Выбираем ультрапортативные компьютеры

Windows IT Pro/RE

Март–апрель 2006

ИТ-профи соединяют технологии с бизнесом

Обходим ограничения SHAREPOINT

Насколько «дыра» широка?

Спасение медленной сети

Отключение ActiveX как способ защиты сетей

ADO.NET 2.0: умнее, быстрее, лучше

Разбираясь с DNS

Легкое кодирование с SMO

Безопасность сетей 802.11g — это просто

ISSN 1563-101X

06002

9 771563 101008

Издание ориентировано на специалистов, использующих в своей работе технологии компании Microsoft. Ранее журнал носил название «Windows 2000 Magazine/RE», «Windows & .Net Magazine/RE»

Главный редактор: Д. **Торопов** (toropovd@osp.ru)
Редактор электронной версии: **О. Лохин**
Литературный редактор: **Е. Петровичева**
Корректор: **Л. Теременко**
Верстка и дизайн: **И. Вакштейн**
Служба рекламы: А. Бурилин (aby@osp.ru)
Номер также готовили: **Т. Евдокимова, А. Гапанович, А. Китаев, М. Конов, Л. Линьков, Е. Овсянников, А. Федотов, Т. Лим, Г. Лим**

Адрес редакции: Россия, 127254, Москва, ул. Руставели, 12а, стр. 2
Адрес для писем: 127254, Москва, а/я 42.
Телефоны: (095) 253-7577 (редакция)
(095) 253-9116/9117/7174, 956-3306 (реклама)
(095) 725-4785 (подписка, распространение)
Факс: (095) 725-4783,253-9204
E-mail: windowsitpro@osp.ru
Отдел распространения: xpress@osp.ru

Свидетельство о регистрации средства массовой информации
ПИ Ns ФС77-19042 от 1 декабря 2004 г.
Цена свободная. Выходит 8 раз в год.

ОТКРЫТЫЕ СИСТЕМЫ

Учредитель и издатель:
ЗАО «Издательство «Открытые системы»
109072, Москва, ул. Серафимовича, д. 2, к. 3
Президент **М. Е. Борисов**
Генеральный директор **Г. А. Герасина**
Директор ИТ-направления **П. В. Христов**
Коммерческий директор **Т. Н. Филина**
Директор по маркетингу **Е. Н. Сыбачина**

Подписные индексы по каталогам:
АПР-38185, Роспечать-79741, МАП-99483.

Отпечатано в ООО «Богородский полиграфический комбинат».
142400, Московская область,
г. Ногинск, ул. Индустриальная, д. 40 б
Scanned and Recognized by -=N=-

Богатство Vista

Заинтриговав пользователей в начале года, компания Microsoft все-таки предоставила окончательный список версий нового семейства Windows Vista. Но ясности от этого не прибавилось. Пять версий, а с учетом 64-разрядных вариантов и того больше — есть о чем задуматься и пользователям, и системным администраторам, которым если не в этом, то уж в следующем году точно придется поломать голову над вопросом — устанавливать или нет, и если да, то какую? Редакции Windows Vista будут разбиты на два класса, Home и Business. В классе Home компания Microsoft планирует подготовить три редакции продукта: Windows Vista Home Basic (и Home Basic N для европейского рынка), Windows Vista Home Premium и Windows Vista Ultimate. В классе Business Microsoft создаст две редакции: Windows Vista Business (вместе с Business N для европейского рынка) и Windows Vista Enterprise. Вот так и получается пять версий, планируемых для Windows Vista (или семь, если считать редакции N Editions различными).

Как объясняют представители Microsoft, цель такого разнообразия версий продукта в Windows Vista состоит в том, чтобы дать «ясное ценовое предложение» для всех потребительских сегментов и внедрить инновационные наработки поколения XP, такие как Media Center и Tablet PC, в состав основного кода всех версий. В то же время следует уже сейчас отметить, что, при всей новизне еще не появившихся версий Windows Vista, с точки зрения перехода на полностью 64-разрядную платформу они выглядят промежуточными, поскольку редакции Windows Vista предлагаются и для платформы x86 (32-разрядной), и для платформы x64 (64-разрядной). По-видимому, Microsoft намеревается полностью перевести семейство клиентских продуктов Windows на платформу x64 лишь после выпуска Windows Vista. Напомню, что свои основные серверные продукты, в частности Exchange 12, компания планирует выпускать только в 64-разрядной редакции, аргументируя это тем, что, по прогнозам аналитиков, переход на 64-разрядные вычисления наиболее востребован именно в области аппаратного обеспечения серверов.

Заставляет задуматься, конечно, то, как широко развернула Microsoft свою линейку продуктов. Как и в случае семейства Office, Microsoft, на мой взгляд, допускает некоторый перебор с числом редакций продукта. Это приведет к растерянности корпоративных и индивидуальных пользователей, не говоря уже об администраторах, которым такое разнообразие только прибавит работы. Попробуйте предположить, какую версию Windows Vista начнут ставить производители компьютерной техники на свои изделия. Обычно сплошь и рядом сталкиваешься с ситуацией, когда на ноутбук, предназначенный для корпоративного использования, устанавливается версия Windows XP Home. Теперь таких версий будет две (и даже три, с учетом версии для Европы), и все они для использования в корпоративной сети не годятся. И прежде чем ломать голову на вопросами пользователей, а почему, собственно, я не могу подключиться к своему компьютеру удаленно или как мне предоставить файлы в общий доступ, администраторам придется сверяться с таблицами функциональных возможностей каждой версии, иначе они рискуют потратить чересчур много времени на решение не имеющей решения задачи.

До полноты картины предлагаю прикинуть, сколько всего теперь версий Windows можно будет встретить на компьютерах дома и на работе: Windows 2000 Server, Windows Server 2003, Windows 2000 Pro, Windows XP Home и Pro, пара версий Media Center и ПЯТЬ версий Vista. Боюсь, что ничего хорошего в таком разнообразии все-таки нет: когда наступит пора обновления, богатство выбора, скорее всего, приведет, по меньшей мере, к путанице..

Windows IT Pro/RE
№ 2 МАРТ–АПРЕЛЬ 2006

СОДЕРЖАНИЕ

И это еще не все! Только в Web!

В дополнение к материалам печатного номера вы всегда найдете на нашем сайте: новости, постоянно обновляемые обзоры продуктов Microsoft и независимых разработчиков, статьи по безопасности, управлению системами Exchange, автоматизации административных операций и интеграции приложений.

Читайте на www.windowsitpro.ru:

Чтобы получить ответы на свои вопросы, подпишись на новостную ленту на www.windowsitpro.ru

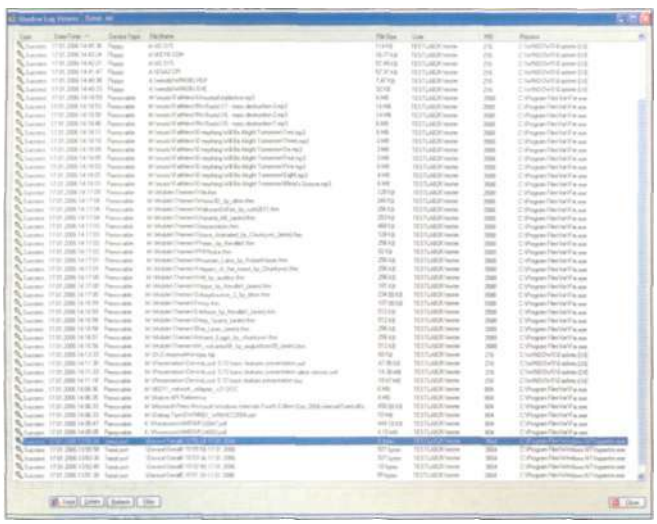
Разработка

Бета-тестирование DeviceLock 6.0

Компания «Смарт Лайн Инк» приглашает всех желающих принять участие в бета-тестировании новой версии программы DeviceLock 6.0, которая управляет доступом к дисководам, накопителям CD-ROM, а также портам USB и FireWire, инфракрасным, принтерным (LPT) и модемным (COM) портам, адаптерам WiFi и Bluetooth. Версия Beta 2 привносит в DeviceLock следующие дополнительные функции:

- функцию авторизации носителей. Белый список носителей работает аналогично белому списку USB-устройств, но в отличие от него здесь авторизуются не устройства, а сами данные. Белый список носителей позволяет идентифицировать определенный CD/DVD-диск на основе записанных на него данных и разрешить его использование, даже если сам привод CD/DVD-ROM заблокирован. Любое изменение в авторизованных данных приведет к изменению уникального идентификатора носителя, и диск перестанет распознаваться как авторизованный. Каждому пользователю и/или группе может назначаться свой белый список носителей. Данная технология позволяет предотвратить проникновение неавторизованной информации внутрь корпоративной сети;
- функцию теневого копирования данных. Все файлы, копируемые пользователем на внешние носители (Removable и Floppy), будут зеркалироваться и сохраняться для последующего просмотра администратором. Сохраняются полные копии файлов. Теневое копирование (Shadowing) — это расширение уже существующей функции аудита, оно также может быть включено для отдельных пользователей или групп. Функция теневого копирования данных теперь поддерживается и для COM- и LPT-портов.

Поучаствовать в программе и получить дополнительную информацию можно на http://www.protect-me.com/ru/news/857.html



Одним из последних примеров внедрения DeviceLock стал Нижегородский институт «Атомэнергопроект», который является Федеральным Государственным унитарным предприятием, осуществляющим научно-исследовательские и проектно-конструкторские работы, а также инженерно-консультационные услуги по выбору площадок, строительству, монтажу, пусконаладочным работам и освоению проектных мощностей атомных, тепловых, газотурбинных электростанций и других строительных объектов. В настоящее время ФГУП НИАЭП осуществляет проектирование атомных и тепловых электростанций, систем теплоснабжения городов и промышленных комплексов, а также объектов жилищного и культурно-бытового назначения. Принятие дополнительных мер по обеспечению информационной безопасности «Атомэнергопроекта» было обусловлено необходимостью защиты от несанкционированного использования флэш-дисков и подключений к Internet через мобильные телефоны.

Решение использовать именно DeviceLock было принято в связи с тем, что данное программное обеспечение позволяет закрыть возможные каналы утечки информации из локальной сети института. Изначально проблема была вызвана недостаточно строгим контролем использования устройств внешних носителей информации и USB-портов. Галина Ивановна Шипкова, главный специалист отдела информационных технологий института, прокомментировала идею внедрения DeviceLock на 600-х компьютерах так: «Мы пришли к выводу, что DeviceLock — это наиболее простое и относительно недорогое программное решение. Руководство института и системный администратор остались довольны результатами внедрения программы».

- Дополнительная информация — на www.protect-me.com.

Антиспам

EservAgava

Компания «Агава» представляет разработанное совместно с компанией «Етайп» решение, предназначенное для использования почты, — EservAgava mail server (http://spamprotexx.ru/eserv.shtml). Продукт адресован исключительно корпоративным клиентам. Серверный комплекс для Windows способен обеспечить комфортную, безопасную и качественную работу с почтой в любой организации. В комплект EservAgava mail server включены: почтовый сервер (SMTP, POP3, IMAP4), Web-сервер (HTTP), файловый сервер (FTP), SNMP-сервер, SSL/TLS-версии всех серверов (HTTPS, SMTPS, POP3S, IMAPS, FTPS), программы управления комплектом серверов, статистический спам-фильтр SpamProtexx и подключаемый модуль Dr.Web для антивирусной проверки почты. EservAgava mail server реализует все функции, типичные для современного почтового сервера, а кроме того, имеет ряд уникальных преимуществ. Акцент сделан на возможность тонкой настройки каждого элемента сервера, максимальную расширяемость, функции интеграции с другими программами и масштабируемость. Возможности данного серверного комплекса позволяют

решать любые вопросы, возникающие в процессе настройки и использования почты в сети.

Рекомендуемая минимальная конфигурация: компьютер с процессором Celeron/600, 128 Мбайт оперативной памяти и Windows 2000. EservAgava будет работать и на более слабых компьютерах с более старыми версиями Windows — 9x и NT4. Некоторые компоненты (в частности, модуль FireWall) не будут работать на Windows9x/ME/NT4. Предпочтительная конфигурация сильно зависит от числа пользователей, работающих с сервером. При 1200 пользователях хорошие результаты показывает сервер с процессором PIII с частотой 1 ГГц, 512 Мбайт памяти, жестким диском емкостью 60 Гбайт на базе Windows 2000 или Windows 2003.

Статистический спам-фильтр Agava Spamprotexx работает со всеми почтовыми клиентами и не требует их настройки, в то время как большинство распространенных фильтров работают как посредники: забирают почту к себе, а потом отдают клиенту. То есть клиент обращается за почтой именно к посреднику, что требует смены настроек. Spamprotexx фильтрует соединения с почтовым сервером в ходе работы и предлагает удобный интерфейс для обучения в таких популярных приложениях, как Outlook и Outlook Express.

Соединения POP3 и IMAP проверяются в режиме реального времени. Пользователю не нужно указывать, какое из соединений используется. Разница между POP3 и IMAP в том, что IMAP позволяет хранить почту и структуру папки на сервере и иметь, таким образом, доступ к той же почте с нескольких компьютеров. Когда используется POP3, Spamprotexx добавляет специальную спам-метку в строку темы спам-сообщения. Когда используется IMAP, Spamprotexx может перемещать все спам-сообщения в папку СПАМ на сервере.

Agava Spamprotexx поддерживает белый список не-спамерских адресов, обладающий несколькими особенностями:

1. Белый список состоит из почтовых адресов и соответствующих им текстовых имен. Письмо от «John Smith» john@domain.com имеет почтовый адрес (john@domain.com) и текстовое имя John Smith. Часто случается, что спам приходит с известных адресов, с которыми вы уже переписывались, это называется подделкой адреса. В то же время спамеры редко подделывают наравне с адресом соответствующее ему текстовое имя. С того момента, как белый список начнет проверять и адрес, и имя, ваш почтовый ящик станет более защищенным.

2. Белый список поддерживается автоматически. Если вы посылаете кому-то письмо, в него добавляются адрес получателя и текстовое имя. Если вы предоставляете сообщение «не спам» для тренировки, его адрес и текстовое имя будут также добавлены в белый список. Если же предоставить фильтру спам-сообщение для обучения, его адрес будет удален из белого списка. Содержимое белого списка может быть защищено от удаления, для этого необходимо поставить галочку в окне подтверждения удаления напротив сообщения.

Не пропустите события!

Семинары Microsoft TechNet Весна 2006 в вашем городе

Традиционные региональные семинары Microsoft для руководителей и сотрудников ИТ-департаментов предприятий и организаций.

Цель семинаров — дать ИТ-специалистам достоверную информацию о новейших продуктах Microsoft из первых рук, а также наглядно продемонстрировать наиболее эффективные пути использования новых технологий для решения различных ИТ-задач. По итогам семинара участникам будут вручены сертификаты.

Мероприятие будет интересно ИТ-специалистам организаций и компаний крупного, среднего и малого бизнеса.

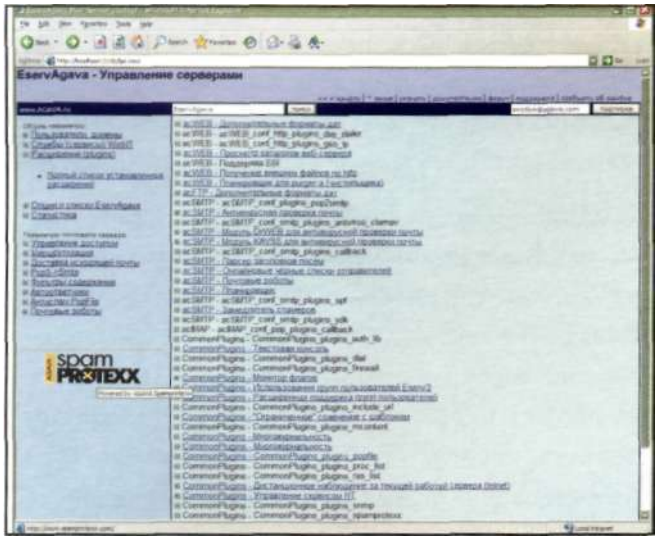
В рамках семинаров TechNet будут освещены новые возможности таких продуктов как:

- Операционная система Windows Vista;
- Платформа для управления и анализа данных Microsoft SQL Server 2005;
- Новая версия Microsoft Office с кодовым названием Office 12;
- Новый Microsoft Exchange Server с кодовым именем Exchange 12.

Регистрация на семинары по адресу http://www.microsoft.com/rus/events/TechNetSpring2006/Default.mspx

Календарь мероприятий

Дата	Город
23 марта	Уфа
28 марта	Москва
29 марта»	Санкт-Петербург
4 апреля	Екатеринбург
5 апреля	Волгоград
11 апреля	Казань
12 апреля	Новосибирск
19 апреля	Самара
20 апреля	Нижний Новгород
26 октября	Самара
27 октября	Нижний Новгород
1 ноября	Казань



3. Белый список также может поддерживаться вручную. Некоторые почтовые серверы запрашивают разрешение на использование SSL. SSL обеспечивает безопасность входящих и исходящих почтовых соединений. Spamprotexx автоматически определяет и поддерживает SSL-соединения, не требуя каких-либо настроек. Фильтр Agava Spamprotexx является обучаемым. Некоторые пользователи избегают подобных спам-фильтров, так как убеждены, что обучение — долгий и утомительный процесс, основанный на расплывчатых критериях. Такие пользователи предпочитают фильтры, основанные на черных списках: SpamCop, ORDB, DSBL, SPEWS и другие.

Подробнее о EservAgava mail server читайте на http://spamprotexx.ru/eserv.shtml.
Тестовая версия находится по адресу: http://www.eserv.ru/download/EservAgava325-setup.exe.

- Дополнительная информация — на http://agava.ru/.

Программное обеспечение

Microsoft Dynamics Snap

Компания Microsoft объявила о выпуске продукта Microsoft Dynamics Snap, коллекции специальных модулей, расширяющих возможности пакета Microsoft Office 2003. Предлагаемые продукты гарантируют более высокую производительность труда служащих организации за счет предоставления им свободного доступа к бизнес-процессам и данным корпоративных систем Microsoft Dynamics AX 3.0 (прежнее название Microsoft Business Solutions-Axapta) и Microsoft Dynamics CRM 3.0, непосредственно из приложений Microsoft Office.

Модуль Timesheet Snap-In позволит задействовать программу Microsoft Outlook для просмотра или записи времени выполнения различных задач. Пользователи смогут связывать записи времени Microsoft Dynamics AX с назначенными встречами и совещаниями из календаря Outlook и обнаруживать внесенные изменения.

Благодаря приложению Vacation Management Snap-In пользователи смогут подавать заявления о предоставлении отпуска через Microsoft Outlook. Сообщение по электронной почте попадает к руководителю, который может внимательно изучить заявление, свериться с графиком отпусков и по результатам проверки удовлетворить или отклонить просьбу об отпуске. В случае предоставления сотруднику отпуска система автоматически делает соответствующую отметку в модуле управления рабочим временем и учета посещаемости Microsoft Dynamics.

Модули Business Data Lookup Snap-In для решений Microsoft Dynamics AX и Microsoft Dynamics CRM предоставят сотрудникам возможности поиска информации в базах данных указанных систем непосредственно из программ Microsoft Office Word, Microsoft Office Excel или Outlook, копирования избранных данных в документы Office 2003 или прикрепления документов Office к записям Microsoft Dynamics AX.

- Дополнительная информация — на www.softline.ru.

ComponentOne DevKit for Visual Studio 2005

Компания выпустила пакет ComponentOne DevKit for Microsoft Visual Studio 2005, в состав которого вошла одна из наиболее популярных на сегодня интегрированных сред разработки Microsoft Visual Studio 2005 и платформа ComponentOne Studio Enterprise, включающая полный набор программных компонентов для создания приложений .NET, ASP.NET и COM.

Более 180 компонентов, вошедших в состав Studio Enterprise, призваны максимально упростить и ускорить процессы проектирования и разработки инновационных программных продуктов для настольных и мобильных систем, а также Web-приложений. Все разработчики, приобретающие продукт, имеют право на получение технической поддержки в течение одного года.

- Дополнительная информация — на www.softline.ru.

О перспективах развития Microsoft Exchange

В статье «Что необходимо знать об Exchange 12 (E12)» (http://www.osp.ru/win2000/exchange/601_13_1.htm) основной акцент был сделан на планах Microsoft по выпуску новой версии сервера обработки сообщений Exchange 12, главного обновления текущей версии Exchange Server 2003. С тех пор кое-что изменилось. И хотя временные рамки создания нового релиза остались прежними — начало 2006 года, в новый продукт будет включен пакет обновлений Exchange Server 2003 Service Pack 2 (SP2).

SP2

Хотя пакет обновлений и получил название SP2, он представляет собой главное обновление. Новые возможности этого выпуска включают поддержку Direct Push Technology (требуется для новых смартфонов под управлением Windows Mobile 5.0 с установленным пакетом Messaging and Security Feature Pack), поддержку Sender ID (интегрированная версия фильтра сообщений Intelligent Message Filter, version 2.0), а также антифишинговые технологии. Кроме того, предельный объем хранилища для Exchange 2003 Standard Edition увеличился с 16 до 75 Гбайт.

Поддержка мобильных устройств, реализованная в SP2, — особенно примечательное новшество. Технология «прямого проталкивания», Direct Push Technology, которая работает со всеми папками Exchange — Inbox, Calendar и Tasks, позволяет владельцам совместимых с новой технологией устройств проводить синхронизацию с Exchange Server «на лету» — Over-The-Air (OTA). Раньше при работе с Exchange 2003 для извещения клиента о наличии обновлений использовался механизм обмена короткими сообщениями Short Message Service (SMS). Сейчас Direct Push Technology выполняет синхронизацию по IP-адресам, что и проще, и надежнее. Как правило, сервер удерживает открытое соединение с клиентом и оповещает устройство, если какой-то элемент, скажем календарь, нуждается в синхронизации. Смартфон Windows Mobile запускает процесс синхронизации и загружает все необходимые данные с Exchange Server. «На выходе» пользователь получает практически перманентную синхронизацию, в основном благодаря двум улучшениям. Во-первых, расход на полосу пропускания сокращен за счет компрессии данных и кэширования соединения. Во-вторых, администратор может настроить объем данных сообщения пользователя, загружаемый автоматически (обычно от 1 до 4 Кбайт), поэтому при загрузке корреспонденции пользователи не будут долго ожидать загрузки из-за наличия большого объема ненужных данных.

