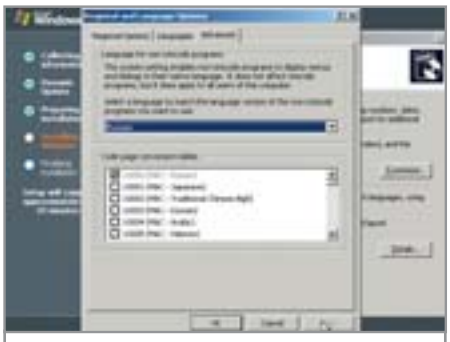


Приглашения для ввода региональных установок и языковых параметров

Шаг 6. В зависимости от выбранной вами страны меняется формат вывода национальной валюты, чисел, времени и даты.

Региональные установки и языковые параметры определяют «формат» общения пользователя с компьютером

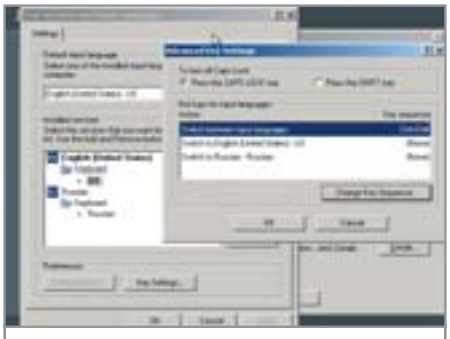
Вкладка «Languages» позволяет установить поддержку азиатских языков. На вкладке «Advanced» выбираем параметры вывода сообщений для программ, не использующих Unicode. Здесь мы рекомендуем выбрать русский язык, иначе большинство сообщений вы просто-напросто не сможете прочесть.



Нужно указать, чтобы «не-Unicode»-программы использовали русский язык

Вернемся к окну, отображенному в шаге 5, и выберем не «Customize», а «Default». После этого мы перейдем к шагу 7.

Шаг 7. Здесь вы сможете указать компьютеру, на каких языках с ним можно будет общаться.



Определение раскладки клавиатуры и сочетания клавиш смены языка

Сказанное выше комментариев не требует, достаточно просто взглянуть на картинку. Теперь нужно опять вернуться к окну, упомянутому в шаге 5, и нажать в нем кнопку «Next».

Шаг 8. Нужно указать имя владельца компьютера и название организации, в которой этот компьютер установлен. Эта информация не играет практически никакой роли в домашней сети, поэтому здесь ваша фантазия может проявиться в полной мере.

При вводе имени владельца компьютера ограничений не накладывается

Далее Microsoft пытается убедиться, что вы являетесь законным владельцем данной копии и требует ввести ключ продукта. »

Важная информация

Драйверы и патчи

При установке могут потребоваться драйверы к видеокартам и другому оборудованию, поэтому позаботьтесь о том, чтобы диски с ними находились у вас под рукой.

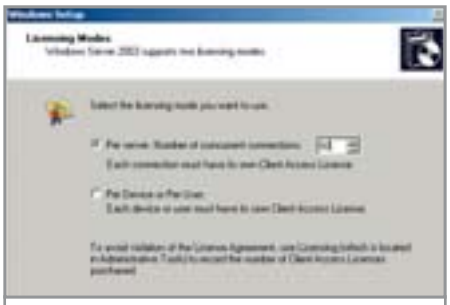
Вам обязательно потребуется заплатка (patch) службы RPC, которую можно скачать по ссылке, приведенной ниже: http://download.microsoft.com/download/8/f/2/8f21131d-9df3-4530-802a-2780629390b9/WindowsServer2003-KB823980-x86-ENU.exe

Этот же патч может быть найден и на сайте «Лаборатории Касперского»: www.avp.ru/news.html?id=1319264.

При помощи ключа продукта Microsoft борется с пиратами

» **Шаг 9.** На этом шаге необходимо определить правила, в соответствии с которыми будет лицензироваться устанавливаемый вами сервер. Операционная система Windows Server 2003 поддерживает два режима лицензирования: «на сервер» (Per Server) и «на рабочее место» (Per Seat).

Для того чтобы сделать осмысленный выбор режима лицензирования, рассмотрим преимущества и недостатки каждого из способов подробнее.



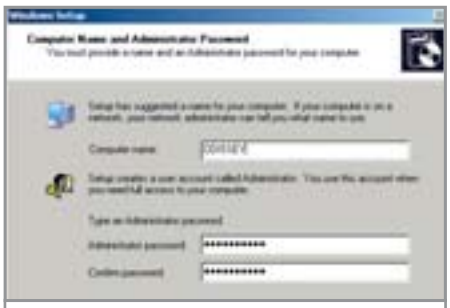
Здесь определяется порядок лицензирования Windows Server 2003

Лицензирование «на сервер» подразумевает необходимость выделения клиентских лицензий для подключения к определенному серверу. Каждая лицензия разрешает одно подключение клиентского компьютера к серверу для доступа к сетевым службам. В итоге количество лицензий должно соответствовать максимальному числу одновременно подключенных к серверу компьютеров.

Такая политика лицензирования предпочтительна для небольших сетей с одним сервером и для серверов Интернета или удаленного доступа, клиентские компьютеры которых лицензировать нельзя. Лицензирование «на сервер» позволяет определить максимальное число параллельных подключений к серверу и отклонить попытки входа в систему дополнительных пользователей. Если вы сомневаетесь, что выбрать, выберите этот режим.

Лицензирование «на рабочее место» требует отдельной клиентской лицензии для каждого компьютера, обращающегося к Windows Server 2003 для доступа к основным сетевым службам. Если компьютер лицензирован, с него разрешено обратиться к любому серверу Windows Server 2003 в сети. Такая политика лицензирования выгодна для больших сетей, где компьютеры соединяются с несколькими серверами.

Шаг 10. На этом шаге необходимо задать имя компьютера и пароль администратора.



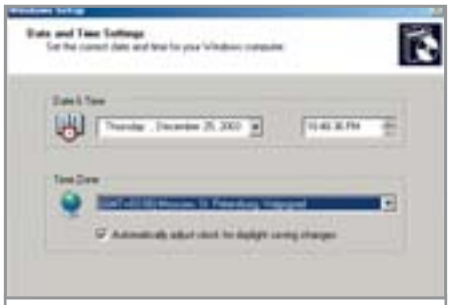
Имя компьютера должно включать в себя от 6 до 15 символов

Лучше не придумывать какое-то особо заковыристое имя сервера, ведь в дальнейшем его придется использовать очень часто. Что касается пароля, то тут требования противоположные. Пароль должен быть достаточно сложным. Лучше всего, если он будет содержать буквы, набранные на разных регистрах, цифры и специальные символы. При этом их сочетание в идеале не должно вызывать никаких ассоциаций. Разумеется, пароль нельзя записывать и хранить в таком месте, откуда он легко может быть похищен.

Краткое изложение требований, предъявляемых к стойкому паролю

А с каким логином необходимо осуществлять вход в сервер? В процессе установки создается пользователь Administrator, пароль для него и создается. Другими словами, необходимо при первом входе в Windows Server 2003 использовать логин Administrator и пароль, который только что был вами придуман. А дальше все делается легко и просто.

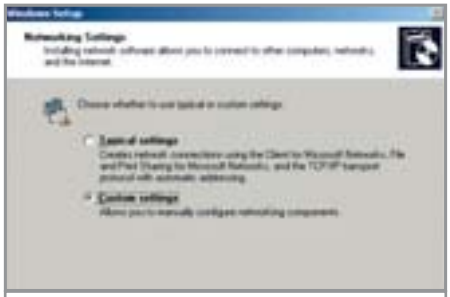
Шаг 11. На этом шаге необходимо указать дату, время и ваш часовой пояс.



Окно установки времени, по которому будет жить компьютер

Обратите внимание на маленькое окно в нижней части экрана. Если в нем будет установлена галочка, то система автоматически будет изменять время при введении летнего или зимнего времени. И здесь есть одна неувязка. Весь мир переходит на зимнее время в конце сентября. Раньше так делала и Россия. Однако сейчас Россия переходит на зимнее время в конце октября, поэтому вам придется «отматывать» время назад в конце сентября и вновь корректировать его в конце октября. Возможная альтернатива — жить месяц с неверным временем на сервере.

Шаг 12. На этом шаге система попросит вас указать, какие сетевые настройки необходимо применять в работе.



Окно выбора характера сетевых настроек Windows Server 2003

Если вы недостаточно опытны, выбирайте «Typical», а не «Custom». Разница между этими режимами заключается в настройке протокола TCP/IP. Если вы хотите, чтобы система сама настроила сетевые параметры, сервер попытается получить IP-адрес с сервера DHCP. Если сервера DHCP в локальной сети нет, то система сама зарезервирует IP-адрес из ранее определенного диапазона.

Шаг 13. Если же на предыдущем этапе вы выбрали не «Typical», а «Custom», то вам придется настроить сервер для работы в локальной сети вручную. »

» В этом окне выбираем «Internet Protocol (TCP/IP)», после чего нажимаем клавишу «Properties» и вводим данные.

Окно настройки сетевых компонентов

Предположим, что вы пытаетесь установить сервер в локальной сети жилого дома или небольшой фирмы. В этом случае вам должен быть известен диапазон сетевых адресов и маска подсети. Первые три поля IP-адреса и маска подсети должны совпадать у всех компьютеров локальной сети, только последнее поле должно быть уникальным. Узнать IP-адрес (в том числе свободный) и маску подсети можно, выполнив на другой машине, входящей в сеть, команду ipconfig /all.

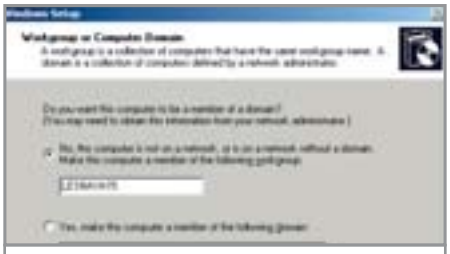
Настройка IP-адресации сервера

У администратора нужно узнать адрес маршрутизатора вашей сети и указать его в качестве шлюза по умолчанию (Default Gateway). Если маршрутизатора в сети нет, то необходимо указать адрес сервера провайдера. Если и интернет-провайдера нет, то нужно оставить это поле пустым.

Адрес DNS-сервера вашей сети нужно указать в поле «Preferred DNS server» (предпочитаемый DNS-сервер). Если этого сервера в сети нет, то нужно оставить поле пустым. В дальнейшем вы сможете установить DNS на этом же сервере, указав его IP-адрес как «127.0.0.1».

Если в сети есть и маршрутизатор и DNS-сервер, но вы не знаете, как раздобыть эту информацию, выполните на другом компьютере команду ipconfig с параметром /all.

Шаг 14. Теперь укажем, в состав какой рабочей группы будет включен сервер. Это делается в следующем окне.



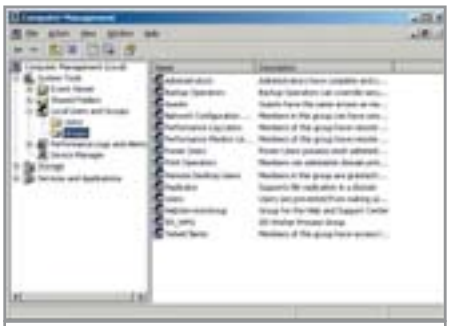
Ввод имени группы или домена

Если в сети уже есть рабочая группа, необходимо указать ее имя. Если нет, то нужно придумать новое. На этом инсталляция завершена. На очереди другая задача — настройка системы.

Новое имя, новая роль

Первое делом создадим пользователя с именем, отличным от Administrator.

Выберем элемент меню «Start → Administrative Tools → Computer Management». После этого на экране появится следующее окно:



В окне управления компьютером можно создавать пользователей и группы

Пользователь, которого мы хотим создать, должен быть включен в группу администраторов. Для создания пользователя, правой кнопкой мыши щелкаем на элементе «Users», затем выбираем элемент «New User». В появившемся окне вводим данные нового пользователя и его пароль. Сейчас пароль можно ввести самостоятельно. Однако в тех случаях, когда будут создаваться записи для реальных пользователей, желательно, чтобы каждый вводил свой пароль самостоятельно. В этом случае пароль пользователя не будет известен даже администратору.

Теперь необходимо включить нового пользователя в группу.

▸ Выбираем «Properties» только что созданного пользователя.

▸ В очередном появившемся окне выбираем вкладку «Member Of», а на ней нажимаем кнопку «Add...».

▸ В появившемся окне нажимаем кнопку «Advanced», затем в очередном окне жмем кнопку «Find Now». Выбрав нужную группу, нажатием клавиши «ОК» добавляем пользователя в эту группу.

Создать группу и включить в нее пользователей очень просто. Нажимаем правой клавишей мыши на элементе «Groups» (не «Users»), затем отвечаем на вопросы.

Пользователи могут одновременно быть членами нескольких групп. Если нужно, чтобы пользователь, включенный в одну из групп, стал членом только что созданной группы и никакой больше, необходимо сначала сделать пользователя членом только что созданной группы, а потом исключить его изо всех остальных групп.

Функции, которые может выполнять сервер, в терминологии Microsoft называются ролями. И на этом этапе нам необходимо определить, какие роли будет играть только что инсталлированный нами сервер.

Для добавления серверу какой-то роли используется такое средство, как «Configure Your Server Wizard». Обратиться к нему можно выбрав элемент «Start → Administrative Tools → Configure Your Server Wizard». После нескольких нажатий кнопки «Next» на отображении появится окно, содержащее список реализуемых сервером ролей.

Выбрав в этом окне необходимые серверу роли, естественно, нужно их правильно сконфигурировать. Но об этом речь пойдет в следующих статьях.

■ ■ ■ Илья Погорелый

Включение пользователя в одну из групп, существующих на компьютере

Служба переписи

Назначение и развертывание

В настоящее время Active Directory является центральным компонентом платформы Windows. В ОС Windows Server 2003 она приобрела новые усовершенствованные возможности как с точки зрения управления объектами, так и с точки зрения взаимосвязи сетевой среды.

Потребность в централизованном хранении информации об объектах распределенных сетей и их свойствах была реализована компанией Microsoft в виде службы каталога Active Directory (AD), впервые появившейся в операционной системе Windows 2000 Server. Что же представляет собой служба каталога? Это хранилище данных, используемое для доступа к информации об объектах (пользователи, компьютеры, домены и т. д.), их свойствах, а также для обеспечения служб аутентификации и безопасности. Стоит особо подчеркнуть, что AD является не только информационным ресурсом, но и механизмом, посредством которого администраторы и пользователи имеют возможность обращаться к этой информации. Необходимо отметить, что Active Directory не работает на Windows Server 2003 Web Edition.

Назначение службы каталога

Если сеть состоит из десятка компьютеров и двух-трех принтеров, администратор способен удержать всю необходимую информацию о ней у себя в голове. Если же сеть — это сложная структура, объединяющая в своем составе значительное число доменов, десятки расположений и тысячи пользователей, необходимость наличия централизованной информационной системы становится очевидной. Служба каталога позволяет:

- обеспечивать единую систему регистрации в сети (используя свое регистрационное имя и пароль, пользователь получает доступ ко всем ресурсам сети независимо от их расположения);
- обеспечивать требуемый уровень безопасности сети для защиты от несанкционированного доступа, используя встроенные »

Рис. 1. Выбор типичной конфигурации ролей для первого сервера AD

Рис. 2. Присвоение имени NetBIOS домену по умолчанию

Рис. 3. Запрет перенаправления запросов на разрешение имен

» в Active Directory средства аутентификации и управления доступом к ресурсам;

▸ осуществлять централизованное управление всеми ресурсами сети, широко используя такие инструменты, как групповые политики, в случае необходимости делегируя рутинную административную работу наиболее опытным пользователям;

▸ поддерживать текущую информацию об объектах сети, облегчая тем самым доступ к этим объектам и их свойствам;

▸ распределять каталог между несколькими серверами (контроллерами домена) в сети с помощью службы репликации, обеспечивая его доступность и отказоустойчивость, а также снижая сетевую нагрузку.

Основные понятия Active Directory

Прежде чем перейти к практическому развертыванию Active Directory, необходимо ознакомиться с ее базовыми понятиями и структурой. Каталог состоит из элементов (entry), представляющих собою набор информации или атрибутов, связанных с реальными объектами сети. Объектами каталога Active Directory могут являться пользователи, группы, компьютеры, принтеры (и другое оборудование), домены, организационные подразделения (далее ОП) и правила политики безопасности.

Элементы каталога организованы в виде иерархической структуры (дерева). Элементы, находящиеся ближе к корню дерева, обычно представляют собой более сложные объекты (например домены и подразделения), элементы на ветвях этого дерева (листья) — более простые объекты: пользователи, устройства, компьютеры. Подобная структура каталога может быть описана в терминах пространства имен. Для определения пространства имен и их разрешения в AD используется соглашение об именовании DNS, что обуславливает тесную интеграцию службы DNS с Active Directory.

Доступ к объектам в Active Directory основан на использовании протокола LDAP (Lightweight Directory Access Protocol, облегченный протокол службы каталогов). Он является механизмом обновления информации, запросов и определения объектов в каталоге. Каждый объект в Active Directory представлен своим различающимся именем (distinguished name) LDAP. Это имя уникальным образом идентифицирует объект (будь то пользователь или домен) в каталоге. Например, различающимся именем для пользователя Sergey, входящего в подразделение Sales домена organization.local, будет следующая конструкция:

CN=Sergey, OU=Sales, DC=organization, DC=local.

Различающееся имя LDAP состоит из трех главных элементов:

CN — общее имя (Common Name), имя объекта в Active Directory;

OU — ОП, имя подразделения в Active Directory (обратите внимание, что для встроенных контейнеров, таких как «Users», может использоваться CN= вместо OU=);

DC — доменная часть имени (Domain Component), DNS-имя домена, в который помещен объект, разделенное на части, соответствующие каждому из уровней иерархии доменов, начиная с нижнего уровня и заканчивая верхним (в нашем случае представлена двухуровневая доменная структура).

Другим способом определения объектов в Active Directory являются относительные различающиеся имена (relative distinguished name). Относительное различающе- »

Глоссарий

Элементы структуры Active Directory

Логическая структура каталога Active Directory включает в себя следующие элементы:

Домен — логически объединенная группа сетевых пользователей и компьютеров, для которой поддерживается единая политика администрирования и безопасности.

Дерево — набор доменов, использующих связанные пространства имен.

Лес — наиболее крупная структура в Active Directory, объединяющая деревья, поддерживающие единую схему (определения объектов и их свойств).

Контейнер — очень важное понятие в AD. Хотя он и является полноправным объектом каталога и частью пространства имен, с ним не может быть сопоставлен какой-либо физический объект. Контейнер представляет собой только логическую оболочку для групп объектов и других контейнеров.

Организационное подразделение (ОП) — контейнер, помогающий группировать объекты для целей администрирования и применения групповых политик. ОП существуют только внутри доменов и могут объединять объекты только из своего домена.

Глобальный каталог — хранилище информации обо всех объектах, существующих в лесу AD.

Контроллеры домена — серверы w2k3, хранящие редактируемую копию каталога (реплику) AD.

Сайт — под сайтом понимается группа TCP/IP-подсетей, между которыми осуществляется высокоскоростная связь.

Рис. 4. Выбор основного режима разрешений для домена

Рис. 5. Выбор пароля для режима восстановления службы каталога

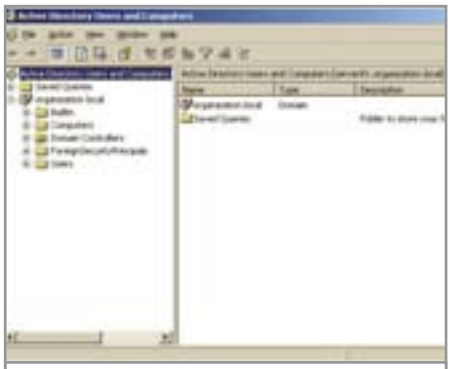


Рис. 6. Окно оснастки «Active Directory Users and Computers»

» еся имя — это более короткий путь описания объекта, применяемый в том случае, если известно, какому контейнеру принадлежит объект.

Развертывание Active Directory

Перейдем непосредственно к развертыванию Active Directory. Будем исходить из предпосылки, что у нас есть несколько компьютеров, объединенных в небольшую локальную сеть, составляющую рабочую группу. На одном из компьютеров (или на нескольких) установлена операционная система Windows Server 2003 Enterprise Edition (в дальнейшем w2k3). Предположим, что предварительно в этой сети не были установлены серверы DNS и DHCP.

Проанализировав потребности нашей организации и требования по администрированию и безопасности, мы решили объединить компьютеры в один домен, используя наш сервер в качестве контроллера домена (для реализации многих преимуществ Active Directory в домене должно устанавливаться как минимум два контроллера домена), создать два организационных подразделения Sales и Marketing и поместить в них пользователей, исходя из выполняемых ими функциональных обязанностей. Кроме того, в ОП Marketing мы создадим вложенное ОП Printers и разместим в нем установленные в нашей сети принтеры.

Для конфигурирования сервера воспользуемся мастером Configure Your Server Wizard. Он может быть запущен из окна «Manage Your Server» выбором опции «Add or remove a role». Его также можно запустить из меню «Start → All Programs → Administrative Tools». Мастер установки Active Directory — Active Directory Installation Wizard — является частью мастера Configure Your Server Wizard.

После проверки сетевых настроек предлагается выбрать роли, которые будет исполнять ваш сервер. Выберем опцию «Typical configuration for a first server» (рис. 1), позволяющую провести одновременную установку на компьютер серверов DNS и DHCP, добавить роль первого контроллера домена и установить Active Directory.

Назовем создаваемый домен organization.local, после чего ему будет присвоено имя NetBIOS (рис. 2), затем выберем опцию, запрещающую серверу DNS делать переадресацию запросов, поскольку не планируем пока разрешать имена вне нашего домена (рис. 3), и мастер сообщит нам о выбранных компонентах для установки.

В следующем окне предлагается выбрать разрешения по умолчанию для объектов «Users» и «Groups». Поскольку наш сервер является сервером w2k3, выбираем вторую из предложенных опций — «Permissions compatible only with Windows Server 2000 or Windows.Net Server operating systems» (рис. 4). После определения пароля для восстановления системы (рис. 5) мастер Active Directory Installation Wizard еще раз показывает выбранные опции, и нажатием кнопки «Next» мы запускаем установку Active Directory.

Управление объектами

Установка AD на сервер добавляет на вкладку «Administrative Tools» инструменты: «Active Directory Domains and Trusts», «Active Directory Sites and Services» и «Active Directory Users and Computers». Последний используется для управления пользователями, компьютерами, группами безопасности и другими объектами в AD. На левой панели этого приложения вы увидите структуру AD, созданный домен organi- »

Рис. 7. Добавление нового ОП в домен organization.local

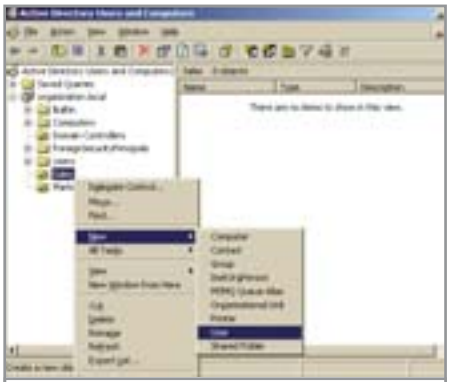


Рис. 8. Создание нового пользователя в ОП Sales домена organization.local

Рис. 9. Пользователь будет помещен в ОП Sales домена organization.local

Рис. 10. Назначение пароля пользователя и выбор его свойств

Рис. 11. Список задач, связанных с администрированием пользователей

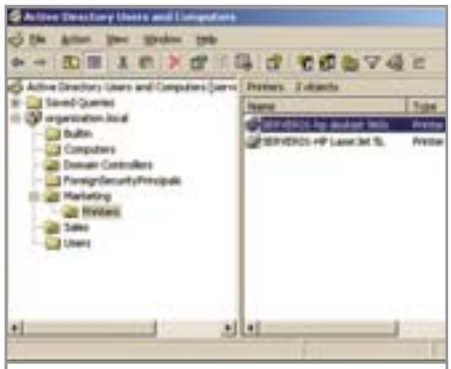


Рис. 12. Принтеры помещены в ОП Printers, вложенное в ОП Marketing

» zation.local и находящиеся в нем встроенные контейнеры (рис. 6). Перейдем к созданию запланированной структуры домена. Поскольку приемы создания и управления любыми объектами с помощью «Active Directory Users and Computers» довольно схожи, рассмотрим их на примере работы с ОП и пользователями. Щелкнем правой кнопкой мыши узел домена organization.local в дереве каталога и выберем из появившегося меню опцию «New», а затем «Organizational Unit» (рис. 7). Назовем это ОП Sales, и после нажатия кнопки «ОК» оно появится в дереве каталога ниже узла домена. Аналогично создадим ОП Marketing.

Пока эти контейнеры пусты. Поместим в них пользователей. Для этого щелкнем правой кнопкой мыши нужное подразделение и выберем из контекстного меню сначала «New», а затем «User» (рис. 8). Заполним появившееся окно свойств пользователя (рис. 9), установим для него пароль (рис. 10) и, проверив эти сведения, нажмем кнопку «Finish». Проделав эту операцию несколько раз, мы разместим всех пользователей в соответствующие подразделения.

Теперь, щелкнув правой кнопкой мыши одного из пользователей и выбрав вкладку «All Tasks», ознакомимся с теми задачами, которые может выполнять с ней администратор (рис. 11).

Контейнеры AD допускают добавление дочерних контейнеров, поэтому не составит большого труда создать ОП Printers, вложенное в подразделение Marketing, и разместить в нем сетевые принтеры (рис. 12).

Заключение

Active Directory является централизованным хранилищем информации об объектах сетевой среды и обеспечивает удобные и надежные средства для поиска и использования этих сведений. Средства безопасности интегрированы в AD посредством единой системы аутентификации пользователей и их авторизации, а также централизованного контроля доступа к объектам каталога. Администраторы получают возможность управлять всей сетью с любого компьютера, а авторизованные пользователи — доступ ко всем разрешенным сетевым ресурсам. Инструменты управления позволяют просто и эффективно решать задачи по созданию и управлению объектами AD.

■ ■ ■ Григорий Еременко

Эволюционное развитие

Новые возможности Active Directory в Windows Server 2003

Для тех, кто уже работал с Active Directory в Windows 2000, будет небезынтересно узнать о новых возможностях AD в w2k3. Эти новые функции делятся на доступные в смешанном режиме (когда не все контроллеры домена работают под управлением Windows Server 2003) и на доступные в основном режиме (когда все контроллеры домена — w2k3). Вот список возможностей Active Directory, доступных на любом контроллере домена под управлением данной ОС:

- предусмотрен выбор нескольких пользовательских учетных записей для одновременного изменения их свойств;
- поддерживается перемещение одного или нескольких объектов AD с помощью функции Drag & Drop в новое расположение в дереве каталога; также можно предоставлять объектам членство в группе, просто перетаскивая их на изображение этой группы;
- поиск объектов теперь может осуществляться с помощью запроса без просмотра, что уменьшает сетевой трафик;
- в оснастке «Active Directory Users and Computers» добавилась функция записи наиболее часто используемых запросов для их повторного обращения к ним;
- появилась возможность управления AD с помощью утилит командной строки;
- предусмотрено кэширование членства в группах (ускоряющее регистрацию в сети), при котором информация об универсальном членстве пользователей в группах сохраняется на выполняющих аутентификацию контроллерах домена.

Новые возможности Active Directory масштаба домена и леса доступны только в основном режиме Windows Server 2003:

- предусмотрено переименование контроллера домена без предварительного понижения его уровня до рядового сервера домена;
- возможно переименование любых доменов, их DNS- и NetBIOS-имен (включая корень дерева и корневой домен леса);
- расширена двухсторонняя транзитивность области видимости с одного леса на другой;
- возможно перемещение существующих доменов в структуре леса;
- предусмотрено отключение неиспользуемых классов или атрибутов схемы;

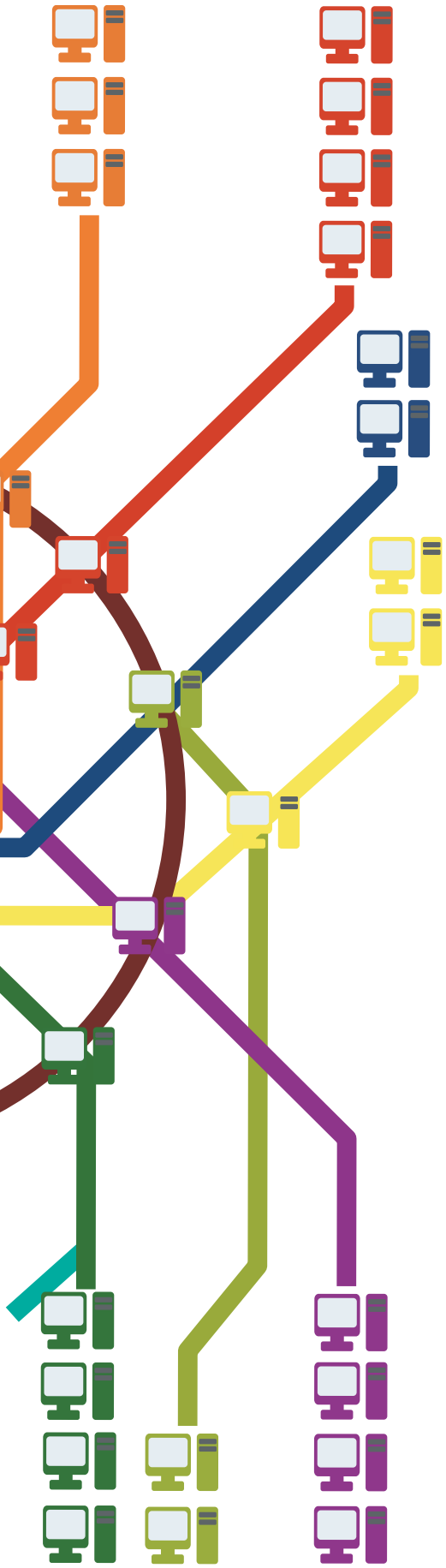
в процессе репликации теперь передается не целая группа как единица репликации, а отдельный член группы.

Общественное достояние

Теория и практика

Одной из основных задач при создании любой сети является предоставление доступа к различным программным и аппаратным ресурсам сети. Выделение ресурса для совместного использования принято называть термином «sharing».

Для работы в сети Windows-машины всегда использовали протокол NetBIOS. Он сам по себе является прикладным, а не транспортным, и доставка пакетов в нем изначально происходила следующим образом: компьютер-отправитель посылает пакет всем обитателям сети (широковещательное сообщение), и все, кроме компьютера-получателя, его игнорируют. Основой для NetBIOS служил транспортный протокол NetBEUI — немаршрутизируемый протокол (за счет отсутствия основы сетевого уровня), использующий только широковещательные сообщения. А NetBIOS — это система исключительно ввода-вывода информации (что отражено и в названии), а не доставки или ее контроля. Логично было бы предположить, что для успешной доставки информации необходимо знать адрес получателя. С другой стороны, для нормального функционирования такого элемента компьютерной системы, как пользователь, необходимо, чтобы компьютеры имели human-readable-идентификаторы — имена. Для сопоставления имен компьютеров сети их адресам (разрешение имен) в старых сетях также использовалось широковещание — компьютер «спамил» сеть, пытаясь выяснить, какому адресу принадлежит имя. »



» Такая схема создает минимум две проблемы: большая нагрузка на сеть и возможность «прослушивания» всех сообщений в сети. Кроме того, широковещательный метод позволяет компьютерам общаться только в рамках одной подсети вследствие своей немаршрутизируемости. Появление в качестве транспортных протоколов TCP/UDP решило проблему связи между различными сетями.

Сервис WINS

WINS (Windows Internet Name Service) — пережиток прошлого, наследие старых протоколов сетей Microsoft, в отличие от DNS, которая является современной системой преобразования имен компьютеров в IP-адреса. Все нынешние операционные системы используют именно ее. Система WINS (она же NetBIOS Name Service) — это по сути особенный DNS, «заточенный» под NetBIOS. Необходимость использовать сервер WINS имеется только при наличии в сети старых систем Windows 95/98/Me.

Служба WINS является, вероятно, простейшим из сервисов в нынешних сетях. Процесс работы службы заключается в следующем: при подключении к сети клиент соединяется с сервером и запрашивает регистрацию. Соответствующее клиенту имя и его адрес заносятся в базу данных сервера. По завершении работы клиент также сообщает серверу о необходимости удаления своей записи из базы. Каждый клиент при необходимости соединения с другим участником сети запрашивает у сервера адрес этого участника по его имени.

Если ваша сеть состоит из нескольких подсетей, то в каждой из них необходимо устанавливать свой WINS-сервер, а иначе в связи с немаршрутизируемостью широковещательных запросов некоторые старые клиенты не смогут правильно функционировать. Между серверами, естественно, должна быть создана система репликации. В новой инкарнации WINS появилась возможность постоянного соединения партнеров репликации. Благодаря экономии времени и ресурсов на открытии и закрытии сессий, базы данных различных WINS-серверов находятся в более актуальном состоянии. Кроме того, новая система идентификаторов версии записи позволяет точно определять достоверную информацию о соответствии имени адресу участника сети.

Репликация базы данных между партнерами WINS происходит в трех режимах: push, pull и push/pull — прием, передача и прием/передача соответственно. В первом случае сервер сообщает о необходимости репликации и изменении своей базы партнерам. Во втором случае сервер периодически запрашивает изменения у партнеров. Третий тип комбинирует первые два.

Установка сервера WINS, как и других сервисов на Windows Server 2003, представляет собой добавление соответствующей роли через консоль, и этот процесс не представляет никакой сложности (рис.1). После инсталляции сервер WINS полностью готов к работе в стандартных условиях и не требует дополнительных настроек.

Сетевые ресурсы

Файловый сервер

Файловый сервер, как следует из названия, служит для хранения или обмена информации. Это могут быть файлы совершенно разных типов, но так или иначе все это хозяйство занимает гигабайты памяти. В использовании дисковых ресурсов клиентов просто необходимо ограничивать (словесные уговоры, как правило, не помогают).

В первом же диалоге при добавлении роли «File Server» нам очень кстати предлагают установить квоты на дисковое пространство для пользователей. Определяя предел, можно установить уровень использования, при котором клиент будет оповещен о необходимости навести порядок в своих файлах. К сожалению, нельзя установить квоты на различные директории. Ограничение выставляется на пользование всеми ресурсами в целом.

Далее можно установить службу индексации. Этот сервис каталогизирует содержимое файлов в «расшаренных» папках и позволяет быстрее находить нужную информацию. Данная служба сильно нагружает сервер и полезна только в том случае, если ваши клиенты очень часто пользуются поиском. В противном случае обязательно отключите ее на вашем сервере.

На последнем этапе система предложит сделать какую-нибудь папку общей. Это действие можно оставить на потом, но консоль управления будет считать роль файл-сервера неактивированной, пока не появится хотя бы одна «расшаренная» папка. Впрочем, это не имеет особого значения.