Для более подробного ознакомления с пакетом обновлений SP2 рекомендую прочитать статью Тони Редмонда «Исследование пакета обновлений Exchange 2003 Service Pack 2», опубликованную в предыдущем номере журнала.

Модернизация до Exchange 12

С момента публикации моего первого обзора возможностей E12 произошло не так много изменений. Exchange 12 станет первым продуктом Microsoft, в котором будет представлена интегрированная версия Monad Shell, командный процессор (командная оболочка) на базе Microsoft .NET Framework. Любая функция E12 может быть выполнена через сценарный интерфейс Monad. Таким образом, в распоряжении администраторов и разработчиков появится новый мощный метод доступа к серверу Exchange через интерфейсы API и Monad.

Поль Тюрро

Редактор новостей в Windows IT Pro. Готовит еженедельные выпуски Windows IT Pro UPDATE, а также ежедневные выпуски новостей WinInfo. С ним можно связаться по адресу: thurott@win2000mag.com

Exchange, как и Longhorn Server, будет состоять из индивидуальных программных компонентов; это позволит сократить площадь возможных атак и обеспечить истинную ролевую архитектуру, когда требуется устанавливать и настраивать только те серверные компоненты, которые действительно необходимы. Exchange Server способен выступать в роли сервера периметра, расположенного за сетевым экраном предприятия, и сможет отразить большую часть вредоносного потока сообщений (при соответствующей настройке) до того, как информация попадет в корпоративную сеть. И хотя эти серверы не будут членами домена, они смогут составить самую первую линию обороны против спама и различных атак с использованием электронной почты.

Кроме того, новый центр управления Exchange System Manager превратится в единую консоль для выполнения всех задач управления сервером Exchange и будет построен поверх сценарного интерфейса Monad. Exchange будет поддерживать непрерывное оперативное резервирование, станет программируемым через API Web-служб, и обе версии Exchange — Exchange 2003 Standard Edition и Exchange 2003 Enterprise Edition будут истинными x64-версиями. Новая информация о возможностях модернизации до E12 будет поступать по мере продвижения работ по созданию нового продукта.

Рекомендации

Пока еще непонятно, кто смог бы сегодня реально конкурировать с Exchange, поэтому в действительности главный вопрос — стоит ли переходить на обновленную версию этого продукта? Я не уверен, что Exchange Server 2003 SP2 предлагает достаточно изменений по сравнению с базовой версией Exchange 2003, чтобы заставить пользователей предыдущих версий Exchange выполнить модернизацию. Но что касается действующих заказчиков Exchange 2003, то для них целесообразно обновить версию Exchange как можно быстрее, пока это еще можно сделать бесплатно (а здесь еще надо учесть и множество исправлений ошибок, и новую функциональность). Что касается перехода к E12, то у нас в запасе еще почти целый год и будет много возможностей протестировать промежуточные выпуски нового продукта.

О Microsoft Client Protection

Microsoft Client Protection — это один из новых элементов системы безопасности Microsoft, сочетающий в себе средства антишпионажа, защиту от вирусов и технологию противодействия вредоносному программному обеспечению. «Наши клиенты говорят, что им не хватает решений для централизованного управления защитой от вредоносных программ, — заявил Пол Брайан, директор по продуктам подразделения Microsoft Enterprise Access and Security Products. — С одной стороны, наши заказчики хотят управлять меньшим количеством средств обеспечения безопасности, с другой стороны, они нуждаются в большей прозрачности при оценке состояния безопасности своих сетей». Во многих отношениях Microsoft Client Protection — это как раз то, что соответствует ожиданиям клиентов Microsoft.

Унифицированная защита предприятия

В декабре 2004 года Microsoft приобрела компанию GIANT Company Software и получила в свое распоряжение самую передовую технологию противостояния шпионским программам. Спустя год Microsoft объявила о намерении в ближайшем будущем предложить антишпионскую технологию GIANT с функциями антивирусной защиты и противодействия вредоносному программному обеспечению и выпустить соответствующее решение для защиты предприятий на основе подписки. Подобное интегрированное ядро, лежащее в основе Microsoft Client Protection, проектируется с целью предоставить администраторам инструмент для детального управления безопасностью.

Что мы получим

По словам Брайана, Microsoft Client Protection будет снабжен заготовками отчетов и оповещений, главное внимание в которых будет уделено возникающим проблемам. «Мы не собираемся выдавать пользователям длинный перечень отчетов, — поясняет Брайан. — Мы предоставим только самые точные данные о конкретных угрозах».

Как продукт Microsoft, Client Protection будет «прозрачно» интегрирован в существующие системы Microsoft. Если вы уже работаете с продуктами для развертывания программного обеспечения, Client Protection сможет интегрироваться с ними, а компании, которые не используют продукты развертывания, смогут воспользоваться службой Windows Software Update Services (WSUS).

Для Microsoft Client Protection требуется Windows Server 2003 SP1 или Windows 2000 Server SP4 в качестве сервера. Продукт сможет защитить клиентов Windows 2000 SP4 и Windows XP SP2 (и более поздних), а также файл-серверы Windows Server 2003. Когда начнутся поставки Windows Vista и Longhorn Server, Microsoft Client Protection также будет поддерживать эти системы.

Что, где, когда?

Большой вопрос — лицензирование — остается пока без ответа, хотя ранее уже сообщалось, что продукт будет лицензироваться по подписке. Брайан говорил в свое время, что ранняя бета-версия продукта будет доступна отдельным клиентам компании в конце 2005 года или чуть позже, и, в зависимости от полученных откликов, Microsoft надеется выпустить готовый продукт в первой половине 2006 года.

Рекомендации

Хотя рекомендовать к использованию Microsoft Client Protection несколько преждевременно, уже сейчас ясно, что интегрированные продукты противостояния вредоносному окружению обещают в 2006 году широкие возможности провайдерам серверных услуг. Предложение Microsoft достойно внимания, поскольку объединяет две лучшие технологии данного класса в единый продукт, а когда компания решит вопрос с лицензированием, оно вообще может стать очень мощным решением. Поживем — увидим.

Не упускайте возможностей виртуализации

Бен Смит

Специалист по безопасности в компании Microsoft. bensmi@microsoft.com

ем, кто работает в сфере ИТ, наверняка знакома сцена, описанная мне приятелем, обслуживающим небольшую сеть. В его офисе цветной принтер стоит у стола Дебби. Фрэнк (через комнату): «Дебби, кто-нибудь сейчас пользуется цветным принтером?» Дебби: «Нет». Фрэнк: «Ничего не печатай, пока я не выведу на печать!» Участники истории не понимают, что печатающее устройство существует лишь для нанесения чернил на бумагу, тогда как виртуализацию процесса подготовки файла к выводу на печать осуществляет программное обеспечение принт-сервера. Программы принт-сервера переводят файл в формат, понятный для печатающего устройства, затем помещают преобразованный файл в очередь для вывода на печать. Виртуализация повышает надежность процесса вывода на печать благодаря исключению возможности сбоя из-за ошибки немеханического характера. Кроме того, она способствует снижению затрат, продвижению на рынок печатающих устройств, поскольку производители избавлены от необходимости писать программы преобразования файлов для каждого производимого ими принтера, а также снижению полной стоимости владения (TCO) за счет взаимозаменяемости печатающих устройств без необходимости повторной подготовки заданий для вывода на печать. Сегодня виртуализация — обязательный элемент в мире печати, и скоро виртуальные машины станут неотъемлемой частью ИТ. Понимают ли в вашем отделе ИТ значение виртуальных машин? Есть ли у вас стратегия виртуализации? Виртуальные машины — это полнофункциональные «гостевые» операционные системы, исполняющиеся в качестве приложений в среде главной операционной системы. Программное обеспечение виртуальных машин, например Microsoft Virtual PC или VMware от EMC, предусматривает абстрагирование от аппаратной части физического компьютера. Гостевая операционная система работает на виртуальной аппаратуре точно так же, как на физической аппаратной платформе. Поскольку реальное аппаратное обеспечение скрыто, в среде главной операционной системы могут функционировать несколько виртуальных систем. Жесткий диск виртуальной системы можно сохранять на диске главной операционной системы в виде файла. Виртуальную машину можно при необходимости запускать из файла или переносить на другой компьютер с аналогичным программным обеспечением для виртуальных машин. Виртуальные машины могут функционировать незаметно для пользователя либо, как и другие приложения, исполняться в отдельном окне.

Использование виртуальной машины может обеспечить значительную экономию затрат, повысить надежность и скорость развертывания. Если стратегия развития ИТ не предусматривает выполнения виртуальных вычислений, компания много теряет. Используя виртуальные компьютеры, можно быстро и в значительной степени снизить затраты на ИТ в следующих трех областях.

Скорость повторного развертывания операционных систем и приложений. Поскольку виртуальные системы мобильны и могут быть сохранены на диске (на сервере либо на DVD), можно создавать их заблаговременно и при необходимости развертывать (с помощью копирования и вставки). Преимущества виртуальных систем позволяют заметно сократить расходы на эксплуатацию выделенных сред для тестирования, киосков и прочих совместно используемых компьютеров, а также сред, предназначенных для обучения. Вместо повторной установки операционной системы и приложений всякий раз, когда в этом возникает необходимость, можно просто использовать базовую виртуальную систему. Даже са-

мая быстрая технология создания образа жесткого диска не может сравниться по скорости с процессом развертывания виртуальных систем. Кроме того, в отличие от использования образов, благодаря абстрагированию от аппаратной части виртуальные системы полностью мобильны.

Сокращение затрат на аппаратное обеспечение. Благодаря использованию виртуальных систем, можно снизить затраты на аппаратное обеспечение в нескольких областях. Для примера рассмотрим системы, где приложения, соответствующие направлению бизнеса, выполняются на одной устаревшей аппаратной платформе. Предположим, что это приложения центра обслуживания вызовов в среде операционной системы OS/2 Warp. Стоимость поддержки унаследованной аппаратной части, на базе которой функционирует операционная система OS/2, значительно выше затрат на поддержку более новой аппаратуры. Экономия затрат обусловлена главным образом повышением надежности и консолидацией серверов. Можно создать виртуальные системы для унаследованной операционной системы OS/2 и запускать их на одном компьютере, работающем под управлением Windows Server 2003 на более надежной и отказоустойчивой аппаратной платформе.

Взглянем на ситуацию с точки зрения пользователя. Пользователи нередко эксплуатируют два компьютера, поскольку работают с приложениями лишь на конкретной платформе. Например, графический дизайнер может использовать машину Apple Macintosh в качестве главной рабочей станции, но ему нужен и компьютер с Windows XP Professional для выполнения некоторых критически важных приложений. Виртуальные системы позволят такому пользователю ограничиться эксплуатацией компьютера Mac, на котором запущен виртуальный экземпляр XP.

В центрах обучения также часто требуется использование нескольких машин. Виртуальные системы дают возможность запускать несколько гостевых операционных систем (даже на разных платформах) на одном компьютере, что позволяет извлекать максимальные возможности из имеющихся аппаратных ресурсов, отведенных для обучения.

Изоляция пользователей. Компьютеры общего пользования, например эксплуатируемые сменным персоналом, могут доставлять массу неудобств. Например, один пользователь устанавливает шпионскую программу и приводит компьютер в нерабочее состояние либо меняет размер курсора мыши, чем приводит в замешательство прочих пользователей этого компьютера. Виртуализация позволяет отвести каждому пользователю свой виртуальный компьютер и тем самым локализовать его действия. Если проблема все же возникает, можно быстро вернуть компьютеру работоспособность путем простой перезагрузки базовой виртуальной системы.

Виртуальные системы также можно применять для изоляции сеансов пользователя. Это полезно в интересах конфиденциальности и защиты персональных данных пользователей информационного киоска, а также повышения надежности самого киоска. Во время каждого сеанса работы пользователя с киоском осуществляется запуск новой виртуальной системы. По окончании сеанса компьютер возвращается в базовое состояние.

Не упускайте возможностей виртуализации, способствующих повышению надежности систем и уменьшению затрат на поддержку и аппаратное обеспечение. Встать на путь реализации потенциала технологии виртуализации поможет простой план.

1. Оцените возможности использования виртуальных систем. В трех областях, обозначенных в этой статье, оцените реальную выгоду от использования виртуальных систем применительно к конкретной компании.
2. Оцените потенциальное повышение надежности и снижение затрат. Определите текущие затраты в целевых областях, для которых планируется применение виртуализации. В определении надежности и эксплуатационных затрат особенно полезны базы данных службы поддержки. Оцените экономию затрат, которую даст виртуализация.
3. Оцените пригодность программного обеспечения виртуальных систем для реализации целевых возможностей. Испытайте программы виртуализации и виртуальную среду и убедитесь в реальной достижимости расчетного увеличения надежности и сокращения затрат.
4. Приступайте к планированию первого проекта виртуализации.

ИТ не терпит риска

Бен Смит
Специалист по безопасности в компании Microsoft.
bensmi@microsoft.com

В период взлета доткомов в конце 1990-х многие критиковали Уоррена Баффета за отказ от инвестиций в Internet-компании. Его ответ акционерам был таков: «То, что толпа с вами не согласна, не может быть критерием ошибочности ваших суждений. Вашу правоту могут подтвердить только верные исходные данные и логичные рассуждения». Со временем правильность этих слов подтвердил рынок, а Internet-бум теперь чаще называют Internet-пузырем. Какой урок могут вынести из этого ИТ-менеджеры? Минимизировать риски при выборе ИТ-проектов можно только путем правильного подбора исходных данных и четких рассуждений и обоснований.

Джордж Хилмейр, бывший директор DARPA, финансировавшего разработку лежащих в основе Internet технологий, выдвинул набор критериев, называемых иногда катехизисом (наставлением) Хилмейра, по которым оценивались соискатели грантов DARPA. ИТ-менеджерам стоит воспользоваться этой методикой при сборе данных, анализе и обосновании предлагаемых проектов, а также для оценки проекта с точки зрения его эффективности для компании. Этот набор критериев поможет подготовить необходимые данные для защиты проекта перед высшим руководством. В данной статье катехизис Хилмейра представлен в виде восьми наборов вопросов. Ответы на эти вопросы помогут подготовить полноценное предложение проекта.

1. Какую проблему вы пытаетесь решить?

Информационная технология — не самоцель, она призвана улучшить или сделать возможными некоторые бизнес-процессы. Исторически специалисты по ИТ часто грешили тем, что пытались адаптировать или рекомендовать новую технологию только потому, что это интересно или потому, что это новейшая технология «на острие прогресса». В результате для решения приходилось подбирать проблему. Это не только очень дорого, но и порождает конфликт с конечными пользователями, которым необходимо просто решать стоящие перед ними задачи. Вопросы архитекторам проекта, как точно описать задачу, которую они пытаются решить, позволяют убедиться, что это настоящая проблема, и рекомендуемые изменения предлагаются не просто ради теоретических изысканий.

Кроме того, такая постановка вопроса позволяет четко определить границы проекта. Если изначально ставится расплывчатая, нечеткая задача, проект неизбежно будет эволюционировать и развиваться для решения новых проблем вне зависимости от того, связаны ли они с исходной проблемой. Если архитекторы проекта не могут четко объяснить, какую задачу они пытаются решить, проект следует отправить на доработку.

2. Как проблема решается сейчас? Какие ограничения присущи текущему решению?

После того как проблема четко обозначена, необходимо определить, каким образом она решается в данный момент. Возможно, что сейчас проблема не имеет решения, но чаще всего решение или обходной путь все-таки существует. Если инициаторы проекта не могут разъяснить, каким образом проблема решается в организации в настоящее время, или утверждают, что проблемой до сих пор никто не занимался, можно смело сделать вывод, что они просто не задавались подобным вопросом.

Следующий вопрос, который следует задать: какие ограничения имеются у существующего подхода к решению проблемы? Он поможет определить, имеются ли у используемого подхода действительно объективные ограничения или же дело в неважном исполнении. В последнем случае следует задуматься: может быть, стоит попытаться наладить имеющийся процесс, прежде чем вкладывать средства в разработку и реализацию нового решения?

3. В чем заключается новизна предложенной идеи?

Ответ на этот вопрос может оказать решающее влияние на успех любого ИТ-проекта, связанного с разработкой программного обеспечения для конечных пользователей. Что нового даст предлагаемое решение по сравнению с программами, используемыми в настоящее время в организации, и с теми, что уже представлены на рынке? Если при ответе на этот вопрос возникают затруднения, значит либо предлагаемая разработка не дает ничего нового, и подобные решения уже существуют, либо не была проведена соответствующая предпроектная подготовка. Вместе с тем проект не следует отвергать только из-за того, что он не обе-

щает новизны — возможно, предлагаемое решение позволит решать те же задачи, что и существующее, но со значительно меньшими затратами.

4. Какую пользу принесет проект?

Если предложившие проект специалисты успешно ответили на первые три вопроса, возможно, предлагаемый проект действительно чего-то стоит. Этот вопрос следует задавать для того, чтобы определить и посчитать ожидаемый эффект от реализации проекта. Когда кто-то предлагает проект, вам предоставляется возможность продать по максимальной цене картинку для менеджеров высшего звена, как их бизнес будет выглядеть в случае успеха проекта. Для ИТ-специалиста ответ на этот вопрос позволит определить, как подсчитать возврат от инвестиций в проект.

Нужно иметь в виду, что, помимо позитивного эффекта, успешный проект может обнажить или даже породить проблемы в других областях бизнеса. Этот потенциальный удар следует обсудить, чтобы можно было определить, как избежать возможных негативных последствий на этапе разработки. Например, можно разработать высококлассный B2B-портал, но компания может не обладать ресурсами для обеспечения логистики и своевременного выполнения заказов.

5. Каким образом будут достигаться ближайшие, среднесрочные и долговременные результаты?

Этот вопрос позволяет понять, как будет организован проект для достижения ближайших, среднесрочных и долговременных целей, как он будет передан проектной команде и как команда будет работать над проектом. В долгосрочной перспективе проект должен вписываться в общий бизнес и технологическую стратегию компании. Если ИТ-персонал не обладает достаточным опытом, возможно, для ответа на этот вопрос понадобится ваше руководство.

6. Как определить продвижение в реализации проекта? Как измерить эффективность реализации проекта?

Чем крупнее проект, тем важнее определить его этапы и использовать их как контрольные точки. Разбиение на этапы позволяет уменьшить сложность общего проекта за счет определения более управляемых и достижимых целей. Измерение продвижения проекта по завершении этапа позволяет ИТ-менеджеру на ранней стадии заметить проблемы и отставание от графика.

Ответ на следующий вопрос имеет особое значение для высшего менеджмента — это основной итог. Компании стараются измерить то, что для них ценно, и ценят то, что они могут измерить. Разработка оценок до начала проекта поможет команде проекта построить/разработать/выбрать соответствующую систему измерений и методик, благодаря чему эффект внедрения проекта будет легко предсказать. Эта информация пригодится при расчете полной стоимости внедрения проекта и возврата инвестиций.

7. Как определить, что проект завершен?

Об этом вопросе часто забывают, но на самом деле он имеет огромное значение в каждом проекте, для которого не существует четкого критерия завершения (как часто бывает с проектами по разработке программного обеспечения). Помимо установки этапов проекта, желательно выяснить, каковы критерии прекращения проекта. Если конец проекта четко не определен, существует опасность, что активные работы по проекту будут продолжаться даже тогда, когда это не приносит никакой реальной пользы. Первоначальный выпуск программного обеспечения не обязан быть совершенным, для этого существуют последующие выпуски, но он должен отвечать поставленной задаче. Критерий прекращения проекта поможет определить, когда следует прекратить работы по проекту.

8. Какова стоимость проекта?

Есть добрая традиция оставлять лучшее напоследок. Какова стоимость проекта? Эта информация нужна не только для того, чтобы подсчитать совокупную стоимость владения и возврат инвестиций. Поскольку бюджет отдела ИТ ограничен, инвестиции в один проект могут означать необходимость сокращения или прекращения инвестиций в другие проекты. Необходимо иметь сведения о стоимости проекта, чтобы правильно распределить сотрудников, ресурсы и финансы и выбрать проекты, которые принесут большую пользу, оптимально используют финансирование, персонал и другие ресурсы. При оценке стоимости проекта полезно учитывать одно правило: любой большой проект требует больше времени и финансов, чем ожидается до его начала. Несколько лет назад одна из менеджеров проекта, с которой мне довелось работать, поделилась своим методом: любую оценку времени и стоимости, которые ей сообщали технологи, она умножала на число Пи. И хотя этот метод абсолютно антинаучен, он позволял получать удивительно точные оценки.

Не полагайтесь на случай

ИТ-менеджерам, как и инвесторам, приходится рисковать и надеяться на то, что сделанный при оценке проекта выбор правилен. ИТ — не Лас-Вегас, чтобы полагаться на волю случая: при оценке проектов необходимо опираться исключительно на проверенные данные.

Обходим ограничения SHAREPOINT

Этан Вилански, Джеф Сандлер

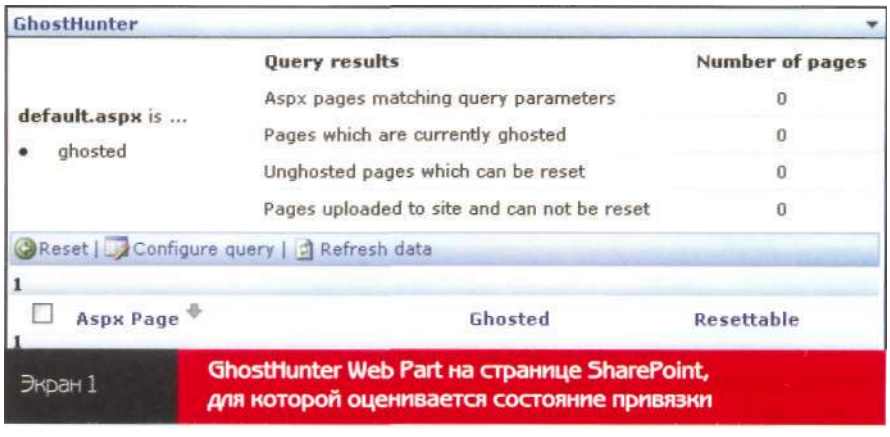
Круг пользователей Microsoft Office SharePoint Portal Server 2003 и Windows SharePoint Services 2.0 быстро растет. Поэтому специалисты по ИТ должны быть готовы к тому, чтобы принять на себя заботы по управлению этими инструментами (возможно, кому-то уже приходится решать подобные задачи).