Оснастка управления файловым сервером включает в себя весь необходимый набор инструментов для манипуляций с общи- »

Рис. 1. Диалоговое окно мастера добавления серверу новой роли

Рис. 2. С общими ресурсами можно проводить различные действия

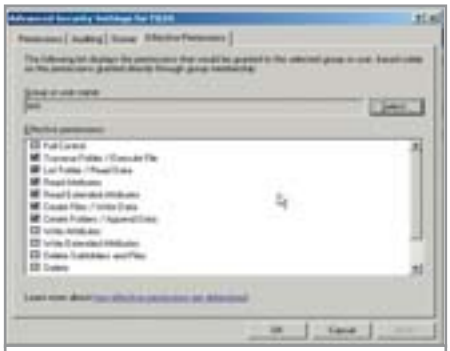


Рис. 3. Просмотр прав пользователя на доступ к папке или файлу

» ми ресурсами, сеансами и томами диска (рис.2). Первым делом заглянем в свойства общей папки. С первого взгляда особых изменений не заметно. Перейдем на закладку «Security» и войдем в расширенные параметры (кнопка «Advanced»). Здесь мы видим долгожданную закладку «Effective Permissions». С помощью этого инструмента теперь мы можем просмотреть реальные права пользователя или группы на доступ к папке или файлу с учетом всех «наследственностей» (рис. 3).

В разделе оснастки «Shares» мы видим еще одно новшество — сервис теневого копирования («Shadow Copies»). Эта система унаследована, если можно так выразиться, из Windows XP и расширена в возможностях. Теневое копирование — это прозрачная для пользователя система архивирования данных. В соответствии с расписанием сохраняются «моментальные снимки» объекта (незаметно для пользователя), а пользователь продолжает работать уже с новой версией. В Windows Server 2003 эта система позволяет создавать точки возврата в предыдущие версии ресурсов. Для понимания работы системы стоит привести пример.

Создадим на диске общую папку FILES, а в ней простой текстовый файл. Откроем панель «Configure Shadow Copies», выберем этот диск и активируем систему («Enable»). Сразу после активации сделаем теневую копию диска (кнопка «Create Now»). После этого сделаем любое изменение в нашем тестовом файле и снова создадим теневую копию. Для получение более наглядной картины повторим процедуру изменения файла и создания тени еще пару раз (рис. 4). После проведения этих манипуляций откроем свойства тестового файла через «Network Neighbourhood». На панели свойств можно наблюдать новую закладку «Previous Versions». Пользователь теперь способен просмотреть, скопировать или вернуться к предыдущим версиям файла, если потребуется (рис. 5). При теневом копировании диска процедуре подвергаются все данные в общих папках.

Некоторые тонкости. Теневое копирование производится только на всем томе (диске). Установка копирования для отдельной папки невозможна. Использовать «Previous Versions» могут только пользователи с операционной системой Windows XP и выше. На Windows XP при этом необходимо установить дополнительное ПО, находящееся в директории %SystemRoot\System32\ clients\ twclient сервера Windows 2003.

Настройка службы теневого копирования заключается в следующем: для каждого тома необходимо установить максимальный размер дискового пространства под копии файлов (минимум 100 Мбайт) и задать планировщику частоту копирования.

Следует еще заметить, что файловый сервер Microsoft Windows 2003 унаследовал от своего предшественника Windows 2000 все основные возможности. Вы можете создавать программные RAID-массивы (динамические и зеркальные тома), пользоваться системой автономных файлов, строить распределенные файловые системы DFS и т. д.

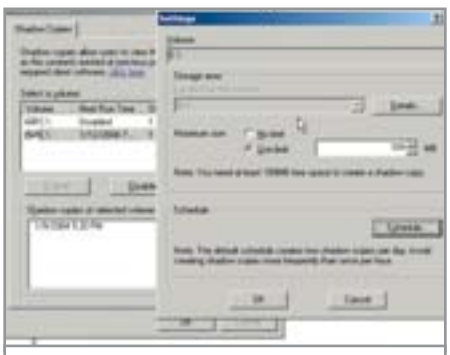


Рис. 4. Панель настроек сервиса теневого копирования

Рис. 5. Есть возможность просмотра, копирования и возврата к предыдущим версиям файла

Служба печати

Службы печати Windows Server 2003 не многим отличаются от служб Windows 2000. В числе основных изменений отсутствие поддержки протокола DLC (Data Link Control), который использовался старыми версиями принт-серверов компании Hewlett-Packard; возможность совместного использования не только принтеров, но и факсов (объединение служб); возможность устанавливать драйверы устройств в режиме ядра с помощью групповых политик (для администраторов). Кроме того, произошли некоторые изменения в сторону производительности и различных интерфейсных украшений. Особенно важным событием в этом отношении стала тесная интеграция служб печати и службы IIS. Благодаря этому печать (отправка факсов) и управление ею стали полностью доступны через веб-интерфейс. Возможность Point and Print — «кликни и напечатай» — позволяет пользователям устанавливать принтеры одним кликом. Драйверы для принтеров тоже можно инсталлировать с веб-сервера. Системные администраторы могут обозревать состояние принтеров и факсов и управлять очередями печати также из веб-интерфейса. »

Рис. 6. Установка драйверов для нового принтера вашей сети

Рис. 7. Можно указать дополнительные драйверы для других ОС

» Установка принт-сервера

А теперь перейдем непосредственно к установке принт-сервера (добавляем роль «Print Server»). На первом этапе определяется необходимость устанавливать драйверы для всех операционных систем семейства Windows или только для Windows 2000/XP. А далее предлагается установить первый принтер, что мы и сделаем (рис. 6). После этого в консоли «Manage Your Server» появляется новый пункт «Print Server» со ссылкой на добавление драйверов. Добавим дополнительные драйверы для других ОС (рис.7). Теперь пользователю не нужно будет искать драйверы в Интернете или лишний раз терроризировать службу технической поддержки. Драйверы автоматически установятся с сервера. В комплект Windows Server 2003 входит огромное количество драйверов для большинства существующих на данный момент моделей устройств печати. Если вы не используете принтеров-новинок, то о проблемах поиска драйверов и хранения «на всякий случай» можно не беспокоиться.

Основным моментом в конфигурировании принт-сервера является настройка spooler (очереди). Приложения генерируют и посылают данные на принтер быстрее, чем он печатает. Для того чтобы разгрузить пользовательское программное обеспечение, данные записываются на принт-сервере и помещаются в очередь для последующей печати. За счет этого увеличивается время вывода на печать. Если отказаться от создания очереди («Print directly to the printer»), то скорость печати увеличится, но при этом замедлится работа пользовательского приложения (рис. 8). Стандартным вариантом настройки spooler для общего принтера является очередь с немедленным началом печати документов («Start printing immediately»).

Для оптимизации работы сетевых принтеров можно использовать системы приоритетов, а также пулы принтеров. Физическое устройство печати может проявляться в системе более чем в одном экземпляре. Установим один и тот же принтер дважды под разными именами. В свойствах одного экземпляра выставим приоритет «1», а во втором «2». Теперь разрешим одной группе пользователей доступ к первому принтеру, а другой — ко второму. При одновременной печати пользователей этих двух групп в первую очередь будут обрабатываться документы из второй группы, так как приоритет их принтера выше. Комбинируя уровни приоритета, различные группы пользователей и время доступности принтеров можно добиться приближения к оптимальному распределению ресурсов печати. Кроме того, физические устройства можно объединять в пулы печати (в противоположность первому способу).

Установка пула печати производится с помощью мастера Add Printer Wizard (мастер установки принтеров), в котором создается новый принтер и затем в окне его свойств (пункт «Properties» контекстного меню) на вкладке «Ports» назначается количество портов вывода, равное количеству сетевых принтеров, которые необходимо объединить в пул. После этого необходимо отметить флажком опцию «Enable printer pooling» (рис. 9). Причем системой не ограничивается количество принтеров в пуле, и порты принтера могут быть одного или разных типов (сетевые, последовательные, параллельные). Стоит отметить, что возможно объединение в пул только идентичных устройств печати.

При использовании пула печати все объединенные в него принтеры отображаются системой как одно сетевое устройство, и при печати на него документ отправляется на тот принтер, который в данный момент свободен. Это позволяет уменьшить время ожидания пользователем очереди печати своего документа.

Невозможно узнать заранее, какой именно принтер пула получит тот или иной документ. Если в сети активирована служба сообщений Messenger Service, то пользователь, отправивший документ на печать, автоматически получит сообщение, в котором будет указано, что печать документа выполнена и отобразится порт вывода принтера. Если же Messenger Service не установлена в вашей сети, рекомендуется разместить все устройства печати в одном физическом месте, что облегчит пользователям «ручной» поиск своих распечатанных документов.

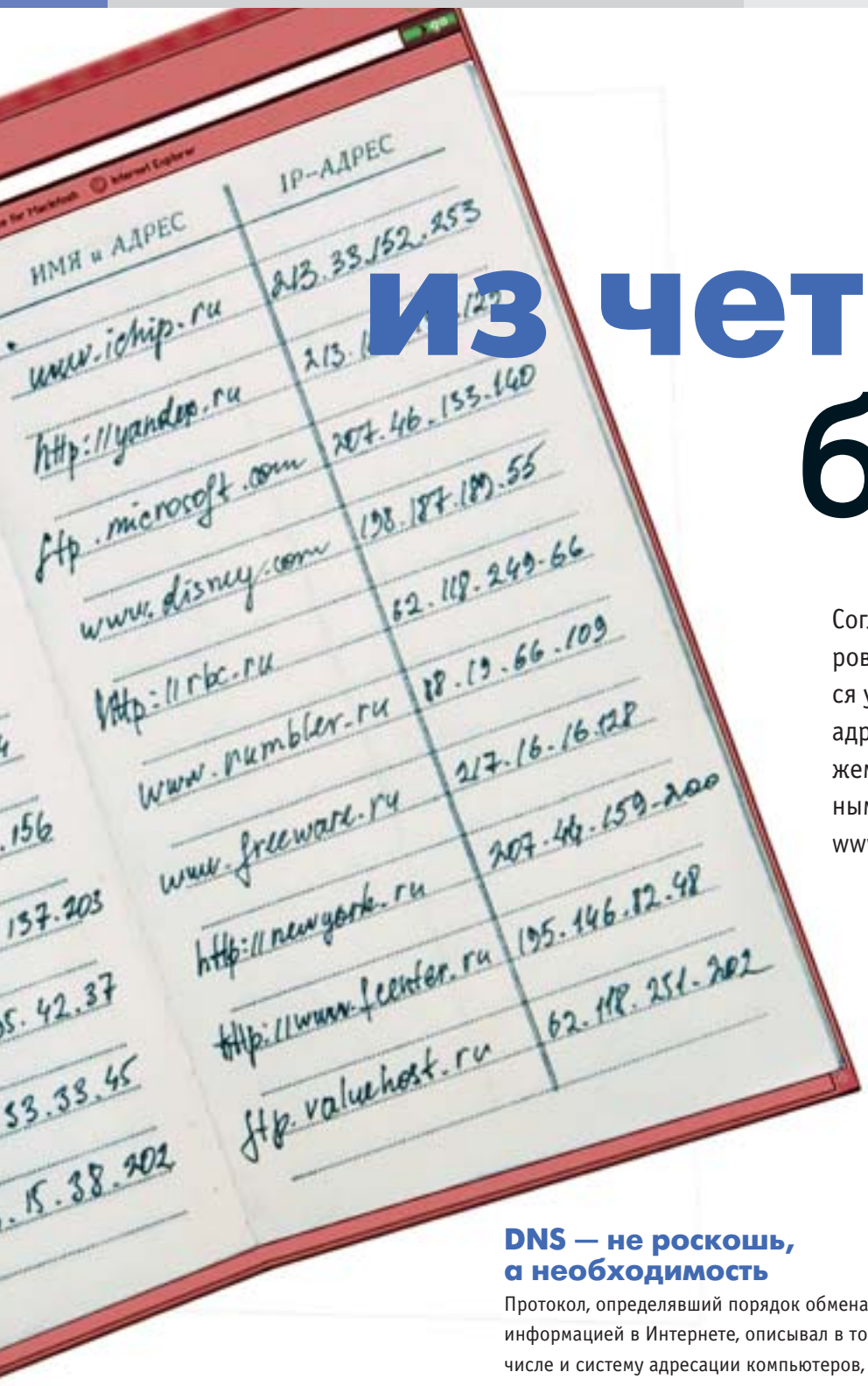
Заключение

Операционная система Windows Server 2003 предоставляет системному администратору широкие возможности по управлению и организации ресурсов общего доступа. Их правильно проведенная настройка позволит пользователям быстро и эффективно обмениваться различной информацией внутри сети и совместно использовать сетевые аппаратные средства, не мешая друг другу.

■ ■ ■ Иван Перпетумов

Рис. 8. Окно выбора дополнительных настроек принтера

Рис. 9. Объединение нескольких принтеров в пул



Имя из четырех байтов

Согласно системе адресации компьютеров в сетях каждой машине присваивается уникальный четырехбайтовый IP-адрес. Но только благодаря DNS мы можем обращаться к ним по более привычным нам именам, например www.ichip.ru, www.mail.ru, а не по набору цифр.

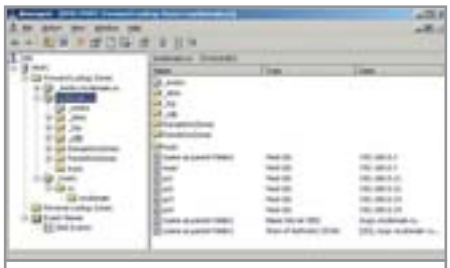
Адресование в сети

DNS — не роскошь, а необходимость

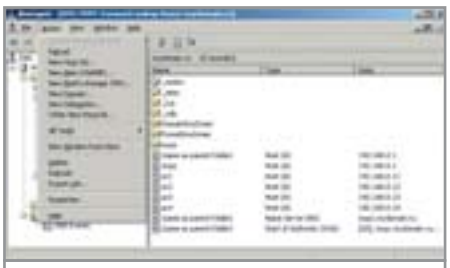
Протокол, определявший порядок обмена информацией в Интернете, описывал в том числе и систему адресации компьютеров, объединенных в эту Сеть. Согласно этой системе, каждому компьютеру присваивался уникальный четырехбайтовый адрес, который стали называть IP-адрес. Стандарт нового протокола и, соответственно, системы адресования были приняты в 1982 году.

Однако человеку гораздо проще запомнить некоторое слово, чем четыре бессодержательных для него числа. Из-за этого сразу после начала работы новой сети у пользователей стали появляться списки, в которых хранились не только адреса, но и соответствующие им имена узлов. Эти данные, обычно хранившиеся в файле с именем hosts, позволяли при указании имени узла мгновенно получить его IP-адрес. Позже процесс внесения корректуры в эти файлы был усовершенствован — последнюю версию файла hosts можно было скачать с нескольких серверов с заранее определенными адресами.

С ростом числа компьютеров в сети корректировать эти файлы вручную стало невозможно. Появилась необходимость в глобальной базе имен, позволяющей производить преобразование имен в IP-адреса без хранения списка соответствия на каждом компьютере. Такой базой стала DNS (Domain Name System) — система именования доменов, которая начала работу в 1987 году. »



В дерево DNS включаются зоны, домены и отдельные компьютеры



В меню перечислены объекты, которые добавляются в дерево DNS

» Структура DNS

В Интернете существует множество DNS-серверов, предоставляющих клиентам необходимую информацию об именах узлов сети. Важнейшим качеством DNS является порядок их работы, позволяющий DNS-серверам синхронно обновлять свои базы. Добавление адреса нового сайта в Интернете проходит за считанные часы.

Вторая особенность системы — это организация DNS-серверов в виде иерархической структуры. Например, запрос от клиента об имени ftp.microsoft.com может пройти через несколько DNS-серверов, от глобального, содержащего информацию о доменах верхнего уровня (.com, .org, .net и т. п.), до конкретного сервера компании Microsoft, в чьих списках перечислены поддомены вида *.microsoft.com, в числе которых мы и находим нужный нам ftp.microsoft.com. При этом множество DNS-серверов организуется в зоны, имеющие права и разрешения, делегированные вышестоящим сервером. Таким образом, при добавлении нового поддомена на местном сервере уведомления остальных серверов в Глобальной сети не производятся, но информация о новых серверах оказывается доступной по запросу.

Зоны, домены и поддомены

С ростом числа доменных имен работа между серверами была распределена по принципу единоначалия. Идея проста. Если организация владеет собственным доменным именем (например microsoft.com или whitehouse.gov), то именование внутри своего домена она производит самостоятельно. Единственная сложность при такой работе — предоставление вышестоящими серверами этих прав нижестоящим серверам.

Уточним термины. Домен — это некий контейнер, в котором могут содержаться хосты и другие домены. Имя домена может не совпадать с именем контроллера домена, то есть домен — это виртуальная структура, не привязанная к компьютеру. Хост же, напротив, соответствует физическому компьютеру, подключенному к сети. Имя хоста является именем конкретного компьютера. Имя хоста может совпадать с именем домена. Имя домена может совпадать с именем зоны, к которой он принадлежит, в этом случае домен является корневым в зоне. При этом зона не обязана содержать в себе одноименный (корневой) домен.

Зона — это контейнер, объединяющий несколько доменов в структуру с общими разрешениями на управление, то есть зоны являются контейнерами для доменов и хостов. Зоны могут быть вложены одна в другую. Разница между зонами и доменами в том, что домену может принадлежать несколько зон, содержащих различные его поддомены. Это дает возможность делегировать полномочия для поддоменов и управлять группами поддоменов.

Зоны используются для делегирования полномочий. Каждый домен должен находиться в составе зоны; при создании поддомена последний может быть переведен в новую зону, либо оставлен в зоне стоящего над ним домена. Для каждой зоны разрешения на создание или удаление всех входящих в нее доменов делегируются отдельно.

Для нормальной работы корпоративной сети в большинстве случаев хватает единственной зоны, более того, очень часто системные администраторы ограничиваются созданием единственного домена.

Интеграция DNS в Active Directory

Компания Microsoft рекомендует использовать DNS-серверы в корпоративных сетях для организации работы компьютеров в составе домена. Дело в том, что технология DNS более универсальна и эффективна, чем использующиеся на старых системах WINS и NetBIOS. Клиенты только посылают запросы серверу и получают ответы без обращения к каким-либо иным узлам сети.

С точки зрения производительности лучше всего интегрировать DNS в Active Directory, что возможно на серверных ОС компании Microsoft начиная с Windows 2000 Server. Совмещение ролей DNS-сервера и контроллера домена упрощает администрирование сети, особенно если размеры ее достаточно велики.

Что нам стоит DNS построить

DNS реализуются в соответствии с единым стандартом, основы которого изложены в »

Стремительное развитие Интернета

Растет как на дрожжах

1995, июль	1,7 млн
1996, январь	2,4 млн
1996, июль	3,3 млн
1997, январь	3,9 млн
1997, июль	4,5 млн
1998, январь	8,2 млн
1998, июль	10,3 млн
1999, январь	12,1 млн
1999, июль	18,7 млн
2000, февраль	24,8 млн
2000, сентябрь	32,6 млн
2001, февраль	36,3 млн

Данные об увеличении числа серверов домена .com за период с 1995 по 2001 год опубликованы на сайте www.ngi.org, принадлежащем организации Center for Next Generation, занимающейся в том числе и связанной с Интернетом статистикой. На графике виден экспоненциальный рост числа сайтов в Интернете.

IP-адрес хоста можно посмотреть в окне его свойств

DNS-сервер может получать данные от DHCP-сервера

Так DNS и DHCP настраиваются на совместную работу

» RFC 1011, 1034 и 1035. В Windows Server 2003 процесс развертывания и управления DNS сделан проще, чем в предыдущих версиях операционных систем, благодаря мастерам настройки ролей сервера. В Windows Server 2003 добавлены и новые функции управления Active Directory, которая может быть интегрирована с DNS воедино.

При создании контроллера домена, то есть сервера, управляющего работой Active Directory, мастер предлагает создать и настроить DNS-сервер. Для этого достаточно в настройках отметить пункт «Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server». В этом случае запускается DNS-сервер и создается зона, одноименная с вашим доменом.

Для имени домена лучше использовать два слова, разделенных точкой (вида mydomen.ru). Технически возможно включить компьютеры вашей сети и в домен верхнего уровня, но Microsoft не рекомендует использовать для домена имя, состоящее из одного слова, так как в этом случае возникают сложности с организацией пересылки запросов (forwarding) и динамических обновлений.

Настройка DNS

После перезапуска системы в окне «Manage Your Server» (управление сервером) и на панели «Администрирование» появятся новые элементы — ссылки на консоли управления Active Directory (три иконки) и DNS (одна иконка). Остановимся подробнее на консоли управления DNS-сервером.

Дерево DNS содержит список DNS-серверов, в нашем случае список будет состоять из одного пункта — имени нашего сервера. Раскрыв его, мы увидим три папки — «Forward Lookup Zones» (зоны прямого просмотра), «Reverse Lookup Zones» (зоны обратного просмотра, пустая папка) и «Event Viewer» .

Папка зон прямого просмотра будет содержать две записи. Зона, чье имя начинается с _msdcs, относится к организации работы системы (DC расшифровывается как Domain Controller, контроллер домена), пока что нам ее трогать не нужно, так же как и папку _msdcs во второй зоне. Выбрав вторую зону, в списке справа мы увидим ее содержимое — собственно говоря, все компьютеры, чьи имена хранятся на нашем сервере, будут перечислены именно там.

Добавление новых хостов будет происходить автоматически. Все операционные системы Windows, начиная с Windows 2000 Professional, поддерживают корректное обновление базы DNS-сервера в своей локальной сети. Новые пункты в список имен хостов на DNS-сервере могут добавляться и при помощи службы «Computer Browser». Вручную же добавление новых доменов и хостов, равно как и удаление существующих, происходит из меню консоли «Action» или из контекстного меню правой клавиши мыши.

После запуска контроллера можно приступить к введению в домен клиентских машин. Повторим, что корректная работа в составе домена возможна только для систем ранга Professional, начиная с Windows 2000 Professional, то есть в домене откажутся работать компьютеры под управлением операционных систем Windows 98, Windows Me или Windows XP Home Edition.

Когда же вы добавляете в домен компьютер с установленной ОС Windows 2000 Professional или Windows XP Professional, система автоматически пошлет запрос DNS-серверу, а тот в свою очередь добавит новый IP-адрес в список.

В сети, состоящей из компьютеров с фиксированными IP-адресами, работа DNS предельно проста. Однако как быть, если в вашей сети IP-адреса должны раздаваться динамически? Тут мы сталкиваемся с определенными сложностями, поскольку в этом случае DNS-сервер должен обновлять свою базу постоянно, основываясь на данных, получаемых от DHCP-сервера.

Впрочем, чтобы настроить DNS и DHCP на совместную работу, не требуется особых усилий. Достаточно открыть «Scope Options» в консоли управления DHCP-сервером и указать имя вашего DNS-сервера в параметре «DNS Domain Name».

IP-адрес самого DNS-сервера может быть динамическим. В этом случае для каждого нового компьютера, выполняющего серверные функции, настройка сетевых параметров при его подключении будет происходить благодаря DHCP-серверу. Также не обязательно, чтобы серверы DHCP и DNS физически находились на одном компьютере. Они будут корректно работать, даже если запущены на разных машинах.

DNS-сервер может производить очистку списка, удаляя из него данные о тех хостах, которые удалены из сети. Чтобы настроить очистку списка хостов, нажмите кнопку «Aging» («Очистка») на вкладке «General» в свойствах зоны — по умолчанию удаление «просроченных» имен выключено (нужно поставить соответствующую галочку). Кроме того, там же указывается параметр автоматического обновления («Dynamic Updates») — по умолчанию он переключен в «Secure Only» и разрешает производить обновления базы на основе запросов только от безопасных источников. »

» Подключаемся к Интернету

У начинающих системных администраторов возникает немало проблем от некорректного обращения с настройками DNS, в том числе с соответствующими настройками на компьютерах пользователей.

Во-первых, все зависит оттого, статические или динамические IP-адреса используются в вашей сети. В случае, если используются статические адреса, убедитесь, что на каждой машине корректно прописан ее IP-адрес, маска подсети и выбираемый по умолчанию DNS-сервер. Если же компьютеры получают свои IP-адреса динамически, посредством DHCP-сервера, то этот же сервер должен указывать и адрес DNS-сервера. Учтите, что для корректной работы клиентов DHCP-сервер в подсети должен быть единственным.

Другая задача, возникающая перед администраторами, — это настройка доступа в Интернет через локальную сеть. Доступ может быть организован по-разному, и, если все клиенты подключаются через прокси-сервер, настраивать DNS для работы в Интернете необходимости нет. Другое дело, если вы используете IP-маскарадинг при помощи NAT. В этом случае клиентские компьютеры в вашей сети должны будут иметь возможность получать ответы от DNS-серверов в Интернете, чтобы подключаться к веб-серверам по их IP-адресам.

Реализовать это просто. Вам нужно настроить пересылку запросов с вашего DNS-сервера на сервер интернет-провайдера (так называемый форвардинг). Лучше всего организовать это в два этапа. Сначала ваш DNS-сервер отправляет запрос на маршрутизатор, а тот уже пересылает его провайдеру.

Можно обойтись и одним шагом, ведь если маршрутизатор предоставляет сервис NAT для выхода в Интернет, то сам DNS-сервер может обращаться непосредственно к провайдеру. Однако такой метод менее грамотен. Например, если вы поменяете провайдера, вам придется править настройки уже на нескольких компьютерах. Кроме того, подключение к Интернету через NAT менее безопасно, чем перенаправление запросов посредством прокси-сервера. Также по соображениям безопасности не рекомендуется совмещать роль DNS-сервера и маршрутизатора на одном компьютере, особенно если он же является и контроллером домена в вашей сети.

Настройка форвардинга происходит в свойствах DNS-сервера из консоли управления. Нажимаем правой кнопкой на значке сервера, затем «Properties → Forwarders», где и указываем имя вышестоящего домена или перечисляем DNS-серверы, к которым будет обращаться наш сервер. На вкладке «Root Hints» перечисляются адреса DNS-серверов сети (не обязательно вышестоящих). Список «Root Hints» может быть заполнен автоматически при помощи мастера Configure DNS Server из меню «Action».

Порядок настройки форвардинга в свойствах DNS-сервера

Предупреждение о нарушении отмечено иконкой

Ошибкой является создание зоны с именем «.». В этом случае наш DNS-сервер начнет считать себя корневым, то есть верхним в глобальном дереве DNS. Разумеется, никакие пересылки вышестоящим серверам работать не будут. При создании зоны, чье имя совпадает с частью имени уже существующих зон после точки (например, у нас есть зона trading.office, а мы создаем зону office), все принадлежащие ей зоны и домены оказываются вложенными в нее.

Если у вашего сервера в свойствах подключения к локальной сети в качестве DNS-сервера указан сам контроллер домена, это тоже не очень хорошо. DNS-запросы никогда не должны приходить на сервер с его же адреса — любой подобный случай однозначно свидетельствует о неправильности настроек.

Разобраться в ситуации поможет «Event Viewer». В случае корректной работы DNS-сервера в журнале должна появиться запись о старте сервера. Также новые записи будут появляться по мере добавления новых имен хостов либо при ручном управлении зонами и доменами.

Для того чтобы детектировать неисправности со стороны клиента, проще всего воспользоваться консольной утилитой nslookup, которая поставляется вместе с операционной системой. После ввода nslookup в командной строке на экране должно появиться имя и IP-адрес вашего DNS-сервера, а после этого вам будет предоставлена возможность протестировать сервер путем отправления запросов на преобразование имени в IP-адрес. Чтобы увидеть справку по параметрам команды nslookup, введите в командной строке nslookup |help.

■ ■ ■ Игорь Логинов

В окне «Root Hints» отображаются другие DNS-серверы сети

Анализ журнала событий поможет и в случае проблем с DNS

Временная прописка

Установка и администрирование

В операционной системе Windows Server 2003 реализовано множество различных служб, предназначенных для управления сетевой инфраструктурой. Одна из этих служб — DHCP — присутствует в серверных операционных системах Microsoft начиная с Windows NT Server 3.5.

DHCP (Dynamic Host Configuration Protocol) — это протокол передачи параметров конфигурации машинам в сетях TCP/IP, разработанный рабочей группой DHC (Dynamic Host Configuration Workgroup), входящей в состав IETF (Internet Engineering Task Force). Основные цели создания DHCP такие: предоставить системному администратору средство для контроля над настройками сетевых параметров, обеспечить конфигурацию сетевых настроек компьютера без участия пользователя и обеспечить уникальность IP-адресов настраиваемых клиентов. DHCP предоставляет администратору хранилище настроек и сервис распределения постоянных или временных IP-адресов. Для обеспечения уникальности выданных IP-адресов в хранилище используется привязка к идентификатору, уникальному для каждого клиента, состоящему из адреса сети и MAC-адреса устройства. Схема работы сервиса распределения адресов проста: клиент запрашивает адрес на определенное время, а сервер этот адрес выдает, причем гарантируется, что тот же адрес не будет выдан другому клиенту в течение указанного периода времени и при последующих запросах по возможности будет выдан тот же самый адрес. В качестве дополнительной гарантии уникальности выданного IP-адреса и клиент и сервер должны его проверить всеми доступными средствами перед использованием. Клиент может продлить срок действия IP-адреса или освободить его. Кроме IP-адреса клиенту могут передаваться и другие параметры, например шлюз по умолчанию и адреса DNS-серверов. Взаимосвязь сервера и клиентов DHCP построена по схеме «вопрос-ответ». »

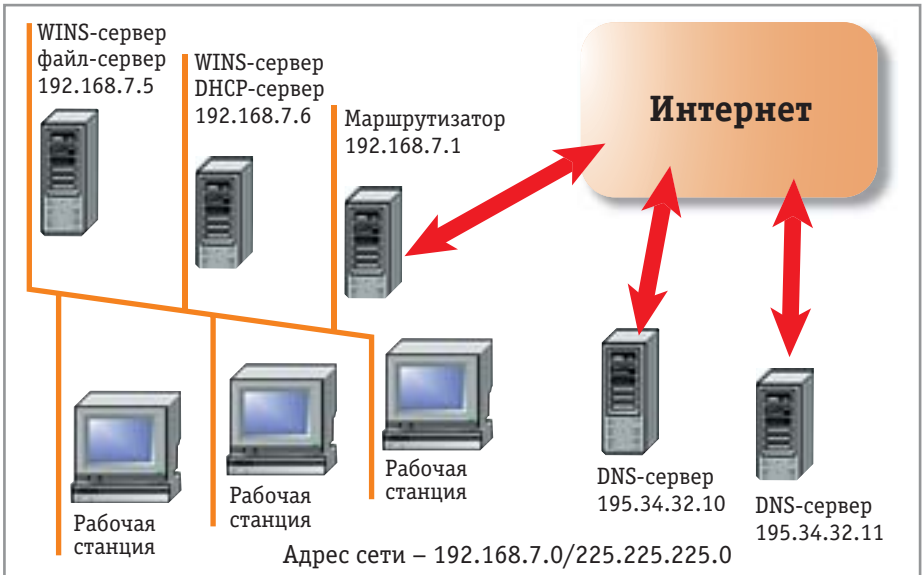


Рис. 1. Схема типичной локальной сети с доступом в Интернет

Преимущества использования DHCP

Предположим, что вы администрируете сеть на 200 машин. И вот в один прекрасный момент вам по какой-то причине потребовалось изменить на всех машинах адрес DNS-сервера или сменить класс сети и соответственно изменить маску и IP-адрес. Если производить замену вручную, тяжелый рабочий день без перерыва на обед обеспечен. А если компьютеры сильно распределены между собой, как, например, в районных сетях и больших офисах? Или в сети не 200 компьютеров, а тысяча двести? В таком случае процесс замены может растянуться на очень длительное время. Иная картина будет, если в локальной сети предусмотрена служба DHCP. Достаточно поменять настройки на сервере — и через некоторое время клиентские машины самостоятельно получат требуемые параметры.

Вот другой пример. Допустим, необходимо развернуть сеть на те же самые 200 компьютеров. Если очень быстро шевелить мышкой и набирать цифры, то на настройки параметров TCP/IP уйдет одна минута. На все машины понадобится три с половиной часа непрерывного выполнения однотипных операций. И опять DHCP-сервер сильно облегчит эту задачу и сэкономит время.

Реализация DHCP

В Windows Server 2003 работоспособность протокола DHCP обеспечивается тремя компонентами. Служба DHCP Server управляет хранилищем настроек и отвечает на запросы клиентов. Служба DHCP Client отправляет запросы серверу, принимает параметры конфигурации и вносит настройки в стек TCP/IP. Консоль управления DHCP предназначена для изменения настроек DHCP-сервера. Хранилище настроек организованно в виде областей действия (scopes). Область действия — это непрерывный диапазон IP-адресов, который задается адресом сети и маской, например 192.168.7.0/255.255.255.0. Обычно эта область совпадает с выбранным адресным пространством для конкретной сети. В области действия определяется диапазон, который будет доступен для выдачи клиентам (address pool), и диапазон адресов, которые клиентам выдаваться не будут (exclusion range). Для каждой области действия задаются необходимые настройки (options), например адрес шлюза по умолчанию, адреса DNS- и WINS-серверов.

Установка DHCP

Перед установкой нужно определиться с диапазоном адресов, доступных для распределения между клиентами DHCP, и списком исключений из этого диапазона. В список исключений попадут машины, на которых IP-адреса должны настраиваться вручную из-за особенностей работающих на них служб. В эту категорию попадают DNS-серверы, маршрутизаторы, серверы удаленного доступа и сам DHCP-сервер. Адреса подобных серверов имеет смысл объединить в одну непрерывную группу, например, взять первые десять адресов выбранной области действия. Для сети, показанной на рис. 1, данные будут такими:

область действия — 192.168.7.0/255.255.255.0
список исключений — адреса с 192.168.7.1 по 192.168.7.10 (зарезервируем десять адресов на случай появления дополнительных серверов)
шлюз по умолчанию — 192.168.7.1
DNS-сервера — 195.34.32.10 и 195.34.32.11
WINS-сервера — 192.168.7.5 и 192.168.7.6

Эти данные потребует мастер установки сервиса DHCP, который можно запустить, добавив выбранному серверу роль DHCP с помощью Manage Your Server. После успешного завершения установки сервер готов к работе.

Администрирование сервера DHCP

Все административные задачи выполняются с помощью консоли управления DHCP. Консоль позволяет активировать/дезактивировать область действия, изменять настройки, создавать резервную копию хранилища DHCP, просматривать список выданных IP-адресов и многое другое. Остановимся подробнее на некоторых моментах. Чтобы изменить, например, адрес сервера WINS, нужно выбрать в консоли раздел «Scope Options», щелкнуть на нем правой кнопкой и выбрать «Configure Options». В появившемся окне выбираем из списка опцию «044 Wins/NBNS Servers» и меняем адреса на те, которые нам нужны (рис. 2). Если нам нужно, чтобы клиентский компьютер гарантированно получал все время один и тот же адрес, можно воспользоваться механизмом резер-

Недостатки DHCP

Проблемы безопасности

Основным недостатком DHCP на данный момент является низкий уровень безопасности самого протокола, в котором не предусмотрена проверка подлинности клиента и сервера. Таким образом, злоумышленник может установить в сети свой сервер DHCP и передавать клиентским машинам нужные ему настройки. Единственный способ борьбы — постоянный мониторинг локальной сети на предмет наличия в ней чужого DHCP-сервера.

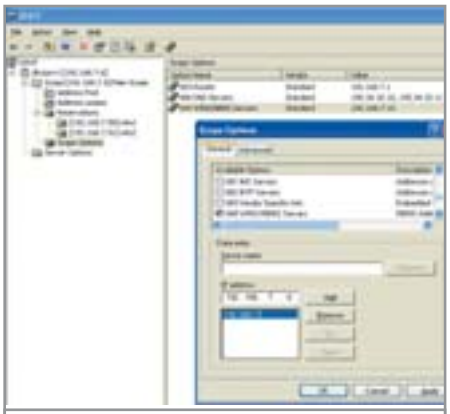


Рис. 2. Изменение адреса WINS не сложнее любых других настроек

Рис. 3. Резервирование IP-адреса клиентского компьютера

Рис. 4. Активация клиента DHCP на рабочей станции

» вирования IP-адресов (рис. 3). Для этого в консоли надо войти в раздел «Reservations», затем в меню «Action» выбрать «New Reservation» и в появившемся окне ввести имя (это поле будет заменено на предоставленное клиентом DHCP), IP-адрес, MAC-адрес и описание. Сюда, например, можно занести имя пользователя клиентского компьютера или причину резервирования. Список выданных адресов доступен в разделе «Address Leases». Служба DHCP автоматически архивирует свою базу данных раз в 60 минут. Резервная копия базы размещается в папке WINDOWS\System32\dhcp\backup. Кроме того, резервное копирование можно запустить вручную с консоли управления DHCP, выбрав пункт меню «Action\Backup» и указав папку, куда требуется положить резервную копию. Доступ к консоли администратора регулируется группами «DHCP Administrators» и «DHCP Users». Лишь пользователи, включенные в первую группу, могут менять настройки сервера.

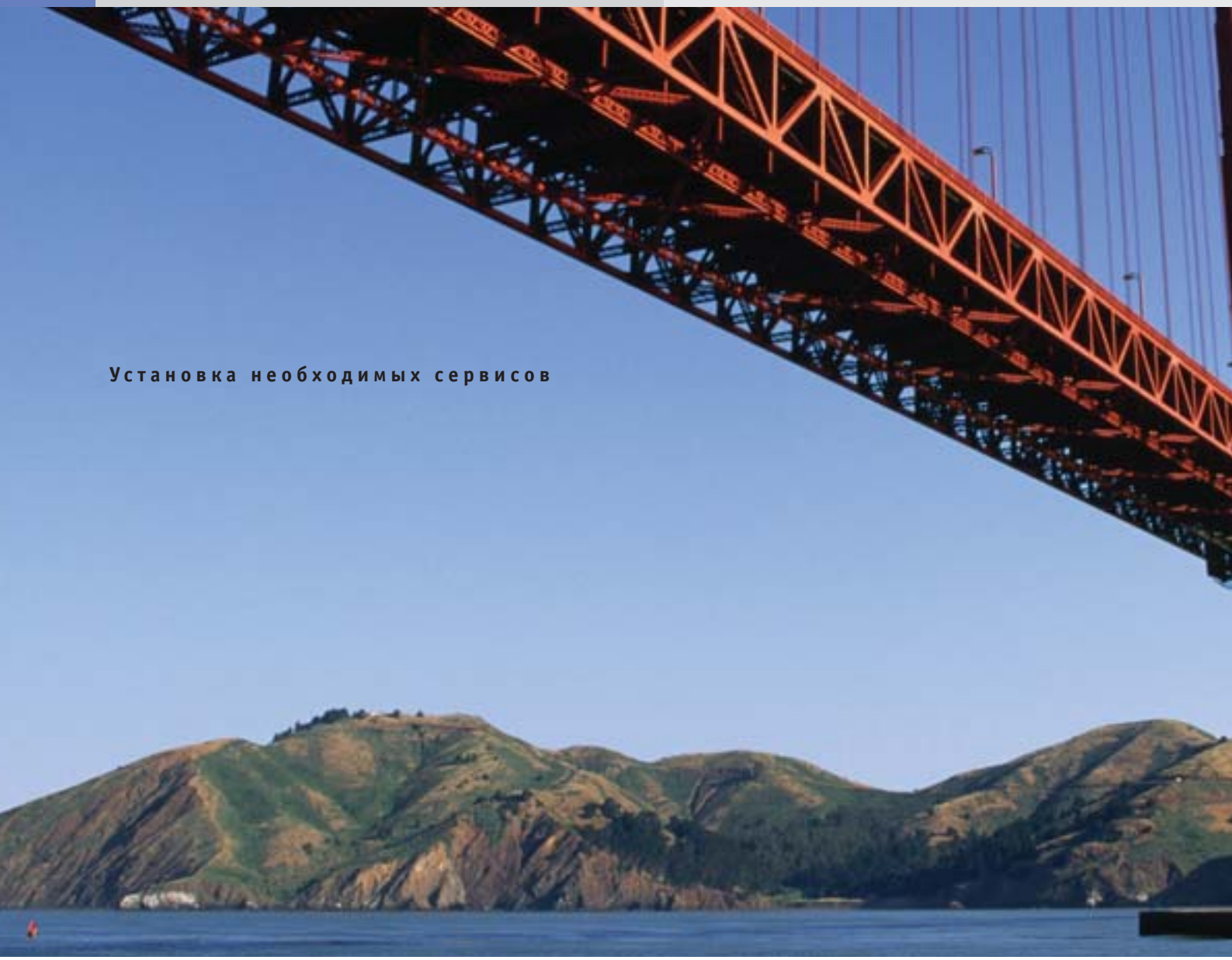
Описание работы клиента DHCP

Чтобы компьютер в локальной сети мог взаимодействовать с DHCP-сервером, на нем нужно активировать службу DHCP Client. Сделать это можно в настройках TCP/IP локального сетевого соединения с помощью включения режимов «Obtain an IP address automatically» и «Obtain DNS server automatically» (рис. 4). После применения этих настроек DHCP-клиент будет активирован, и если в сети присутствует корректно настроенный DHCP-сервер, машина получит IP-адрес. Для проверки работоспособности клиента можно ввести команду ipconfig в его командной строке. Процесс продления и освобождения адреса можно инициировать с помощью этой же команды с ключами /renew и /release. В реализации клиента DHCP Microsoft предусмотрела возможность использования альтернативной конфигурации стека TCP/IP, которая активируется, если DHCP-сервер недоступен. Параметры альтернативной конфигурации выбираются с помощью APIPA (Automatic Private IP Addressing). Режим APIPA работает следующим образом: DHCP-клиент выбирает случайный адрес из диапазона 169.254.0.0/255.255.0.0 и с помощью ARP (Address Resolution Protocol) проверяет, есть ли такой адрес в сети; если адрес занят, то выбор осуществляется заново, если свободен — выбранный IP-адрес и маска сети вносятся в настройки TCP/IP. Таким образом, APIPA служит некоторой подстраховкой на случай отказа DHCP-сервера.

Рис. 5. Схема обмена сообщениями между сервером и клиентом DHCP

Заключение

Как мы видим, Microsoft предоставила системному администратору реализацию замечательной службы, которая избавит его от большого количества рутинной работы, сэкономит время и позволит избежать ошибок, что положительно скажется на качестве работы локальной сети. ■ ■ ■ Роман Сырцев



Установка необходимых сервисов

Операционная система Windows Server 2003 обладает огромными возможностями по настройке и управлению различными сетевыми службами и сервисами. Их грамотное использование позволяет значительно увеличить скорость взаимодействия между членами сети и повысить уровень ее защищенности.

Основные требования, которые предъявляются пользователями современных локальных сетей различного уровня, от небольших домашних до огромных корпоративных, практически одинаковы: скорость передачи данных и возможность доступа к Интернету. Удовлетворить эти запросы можно несколькими способами.

Основным средством, способным помочь быстро и эффективно увеличить скорость передачи данных внутри сети, является служба Routing And Remote Access («Маршрутизация и удаленный доступ»), которая позволит связать несколько разделенных сегментов сети или, другими словами, назначить серверу роль маршрутизатора. Эта же служба поможет провести настройки, необходимые для обеспечения доступа всех членов локальной сети к Интернету.

Проблема роста

По мере увеличения числа компьютеров, входящих в состав той или иной сети, неизбежно снижается и средняя скорость передачи данных внутри нее. Предположим, в вашей сети находятся 40 компьютеров и один сервер, от каждого компьютера в коммуникационный узел протянут провод, »

Наводим мосты

» и все 40 кабелей подключены к двум коммутаторам или концентраторам. Коммутаторы (все описанное в равной мере относится и к концентраторам) соединены вместе, в один из них включен основной сервер. В данной сети используется протокол IP, допустим, что сервер имеет адрес 192.168.1.200, а клиенты — 192.168.1.1, 192.168.1.2,... 192.168.1.40, и в этой сети будет использоваться стандартная маска 255.255.255.0.

Пусть сервер подключен к коммутатору через 100-мегабитный порт, при этом получается, что все сорок клиентских компьютеров используют полосу пропускания 100 Мбит, и в худшем случае (при максимальной нагрузке) каждому клиенту достанется 100/40 = 2,5 Мбит или примерно 300 кбайт в секунду. Возможно, вам не хватает такой скорости работы сети, но нет возможности использовать более дорогое оборудование, то есть переходить со 100 Мбит на 1 Гбит. В этом случае можно просто разделить один сегмент сети, состоящий из 40 компьютеров, на два сегмента по 20 машин. Для этого необходимо установить в сервер дополнительную сетевую плату и, разорвав соединение между коммутаторами, подключить их к разным сетевым платам.

После этих изменений клиенты будут использовать два канала по 100 Мбит каждый, при этом скорость обмена информацией с сервером увеличится в два раза. На физическом уровне проблема действительно решена, но еще остается и уровень логический — после того как сеть была разделена »

Рис. 1. Создание сетевого моста с помощью объединения сетевых карт

Рис. 2. Настройка сетевого протокола TCP/IP для созданного моста

Рис. 3. Диалоговое окно мастера добавления новой роли серверу

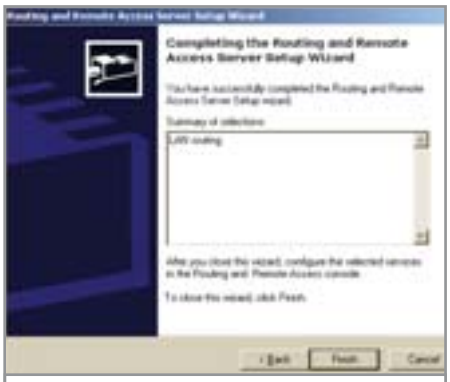


Рис. 4. Завершение работы мастера установки службы «LAN routing»

» на два сегмента, клиенты в разных физических областях сети больше не могут соединяться друг с другом напрямую, как это было возможно раньше.

Межсетевой мост

Первое, что можно сделать, используя Windows Server 2003, чтобы восстановить прежнее состояние, это включить мост и таким образом снова объединить два сегмента в один, но теперь уже на логическом уровне. Для этого необходимо выполнить следующие действия. В настройке «Network Connections», которая находится в панели управления, отображается список установленных сетевых интерфейсов. Удерживая клавишу «Ctrl», отметьте два подключения и затем, вызвав контекстное меню и нажав правую кнопку мыши, выберите раздел «Bridge Connections» («Настройка моста»). После этого произойдет его создание, и в списке подключений появится новое — «Network Bridge» («Сетевой мост») (рис. 1).

Дальнейшие настройки протокола TCP/IP выполняются именно для него. В контекстном меню этого подключения необходимо выбрать раздел «Properties» и в появившемся диалоговом окне в списке «This connection uses the following items» («Компоненты, используемые этим подключением») перейти к свойствам пункта «Internet Protocol (TPC/IP)».

Там необходимо выбрать опцию «Use the following IP address:» («Использовать следующий IP-адрес:») и в появившемся поле ввести адрес, который ранее имел единственный сетевой интерфейс сервера. При переходе к полю «Subnet mask:» («Маска подсети:») оно заполняется автоматически. Подтверждаем свой выбор, нажав «OK» (рис. 2). После успешного проведения этих настроек сервер становится похож на обычный коммутатор. Он будет обрабатывать входящие пакеты следующим образом.

Если пакет приходит из сегмента A и предназначен компьютеру, находящемуся в сегменте A, то такой пакет остается в этом сетевом сегменте.

Если пакет приходит из сегмента A и предназначен компьютеру, находящемуся в сегменте B, он пересылается в сегмент B.

Если из сегмента A приходит широковещательный пакет, он отправляется во все сегменты кроме сегмента A — мост пропускает широковещательные пакеты через себя.

Очевидно, что если широковещательные пакеты составляют сравнительно небольшой процент среди всех обрабатываемых пакетов, в каждом сегменте сети скорость работы увеличивается. В итоге вы получаете при измененной физической структуре сети ту же самую логическую структуру, и при этом нет необходимости выполнять какую-либо конфигурацию протокола IP. Эта возможность построения сетевого моста, появившаяся в Windows Server 2003, представляется очень полезной в описанной ситуации.

И все-таки такой вариант нельзя считать идеальным для любых условий. По мере увеличения размера сегментов и их количества, широковещательные пакеты будут составлять все более значительную долю трафика. Например, если у вас будет 10 сегментов по 50 компьютеров и каждый из них будет посылать широковещательный пакет раз в секунду, то каждый из 500 компьютеров будет 500 раз в секунду получать широковещательный пакет и обрабатывать его.

Маршрутизатор

Скажем, вы бы хотели разделить ваши компьютеры на две IP-сети: 192.168.1.x и 192.168.2.x со стандартной для таких сетей маской. Для этого необходимо изменить IP-адреса компьютеров, оказавшихся во втором сегменте.

Выполнить эту задачу можно разными способами: установить новые адреса вручную или с помощью службы DHCP. Кроме этого необходимо также выбрать адрес для второго сетевого интерфейса сервера. (Причем если до этого использовался мост, необходимо его удалить, после чего станет возможным задавать параметры интерфейсов независимо.) Пусть это будет адрес 192.168.2.200.

Выполнив необходимые настройки, проверьте соединение компьютера C1-1 из сети A с сервером по IP-адресу, используя для этого команду ping. Компьютеры сети A могут обращаться друг к другу, в сети B компьютеры также обращаются к серверу и друг к другу. Сложности возникают при попытке клиента из сети 192.168.1.0 (например компьютера C1-1 с адресом 192.168.1.1) обратиться к клиенту в сети 192.168.2.0 (компьютеру C2-1 с адресом 192.168.2.1). На компьютере C1-1 получаем картину, изображенную на рис. 5. Это сообщение говорит о том, что компьютер C1-1 не определил, куда отправить пакет. Он знает, как отправить пакет компьютерам, расположенным в его сети (192.168.1.x), исходя из своего IP-адреса 192.168.1.1 и маски 255.255.255.0, но не знает, как пакет должен попадать в другие сети. Ему нужен какой-то шлюз, соединяющий его сеть с другими. Таким шлюзом в данной сети будет являться ваш сервер, именно он соединяет сеть 192.168.1.0 и сеть 192.168.2.0. Поэтому его адрес и нужно ввести в поле «Default Gateway:» («Основной шлюз:») в свойствах протокола TCP/IP сетевого подключения на C1-1.

Все, что вы сделали на C1-1, необходимо повторить на компьютере C2-1, ведь теперь он, получив IP-пакет с адресом отправителя (192.168.1.1), должен отправить ответ именно ему. Для этого он должен знать, как его сеть (192.168.2.0) связана с ос- »

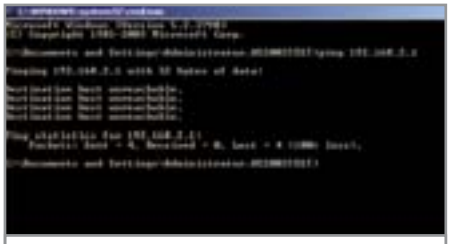


Рис. 5. Попытка компьютера сети A обратится к компьютеру сети B

тальными. А связана она также через ваш сервер, отличие составляет только адрес интерфейса, поэтому в сети 192.168.2.0 шлюзом будет являться 192.168.2.200.

Настроив таким образом оба компьютера, необходимо теперь разобраться и с сервером, который просто не знает о том, что вы хотите использовать его в качестве маршрутизатора. И действительно, для того чтобы использовать сервер в качестве шлюза между сетями, необходимо задействовать службу маршрутизации и удаленного доступа. Включить ее достаточно просто с помощью мастера настройки сервера.

В диалоге «Manage Your Server» («Управление данным сервером») выберите пункт «Add or remove a role» («Добавить или удалить роль») (рис. 3). На экране появляется мастер настройки сервера. После его запуска начнется определение параметров сетевых подключений. В появившемся списке «Server Role» выбираем раздел «Remote Access/VPN Server» («Сервер удаленного доступа или VPN-сервер»). Произойдет запуск мастера установки сервера маршрутизации и удаленного доступа. В списке возможных конфигураций выбираем пункт «Custom configuration» («Особая конфигурация») и после этого в открывшемся окне отмечаем службу «LAN routing» («Маршрутизация ЛВС»). На предложение ОС запустить ее отвечаем утвердительно. На этом мастер настройки сервера заканчивает свою работу (рис. 4). Теперь IP-пакеты отправляются из сети 1 в сеть 2 и обратно.

Маршрутизация IP настраивается достаточно просто. Система Windows Server 2003 сама строит маршруты на основании параметров существующих интерфейсов. Просмотреть сетевые маршруты можно следующими способами.

▸ Набрать в командной строке словосочетание route print.

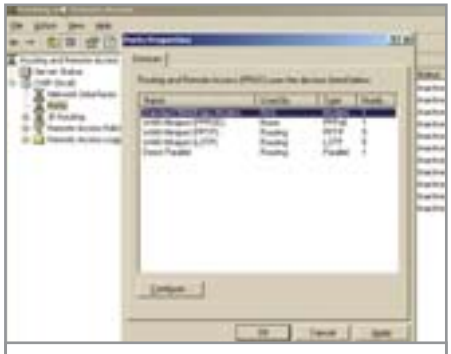


Рис. 6. Устройства используемые службой «Routing and Remote Access»

Рис. 7. Модем будет применяться для установления вызова по требованию

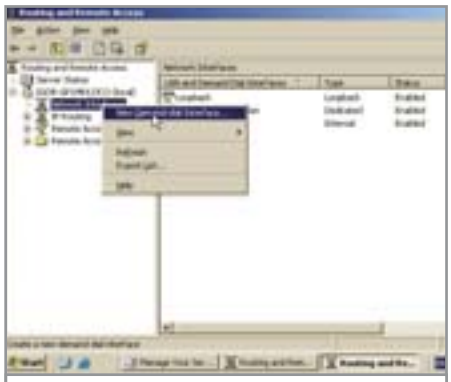


Рис. 8. Создание нового интерфейса вызова по требованию

▸ Выбрать в окне «Manage Your Server» пункт «Manage this remote access/VPN server» («Управление удаленным доступом или VPN-сервером»).В появившейся консоли управления службой маршрутизации выберите свой сервер, затем, «IP Routing → Static Routes» и вызовите контекстное меню. Выберите в меню пункт «Show IP Routing Table...» («Отобразить таблицу IP-маршрутизации...»).

Кажется, что разделение одной IP-сети на две завершено, но это не совсем так. Сложности возникают при попытке компьютера C1-1 из сети A обратиться к компьютеру в сети B по имени. Это говорит о том, что компьютер C1-1 не может выполнить преобразование имени в IP-адрес. И тут пришло время задуматься о том, почему это преобразование работало раньше, когда сеть состояла из одного сегмента, и позже, когда использовался мост. В системе Windows преобразование имен выполняется с помощью двух механизмов: DNS и NetBIOS. Если вы ранее не настраивали DNS, в вашей сети работало преобразование имен через NetBIOS. Оно происходило следующим образом — компьютер, желающий преобразовать имя C2-1 в IP-адрес, посылал широковещательный запрос всем: «Какой компьютер имеет имя C2-1?» Компьютер с таким именем посылал ответ и сообщал в нем свой IP-адрес. Пока сегмент был один или использовался мост, широковещательные пакеты приходили ко всем компьютерам сети, поэтому преобразование имен NetBIOS работало. Теперь же, когда вы построили две различные IP-сети, широковещательный пакет, посланный в сети A, остается в ней: компьютеры в другой сети его не получают, теперь таким способом их имена не могут быть преобразованы в IP-адреса. Если вы используете клиентские компьютеры с системами Windows 95, то для решения возникшей проблемы можно включить на сервере службу WINS, которая будет собирать имена и адреса компьютеров, работающих в каждой из сетей и выполнять преобразование имен в IP-адреса по запросу клиентов. Для современных клиентских операционных систем рекомендуется использовать систему преобразования имен DNS. Выполнив и эти настройки, вы получили сеть организации, состоящую из двух различных IP-сетей, в которой все клиенты могут обращаться к серверу и друг к другу по IP-адресам и именам.

Удаленный доступ

Теперь пришло время подумать о подключении этой сети к Интернету. Для этого понадобится установить необходимое оборудование: модем, ISDN или DSL.

Далее будет рассмотрено подключение с помощью модема, но все описанное в равной мере относится и к другому оборудованию, работающему по протоколу PPP (например ISDN). Если же используется Ethernet-интерфейс, то, с точки зрения Windows, это будет такая же сетевая плата, как и остальные, поэтому настройку удаленного доступа выполнять не требуется и вы можете перейти сразу к следующему разделу «Протокол NAT».

Установите модем на вашем сервере. Настройку подключения с помощью мастера выполнять не нужно. Подключение к Интернету вы проведете, воспользовавшись возможностями системной службы «Routing and Remote Access».

Помимо того что эта служба может маршрутизировать пакеты между разными сегментами сети, она также может выполнять подключение по требованию к другим сетям (в том числе и к Интернету). Это озна-

Рис. 9. Настройка протокола брандмауэра NAT/Basic Firewall

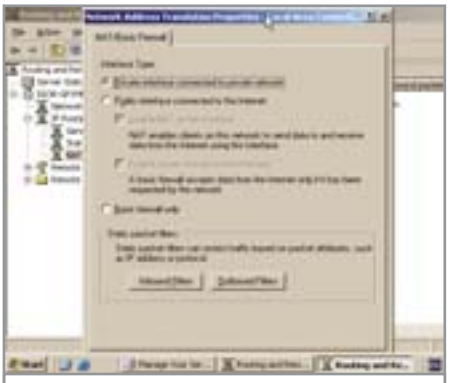


Рис. 10. Режим настройки внутренних интерфейсов

» чает, что служба будет устанавливать заданное соединение по мере необходимости (по запросу ваших клиентов). Кроме этого, если соединение в течение определенного времени не используется, оно может быть разорвано.

Выполните настройку интерфейса подключения к Интернету по требованию следующим образом. В консоли управления службой маршрутизации измените свойства вашего сервера. Для этого на вкладке «General» установите переключатель в положение «LAN and Demand-dial routing». В ответ на предложение перезапустить сервер ответьте утвердительно. Обратите внимание, что в списке доступных модулей сервера маршрутизации появились также «Ports». Просмотрите их свойства. Выберите в появившемся списке установленный модем и нажмите кнопку «Configure» (рис. 6). Учитывая то, что вы хотите использовать модем для установления вызова по требованию, отразите это в настройках (рис. 7). Осталось только определить соответствующий интерфейс по требованию — в контекстном меню «Network Interfaces» выберите пункт «New Demand-dial Interface...» (рис. 8). С помощью мастера создания интерфейса определите необходимые параметры подключения к провайдеру, такие как название интерфейса, тип подключения, используемый адаптер и номера телефонов вашего интернет-провайдера.

Проверьте используемые параметры безопасности (возможно, вам придется использовать незашифрованный пароль для подключения к Сети).

На следующем экране нам необходимо определить маску сети, обслуживаемой вашим интерфейсом. Затем задаются имя и пароль пользователя, которые должны быть назначены провайдером. На этом работа мастера настройки интерфейса вызова по требованию заканчивается.

Теперь, как только вы обратитесь с сервера к внешнему (находящемуся за пределами ваших двух сетей) узлу, служба будет устанавливать соединение с Интернетом автоматически. Вы сможете, находясь на сервере, работать в Интернете, но ваши клиенты по-прежнему не имеют такой возможности. Прежде чем исправить это положение, необходимо определить, каким образом вы подключаетесь к Интернету. Получили ли вы один или несколько реальных IP-адресов или же подключаетесь по dial-up, при этом IP-адрес всего один, и он динамически изменяется от подключения к подключению.

В случае, если провайдер выделил несколько IP-адресов (по числу установленных компьютеров) и вы решили использовать для машин в своей сети реальные IP-адреса, необходимо изменить логическую структуру своей сети. Назначьте каждому компьютеру адрес из выданного диапазона и настройте маршрутизацию — установка дополнительных компонентов на сервер не потребуется.

Протокол NAT

Если же IP-адресов получено меньше, чем компьютеров в сети, вы не сможете выдать каждому ПК реальный IP-адрес. Возможно, для некоторых программ это является серьезным ограничением, но все-таки большинство программ работают не на уровне IP, а выше — с протоколами TCP/UDP. В этих протоколах помимо номера компьютера (IP-адреса) определен также номер порта (16-битное число, связанное в компьютере с определенным сетевым приложением). Пакет, который отправляется одним сетевым приложением другому, помимо адресов отправителя/получателя содержит также и их порты.

Протокол NAT (Network Address Translation), реализованный в службе маршрутизации Windows Server 2003 позволяет «сэкономить» на IP-адресах, учитывая порты передаваемых пакетов. Каждый пакет, который отправляется из внутренней сети во внешнюю, подвергается обработке. NAT-преобразователь заносит адрес/порт компьютера/приложения, отправившего пакет, в свою таблицу (например 192.168.1.1:8019). Кроме этого он выбирает свой свободный порт (например 8139) и также запоминает его в таблице. Затем он заменяет адрес отправителя (из внутренней сети 192.168.1.1) своим реальным адресом (например 1.0.0.1) и порт отправителя (8019) выбранным (8139). Когда вызываемый клиентом узел Интернета возвращает ответ, он возвращает его по внешнему адресу сервера (1.0.0.1:8139). NAT-преобразователь найдет в таблице запись, связанную с данным портом (8139), и перешлет пакет компьютеру/порту, указанному в этой записи (192.168.1.1:8019). Таким образом, с точки зрения клиента, все выглядит прозрачно, его приложения работают так, как они работали бы с реальным IP-адресом.

Помимо того что можно обеспечить выход в Интернет нескольким компьютерам, используя всего один реальный IP-адрес, вы также получаете дополнительную степень защиты. Адреса компьютеров вашей внутренней сети остаются внутри — пока работает NAT-преобразование, подключиться к ним из внешней сети невозможно. Протокол NAT превращает ваш сервер в брандмауэр или межсетевой экран. Теперь сервер разделяет сети, при этом Windows Server 2003 не пропустит через себя пакеты, предназначенные компьютерам во внутренней сети. Иногда все же возникает необходимость открыть доступ к некоторым при- »

Рис. 11. Установка DNS-сервера

» ложениям (портам) в вашей внутренней сети. Например, вы захотите опубликовать веб-сервер, работающий на компьютере во внутренней сети. Для этого вы можете определить статическое преобразование — задать, что обращения к определенному порту (например 80-й порт — веб-сервер) должны направляться к компьютеру, расположенному во внутренней сети (например с адресом 192.168.1.1).

Настроить протокол NAT достаточно просто. Если вы обратите внимание, в списке модулей IP-маршрутизации уже присутствует протокол NAT/Basic Firewall.

Вызовите контекстное меню этого протокола и выберите «New Interface» (рис. 9).

Выберите интерфейс «Internal», в свойствах NAT установите параметры «Public interface connected to the Internet», «Enable NAT on this interface», «Enable a basic firewall on this interface». Если провайдер выдал вам несколько статических адресов, задайте их на вкладке «Address Pool», кроме этого вы можете назначить перенаправление пакетов, предназначенных определенным приложениям, работающим во внутренней сети, на вкладке «Services and Ports». На вкладке «ICMP» вы можете задать, будет ли ваш сервер передавать управляющие и тестирующие сообщения протокола IP. После этого подтвердите свой выбор, нажав кнопку «OK».

Затем добавьте внутренние интерфейсы и отметьте их как «Private interface connected to private network» (рис. 10).

Далее необходимо также настроить клиентов на использование DNS. Это можно сделать, задав адрес, указанный провайдером на каждом из компьютеров в поле «DNS server». Можно использовать службу DNS-сервер, входящую в состав операционной системы Windows Server 2003. Для этого установите ее, воспользовавшись мастером управления вашим сервером. Выберите пункт «Add or remove a role». В списке «Server Role» на этот раз выберите «DNS server» (рис. 11). Дождитесь окончания настройки компонентов Windows (возможно, вам понадобится вставить установочный компакт-диск Windows Server 2003). По окончании установки будет запущен мастер настройки DNS-сервера (рис. 12). Настройку сервера DNS вы проведете вручную. В диалоговом окне «Manage Your Server» выберите ссылку «Manage this DNS server». На экране появляется консоль управления вашим DNS-сервером. Вызовите на экран диалог определения свойств сервера. На его вкладке «Forvarders» укажите адрес DNS-сервера вашего провайдера (рис. 13). Выполнив настройку сервера, установите его адрес в поле «DNS server» в параметрах протокола TCP/IP каждого сетевого клиента.

Рис. 12. Диалоговое окно мастера настройки DNS-сервера

Рис. 13. Указание адреса DNS-сервера интернет-провайдера

Результаты работы

В итоге вы получили работающую IP-сеть, состоящую из нескольких физических сегментов, в которой каждый клиент может обращаться к серверу, соседним компьютерам и к серверам в сети Интернет. Для этого вам понадобилось только обычное сетевое оборудование: недорогие сетевые платы, коммутаторы/концентраторы, модем или ISDN/DSL и всего один сервер, работающий под управлением Windows Server 2003. Удобный интуитивно понятный интерфейс различных мастеров Windows Server 2003, предоставляет системному администратору эффективный механизм для развертывания сети и управления объединими компьютерами. ■ ■ ■ Александр Лахин

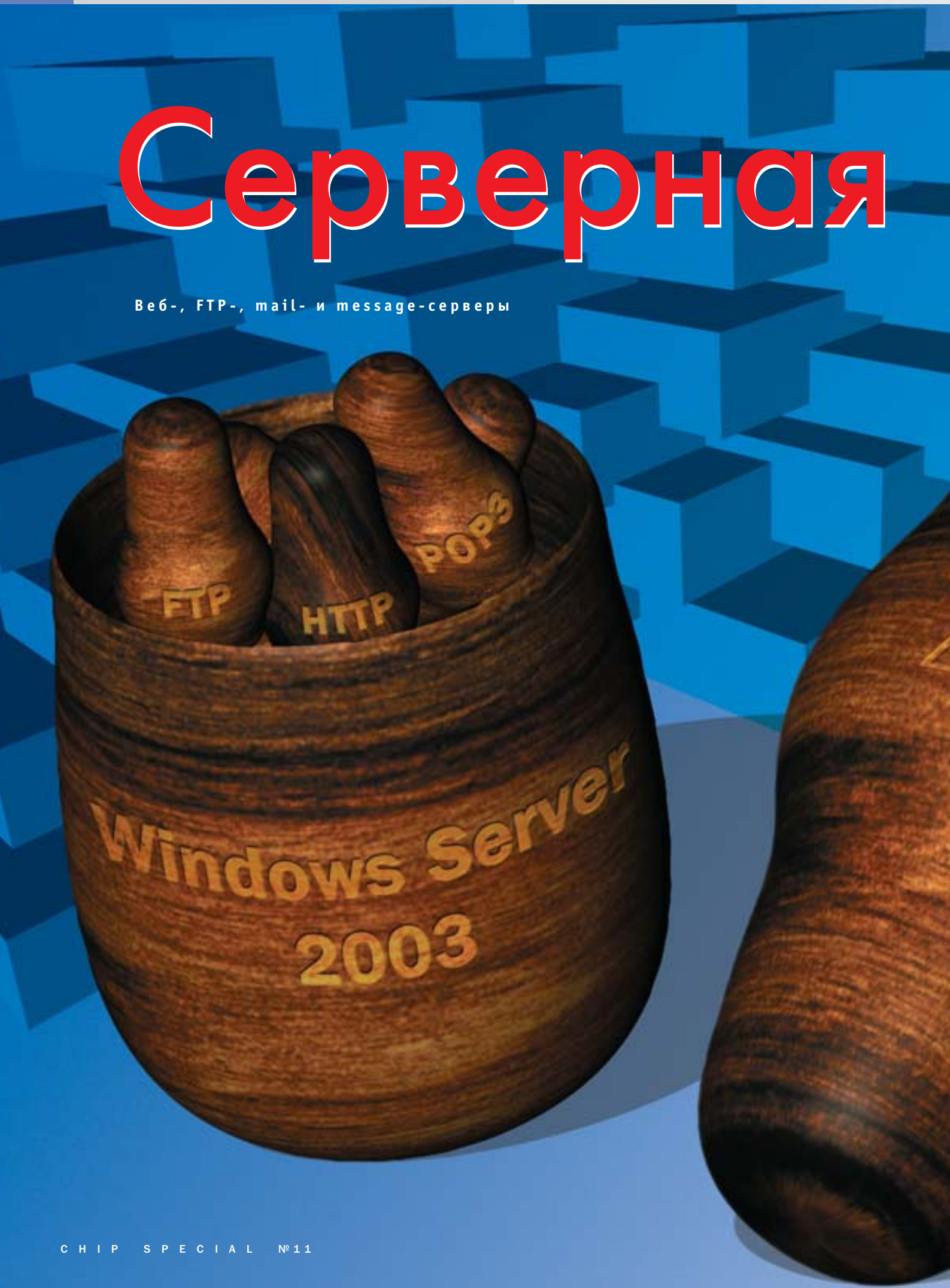
Прокси-серверы

Дальнейшее развитие

Вы можете продолжить развитие вашей сети, если внедрите в ней HTTP-прокси-сервер. У вашей сегодняшней сети есть определенные недостатки. Во-первых, если один пользователь обращается в Интернет за страницей www.ipaddress.org, а через несколько минут за ней обратится другой пользователь, то его компьютер будет снова устанавливать соединение с соответствующим веб-узлом и загружать эту страницу. В результате вы будете оплачивать многократную загрузку одних и тех же данных, а вместе с этим снизится скорость использования Интернета другими пользователями. Во-вторых, вы не можете гибко ограничивать посещение вашими пользователями сайтов сомнительного содержания. Проблемы эти нельзя решить используя только протокол NAT, так как он работает на уровне TCP и UDP, а вам нужно оперировать с понятиями «веб-страница» и «веб-сервер». А они существуют на уровне HTTP. Эти проблемы поможет решить кэширующий HTTP-прокси-сервер. В состав Windows Server 2003 не входит встроенный HTTP-прокси-сервер, но можно использовать дополнительные программные продукты: Internet Security and Acceleration server от Microsoft (www.microsoft.com/ISAServer/) или Winroute Firewall, пришедший на замену WinGate от компании DeerField (www.deerfield.com/products/winroute-firewall/). Если вы решите использовать один из множества доступных кэширующих HTTP-прокси-серверов, он будет заносить загруженные из Интернета веб-страницы в собственный кэш. При повторном обращении клиентов к тем же страницам он выдаст их из своего кэша, что приведет к значительному увеличению скорости загрузки веб-содержимого. Помимо этого вы можете гибко ограничивать количество сайтов, посещаемых вашими пользователями, воспользовавшись фильтрами.