Выходят в свет книги и статьи, призванные помочь администраторам научиться управлять сервером SharePoint Portal Server и службой Microsoft Windows SharePoint Services (в данной статье они будут представлены под общим названием SharePoint). Существуют ресурсы, в которых объясняется, как воспользоваться многочисленными достоинствами SharePoint. Но лишь немногие авторы рассказывают о слабых сторонах SharePoint. Работая с SharePoint, нам пришлось затратить на устранение пробелов в функциональности SharePoint и подготовке возможных решений больше времени, чем хотелось бы. Но мы не собираемся огульно критиковать, а просто пришли к выводу, что, обойдя некоторые очевидные ограничения — при радикальной настройке на конкретное применение, интернационализации или локализации на уровне портала и в функциях поиска, - можно более плодотворно работать с SharePoint сразу же после установки продукта.

Разработчики Microsoft внимательно прислушиваются к мнениям потребителей, поступавшим в компанию при проведении различных программ поддержки, в том числе Developer Advisory Council (DAC), Partner Advisory Council (PAC) и Technology Adoption Program (TAP). Так что многие из отмеченных нами недостатков в следующей версии Microsoft Office с условным названием Office 12 будут устранены. Мы активно изучаем программу SharePoint из пакета Office 12 Beta 1, но судить об улучшениях можно будет только после того, как выйдет окончательный продукт. Пользователям же версий, предшествующих Office 12, будет полезно знать о недостатках продукта.

Недостаток № 1: индивидуальная настройка портала

Большинство компаний стараются придать своему порталу отличительные особенности. С помощью XML-технологий, применяемых во многих современных продуктах для порталов, легко получить настраиваемые и расширяемые архитектуры. XML широко используется в SharePoint, но специалисты Microsoft не приложили особых усилий для отделения бизнес-логики и базовых данных от уровня презентаций; поэтому глубоко настроить SharePoint на конкретное применение сложно. Под глубокой настройкой имеются в виду такие изменения, как перестройка глобальной навигационной структуры, шаблона результатов поиска или подготовка новых определений сайта



Экран 1 GhostHunter Web Part на странице SharePoint, для которой оценивается состояние привязки

SharePoint. Многие поставщики порталов (например, BEA Systems, IBM, Oracle, Vignette) в конкурентной борьбе с SharePoint делают акцент на простоте настройки своих продуктов. В архитектуре таких продуктов презентация полностью отделена от компонентов портала и структуры сайта; в SharePoint презентация, контент и структура тесно связаны. Компания Microsoft выпустила несколько документов, которые помогают настроить SharePoint, но единого руководящего документа не существует.

Решение. Для успешной настройки SharePoint требуется провести тщательное исследование. Необходимо разобраться в определениях сайта — сложных наборах файлов ASP.NET (.aspx) и XML, составленных с помощью языка Collaborative Application Markup Language. CAML — язык на основе XML, используемый программистами для создания и настройки областей SharePoint, сайтов и других элементов (например, списков). Настройку помогает упростить такой инструмент, как Visual Studio.NET (VS.NET) 2005 или VS.NET 2003. Кроме того, может пригодиться практический опыт программирования ASP.NET и знание объектных моделей SharePoint.

В некоторых источниках для настройки SharePoint рекомендуется использовать Microsoft FrontPage 2003. Действительно, применение FrontPage — самый простой способ настроить область SharePoint Portal Server или страницы сайта Windows SharePoint Services, но при этом SharePoint отсоединяет (unghost) страницу от базового шаблона. Достаточно открыть страницу SharePoint внутри FrontPage и щелкнуть на кнопке Save, и страница отсоединяется от шаблона, даже если в ней не сделано никаких изменений.
Отсоединение отделяет сайт или страницу области от шаблона файловой системы, из которого были получены сайт или страница. Если сайт или страница отсоединяются, SharePoint извлекает контент и метаданные страницы из базы данных,

Возможности портала

Сетевой инженер Лэйси Рассел и пользователи компании, где она работает, получают необходимую информацию из портала SharePoint.

Энн Грабб

Как большинство компаний, InterKnowlogy — огромная «кладовая» информации. Но три года назад значительная часть ее «сокровищ» была глубоко скрыта в папках и файлах в сети и на компьютерах служащих, в тематических цепочках сообщений электронной почты и непосредственно в памяти сотрудников. В 2002 г. компания начала использовать инструменты коллективной работы Microsoft, Windows SharePoint Services и, позднее, Microsoft SharePoint Portal Server, чтобы облегчить доступ и совместное применение этих знаний для сотрудников и приглашенного персонала. В беседе со старшим редактором Энн Грабб сетевой инженер и специалист компании InterKnowlogy по общему обслуживанию ИТ **Лэйси Рассел** рассказала о том, как настроена в их компании конфигурация SharePoint, какую пользу получают от продукта конечные пользователи, и дала несколько практических советов.

Что побудило InterKnowlogy к переходу на SharePoint? Какие приложения компания использовала в прошлом, прежде чем заменить их порталом?

Мы использовали специализированный Web-узел Active Server Pages (ASP) для развертывания таблицы штатных сотрудников, в которой содержатся сведения об аттестатах, квалификации и другие данные, в частности адреса электронной почты и номера телефонов. Вся эта информация хранилась на небольших страницах, добавляемых в специализированные ASP, с которыми время от времени работали двое наших специалистов. Новых сотрудников приходилось вносить в базу данных вручную с помощью SQL Server Enterprise Manager. Эта процедура была очень утомительной. Много информации хранилось в разделяемых папках и было скрыто на настольных компьютерах и рабочих серверах, Фрагментированная информация была рассеяна повсюду.
Мы начали использовать Windows SharePoint Services в Microsoft Office Project Server. В процессе работы Project Server создает для проекта сайт Windows SharePoint Services. Мы использовали этот сайт для хранения всех результатов проекта. Когда была выпущена бета-версия SharePoint Portal, мы стали экспериментировать с ней. Потом мы опробовали SharePoint в других проектах (это была уже версия Beta 2) и решили применять этот продукт более широко. Сегодня компания использует как SharePoint Services (в Project Server), так и SharePoint Portal Server (домашняя страница InterKnowlogy представлена на экране 1).

Расскажите об этапах типичного проекта, от начала до конца, и роли SharePoint в этом процессе.

После того как назначается дата начала проекта, мы используем Project Server, чтобы составить расписание проекта, и создаем сайт Windows SharePoint Services, содержащий все элементы, относящиеся к проекту. Сайт содержит заранее подготовленные списки, настроенные на нужды нашей компании, в которых, в частности, содержится информация о неполадках и ошибках, а также целые документы, например техническое задание и все заключенные договоры.
На первом совещании по проекту менеджер программы дает каждому участнику ссылку на сайт. Как администратор, я могу делегировать менеджеру программы полномочия по обслуживанию

а не из исходного шаблона файловой системы. Любые последующие изменения в шаблоне файловой системы в отсоединенной странице не отражаются. Благодаря кэшированию шаблонов страницы, как правило, извлекаются из файловой системы быстрее, чем из базы данных.

К счастью, компания Bluedog Limited выпустила компонент Web Part, именуемый GhostHunter, с помощью которого можно обнаружить и вновь присоединить отсоединенную страницу. GhostHunter привязывает страницу к шаблону файловой системы, из которого была построена страница. На экране 1 показано, как GhostHunter Web Part выглядит на странице, для которой оценивается состояние привязки. Особенность GhostHunter: любые изменения, сделанные в отсоединенной странице, при восстановлении привязки теряются.

Поэтому, вопреки рекомендациям Microsoft, мы не советуем задействовать FrontPage 2003 в качестве инструмента для настройки SharePoint. FrontPage 2003 вполне приемлем для сайтов небольших групп, которым требуется лишь незначительная настройка, но для глубокой переработки нескольких сайтов следует использовать такой инструмент, как VS.NET.

Экран 2 Сайт Windows SharePoint Services на французском языке

Недостаток № 2: поддержка нескольких языков в SharePoint Portal Server

В Windows SharePoint Services 2.0 разработчики уделили больше внимания совместимости с локализованными языками, и в настоящее время продукт в этом отношении не уступает Office. Устанавливая пакеты языковых шаблонов Windows SharePoint Services 2.0 (с общим именем Windows SharePoint Services 2.0 Language Template Pack) и настраивая региональные параметры, можно разместить несколько языковых сайтов на виртуальном сервере Windows SharePoint Services или на ферме серверов.

После установки пакета Language Template Pack и в процессе создания сайта можно добавлять сайты Windows SharePoint Services на поддерживаемых языках. Единственный обязательный дополнительный шаг

Возможно[illegible]ия

сайта — например, добавлять пользователей. Это очень удобно. Разработчики могут обращаться к сайту и создавать списки дискуссий, отыскивать контактную информацию клиента, им доступна вся информация, помещенная на сайт менеджером программы. Сосредоточив данные в одном месте, можно сэкономить много места, отведенного под электронную почту, так как исчезают длинные цепочки сообщений.

Как еще может применяться SharePoint?

Мы используем Windows SharePoint Services с Microsoft Office InfoPath 2003. В настоящее время мы переводим заявления о предоставлении отпусков в форму InfoPath. Пользователь обращается на Web-узел, выбирает форму заявления на отпуск, заполняет и отсылает ее. Форма автоматически заносится в библиотеку, и менеджер может вынести свою резолюцию.

SharePoint — превосходная база знаний. Предположим, что разработчик нашел решение проблемы, над которой работал в течение нескольких недель. Разработчик вносит свое решение в подготовленный нами список — базу знаний. Каждая запись содержит ссылку на описание проблемы, решения и причины неполадки. Если другой сотрудник сталкивается с этой проблемой, он может сразу найти в базе знаний нужные сведения и не изобретать велосипед.

Кроме того, я использую SharePoint для обслуживания ИТ-инфраструктуры. Если пользователь нуждается в помощи, он заполняет форму на сайте SharePoint, излагает суть проблемы и предполагаемую дату ее устранения. Я могу обратиться к SharePoint и просмотреть список задач по обслуживанию. В другом списке мой руководитель может увидеть, над какими проблемами я работаю и на какой стадии находятся эти процессы. Такое применение SharePoint экономит массу времени, так как мне не приходится проводить часовые совещания с шефом, чтобы представить ему отчет о своем продвижении по списку задач. Он может просто посмотреть список и оценить степень реализации каждого проекта. А пользователи могут обратиться к своим вопросам, чтобы выяснить, получен ли ответ и не нужна ли мне дополнительная информация для решения проблемы.

Итак, информация собрана на одном сайте, обратиться к которому может каждый, а не заперта на чьем-то компьютере. Эти знания всегда доступны, даже если отсутствует администратор, «хранитель» этих данных?

Да. Я могу уйти в отпуск и не беспокоиться, не забыла ли я перед уходом сказать кому-то что-то важное. Вся необходимая информация есть на сайте.

Приходилось ли вам сталкиваться с неожиданностями в процессе использования SharePoint?

Одна из неожиданностей заключается в том, что человеку, ранее не знакомому с SharePoint, требуется удивительно мало времени, чтобы привыкнуть к нему. Некоторые пользователи привыкли получать информа-

Экран 2 Тот же сайт Windows SharePoint Services на испанском языке

при создании сайта — выбрать язык из раскрывающегося списка Language в нижней части страницы New Share-Point Site. На экране 2 показан итоговый сайт на французском; на экране 3 — тот же сайт на испанском языке. Можно строить локализованные сайты с использованием stsadm.exe и операции create-site, указав соответствующий языковой пакет с помощью ключа -lcid и кода языка locale ID (LCID).

Пакет Language Template Pack добавляет в файловую систему переведенные шаблоны сайтов Windows SharePoint Services для каждого примененного пакета. Windows SharePoint Services переводит все поддерживаемые страницы и типовые элементы сайтов, такие как панель навигации, панель ссылок и панели быстрого запуска. Готовые компоненты Web Part (в том числе встроенный контент) также переведены, но для всех специальных Web Part требуется отдельная локализация, вручную. Чтобы увидеть коды LCID установленных языковых пакетов, следует заглянуть в каталог %programfiles%\common files\microsoft shared\web server extensions\60\template на сервере или серверах, на которых размещается Windows SharePoint Services. Каждый пакет расположен в соответствующем подкаталоге LCID в данном каталоге. Установленные языковые пакеты можно увидеть и в разделе Add/Remove Programs панели управления сервера.

SharePoint Portal Server не обеспечивает такой же гибкой поддержки языков, как Windows SharePoint Services. Хотя SharePoint Portal Server и Windows SharePoint Services совместимы с одними и теми же языками, поддержка SharePoint Portal Server ограничивается одним языком для экземпляра портала. Язык, выбранный при создании портала, — единственный, который можно употреблять в любом его экземпляре; этот язык также используется по умолчанию для всех сайтов Windows SharePoint Services в данном портале, несмотря на возможность разместить сайты на нескольких языках в одном

цию определенным способом, а в SharePoint все выглядит иначе. Но, поработав с продуктом, легко запомнить его особенности, так как графический интерфейс стабилен. Например, определенные ссылки находятся всегда в одном месте, если только интерфейс не подвергается радикальной перестройке. При развертывании задача настройки SharePoint на работу с некоторыми приложениями может оказаться трудоемкой. Например, мы хотим интегрировать SharePoint Portal Server и Active Directory (AD), поэтому строим компонент Web Part для управления AD через портал. Для решения таких задач требуется много времени.

Расскажите о выполнении резервного копирования и восстановления баз данных SharePoint. Часто приходится слышать, что эти операции, особенно восстановление, вызывают затруднения.

Да, восстановить базу данных несколько сложнее. Я выяснила, что лучший способ — выполнить восстановление на другом сервере. В сущности, вместо прямого восстановления на производственном сервере строится клон исходного сервера, и данные извлекаются из него. Это процесс довольно трудоемкий. (Некоторые поставщики, такие как CommVault и Symantec, выпускают агентов специально для резервного копирования и восстановления баз данных SharePoint. — *Прим. ред.)*

Какое обучение проходят конечные пользователи SharePoint?

Обучение, безусловно, обязательно. В процессе начального развертывания SharePoint мы провели два четырех- или пятичасовых сеанса обучения, один для менеджеров программ и управляющих пользователей, другой — для разработчиков. Наши специалисты подготовили презентацию, в которой показано, как перемещаться по Web-узлу и где находится различная информация.

SharePoint не относится к числу продуктов, которые можно просто передать сотрудникам с требованием обязательного применения. Новому пользователю нужно провести по меньшей мере час со специалистом, который покажет ему приемы работы. Однако достоинство SharePoint в том, что, если администратор верно назначил полномочия, сломать его практически невозможно.

Был ли переход на SharePoint удачным шагом для InterKnowlogy?

Я считаю, что благодаря SharePoint каждый сотрудник компании экономит много времени. «Докапываться» до информации больше не требуется. Данные легко найти всегда, когда в них возникает необходимость; не приходится спрашивать у коллег, где найти те или иные сведения. Цена SharePoint достаточно умеренна, 3995 долл. за сервер плюс клиентские лицензии доступа (CAL), если учесть огромный объем полезной информации, которую получают наши пользователи.

Энн Грабб
Старший редактор в Windows IT Pro. Она имеем более чем двадцатилетний опыт работы, является автором и редактором статей, книг и других материалов по компьютерной и юридической тематике. agrubb@windowsitpro.com

Организация поиска на сайтах

Для использования функций поиска на сайтах Windows SharePoint Services необходимо в ходе развертывания Windows SharePoint Services выбрать режим установки Server Farm, чтобы впоследствии указать путь к экземпляру Microsoft SQL Server, на котором размещается Windows SharePoint Services. Чтобы настроить Windows SharePoint Services на использование компонента SQL Server Full-Text Search, следует перейти на страницу Windows SharePoint Services Central Administration-Configure Full-Text Search и установить флажок Enable full-text search and index component. Поиск на сайтах доступен только через SQL Server, но не Microsoft SQL Server Desktop

наборе сайтов Windows SharePoint Services.

Решение. Если необходимо обеспечить поддержку нескольких языков на уровне портала, то самое практичное решение — установить несколько экземпляров SharePoint Portal Server. Если требуется совместимость с несколькими языками и в Windows SharePoint Services, то можно построить один виртуальный сервер Windows SharePoint Services со многоязыковыми пакетами.

Этот метод — лучший на сегодня, но следует помнить, что при установке нескольких экземпляров SharePoint Portal Server возрастает сложность администрирования. Приходится обслуживать несколько языков для установленных SharePoint Portal Server и отдельно управлять конфигурацией каждого экземпляра сервера в портале. Кроме того, простого способа поддерживать несколько языков в одном экземпляре Windows SharePoint Services не существует. Попытка решить эту проблему с помощью зеркального отображения контента в смежных экземплярах портала или нескольких сайтах (в каждом экземпляре или сайте используется свой язык) — дополнительная нагрузка для администратора. Однако обслуживание нескольких языков на любой Web-платформе (как Microsoft, так и других) — огромный труд. Каждый фрагмент контента должен быть переведен на все языки. Существуют технологии автоматического перевода, но их результаты неудовлетворительны. Задача обслуживания многоязыковой Web-платформы может оказаться более сложной, чем администрирование предложенного в статье решения.

Недостаток № 3:

поиск на сайтах Windows SharePoint Services

Если установлена база данных с компонентом Full-Text Search, а служба Windows SharePoint Services настроена на использование SQL Full-Text Search, то можно задействовать механизм поиска на сайтах Windows SharePoint Services. Дополнительные сведения приведены во врезке «Организация поиска на сайтах».

Даже если компонент SQL Server Full-Text Search установлен и интегрирован со службой Windows SharePoint Services, область поиска ограничивается сайтом Windows SharePoint Services, из которого запущен поиск. Нельзя ввести в запрос родительские или дочерние сайты из одного или нескольких наборов сайтов либо контент из других источников вне Windows SharePoint Services (например, файловой системы, узлов Internet). Более того, разрешается использовать только простые поисковые фразы, отсутствуют передовые функции поиска, нельзя искать в присоединенных файлах, составляя списки элементов.

Решение. Самый простой способ — установить SharePoint Portal Server в качестве внешнего компонента уровня портала, привязав его к виртуальному серверу Windows SharePoint Services и соответствующим наборам сайтов. Кроме того, из страницы Site Settings-Configure Search and Indexing портала можно принимать или отвергать сайты для индексации контента. Служба SharePoint Portal Server Search (SharePointPSSearch) обследует и индексирует выбранные сайты. После завершения индексации поисковая операция в портале возвращает результаты из портала и всех выбранных сайтов Windows SharePoint Services.

Если режим Advanced Search Administration Mode активизирован через SharePoint Portal Server Central Administration, то можно расширить функцию поиска сайта/каталогов, построив источник контента сайта/каталогов. Можно добавить инструкции для обследования контента, размещенного вне портала, в частности общих каталогов, общедоступных папок Microsoft Exchange Server и других сайтов Internet.

Существуют и программные способы расширения поиска. Если разместить сайты Windows SharePoint Services на сервере SharePoint Portal Server, то можно заменить Web-элемент управления поиском Windows SharePoint Services Web-элементом управления поиском портала для поиска по содержимому локального сайта (или во всех сайтах в иерархии набора сайтов) из сайта Windows SharePoint Services. Решения от независимых поставщиков, такие как CorasWorks Workplace Suite, располагают компонентами Web Part для поиска внутри набора сайтов или в нескольких наборах сайтов.

Помните об ограничениях

Безупречных программных продуктов не существует. У любого сложного приложения есть какой-нибудь недостаток, особенно если круг пользователей разнообразен. Выявление недостатков и поиск решений — важный компонент оценки продукта и его настройки на работу в конкретных условиях. Если кому-то из читателей случится обнаружить другие изъяны SharePoint, просим сообщить нам; мы постараемся проанализировать их в будущих статьях. W

Этан Вилански — редактор Windows IT Pro и директор по технологии компании EDS и ее подразделения Technology Strategy and Architecture.
ewilansky@windowsitpro.com

Джеф Сандлер — ведущий технолог компании EDS и ее подразделения Technology Strategy and Architecture. Его стаж в EDS как архитектора и разработчика разнообразных технологических платформ составляет 15 лет.
jsandl01@gmail.com

Отключение ActiveX как способ защиты сетей

Использование групповой политики для активизации ограниченного числа надстроек

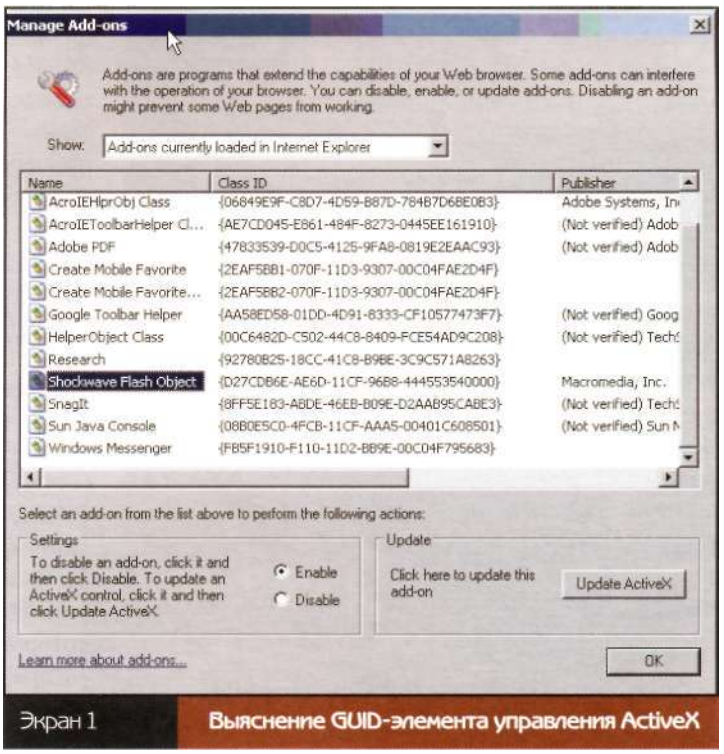
Ник Виттом

Директор консультационной компании NTES из Ирландии, Microsoft MVP по Small Business Server. nick@nte.ie

Когда речь заходит об обеспечении безопасности сети малого бизнеса, неважно — на базе Windows Small Business Server 2003 (SBS 2003) или Windows Server 2003, я советую блокировать компоненты ActiveX на компьютерах Windows XP Service Pack 2 (SP2), и уж если разрешать, так только специально выбранные элементы управления. Блокируя элементы управления ActiveX, можно в значительной степени снизить риск запуска на компьютерах пользователей несанкционированного кода через Microsoft Internet Explorer (IE) и тем самым защитить системы клиентов от разного рода вредоносных программ, шпионского программного обеспечения и вирусов.

В своих продуктах SBS 2003 и Windows 2003 компания Microsoft предложила нам новый набор утилит Group Policy для управления ActiveX в доменах. Используя настройки новых групповых политик, администраторы могут добавлять в «белые списки» Group Policy разрешенные к применению ActiveX и блокировать запуск на компьютерах клиентов всех остальных ActiveX. К сожалению, этот процесс организован не так просто, как хотелось бы. Требуется отыскать глобальный уникальный идентификатор — Globally Unique Identifier (GUID), или Class ID, тех активных элементов ActiveX, запуск которых планируется разрешить, и вручную прописать длинные строки, состоящие из букв и цифр, вместо того чтобы просто использовать операции копирования-вставки. Надеюсь, данная статья поможет читателям преодолеть «кочки и ухабы» этого процесса; в остальном же будем надеяться на то, что в Windows Vista и IE 7.0 процедура будет усовершенствована и станет попроще.

Эта статья написана для тех, кто работает с сетями на базе SBS 2003, где присутствуют такие компоненты, как Windows SharePoint Services и Microsoft Outlook Web Access (OWA), и где задействованы механизмы использования надстроек IE. Но похожим образом все устроено и в больших сетях, где имеются аналогичные службы и используются те же самые механизмы.



Экран 1 Выяснение GUID-элемента управления ActiveX

Шаг 1. Поиск GUID для "белого списка»

Чтобы поместить элементы ActiveX в «белый список» групповой политики, сначала надо выяснить, какие элементы управления нужны пользователям. После этого требуется отыскать Class ID каждого такого элемента и вписать его в объект групповой политики — Group Policy Object (GPO).

На компьютере клиента, на котором, по всей вероятности, находятся элементы ActiveX и которые могут пригодиться остальным пользователям, следует запустить IE. Нужно выбрать в меню Tools команду Manage Add-ons. В окне Manage Add-ons представлены два списка элементов управления ActiveX: список элементов ActiveX, загруженных в системе в данный момент, и список элементов ActiveX, которые ко-

гда-либо загружались в системе. Необходимо открыть контекстное меню заголовка любого из двух списков, выбрать Class ID и добавить колонку Class ID в диалоговое окно (см. экран 1).

Далее следует просмотреть оба списка ActiveX и выписать идентификаторы класса (Class ID) тех активных элементов, которые предполагается поместить в «белом списке» GPO, в том виде, в каком они представлены в окне Manage Add-ons, — со всеми открывающими и закрывающими скобками и всеми дефисами. К сожалению, невозможно просто скопировать Class ID из списка и вставить содержимое буфера прямо в GPO. Надо быть готовым к тому, что Class ID придется вводить вручную, так что следует быть внимательным, переписывая идентификатор класса.

Но это еще не все. Списки Manage Add-ons в IE 6.0 не отображают всех запущенных в системе элементов ActiveX. Это очевидно, поскольку надстройки «спрятаны» за другими процессами. Мне пришлось провести небольшое расследование и собрать список надстроек, которые необходимы для того, чтобы те или иные возможности SBS 2003 заработали в полной мере, например Remote Web Workplace или OWA. В приведенной ниже таблице показан список ActiveX, обновляемый по мере необходимости (см. также статью Microsoft «Outlook Web Access and Small Business Server Remote Web Workplace do not function if XP Service Pack 2 Add-on Blocking is enabled via group policy», http://support.microsoft.com/kbid?=555235). Необходимо переписать идентификаторы класса для надстроек и указать их в списке разрешений GPO для включения соответствующей функциональности SBS 2003.

Таблица. Скрытые надстройки, необходимые для нормального функционирования SBS 2003

GUID	ActiveX Control
Remote Web Workplace	
{F414C260-6AC0-11CF-B6D1-00AA00BBBB58}	JavaScript
{B54F3741-5B07-11cf-A4B0-00AA004A55E8}	VBScript
{7584C670-2274-4EFB-B00B-D6AABA6D3850}	Microsoft RDP Client Control (redist)
OWA	
{8D91090E-B955-11D1-ADC5-006008A5848C}	DEGetBlockFmtNamesParam Class
{2D360201-FFF5-11D1-8D03-00A0C959BC0A}	DHTML Edit Control Safe for Scripting
{2933BF90-7B36-11D2-B20E-00C04F983E60}	XML DOM Document
{F6D90F11-9C73-11D3-B32E-00C04F990BB4}	XML DOM Document
{F6D90F16-9C73-11D3-B32E-00C04F990BB4}	XML HTTP
{ED8C108E-4349-11D2-91A4-00C04F7969E8}	XML HTTP Request
{3050f4f8-98b5-11cf-bb82-00aa00bdce0b}	Microsoft HTML Component
{B45FF030-4447-11D2-85DE-00C04FA35C89}	SearchAssistantOC
{8856f961-340a-11d0-a96b-00c04fd705a2}	Microsoft Web Browser
Windows SharePoint Services	
{3050F819-98B5-11CF-BB82-00AA00BDCE0B}	HtmlDlgSafeHelper Class
{47B0DFC7-B7A3-11D1-ADC5-006008A5848C}	DEInsertTableParam Class
{E18FEC31-2EA1-49A2-A7A6-902DC0D1FF05}	Office 11 name.dll
{9F9C4924-C3F3-4459-A396-9E9E0D8B83D1}	SharePoint OpenDocuments Class
{BDEADE9E-C265-11D0-BCED-00A0C90AB50F}	SharePoint Spreadsheet Launcher
{65BCBEE4-7728-41A0-97BE-14E1CAE36AAE}	Microsoft Office List 11.0
{E543A17A-F212-49C0-B63D-BF09B460250E}	OISClientLauncher Class
{07B06095-5687-4D13-9E32-12B4259C9813}	STSUpld UploadCtl Class
{3FD37ABB-F90A-4DE5-AA38-179629E64C2F}	SharePoint Spreadsheet Launcher
{BDEADEF4-C265-11D0-BCED-00A0C90AB50F}	SharePoint Stssync Handler
{003FAFEF-54E3-4D94-9765-44C55997A91C}	MsSvAbw.AddrBookWrapper
ConnectComputer (client setup)	
{485D813E-EE26-4DF8-9FAF-DEDF2885306E}	NSHelp Class
Microsoft Office	
{E18FEC31-2EA1-49A2-A7A6-902DC0D1FF05}	Office 11 name.dll

В зависимости от того, какие еще надстройки нужны, возможно, потребуется дополнительное расследование на предмет выявления других элементов ActiveX, в которых могут нуждаться клиенты для взаимодействия в сети. Очень важно проделать эту работу заблаговременно, до того, как будут заблокированы все элементы управления ActiveX (за исключением тех, которые окажутся в «белом списке»). Процесс блокирования надстроек будет описан в шаге 2.

Однако на данный момент следует иметь в виду, что некоторые важные элементы ActiveX будут не учтены, поэтому в дальнейшем понадобится внести дополнительные идентификаторы Class ID в «белый список» — уже после того, как блокирование ActiveX вступит в силу.

Чтобы обнаружить все Class ID, которые подгружаются в систему клиента при обращении к тому или иному Web-сайту, сначала нужно загрузить и установить специальную утилиту Microsoft Debugging Tools for Windows (по адресу http://www.microsoft.com/whdc/devtools/debugging/default.mspx). Следует запустить программу WinDbg и настроить путь к отладочным символам на общедоступный сервер отладки, расположенный по адресу http://msdl.microsoft.com/download/symbols.

Затем требуется подключиться к процессу IE (IEXPLORE), который к тому времени уже должен быть запущен, и установить следующую точку останова в консольном окне:

```
bp  SHLWAPIISHCoExtensionAllowed
  «db poi(esp+4); g»
```

Нажмите F5, чтобы разрешить работу IE, и откройте Web-сайт, с которым предполагается взаимодействовать через IE.

В окне отладчика должен появиться дамп памяти компьютера (см. экран 2). Каждая строка олицетворяет элемент управления ActiveX, для запуска которого требуется разрешение оператора (каждый элемент управления может появиться не один раз). По сути, это символьные строки, которые

```
0013e4cc  60 c2 14 f4 c0 6a cf 11-b6 d1 00 aa 00 bb bb 58  `....j.........X
0013e4dc  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0013e4ec  a4 d2 00 00 2c e5 13 00-86 b5 1c 7d 02 00 00 00  ....,.....}....
0013e4fc  d0 b3 1c 7d 60 c2 14 f4-c0 6a cf 11 b6 d1 00 aa  ...}`....j......
0013e50c  00 bb bb 58 50 27 bf 01-50 7a 4e 01 a0 95 10 7d  ...XP'..PzN....}
0013e51c  ac e5 13 00 10 7d 4e 01-10 7d 4e 01 00 00 00 00  .....}N..}N.....
0013e52c  bc e5 13 00 24 6c 1c 7d-a8 e5 13 00 50 27 bf 01  ....$l.}....P'..
0013e53c  01 00 00 00 00 00 00 00-10 7d 4e 01 10 7d 4e 01  .........}N..}N.
```

Экран 2 Результаты WinDbg содержат Class ID для надстроек

```
60 c2 14 f4 c0 6a cf 11-b6 d1 00 aa 00 bb bb 58

{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
```

Экран 3 Строка результатов WinDbg и соответствующий ей Class ID

в окне отладчика не отформатированы в Class ID, их еще предстоит транслировать в нужный формат.

Например, первая строка на экране 2 содержит строку, указанную в первой строке на экране 3. Если поменять порядок следования первых восьми чисел/символьных пар, убрать пробелы и добавить скобки и дефисы, получим Class ID для надстройки JavaScript, которая показана во второй строке на экране 3. Раз у нас в руках появились нужные идентификаторы класса, осталось только определить, требуются ли клиенту соответствующие надстройки и стоит ли добавлять их в разрешенный список (я не говорю, что это сделать просто). Если точно известно, что необходимо разрешить работу некоторой специфической надстройки, которая не отображается в списках IE Manage Add-ons, можно связаться с разработчиком этой надстройки и затребовать у него Class ID.

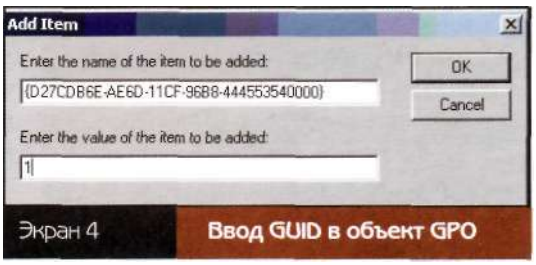
Просмотр трассы отладчика и выписывание всех GUID для всех ActiveX вручную — занятие утомительное. Единственное утешение — сделать это придется только один раз, если воспользоваться GPO для применения списка разрешений.

Шаг 2. Добавление GUID в список разрешений GPO

Итак, у нас в руках необходимые глобальные уникальные идентификаторы. Теперь можно добавить их в «белый список» GPO. На компьютере с XP SP2 следует открыть самую последнюю версию консоли Group Policy Management Console (GPMC), которую можно загрузить по адресу http://www.microsoft.com/downloads/details.aspx?familyid=0a6d4c24-8cbd-4b35-9272-dd3 cbfc81887&displaylang=en. Или можно загрузить шаблоны XP SP2 Administrative Template (.adm) по адресу http://www.microsoft.com/downloads/details.aspx?familyid=92759d4b-7112-4b6c-adabbf3802a5c9b&displaylang=en и использовать их вместе с GPMC со своего сервера. Конечно, если версия Windows 2003 SP1 уже установлена, нужные точки входа GPO, которые были введены впервые в XP SP2, уже включены.

После открытия GPMC можно отредактировать одну из существующих политик или создать новую, специальную, с учетом требуемых настроек. Я, например, создал отдельную политику для своего списка разрешений и поэтому, если понадобится, всегда могу отключить новую политику и это не окажет никакого влияния на работу остальных политик.

Теперь следует открыть политику и под узлом User или Computer перейти в Administrative Templates\Windows Components\ Internet Explorer\Security Features\Add-on Management. Установим флажок Deny all add-ons unless specifically allowed in the add-on list для разрешения запуска на станциях XP SP2 только тех ActiveX, которые будут внесены в специальный список.



Экран 4 Ввод GUID в объект GPO

Узел под Add-on Management — это список надстроек Add-on List. Его нужно открыть, выбрать Enabled и щелкнуть Show. Появится окно, в котором отображены все допустимые GUID элементов управления ActiveX. Здесь можно самостоятельно указать нужные GUIDs.

Далее следует щелкнуть Add и набрать GUID для надстройки, работу которой необходимо разрешить, не забывая об обязательных открывающих и закрывающих фигурных скобках и дефисах, и установить значение равным 1, если надстройку нужно разрешить. На экране 4 показано диалоговое окно Add Item с указанным глобальным идентификатором GUID для Macromedia Shockwave Flash Object. Необходимо внимательно проверить набранное значение идентификатора, прежде чем нажимать OK. После нажатия OK для данного GUID вернуться назад и отредактировать запись будет невозможно. Если была допущена ошибка, придется удалять всю запись целиком и добавлять ее снова. Это действительно непросто — вводить длинные строки цифр и символов для каждого GUID. После того как все GUID, необходимые для внесения в «белый список», указаны, нужно закрыть GPO. Затем следует открыть окно командной строки на клиентской системе и набрать

```
GPUpdate /force
```

или перезагрузить ее, после чего протестировать список разрешений, подключаясь к Web-сайтам, посещаемым пользователями сети, и убедиться, что все страницы загружаются нормально. Блокировка надстроек — очень мощная функция XP SP2. Нет сомнений, что Microsoft могла бы усовершенствовать описанную процедуру разрешения определенного списка ActiveX в GPO. Будем надеяться на некоторые улучшения в разрабатываемой версии IE 7.0, а пока что остается использовать этот инструмент, который позволяет надежно блокировать работу нежелательных элементов управления на станциях пользователей в различных сетях.

Планирование

Насколько «дыра» широка?

Анализируем риски, связанные с наличием уязвимостей в информационной системе

Сергей Гордейчик

Системный архитектор, преподаватель компании «Информзащита». Имеет сертификаты MCES, MCT, CISSP. gordey@infosec.ru

Информация о степени риска, связанной с тем или иным уязвимым местом в компьютерной системе, является важным параметром для выполнения ряда повседневных задач специалиста по информационной безопасности. На основании этих данных проводится анализ рисков, связанных с уязвимостью в конкретной сети или информационной системе, и соответственно принимается решение о целесообразности и оперативности устранения проблемы. В случае подозрения на возникновение инцидента в зависимости от степени риска уязвимости оцениваются средства, выделяемые для его расследования. При настройке системы обнаружения атак или сканера системы безопасности специалист по степени риска уязвимости принимает решение об использовании или отключении сигнатуры с целью повышения производительности или снижения уровня ложных срабатываний и т. д. и т. п.

Системы оценки уязвимостей

Как правило, степень риска присваивается уязвимости производителем системы, в которой изъян был обнаружен, либо компанией, выпускающей средства защиты (сканеры уязвимостей, системы обнаружения атак и т. д.). В этом случае используется привычная по правилам дорожного движения схема: низкая степень риска (зеленый), средняя степень риска (желтый), высокая степень риска (красный). Иногда выделяется дополнительный, четвертый уровень риска — критические уязвимости.

Такого подхода придерживаются многие производители, например, Microsoft в своих уведомлениях об обновлениях программного обеспечения использует четыре уровня критичности уязвимостей, приведенные в табл. 1.

Этот простой подход не всегда удовлетворяет требованиям администратора. Степень риска, связанная с уязвимостью, с течением времени может меняться. Одно дело — критическая уязвимость, о деталях эксплуатации которой известно только специалистам компании-разработчика, а другое — важная уязвимость, программа использования которой общедоступна.

Чтобы учесть факторы, связанные с вероятностью эксплуатации уязвимости, можно ввести в стандартную «светофорную» модель дополнительные условия. Например, SANS при анализе уязвимостей (SANS Critical Vulnerability Analysis) присваивает критический уровень тем уязвимостям, для которых существует общедоступная программа, использующая эти уязвимости, или использование которых не требует специальных навыков. В противном случае даже потенциально весьма опасная проблема будет иметь высокий, а не критический уровень риска. Кроме простоты эксплуатации при оценке уязвимости по методике SANS учитывается распространенность уязвимых систем.

Группа PSS компании Microsoft применяет методику оценки риска (см. табл. 2), связанного с вредоносным программным обеспечением (т. е., по сути, с атаками, использующими уязвимость), учитывающую наличие обновления, устраняющего ошибку, количество векторов, которые может применять атакующий, распространенность уязвимых систем.

Например, «критически опасный червь» должен распространяться через лазейку в программном обеспечении Microsoft, для которой отсутствует обновление, используя два и более вектора атаки в широко распространенных системах.

Перечисленные методы дают трех- или четырехуровневую оценку, что затрудняет их применение при качественном или количественном анализе рисков. Методика, используемая US-CERT, предполагает присвоение уязвимости степени риска в виде весового значения от 0 до 180, в зависимости от приведенных ниже критериев.

- Насколько доступна информация об уязвимости?
- Зарегистрированы ли случаи использования уязвимости?
- Подвержены ли опасности критичные для сети Internet-узлы?
- Какое количество узлов сети уязвимо?
- Каковы последствия использования уязвимости?
- Насколько легко воспользоваться уязвимостью?
- Каковы условия использования уязвимости?

К сожалению, связь между условиями, их возможными весами и результирующей степенью риска формально не определена, что оставляет большой простор для расхождений в оценках одной и той же уязвимости. Кроме того, перечисленные методики дают значение риска для Internet в целом, а не для конкретной информационной системы или корпоративной сети.

Резюмируя сказанное, можно сформулировать требования к методике оценки уязвимости следующим образом:

- должна присутствовать возможность оценки степени риска уязвимости в зависимости от возможности ее эксплуатации;
- результатом применения методики должно быть числовое значение, подходящее для использования при анализе рисков;
- методика должна иметь возможность адаптации к конкретной информационной системе;
- параметры, используемые при расчете, должны допускать минимум разночтений;
- механизм расчета результирующего значения должен быть прост и понятен.

Common Vulnerability Scoring System

Подобные соображения были заложены в основу общей системы оценки уязвимостей Common Vulnerability Scoring System (CVSS). Система CVSS предполагает разбиение характеристик уязвимости на три группы: базовые, временные и связанные со средой. Для каждой из групп определен четкий набор параметров, имеющих предопределенный набор возможных значений. В результате применения методики для каждой из групп получается число в диапазоне от нуля до десяти.

Расчет базовых характеристик

Базовые характеристики уязвимости включают параметры, не изменяющиеся с течением времени. Сюда входят такие параметры, как вектор эксплуатации (Access Vector), сложность использования (Access Complexity), требования к аутентификации (Authentication), последствия использования уязвимости с точки зрения целостности, доступности или конфиденциальности (CIA Impact) с учетом подверженности уязвимости различных свойств информации (Impact Bias).

При оценке вектора эксплуатации определяется, является ли данная уязвимость локальной (Local) или удаленной (Remote). Сложность доступа может быть высокой: (High) (например, требуется вмешательство пользователя) или низкой (Low). Параметр «аутентификация» может принимать два значения: для использования уязвимости требуется аутентификация (Required) либо не требуется (Not Required). В том случае если уязвимость может эксплуатироваться только локально, но не требует дополнительной аутентификации, значение данного критерия приравнивается к единице (аутентификации не требуется).

При оценке последствий эксплуатации учитывается возможное влияние уязвимости на целостность, доступность и конфиденциальность по трехбалльной шкале: влияние отсутствует (None), частичное влияние (Partial), полное нарушение одного из свойств информационной системы (Complete).

Параметр Impact Bias может принимать одно из трех значений:

Normal — уязвимость в равной степени распространяется на все свойства информационной системы;

Confidentiality — уязвимость в большей степени затрагивает конфиденциальность;

Integrity — уязвимость в большей степени затрагивает целостность;

Availability — уязвимость в большей степени затрагивает доступность.