Серверная

Веб-, FTP-, mail- и message-серверы



Управление ролями w2k3 осуществляется удобно и просто

Перед настройкой роли производится диагностика сетевых соединений

W2k3-сервер способен «играть» самые разнообразные роли

» ложение, то не беспокойтесь. Откройте стартовое меню, выберите в нем «Administrative Tools», после чего в выпавшем меню выберите «Manage Your Server».

После выбора пункта «Add or remove a role» («Добавить или удалить роль») сначала появится окно диагностики сетевых соединений и проверки настроек имеющихся служб.

Затем можно выбрать, какую именно роль необходимо добавить. При этом для каждой роли показывается краткое описание и дается ссылка на раздел помощи, в котором говорится об особенностях настройки той или иной службы, включая вопросы обеспечения безопасности.

В дальнейшем для добавления новой роли или настройки уже работающих служб мы будет использовать приложение Manage Your Server.

Веб-сервер своими руками

Использование продуктов линейки Windows Server 2000/2003 в качестве веб-серверов является весьма распространенной практикой. Многим по большому счету даже не нужны другие возможности w2k3, такие как, скажем, сервер приложений или контроллер домена Active Directory. По этой причине Microsoft даже выпустила отдельный вариант серверной операционной системы w2k3 — Web Server Edition. При использовании этого варианта многим законопослушным системным администраторам не придется переплачивать за полнофункциональную версию w2k3, возможности которой они все равно полностью не используют.

Мастер на все руки

Internet Information Services (IIS) 6.0 является полноценным многофункциональным сервером. Он был в значительной степени оптимизирован для выполнения веб-приложений, работы служб в изолированных средах, для увеличения пропускной способности и обеспечения масштабируемости при использовании на многопроцессорных платформах. IIS может изолировать отдельное веб-приложение или несколько сайтов в рамках одного процесса, взаимодействующего непосредственно с ядром ОС. Такой подход не позволяет одному приложению или сайту нарушить работу других веб-служб или приложений на сервере.

Кроме того, IIS предоставляет возможности мониторинга состояния, благодаря чему можно локализовать, диагностировать и предотвращать нарушения работы веб-приложения.

Для повышения уровня безопасности, являющейся важным аспектом нормальной работы любого веб-сервера, IIS 6.0 предусматривает значительное количество превентивных мер, которые должны защитить веб-сервер от множества распространенных типов атак.

При помощи IIS Manager, сценариев администрирования или непосредственного редактирования конфигурационного файла IIS, хранящегося в формате XML, можно с легкостью настроить IIS для решения конкретных задач и выполнения требуемых сценариев.

Умения и навыки IIS

W2k3 вместе с IIS 6.0 представляет надежную платформу, благодаря которой возможно следующее:

- создавать масштабируемые серверные конфигурации, отвечающие современным требованиям;
- разрабатывать нетривиальные веб-приложения;
- публиковать информацию в локальных сетях и Интернете;
- получать доступ к базам данных, необходимым для создания среды, ориентированной на данные;
- разрабатывать веб-сайты, от персональной страницы до полномасштабного веб-сервера предприятия.

Установка IIS

Для того чтобы установить IIS и отдельные его компоненты, можно воспользоваться апплетом «Add or Remove Programs» («Установка и удаление программ») панели управления. В перечне устанавливаемых компонентов Windows компоненты IIS выбираются в списке «Application Server» («Сервер приложений»). С другой стороны, можно воспользоваться и приложением Manage Your Server.

Особое внимание следует обратить на дополнительные компоненты сервиса World Wide Web («Application Server → Details → Internet Information Service → Details → World Wide Web Service → Details»), такие как Active Server Pages и Remote Administration (HTML), которые в дальнейшем могут использоваться для работы и удаленной настройки сервера.

Стандартные каталоги

При установке IIS использует следующие каталоги:

- \Inetpub
- \%SystemRoot%\Help\iisHelp
- \%SystemRoot%\system32\inetsrv

Изменить положение этих каталогов нельзя, хотя во время установки можно с помощью файла ответов, используемого на этом этапе, задать местонахождение каталогов wwwroot и ftproot. При деинсталляции IIS каталог iisHelp будет »

Управление ролями w2k3 осуществляется удобно и просто

Перед настройкой роли производится диагностика сетевых соединений

W2k3-сервер способен «играть» самые разнообразные роли

» ложение, то не беспокойтесь. Откройте стартовое меню, выберите в нем «Administrative Tools», после чего в выпавшем меню выберите «Manage Your Server».

После выбора пункта «Add or remove a role» («Добавить или удалить роль») сначала появится окно диагностики сетевых соединений и проверки настроек имеющихся служб.

Затем можно выбрать, какую именно роль необходимо добавить. При этом для каждой роли показывается краткое описание и дается ссылка на раздел помощи, в котором говорится об особенностях настройки той или иной службы, включая вопросы обеспечения безопасности.

В дальнейшем для добавления новой роли или настройки уже работающих служб мы будет использовать приложение Manage Your Server.

Веб-сервер своими руками

Использование продуктов линейки Windows Server 2000/2003 в качестве веб-серверов является весьма распространенной практикой. Многим по большому счету даже не нужны другие возможности w2k3, такие как, скажем, сервер приложений или контроллер домена Active Directory. По этой причине Microsoft даже выпустила отдельный вариант серверной операционной системы w2k3 — Web Server Edition. При использовании этого варианта многим законопослушным системным администраторам не придется переплачивать за полнофункциональную версию w2k3, возможности которой они все равно полностью не используют.

Мастер на все руки

Internet Information Services (IIS) 6.0 является полноценным многофункциональным сервером. Он был в значительной степени оптимизирован для выполнения веб-приложений, работы служб в изолированных средах, для увеличения пропускной способности и обеспечения масштабируемости при использовании на многопроцессорных платформах. IIS может изолировать отдельное веб-приложение или несколько сайтов в рамках одного процесса, взаимодействующего непосредственно с ядром ОС. Такой подход не позволяет одному приложению или сайту нарушить работу других веб-служб или приложений на сервере.

Кроме того, IIS предоставляет возможности мониторинга состояния, благодаря чему можно локализовать, диагностировать и предотвращать нарушения работы веб-приложения.

Для повышения уровня безопасности, являющейся важным аспектом нормальной работы любого веб-сервера, IIS 6.0 предусматривает значительное количество превентивных мер, которые должны защитить веб-сервер от множества распространенных типов атак.

При помощи IIS Manager, сценариев администрирования или непосредственного редактирования конфигурационного файла IIS, хранящегося в формате XML, можно с легкостью настроить IIS для решения конкретных задач и выполнения требуемых сценариев.

Умения и навыки IIS

W2k3 вместе с IIS 6.0 представляет надежную платформу, благодаря которой возможно следующее:

- создавать масштабируемые серверные конфигурации, отвечающие современным требованиям;
- разрабатывать нетривиальные веб-приложения;
- публиковать информацию в локальных сетях и Интернете;
- получать доступ к базам данных, необходимым для создания среды, ориентированной на данные;
- разрабатывать веб-сайты, от персональной страницы до полномасштабного веб-сервера предприятия.

Установка IIS

Для того чтобы установить IIS и отдельные его компоненты, можно воспользоваться апплетом «Add or Remove Programs» («Установка и удаление программ») панели управления. В перечне устанавливаемых компонентов Windows компоненты IIS выбираются в списке «Application Server» («Сервер приложений»). С другой стороны, можно воспользоваться и приложением Manage Your Server.

Особое внимание следует обратить на дополнительные компоненты сервиса World Wide Web («Application Server → Details → Internet Information Service → Details → World Wide Web Service → Details»), такие как Active Server Pages и Remote Administration (HTML), которые в дальнейшем могут использоваться для работы и удаленной настройки сервера.

Стандартные каталоги

При установке IIS использует следующие каталоги:

- \Inetpub
- \%SystemRoot%\Help\iisHelp
- \%SystemRoot%\system32\inetsrv

Изменить положение этих каталогов нельзя, хотя во время установки можно с помощью файла ответов, используемого на этом этапе, задать местонахождение каталогов wwwroot и ftproot. При деинсталляции IIS каталог iisHelp будет »

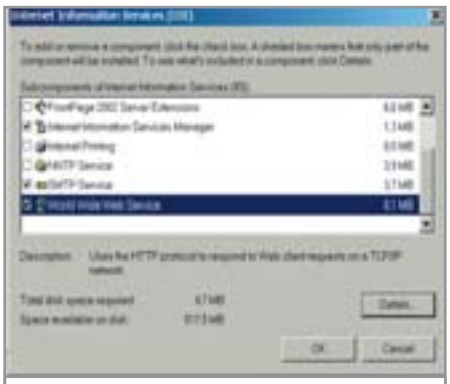
» удален, а каталоги Inetpub и inetsrv останутся на компьютере.

Дополнительные компоненты IIS

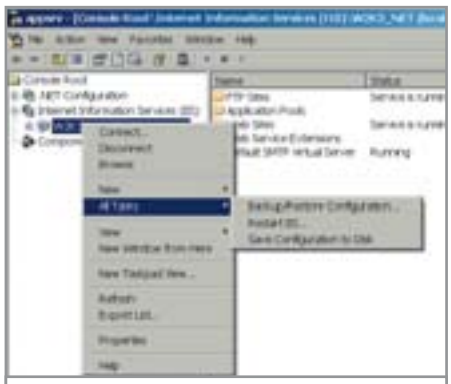
IIS включает множество дополнительных компонентов, которые можно установить или удалить с помощью апплета «Add or Remove Programs» панели управления. Ниже будет рассмотрено назначение этих компонентов и их влияние на функциональность IIS. Файлы для компонентов Active Server Pages, Internet Data Connector, Server Side Includes и WebDav при установке w2k3 с нуля копируются на компьютер, но сами компоненты по умолчанию отключены. При установке w2k3 в качестве обновления все компоненты IIS по умолчанию будут включены.

BITS Server Extensions

BITS (Background Intelligent Transfer Service) является механизмом фоновой передачи данных и управления очередями. BITS минимизирует файловые запросы для увеличения пропускной способности и уменьшения времени отклика сервера. Установка BITS позволяет обеспечивать на веб-сервере необходимый уровень качества обслуживания (Quality of Service, QoS).



Список дополнительных компонентов Internet Information Services



Manager позволяет удобно и наглядно управлять работой сервера IIS

Common Files

В целях повышения уровня безопасности веб-сервера возможно отключить установку некоторых общих файлов, однако если сделать это, то IIS не будет установлен вовсе. Поэтому при инсталляции IIS разрешите установку этого компонента и при необходимости ограничить перечень служб и сервисов отключите их в списке «Common Files».

File Transfer Protocol (FTP) Server

Протокол FTP используется для обмена файлами с удаленными компьютерами. В рамках наших задач — обустройства локальной сети — настоятельно рекомендуется установить этот компонент. Его использование позволит организовать обмен файлами на сервере без необходимости идти на компромиссы в обеспечении безопасности, на которые почти наверняка пришлось бы пойти при использовании для этих целей w2k3 в качестве файл-сервера.

FrontPage 2002 Server Extensions

Данный компонент позволяет просматривать и редактировать содержимое веб-сайта. При помощи этой программы можно не только быстро создавать сайты на своем сервере, но также создавать, редактировать и размещать веб-страницы на IIS удаленного сервера. Если компонент FrontPage 2002 Server Extensions не будет установлен, то копировать файлы веб-сайта и изменять его настройки придется вручную.

IIS Manager

IIS Manager является графическим интерфейсом для администрирования веб-сервера. Без использования данного компонента осуществлять управление веб-сервером можно, но для этого придется использовать скрипты, которые в свою очередь используют IIS API для создания сайтов, настройки приложений, виртуальных директорий, а также параметров безопасности.

NNTP Service

Протокол NNTP используется для распространения новостных рассылок между серверами новостей и NNTP-клиентами. Если компьютер не планируется использовать в качестве news-сервера, устанавливать этот компонент не следует.

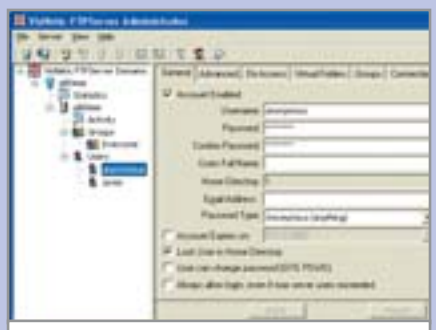
SMTP Service

Протокол SMTP можно использовать для организации почтового интранет-сервера. Этот компонент также будет установлен при инсталляции службы POP3 из компонентов w2k3 e-mail services. »

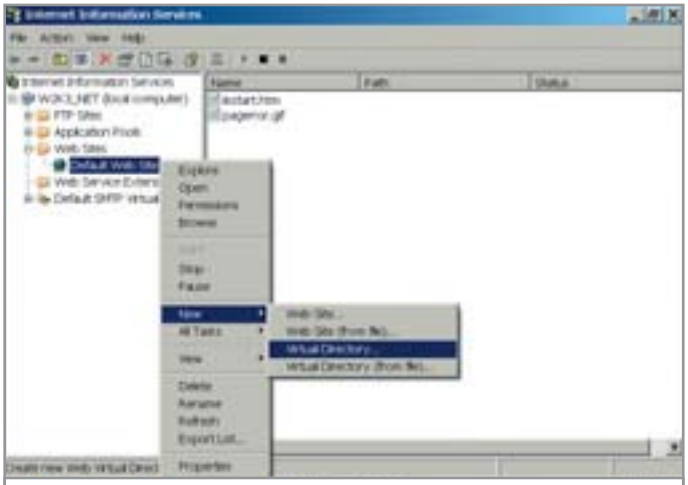
Альтернативы IIS

Веб- и FTP-серверы сторонних фирм

При всей своей распространенности IIS, несомненно, является не единственным доступным веб- и FTP-сервером. Одно из главных преимуществ IIS — возможность его работы в тесной интеграции с другими службами w2k3, такими как Active Directory. Однако, возможно, в некоторых случаях более предпочтительным окажется использование продуктов сторонних фирм или так называемых облегченных решений. Среди веб-серверов можно назвать Apache, который, не будучи облегченным, куда более компактен, чем IIS (www.apache.org), TinyWeb (www.ritlabs.com/tinyweb), Abyss Web Server (http://abyss.sourceforge.net). Из наиболее распространенных FTP-серверов для Windows можно отметить Serv-U (www.serv-u.com), WarFtp (www.jgaa.com/index.php?menu=154), VisNetic Ftp Server (www.deerfield.com/products/visnetic_ftpserver). Обладая всеми необходимыми функциями для организации удобного и безопасного FTP-сервера, они весьма компактны. Установить и настроить их довольно просто.



Альтернативные FTP-серверы обладают полной функциональностью



Создание новой виртуальной директории для хранения данных веб-сервера при помощи программы IIS Manager

Опубликование каталога с веб-страницами легко и просто осуществить с помощью Проводника

» **World Wide Web Publishing Service**

Этот компонент должен быть установлен для выполнения IIS его основной функции — работы в качестве веб-сервера. World Wide Web Publishing Service включает следующие подкомпоненты:

- Active Server Pages — без данного компонента невозможно будет использование на сервере ASP-страниц.
- Internet Data Connector — этот компонент необходим для возможности обработки файлов .idc, которые используются в IIS для указания источников данных ODBC, имен пользователей, шаблонов и операторов SQL для обмена данными с базами данных.
- Remote Administration (HTML) — интерфейс удаленного администрирования для IIS. Использовать этот компонент следует осторожно и, пожалуй, в целях безопасности не стоит его устанавливать, если нет острой необходимости удаленно администрировать свой сервер.
- Remote Desktop Web Connection — это компонент ActiveX для удаленного администрирования. Соображения относительно необходимости его установки аналогичны предыдущему пункту.
- Server Side Include — данный компонент необходим для корректного отображения файлов .shtm, .shtml и .stm, которые используются для того, чтобы собирать страницы из готовых частей и вставлять в них результаты работы различных скриптов.
- WebDAV Publishing. Служба Web Distributed Authoring and Versioning (WebDAV) во многом схожа с FTP, однако может обеспечить защиту при помощи пароля и шифрование при пересылке данных на веб-сервер посредством SSL.
- World Wide Web Service — без этой службы IIS не сможет предоставлять доступ к веб-сайтам.

Настройка веб-сайтов

Для опубликования веб-страниц на сервере существует два основных варианта: задать еще одну директорию в рамках веб-сайта по умолчанию или же создать дополнительный веб-сайт, который будет доступен на отдельном IP-адресе и порте.

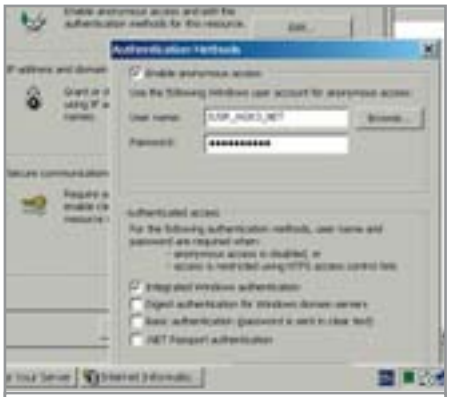
Для опубликования каталога на уже имеющемся сайте можно создать новую виртуальную директорию либо непосредственно в IIS Manager, либо просто в свойствах каталога в Проводнике Windows выбрать соответствующую опцию на вкладке «Web Sharing».

При этом необходимо учесть два важных момента. Во-первых, права доступа на каталог должны быть выставлены на чтение для «Everyone» (всех), в противном случае будет невозможен анонимный доступ к этому виртуальному каталогу — веб-сервер затребует авторизацию. Во-вторых, при опубликовании каталога с помощью Проводника анонимный доступ к каталогу по умолчанию выключен, и необходимо включить его явно. Для этого надо в свойствах виртуального каталога в IIS Manager выбрать вкладку «Directory Security», затем в группе «Authentication and Access Control» нажать кнопку «Edit» и установить флажок «Enable anonymous access». Ярлык для запуска самого IIS Manager можно найти в группе «Администрирование» панели управления.

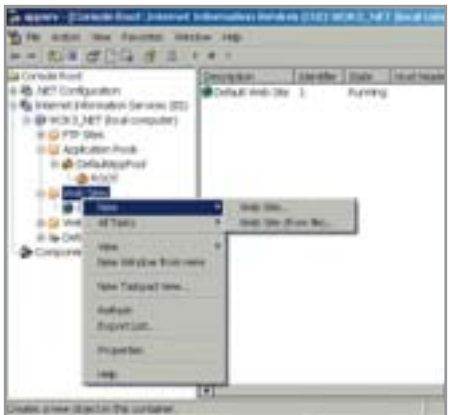
Создать новый веб-сайт с помощью IIS Manager совсем не сложно, поэтому мы не будем подробно на этом останавливаться.

После его создания следует выбрать IP-адрес сервера и порт, который будет использоваться для доступа к сайту. Затем необходимо указать местонахождение файлов страниц, составляющих сайт (Home Directory), а также параметры безопасности и, возможно, используемые ISAPI-фильтры.

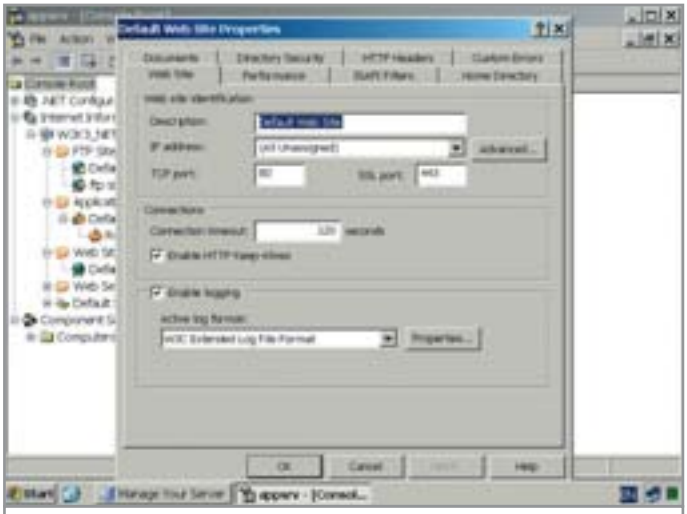
Созданный веб-сайт будет доступен сразу же по завершении его настройки. »



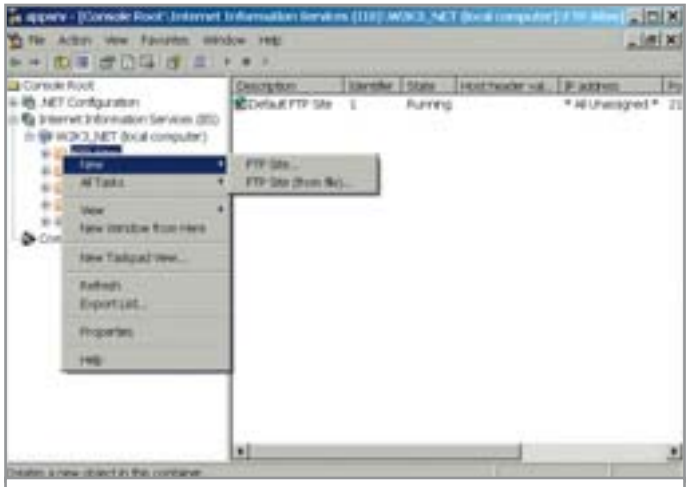
При опубликовании каталога с помощью Проводника анонимный доступ необходимо разрешить явно



IIS позволят организовать несколько виртуальных веб-сайтов



Настройка нового веб-сайта, созданного средствами IIS



Вы можете организовать несколько FTP-сайтов, которые будут размещены на одном физическом сервере

» Для создания и оформления его содержимого вы можете воспользоваться программами для верстки сайтов, например Microsoft FrontPage.

Настройка FTP-сервера

В целом настройка FTP-сервера очень напоминает настройку веб-сервера. Здесь так же можно помимо структуры каталогов в \Inetpub\ftproot задать еще и виртуальные каталоги, кроме того, компонент IIS FTP Service позволяет организовать на одном физическом сервере несколько FTP-сайтов, которые будут представляться как различные виртуальные FTP-серверы. Для этого необходимо запустить IIS Manager через ярлык в папке «Администрирование» панели управления и из контекстного меню группы «FTP Sites» выбрать пункт «New → FTP Site».

При создании FTP-сайта одним из важных параметров является уровень изоляции пользователей, от его настройки зависит, смогут ли пользователи заходить в домашние каталоги других пользователей. Кроме того, IIS позволяет указать уровень доступа пользователей ко всему сайту на чтение или запись.

В настройках FTP-сайта можно задать ряд дополнительных параметров, таких как положение каталога с содержимым FTP-сайта, уровень доступа к отдельным подкаталогам, сообщения, выдаваемые пользователям при входе и выходе с FTP-сайта и т. д.

Особенно важно обратить внимание на настройки, доступные на вкладке «FTP Site» свойств FTP-сайта. Здесь, в частности, задается IP-адрес сервера и порт, на котором будет доступен FTP-сервер с этим сайтом. Само собой разумеется, что несколько FTP-сайтов не могут использовать один и тот же IP-адрес и порт.

В свойствах FTP-сайта задаются основные его параметры: расположение на диске, уровень доступа к каталогам и т. д.

Настраиваем почтовый сервер

Одним из наиболее используемых в компьютерных сетях сервисов является электронная почта. Появившаяся практически одновременно с сетями, она стала незаменимым средством общения и пересылки различных данных. В локальных компьютерных сетях почта также широко используется в системном администрировании для отправки разного рода отчетов, уведомлений, справок и т. п.

Если рассматривать небольшую сеть компьютеров в рамках одного района города, то и здесь электронная почта будет небесполезна, с ее помощью можно организовывать разного рода информационные рассылки, а также обеспечивать связь поль- »

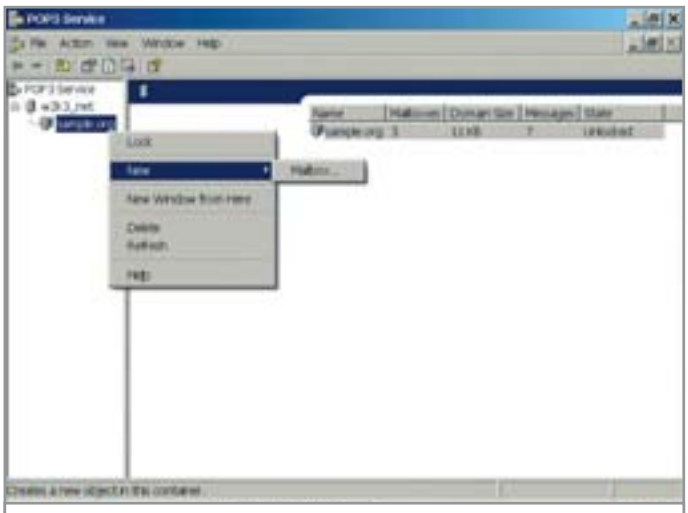
Альтернативная почта

Конкуренты не дремлют

Служба POP3, входящая в состав w2k3, позволяет довольно легко организовать почтовый сервер почти любого масштаба: от домашнего сервера на нескольких пользователей с интеграцией в Active Directory до массовой почтовой службы с хранением зашифрованных паролей и распределением пользователей по нескольким почтовым доменам. Но весьма вероятно, что у кого-то окажутся специфические условия, в которых более удобным будет почтовый сервер с несколько иной функциональной направленностью.

Альтернатив предостаточно. Microsoft Exchange Server 2000/2003 — средство построения систем обмена информацией уровня большого предприятия. Можно отметить Kerio Mail Server (www.kerio.com/kms_home.html), полностью интегрирующийся с Active Directory, но обладающий при этом рядом дополнительных возможностей, среди которых поддержка SMTP-аутентификации, черных списков спамеров, система фильтрации писем, антивирусная защита, удобный веб-интерфейс и многое другое. Нельзя не отметить такой почтовый сервер, как MDaemon (www.altn.com), обладающий гибкими средствами маршрутизации и фильтрации почты, а также поддержкой протоколов безопасного подключения.

Управление почтовым сервером POP3



Создание почтовых ящиков для пользователей

зователей друг с другом в условиях, когда непосредственное общение, скажем, в чате по тем или иным причинам невозможно.

POP3 + SMTP = почтовая система

Для работы электронной почты в w2k3 используется сервис POP3, обеспечивающий получение пользователями сообщений с почтового сервера, а также хранение и управления почтовыми учетными записями на сервере. Для отправки сообщений и для их передачи от сервера к серверу используется сервис SMTP, который устанавливается как часть почтового сервиса вместе с POP3-сервисом.

Система доставки электронной почты работает по определенному протоколу и позволяет в соответствии с определенным протоколом скачивать почтовые сообщения с сервера на локальный компьютер пользователя. Сервис POP3 в качестве такового использует, как можно было предположить, протокол POP3, контролирующий сеанс связи между POP3-клиентом и почтовым сервером, на котором хранятся сообщения.

Службу POP3 можно установить через пункт «Add or Remove Programs» в Панели управления

При администрировании работы сервиса POP3 приходится управлять его действиями на трех организационных уровнях: на уровне почтовых серверов, почтовых доменов, а также отдельных почтовых ящиков. Почтовым сервером является компьютер, на котором установлен сервис POP3 и с которым соединяются пользователи для получения почты (например w2k3net.sample.org).

Почтовый домен должен быть зарегистрирован как доменное имя, интернет-провайдер должен создать MX-запись (Mail eXchange). Впрочем, если предполагается пересылка почты лишь в рамках небольшой локальной сети, то это правило соблюдать необязательно. Каждому пользователю, входящему в домен, принадлежит почтовый ящик (например user@ sample.org), который соответствует каталогу в почтовом хранилище, в котором находятся письма до момента их получения.

Почтовое хранилище

Под почтовым хранилищем понимается каталог, в котором сервис POP3 хранит всю почту до того, как пользователи заберут ее с помощью почтовых клиентов.

В общем случае структура почтового хранилища может быть следующей. На локальном диске выделяется каталог для хранения почтовых сообщений. При создании почтового домена служба POP3 делает в каталоге почтового хранилища соответствующий подкаталог. Для каждого пользователя из определенного почтового домена создается подкаталог в каталоге, созданном для этого домена. Каждое почтовое сообщение, адресованное пользователю, сохраняется в подкаталоге пользователя в виде отдельного файла до тех пор, пока пользователь не получит это сообщение с помощью почтовой программы-клиента.

К примеру, полный путь к файлу с сообщением, полученным по электронной почте, может быть таким: C:\inetpub\mailroot\mailbox\sample.org \P3_username.mbx\P865341.eml

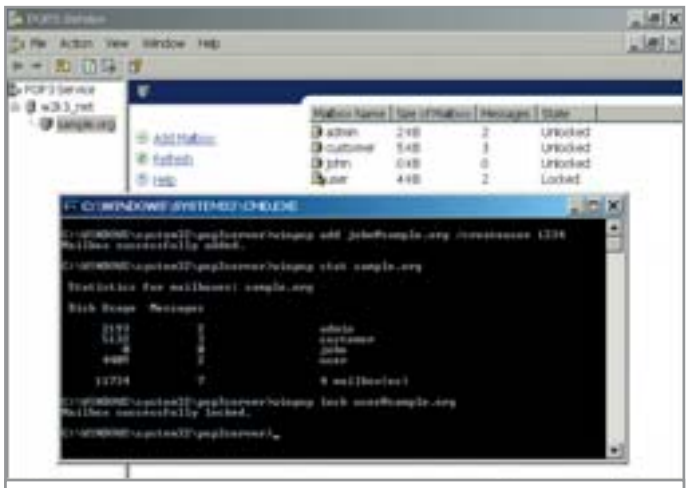
Здесь mailroot соответствует каталогу хранилища сообщений, sample.org является директорией почтового домена, P3_username.mbx — директория почтового ящика пользователя username, а P865341.eml — отдельное сохраненное сообщение.

Права на доступ к файлам и подкаталогам в почтовом хранилище одинаковы для каждого подкаталога. При настройке хранилища права на доступ к его подкаталогам даются только для локальных и доменных администраторов, а также учетной записи «Network Service», под которой запускается служба POP3. Никаким другим пользователям прав доступа к почтовому хранилищу не предоставляется.

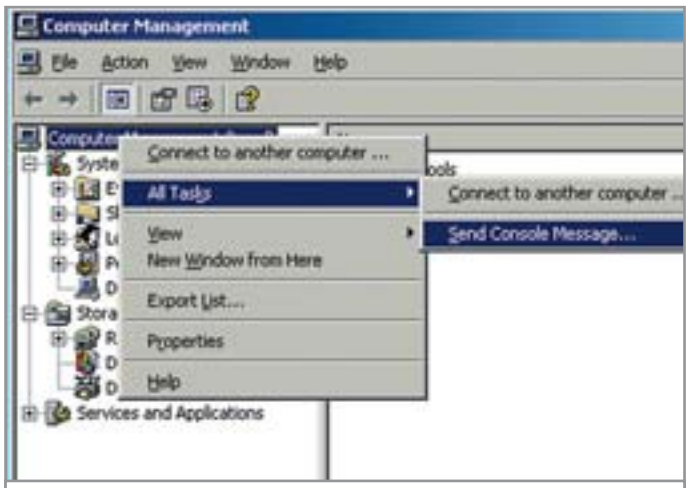
Устанавливаем почту

Итак, после многочисленных приготовлений и разбирательств пришла пора заняться делом. Начать следует с установки служб POP3 и SMTP. Добавить POP3 можно через пункт «Add/Remove Windows Components» апплета панели управления «Add or Remove Programs». При выборе службы POP3 служба SMTP будет также автоматически выбрана.

При этом на первых порах следует воздержаться от использования средств администрирования через веб-интерфейс. Ис-



При использовании консольной winpop доступны все возможности по администрированию POP3-сервера



При помощи встроенного сервиса Messenger пользователи могут обмениваться короткими сообщениями

» пользование этого интерфейса без должной настройки сопряжено с рядом возможных брешей в системе безопасности, кроме того, мы исходим из предположения, что администрируем пока только один сервер, на котором работаем в качестве локального пользователя, так что удаленный доступ через веб-интерфейс здесь избыточен.

Последние штрихи

После добавления роли почтового сервера внешний виде окна приложения Manage This Server несколько изменится — теперь здесь будет значиться роль «Mail Server (POP3)» и будет доступен пункт для управления созданным сервером.

В апплете управления сервисом POP3 (его можно запустить через ярлык «POP3 Service» из группы «Administrative Tools») следует перед созданием почтового домена сразу определиться, какой тип аутентификации будет использоваться, поскольку в дальнейшем смена типа аутентификации будет сопряжена с большими трудностями.

После создания необходимых почтовых доменов можно создать пользовательские почтовые ящики. При этом если для сервера выбрана опция «Always create an associated user for new mailboxes» («Всегда создавать для новых почтовых ящиков соответствующего пользователя»), то соответствующие пользователи будут создаваться в списке локальных пользователей на сервере, где работает служба POP3.

На этом настройку почтовой системы можно считать законченной. Для полноты картины следует отметить, что в состав стандартного почтового POP3-сервера w2k3 входит также консольная утилита winpop. Возможно, имена она придется по вкусу тем, кто привык работать с командной строкой, так как winpop позволяет осуществлять более тонкую настройку.

Службы общения

Не менее важными, нежели веб-, FTP- и почтовые сервисы, являются службы, предоставляющие возможность непосредственного общения в сети с помощью коротких сообщений. В этих случаях можно организовать либо чат-сервер, либо IM-сервер. Главное, чтобы все пользователи могли легко установить и настроить соответствующие клиентские программы.

В стандартной поставке w2k3, к сожалению, нет IM-сервера, есть лишь служба сообщений Messenger. Эта служба позволяет посылать уведомления на компьютеры под управлением Windows 2000/XP. Однако в отличие от Instant Message-сервера она предназначена скорее для экстренных случаев, нежели для повседневного общения. Фактически эта служба является оболочкой над командой net send и используется администраторами сети для оповещения пользователей о необходимости производства каких-либо действий.

Из простых чат-клиентов в рамках сети можно отметить Intranet Chat (http://vnalex.tripod.com), а также Friendly Chat (www.kilievich.com/rus/fchat/). Обе программы позволяют организовать общение без использования дополнительных серверных компонентов (хотя для Intranet Chat существует серверный вариант, позволяющий объединить несколько подсетей). Friendly Chat обладает куда более привлекательным интерфейсом и большими возможностями, хотя его настройка значительно сложнее.

В качестве чат-сервера можно использовать один из вариантов реализации jabber-протокола (www.jabber.org). Jabber является набором потоковых протоколов на основе XML и технологий, позволяющих любым объектам в Интернете обмениваться сообщениями, данными о своем состоянии и другой структурированной информацией почти в режиме реального времени. Существует множество реализаций этого протокола как для серверов, так и клиентов, в частности есть jabber-плагин для весьма популярного IM-клиента Miranda (www.miranda-im.org). В крайнем случае можно воспользоваться бесплатным сервером ICQ Groupware — проектом разработчика программы ICQ фирмы Mirabilis, купленной впоследствии America OnLine.

Заключение

Итак, Windows Server 2003 предоставляет богатые возможности по удобной реализации в рамках локальной сети многочисленных служб: веб- и FTP-сервера, электронной почты, файлового сервера и многих других, о которых уже было сказано. Вместе с тем некоторых сервисов, таких, например, как обмен короткими сообщениями, в w2k3 нет, и в этих случаях приходится искать и использовать сторонние разработки. Но, как бы то ни было, широкие возможности w2k3 делают эту платформу весьма привлекательной для использования, в частности в небольших сетях, где основные службы требуется реализовать быстро, надежно и просто.

■ ■ ■ Денис Патраков

Защитники сервера

За «огненной стеной»

Когда мы начинаем думать о защите сети, первое что приходит в голову — это слово firewall, которое в русском варианте звучит менее благозвучно — «брандмауэр». Действительно, от этого продукта, который может быть и программой и железом, зависит, насколько хорошо сеть будет защищена.

Брандмауэр является той «огненной стеной», которая будет ограждать вас от вредного воздействия окружающей среды под названием Интернет. На сегодняшний день на рынке существует огромное количество продуктов, выполняющих функции firewall. Стоимость таких решений может быть равна нулю (например, цена ICF, входящего в состав Windows Server 2003, включена в стоимость операционной системы), а может составлять и десятки тысяч долларов. Для того чтобы разобраться в этом многообразии продуктов и сделать правильный выбор, необходимо сначала кратко ознакомиться с теорией сетевого взаимодействия и выяснить, от чего же мы все-таки должны защищаться.

Эшелонированная оборона

Для того чтобы производители сетевого оборудования и программного обеспечения для него могли общаться на одном языке и обеспечивать совместимость своих устройств, была разработана так называемая модель OSI (Open System Interconnection). Она содержит семь уровней, каждый из которых обеспечивает выполнение определенной части сетевых функций при обмене данными в сети.

В процессе обмена информацией между двумя компьютерами задействованы все семь уровней этой модели, однако реализовано это таким образом, что протокол одного уровня не подозревает о существовании протоколов другого уровня. Например, протокол четвертого уровня передающей станции взаимодействует с протоколом только четвертого уровня приемной станции и т. д. Разбиение всего порядка взаимодействия на отдельные уровни дает разработчикам возможность заниматься реализацией каждого уровня независимо.

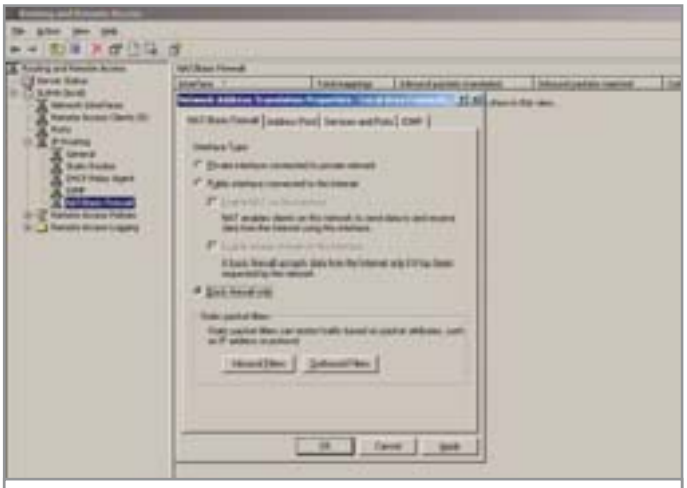
Например, производители сетевых карт не обязаны знать, какие программы будут обмениваться данными между собой, а производители кабельной продукции катего- »

рии 5 уверены, что по их кабелю будет идти трафик, сгенерированный любой сетевой картой, поддерживающей стандарт Ethernet. Знание уровней данной модели необходимо и при понимании стратегии защиты локальной сети, поэтому кратко рассмотрим эти семь уровней.

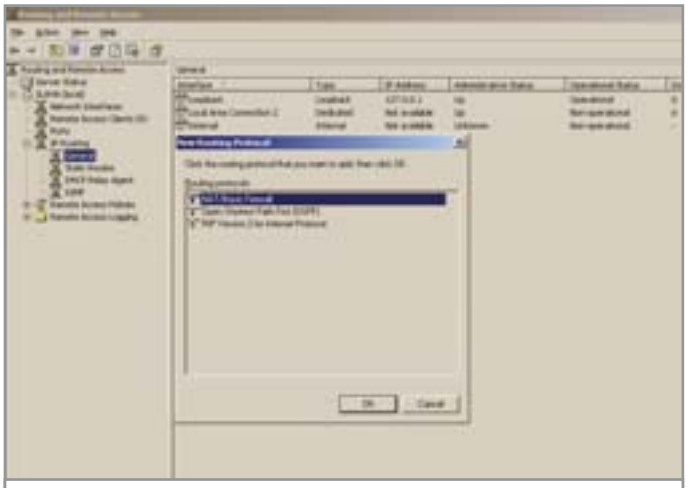
Нижним уровнем модели OSI является физический уровень. Он определяет тип среды передачи, кодирование данных, методы передачи, форму и тип разъемов. Другими словами, стандарты разъемов (например RJ-45), модуляции и тому подобное относятся к стандартам физического уровня.

Второй уровень называется уровнем канала данных. Он обеспечивает физическую адресацию, уведомления об ошибках, порядок доставки кадров и управление потоком данных. Обычно функции этого уровня реализованы в сетевом адаптере и в коммутаторе. Примером стандарта этого уровня являются различные варианты протокола Ethernet.

Третий уровень — сетевой, на нем работает протокол IP, который обеспечивает взаимодействие между сетями. Четвертый уровень — транспортный. Он отвечает за взаимодействие между приложениями. Третий и четвертый уровни являются самыми важными с точки зрения сетевого взаимодействия и сетевой безопасности. »



Из консоли Routing and Remote Access в том числе осуществляется и настройка firewall



Включение протокола NAT/Basic Firewall осуществляется из консоли Routing and Remote Access

» На этих уровнях работают основные протоколы, используемые в Интернете (IP, TCP, UDP, ICMP). Сетевой уровень обеспечивает доставку данных между любыми двумя узлами в сети, при этом он не берет на себя никаких обязательств по надежности передачи данных. Этим занимается транспортный уровень, который обеспечивает передачу данных между любыми узлами сети с требуемым уровнем надежности. Для этого на транспортном уровне имеются средства установления соединения, нумерации, буферизации и упорядочивания пакетов. Примером протокола с гарантированной передачей данных является TCP.

Пятый уровень — сеансовый, организует диалог между процессами на разных машинах. Шестой — уровень представления. Его задачей является трансляция из одного формата данных в другие, сжатие данных, шифрование и т. д. Седьмой — уровень приложений. На этом уровне работают приложения, с которыми имеет дело пользователь.

Пятый, шестой и седьмой уровни мы будем рассматривать в данной статье как один, так как с точки зрения сетевой безопасности разбиение взаимодействия между системами на эти уровни не существенно и может скорее запутать, нежели прояснить ситуацию. Для полноты картины мы просто привели названия этих уровней, которые в дальнейшем будем называть уровнем приложений.

Построение защиты

Итак, ознакомившись со всеми уровнями сетевого взаимодействия, мы можем начать строить защиту для каждого уровня отдельно. Соответственно, выбирать продукты, которые позволят нам получить необходимую функциональность, нужно тоже для каждого уровня в отдельности. Дело в том, что не все firewall работают на каждом из семи уровней, и выбор конкретного продукта будет зависеть от наших задач и, разумеется, от финансовых возможностей. Наиболее полные решения работают на всех уровнях, начиная со второго.

На втором уровне модели OSI находится протокол Ethernet. Несмотря на то что этот протокол определяет порядок взаимодействия внутри локальной сети, зачастую не нужно, чтобы все компьютеры внутри сети имели доступ ко всем возможным ресурсам. Особенно это справедливо для беспроводных сетей. Поэтому иногда может оказаться желательным, чтобы firewall обеспечивал фильтрацию пакетов, поступающих из сети, по так называемым MAC-адресам сетевых карт, то есть практически по физическому адресу компьютера.

Каждая сетевая карточка после выхода с конвейера производителя имеет свой уникальный MAC-адрес, по которому ее можно идентифицировать. Несмотря на это, существуют программные продукты, которые умеют подменять эти адреса, поэтому на 100% полагаться на такой способ идентификации пользователей все-таки не следует. С одной стороны, за компьютером, в котором установлена сетевая карта с доверенным MAC-адресом, может сидеть кто угодно. С другой стороны, как уже было сказано, злоумышленник может просто-напросто перехватить посылаемые картой пакеты и подменить в них MAC-адрес сетевой карты.

Написав списки доступа (в программном обеспечении, поставляемом с аппаратным брандмауэром, или в firewall-программе от сторонних производителей) для фильтрации трафика на втором уровне, в случае необходимости мы должны перейти к защите сети на следующем, третьем уровне.

На этом уровне работает протокол IP, который осуществляет маршрутизацию пакетов. Каждый компьютер в Интернете имеет свой уникальный IP-адрес. Поэтому, если мы не хотим получать трафик от какого-либо компьютера или целой сети, мы должны аналогичным образом написать списки доступа, указав в них нежелательные IP-адреса.

Однако зачастую у нас нет возможности заранее узнать, какая сеть является надежной, а какая — нет. Более того, потенциально опасным нужно считать любой компьютер в Интернете и, чтобы максимально обезопасить себя от возможных атак, нам необходимо пропускать трафик только для нужных приложений. В результате мы поднимаемся на четвертый уровень. На данном уровне мы будем защищать сеть, основываясь на знании того, какие приложения у нас работают. Например, мы знаем, что в нашей сети есть только почтовый сервер. Значит, мы должны разрешить только соединения по протоколам SMTP и POP3 и закрыть все остальные протоколы.

Зачастую сама операционная система открывает различные порты для своих служебных целей, что может быть использовано хакерами для проникновения в нашу сеть. Каждое приложение, которое обменивается данными по сети, использует протокол (SMTP, HTTP и другие), которому приписан определенный номер, так назы- »

» ваемый номер порта. Если мы хотим допустить SMTP-трафик в нашей сети, то в настройках firewall надо разрешить работу по порту 25. Некоторые производители firewall облегчают нашу жизнь в этом вопросе и не заставляют учить наизусть номера портов всех протоколов, а используют их словесное описание.

Многие недорогие решения ограничиваются возможностью защиты на третьем и четвертом уровнях модели OSI. Для отражения большинства угроз этого может оказаться достаточно, однако для полной защиты сети необходима защита и на уровне приложений. Что это значит?

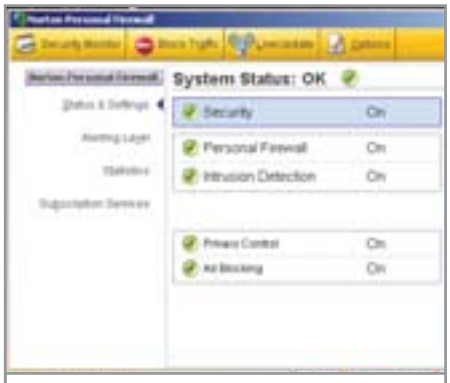
Допустим, внутри сети есть веб-сервер и мы настроили наш firewall на пропускание пакетов только на этот сервер и только по порту 80, что соответствует поддержке HTTP-протокола. Однако в любом программном обеспечении есть ошибки, и веб-серверы не являются исключениями. Хакер может послать специально сконструированный запрос на наш веб-сервер. Обработка запроса приведет к ошибке, что повлечет за собой либо «падение» сервера, либо получение злоумышленником контроля над ним и, возможно, доступа к локальной сети, в которой этот сервер находится.

За 2003 год во всем мире было множество вирусных эпидемий, использующих ошибки в реализации веб-серверов. Чтобы исключить возможность подобного рода атак, необходимо проверять на входе в нашу сеть не только IP-адреса и номера портов отправителя и получателя запроса, но и следить за корректностью формата HTTP-запросов в случае с веб-сервером.

Реализация защиты на уровне приложений является нетривиальной задачей, поэтому если вы будете искать firewall, обладающий такими функциями, то приготовьтесь потратить достаточно крупную сумму денег. В некоторых случаях производители веб-серверов облегчают нам жизнь и выпускают для своих продуктов утилиты, выполняющие роль firewall уровня приложений, например утилита URLScan для IIS компании Microsoft.

Помимо анализа отдельных пакетов или небольших групп пакетов на предмет их надежности, существуют более интеллектуальные системы, способные анализировать сложные модели трафика и предупреждать о возможных атаках. Например, сканирование портов является возможной причиной

Внешний вид аппаратного брандмауэра Cisco PIX Firewall



Norton Personal Firewall — представитель семейства Personal Firewalls

для беспокойства администратора. Разумеется, если firewall оказался бы в состоянии обнаружить сканирование и временно закрыть все порты, то такая функция могла бы оказаться весьма полезной. Системы, которые могут обнаружить хакерскую или вирусную активность, основываясь на анализе входящего трафика, называются Intrusion Detection System (IDS). Наличие такой функциональности может повлиять на выбор средства защиты.

Все виды обороны

Прежде чем перейти к рассмотрению конкретных моделей, сначала выясним, какими еще интересными функциями может обладать firewall. Если firewall работает на границе между локальной сетью и Интернетом, то необходимо, чтобы он выполнял функцию трансляции адресов (NAT — Network Address Translation). Это означает, что внутри сети мы обычно используем так называемые частные IP-адреса, которые можно использовать в пределах собственной локальной сети, но нельзя использовать в Интернете. Чтобы получить доступ к информации в Интернете, нам необходимо преобразовать частный IP-адрес нашего компьютера в публичный, выданный провайдером.

В последнее время задача такой трансляции относится больше к стандартным функциям маршрутизатора. Так, например, в Windows Server 2003 это настраивается в свойствах Routing and Remote Access сервера. Однако в системах Linux трансляция адресов является частью функций firewall. И те и другие по-своему правы, так как, с одной стороны, NAT является протоколом маршрутизации, поскольку он маршрутизирует трафик с одного интерфейса (сетевой карты) на другой. С другой стороны, NAT является инструментом безопасности, так как скрывает компьютеры в локальной сети путем трансляции IP-адресов всех компьютеров в один или несколько реальных IP-адресов.

Помимо собственно защиты firewall может ограничивать доступ к Интернету для пользователей локальной сети. Если вы не хотите, чтобы пользователи вашей сети скачивали из Интернета музыку, видеофайлы или страницы определенного содержания, то необходимо искать firewall с поддержкой технологии content filtering, которая ограничивает доступ к сайтам выбранных вами категорий.

Необходимо помнить, что помимо внешних угроз, к которым относятся атаки вирусов и хакеров, не меньшую опасность могут представлять и сами пользователи локальной сети. По утверждениям различных западных компаний, занимающихся разработкой систем безопасности, 80% всех взломов осуществляется самими сотрудниками. Возможно, в российских условиях этот процент несколько меньше, тем не менее не следует об этом забывать. Поэтому если в вашей сети есть конфиденциальная информация, требующая серьезной защиты, то имеет смысл осуществлять к ней доступ также через внутренний firewall.

Hard или soft?

Перейдем теперь к рассмотрению конкретных продуктов. Firewall можно разделить на два типа:

- решения, защищающие отдельный компьютер (Personal Firewall);
- решения, работающие на границе локальной сети и защищающие всю сеть.

Второй тип можно разделить еще на две группы: это программные и аппаратные средства. »

Настройка системы обнаружения вторжений в Norton Personal Firewall

Настройка списка блокируемых сайтов в Norton Personal Firewall

Полная безопасность дорого стоит

Наиболее популярными аппаратными решениями являются Cisco PIX Firewall (www.cisco.com/go/pix) и CheckPoint Firewall-1 (www.checkpoint.com). Это довольно сложные и дорогие решения, защищающие вашу сеть на всех уровнях и обеспечивающие возможность создания защищенных каналов между сетями или между удаленным пользователем и сетью (VPN). Именно в силу дороговизны применение подобной техники могут позволить себе только достаточно богатые компании.

Настройка маршрутизации

Если у вас небольшая сеть или вы готовы пожертвовать очень высокой производительностью, то можно ограничиться программным решением, которое будет работать на устройстве, осуществляющем маршрутизацию. Если маршрутизатором является Windows Server 2003, то он обладает необходимой функциональностью для защиты сети на третьем и четвертом уровнях модели OSI.

Настройка Windows Server 2003 в качестве маршрутизатора с поддержкой firewall и NAT осуществляется в консоли Routing and Remote Access (RRAS). Перед тем как начать настройку, надо знать IP-адрес, который дал провайдер, и определиться, какие адреса будут использоваться в нашей локальной сети. Внутри локальных сетей могут использоваться адреса одного из трех диапазонов: 10.0.0.0 — 10.255.255.255, 192.168.0.0 — 192.168.255.255 либо 172.16.0.0 — 172.31.255.255. Такие адреса никогда не будут присвоены реальным сетевым устройствам и компьютерам, доступным из Интернета.

После выяснения этой информации необходимо зайти в консоль RRAS и убедиться в том, что в список протоколов маршрутизации включен NAT/Basic Firewall. Если этого нет, то его нужно добавить.

Делается это нажатием правой кнопки мышки на пункте «General» и выбором пункта меню «New Routing Protocol». Затем необходимо указать серверу, какой интерфейс (сетевая карта) является внутренним, а какой внешним. Нажимаем правую кнопку мыши на пункте «NAT/Basic Firewall», выбираем «New Interface», указываем нужный интерфейс и то, является ли он внутренним (private) или внешним (public). Для внешнего интерфейса также необходимо указать диапазон адресов, выданный провайдером. После этого настройка NAT будет закончена.

Варианты защиты

После настройки NAT необходимо выбрать тип firewall, если мы предполагаем пользоваться внутренними средствами операционной системы. Windows Server 2003 предлагает нам два варианта. Первый — использование простого firewall (basic firewall). При этом firewall по умолчанию будет пропускать в сеть только тот трафик, который был из нее инициирован. Например, если пользователь пытается открыть веб-страничку на удаленном сервере, то трафик от сервера к этому пользователю будет пропущен. Если же какой-либо компьютер в Интернете попытается сам получить доступ к компьютеру в нашей локальной сети, то эти попытки будут полностью пресекаться. Но если в нашей сети есть серверы, например почтовый, которому необходимо принимать запросы на подключения, то есть возможность создать соответствующие исключения. Для этого надо пойти в консоль RRAS, найти в ней пункт «NAT/Basic Firewall», в правом окне выбрать тот интерфейс, который «смотрит в сторону» провайдера, и выбрать вкладку «Services and Ports». После этого необходимо поставить галочку напротив названия соответствующего сервера и указать его IP-адрес в локальной сети.

Для многих небольших сетей такой защиты будет достаточно. Если же у вас уже есть опыт настройки firewall, то вы можете самостоятельно определять конкретные правила для пакетов на основе IP-адресов, номеров портов и протоколов. В окно ввода правил можно попасть, нажав кнопки «Inbound Filters» и «Outbound Filters», которые располагаются там же, где мы определяли типы интерфейсов.

Если и этих возможностей покажется недостаточно, и вы хотите защищать сеть на всех семи уровнях, то в этом случае Microsoft предлагает свой продукт под названием IAS Server (Internet Acceleration and Security). Помимо функций обеспечения безопасности, этот продукт включает в себя прокси-сервер, который используется для кэширования веб-страниц и таким

С концептуальной точки зрения взаимодействие протоколов модели OSI осуществляется «по горизонтали»

» образом ускоряет доступ к ресурсам Интернета. Поэтому в названии продукта и присутствует слово Acceleration.

Персональные телохранители

В ряде случаев у вас нет возможности доверить свою безопасность сетевому firewall, например, если вы путешествуете с ноутбуком или выходите в Интернет из дома. Для таких целей существует класс продуктов под названием Personal Firewall, то есть личный брандмауэр, который защищает только ваш компьютер.

Иногда такие программы интегрируются с антивирусным ПО для обеспечения комплексной защиты. Кроме того, некоторые личные брандмауэры обладают одной полезной особенностью. Поскольку они работают на том же компьютере, который и защищают, то у них есть возможность определять, какая программа, работающая на вашем компьютере, пытается выйти в Интернет, к какому IP-адресу и порту производится обращение. Это может оказаться очень полезным, если вы не хотите, к примеру, чтобы какой-нибудь вирус отослал своему создателю все ваши пароли.

Однако надо учитывать, что современные программы довольно часто пытаются выйти в Интернет и выполнить необходимые им действия, например, проверить наличие обновлений на сайте фирмы-разработчика. Поэтому если ваш личный firewall сообщает, что какая-то неизвестная программа пытается соединиться с неким сайтом в Интернете, то не стоит паниковать, тут же блокировать этот трафик и скачивать последние антивирусные обновления. Возможно, это просто запустился Windows Update или Real Player пошел искать новые сетевые радиостанции.

К классу Personal Firewall относится встроенный в Windows XP и Windows Server 2003 Internet Connection Firewall (ICF). Несмотря на то что этот продукт обладает весьма скромной функциональностью, он очень прост в настройке и для большинства пользователей и начинающих системных администраторов может оказаться весьма полезным. Настраивается этот firewall в свойствах сетевого подключения на вкладке «Advanced», где необходимо поставить галочку напротив фразы «Protect my computer and network by limiting or preventing access to this computer from the Internet».

Определение прав на доступ к Интернету в Norton Personal Firewall

Настройка системы фильтрации трафика в популярной firewall-программе ZoneAlarm Pro

Если на компьютере работает, например, веб-сервер, к которому мы хотим открыть доступ, то необходимо в настройках ICF перейти на вкладку «Services» и поставить галочку напротив «Web Server (HTTP)».

На вкладке «ICMP» можно разрешить компьютеру отвечать на команду ping и другие более сложные служебные запросы из Интернета. Иногда это может оказаться полезным, например, если у вас есть удаленный компьютер и вы хотите периодически проверять, не «отвалился» ли он от сети. Однако ping используется и при сканировании сети в поисках потенциальной жертвы. Если вы все же решили разрешить вашему компьютеру отвечать на ping, то поставьте галочку напротив «Allow incoming echo request». Если вы не знаете назначения остальных параметров, то их лучше оставить выключенными.

Как уже упоминалось выше, ICF обладает довольно ограниченной функциональностью, поэтому для повышенной безопасности имеет смысл обратить внимание на ряд других продуктов. Рассмотрим, что нам может предложить Personal Firewall на примере Norton Personal Firewall.

Эта программа обладает практически полным набором инструментов для создания надежной защиты. С помощью Norton Personal Firewall вы можете следующее.

- Определять стандартные правила на основе IP-адресов и номеров портов.
- Указывать, каким компьютерам вы разрешаете доступ к своим общим папкам, а каким нет.
- Указывать, каким программам разрешен выход в Интернет.
- Выявлять различные атаки на компьютер с помощью модуля Intrusion Detection.
- Вырезать рекламные баннеры из страниц сайтов. Данная функция может оказаться не очень полезной в российских условиях, так как ее фильтры настроены на западные сайты. Но, естественно, если какой-то из российских сайтов начнет докучать навязчивой рекламой, проще простого добавить его в черный список блокируемых сайтов.
- Указывать, какая информация не должна покидать пределы вашего компьютера.

Несмотря на кажущуюся сложность продукта, он имеет вполне приемлемые рабочие настройки по умолчанию, которые можно оставить на первое время и изменять их по мере вашего совершенствования в области сетевой безопасности.

Также широко известен продукт ZoneAlarm Pro with Web Filtering компании Zone Labs. Этот firewall имеет собственную базу сайтов, разбитую на категории. Кроме того, программа умеет сканировать и анализировать содержимое загружаемых страниц, после этого принимать решение о принадлежности страницы к определенной категории и производить только те действия, которые разрешены при посещении сайтов этой категории.

Большинство программ типа Personal Firewall имеют очень похожую функциональность и отличаются только интерфейсом и удобством настроек. На сегодняшний день на рынке представлено достаточно большое количество таких программ, и отдать предпочтение какой-либо из них достаточно сложно.

Однако надо помнить, что информация в наше время зачастую стоит очень дорого. Небольшая оплошность или просто небрежность при построении системы безопасности может привести к печальным последствиям. Поэтому мы еще раз настойчиво рекомендуем уделять вопросам безопасности самое пристальное внимание.

■ ■ ■ Вячеслав Лущинский

На зависть Цезарю

Защита данных и сетевых принтеров

Едва ли не основной задачей любой серверной операционной системы является обеспечение безопасности информации, хранимой как на самом сервере, так и на клиентских компьютерах. Не стала исключением и Windows Server 2003.

Существуют две основных концепции обеспечения безопасности операционной системы. Первая предполагает, что важнее всего доступ к ресурсам, и ее можно сформулировать так — «Разрешено все, кроме того, что запрещено». Вторая является ее диаметральной противоположностью и гласит: «Запрещено все, кроме того, что указано вручную».

Раньше все операционные системы Microsoft строились, используя первую концепцию, то есть в их основе лежал принцип доступности в ущерб безопасности. Но виртуальный мир развивается не только в лучшую сторону, появляется все большее количество злоумышленников, стремящихся похитить или повредить не принадлежащую им информацию. И как следствие этого уровню безопасности ОС стали предъявляться более высокие требования.

В начале 2002 года корпорация Microsoft предложила концепцию безопасности SD3+C (Secure by Design, Secure by Default, Secure in Deployment and Communications — безопасность в архитектуре, безопасность по умолчанию, безопасность при »

Рис. 1. Сообщение об ошибке доступа к зашифрованному файлу

Рис. 2. Указание системе о необходимости шифрования информации

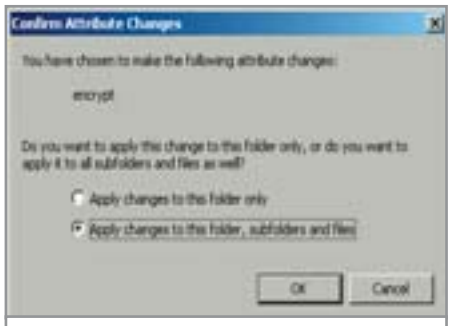


Рис. 3. Выбор необходимого режима шифрования папки

установке и взаимодействие). Одновременно с этим Microsoft заявила о начале разработки защищенной информационной системы (Trustworthy Computing), которая базируется на четырех основных принципах: обеспечение безопасности, защита личных сведений, надежность и целостность. ОС Windows Server 2003 является первым продуктом корпорации, построенным с использованием этих элементов.

Угроза для внутрисетевой информации может исходить не только от внешних источников, но и от дочерних клиентов самой сети, причем не только по злому умыслу, но и просто из-за неопытности пользователей. А защита от корпоративного шпионажа уже несколько лет, как лежит во главе угла при организации и развертывании сетей многих предприятий. Windows Server 2003 предоставляет широкие возможности по обеспечению безопасности ресурсов локальной сети.

Под понятием безопасности ресурсов подразумевается разграничение прав доступа и разрешенных манипуляций с объектами сети, то есть без наличия соответствующих полномочий пользователь не сможет, например, открыть, удалить или переименовать тот или иной ресурс. Ограничение доступа к объектам может проводиться несколькими способами. Основные из них — распределение прав и полномочий на проведение различных действий, шифрование и авторизация. Подробно о распределении прав и полномочий среди пользователей сети будет рассказано в следующей статье, а здесь мы рассмотрим другие возможности безопасности, предоставляемые Windows Server 2003.

Надежная защита

Единственным надежным средством защиты информации является ее шифрование. Такое утверждение связано с тем, что операционную систему можно загрузить не только с жесткого, но и с гибкого диска. Это позволяет злоумышленнику, получившему физический доступ к компьютеру, обойти средства управления доступом системы NTFS и, используя специальные программные инструменты, прочесть информацию с жесткого диска. Огромные преимущества шифрование предоставляет и при использовании его в разграничении прав доступа к различной информации, находящейся в общих папках.

Система EFS

Основным механизмом шифрования, используемым в Windows Server 2003, является Encrypting File System (EFS, шифрующая файловая система), работающая только на NTFS 5.0 и впервые появившаяся в Windows 2000.

По умолчанию конфигурация EFS позволяет всем пользователям шифровать/дешифровать свои файлы без всякого вмешательства со стороны администратора, естественно, в том случае, если их данные располагаются на диске с файловой системой NTFS 5.0. Сам процесс шифрования/дешифрования происходит автоматически и абсолютно прозрачен для пользователя. То есть с файлом можно работать так же, как и до установки его защиты. Например, можно запустить табличный процессор Excel, загрузить в нем необходимый документ, отредактировать его и затем сохранить. Система сама определяет, есть ли у пользователя разрешение на открытие файла, и в том случае, если его нет, она выдает сообщение об ошибке доступа (рис. 1).

Шифрование файлов и папок

Для шифрования информации укажите необходимые файл или папку, вызовите кон-

Средства аутентификации

Протокол Kerberos

Для создания практически любой системы безопасности необходимо присутствие в ней средств, позволяющих проверять, является ли объект в действительности тем, за кого он себя выдает. Процесс такой проверки принято называть аутентификацией.

Основным механизмом аутентификации, используемым в Windows Server 2003, является протокол Kerberos пятой версии. Данный протокол установлен в w2k3 по умолчанию и не нуждается в развертывании и дополнительной настройке. Единственный компонент, который ему нужен для работы, — это установленный доменный контроллер.

Любой запрос на аутентификацию проходит проверку несколькими системами Kerberos, что практически полностью исключает возможность подделки сетевого имени. Его алгоритм является системой идентификации, основанной на доверии уже обработанных Kerberos-клиентов. Для доказательства проверки Kerberos-сервером используется так называемая квитанция (пакет данных), проверяя ее, сервер производит идентификацию пользователя — если она пройдена, то запрос клиента принимается.

Так же для подтверждения личности клиента в Kerberos применяются так называемые удостоверения. Удостоверение содержит дополнительную информацию, которая при сравнении подтверждает, что клиент, предоставляющий квитанцию, является именно тем, кому эта квитанция была действительно выдана.

Эту систему можно считать самой эффективной из всех подобных, существующих на данный момент.

Рис. 4. Окно выбора разрешений на доступные действия с ресурсом

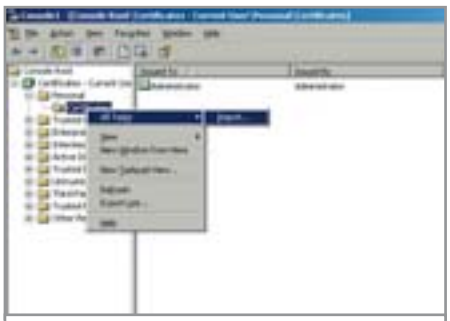


Рис. 5. Запуск процесса импортирования сертификата восстановления

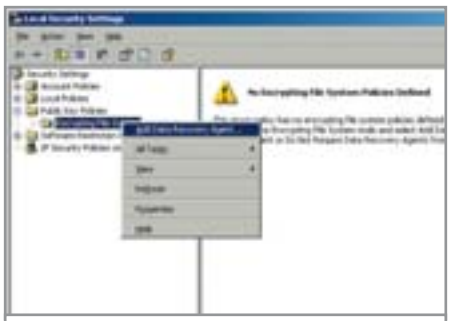


Рис. 6. Владелец данного сертификата станет агентом восстановления

текстное меню и в нем выберите команду «Properties». В окне свойств на вкладке «General» нажимаем кнопку «Advanced». В появившемся окне «Advanced Attributes», отмечаем пункт «Encrypt content to secure data» («Шифровать содержимое для защиты данных») (рис. 2) и нажимаем кнопку «ОК». После подтверждения внесенных изменений в свойства файла или папки появляется окно выбора режима шифрования. В случае шифрования отдельного файла доступны режимы «Encrypt the file and the parent folder» («Шифровать файл и родительскую папку») и «Encrypt the file only» («Шифровать только файл»). В случае шифрования папки можно выбрать режимы «Apply changes to this folder» («Только к этой папке») или «Apply changes to this folder, subfolder and files» («К этой папке и всем вложенным папкам и файлам») (рис. 3).

Необходимо сказать, что пользователям (в большей степени это относится к администраторам) не стоит шифровать те файлы, которые находятся в системном каталоге, так как они могут быть необходимы для загрузки системы, в процессе которой дешифрование невозможно, и в результате этого система может потерять работоспособность. ОС препятствует возникновению такой ситуации и не позволяет шифровать файлы, имеющие атрибут «Системный».

В отличии от Windows 2000 Server, w2k3 разрешает организовывать совместный доступ к зашифрованным файлам, которые находятся на общих сетевых ресурсах. Для создания такого доступа необходимо снова перейти к окну «Advanced Attributes» и в нем нажать кнопку «Details». Появится новое окно, и, нажав в нем кнопку «Add», можно перейти к окну добавления пользователей, которые смогут работать с зашифрованным файлом.

Отключение шифрования файлов и папок, также происходит в окне «Advanced Attributes», в котором необходимо сбросить флажок с пункта «Encrypt content to secure data».

Создание агента восстановления

Самая серьезная ошибка, которую допускают при работе с EFS, — используя на своем компьютере систему шифрования данных, пользователи затем по какой-либо причине переустанавливают ОС. После этой операции все такие данные будут безвозвратно утеряны, так как доступ к ним в предыдущей ОС, на которой они и были зашифрованы, имели два пользователя — тот, кто провел операцию шифрования, и агент восстановления. Ошибка заключается в том, что для декодирования данных необходимо предъявить сертификаты одного из этих пользователей, а для этого их необходимо было экспортировать и сохранить, чего очень часто не делается.

Процедура создания агента восстановления должна выполняться на компьютере, на котором планируется использовать систему EFS. На первом этапе необходимо создать сертификат агента восстановления. Для этого войдите в систему под учетной записью администратора. В командной строке запустите команду cipher /R:имяФайла (без расширения). После этого по запросу системы дважды введите пароль, который необходим для защиты личного ключа. Будет создано два файла: один с расширением .cer, содержащий только сгенерированный ключ, второй с расширением .pfx, содержащий помимо ключа и сертификат агента восстановления. Рекомендуется сохранить их на дискету или на любой другой носитель.

Для импорта сертификата восстановления на другой компьютер необходимо зарегистрироваться на нем как администратор, запустить оснастку «Certificates» и в ней перейти к узлу «Certificates» в папке «Personal». В контекстном меню из раздела «All Tasks» запускаем процесс импортирования pfx-файла (рис. 5).

Секретный офис

Система Information Rights Management

Стоит отдельно рассказать еще об одной технологии безопасности, которая не является интегрированной в ОС Windows Server 2003, но ее возможности входят в рамки данной статьи. Эта технология носит название Information Rights Management (IRM), и она впервые реализована в Microsoft Office 2003 и службах Windows SharePoint. Технология IRM позволяет распределять и ограничивать в документах функции копирования, вставки, печати, а для электронных сообщений и отправки. Но самой интересной является возможность разграничения доступа к отдельным частям одного документа. То есть при совместной работе нескольких человек с одним документом каждому из них можно указать те разделы документа, с которыми он сможет работать, и закрыть доступ к другим. Это позволит нескольким пользователям редактировать документы, содержащие конфиденциальную информацию, уровень доступа к которой у различных членов коллектива неодинаков. Также это позволит избежать конфликтов при объединении нескольких частей, созданных разными авторами, в единый документ. Плюс к этому можно установить и срок жизни документа, по истечении которого он просто перестанет открываться. Все сказанное относится и к письмам электронной почты.