Данный параметр введен для возможности назначения приоритетов того или иного свойства информационной системы с точки зрения выполняемых системой функций. Например, если уязвимость в шифрующей файловой системе в равной сте-

Таблица 1 Градация степеней риска уязвимостей Microsoft

Степень риска	Определение
Critical	Уязвимость может быть использована для создания Internet-«червя», распространяющегося без вмешательства пользователя
Important	Атака с использованием уязвимости может привести к снижению уровня целостности, доступности или конфиденциальности данных пользователя или целостности и доступности обрабатываемых ресурсов
Moderate	Возможность использования уязвимости затруднена различными факторами, такими как настройки по умолчанию, детективные средства защиты или сложность эксплуатации
Low	Воспользоваться уязвимостью очень сложно либо последствия минимальны

Таблица 2 Оценка критичности вредоносного ПО согласно Microsoft PSS

Характеристика	Значение
Уязвимость в продукте Microsoft	Да/обновление отсутствует
Кол-во векторов распространения	>= 2
Используется новый вектор	Да/нет
Распространенность	Высокая
Возможна потеря уникальных данных	Да/нет
Возможен отказ служб	Да

пени затрагивает (полностью нарушает) и конфиденциальность, и доступность данных, конфиденциальности должен быть отдан приоритет. Каждому из полученных значений присваивается весовой коэффициент в соответствии с приведенными ниже правилами.

```
AccessVector   = case AccessVector of
        local:      0.7
        remote:     1.0
AccessComplexity = case AccessComplexity of
        high:       0.8
        low:        1.0
Authentication  = case Authentication of
        required:   0.6
        not-required:  1.0
ConfImpact   = case ConfidentialityImpact of
        none:       0
        partial:    0.7
        complete:   1.0
ConfImpactBias  = case ImpactBias of
        normal:     0.333
        confidentiality: 0.5
        integrity:  0.25
        availability:  0.25
IntegImpact  = case IntegrityImpact of
        none:       0
        partial:    0.7
        complete:   1.0
IntegImpactBias = case ImpactBias of
        normal:     0.333
        confidentiality: 0.25
        integrity:  0.5
        availability:  0.25
AvailImpact  = case AvailabilityImpact of
        none:       0
        partial:    0.7
        complete:   1.0
AvaiilmpactBias = case ImpactBias of
        normal:     0.333
        confidentiality: 0.25
        integrity:  0.25
        availability:  0.5
```

На основании этих данных происходит расчет базового значения по формуле:

```
BaseScore = roundjojlecimal(10 * AccessVector
          * AccessComplexity
          * Authentication
          * ((ConfImpact * ConfImpactBias)
          + (IntegImpact * IntegImpactBias)
          + (AvailImpact * AvaiilmpactBias)))
```

Базовая оценка уязвимости представляет собой значение, сходное с возможными последствиями эксплуатации уязвимости (Single Loss Expectancy, SLE) в классической методике анализа рисков без учета ценности ресурса. Этот параметр может присваиваться уязвимости производителем системы при выпуске обновления.

Вероятность атаки

При оценке характеристик уязвимости, изменяющихся с течением времени, используются такие параметры, как возможность использования (Exploitability), наличие возможности устранения уязвимости (Remediation Level) и достоверность информации об уязвимости (Report Confidence).

Возможность эксплуатации оценивается по наличию информации об использовании уязвимости или соответствующих программ. Этот параметр может принимать следующие значения:

- Unproven. Метод использования не описан или носит теоретический характер.
- Proof of Concept. Существует код (или информация), доказывающий возможность использования уязвимости, но его нельзя задействовать для атак без модификаций.
- Functional. Существует работоспособная программа, использующая уязвимость.
- High. Существует червь либо полностью автоматическая программа, использующая уязвимость.

Возможность устранения уязвимости оценивается в зависимости от наличия официального (Official Fix) и временного (Temporary Fix) исправления, устраняющего уязвимость. При наличии рекомендаций по снижению степени риска данный параметр принимает значение Workaround.

Уязвимость может иметь статус неподтвержденной (Unconfirmed) либо быть подтвержденной несколькими независимыми источниками (Uncorroborated) или производителем (Confirmed). Статус Confirmed уязвимость может получить и в случае отсутствия реакции производителя, например при наличии работоспособной программы, использующей уязвимость.

Полученным значениям присваиваются веса в соответствии с приведенными ниже правилами, которые затем используются в формуле для модификации базового значения риска.

```
Exploitability  = case Exploitability of
        unproven:      0.85
        proof-of-concept:  0.9
        functional:    0.95
        high:          1.00
RemediationLeve! = case RemediationLevel of
        official-fix:    0.87
        temporary-fix:   0.90
        workaround:    0.95
        unavailable:   1.00
ReportConfidence = case ReportConfidence of
        unconfirmed:   0.90
        uncorroborated:  0.95
        confirmed:     1.00
TemporalScore = round_toJ_decimal(BaseScore *
Exploitability
              * RemediationLevel
              * ReportConfidence)
```

Таким образом, значение TemporalScore отображает риски, связанные с уязвимостью в динамике ее жизненного цикла, и учитывает текущую вероятность использования уязвимости. С точки зрения классической модели анализа полученное число близко по смыслу к показателю Annual Loss Expectancy (ALE).

Полученное значение может применяться в различных базах данных уязвимостей, включая базы данных, используемые такими средствами защиты, как сканеры системы безопасности.

Применение к конкретной системе

Третья часть параметров позволяет учесть влияние уязвимости на конкретную информационную систему. Учитываются два параметра — потенциальный ущерб от использова-

Дополнительные источники

1. **Microsoft Security Response Center Security Bulletin Severity Rating System,** http://www.microsoft.com/technet/security/bulletin/rating.mspx.
2. **SANS Critical Vulnerability Analysis Archive,** http://www.sans.org/newsletters/cva/.
3. **PSS Security Team — Security Alert Severity Matrix,** http://www.microsoft.com/technet/security/alerts/matrix.mspx.
4. **US-CERT Vulnerability Note Field Description,** http://www.kb.cert.Org/vuls/html/fieldhelp#metric
5. **Common Vulnerability Scoring System,** http://www.first.org/cvss/.
6. **National Vulnerability Database,** http://nvd.nist.gov/.

ния уязвимости (Collateral Damage Potential) и количество уязвимых систем (Target Distribution).

Потенциальный ущерб учитывает материальный либо косвенный ущерб, который может понести информационная система в случае атаки с использованием уязвимости. Зарезервированы значения Low, Medium и High. Количество уязвимых систем может принимать следующие значения:

None — потенциальные цели атаки отсутствуют или присутствуют только в непродуктивных системах;

Low — уязвимо до 15% всех систем;

Medium — уязвимо от 16 до 49%;

High — более 50% всех систем могут стать целью атаки.

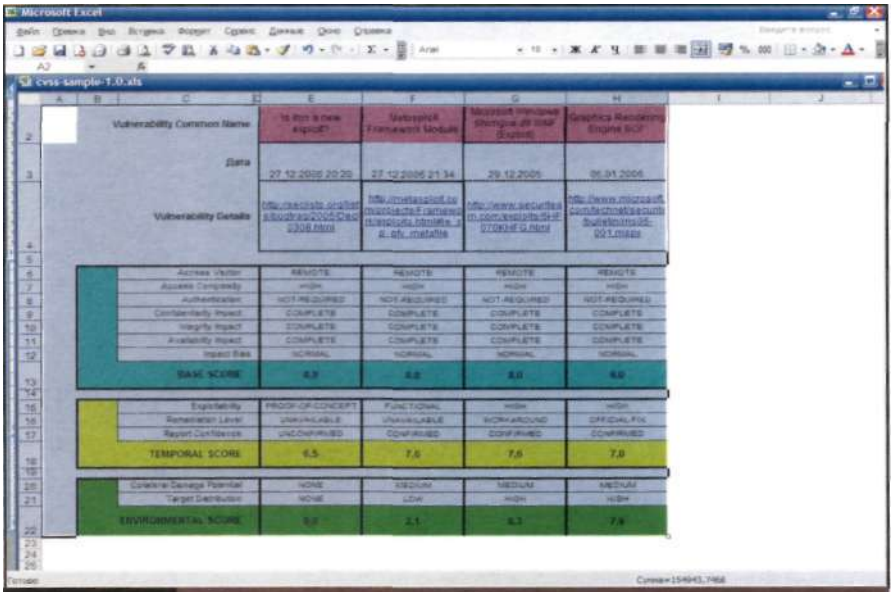
Для учета полученных значений используются следующие весовые коэффициенты и формулы:

```
CollateralDamagePotential = case
CollateralDamagePotential of
            none:    0
            low:    0.1
            medium:    0.3
            high:    0.5
TargetDistribution    = case TargetDistribution of
            none:    0
            low:    0.25
            medium:    0.75
            high:    1.00
EnvironmentalScore =
round_to_1_decimal((TemporalScore + ((10 —
TemporalScore)
            * CollateralDamagePotential))
            * TargetDistribution)
```

Практическое использование

Рассмотрим использование CVSS на примере уязвимости CVE-2005-4560 (MS06-001), также известной как WMF Bug, для сети, в которой присутствует около 15% рабочих станций под управлением Windows XP. В общем доступе информация появилась 27 декабря 2005 года (сообщение в списке рассылки Bugtraq). Само сообщение содержало ссылку на программу, использующую уязвимость для установки вредоносного программного обеспечения. Поскольку не ясно, какие системы подвержены данной уязвимости, расчет характеристик для сети не проводился (см. экран 1).

Буквально через час появилась работоспособная версия программы, использующей уязвимость для Windows XP в виде модуля для Metasploit Framework. Наличие уязвимости было подтверждено, что привело к повышению ее временных характеристик. Кроме того, на основе данных об уязвимых операционных системах было рассчитано значение риска, связанного с уязвимостью для конкретной сети. 29 декабря появилась более работоспособная версия программы, использующей уязвимость. Также были опубликованы рекомендации по временному устранению проблемы, что компенсировало рост временных характеристик риска. Кроме того, стало ясно, что уязвимость может быть использована не только в Windows XP, что увеличило результирующее значение риска.



Экран Расчет по методике CVSS для оценки риска, связанного с уязвимостью, в формате WMF.

Пятого января компания Microsoft выпустила обновление, устраняющее брешь в системе, что привело к снижению степени риска, связанного с уязвимостью. В дальнейшем, по мере установки обновлений на компьютеры, значение риска будет снижаться.

Перспективы использования

Лежащая в основе CVSS методика позволяет оценить информацию о существующих уязвимостях в информационных системах на основании различных критериев. Использование доступного математического аппарата дает возможность адаптировать методику под конкретные нужды.

Например, при анализе рисков, связанных с конкретной информационной системой (в процессе контроля защищенности или тестирования на проникновение), можно учитывать важность конкретного сервера с точки зрения бизнеса компании. Для этого значения важности потенциальных потерь (например, качественная оценка в диапазоне от 0 до 9), целостности, доступности и конфиденциальности вводятся в качестве весовых коэффициентов в формулу расчета базового значения.

В настоящий момент далеко не все производители используют CVSS для оценки риска уязвимостей в своих продуктах. Однако простота применения позволяет на основе общедоступной информации (например, уведомлений от производителя) рассчитать необходимые значения. На данный момент только база данных National Vulnerability Database содержит оценку уязвимости согласно CVSS. Однако присутствующие в ней значения зачастую далеки от реального положения дел, что компенсируется наличием калькулятора, позволяющего быстро провести расчет.

Помимо программы для расчета на nvd.nist.gov/, можно воспользоваться готовой таблицей в формате MS Excel (http://www.First.org/cvss/cvss-sample-1.O.zip) или Web-страницей http://www.patchadvisor.com/PatchAdvisor/CVSSCalculator.aspx.

Спасение медленной сети

Модернизация сети одной из компаний

Марк Барнетт

Независимый консультант по безопасности и автор, специализирующийся на безопасности в Windows. Имеет звание IIS MVP. Автор книги Perfect Passwords and Hacking the Code (Syngress). mburnett@xato.net

Многие компании, зависящие от беспроводных сетей стандарта 802.11b, объединяют их со своими проводными сетями. При этом беспроводные сети зачастую требуют индивидуального подхода к решению проблем и повышенного внимания к себе. Небольшие неполадки могут налагаться друг на друга и приводить к полной остановке беспроводной сети. Эксперименты в конструировании и управлении, проводимые на действующей сети, весьма опасны. Специалисты компании UtahWISP, поставщика услуг доступа в Internet на базе технологий беспроводных сетей (wireless ISP, WISP), создавали свою инфраструктуру, преодолевая множество трудностей.

Когда UtahWISP начала свою деятельность в Северной Юте, она была одной из первых компаний, обеспечивавших широкополосный доступ в Internet в местах, не охваченных сетями других компаний, продвигавших широковещательные решения. Сотрудники компании создали пару беспроводных точек доступа (AP) на расположенных неподалеку друг от друга башнях и установили приемники на высоких зданиях у своих клиентов. Таким образом, те, кто находился в прямой видимости башни, имел широкополосный доступ в Internet.

Поскольку компания обеспечивала сервис, который никто другой в этой местности не предоставлял, сеть UtahWISP стало лихорадить из-за быстрого роста количества пользователей. Когда число клиентов превысило 200, а количество точек доступа достигло 12, некоторые клиен-

ты, обслуживаемые беспроводной сетью, начали испытывать затруднения при просмотре сети, появлялись потерянные пакеты, замедление ответов от ping. Поскольку нагрузка на сеть UtahWISP заметно возросла, клиенты стали периодически терять соединение.

Перегрузка беспроводной сети усугубила общие проблемы, хотя, на мой взгляд, UtahWISP имеет далеко не худшие показатели производительности сети. Собрав некоторую дополнительную информацию по общим показателям производительности, я посетил UtahWISP, чтобы посмотреть, как можно повысить скорость работы сети. В этой статье я расскажу о проведенных мероприятиях по модернизации сети с целью увеличения ее производительности. Здесь будет последовательно описан весь процесс модернизации, от поверхностного взгляда на проблему до идентификации потенциальных неполадок и реализации решений, которые привели, в конце концов, крещению поставленной задачи.

Общее представление

Я знал, что сеть была медленной, но после тщательной проверки мне так и не удалось обнаружить причины замедления работы. Я видел, что имеется значительная неиспользуемая полоса пропускания, а причины снижения производительности не удается подвести под общепринятые шаблоны. Более того, общая производительность не зависела от количества пользователей и от времени их работы. Некоторые пользователи регулярно сообщали о затруднениях в работе, хотя в то же время другие имели хорошую скорость соединения и малое время отклика на команду ping. Дейл Мередит, ИТ-менеджер UtahWISP, сказал, что ему не удается установить причин происходящего.

В прошлом я имел дело с медленными беспроводными сетями, но этот случай был одним из самых трудных. В обслуживаемой UtahWISP беспроводной среде многие проблемы накладывались одна на другую и влияли на производительность сети. Но чем же эта сеть в действительности отличалась от других? Конечно же, сигнал экранировался и блокировался зданиями и деревьями. Это совсем не то, что имеет место в офисах, где препятствием для сигнала становятся стены и мебель. Настоящее различие было в масштабах сети.

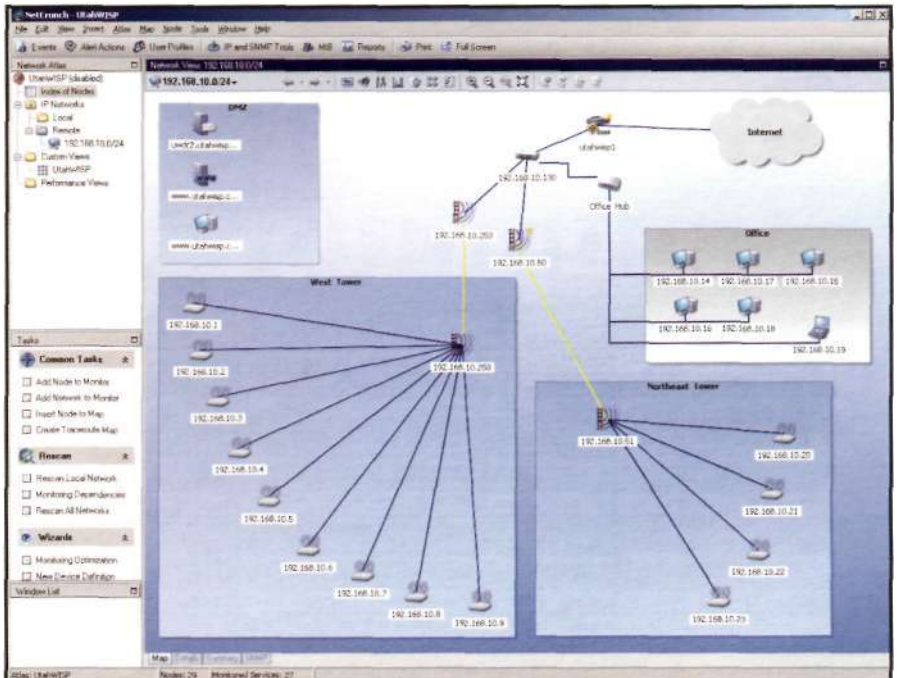
Прежде чем погружаться в подробности, еще раз вернемся к общей картине сети. Я знал, что UtahWISP имеет 12 точек доступа на двух башнях. Каждая из башен обслуживала клиентов на территории радиусом десять миль и имела быстрый беспроводной канал связи с главным офисом. В этом офисе находилась точка подключения к главному маршрутизатору UtahWISP.

Чтобы получить карту сети, я использовал AdRem Net-Crunch 3.1 Premium. NetCrunch не только позволил мне начать процесс построения наглядной карты сети, но и предоставил компании UtahWISP полноценную систему мониторинга и создания отчетов. Получив возможность производить автоматическое обнаружение, я построил пространственную карту сети. Хотя результаты автоматического поиска потребовали кое-что сделать вручную, они помогли мне сэкономить немало времени. После некоторой обработки я получил точное представление о сети Utah-WISP, показанное на экране 1.

Для наблюдения за производительностью сети компания использовала множество различных утилит, включая ping. Когда клиенты звонили с вопросами по поводу сравнительно низкой производительности, администраторы запускали ping по адресу этого клиента в течение некоторого времени и просматривали результаты на предмет ошибок. К сожалению, Windows-утилита ping не обладает достаточной гибкостью, а продолжительные ответы на эхо усугубляли проблемы пользователей, генерируя еще больший трафик. Более того, ping плохо масштабируется, а вывод команды сложен для разбора.

NetCrunch обеспечивает более широкие возможности мониторинга, в том числе возможность мониторинга счетчиков SNMP, данных системных журналов и счетчиков производительности Windows, в частности время отклика на ping. Программа имеет десятки параметров для настройки мониторинга отдельных сетей. NetCrunch предоставляет развитые средства построения диаграмм и графиков для отслеживания выбранных параметров в реальном времени.

Я решил использовать этот продукт прежде всего для отслеживания проблем с производительностью сети. Карта сети Net-Crunch сразу показа-



Экран 1 Карта сети UtahWISP, созданная программой NetCrunch

ла наличие проблемы. На ней были видны медленные ответы и большие задержки для некоторых хостов, а в определенные периоды времени сеть казалась особенно медленной. Я замечал, что хосты часто отключались и на карте появлялись красные значки отключившихся устройств. Возможно, это было результатом потери пакетов, поскольку значки на карте становились красными произвольно.

Сбор статистики

Стало ясно, что проблемы в UtahWISP были серьезнее, чем я мог предположить. Обычно можно выделить основную проблему, но эта сеть была иной. Я не нашел главной проблемы, но увидел множество мелких неполадок, результатом которых было значительное снижение производительности сети.

Мне необходимо было получить как можно больше информации о сети, поэтому я решил установить устройство Network Intelligence enVision HA Series для сбора информации из журналов. Это устройство позволило собрать статистику от различных устройств по сети и объединить все данные в одном месте для анализа.

Система Network Intelligence HA была настроена при помощи программного обеспечения enVision, которое оказалось очень удобным для сбора, объединения и создания отчетов по данным журналов с различных платформ. Система имеет встроенный набор шаблонов для интерпретации сообщений о событиях, приходящих с десятков маршрутизаторов, брандмауэров и других сетевых устройств. Система предназначена для сбора журналов на высоких скоростях и может принимать десятки и тысячи событий в секунду, что особенно полезно для перегруженной среды WISP. Система позволила мне проверять индивидуальные события, происходившие в сети, и соединять и просматривать данные через отчеты и создаваемые мною запросы. При помощи системы я сформулировал комплексные зависимости, которые генерировали сообщения на основе множества событий от множества источников.

Я настроил маршрутизатор Cisco на отправку данных Syslog в систему Network Intelligence. Кроме того, я настроил enVision для сбора журналов, событий Windows с важных серверов компании, таких как почтовые серверы, Web и DNS. Это позволило мне сопоставить системные события, происходящие на многих устройствах, находящихся в различных местах сети, и получить необходимые данные для того, чтобы вернуться назад и отследить любую проблему.

После нескольких минут работы по сбору данных журналов я увидел картину монитора сообщений enVision, которая показана на экране 2, и определил по крайней мере одну из возможных причин возникновения проблем с производительностью: сеть была поражена вирусами и шпионским программным обеспечением и загружена трафиком от одноранговых сетей (P2P).

Экран 2 Монитор сообщений EnVision

Объединение беспроводных сетей

Когда была создана «энциклопедия» журналов событий, я поставил себе задачу узнать больше о трафике беспроводной сети. Я определил, что беспроводной трафик был полудуплексным, из чего можно было заключить, что присутствует значительное количество коллизий. В полудуплексных сетях множество станций разделяют между собой единую среду, такую, например, как сетевой кабель, а в нашем случае это был беспроводной канал. Поскольку осуществлять передачу в данный момент времени в подобной среде может только один хост, необходимо иметь алгоритм управления трафиком для предотвращения коллизий пакетов. Этот процесс должен гарантировать, что другие передающие станции будут обнаруживать коллизии. Если пакеты передаются одновременно, происходит коллизия, и их необходимо передавать заново. Если в одной и той же среде работает много хостов, появляется большое количество коллизий и, соответственно, увеличивается число повторных передач пакетов. По этим причинам эффективность полудуплексной сети сильно зависит от количества хостов и генерируемого ими сетевого трафика.

В полудуплексной кабельной сети использовался общий концентратор. В полнодуплексной кабельной сети у вас имеется коммутируемая среда. Utah-WISP имела эквивалент гигантского концентратора с включенными в него более чем двумя сотнями пользователей.

Проблема оказалась еще сложнее. Каналы беспроводной сети проходили через перегруженные, ненадежные и иногда пересекающиеся спектры частот. Фреймы, передаваемые через радиосеть, терялись и требовали повторной ретрансляции. Частые повторные передачи вызывали заметные задержки в передаче TCP/IP-пакетов и перегрузку в сети. Стандарт TCP/IP рассчитан на потери пакетов при перегрузке сети, но не на потерю пакетов от разрыва соединений. Когда пакет теряется, для протокола это означает, что сеть перегружена и занята. Соответственно, он реагирует дроблением окна передачи перед повторной передачей пакетов. Запускается таймер ретрансляции, замедляющий передачу, компенсируя тем самым с точки зрения протокола нагрузку на сеть. В результате снижается загрузка сети и производительность.