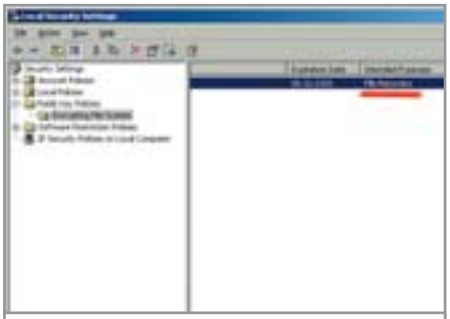


Рис. 7. Владелец переданного сертификата стал агентом восстановления

Рис. 8. Определение функций, доступных для пользователя или группы

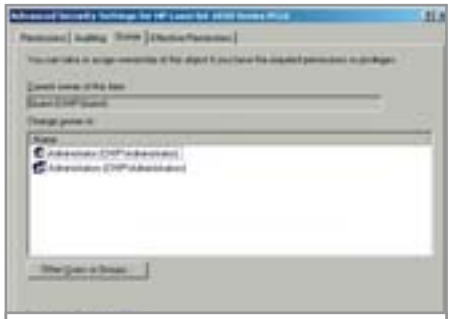


Рис. 9. Окно передачи прав владения другому пользователю

» Теперь необходимо указать, что владелец данного сертификата является агентом восстановления шифрованных данных. Для этого нужно проследовать по пути «Start → Administrative Tools → Local Security Policy». В появившемся окне «Local Security Settings» внутри узла «Public Key Policy» открываем папку «Encrypting File System» и в контекстном меню запускаем команду «Add Data Recovery Agent...» (рис. 6). Начнет выполняться мастер Add Recovery Agent Wizard. Нажатием на кнопку «Browse Folders» указываем расположение ранее созданного файла с расширением .cer. После этого сертификат будет успешно импортирован на данный компьютер, а его владелец получит статус агента восстановления. Это указано в столбце «Intended Purposes» — только что импортированный сертификат обозначен как «File Recovery» (рис. 7).

Безопасность сетевых принтеров

Не менее важным является обеспечение должного уровня безопасности принтеров, выделенных для общего использования. Неправильное распределение уровня доступа к ним между пользователями сети может привести к весьма неприятным последствиям, начиная от большого уровня использования расходных материалов до безвозвратной потери документов.

Изначально все созданные сетевые принтеры доступны для использования всеми клиентами локальной сети. Для распределения уровня доступа к принтеру необходимо быть его владельцем или иметь соответствующее разрешение.

Управление списком функций, которые будут определены для того или иного пользователя или их группы, проводится в окне свойств каждого принтера на вкладке «Security» (рис. 8). Список доступных действий, которые можно назначить пользователям, приведен в табл. 1. Если на этой вкладке нажать кнопку «Advanced», откроется окно дополнительных настроек безопасности, в котором, перейдя ко вкладке «Owner» (рис. 9), владелец принтера может передать свои права другим пользователям сети, с соответствующим делегированием разрешений на проведение различных действий, доступных для владельца этого сетевого принтера.

Изначальные установки Windows Server 2003 выдают разрешения «Manage Printers» и «Manage Documents» только тем пользователям, которые входят в группы «Administrators», «Print Operators» и «Server Operators». Все остальные пользователи имеют разрешение «Print», то есть могут управлять печатью только собственных документов.

Аудит системной безопасности

Для увеличения уровня безопасности системы также следует регулярно просматривать журнал событий «Event Viewer» и особое внимание уделять его разделу «Security», в котором содержатся записи, отображающие режимы работы всей системы безопасности. Это позволит заметить попытки проведения несанкционированных действий, осуществления неавторизованного доступа и так далее и принять необходимые превентивные меры.

Заключение

На сегодняшний день операционная система Windows Server 2003 является наиболее защищенной системой от Microsoft, предоставляющей ее пользователям надежную защиту данных. Однако не стоит забывать о том, что нельзя построить защищенную систему, если ее пользователи не будут соблюдать элементарных мер безопасности и станут, например, записывать собственные пароли на бумаге, доступной для общего обозрения.

■ ■ ■ Игорь Пыжов

Табл. 1. Список разрешенных операций при работе с принтером

Функции печати, которые можно выполнять	Разрешения		
	Print	Manage Printers	Manage Documents
печатать документы	•	•	•
приостанавливать, продолжать, перезапускать и отменять печать документа, принадлежащего пользователю	•	•	•
устанавливать соединение с принтером	•	•	•
управлять установками для всех заданий печати	–	•	•
приостанавливать, перезапускать и удалять все документы	–	•	•
выделять принтеры в совместное использование	–	•	–
изменять свойства принтера	–	•	–
удалять принтер	–	•	–
изменять разрешения принтера	–	•	–

Что дозволено Юпитеру...

Управление доступом к объектам

При установке Windows Server 2003 возникает вопрос о том, какие права должны быть предоставлены пользователю или группе, какие действия с объектами файловой системы NTFS должны быть разрешены, ведь небольшие сети строятся чаще всего на основе рабочих групп.

Группа — это набор учетных записей пользователей, имеющих одинаковые права и разрешения. Член группы имеет права, предоставленные группе. При добавлении членов в группы необходимо учитывать следующее:

- становясь членом группы, пользователь получает все права и разрешения, предоставленные группе;
- пользователь может входить в несколько групп (группа представляет собой всего лишь список членов).

В группе могут быть созданы группы более низкого уровня, например, в группе, соответствующей отделу, могут быть созданы группы, соответствующие бюро. Кроме того, некоторые пользователи могут работать только на каких-то определенных компьютерах. Таким образом, пользователи могут объединяться в группы по функциональному и географическому признакам, то есть могут создаваться как рабочие, так и локальные группы.

Записями о локальных группах управляет SAM (Security Accounts Manager, диспетчер учетных записей безопасности), который представляет собой локальную базу данных системы безопасности. Локальные группы используются для предоставления разрешений на доступ к ресурсам и предоставления прав на выполнение системных задач только на том компьютере, на котором создана данная группа. В отличие от рабочих групп локальные не могут быть членами других групп.

Для создания локальной группы необходимо быть членом «Administrators» («Администраторы») или «Account Operators» («Операторы учета»).

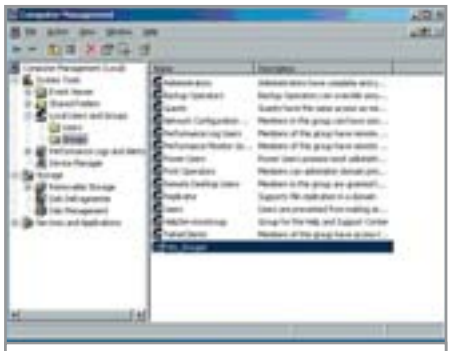
Кроме того, Windows Server 2003 при инсталляции по умолчанию создает несколько групп с предопределенными правами на выполнение системных задач на локальном компьютере. Удалить эти заранее созданные группы невозможно никакими способами.

Тактика и стратегия

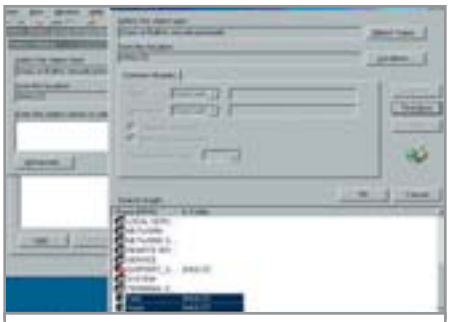
Пользователь, желающий получить доступ к ресурсам, должен иметь учетную запись на данном компьютере. Если нескольким пользователям требуется иметь доступ к одним и тем же ресурсам, следует создать группу для предоставления прав, а затем добавить в нее пользователей. Этот способ известен под названием стратегии ALP, которая заключается в следующем:

- A (Account) — добавить пользователя в
- L (Local Group) — локальную группу на том компьютере, на котором располагается запрашиваемый ресурс;
- P (Permission) — предоставить разрешения или права локальной группе.

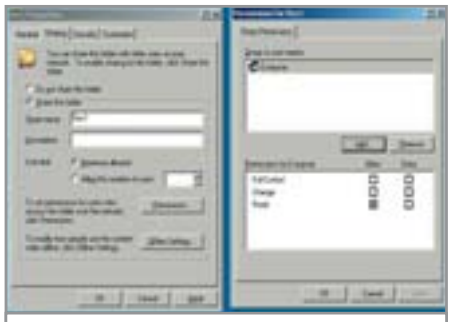
»



Группы, автоматически создаваемые Windows Server 2003



При помощи консоли Computer Management осуществляется управление списками групп и пользователей



По умолчанию все пользователи (группы «Users» и «Everyone») имеют разрешение только на чтение

» Если права могут быть предоставлены путем добавления пользователя во встроенную группу, то следует поступить именно так.

Как сохранить секреты

Файловая система NTFS позволяет наделять пользователей различными правами и управлять уровнем доступа к ресурсам, а также шифровать файлы на диске.

Разрешениями наделяются пользователь и группа, которым необходим доступ к ресурсу. Разрешения действуют независимо оттого, осуществляется доступ к ресурсу на данном компьютере или по сети.

Таблица управления доступом

NTFS хранит таблицу ACL (Access Control List, таблица управления доступом), в которой определяется уровень доступа пользователя, группы и компьютера к файлам и папкам NTFS-раздела. Для доступа пользователя к ресурсу в таблице ACL должна содержаться запись ACE (Access Control Entry, запись управления доступом), описывающая разрешенные действия.

Откорректировать ACL и ACE можно при помощи консоли безопасности — «Start → Administrative Tools → Local Security Policy».

При инсталляции Windows Server 2003 автоматически наделяет группу «Users» разрешением только на чтение, при этом группа будет иметь доступ на чтение всех папок и файлов, созданных в корне.

Разрешения NTFS в системе Windows Server 2003

По умолчанию пользователи, получившие разрешения на доступ к папке, получают доступ к вложенным папкам и файлам. Если разрешения на доступ имеют и пользователь и группа, членом которой он является, тогда такой пользователь получает несколько разрешений на доступ к одному и тому же ресурсу.

Объединение разрешений

Действующие для пользователя разрешения на доступ к ресурсу получаются объединением разрешений NTFS, предоставленных пользователю и группе, членом которой он является. Например, если пользователь имеет разрешение Read на доступ к папке и является членом группы, имеющей разрешение Write на ту же папку, тогда такой пользователь получает разрешения Read и Write на эту папку.

Файл важнее папки

Разрешения на доступ к файлам имеют приоритет над разрешениями на доступ к папкам. Например, пользователь с разрешением Modify на файл может вносить изменения в этот файл даже в том случае, если имеет только разрешение Read на папку, содержащую данный файл.

Запрет — главное разрешение

Для пользователя доступ к конкретному файлу или папке можно запретить, задав разрешение Deny (отклонить). Если пользователю как члену группы разрешен доступ к файлу или к папке, то запрет отменяет все ранее предоставленные разрешения.

Группы и ресурсы нужно организовывать таким образом, чтобы для управления доступом было достаточно разрешений.

Предотвращение наследования

По умолчанию разрешения, которые предоставлены родительской папке, наследуются вложенными папками и файлами, то есть переносятся на них.

Чтобы предотвратить наследование разрешений, сохраните только те из них, которые были предоставлены явным образом.

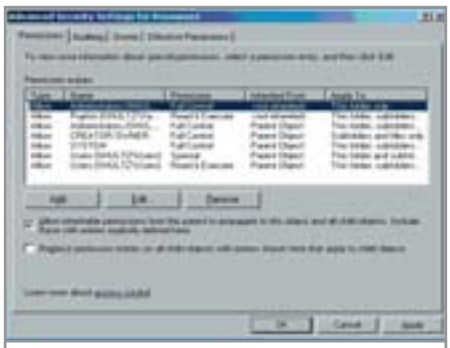
Та вложенная папка, для которой предотвращается наследование разрешений от соответствующей родительской папки, становится новой родительской папкой и вложенные в ней папки и файлы наследуют предоставленные для нее разрешения. »

Табл. 1. Стандартные разрешения на доступ к папкам и файлам NTFS

Разрешения	на доступ к папке NTFS	на доступ к файлам NTFS
Read (чтение)	просматривать файлы и вложенные папки в данной папке, а также атрибуты папки, имя владельца и разрешения	читать файл и просматривать его атрибуты, имя владельца и разрешения
Write (запись)	создавать новые файлы и вложенные папки, изменять атрибуты папки, просматривать имя владельца папки и разрешения	перезаписывать содержимое файла, изменять его атрибуты, просматривать имя владельца файла и разрешения
List Folder Contents (список содержимого папки)	просматривать имена файлов в данной папке и вложенных в нее папок	–
Read & Execute (чтение и выполнение)	выполнять действия, предусмотренные разрешением Read и разрешением List Folder Contents	запускать приложения и выполнять действия, предусмотренные разрешением Read
Modify (изменение)	удалять папку и выполнять действия, предусмотренные разрешениями Write и Read & Execute	выполнять действия, предусмотренные разрешениями Write и Read & Execute
Full Control (полный доступ)	осуществлять все возможные действия	осуществлять все возможные действия

Разрешения NTFS указываются в окне «Properties» для конкретной папки

Определение параметров доступа для файла или папки



Предотвращение наследования разрешений иногда бывает полезно

Копирование файлов и папок

При копировании унаследованных файлов или папок разрешения на доступ к ним могут меняться. При копировании в пределах одного NTFS-раздела или между NTFS-разделами копия наследует разрешения, предоставленные той папке, которая стала для скопированных родительской.

Чтобы копировать в рамках одного NTFS-раздела или между NTFS-разделами, необходимо иметь разрешение Read на исходную папку и разрешение Write на папку, в которую будет произведено копирование.

Перемещение файлов и папок

При перемещении папки или файла в рамках NTFS-раздела сохраняются их первоначальные разрешения. При перемещении между NTFS-разделами папка или файл наследует разрешения целевой папки. Чтобы перемещать файлы и папки, необходимо иметь разрешение Write на целевую папку и разрешение Modify на исходную папку или файл. Разрешение Modify требуется для перемещения папки или файла, потому что при перемещении после выполнения копирования исходная папка или файл удаляется.

Табл. 2. Возможности определения разрешений для пользователя

Параметр	Описание
Name (имя)	выбор пользователя или группы, для которых требуется изменить разрешения или которые требуется удалить из приведенного списка
Permissions (разрешения)	Allow (разрешить) — предоставить соответствующее разрешение. Deny — запретить соответствующие действия
Add (добавить)	открыть диалоговое окно «Select User, Groups, or Computers» («Выбор пользователя, группы или компьютера»), используемое для выбора пользователей или групп, добавляемых в список Name
Remove (удалить)	удалить выбранную запись пользователя или группу

Табл. 3. Возможности объектов по наследованию разрешений

Вариант	Описание
Copy	копирование унаследованных разрешений от родительской папки для вложенных папок и файлов и запрещение дальнейшего наследования разрешений
Remove	удаление унаследованных разрешений для вложенных папок и файлов, сохранение только тех разрешений, которые предоставляются в явном виде

Использование разрешений NTFS

Администраторы и пользователи, имеющие разрешение Full Control, владельцы файлов и папок могут предоставлять пользователям и группам разрешения на файлы и папки.

Всегда предоставляйте разрешения в соответствии с реальными потребностями групп и пользователей. Предоставление разрешений NTFS производится в диалоговом окне «Properties» для конкретной папки.

При предоставлении или изменении разрешений NTFS на файл или папку можно добавлять или удалять пользователей, группы или компьютеры с разрешениями на доступ к ним.

На вкладке «Security» диалогового окна «Properties» для файла или папки задаются параметры, приведенные в табл. 2.

Рекомендуется позволить системе Windows Server 2003 переносить разрешения, предоставленные для родительской папки, на содержащиеся в ней вложенные папки и файлы.

Для предотвращения наследования вложенной папкой или файлом разрешений родительской папки нажмите кнопку «Advanced» на вкладке «Security» окна свойств папки. После этого снимите флажок «Allow inheritable permissions from parent to propagate to this object and all child objects. Include these with entries ex-

Табл. 4. Возможные значения специальных разрешений

Параметр	Описание
Name (имя)	определяется имя пользователя или группы. Для выбора одного из них нажмите кнопку «Change»
Apply to (применять)	определяется уровень иерархии папки, на котором наследуются эти специальные разрешения NTFS. Значением по умолчанию является «This folder, subfolders and files» («Для этой папки и вложенных в нее папок и файлов»)
Permissions (разрешения)	названия специальных разрешений
Apply these permissions to objects and/or containers within this container only (применять эти разрешения к объектам и контейнерам только внутри этого контейнера)	определяется возможность наследования вложенными папками и файлами специальных разрешений

» plicitly defined here» («Переносить наследуемые от родительского объекта разрешения на этот объект и все вложенные объекты. Включить их с данными, явно определенными здесь») и выберите один из двух вариантов, описанных в табл. 3.

Специальные разрешения

Специальные разрешения дают более широкие возможности предоставления прав доступа к ресурсам. Стандартные разрешения NTFS представляют собой различные сочетания тринадцати специальных разрешений. Например, стандартное разрешение Read разбивается на специальные разрешения Read Data (чтение данных), Read Attributes (чтение атрибутов), Read Permissions (чтение разрешений) и Read Extended Attributes (чтение дополнительных атрибутов).

Разрешение Change Permissions (смена разрешений) предоставляет пользователю возможность изменять разрешения для файла или папки, а Take Ownership (смена владельца) — стать владельцем файлов и папок. Разрешение Change Permissions обычно дается другим администраторам и пользователям для того, чтобы те, не обладая разрешением Full Control, имели право изменения разрешений на файл или папку. В этом случае администратор или пользователь не сможет ни удалить файл или папку, ни изменить их содержимое, однако сможет предоставлять другим разрешения на этот файл или папку.

Чтобы дать администраторам возможность изменять разрешения, наделите группу «Administrators» разрешением Change Permissions на требуемый файл или папку.

Разрешение Take Ownership позволяет передавать право владения от одного пользователя другому или к группе. К смене владельца файла или папки применяются следующие правила:

- текущий владелец или любой пользователь, имеющий право доступа Full Control, может наделять стандартным разрешением Full Control или специальным разрешением Take Ownership другого пользователя или группу;
- администратор может стать владельцем папки или файла независимо от предоставленных разрешений для этой папки или файла. Если администратор становится владельцем, владельцем становится и группа «Administrators», любой член группы «Administrators» может изменять разрешения для этого файла или папки и предоставлять разрешение Take Ownership.

Специальные разрешения, устанавливаемые для папок и файлов

Предоставление специальных разрешений пользователям и группам

Чтобы предоставить пользователям или группам специальные разрешения, необходимо выполнить следующие действия.

1. На вкладке «Security» диалогового окна «Properties» для файла или папки нажать кнопку «Advanced».

2. На вкладке «Permissions» диалогового окна «Advanced Security Settings» выбрать того пользователя или группу, которым нужно предоставить специальные разрешения NTFS, а затем нажать кнопку «Edit».

3. В диалоговом окне «Permissions Entry» для файла или папки задать описанные в табл. 4 параметры.

Отметим, что в большинстве случаев предоставлять специальные разрешения необходимости не возникает.

Минимум разрешений — максимум безопасности

Из сказанного можно сделать два вывода. Первый заключается в том, что в любом случае нужно стремиться свести число пользователей и групп к минимуму. Это облегчит работу администратора и, естественно, улучшит управляемость сети.

Вывод второй — предоставление пользователю минимально необходимых разрешений и прав обеспечивает максимально возможную безопасность.

Надеемся, понимание того, каким образом можно закрыть лазейки для хакеров при помощи правильного использования системы разрешений, поможет вам создать действительно безопасную и надежно функционирующую сеть.

■ ■ ■ Александр Гузиков

Хорошая практика

Правила, написанные жизнью

При предоставлении разрешений на доступ к ресурсам NTFS желательно учитывать следующие рекомендации.

- Предоставлять разрешения группам, а не пользователям. Это уменьшит размер ACL и повысит быстродействие.
- Группировать в папки приложений наиболее часто используемые программы, в папки данных — общие файлы данных, в домашние папки — файлы пользователя. Держите домашние папки и папки данных на отдельном разделе.
- Предоставлять пользователям права, обеспечивающие минимально необходимый уровень доступа.
- Создавать группы с уровнем доступа, требующимся членам группы, а затем при необходимости наделять их дополнительными разрешениями.
- При предоставлении разрешений на папки приложений наделять группы «Users» и «Administrators» только разрешением Read & Execute. Это позволит предотвратить случайное удаление или повреждение данных и приложений пользователями или вирусами.
- При предоставлении разрешений на папки данных наделять разрешениями Read & Execute и Write группу «Users», а разрешением Full Control — владельца. Это дает пользователям возможность читать и изменять документы, созданные другими пользователями, и читать, изменять и удалять файлы и папки, созданные ими самими.
- Разрешение Deny использовать только в тех случаях, когда необходимо запретить доступ к ресурсу.

Внутренний караул

Как сохранить конфиденциальность информации

Основным аргументом противников операционной системы Windows является ее недостаточная безопасность. Посмотрим, какие усилия при разработке новой серверной ОС были приложены фирмой Microsoft и как они повлияли на безопасность.

При разработке Windows Server 2003 особое внимание уделялось вопросам безопасности. С этой точки зрения одно из самых важных изменение в новой ОС — это изменение настроек сервера, принятых по умолчанию. Теперь по окончании установки сервер будет иметь очень ограниченный набор функций. Для того чтобы запустить, например, веб-сервер, придется дополнительно инсталлировать IIS (Internet Information Service), а затем и настраивать его. Впрочем, об этом мы уже говорили, поэтому давайте перейдем непосредственно к настройке безопасности встроенных серверов, так как электронная почта и доступ к ресурсам веб- и FTP-серверов по природе своей являются самыми распространенными лазейками для вирусов и хакеров.

Чтобы не увязнуть в Паутине

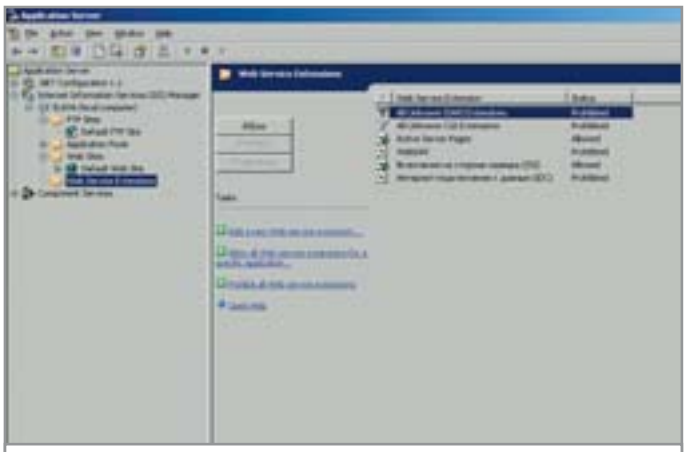
Итак, мы решили сделать из нашего свежеустановленного Windows Server 2003 веб-сервер. После завершения первоначальной его установки мы получим веб-сервер, обладающий минимальной функциональностью, при обращении он сможет выдавать только статические странички. Чтобы включить потенциально опасные возможности, такие, например, как поддержка технологий SSI (Server Side Include, включения на стороне сервера) и ASP (Active Server Pages, активные серверные страницы), необходимо вручную в приложении IIS Manager найти папку «Web Service Extensions» («Расширения веб-службы»), в которой разрешить работу дополнительных компонентов веб-сервера.

Необходимо убедиться, что у каталога, в котором находятся ASP-скрипты, есть разрешение на запуск этих скриптов. Это разрешение настраивается в свойствах папки из консоли управления IIS (IIS Manager). Если мы хотим ограничить доступ к веб-серверу или к его части в соответствии с учетными записями пользователей или их IP-адресами, то мы можем это сделать в тех же свойствах папки на вкладке «Security».

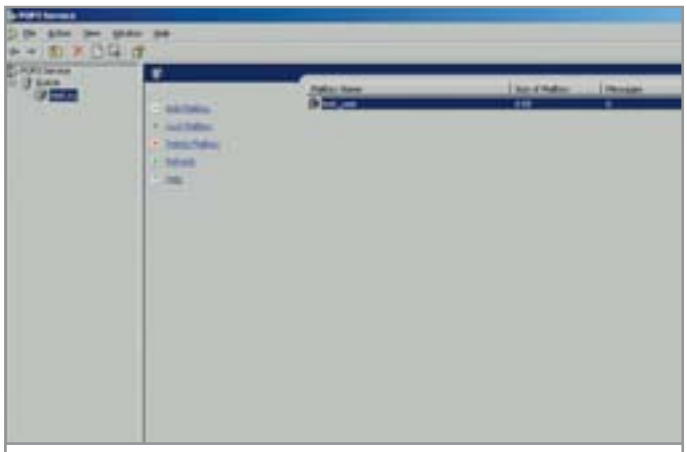
Теперь о вирусах. Вирусы используют специальным образом сформированные URL (в текст URL включаются специальные символы, в совокупности образующие скрипт), которые позволяют получить управление сервером и заставить его выполнять команды злоумышленника. Чтобы не допустить этого, необходимо использовать firewall с возможностью фильтрации URL или применять дополнительные средства, интегрирующиеся непосредственно в IIS. Например, у компании Microsoft есть утилита UrlScan, которая позволяет блокировать подозрительные запросы к веб-серверу.

На страже файлов

При создании FTP-сервера (и, соответственно, для последующей настройки его безопасности) необходимо указать каталог «Home Directory», к которому пользователи будут иметь доступ по протоколу FTP, а также права пользователей на закачивание и скачивание файлов. Помимо общих прав на запись или чтение, которые настраива- »



Работа потенциально опасных компонентов должна быть явно разрешена администратором вручную



Панель настройки POP3 позволяет добавлять, блокировать и удалять почтовые ящики пользователей

ются там же, на вкладке «Home Directory» в свойствах FTP-сервера, права доступа к конкретному файлу определяются NTFS-правами на локальный доступ к файлу. Ограничивать доступ к серверу можно и по IP-адресам, так же, как и в случае с веб-сервером. Соответствующая вкладка называется «Directory Security».

Еще один параметр, на который стоит обратить внимание, — это количество одновременных подключений к серверу (ftp site connection). Это число должно определяться шириной вашего канала в Интернете. По умолчанию оно составляет 100 000, но необходимо сократить его на несколько порядков. В противном случае ваш сервер может пасть жертвой DoS- (Denial of Service, отказ в обслуживании) или DDoS-атаки (Distributed DoS, DoS-атака, производимая одновременно с большого числа компьютеров).

Однако FTP-сервер, входящий в состав IIS, отвечает не всем потребностям администраторов. Для тех, кому не хватает возможностей по настройке безопасности встроенного FTP-сервера, можно порекомендовать популярный FTP-сервер Serv-U компании RhinoSoft (www.serv-u.com).

Надежный почтальон

Говоря о защите почтового сервера, необходимо вспомнить о том, что авторизация по протоколу POP3 может происходить как в обычном, так и в безопасном режиме с использованием технологии SPA (Secure Password Authentication, безопасная аутентификация пароля). Метод SPA передает пароли от клиента к серверу в зашифрованном виде, что позволяет исключить возможность перехвата. Однако способ авторизации на почтовом сервере является единственной настройкой, которой вы можете управлять. Использовать такой сервер в качестве почтового можно лишь внутри небольшой организации. Если вы планируете получать почту из Интернета или разворачивать полноценную систему корпоративной электронной почты, то без установки Exchange-сервера вам не обойтись.

Вирусам — бой!

На сегодняшний день есть три основных способа защиты от почтовых вирусов. Рассмотрим их в порядке увеличения надежности.

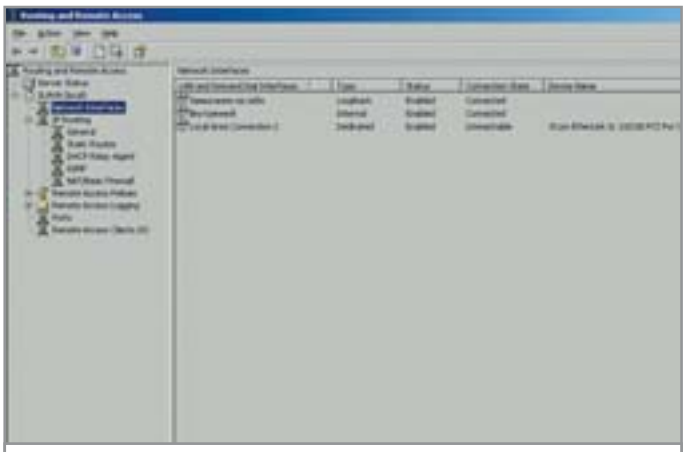
Третье место занимает антивирусное программное обеспечение, установленное на локальном компьютере каждого пользователя и проверяющее все приходящие письма. Очевидным недостатком такого подхода является отсутствие централизованного управления защитой. Антивирусное ПО может быть отключено, база данных вирусов может не обновляться, и, наконец, пользователь может просто использовать почтовую программу, в которую это антивирусное ПО не интегрируется.

Решением этих проблем является проверка почты непосредственно на сервере. Есть ПО, которое интегрируется прямо в почтовый сервер, например в Exchange, и наблюдает за почтовыми ящиками пользователей. Основным недостатком этого способа является невозможность обновления почтового сервера без одновременного обновления антивирусного ПО. Например, если компания Microsoft выпускает новый Service Pack для Exchange-сервера, то неизвестно, как поведет себя антивирус-

Учет произошедшего с сервером

Контора пишет

Все сервисы, предоставляемые операционной системой Windows Server 2003, имеют возможность ведения журнала для статистики использования ресурсов и выявления источников возможных атак на сервер. Например, если ваш веб-сервер стал очень медленно работать или совсем «завис», то имеет смысл заглянуть в журнал обращений к серверу и узнать, нет ли там некорректных запросов. То же самое относится к FTP-, SMTP-, POP- и другим серверам. Некоторые серверы имеют свой собственный лог-файл, формат и расположение которого настраивается в свойствах данного сервера (веб, FTP). Другие записывают необходимую информацию в общий журнал событий Windows, доступный для просмотра из приложения «Event Viewer» (SMTP, POP). По умолчанию события в лог-файлы таких серверов, как веб и FTP, пишутся в текстовом виде и непригодны для детального изучения. Чтобы получать наглядную картину и статистику, имеет смысл настроить запись событий в базу данных и потом с помощью специальных приложений, например, Crystal Report, строить таблицы и графики посещений сервера. Это позволит получить представление о том, что происходит на сервере, и быстро выявить атаку или просто неполадку в работе.



Remote Access Server может осуществлять подключения в нескольких разных режимах (VPN, dial-up и т. д.)

Возможности, предоставляемые Remote Access Server, достаточно широки — NAT, firewall, router

» ное ПО после обновления сервера и будет ли оно работать вообще.

Поэтому оптимальным представляется такой способ, при котором антивирус, установленный на программном или аппаратном firewall, сам сканирует получаемую почту. В этом случае можно порекомендовать запустить два почтовых сервера. Первый, вспомогательный, будет принимать письма, передавать их без изменений антивирусу и, в зависимости от результатов работы антивируса, удалять или передавать основному. Основной почтовый сервер будет в результате получать почту, уже проверенную на наличие вирусов. Соответственно и в ящик пользователей попадет почта, уже очищенная от всякой заразы. Этот способ является не только самым удобным, но и самым безопасным. Даже в случае выхода из строя антивирусного ПО в результате вирусной или хакерской атаки ваша почтовая система останется работоспособной по крайне мере для обмена почтой внутри компании.

Как самому не стать спамером

Еще одним бедствием, имеющим отношение к электронной почте, является спам, то есть рассылка рекламных сообщений по множеству адресов. Некоторые спамеры ищут в Интернете незащищенные почтовые сервера и используют их для массовой рассылки писем. Чтобы не оказаться в неприятной ситуации, убедитесь, что ваш почтовый сервер не может работать в качестве Relay-сервера, то есть он принимает почту только для пользователей своего домена и отправляет почту также только от пользователей своего домена. Не все почтовые сервера имеют такую установку по умолчанию.

Если же вы окажетесь жертвой спамеров, то вас могут поджидать две крупные неприятности. Во-первых, ждите от вашего провайдера счет на крупную сумму (если вы платите за трафик). Во-вторых, у вас могут возникнуть неприятности с законом, так как борьба со спамерами в настоящее время переходит из области технической в область юридическую.

Посторонним вход воспрещен!

Предоставление удаленного доступа для сотрудников компаний подвергает вашу сеть дополнительному риску. Для того чтобы попасть в локальную сеть изнутри, нужно не только указать логин и пароль, но и как минимум пройти мимо пункта охраны. В случае же удаленного доступа вам придется доверять только технике и программному обеспечению.

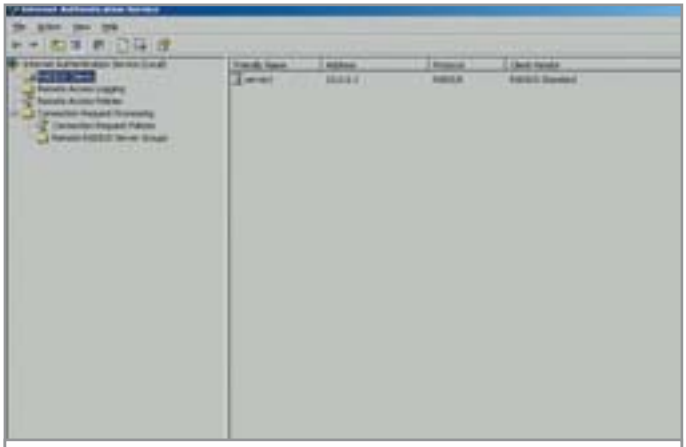
Персональная идентификация

Одной из самых надежных является система одноразовых паролей. В такой системе каждый желающий получить удаленный доступ имеет жетончик с дисплеем, на ко- »

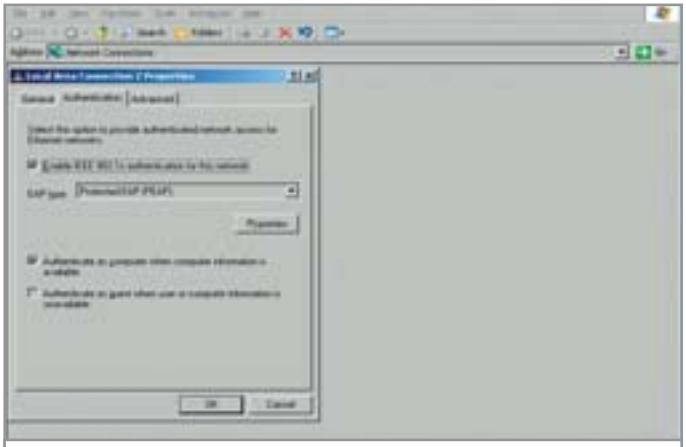
Недоработка в системе защиты

Даже стены имеют уши

Электронные письма на пути до адресата проходят через массу почтовых серверов. Администратор каждого их них может при желании прочесть содержимое вашего письма. Более того, существует возможность фильтровать почтовый трафик и вылавливать письма, содержащие заранее определенные сочетания символов, как в служебных полях, так и в самом теле письма. Поэтому свои сообщения необходимо защищать. В почтовом сервере в Windows Server 2003 никаких средств защиты исходящего трафика не предусмотрено. Забота об этом ложится на почтового клиента. При необходимости сохранить послание в тайне можно воспользоваться программами шифрования, например, широко известной PGP или же программами стеганографии. В первом случае вероятность того, что сообщение прочтет только адресат, практически равна единице. Во втором вы сможете скрыть не только содержание сообщения, но и сам факт посылки сообщения. Сервис Messenger, который является просто красивой оболочкой над командой net send, вообще беззащитен. Это означает, что сообщения, посланные при помощи Messenger, могут быть с легкостью получены любым пользователем сети. Никаких средств защиты текста в Messenger не предусмотрено. Отсюда выводы — этим средством передачи сообщений следует пользоваться либо в абсолютно защищенных сетях, либо предварительно шифровать текст, либо не передавать важные сообщения при помощи Messenger. Можно достичь цели и одним ударом — запустить сервис IPSEC, который возьмет на себя задачу шифрования трафика.



Internet Authentication Service позволяет быстро и легко получить информацию о каждом пользователе сети



Не установив эту галочку, администратор рискует скомпрометировать всю конфиденциальную информацию

тором высвечивается некоторое число, меняющееся через определенные промежутки времени и по определенному алгоритму. По такому же алгоритму меняются числа на самом сервере, отвечающем за предоставление доступа. При авторизации через удаленный доступ пользователь должен ввести свой PIN и это число. Пароль составляется из этих двух компонентов.

Одновременная компрометация PIN и утрата пользователем своего жетона, разумеется, маловероятны. Даже если злоумышленник, зная ваш PIN, подглядит цифры на жетоне, то через пару минут этот пароль уже устареет и воспользоваться им будет нельзя.

Защита корпоративных ресурсов

Впрочем, можно ограничиться обычной авторизацией с помощью стандартного имени пользователя и пароля. Для того чтобы сделать из Windows Server 2003 сервер удаленного доступа, необходимо добавить ему роль, которая так и называется — сервер удаленного доступа.

После установки этой роли сервер сможет выполнять следующие основные функции.

- Создавать VPN-сервер для подключения удаленных клиентов через Интернет.
- Предоставлять удаленный доступ для подключения клиентов по модему.
- Осуществлять маршрутизацию по требованию (demand-dial connections). Если сервер работает в качестве маршрутизатора и подключается к провайдеру по модему, то поддерживать соединение постоянно не обязательно, особенно если вы платите за время подключения. Когда кто-нибудь из пользователей решит, например, почитать новости на сайте или отослать письмо, то сервер получит запрос, требующий получения доступа к внешним ресурсам, и сам дозвонится до провайдера. По истечении тайм-аута в случае отсутствия внешнего трафика произойдет отключение модема.
- Осуществлять трансляцию адресов (NAT) и фильтрацию трафика (firewall).
- Настраивать сервер в качестве маршрутизатора. Поддерживаются протоколы динамической маршрутизации RIP и OSPF. После настройки сервера управление и конфигурация осуществляются через консоль Routing and Remote Access. Авторизация пользователей на сервере удаленного доступа может происходить с использованием учетных записей самого Windows Server 2003 и с использованием специального протокола RADIUS.

Этот протокол является протоколом авторизации, и существуют его реализации для всех известных платформ. Сервер, на котором хранится база пользователей, работающий по этому протоколу, называется RADIUS-сервером. Его использование оправданно в тех случаях, когда в сети есть несколько серверов доступа и необходимо иметь единую централизованную базу пользователей.

RADIUS-сервер можно установить и на Windows Server 2003. Однако по каким-то причинам в Windows Server 2003 он называется Internet Authentication Service. Установка его производится через через консоль Add or Remove Programs.

RADIUS-сервер может оказаться очень полезным при развертывании беспроводных сетей. Любой человек с ноутбуком или наладонником, в котором установлена карта радиодоступа, может перехватить гуляющую в радиосети информацию, близко подойдя к ней. Для борьбы с этой проблемой используются различные протоколы шифрования трафика, которые делают процесс декодирования весьма трудоемким. Однако эта задача является проблемой точек доступа и сетевых беспроводных карт и сам Windows Server 2003 тут вряд ли чем-то поможет.

Однако беспроводные сети таят в себе и другую опасность. Если не используется никакой механизм авторизации доступа к сети, то любой желающий может стать ее частью и использовать ее ресурсы, то есть получить бесплатный доступ к Интернету и к конфиденциальным ресурсам организации. Для предотвращения подобных случаев был разработан протокол 802.1x. На сегодняшний день он поддерживается практически всеми коммутаторами и точками радиодоступа и реализован в Windows XP и Windows Server 2003. В свойствах сетевого подключения есть вкладка «Authentication», в которой можно настроить доступ к сети в том случае, если для этого требуется авторизация 802.1x.

Сам протокол работает следующим образом. Точка радиодоступа получает запрос от нового клиента на доступ в сеть и запрашивает его пароль. Клиентский компьютер посылает в ответ имя и пароль учетной записи. По умолчанию посылаются имя и пароль учетной записи работающего в данный момент пользователя. Точка радиодоступа, получив ответ, пересылает его на RADIUS-сервер, который проверяет, есть ли у него такая запись в своей базе. Если RADIUS-сервер дает добро, то точка доступа разрешает данному клиенту работать в сети.

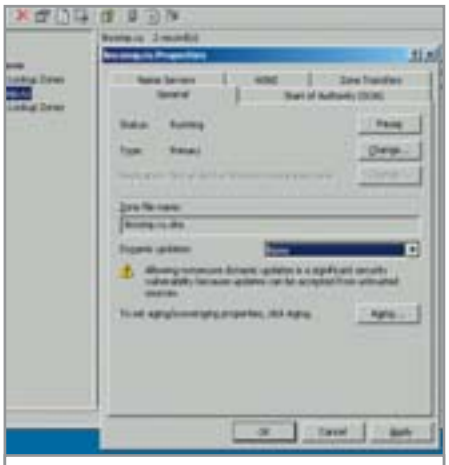
» Заделываем щели

По мере роста числа компьютеров управление сетью становится все более трудоемкой задачей. Каждому компьютеру надо присвоить IP-адрес, сообщить адрес шлюза по умолчанию и DNS-сервера. Для того чтобы избавить себя от беготни к каждому компьютеру в случае изменения адреса DNS-сервера, можно раздавать все эти настройки централизованно, используя для этого сервер DHCP. При загрузке операционной системы она пытается найти в сети этот сервер и, в случае успеха, просит сообщить всю интересующую ее информацию.

Но авторизовать DHCP-сервер, к сожалению, невозможно. Если кто-то внутри локальной сети установит и запустит свой DHCP-сервер, то клиентский компьютер может получить неправильный IP-адрес со всеми вытекающими отсюда последствиями. Если вдруг вы обнаружите, что компьютер получил какой-то странный адрес, то вам придется искать в вашей сети «левый» DHCP-сервер.

Команда ipconfig /all поможет узнать адрес DHCP-сервера, с которого компьютер получает свои настройки. Если сервер является частью Active Directory, то запустить DHCP-сервер уже не получится, однако можно установить Windows Server 2003 в режиме Standalone и дальше делать что хотите.

DNS-сервер отвечает за привязку имен компьютеров к IP-адресам. Если вы владеете собственным доменным именем, то записи о компьютерах в вашем домене будут храниться на DNS-сервере, который может располагаться либо у провайдера, либо непосредственно в вашей локальной сети. Если вы решите установить свой собственный DNS-сервер, то будьте крайне осторожны и внимательны при его настройке. Реализация этого сервера в Windows Server 2003 поддерживает динамическое обновление записей. Однако если вы не уверены, что вам это нужно, то лучше данную функцию отключить. Но динамическое обновление необходимо в случае установки на сервере контроллера домена. ■ ■ ■ Вячеслав Лущинский



Ответственность за принятие решения о характере динамического обновления DNS-сервера ложится на администратора сети

Шифрование трафика

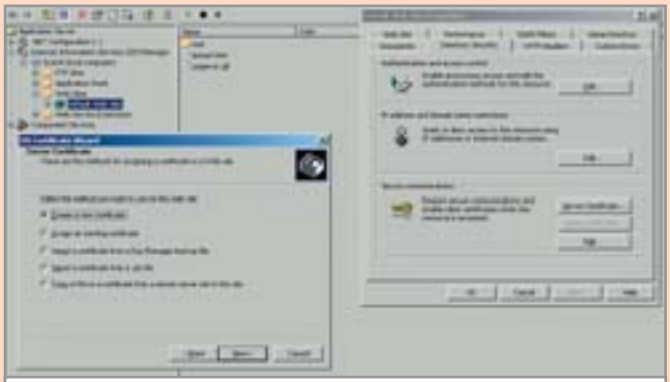
Прочитал буквы, но не понял слова

Операционная система Windows Server 2003 обладает богатым набором функций всевозможного шифрования. В частности, вы можете шифровать трафик между сетями или между компьютерами. Настройка шифрования трафика по протоколу IPSEC в среде серверов Windows не является очень сложной задачей, поэтому после настройки сервера стоит подумать, для защиты какой категории данных следует приложить дополнительные усилия.

Некоторые серверы, такие как почтовый или веб-сервер, имеют собственные механизмы шифрования трафика. Для веб-серверов этот механизм называется SSL (Secure Socket Layer). Однако для его настройки вам придется ознакомиться с технологией цифровых сертификатов, что потребует значительных усилий, так как тема эта достаточно сложна и объемна. После этого вам придется разворачивать сервер выдачи сертификатов либо на базе собственного Windows Server 2003, либо заказывать такой сертификат у других организаций, предоставляющих подобные услуги, например у компании VeriSign (www.verisign.com). Выданный сертификат должен пользоваться доверием как отправителя, так и получателя сообщения.

На рынке существует много продуктов, позволяющих контролировать входящий трафик. Эти системы называются IDS (Intrusion Detection System, системы обнаружения вторжения). Такие системы помимо стандартных функций firewall позволяют контролировать трафик на соответствие стандартам различных протоколов (HTTP, SMTP, FTP и другие), и если встроенные в операционную систему средства защиты окажутся недостаточными, то всегда можно построить «пуленепробиваемую стену» вокруг вашей сети.

Консоль установок безопасности — сердце всей системы безопасности компьютера



Для настройки и получения цифровых сертификатов используется специальный wizard

Чтобы сервер был здоров

Регулярные операции

Надежная работа каждого сервера зависит не только от типа установленной ОС, но также и от его периодического обслуживания. Внимание и регулярность при выполнении операций резервного копирования, отслеживания событий системы, дефрагментации и установки пакетов обновлений обеспечат стабильную функциональность сервера.

Итак, вы установили операционную систему и выполнили настройку вашего сервера. С этого момента администратор обязан регулярно отслеживать состояние основных компонентов и служб Windows. В большинстве случаев в этом поможет «Event Viewer» («Просмотр событий»), доступный в разделе «Administrative Tools» («Администрирование»). Это приложение состоит из нескольких журналов, чье количество зависит от функциональных ролей, которые выполняет ваш сервер (рис. 1). Замечательной особенностью оснасток w2k3 является их возможность отображать не только локальные ресурсы, но ресурсы любого другого компьютера, работающего под управлением Windows Server 2003. Используя консоль управления Microsoft (mmc.exe), можно настроить отображение событий сразу со всех серверов. В журналах регистрируется множество событий, прямо или косвенно влияющих на работу операционной системы. Следует обращать внимание на источник события и его идентификационный номер (event ID), а также на его тип (предупреждение или ошибка). Если что-то вызывает у вас подозрение, выполните анализ сообщения, посмотрите, когда оно стало появляться, не связано ли его появление с вашими действиями по настройке/изменению системы или оборудования. Если причина появления по-прежнему остается для вас »

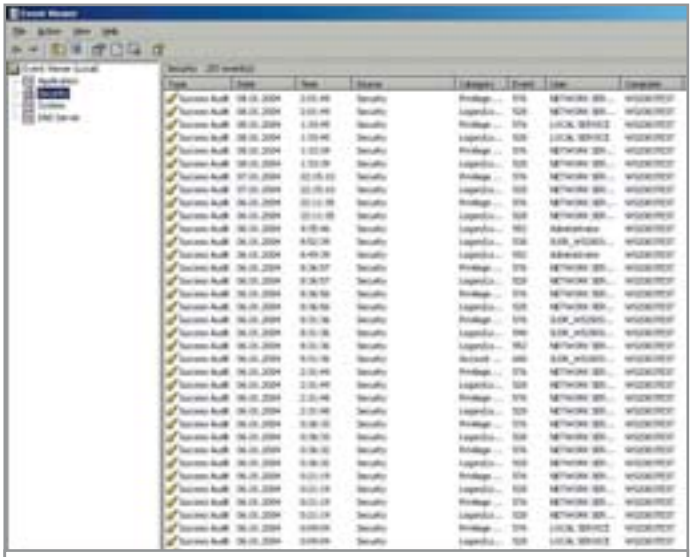


Рис. 1. В журнале «Event Viewer» регистрируется множество системных событий

Рис. 2. Выбор необходимых компонентов, подлежащих регулярному резервному копированию

» загадкой, следует выполнить поиск по номеру и источнику события в базе знаний Microsoft, находящейся по адресу http://support.microsoft.com/default.aspx?scid=fh;RU;KBHOWTO (рис. 3) (или специальный ресурс http:// eventid.net /search.asp). Регулярный просмотр журналов w2k3 позволит вам выявлять потенциальные проблемы заранее.

Резервное копирование

Если с журналами все в порядке, то следующим шагом необходимо составить план резервного копирования. В зависимости от ролей сервера (файловый сервер, маршрутизатор или доменный контроллер) план должен быть у каждого свой. Прежде всего необходимо обеспечить резервирование компонентов операционной системы, а уже потом программных файлов и данных. Основные компоненты представлены в «System State», отображаемой программой архивации (ntbackup.exe) как отдельный элемент в списке выбора (рис. 2). Наиболее приемлемым является резервирование состояния системы, разделов «\Document and Settings», «\Program Files», «\Windows» и файлов из корня системного раздела. Остальное для Windows, как правило, не важно. В Windows Server 2003 есть мастер аварийного восстановления системы, вызываемый из программы архивации, который может упростить восстановление сервера в случае сбоя. Однако он обладает существенным недостатком — нельзя выполнять автоматическое создание резервного набора. Администратор должен лично находиться за консолью компьютера. А хотелось бы автоматизировать процесс резервирования. Как это правильно сделать? Рекомендуется выполнять такую последовательность действий.

Рис. 3. База знаний Microsoft

- Спланируйте, что вы хотите резервировать, когда и куда будете сохранять резервные копии.
- Необходимыми правами на выполнение резервного копирования системных каталогов обладают учетные записи, являющиеся членами локальных групп «Administrators» и «Backup Operators». Поэтому следует создать новую учетную запись (например «BackupUser»), установить свойство «Password never expires» («Пароль никогда не истекает») и включить его в одну из вышеперечисленных групп.
- Зарегистрируйтесь на сервере от имени этого пользователя и запустите программу архивации («Start → Accessories → System Tools → Backup»).
- Выберите режим «Schedule» («Расписание»), при этом будет предложено сохранить в отдельном файле пути к тем компонентам, которые вы выбрали (по умолчанию этот файл будет сохранен в локальном профиле текущего пользователя). Задайте понятное имя вашему расписанию, лучше всего это сделать в формате ЧТО_КУДА, например SystemStateToServer01.
- После этого расписание будет создано. Удобнее всего управлять им не через программу архивации, а через «Scheduled Task» («Назначенные задания») в «Control Panel». Запустите его и убедитесь, что резервная копия создана.

Несколько рекомендаций по резервированию. Не создавайте назначенные задания от имени администратора, так как при смене им пароля запланированное задание перестает выполняться, практически никак вас об этом не предупреждая. Выполняйте спаренное резервирование по сети (если отсутствуют ленточные накопители), то есть сохраняйте резервную копию одного сервера в общую папку другого. Правильно настройте списки доступа к таким общим папкам — полный доступ должен быть предоставлен только пользователю «BackupUser», а их чтение администраторам. Остальные пользователи не должны иметь доступ к этим каталогам.

Профилактика

Основные моменты обслуживания мы затронули. Однако для увеличения надежности и производительности системы необходимо проводить и некоторые профилактические работы. Основной из них является дефрагментация жестких дисков. Microsoft наконец-то включила в состав ОС команду вызова дефрагментации (ранее для проведения дефрагментации сер- »

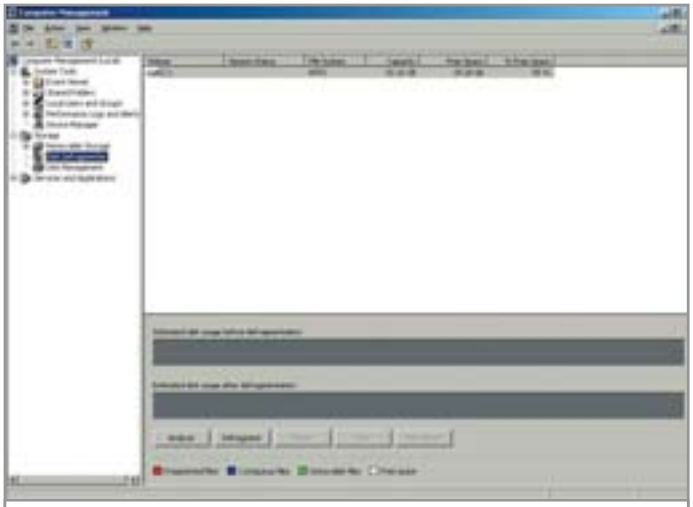


Рис. 4. Дефрагментацию разделов диска можно запустить из оснастки «Computer Management»

Рис. 5. Также дефрагментацию разделов можно провести с помощью консольной команды defrag.exe

» вера требовалась непосредственная регистрация на консоли сервера). Дефрагментацию разделов можно запустить либо из оснастки «Computer Management» («Управление компьютером») (рис. 4), либо командой defrag.exe из командной строки (рис. 5). Особенно полезно выполнять регулярную дефрагментацию разделов для файловых серверов. Так же как и для резервного копирования, необходимо составить план дефрагментации разделов сервера и выполнять его по расписанию. Для этого следует создать командный файл с командой defrag.exe и соответствующими ключами. Затем необходимо задать новое назначенное задание, которое и будет запускать только что созданный файл в установленное время. Естественно, что дефрагментацию следует выполнять в часы наименьшей нагрузки сервера.

Рис. 6. Настройка режимов автоматического обновления системы

Установка обновлений

И, напоследок, на операционную систему необходимо устанавливать пакеты исправлений, которые Microsoft периодически выпускает. Пакеты исправлений и заплатки доступны для загрузки с сайта http://windowsupdate.microsoft.com напрямую. Однако в ОС предусмотрена возможность автоматической загрузки обновлений. Этот режим реализован службой «Automatic Updates» («Автоматическое обновление»). Чтобы выполнить настройку этой службы, необходимо обладать правам администратора системы. В панели управления необходимо выбрать элемент «System» и перейти на закладку «Automatic Updates» (рис. 6), а затем установить переключатель в положение «Automatically download the updates, and install them on the schedule that I specify» («Автоматически загружать обновления и устанавливать их по расписанию, которое будет указано»). Выберите время, в которое вы желаете устанавливать обновления. Служба автоматического обновления будет загружать недостающие обновления в фоновом режиме. После завершения загрузки служба дождется назначенного времени и установит обновления, при этом все пользователи, подключенные к консоли, получат уведомление о готовности установить закачанное обновление. Если подтверждения или отказа от установки не последует в течение пяти минут, то сервер самостоятельно установит обновления и перезагрузит сервер. Можно отказаться от продолжения установки в этот раз и перенести ее на следующее назначенное время. Будьте внимательны — если подобный режим работы не пригоден для вашего сервера, следует выбрать другие варианты установки обновлений. Помните о том, что желательно иметь резервную копию состояния системы, так как в случае ошибки при установке обновления сервер может стать неработоспособным.

Вариант с автоматической загрузкой обновлений из Интернета неплох, если у вас один сервер, а что делать, когда таких серверов несколько? В этом случае можно развернуть в сети службу Software Update Services (служба установки обновлений). При этом только один сервер будет подключаться к серверу Windows Update и закачивать обновления, остальные компьютеры смогут забирать эти обновления по локальной сети. Этот дополнительный компонент доступен для загрузки непосредственно с сайта Microsoft (http://microsoft. com/windowsserver2003/sus/default.mspx). Примеры настройки и работа с данной службой выходят за рамки статьи, но важно знать, что такая возможность все же есть.

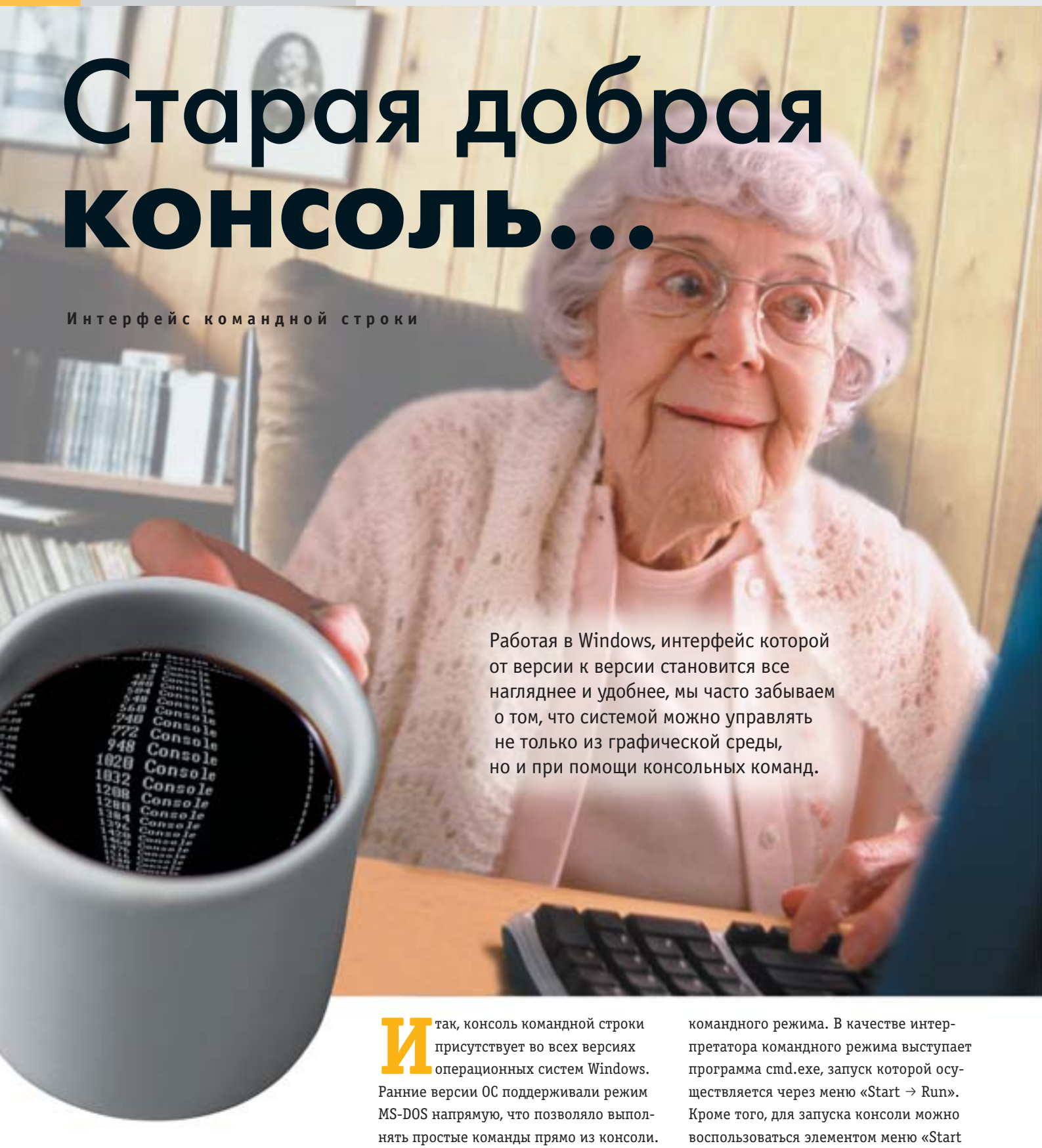
Заключение

Правильно спланированное и регулярное проведение различных профилактических и сервисных работ позволит предотвратить большинство сбоев не только самого сервера, но и сети в целом. Как правило, проведение всех этих действий занимает гораздо меньше времени, чем даже однократное восстановление работоспособности отказавшего сервера, которому администратор не уделял достаточного внимания.

■ ■ ■ Владимир Елисеев

Старая добрая консоль...

Интерфейс командной строки



Работая в Windows, интерфейс которой от версии к версии становится все нагляднее и удобнее, мы часто забываем о том, что системой можно управлять не только из графической среды, но и при помощи консольных команд.

Итак, консоль командной строки присутствует во всех версиях операционных систем Windows. Ранние версии ОС поддерживали режим MS-DOS напрямую, что позволяло выполнять простые команды прямо из консоли. Представители же семейства NT, такие как Windows 2000 или Windows Server 2003, работают уже совсем по другим принципам, однако MS-DOS в них тоже поддерживается, но через виртуальную машину (NT Virtual DOS Machine, NTVDM), что позволяет контролировать и администрировать системные ресурсы прямо из консоли командного режима. В качестве интерпретатора командного режима выступает программа cmd.exe, запуск которой осуществляется через меню «Start → Run». Кроме того, для запуска консоли можно воспользоваться элементом меню «Start → All Programs → Accessories → Command Prompt».

Запустив консоль командного режима, пользователь может управлять ресурсами как локальной системы, так и ресурсами удаленной машины. Существуют команды, выполняющие мониторинг системы и выявляющие критические места в настрой- »

» ках сервера. Отличием работы из командной строки является полное отсутствие больших и громоздких графических утилит. Программы командной строки позволяют более тонкую настройку в виде параметров-ключей, указанных справа от самой команды.

С помощью специальных файлов-скриптов (наборов команд, выполняющихся последовательно или в запрограммированном порядке) администратор может свести к минимуму выполнение рутинных ежедневных операций. Существующие современные утилиты могут запускать такие скрипты с заданной периодичностью без присутствия администратора системы.

Сам администратор может выполнять как одиночные команды, так и список команд, используя специальные управляющие символы (&, |). Например:

Команда 1 & Команда 2 — сначала будет выполнена Команда 1 и только затем Команда 2;

Команда 1 && Команда 2 — только после успешного выполнения Команды 1 будет запущена Команда 2.

Существует возможность перенаправить выводимый программой поток напрямую в текстовый файл для дальнейшей обработки. Для этого необходимо использовать управляющий символ «>» и имя текстового файла. Пример вывода содержания текущего каталога в текстовый файл Report.txt при помощи команды dir приведен ниже:

```
dir > Report.txt
```

Администратор может запустить несколько копий консоли, вызвав в командной строке программу cmd.exe. Использование вложенной консоли позволяет работать с переменными окружения операционной системы без каких-либо последствий для всей системы в целом, так как после закрытия вложенной консоли изменения переменных окружения не сохраняются. Для контроля над этим процессом используются команды setlocal, endlocal и set.

В современных операционных системах существует множество команд и утилит. Запомнить такое количество различных программ, а тем более их параметров очень сложно, поэтому одним из самых важных параметров для каждой программы является сочетание символов /?. Выполнив команду с таким параметром, пользователь получит исчерпывающее сообщение о применении утилиты и синтаксисе ее параметров.

Обратите внимание, что на рисунке в левом верхнем углу следующей страницы использован сложный синтаксис. Так, сразу после команды shutdown /? после специального разделителя «|» идет команда more, что позволяет выводить информацию на экран не целиком, а определенными порциями, удобными для дальнейшего чтения.

Для того чтобы закрыть консоль командной строки, необходимо выполнить команду exit.

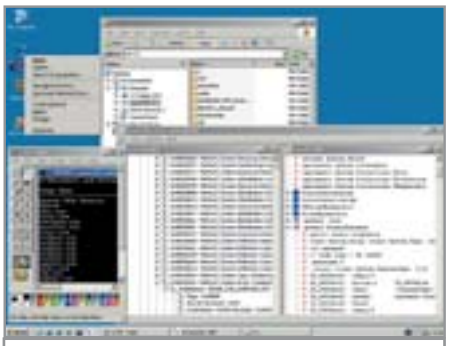
Кто здесь главный?

По своим возможностям консольные программы делятся на:

- команды управления операционной системой — это такие команды, как shutdown или taskkill;
- сетевые команды — net и ipconfig;
- команды для мониторинга системы — tasklist и systeminfo;
- команды для поддержки файловой системы — dir, mkdir, copy;
- команды для обслуживания жестких дисков — defrag и diskpart;
- команды для поддержки службы каталогов (Active Directories) — addrep и dsadd;
- вспомогательные команды, в этот раздел входят различные утилиты для создания сценариев, настройки принтеров, работы с переменными окружения и т. д.

Рассмотрим типичных представителей каждой группы и позволим себе дать некоторые рекомендациями по использованию включенных в них команд.

Вызов команды на выполнение (элемент «Run» отмечен подсветкой)



Графический интерфейс Windows Server 2003 не всегда более удобен

Команды мониторинга и диагностики

Для выявления неполадок в аппаратной части и проблем с программным обеспечением предназначены команды мониторинга, такие как systeminfo и tasklist. Эти утилиты впервые появились только в операционной среде Windows Server 2003, поэтому администраторы еще не в полной мере оценили функциональные возможности этих команд. Так, например, теперь не надо залезать в закладку «Свойства» иконки «Мой компьютер» — команда systeminfo напечатает на экране консоли основную информацию обо всех компонентах системы с полной расшифровкой. Параметр /s выведет информацию о любом удаленном компьютере. Например, для выяснения конфигурации компьютера TESTSERVER необходимо выполнить следующую команду:

```
systeminfo /s TESTSERVER
```

А утилита tasklist покажет процессы, запущенные на вашем компьютере.

Утилита tasklist позволяет опрашивать системы, соединенные в сеть. Параметр /v дает возможность получать подробные листинги с полезной информацией, в том числе и об именах пользователей, а параметр /m показывает процессы, загрузившие конкретный dll-файл. Другая полезная утилита — openfiles — позволяет получить информацию обо всех открытых файлах локальной и удаленной операционной системы. В прежних версиях операционных систем Windows приходилось использовать команду oh.exe, в современных версиях достаточно выполнить в командной строке консоли команду, которая устанавливает режим мониторинга для всех открытых файлов системы: »

Результат выполнения операции shutdown /? весьма информативен

```
openfiles /local on
```

Пользователь получит информацию обо всех открытых файлах системы, используя команду с простым синтаксисом:

```
openfiles
```

Команда openfiles с параметрами /query /v показывает, какие пользователи запустили процессы, открывшие файлы. С помощью других параметров-ключей можно задать различный режим вывода информации.

Команды управления операционной системой

Windows Server 2003 предоставляет администраторам новые команды, которые помогают не только диагностировать систему, но и управлять ею. К таким командам можно отнести утилиту shutdown. В качестве параметров-ключей этой утилиты можно использовать следующие:

- /s — полное штатное отключение системы;
- /r — перезагрузка;
- /p — выключение питания;
- /f — завершение работы активных приложений;
- /h — переход в режим пониженного энергопотребления;
- /I — завершение сеанса без отключения компьютера.

В виде средства, регистрирующего все штатные выключения компьютера, выступает обработчик событий штатных выключений (Shutdown Event Tracker), который собирает и диагностирует все отключения, выполненные администратором. Также предусмотрена возможность выключать систему с указанием причины, для этого необходимо использовать ключ /d.

Команда taskkill, аналог команды kill в операционных системах семейства *nix, позволяет «убить» зависшее приложение. Совместно с командой tasklist эти утилиты представляют собой мощное средство для оперативного вмешательства в ход выполнения приложений, представляющих потенциальную угрозу для производительности сервера. Из параметров этой команды необходимо отметить ключ /pid, который позволяет завершать процесс по его уникальному идентификатору, и ключ /im — для завершения приложения с указанным именем. Следующий пример позволяет завершить процессы с идентификаторами 1000 и 1240:

```
taskkill /pid 1000 /pid 1240
```

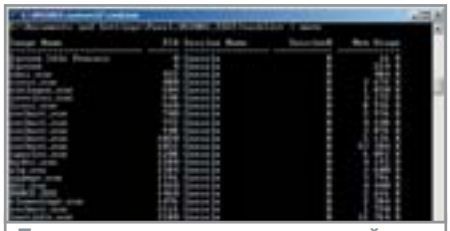
Команды для обслуживания жестких дисков

Оптимизацию жесткого диска позволяет выполнить команда defrag. Утилита умеет дефрагментировать диски с файловой системой FAT, FAT32 и NTFS. Defrag одинаково хорошо работает как с динамическим типом диска, так и с базовым. Синтаксис вызова этой команды следующий:

```
defrag диск [ -a ] [ -f ][ -v ] [ -? ]
```

Параметр -a предусматривает только анализ информации на диске, параметр -f — оптимизацию информации, в том числе и при отсутствии необходимого дискового пространства для создания временных файлов, а параметр -v — вывод отчета о ходе оптимизации. Не забудьте, что для успешной дефрагментации диск должен содержать как минимум 15% свободного места.

Команда fdisk уже не поддерживается ядром операционной системы Windows Server 2003. На смену ей пришла команда diskpart, также предназначенная для обслуживания жестких дисков. Разбить диск на разделы, создать логические диски, удалить их — вот лишь некоторые задачи, решаемые этой утилитой. В основном команда diskpart ориентирована на работу со специальными файлами-сценариями,



Пример выполнения консольной команды tasklist

в которых описаны процедуры обслуживания жестких дисков. Вот как выглядит вызов этой команды для файла-сценария Script1.txt:

```
diskpart /s Script1.txt
```

Каждая строка такого файла является инструкцией для какой-нибудь операции. Так, например, дает команду для создания нового раздела с определенным размером строка

```
create partition logical size=2048
```

Сетевые команды

Среди сетевых команд хотелось бы выделить две утилиты. Первая — это команда ipconfig, вторая — netstat. Системные администраторы используют эти команды не только для мониторинга сети, но и для защиты от опасных программ, пытающих установить контроль над системой.

При помощи утилиты ipconfig пользователь может узнать сетевой адрес своего компьютера, а вызвав эту команду с параметром /all, получить полную информацию о конфигурации сети на локальном компьютере. Параметр /renew позволяет изменить сетевые настройки без перезагрузки всей системы в целом.