Более того, когда радиосигнал слабый, производительность страдает еще сильнее. «Некоторые поставщики продавали нам оборудование, находившееся в опытной эксплуатации, — пояснил Дейл. — Наложение спектров в нашей сети значительно больше, чем в других региональных городских радиосетях». Эти перекрывающиеся спектры в сочетании с унаследованными и устаревшими технологиями были основной проблемой, затмевающей все остальные. Некоторые из этих проблем можно было гарантированно решить, но для этого требовалось устранить любой нежелательный трафик.

Реализация проекта в три этапа

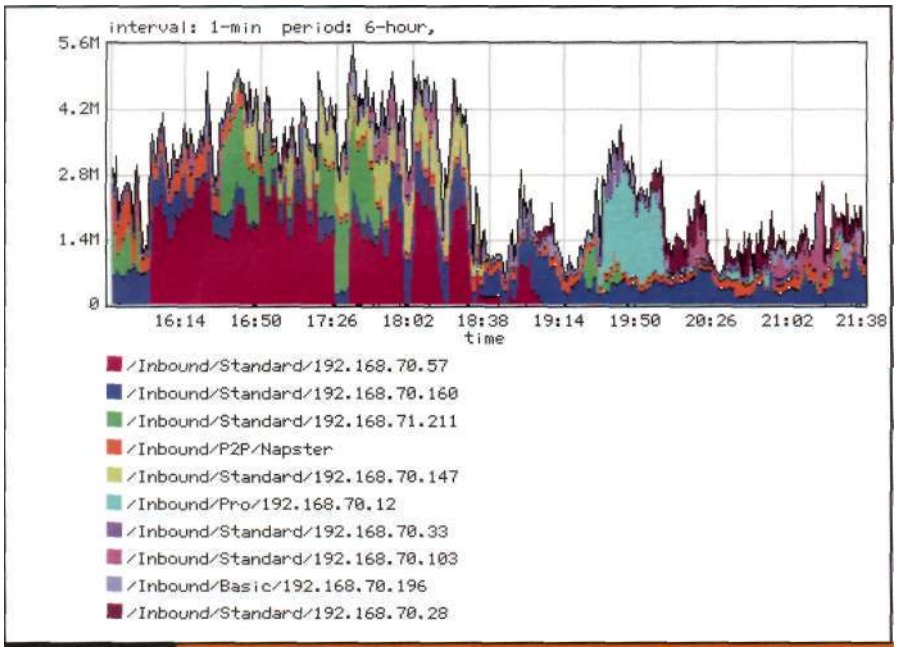
Проверяя настройки маршрутизатора, я обнаружил, что он довольно сильно перегружен. У меня возникло предположение, что это не только из-за количества посланных через сеть байтов, но и из-за количества переданных пакетов. Я решил, что необходимо приложить усилия к снижению количества пакетов в сети путем снижения широковещательного трафика, защиты сети от трафика, вызванного вредоносным программным обеспечением, и организации управления сетевыми ресурсами.

Снижение широковещательного трафика. Возможно, проще всего было снизить широковещательный трафик. Компьютеры используют широковещательные сообщения для обнаружения других систем в сети и оповещают о своем присутствии в этой сети. Широковещательный пакет проходит через всю сеть. Допустим, в сети Utah-WISP одна из клиентских систем посылает подобный пакет на башню, которая передает его всем остальным клиентам в зоне обслуживания. Затем пакет посылается обратно в главный офис, который вновь пересылает его на другую башню, а та передает этот пакет всем клиентам своей зоны обслуживания. Так каждый широковещательный пакет попадает на каждую из систем сети.

Чтобы решить эту проблему, мы быстро перестроили структуру подсетей и настроили маршрутизаторы для снижения уровня широковещательного графика. По сути, мы разорвали сеть и разместили системы в небольших сегментах так, чтобы широковещательный трафик не ходил по всей сети. Чтобы в будущем снизить широковещательный трафик через сеть, мы активизировали на коммутаторах функции кэширования протокола ARP Address Resolution Protocol и управление ARP-протоколами. Это действие не принесло особенной пользы, но повышение производительности было заметно на операциях загрузки файлов по беспроводной сети, скорость которой немного возросла.

Обеспечение безопасности сети. Работая с провайдером WISP, я не имел возможности управлять клиентскими системами и не мог установить обновления и персональные брандмауэры. Также нельзя было наложить слишком много ограничений на различные типы трафика с целью его блокировки. Хотя пользователям разослали по почте сообщения с рекомендациями по улучшению защиты систем, я знал, что кто-то проигнорирует эти советы, а кто-то не имеет достаточного опыта и знаний для того, чтобы ими воспользоваться.

К счастью, провайдер имел четко определенную политику использования сети, описанную в контрактах на подключение. Политика запрещала запуск в сети серверов и работу в одноранговых сетях P2P с использованием разделяемых локальных ресурсов. Поэтому UtahWISP начала блокировать соответствующий трафик,



Экран 3 Снижение сетевого трафика, показанное PacketShaper

такой как входящий Web и почтовый трафик. Таким образом компания значительно снизила уязвимость сети от некоторых клиентов, которые по незнанию открывали лазейки спамерам и взломщикам.

В процессе обновления сети система обнаружения вторжений, Intrusion Detection System (IDS), сообщила, что некоторые из клиентских систем часто сканировали другие системы сети. Но ведь клиентским системам не было никакого смысла подключаться к другим системам. Я принял эту активность за наиболее общий признак заражения систем червями. Одним из привычных средств распространения подобных вредоносных программ является электронная почта. Таким образом, если бы UtahWISP удалось предотвратить проникновение вирусов и червей в сеть через почту, шансы пользователей подцепить подобные вредоносные программы вместе с почтовыми сообщениями устремились бы к нулю.

Черви оказывали влияние на две системы электронной почты: Microsoft Exchange Server 2003 и NetIQ MailMarshal SMTP. Переход на Exchange 2003 является более надежным и хорошо защищенным решением. Для продуктов, используемых в UtahWISP, очень важна полная интеграция с Windows Server, позволяющая создавать для каждого клиента одну учетную запись, которая будет использоваться им при работе с Web, дисковыми хранилищами и электронной почтой. Другими важными характеристиками являются надежность, производительность и масштабируемость. Одним из наиболее важных требований к продуктам в UtahWTSP была возможность обеспечения доступа к почте через Web с помощью Outlook Web Access (OWA). После того как мы разобрались с Exchange, я приступил к настройке и установке продукта компании NetIQ MailMarshal. Это продукт, обеспечивающий безопасность и интегрируемый напрямую с Exchange. Его можно использовать в качестве самостоятельного SMTP-шлюза. Я выбрал вариант SMTP-версии, поскольку хотел, чтобы шлюз работал отдельно от сервера Exchange, а UtahWISP не имела особой нужды в их интеграции, хотя MailMarshal наиболее уместен в корпоративной среде, где политики управления более закрытые и сильные. Я настроил продукт более консервативно по сравнению с другими провайдерами WISP и заблокировал только те сообщения, которые явно содержали вирусы. Практически сразу после установки я зафиксировал почти 30-процентное снижение объема почты, обрабатываемой сервером Exchange. Каждое сообщение, содержащее спам, не проходило через шлюз и каждый заблокированный вирус снижал общий уровень загрузки сети.

Таким образом, я успешно ограничил появление множества ненужных пакетов в сети. Но хотя разница была заметная, этого оказалось недостаточно. Посмотрев на карту, созданную NetCrunch, я все еще наблюдал в сети задержки запросов ping.

Управление сетевыми ресурсами. Следующим шагом было управление реальным трафиком, проходящим через сеть. Вместо установки брандмауэра и полной блокировки некоторых типов трафика я выбрал управление этим трафиком. Для этой цели я воспользовался продуктом компании Packeteer PacketShaper 6500. Монитор сетевого трафика позволил мне сформулировать правила, которые устанавливали высокие приоритеты для одного типа трафика и ограничивали скорость передачи пакетов других типов. Например, высший приоритет был предоставлен браузеру Web, а трафик одноранговых сетей P2P был ограничен скоростью, сопоставимой со скоростью модемного соединения. Более того, клиенты получили от UtahWISP тарифные планы, зависящие от необходимой им полосы пропускания. Ранее компания реализовывала эти ограничения на основе соответствующих настроек точек доступа, теперь же с помощью PacketShaper UtahWISP получила возможность более гибкого управления полосой пропускания каждого пользователя. Появилась возможность создания отчетов об актуальном использовании полосы пропускания.

Я позволил устройству PacketShaper собрать статистику за несколько часов и затем просмотрел некоторые графики. Я знал, что трафик одноранговых сетей P2P у UtahWISP велик, но у меня не было возможности оценить его объем до тех пор, пока я не посмотрел на эти графики. В действительности полоса пропускания, используемая P2P-трафиком, была так велика, что на диаграмме она перекрывала все остальные типы тра-

фика. Более того, я был удивлен, увидев, что основную часть этой полосы занимают всего несколько пользователей. Некоторые пользователи имели пять и более одновременно запущенных P2P-приложений. Наличие общей оценки сети оказалось очень полезным для определения того, в каком направлении двигаться дальше. Я установил ограничения на весь P2P-трафик и предоставил таким протоколам, как HTTP и DNS, высокий приоритет в сети. Наконец, я распределил всех клиентов по отдельным классам обслуживания на основе тарифных планов, которые они приобрели.

После установки всех правил я включил монитор пакетов и сразу же увидел значительное снижение сетевого трафика, как показано на экране 3. Теперь, когда P2P-трафик был ограничен, я смог идентифицировать другие сетевые проблемы, покрывавшиеся ранее трафиком одноранговых сетей. Например, я заметил, что один из клиентов генерировал необычайно большое количество исходящих сообщений электронной почты. Значит, либо он является спамером, либо, что более вероятно, его станция поражена вирусом. Представители службы технической поддержки UtahWISP связались с клиентом и помогли решить проблему.

DMZ и серверное оборудование

Хотя исходная проблема была ликвидирована, я решил пойти на шаг дальше и проверить демилитаризованную зону DMZ UtahWISP. DMZ - это специальный сетевой сегмент, изолированный как от Internet, так и от внутренней сети. Оказалось, что в компании DMZ отсутствовала вообще. Вместо этого все критически важные серверы и офисные компьютеры находились в одной сети с клиентскими компьютерами. Если бы серверы Utah-WISP удалось взломать, они превратились бы в площадку для запуска других атак внутри сети. Для построения DMZ я воспользовался системой компании Network Engines NS6300 ISA Server.

Система Network Engines представляет собой сервер с установленной операционной системой Windows Server 2003 и ISA Server 2004, предварительно соответствующим образом настроенный и готовый к проведению базовой настройки. Вскоре я получил полнофункциональную DMZ, изолированную от остальной сети. Для начала я создал отдельную сеть для офисных компьютеров. Поскольку устройство имеет на передней панели шесть сетевых портов, один из них я выделил для внешнего соединения, другой для управления устройством и еще четыре — для создания изолированных сегментов сети. Сейчас серверы UtahWISP размещены в DMZ и защищены брандмауэром. Затем я проверил сами серверы. Их аппаратная часть соответствовала задачам компании, но я знал, что производительность Web-сервера значительно улучшится, если расширить имеющуюся оперативную память с 256 Мбайт до 4 Гбайт. Поэтому я установил восемь модулей памяти по 512 Мбайт, изготовленных компанией Micron Technologies для модернизации самого важного сервера. Хотя я и не выполнил официальных тестов производительности до и после модернизации, после увеличения оперативной памяти скорость явно возросла.

Серверная стойка

Моей главной целью была полная модернизация сети, поэтому я осмотрел стойки с серверами UtahWISP. Возле каждой стойки я обнаружил множество мониторов, клавиатур и мышей, предназначавшихся для управления различными серверами. Проходя различные этапы модернизации, я часто хватал не ту мышь или набирал что-то не на той клавиатуре. Кроме того, управлять несколькими серверами во время настройки было неудобно.

Решить проблему помог 16-портовый переключатель клавиатуры и мониторов с пятиметровыми кабелями OmniView компании Belkin. В этом переключателе кабели мыши, клавиатуры и видео, идущие от двух серверов, комбинируются в единый кабель. Такая конструкция позволила мне без труда объединить все серверы компании в один переключатель клавиатуры и управлять ими с одного стола, расположенного неподалеку от серверов.

В компании Belkin был закуплен стоечный источник бесперебойного питания mni-Guard 3200VA, позволивший заменить четыре старых источника бесперебойного питания, использовавшихся до модернизации. Этот источник обеспечивал ту же мощность, что и старые системы, но места при этом занимал вчетверо меньше. Сетевые кабели различных цветов помогли мне без труда различать сегменты сети.

Финальный аккорд

После недели работы сети в UtahWISP было проведено совещание для подведения итогов и обзора сделанных изменений. Администратор сети сообщил, что скорость работы сети увеличилась как минимум на 50 процентов, а клиенты, имевшие наибольшее количество проблем, отметили значительный рост производительности. Кроме того, когда добавились новые компоненты, администратор сети получил дополнительные возможности для отслеживания специфичных проблем. Таким образом, реконструкция сети была закончена и клиенты остались довольны.

Программы антишпионажа для предприятия

Сравниваем три *продукта для* поиска шпионских *программ на предприятии*

Джеф Феллинг

Директор по информационной безопасности компании Quantive. Автор книги IT Administrator's Top 10 Introductory Scripts for Windows (издательство Charles River Media). jeff@blackstatic.com

Шпионское программное обеспечение представляет собой растущую угрозу для предприятия. С помощью шпионских программ посторонние лица могут узнать важную информацию о компании и ее клиентах. Шпионские программы не только снижают скорость работы компьютера, но и пересылают конфиденциальную информацию злоумышленникам без ведома жертвы. Вирусы и черви заражают и портят единственный файл, и обнаружить и удалить их сравнительно просто, тогда как «шпионы» гораздо более коварны и часто устанавливают свои компоненты незаметно для владельца компьютера. Авторы шпионских программ искусно маскируют их, например под безобидные вспомогательные панели для Microsoft Outlook, которые позволяют добавлять выразительные пиктограммы, а в фоновом режиме отслеживают сообщения электронной почты. «Шпионы» собирают самые разные сведения, от содержимого файлов в компьютере до контактной информации электронной почты и адресов посещаемых пользователем Web-узлов. Шпионские программы могут даже регистрировать нажатия на клавиши, делать снимки экрана, перенаправлять браузер на нежелательные сайты или нарушать работоспособность компьютера.

Многие поставщики программ безопасности выпускают средства для поиска и удаления шпионского программного обеспечения. В данной статье сравниваются три автономных продукта для борьбы со шпионажем на предприятии. Речь пойдет о характеристиках, которые следует учитывать при выборе продукта. Во врезке «Недостатки пакетов» рассказано о типичных недостатках, свойственных решениям, в которых объединены комплексные и автономные программы.

Недостатки комбинированных пакетов

В основной статье рассмотрены три автономных продукта для борьбы со шпионажем, ориентированные на средние и крупные предприятия. Многие другие поставщики объединяют программы антишпионажа в одном продукте с другими компонентами. Например, помимо функций обнаружения шпионских программ, в состав LANDesk Security Suite входят инструменты для блокирования попыток соединений с сетью с незащищенных компьютеров, средства поиска уязвимых мест и анализа и мощные функции управления исправлениями. В исчерпывающем комплексе F-Secure Anti-Virus Client Security вместе с программой антишпионажа реализован клиентский брандмауэр, антивирусная программа и компоненты для обнаружения несанкционированного доступа.

Однако общий недостаток комбинированных пакетов — невозможность выборочного использования компонентов пакета. Например, если ранее было развернуто автономное антивирусное решение от одного поставщика, то нельзя использовать только функции антишпионажа встроенного клиента антивирусной/шпионской защиты из пакета другого поставщика, не удалив предварительно существующий антивирусный продукт.

Тестирование продуктов

Продукты, представленные в данном обзоре, обнаруживают и удаляют только шпионское программное обеспечение, но не вирусы, поэтому для работы с любым из этих продуктов приходится приобретать определенный антивирусный пакет. Из автономных инструментов можно собрать более надежный пакет, нежели интегрированное решение, так как они ориентированы исключительно на поиск «шпионов», а не на решение нескольких задач. Некоторые поставщики антивирусных программ утверждают, что с помощью их антивирусных алгоритмов можно обнаружить некоторые варианты программ-шпионов, но, по моим наблюдениям, они уступают автономным продуктам.

Эффективность средств для борьбы со шпионскими программами зависит от функциональных возможностей механизма обнаружения, а также аккуратности и своевременности обновлений — не только для поиска новых «шпионов», но и для исключения ложных положительных срабатываний, свойственных предшествующим версиям. В продукте должна быть предусмотрена возможность автоматической загрузки новых сигнатур по расписанию. Большинство компаний, в том числе те, чьи продукты представлены в данном обзоре, предоставляют новые сигнатуры через службу подписки с ежегодной платой за обслуживание.

В статье рассмотрены Counter-Spy Enterprise компании Sunbelt Software, Trend Micro Anti-Spyware Enterprise Edition и Webroot Spy Sweeper Enterprise. Продукты, предназначенные для средних и крупных предприятий с числом рабочих мест не менее 50, располагают такими функциями,

Таблица **Сравнительные характеристики**

	Sunbelt Software CounterSpy Enterprise	**Trend Micro Anti-Spyware Enterprise Edition**	**Webroot Spy Sweeper Enterprise**
Серверная платформа	Windows Server 2003, Windows XP Professional Edition, Windows 2000 Server Service Pack 2 (SP2) или более поздняя версия, Windows 2000 Professional SP2 или более поздняя версия	Windows **2003,** Windows **2000** или Windows 2000 Advanced Server SP4	Windows 2003, XP, Windows 2000
Клиентская платформа	Windows 2003, XP Pro, Windows XP Home Edition, Windows 2000 Server SP2 или более поздняя версия, Windows 2000 Pro SP2 или более поздняя версия, Windows NT Server 4.0 SP6 или более поздняя версия, Windows 98 Second Edition (Win98SE), Windows Me	Windows 2003, XP, Windows 2000 Server или Windows 2000 Pro	Windows 2003, XP, Windows 2000, NT Server 4.0, Windows Me, Win98SE
Административная консоль	Приложение Win32	IIS или Web-страница на базе Apache	Web-сервер через IE 6.0 или более позднюю версию
База данных анализа угрозы	Sunbelt Spyware Research Team, ThreatNet Community; исследовательская группа антишпионажа Microsoft	TrendLabs	Webroot Threat Research Team с использованием автоматизированных элементов Phileas
Совместимость с базами данных	Microsoft SQL Server, Microsoft Access	MySQL	SQL Server, DBISAM компании Elevate Software
Функции клиента	Сканирование, сброс данных, удаление, подготовка отчетов	Клиент скрытый	Локальная настройка большинства параметров сканирования
Защита в реальном времени	Active Protection Monitoring обеспечивает отслеживание 35 параметров Windows, сети и Microsoft Internet Explorer (IE)	С помощью Active Application Monitoring можно разрешить, запретить или сделать запрос о подозрительных выполняемых файлах	Элементы Smart Shields отслеживают Windows, IE, безопасность начальной загрузки, рекламные сайты, файл HOSTS и параметры установки шпионских программ
Методы развертывания клиентов	Windows Installer (.msi), .exe, «передача/загрузка» с использованием имени компьютера, IP-адреса, просмотра сети, AD	.msi, автоматическое доменное «проталкивание»	.msi, .exe, NetBIOS
Действия в отношении шпионских программ	Игнорировать, только отчет, карантин, удалить	Сканировать, очистить, восстановить	Только протоколировать, карантин, удалить
Централизованные, специализированные и плановые проверки в реальном времени	Да	Да	"
Отчеты	Семь встроенных отчетов Crystal Report, экспортируемых в .pdf-файл, Excel, Word	Пять отчетов о текущих и удаленных угрозах, журнал событий	Девять руководителей, отчеты о шпионских программах, обновление отчетов, в том числе сводки для информации о состоянии; совместимость с форматом PDF
Внешние предупреждения	Предупреждения по электронной почте	Отсутствуют в протестированной версии	Предупреждения по электронной почте

как централизованная настройка конфигурации, дистанционное развертывание и управление клиентами, подготовка отчетов и рассылка предупреждений. Сравнительные сведения о важнейших характеристиках продуктов приведены в таблице .

Для данного обзора я сравнивал удобство эксплуатации и эффективность поиска и удаления шпионских программ. В ходе тестирования проводилось развертывание агентов, сканирование удаленных клиентов и устранение всех обнаруженных угроз.

В качестве тестовой системы использовался компьютер Windows XP Service Pack 2 (SP2) со всеми исправлениями для системы безопасности. В систему были загружены разнообразные шпионские и рекламные программы, в том числе программы захвата модема (dialers), перенаправления браузера (hijackers) и системные шпионы, такие как регистраторы нажатий на клавиши (keyloggers). Для тестирования использовались шпионские программы abcsearch4u, панель инструментов 550Access, Track4Win, pinfo dialer, FindWhateverNow, CoolWeb search, Chat Blocker, Activity Monitor 2002, SpyBuddy, DialerClub и Mysearchpage.

Из централизованной консоли каждого продукта антишпионажа я сканировал зараженный клиентский компьютер, чтобы выяснить, насколько успешно продукт обнаруживает и удаляет вредителей. Затем я перезагружал зараженную систему и использовал тот же продукт для повторного сканирования.