Если вы заметили, что с вашим компьютером происходит что-то неладное, то в этом случае поможет команда netstat, которая не только укажет на открытые сетевые порты, по которым злоумышленники могли подсоединиться к вашей системе, но и идентифицирует процессы, запу-

Команда	Описание
whoami	выводит информацию о доменном имени, имени компьютера, имени пользователя, имени группы, привилегиях и политике для текущего пользователя
ftp	запускает процесс обмена данными по протоколу FTP
nlb	позволяет производить мониторинг сетевых соединений
nlbmgr	производит настройку системы кластеров Network Load

Табл. 1. Сетевые команды операционной системы Windows Server 2003

Команда	Описание
copy	копирует файлы
del	удаляет один или более файлов
dir	выводит список файлов и поддиректорий в выбранном каталоге
find	ищет заданную подстроку в файлах
move	перемещает файлы
mkdir	создает каталоги
rmdir	переименовывает и удаляет каталоги
tree	выводит иерархическое дерево всех файлов и поддиректорий в выбранном каталоге

Табл. 2. Список команд для поддержки работы с файлами и директориями в операционной системе Windows Server 2003

» щенные на сервере без вашего ведома. Так, ключ /o выводит информацию об идентификаторе процесса (PID), использующего то или иное сетевое соединение. Существует возможность посмотреть, какие компьютеры в сети взаимодействуют с вашей локальной операционной системой. Примерный список других полезных сетевых команд приведен в табл. 1.

Команды для поддержки службы каталогов

Вся сеть состоит из компонентов и представляет собой сложную иерархическую структуру, построенную в виде дерева. Объектами такой системы являются сайты, подсети, серверы, компьютеры, группы, пользователи, контакты, разделяемые сетевые устройства.

Для мониторинга такой сложной структуры в операционной системе предусмотрена команда dsquery, которая предназначена для расширенного поиска компонентов службы каталогов. Также этой командой можно пользоваться для вывода информации о свойствах выбранных компонентов (ключ -attr). Параметры -scope, -subtree, -onelevel, -base определяют уровень вложенности поиска, а ключ -filter позволяет задействовать фильтр поиска.

Команда dsmod может помочь в случае необходимости модификации одной или нескольких учетных записей для выбранного компонента службы каталогов. Например, можно удалить пользователя из группы или назначить ему новый пароль. Пример изменения учетной записи для пользователя TestUser приведен ниже:

```
dsmod user
"CN=TestUser,CN=Users,DC=bigtex,DC=net
" -pwd Uf@tfingereIt -mustchpwd yes
```

Команда dsmove перемещает объект в пределах текущего домена. При помощи ключей -newname и -newparent можно задавать новое имя объекта и менять его местоположение.

Команды для поддержки файловой системы

Описание некоторых часто употребляющихся команд для работы с файлами и директориями представлено в табл. 2. Команду deltree, которая выполняла каскадное удаление папок и файлов в них, заменяет теперь rmdir с ключом /s.

Заключение

Ну, вот и все. Мы рассказали об основах работы с консолью. Дальше предоставляем вам возможность самим исследовать функциональность и многообразие консольных команд. Только не забывайте заветный ключ /?, а остальное придет со временем и опытом. ■ ■ ■ Андрей Озеров

Тонкая настройка консоли

Маленькие секреты большой системы

Изменение приглашения для командной строки

Найдите в реестре ключ:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session\Manager\Environment]
Создайте в этом ключе строковый параметр «PROMPT» с типом (REG_EXPAND_SZ) и присвойте одно из следующих значений:

- $B — вертикальная черта «|»;
- $D — текущая дата;
- $G — знак больше «>»;
- $L — знак меньше «<»;
- $N — текущий диск;
- $P — текущий диск и путь;
- $Q — знак равно «=»;
- $T — текущее время;
- $V — версия Windows;
- $$ — знак доллара «$».

После перезагрузки вы увидите приглашение в определенном вами виде.

Автонабор команд

Для включения возможности автонабора команд по нажатию клавиши «Tab», найдите в реестре ключ:
[HKEY_CURRENT_USER \Software \Microsoft \Command Processor]
Затем установите значение параметра CompletionChar равным 9, что соответствует идентификатору клавиши «Tab», закройте реестр и перезагрузите компьютер. В окне консоли, набирая часть имени команды, вы можете теперь нажать клавишу «Tab», и Windows автоматически подставит необходимую команду.

Изменение цвета консоли

Найдите в реестре ключ:
[HKEY_CURRENT_USER\Software\Microsoft\Command Processor]
Измените параметр DefaultColor. Значение -F0 определит вывод черного текста на белом фоне, а значение 1E удивит вас желто-синей расцветкой консоли.

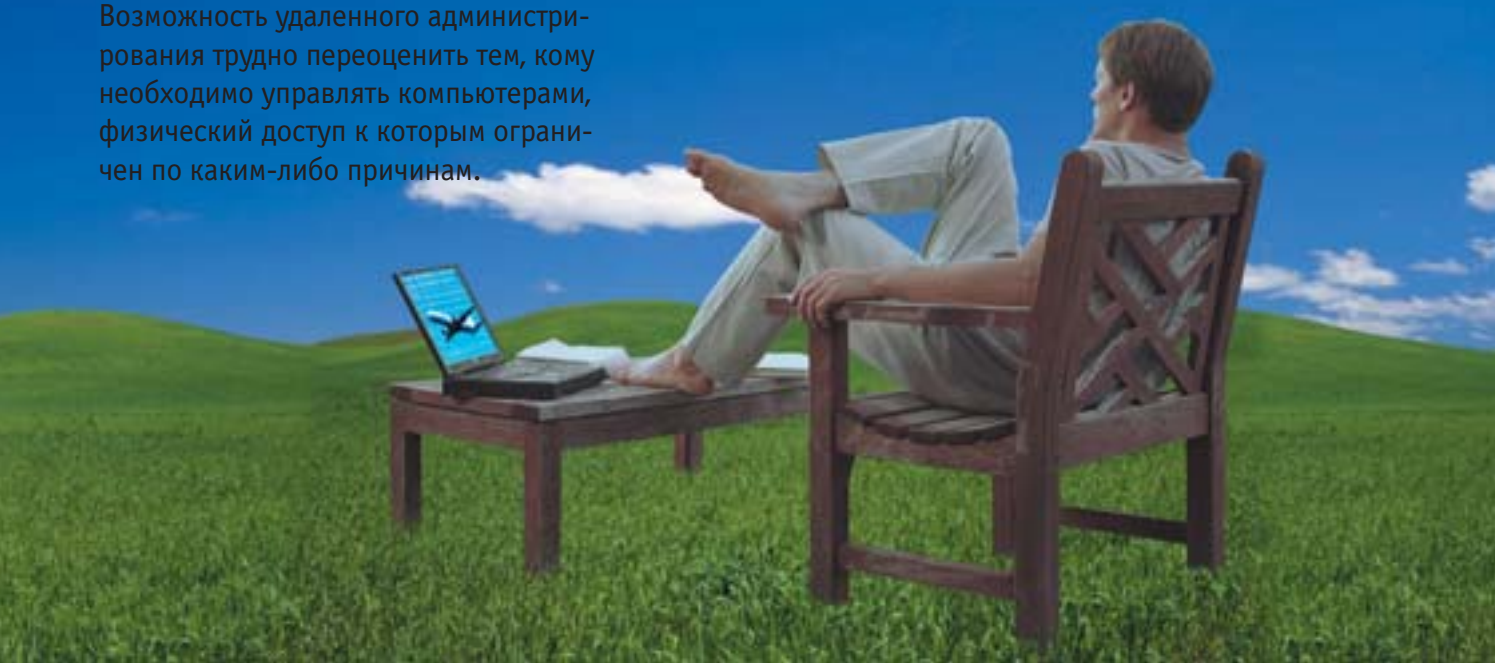
Быстрый запуск консоли командной строки из контекстного меню

Найдите в реестре ключ:
[HKEY_CLASSES_ROOT \Directory \Shell]
Добавьте в него подразделы «CommandPrompt → Command». Параметру Default ключа Command присвойте значение «cmd.exe /k cd "%1"»
Параметру Default ключа Command Prompt присвойте значение «Open Command Prompt».
Щелкнув правой кнопкой мыши на любой папке в Проводнике, можно выбрать команду Open Command Prompt, которая запустит консоль с командной строкой в нужной директории.

Настройка серверной и клиентских частей

Дистанционное командование

Возможность удаленного администрирования трудно переоценить тем, кому необходимо управлять компьютерами, физический доступ к которым ограничен по каким-либо причинам.



Основное назначение Terminal Services заключается в предоставлении возможности работать с удаленной машиной так же, как и с локальной, то есть оставлять пользователя в рамках привычного для него интерфейса. Кроме этого она позволяет множеству клиентов совместно использовать ресурсы одного мощного компьютера, а также выполнять на нем задачи, для которых локальному компьютеру не хватает ресурсов. Схема работы Terminal Services (рис. 1) такая: при подключении клиента на сервере создается сессия с виртуальным дисплеем, на который выводят информацию запускающиеся в этой сессии программы, клиенту же передается только информация об изменении изображения на виртуальном дисплее. Таких сессий, естественно, может быть много. В w2k3 кроме передачи изображения также реализованы и возможности подключения к сессии на сервере дисков, последовательных портов, принтеров и переадресации звука с сервера на локальный компьютер. Мы рассмотрим применение Terminal Services для удаленного управления серверами и рабочими станциями.

Настройка сервера

Remote Desktop for Administration — это вариант Terminal Services с немного ограниченной функциональностью (позволяется создание максимум двух одновременных соединений и сокращены возможности многопользовательского доступа к приложениям), однако имеющихся функций для администрирования хватит с избытком. Активировать Remote Desktop можно с помощью инструмента System из контрольной панели. Для этого на вкладке «Remote» нужно установить флажок «Allow users to connect remotely to this computer» (рис. 2). Сразу после применения настроек сервер готов принимать входящие соединения. По умолчанию удаленный доступ к серверу имеют только те пользователи, которые входят в локальную группу »

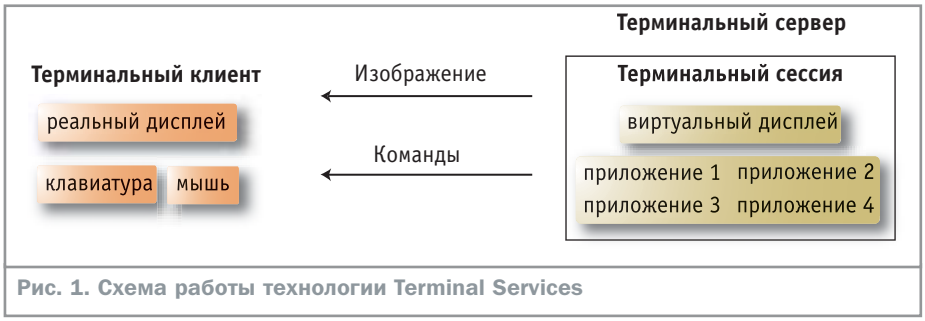


Рис. 1. Схема работы технологии Terminal Services

«Administrators». Если нужно, что бы удаленный доступ к серверу имели и пользователи, которым вы не хотите давать администраторские полномочия, это можно сделать, нажав на кнопку «Select Remote Users» и добавив в появившемся диалоговом окне нужные вам учетные записи. Реально с помощью этого окошка изменяется членство в локальной группе «Remote Desktop Users», в которой и назначены права доступа, необходимые для установления соединения и работы в терминальной сессии. Право доступа к терминальной сессии регулируется также с помощью флажка «Allow logon to terminal server» на вкладке «Terminal Services Profile» в свойствах учетной записи пользователя. По умолчанию этот флажок включен. Поведение сервера после установления соединения определяется следующими параметрами.

- Максимальное время активной работы пользователя в терминальной сессии (Active Session Limit). Отсчет времени начинается с момента входа в систему.
- Максимальное время бездействия пользователя в терминальной сессии (Idle Session Limit). Отсчет времени начинается с последнего совершенного пользователем действия в системе.
- Действие, которое выполняется сервером при разрыве соединения или при достижении лимита времени работы, — здесь возможно либо отключение (при этом все запущенные программы продолжают нормальную работу), либо полное закрытие сессии.
- Время, через которое отключенная сессия будет полностью закрыта (End Disconnected Session).
- Ограничение на адреса, с которых может проводиться повторное подключение к отключенной сессии. Здесь возможно два варианта — или с того же самого адреса (From Previous Client), или с любого (From Any Client).

Рис. 2. Активация системы Remote Desktop

Все эти параметры можно менять либо каждому пользователю индивидуально (вкладка «Sessions» в свойствах учетной записи пользователя, либо сразу для всех пользователей сервера с помощью оснастки «Terminal Services Configuration» из меню «Administrative Tools». Если включить эти опции на сервере, то индивидуальные настройки учетных записей действовать не будут. На сервере можно так же переопределить и другие параметры, например отключить переадресацию дисков, принтеров, буфера обмена и звука и т. д. Оснастка «Terminal Services Manager» (рис. 3) предназначена для управления активными терминальными сессиями. С ее помощью можно отключить или сбросить пользователя с сервера, послать ему сообщение, подключиться к активной сессии, посмотреть список запущенных в сессии приложений и даже принудительно какое-нибудь завершить.

Настройка клиента

Для удаленного подключения к серверу используется специальная программа Microsoft Terminal Services Client, которая ставится по умолчанию на операционные системы линейки XP (найти ее можно в меню «All Programs → Accessories → Communications → Remote Desktop Connection»). Версию для других операционных систем семейства Windows можно загрузить с сайта Microsoft (www.microsoft.com/windowsxp/pro/downloads/rdclientdl.asp). Для соединения требуется ввести имя или IP-адрес сервера и нажать кнопку «Connect» (рис. 4). Дополнительные настройки можно провести, нажав на кнопку «Options». Здесь на вкладке «General» вводятся имя пользователя, пароль и домен. Тут же есть возможность записать все настройки в файл. На вкладке «Display» устанавливается разрешение виртуального экрана и глубина цвета. На вкладке «Local Resources» можно разрешить подключение локальных принтеров, дисков к терминальной сессии, а так же включить переадресацию звука с удаленного компьютера на локальный. На вкладке «Programs» можно указать программу, которая будет запускаться после успешного входа на удаленную систему. На вкладке «Experience» выбирается качество соединения или вручную задаются влияющие на него параметры. Как уже говорилось, настройки подключения можно сохранить в файл. Если открыть такой файл, то будет запущен терминальный клиент и произойдет автоматическое подключение к серверу с сохраненными настройками. Можно также подключиться непосредственно к консоли сервера. Для этого надо запустить терминального клиента с ключом /console.

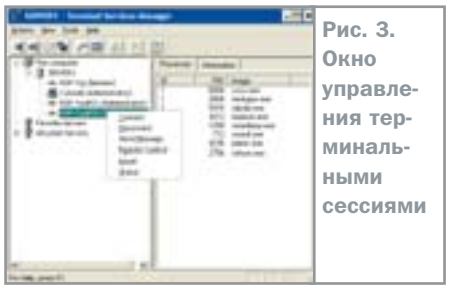


Рис. 3. Окно управления терминальными сессиями

Рис. 4. Запуск удаленного подключения

Заключение

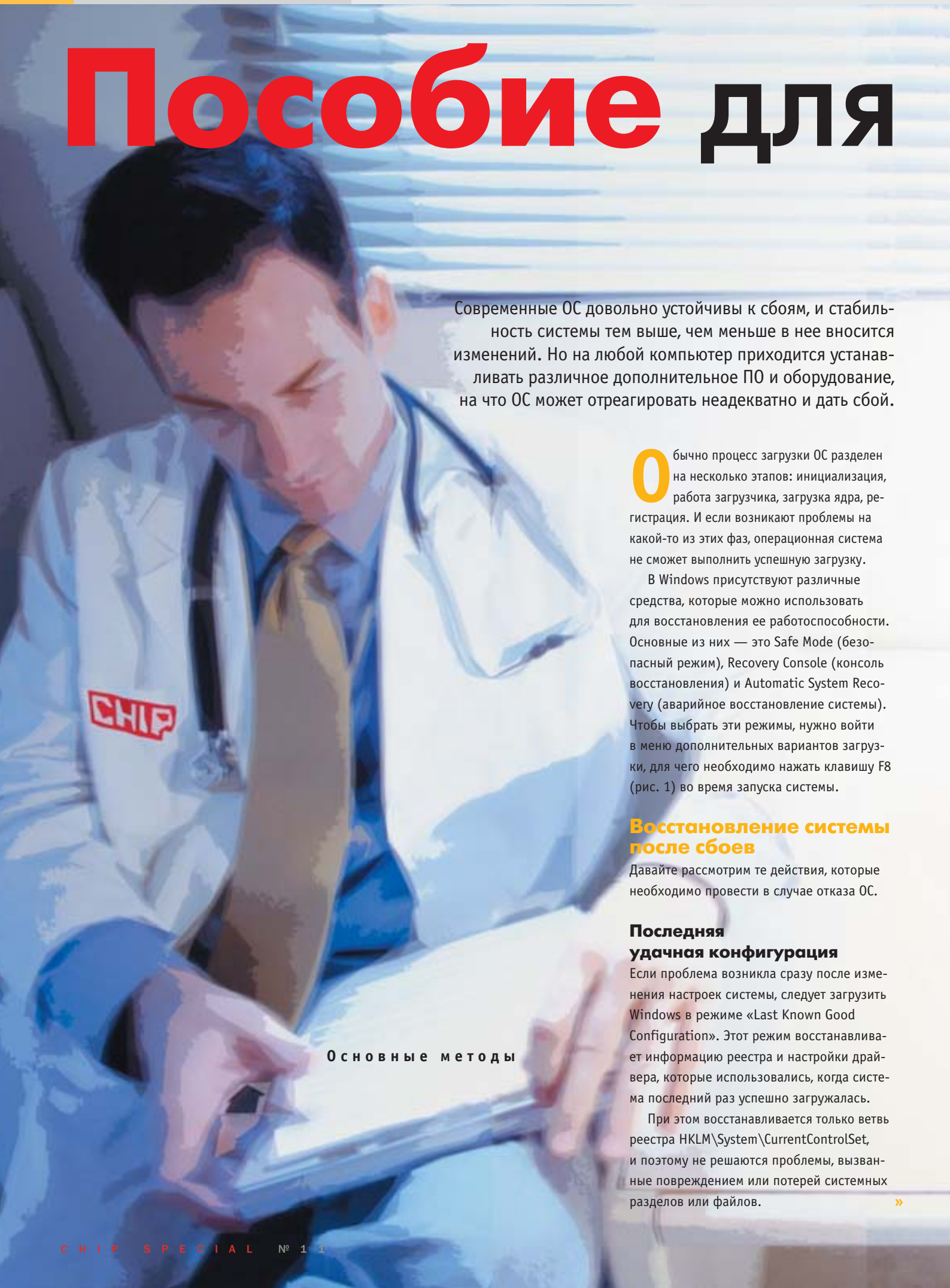
Сервис Remote Desktop for Administration несомненно полезен, а в некоторых случаях просто незаменим. Управлять десятком серверов, расположенных в разных районах города, быстрее и удобнее не покидая своего рабочего места. ■ ■ ■ Роман Сырцев

Советы по использованию

Важные мелочи

- Не забывайте о том, что управление сервером происходит удаленно. Следует с осторожностью относиться к действиям, которые требуют перезагрузки сервера или связаны с изменением сетевых настроек. Например, забытая в дисководе дискета не даст серверу загрузиться, а смена IP-адреса приведет к недоступности сервера из-за отсутствия правила в firewall для нового IP-адреса.
- Рекомендуется настроить сервер так, чтобы он отключал, а не завершал сессию при разрыве связи. Благодаря этой настройке запущенные в сессии программы будут работать, если неожиданно прервется связь. У всех, кто имеет удаленный доступ к серверу, должны быть установлены сложные пароли. Это особенно важно в том случае, если сервер находится в Интернете или в районной сети.

Пособие для



Современные ОС довольно устойчивы к сбоям, и стабильность системы тем выше, чем меньше в нее вносится изменений. Но на любой компьютер приходится устанавливать различное дополнительное ПО и оборудование, на что ОС может отреагировать неадекватно и дать сбой.

Обычно процесс загрузки ОС разделен на несколько этапов: инициализация, работа загрузчика, загрузка ядра, регистрация. И если возникают проблемы на какой-то из этих фаз, операционная система не сможет выполнить успешную загрузку.

В Windows присутствуют различные средства, которые можно использовать для восстановления ее работоспособности. Основные из них — это Safe Mode (безопасный режим), Recovery Console (консоль восстановления) и Automatic System Recovery (аварийное восстановление системы). Чтобы выбрать эти режимы, нужно войти в меню дополнительных вариантов загрузки, для чего необходимо нажать клавишу F8 (рис. 1) во время запуска системы.

Восстановление системы после сбоев

Давайте рассмотрим те действия, которые необходимо провести в случае отказа ОС.

Последняя удачная конфигурация

Если проблема возникла сразу после изменения настроек системы, следует загрузить Windows в режиме «Last Known Good Configuration». Этот режим восстанавливает информацию реестра и настройки драйвера, которые использовались, когда система последний раз успешно загружалась.

При этом восстанавливается только ветвь реестра HKLM\System\CurrentControlSet, и поэтому не решаются проблемы, вызванные повреждением или потерей системных разделов или файлов. »

Основные методы

реаниматора

» Если удалось загрузить Windows в режиме последней удачной конфигурации, то последние изменения, которые были сделаны в системе, и явились, скорее всего, причиной, препятствующей корректному запуску. Удалите или выполните обновление сбойной программы или драйвера, затем загрузитесь в обычном режиме.

Безопасный режим

При загрузке в Safe Mode запускаются только те драйверы и службы, которые необходимы для работы. Данный режим используется для решения проблем, вызванных ошибками в драйверах, сбойными программами или службами, которые запускаются автоматически. Загрузившись в этом режиме, отключите или удалите некорректно работающий компонент, который препятствует загрузке Windows.

Если компьютер не смог загрузиться в безопасном режиме, следует воспользоваться Recovery Console. Если же и этот способ не помогает, то проблемы, скорее всего, вызваны только что установленным оборудованием. Отключите его и попробуйте загрузить компьютер в обычном режиме.

В том случае, если загрузка в Safe Mode была выполнена успешно, необходимо определить причину сбоя в процессе загрузки. В операционной системе имеется несколько инструментов, которые могут в этом помочь.

Выполните вход под учетной записью с правами администратора системы и просмотрите журналы событий (eventvwr.msc). Необходимо провести анализ журнала системы и журнала приложений на наличие предупреждений и сообщений об ошибках (рис. 2). Обращайте внимания на источники событий.

Рис. 1. Меню вариантов загрузки ПК

Консоль восстановления

Recovery Console представляет собой набор средств командной строки, способных помочь восстановить ОС. Доступ к этой консоли можно получить двумя способами: с загрузочного CD Windows Server 2003 или без него, если консоль уже установлена на компьютере. Ее следует запускать только в том случае, если предыдущие способы положительного эффекта не дали.

В этом режиме можно выполнять следующие операции:

- получать доступ к локальным дискам;
- разрешать или запрещать драйверы устройств или служб;
- копировать файлы с установочного диска или съемных носителей (обратное копирование запрещено);
- создавать новый загрузочный сектор и новую основную загрузочную запись (MBR); это может потребоваться при сбое загрузки с существующего загрузочного сектора.

Recovery Console препятствует неавторизованному доступу к разделам, требуя ввести пароль локального администратора системы. Для доменных контроллеров этот пароль задается на этапе работы мастера DCPROMO или при помощи команды ntdsutil.exe с дальнейшим выбором режима Set DSRM Password.

Прежде чем начать работу с командами, необходимо проверить состояние жесткого диска. Для этого используется команда chkdsk /F /R.

Если команда chkdsk не может решить проблемы жесткого диска, то файловая система или основная загрузочная запись, возможно, повреждены или недоступны. Попытайтесь использовать команды fixmbr и fixboot для их восстановления, в противном случае придется создать разделы заново и переформатировать жесткий диск или обратиться в компании, которые занимаются их ремонтом.

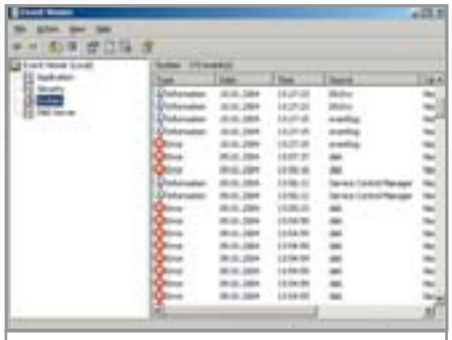


Рис. 2. Анализ журнала событий

Кроме того, невозможность использования Safe Mode для загрузки системы может быть вызвана и повреждением системного реестра Windows или загрузочных файлов. Загрузочные файлы (Ntldr, Ntdetect.com, Boot.ini, Ntbootdd.sys — для контроллеров SCSI, bootfont.bin — для локализованных версий Windows), расположенные в корне системного раздела, могут быть восстановлены из каталога i386 на установочном дистрибутиве Windows Server 2003. Файлы системного реестра каждый раз после создания копии System State (состояния системы) сохраняются на системном разделе в каталоге %Systemroot%\Repair. Используя Recovery Console, можно восстановить поврежденные файлы реестра из этого каталога в исходную папку — %Systemroot%\system32\config. Не забудьте предварительно сохранить текущие файлы в другой каталог перед выполнением этой процедуры восстановления. После этого реестр Windows будет содержать информацию, которая существовала на момент выполнения последнего копирования состояния системы. Все изменения, произошедшие в системе после этого момента, будут потеряны после восстановления. Если резервное копирование ни разу не производилось, то в каталоге Repair будет содержаться копия данных, сделанная непосредственно после установки Windows.

Аварийное восстановление системы

Как бы то ни было, существует вероятность выхода сервера из строя. Режимы загрузки »

Рис. 3. Мастер создания ASR

сервера, такие как Safe Mode и Last Known Good Configuration, могут помочь восстановить систему. Однако резервные копии Automatic System Recovery (аварийного восстановления системы, ABC) должны быть включены в регулярный план по обслуживанию сервера как последняя возможность восстановления Windows.

ABC выполняет восстановление системного раздела и состояния системы, необходимых для запуска и работы компонентов Windows Server 2003.

Для создания набора ABC необходимо запустить мастер создания Automatic System Recovery (рис. 3) из программы архивации (ntbackup.exe). Потребуется пустая дискета 1,44 Мбайт, на которую будут сохранены информация об архиве, конфигурации диска (основного или динамического) и данные, необходимые для выполнения процедуры восстановления, а также путь к носителю данных архива и тип самого носителя (рис. 4).

В набор будет включен системный раздел полностью: System State, системные службы, а также файлы, связанные с компонентами операционной системы (рис. 5). Размер файла архива обычно составляет не менее 1,4 Гбайт. После создания набора ABC вы должны хранить вместе дискету и носитель ABC, поскольку вам будет нужна именно эта дискета, чтобы иметь возможность воспользоваться носителем резервной копии. Дискета ABC не является загрузочной, она может быть использована

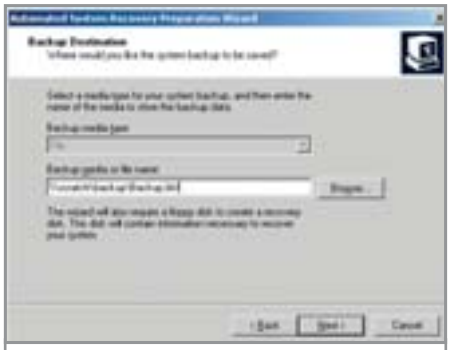


Рис. 4. Укажите путь к архиву

только для объединения набора восстановления с основного носителя.

Наборы аварийного восстановления выполняются программой архивации только в интерактивном режиме. Нельзя назначить запланированные задания по их созданию. Рекомендуется сделать набор ABC сразу после установки и первоначальной настройки Windows. Это обеспечит начальную точку восстановления в будущем. К тому же архив, сделанный при помощи мастера Automatic System Recovery, может быть использован для ручного восстановления после установки новой копии Windows.

Восстановление системы

Заблаговременные меры

Резервное копирование

Регулярное резервное копирование Windows и System State является хорошим заделом для восстановления. В том случае, если вы не используете RAID-массив, а системный диск вышел из строя, то Windows можно будет восстановить из резервной копии. При этом потребуется сначала установить новую копию Windows Server 2003 перед восстановлением из архива. Создайте запланированное задание по архивации System State и системного раздела. Так же желательно выполнять копирование всех локальных каталогов, предоставленных в общий доступ. Это необходимо для того, чтобы после восстановления из полной резервной копии все общие папки по-прежнему были доступны для клиентов сервера. Для сопоставления локальных папок с общими папками из командной строки воспользуйтесь командой net share.

Консоль восстановления

Несмотря на то что можно запустить консоль восстановления, загрузившись непосредственно с установочного CD, намного более удобной является ее установка в меню выбора вариантов загрузки Windows. Чтобы установить консоль восстановления, откройте меню «Start → Run...» и наберите d:\i386\winnt32.exe /cmdcons, где d — буква вашего привода CD-ROM.

Загрузочная дискета

Загрузочная дискета может помочь в том случае, если были потеряны файлы запуска Windows. Она не является каким-то универсальным средством запуска для каждой машины Windows Server 2003. Однако если у вас стандартная конфигурация нескольких компьютеров, то эта дискета будет работать только у тех машин, у которых ОС установлена на одинаковые загрузочные разделы (к примеру, только C:\). Для создания такой дискеты следует скопировать на пустую и отформатированную дискету файлы: Ntdetect.com, Ntldr, boot.ini (а также файл bootfont.bin для локализованных систем и Ntbootdd.sys для контроллеров SCSI). Эти файлы расположены в корне системного/загрузочного раздела (по умолчанию они имеют атрибут «скрытый»).

Восстановление из резервной копии

Самым последним вариантом является восстановление из резервной копии, которую вы регулярно должны были делать на работающей системе. Для ее использования необходимо установить новую копию Windows. Если локальный диск является работоспособным, то удаляем существующий системный раздел и создаем новый (при этом размер нового раздела должен быть не меньше, чем у прежнего). Устанавливаем новую копию Windows Server 2003 на тот же самый раздел, где размещалась Windows ранее. После этого можно приступить к восстановлению из резервной копии.

Имейте в виду, что когда выполняется установка Windows Server 2003, то не про-

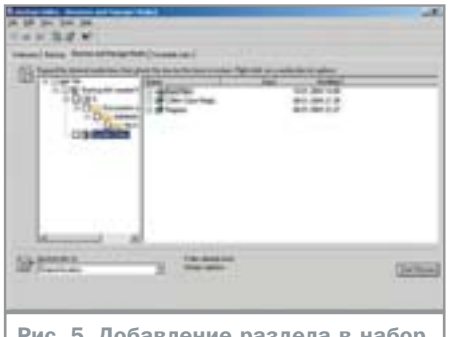


Рис. 5. Добавление раздела в набор

» изводится запрос на изменение каталога установки по умолчанию. Каталог по умолчанию будет \WINDOWS.

Невозможность указания установочного каталога в процессе инсталляции из командной строки обычно значения не имеет, но только до тех пор, пока не возникнут проблемы с системным разделом или пока вы не переформатируете исходный раздел и не переустановите Windows. Для того чтобы иметь возможность восстановить систему из резервной копии, вы должны установить Windows Server 2003 в системный каталог с тем же именем, который он имел в исходной системе, и только затем выполнить восстановление поверх новой копии Windows.

Почему это является важным для нас? Программа архивации (ntbackup.exe) может восстановить данные из резервной копии в альтернативное местоположение, но это не относится к восстановлению System State, а ведь именно оно поможет вернуть работоспособность системы. К тому же если ваш системный каталог не носил имя \WINDOWS, то нельзя будет выполнить полное восстановление без переустановки Windows Server 2003 в каталог с исходным названием. Обычно подобная ситуация возникает, если предыдущая копия Windows 2000 Server перед ее обновлением до Windows Server 2003 находилась в другом каталоге (\WINNT), в результате чего было сохранено старое название каталога.

Как можно заставить Windows сменить каталог? Это ограничение обходится в следующих случаях: если каталог \WINNT уже существует, то можно выполнять автоматическую установку с указанием параметра TargetPath=... в файле ответов или путем выбора нового каталога в дополнительных параметрах при запуске программы winnt32.exe из уже установленной копии операционной системы.

Рис. 6. Настройка важного режима работы процедуры восстановления

Рис. 7. Установка необходимого параметра при восстановлении домена

Удобнее всего воспользоваться установкой Windows в альтернативный системный каталог %SystemRoot% при помощи параметра TargetPath=NAMEWINDIR. Этот способ можно использовать и при установке с компакт-диска Windows Server 2003. Используя блокнот, создайте файл winnt.sif, содержащий представленные ниже параметры, и сохраните его на дискету. Убедитесь в том, что файл называется именно winnt.sif и не имеет добавочного расширения .txt.

```
[Unattended]
UnattendMode=GuiAttended
OemPreinstall=No
TargetPath=WINNT
(где WINNT — это название вашего старого каталога)
[data]
unattendedinstall=yes
msdosinitiated=0
```

Выполните загрузку с CD при этом дискета с файлом ответов должна находиться в дисководе. Программа установки воспользуется параметрами файла ответов и создаст то имя системного каталога, которое указанно в параметре TargetPath.

После успешной установки Windows Server 2003 в каталог со старым названием используйте программу архивации (ntbackup.exe) для выполнения полного восстановления системы (включая System State) с последней резервной копии. Необходимо воспользоваться дополнительными параметрами и указать режим замены существующих данных для восстановления файлов, уже имеющихся на компьютере. Это обеспечит восстановления всех файлов из вашей резервной копии, в противном случае при совпадении имен файлов архива и файлов новой копии системы файлы из архива восстановлены не будут (рис. 6).

При восстановлении System State доменного контроллера, который являлся единственным в домене, необходимо установить параметр «When restoring replicated data sets, mark the restored data as the primary data for all replicas» («При восстановлении реплицируемых наборов данных помечать восстановленные данные как основные для всех реплик») (рис. 7). В этом режиме будет построена новая база данных для службы репликации файлов (ntfrs) из данных, расположенных в системном каталоге SYSVOL только этого контроллера домена. Если производится восстановление одного из нескольких доменных контроллеров, то упомянутый параметр указывать не нужно.

Подводя итоги

Абсолютно надежной операционной системы не существует, и поэтому необходимо подготовиться к ее сбою. Для этого спланируйте процедуру восстановления и составьте описание компонентов сервера и его настроек в соответствии с задачами, решаемыми в вашей локальной сети.

Владимир Елисеев

Система ASR

Шаг за шагом

Чтобы восстановить операционную систему после сбоя, используя Automatic System Recovery, необходимо выполнить следующие несложные шаги.

1. Перед началом процедуры восстановления у вас должны быть:
- созданная заранее дискета ABC;
- созданный заранее носитель с архивом системного раздела;
- компакт-диск с дистрибутивом;
- если в системе используется контроллер дисковых массивов или накопителей, то необходимо иметь драйвер для него на отдельной дискете.

2. Выполните загрузку с установочного диска Windows Server 2003.

3. Если есть дополнительный драйвер, упомянутый на первом шаге, нажмите клавишу F6, чтобы его использовать в процессе инсталляции.

4. Нажмите F2, когда режим установки предложит это сделать внизу экрана. Вставьте в дисковод дискету ABC. После чего система выполнит восстановление в автоматическом режиме.