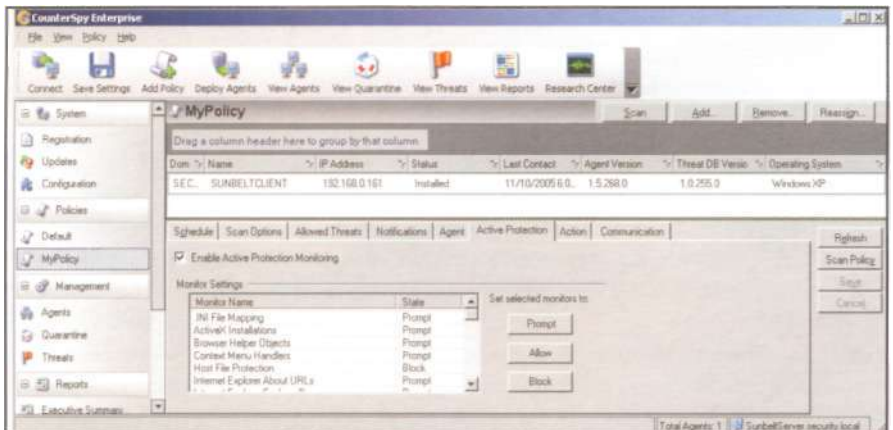
Все три продукта блокировали все шпионские программы на тестовой системе. Spy Sweeper обнаружил и незаметно удалил все опасные программы. После перезагрузки функция защиты в реальном времени продукта CounterSpy разукрасила консоль как рождественскую елку, предотвращая множество попыток повторного заражения. Инструмент Trend Micro предложил перезапустить клиентский компьютер, чтобы полностью очистить его; в сообщении содержалось указание на возможность очистки блокированных файлов. Только продукт Trend Micro выдал приглашение выполнить перезагрузку, но для полной очистки системы любым продуктом потребовалось перезагружаться несколько раз.

CounterSpy Enterprise

CounterSpy Enterprise компании Sunbelt Software обеспечивает централизованный поиск шпионских программ и защиту в реальном времени при невысокой цене. Для доступа из главного экрана к любой функции для управления агентами, политиками, карантином и отчетами достаточно несколько раз щелкнуть мышью. Консоль на базе Win32 проста в использовании, но, похоже, ориентирована на управление небольшим числом клиентов и лишена некоторых функций, полезных для корпоративного продукта. Например, только один пользователь может одновременно обращаться к консоли через Terminal Services. Если подключить две консоли к одному серверу, то изменения, выполненные из одной консоли, не отражаются в другой.

Для управления удаленным агентом используются настраиваемые политики. Можно составить одну или несколько политик и назначить им различных агентов в соответствии с потребностями компании. Например, можно чаще проверять интенсивно используемые рабочие станции и назначить «быструю» политику сканирования, которая не снижает производительности серверов. Удобная функция — возможность выбирать между двумя типами сканирования, «быстрым» (quick) и «глубоким» (deep). Параметры сканирования любого типа можно настраивать, например задавать глубину просмотра папок, проверку процессов, поиск следящих файлов-маяков и следов шпионского программного обеспечения в реестре.

CounterSpy обнаруживает множество угроз и группирует их по 40 категориям, таким как рекламное программное обеспечение, программы обмана браузера, захвата модема и регистраторы нажатий на клавиши. База данных опасных программ доступна с административной консоли, что позволяет быстро анализировать угрозы. В консоли приведена ссылка на исследовательскую лабораторию CounterSpy, откуда можно получить подробные сведения о типе угрозы, описание и советы по защите. Помимо собственной группы специалистов и общественной сети оповещения о шпионах, компания Sunbelt использует сигнатуры «шпионов» из программы Microsoft Windows



Экран 1 Окно ActiveProtection в CounterSpy

CounterSpy Enterprise 1.5

Достоинства: простые процедуры настройки и сканирования за счет графического интерфейса; благодаря совместимости с AD упрощается составление списков клиентов; простая процедура установки клиентов.

Недостатки: из-за отсутствия панели управления затрудняется общий анализ после сеанса сканирования; суммирование в отчетах сведений об угрозах, полученных в разных сеансах сканирования, может ввести в заблуждение; неудобные процедуры управления карантином.

Оценка: 3,5 из **5.**

Цена: 1800 долл. для 100 рабочих мест; 11 тыс. долл. для 1000 рабочих мест.

Рекомендации: удачный выбор для предприятий, ограниченных в средствах.

Контактная информация: Sunbelt Software http://www.sunbeltsoftware.com.

Defender (в прошлом Microsoft Windows AntiSpyware beta). В политиках можно указать белый список приемлемых, не таящих серьезной опасности программ, которые могут быть даже полезны, например рекламные файлы-маяки для доставки целевой рекламы. Выдающийся компонент пользовательского интерфейса CounterSpy — функции сортировки и группировки данных, особенно полезные при просмотре больших объемов данных, например списка угроз. В этом случае возможность разбить информацию на категории действительно упрощает задачу.

Как и для других продуктов в данном обзоре, для CounterSpy необходимо развернуть агентов на каждом клиентском компьютере. Компьютеры для мониторинга можно выбрать с помощью Active Directory (AD), путем просмотра сети или указав имена либо IP-адреса систем, а затем установить программу с использованием автоматизированной процедуры «передачи и загрузки». Иначе можно распространять агентов вручную или с применением Group Policy, сценариев регистрации либо продукта развертывания пакетов от независимого поставщика.

Пользователям можно разрешить запускать сеансы проверки, записывать данные в локальные журналы, спрятать или поместить на панель инструментов пиктограмму агента, установить частоту обновления программы и сигнатур шпионских программ. После установки на экран выводится минимальный пользовательский интерфейс агента. Если пиктограмма на панели задач активизирована, можно определить, выполняется ли в данный момент проверка. Щелчком правой кнопки можно запустить сеанс проверки и отменить изменения, внесенные в компонент Active Protection.

Active Protection — компонент мониторинга почти в реальном времени, который состоит из многих централизованно активизируемых мониторов (экран 1). Благодаря этим мониторам конечный пользователь может выполнять рискованные операции, например установить элементы управления ActiveX и вспомогательные модули браузера либо редактировать HOSTS-файл. В отличие от подробных сведений в базе данных «шпионов», в продукте не описано назначение каждого монитора, и пользователю приходится обращаться за дополнительной информацией к документации.

По умолчанию каждая политика просто сообщает о шпионских программах, что позволяет увидеть обнаруженные продуктом угрозы. После нескольких сеансов сканирования пользователь может пожелать повысить уровень защиты до Quarantine или Delete. В режиме Quarantine потенциальные угрозы помещаются в специальный репозитарий, из которого их можно извлечь позже, когда выяснится, что они не представляют опасности. В CounterSpy можно назначить различные действия для каждой категории «шпионов». Например, можно удалить рекламные программы и регистраторы нажатий на клавиши, но отправить в карантин модули расширения для браузера. Однако управлять шпионскими программами в карантине неудобно, поэтому для такой категории, как файлы-маяки, которые генерируют множество угроз, лучше обойти карантин и использовать режим Delete.

В CounterSpy Enterprise имеется семь шаблонов отчетов, которые можно настраивать по дате. Интерпретировать данные следует особенно внимательно, так как в отчетах, похоже, представлено несколько случаев отдельных угроз, обнаруженных за один период времени. Рассмотрим эту особенность программы подробнее. Если проверить компьютер 10 раз и в каждом сеансе будет обнаружена одна и та же угроза, то в отчете будет представлено 10 экземпляров программы-шпиона. Одна угроза должна учитываться только один раз. Для генерации отчетов используется механизм Crystal Reports с дополнительными функциями, в том числе повышенной детализацией. Можно экспортировать отчеты в формат файла Adobe PDF, электронной таблицы Microsoft Excel или в документ Microsoft Office Word.

В CounterSpy не хватает такого компонента, как динамическая панель управления, в которой отображается «шпионская» картина сети. Динамическая панель управления позволяет действовать напрямую и даже отменять параметры политики — например, отправить в карантин обнаруженную угрозу или удалить вредителя, направленного в карантин во время предыдущего сеанса. В некоторых случаях можно выделить несколько элементов, например при очистке карантина. В малых сетях такие недостатки не доставляют ощутимых неприятностей, но на крупном предприятии масштаб проблемы резко возрастает.

Trend Micro Anti-Spyware Enterprise Edition 3.0.

Системные администраторы почувствуют себя в знакомой обстановке, управляя инфраструктурой Trend Micro Anti-Spyware Enterprise Edition (ASEE), в которой в качестве внешнего прикладного сервера используется Microsoft IIS или серверная Web-служба Apache, а в качестве внутренней базы данных — MySQL. Благодаря их использованию упрощается интеграция продукта в сетях круп-

ных компаний, уже знакомых с этими технологиями.

Сотрудники малых офисов и дотошные администраторы могут предпочесть детализированные функции других продуктов, зато ASEE понравится администраторам, нуждающимся в продукте, о котором после установки можно забыть. ASEE — автономный продукт, но он совместим с корпоративной инфраструктурой Control Manager компании Trend Micro. Недостаток ASEE заключается в том, что некоторые функции, такие как уведомление об опасности, предоставляются только через инфраструктуру Control Manager.

Процедура установки занимает всего несколько минут, после чего можно приступать к созданию политик, управлять клиентами, запускать сеансы сканирования. Все эти операции выполняются из браузера. Благодаря использованию браузера административную консоль можно запустить из любого места сети, но Web-окно управления ASEE кажется устаревшим по сравнению с графическим интерфейсом других продуктов в данном обзоре. Например, при каждом щелчке на элементе браузер обновляется и навигация замедляется. К сожалению, нельзя открыть контекстное меню щелчком правой кнопки и переносить элементы с помощью мыши.

Поведение клиентской системы определяется политиками, назначаемыми администратором. Можно указать способы установки и обновления клиента, определить тип и время запуска сканирования, задать режим автоматического удаления угроз. В ASEE можно определить один тип сканирования для каждой политики — «быстрый» или «полный» — и составить расписание сеансов проверки (один раз или повторно в течение недели, а также при начальной загрузке). Процедуру проверки можно запустить вручную в любой момент и устранять угрозы, щелкая кнопкой мыши. После сканирования можно составить белый список программ, которые не следует удалять.

На вкладке My Enterprise Network в административной консоли представлен фильтруемый список серверов, защищенных ASEE, и общая информация о состоянии сети, в том числе о клиентах и угрозах. После завершения сканирования на этой вкладке красным цветом отображается число обнаруженных «шпионов». Получить более подробную информацию о них не составляет труда.

По щелчку на кнопке Clean All Threats программа ASEE передает клиентам команду ликвидировать угрозу в соответствии с указанными в политике параметрами. В частности, можно исключить из рассмотрения указанное шпионское программное обеспечение либо провести полный или быстрый поиск. Если по ошибке был удален объект, который в действительности был нужным файлом-маяком или приложением, операцию удаления можно отменить, восстановив систему в состояние, соответствующее контрольной точке. При восстановлении список конкретных компонентов удаленного шпионского программного обеспечения не приводится, хотя имеется перечень сеансов сканирования, но по нему тоже сложно судить о программах, удаленных в каждом сеансе.

Экран 2 Отчет Cleaned Chart программы Trend Micro

Trend Micro Anti-Spyware Enterprise Edition 3.0

Достоинства: после настройки можно запустить продукт, не затрачивая более усилий на его обслуживание; компактная консоль на базе браузера доступна из любого узла сети.

Недостатки: отсутствие обратной связи на клиентском уровне о событиях, происходящих в фоновом режиме; мало клиентских параметров, настраиваемых с сервера; недостаточно развитый графический интерфейс на базе Web.

Оценка: 4 из **5.**

Цена: 1645 долл. для 100 компьютеров; 9450 долл. для 1000 рабочих мест.

Рекомендации: продукт для предприятий, нуждающихся в надежном механизме обнаружения и удаления без подробных отчетов или детальных параметров настройки клиентов.

Контактная информация: Trend Micro, http://www.trendmicro.com.

Механизм Trend Micro для защиты в реальном времени называется Venus Spy Trap (VSP). VSP предотвращает установку и запуск шпионских программ. VSP можно централизованно настроить на разрешение или блокирование запуска исполняемых файлов, сигнатура которых соответствует известным «шпионам», либо предоставить решение пользователю, но этим возможности настройки и ограничиваются. Размеры клиентской программы невелики, и для конечного пользователя она невидима. Единственное свидетельство о работе клиентской программы — процесс в Task Manager и журнал активности в папке Trend Micro. Все задачи по управлению, такие как запуск сеансов сканирования, должны выполняться из административной консоли. При очистке клиентского компьютера иногда требуется перезапустить систему, если это необходимо для удаления «шпиона». Другие продукты в данном обзоре не предлагают перезапустить компьютер, даже если это нужно для полного удаления шпионской программы.

Отчеты ASEE минимальны: в четырех отчетах на базе Java показаны диаграммы текущих угроз, список обнаруженных опасностей, удаленные вредители и список имеющихся доменов. На экране 2 показан отчет об удаленных «шпионах». Отчеты содержат данные о «шпионах», найденных в ходе последнего сеанса сканирования, и напоминают панель управления, но без функции детализации. Интерфейс отчетов ASEE обеспечивает доступ к журналу событий, в котором собраны результаты сканирования и история событий для каждого клиента. Благодаря кнопке Power Search упрощается фильтрация обширного списка событий.

Очень удачна функция автоматической установки, которая регулярно опрашивает контроллер домена (DC) о новых компьютерах и автоматически пересылает программу-клиента на новые системы. В результате администратору не приходится прибегать к другим методам установки. С помощью административной консоли ASEE можно также просмотреть домен, добавить клиентов в базу данных, а затем развернуть клиентов. Однако ASEE не создает специализированных пакетов развертывания для ручных и сценарных операций. Вместо этого необходимо настроить типовой пакет установки с использованием параметров сервера, таких как IP-адрес сервера ASEE, и управлять каждой лицензией отдельно. В результате дистанционное развертывание на автономных рабочих станциях оказывается сложнее, чем в других продуктах данного обзора.

Webroot Spy Sweeper Enterprise

Webroot Spy Sweeper Enterprise компании Webroot Software располагает разнообразными достоинствами: панелью управления для быстрого доступа к информации о шпионских программах на предприятии; сканированием по расписанию; автоматической защитой с использованием элементов Smart Shields; полнофункциональным, централизованно управляемым клиентом; инструментарием командной строки для расширения возможностей продукта с помощью сценариев.

Административная консоль функционирует как Web-служба, поэтому обращаться к ней можно с любого компьютера в сети, но ее внешний вид отличается от типичной Web-страницы. Красивый интерфейс хорошо организован. Одного взгляда на панель управления достаточно, чтобы увидеть проигнорированные сеансы сканирования (sweep, по терминологии Spy Sweeper); устаревшие определения; текущие заражения и список основных «шпионов» в сети предприятия. К большому сожалению, нельзя получить более детальную информа-

Webroot Spy Sweeper Enterprise 2.5.1

Достоинства: полнофункциональный пользовательский интерфейс; благодаря инструментарию командной строки действие продукта распространяется за рамки консоли.

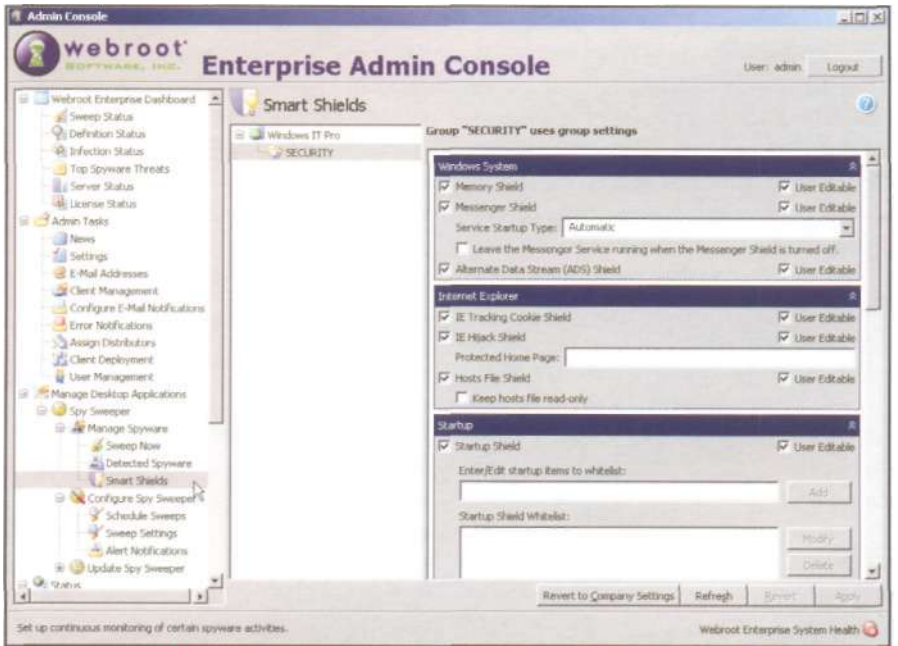
Недостатки: высокая цена.

Оценка: 4,5 из 5.

Цена: 2077 долл. для 100 рабочих мест; 15 280 долл. для 1000 рабочих мест.

Рекомендации: данный продукт превосходит остальные благодаря широким возможностям настройки, мощным функциям сканирования и защите в реальном времени, а также гибким функциям удаления вредителей.

Контактная информация: Webroot Software, http://www.webroot.com



Экран 3 Панель навигации административной консоли Spy Sweeper

цию об этих показателях панели управления, но данные можно экспортировать в файл с разделением запятыми (CSV) для обработки в других программах. Пользовательский интерфейс навигационной панели напоминает показанную на экране 3 привычную для администраторов Microsoft Management Console (MMC). Административная консоль предоставляет различную информацию о выполняемых действиях. Так, во время сеансов сканирования и других операций Spy Sweeper выводит шкалу хода исполнения и счетчик элементов, и пользователь может получить точное представление о происходящем и времени завершения сеанса.

Процедура развертывания клиентов проста, но с административной консоли установить их можно только на компьютерах, доступных по NetBIOS. Клиентов можно развертывать с помощью Group Policy, непосредственно из общего раздела диска, либо вручную, запустив программу установки клиента на каждом компьютере с использованием сценария регистрации.

Spy Sweeper управляет различными клиентскими конфигурациями через членство в группах, организованных администратором. Для каждой группы можно назначить длительность содержания угроз различных категорий в карантине, внести полезные программы в белый список, запускать сеансы сканирования, настраивать параметры Smart Shield. По умолчанию файлы содержатся в карантине 30 дней, а затем автоматически удаляются. Такой режим обеспечивает страховку на случай, если Spy Sweeper удаляет нужный файл или параметр, и одновременно избавляет от необходимости удалять каждого вредителя вручную.

Большинство связанных с клиентом компонентов настраиваются централизованно из административной консоли, но можно предоставить конечным пользователям право изменить настройки. На уровне группы можно назначить расписание проверок и действия Spy Sweeper при начальной загрузке — например, следует ли повторить пропущенную проверку, перенести время начала сеанса на более поздний срок или сканировать только уязвимые для «шпионов» папки. Помимо проверок накопителей, папок, памяти и реестра, можно сделать Spy Sweeper невидимым, вывести пиктограмму в панели задач или всплывающее окно в ходе сеанса. Если программа видима, то полнофункциональный клиент показывает настройки локального экземпляра и даже позволяет изменить их «на ходу». Многие администраторы запрещают пользователям изменять конфигурацию, но Spy Sweeper предоставляет им, как и сотрудникам службы поддержки, возможность отменить это ограничение с помощью одного нажатия клавиши и пароля, введенного на клиенте. Благодаря такому мгновенному доступу упрощается и ускоряется диагностика локальных неисправностей.

Элементы Smart Shields обеспечивают защиту клиентов в реальном времени, препятствуя попыткам шпионских программ воздействовать на различные компоненты системы. Например, наряду с блокированием рекламных сайтов и установкой «шпионов», Spy Sweeper располагает элементами Smart Shields для защиты памяти, альтернативных потоков данных, HOSTS-файла и программ, запускаемых в ходе начальной загрузки. Конечные пользователи могут не подозревать о существовании Smart Shields, но если пользователь неосторожно попытается установить шпионскую программу, то элементы защиты скрыто остановят ее.

Spy Sweeper работает в замечательно организованном браузере. Например, можно переместить любой созданный объект с помощью мыши к другим объектам, чтобы передавать различные типы оповещений, ошибки пересылки, уведомления и информацию на один адрес электронной почты, а предупреждения о шпионской угрозе — на другой. Аналогично, щелкая правой кнопкой мыши на объектах, чтобы отобразить дополнительные меню, можно выбрать несколько объектов с помощью клавиши Shift или Ctrl. Spy Sweeper производит впечатление мощного приложения, даже при работе с удаленного компьютера только через браузер. Кроме того, все административные действия заносятся в журнал, который хранится в течение заданного периода времени, что упрощает аудит действий нескольких администраторов.

В Spy Sweeper имеется девять шаблонных отчетов, в том числе о тенденциях шпионажа, самых распространенных шпионах, статусе заражения, особенностях шпионских программ, зараженных системах и предыстории. Отчеты можно вывести на экран в виде диаграмм или записать в PDF-файлы. Кроме того, продукт располагает несколькими инструментами командной строки для обработки отчетов в командных файлах или плановых заданиях Windows.

Лучший из трех

Выбор автономного решения для борьбы со шпионским программным обеспечением, как правило, означает, что на настольных системах придется разместить еще одного клиента, но возможности автономных продуктов часто шире, чем интегрированных. На мой взгляд, лучшее из трех корпоративных решений для борьбы со шпионскими программами — Webroot Spy Sweeper Enterprise. Его выдающиеся достоинства — детализированные функции, защита в реальном времени, полный клиентский интерфейс, панель управления отчетами и внешний инструментарий командной строки.

Разбираясь с DNS

Понимание DNS *приходит с опытом*

Дуглас Тумбс
Редактор журнала Windows IT Pro.
help@toombs.us

Недавно в нашей сети стали возникать блуждающие ошибки разрешения имен DNS. Отлавливать спорадические ошибки разрешения имен — занятие неблагодарное, тем более что с неполадками в DNS я не сталкивался достаточно давно и мои навыки слегка «запылились». Я бы предпочел сразиться с дюжиной других проблем, чем с этой. О существовании службы DNS легко забыть, пока она не начнет давать сбой, — все просто работает, как должно, — Internet, почтовый клиент, почтовый сервер, контроллеры домена. Прошло несколько лет с тех пор, как мне в последний раз довелось устранять проблемы с DNS, так что я расценил возникшие ошибки как знак свыше: пора вспомнить полезные навыки.

Поскольку DNS является основой нормального функционирования среды AD, а также тем звеном, которое соединяет в цепочку все сети в Internet, умение точно обнаруживать источник неполадок в DNS и устранять причину ошибки имеет огромное значение для сопровождения корпоративной сети. Сначала мы рассмотрим особенности решения проблем DNS, не связанные с AD, а затем посмотрим, что привносит AD.

Разрешение имен

Вся иерархия DNS строится от корневого домена (root domain). Корневой домен поддерживается 13 главными отдельными серверами, работа которых обеспечивается коммерческими, правительственными и образовательными учреждениями. В предельном случае эти корневые серверы участвуют в процессе разрешения всех публичных имен в Internet. Когда сетевой компьютер обращается к хосту с именем download.beta.example.com, в первую очередь он должен получить IP-адрес этого хоста. Этот процесс может потребовать до 10 различных запросов DNS, начиная с первого, с которым компьютер обращается к серверу, настроенному как сервер DNS. Стандартный процесс разрешения имен изображен на рис. 1.

Как видно из рисунка, локальный сервер DNS для определения соответствующего IP-адреса использует рекурсивные запросы — один из двух видов запросов DNS (второй тип называется итеративным). Каждый публичный сервер DNS, на который попадает запрос, либо выдает конечный результат (выполняет разрешение имени), если ему известен ответ, либо отправляет на связанный с ним вышестоящий сервер DNS, пытаясь определить неизвестный адрес. Поскольку корневой сервер DNS ничего не знает о конечных индивидуальных хостах в Internet, каковым является компьютер beta.example.com, он сообщает, что ничего не знает о подобном адресе, но советует опросить сервер, обслуживающий домен .com. По мере того как рекурсивный процесс продолжается, разрешение имени может произойти на одном из этапов, и результатом запроса будет либо искомый IP-адрес, либо отказ.

Описанная процедура разрешения имен может ввести пользователя в заблуждение: можно подумать, что корневые серверы доменов — это гигантские суперкомпьютеры, которые к тому же часто ломаются из-за чрезмерной

нагрузки. В действительности же корневые серверы большой нагрузки не испытывают благодаря второму элементу процесса разрешения имен — кэшированию.

О кэшировании

Вернемся к изображенному на рис. 1 процессу разрешения имен, но на этот раз допустим, что локальный сервер DNS уже обращался к почтовому серверу для домена example.com, прежде чем обратиться к download.beta.example.com. В этом случае локальный сервер DNS уже обладает информацией о том, как находить ответственный за домен example.com сервер DNS (по крайней мере, он был таковым несколько минут назад). В этом случае можно обратиться непосредственно к серверу DNS домена example.com вместо того, чтобы вновь обращаться к серверу корневого домена. В этом случае шаги 2, 3, 4 и 5 в процессе разрешения имени окажутся необязательными, благодаря чему коммуникационный трафик снижается на 40%.

Кэширование выполняется на всех уровнях иерархической инфраструктуры DNS. Забегая вперед, скажу, что, если кто-нибудь еще в локальной сети обратится к тому же хосту download.beta.example.com, локальный сервер DNS сможет обработать запрос из локального кэша, поскольку нужный хост уже был недавно найден, и таким образом остаются только шаги 1 и 10 из схемы, приведенной на рис. 1. Это соответствует 80-процентному сокращению коммуникационного трафика.

Кэширование выполняют не только серверы DNS, но и клиенты, так что любая рабочая станция, которая недавно запрашивала разрешение имени хоста, будет некоторое время помнить его. Если приложение (Web-браузер, почтовый клиент) на хосте повторно запросит запись DNS, Windows будет использовать локальную копию вместо того, чтобы каждый раз направлять запрос DNS. Таким образом, коммуникационный трафик сокращается до нуля.

Эта иерархия кэширования, которая выполняется на каждом сервере и клиенте, вовлеченном в процесс разрешения имен DNS, поддерживает работоспособность DNS во всем Internet. Однако кэширование во время поиска и устранения неисправностей может и помешать.

Техника поиска и устранения ошибок

Понимание принципов взаимодействия и кэширования DNS позволит тратить меньше времени на поиск и устранение неисправностей. Давайте рассмотрим, как работает механизм разрешения имен DNS при попытке разрешения имени DNS в IP-адрес. Как показано на экране 2, в первую очередь выполняется проверка имени в локальном кэше, и, если искомый адрес уже известен, он сразу возвращается, и никакого сетевого трафика не генерируется, в противном случае выполняется стандартная процедура разрешения имен. Это кажется очевидным, но все же следует знать, что именно происходит в кэше.

В кэше хранятся два основных типа записей — те, которые были найдены в результате запросов к серверу DNS, и те, что были предварительно загружены из файла \%systemroot%\ system32\drivers\etc\hosts. Записи пер-

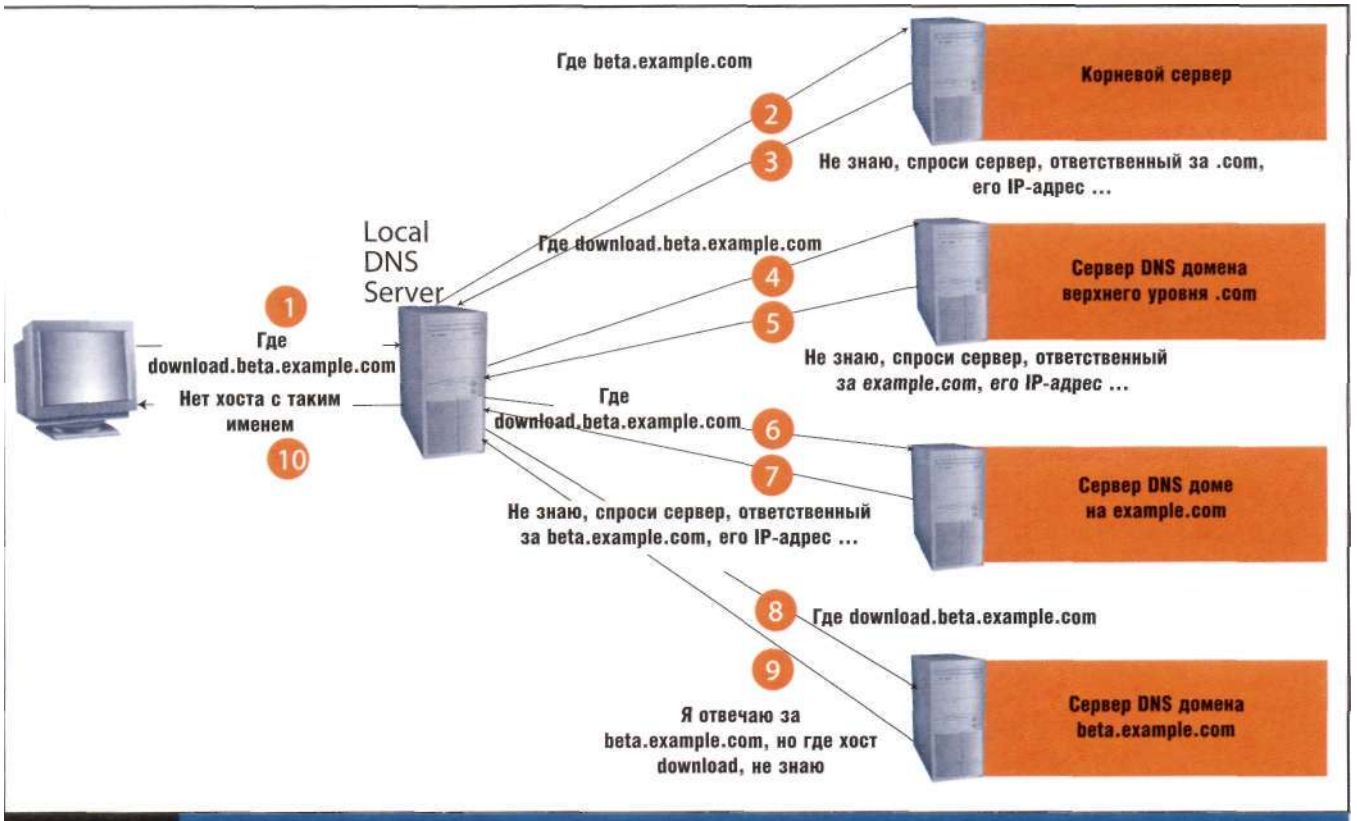
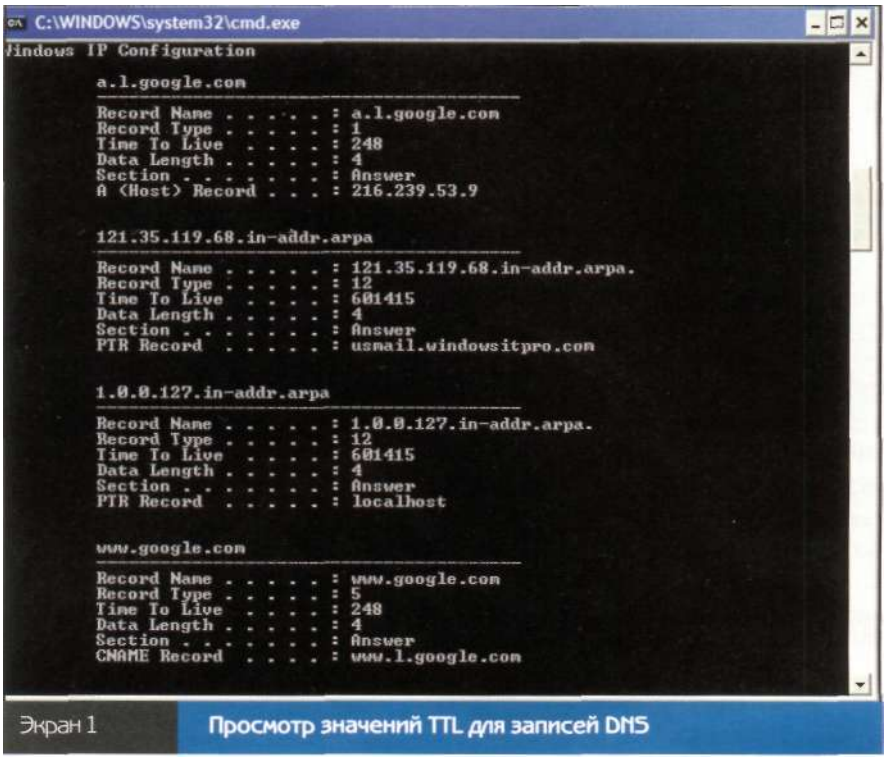


Рисунок 1 Стандартное разрешение имен DNS

вого типа устаревают по истечении определенного интервала времени TTL (Time To Live), который задается в полученном от сервера DNS ответе. Для просмотра содержимого кэша и определения оставшегося времени можно запустить из командной строки команду ipconfig /displaydns. В качестве примера я запустил поисковый запрос на www.google.com, а затем выполнил проверку ipconfig /displaydns. Как показано на экране 1, запись имеет значение TTL, равное 248 секундам. На момент выполнения запроса DNS время хранения информации TTL о домене google.com составляло 5 минут — что, впрочем, неудивительно для компании, которая имеет обширное и динамически изменяющееся присутствие в Internet. Более статичные организации обычно имеют более длительное значение TTL, например один день (86 400 секунд). В любом случае эта запись будет сохраняться в кэше в течение 5 минут, и, если обратиться к google.com повторно, Windows не будет направлять запрос к серверу DNS, а возьмет адрес из кэша.



Экран 1 Просмотр значений TTL для записей DNS

Помимо кэширования положительных ответов, Windows также запоминает отрицательные ответы. Отрицательный ответ заключается в том, что сервер DNS считает себя ответственным за данный домен, но

Ошибка маленькая — проблемы большие

Администратор сети Скотт Рассел расследует мистическую ошибку DNS

«Я дважды переустановил сервер DNS в соответствии с имеющейся документацией, но это не помогло. В конце концов я связался с провайдером и узнал, что головная компания поменяла записи DNS и MX на всех серверах...»

Когда в 8 вечера Скотту Расселу позвонил ИТ-администратор с прежнего места работы, он понял, что это не просто дань вежливости. Два дня назад у них в компании перестало работать подключение к Internet. Сотрудники не могли пользоваться электронной почтой через корпоративный сервер Exchange и регистрироваться в сети Windows 2000 Server. Специалисты по ИТ испробовали все, что могли, но безуспешно. Скотт согласился помочь, и скоро выяснилось, что все дело в ошибке настройки DNS. Рассел работает в области ИТ более 10 лет, в настоящее время он является администратором сети в канадской компании ABC Window Company. Старший редактор Windows IT Pro Энн Грабб побеседовала со **Скоттом Расселом** о том, как ему удалось определить источник проблемы и восстановить работоспособность компании.

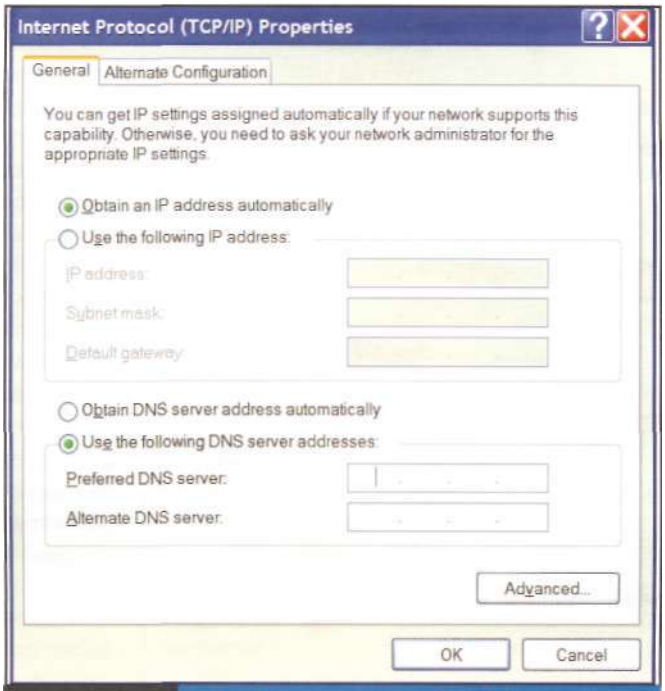
ИТ-администратор с вашей предыдущей работы попросил помочь устранить проблему, которую они не могли решить два дня. В чем же было дело?

Да, у них ничего не работало: они не могли регистрироваться в сети, пользоваться Internet и электронной почтой. Когда я был там сетевым администратором, мы создали два домена — внешний домен company.com для Web и SMTP и внутренний домен company.net. Мы не регистрировали домен .net, поскольку он был внутренним, Наш провайдер обеспечивал работу Web-сайта компании и держал у себя внешние записи DNS и MX.

Прибыв на место, я в первую очередь проверил настройки DNS, дабы убедиться, что все в порядке. В компании имеется три контроллера домена и два сервера DNS, которые я настраивал, когда работал сетевым администратором — там использовалась служба Windows DNS, интегрированная со службой каталога AD. Я дважды переустановил сервер DNS по той документации, которую подготовил перед уходом. Это был довольно трудоемкий процесс,

Надо было разобраться, почему DNS не мог разрешить IP-адрес контроллера домена для локального домена company.net. Мы задействовали утилиту Traceroute для адреса IP, который мы использовали, как нам казалось, и выяснилось, что в результате возвращается совершенно другой внешний IP-адрес. У нас не было никаких предположений относительно того, что происходит, хотя адрес был из того же диапазона, что и наш. Первым делом мы подумали о внешнем вторжении в сеть.

у него нет записи о хосте, требуемой в запросе. Хотя в отрицательных ответах не содержится сведений о TTL, Windows запоминает эти ответы на период времени от 5 до 15 минут, в зависимости от используемой версии Windows и дополнительных настроек. Более подробно об управлении кэшированием отрицательных ответов с помощью настроек реестра рассказано во врезке «Управление положительным и отрицательным кэшированием».



Экран 2 Свойства протокола TCP/IP для сетевого адаптера по умолчанию

Те, кому пришлось столкнуться с проблемами разрешения имен в своей сети, могут очистить кэш DNS с помощью команды ipconfig /flushdns (и вовсе не обязательно править реестр). Очистка кэша DNS — это однократная операция, которая удаляет из памяти все сохраненные значения и позволяет начать все с чистого листа. Очистку кэша можно повторить в любой момент. При этом следует иметь в виду, что, если у вас имеется локальный сервер DNS, он, скорее всего, запоминает все адреса, к которым обращаются компьютеры сети. Чтобы очистить кэш DNS на серверах DNS, стоит воспользоваться оснасткой DNS консоли управления MMC. Для запуска в меню «Пуск» нужно выбрать «Программы», «Администрирование», DNS. Щелкните правой кнопкой мыши на имени сервера DNS и выберите Clear Cache.

Очистка кэша DNS — хорошее средство отладки для тех, кто занимается тестированием в сети чего-либо, связанного с разрешением имен, если нежелательные события произошли за последние 5-15 минут. Следует иметь в виду, что при очистке кэша DNS Windows автоматически сразу загружает в кэш адреса из файла \%systemroot%\system32\drivers\etc\hosts.

Энн Грабб

Старший редактор в Windows IT Pro. Она имеем более чем двадцатилетний опыт работы, является автором и редактором статей, книг и других материалов по компьютерной и юридической тематике. agrubb@windowsitpro.com

Как же вы определили, кому принадлежит этот IP-адрес?

Ну, во-первых, я зашел на сайт поддержки Microsoft (http://www.support.microsoft.com) и провел там почти два с половиной часа. Пока я изучал материалы сайта, мне пришло в голову, что кто-нибудь мог просто зарегистрировать это доменное имя. Тогда я решил позвонить провайдеру. Через три часа мне сообщили, что неизвестный адрес принадлежит их материнской компании. В этот момент выяснилось, что материнская компания зарегистрировала доменное имя, совпадающее с нашим локальным доменом .net.

Обратившись к ним, мы убедились, что так оно и есть. Они зарегистрировали домен .net и изменили все записи DNS, включая и MX, ничего не сообщив своим пользователям.

Но когда вы обнаружили, что имя внутреннего домена зарегистрировано материнской компанией провайдера, вам необходимо было избежать переименования своего домена. Как вы вышли из положения?

Сначала я запросил у провайдера новый IP-адрес и информацию о зонах для их DNS. Затем потребовалось зарегистрировать нашу запись DNS в качестве вторичного сервера DNS для их сервера DNS, чтобы мы смогли зарегистрироваться в системе и выполнить необходимые изменения. Я добавил вторичную зону в нашу запись DNS и настроил их DNS в качестве вторичного DNS у нас, так что наш сервер DNS смог распознавать внешние имена company.com корректно.

С этого момента у нас появилась возможность работать с Internet. Затем нам потребовалось реплицировать вторичную зону DNS в AD. Когда мы это сделали, все стало работать нормально, пользователи получили возможность регистрироваться на сервере и работать с электронной почтой.

Какие рекомендации вы могли бы дать коллегам по цеху с учетом уроков, извлеченных из этой истории?

Во-первых, при возникновении проблем с Internet нужно обязательно обращаться к локальному провайдеру и его материнской компании. Прежде чем менять настройки своих серверов DNS, надо узнать у технического персонала провайдера, не изменяли ли они что-либо в конфигурации. Учитывая нынешние тенденции слияния и поглощения компаний, такое случается сплошь и рядом. Я надеюсь, наш провайдер тоже усвоил, что, изменив свои настройки, следует сообщать об этом клиентам.

И конечно, я хорошо запомнил свою ошибку с использованием домена .net. Теперь для всех внутренних настроек DNS я использую суффикс .local.

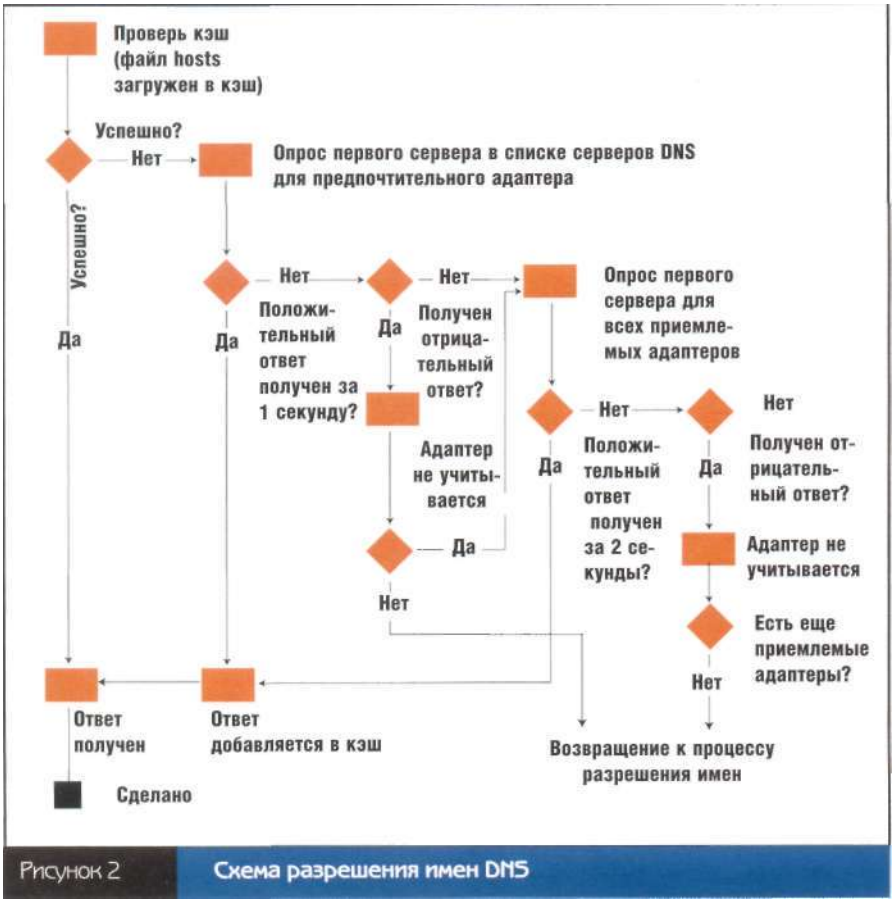


Рисунок 2 Схема разрешения имен DNS

исправностей, позволяющим управлять разрешением имен DNS.

Например, когда несколько серверов отвечают на одно и то же имя, а требуется, чтобы мой компьютер подключался к одному конкретному, я могу использовать файл hosts. Рассмотрим случай, когда несколько серверов доступа Microsoft Outlook Web Access используют общий адрес URL, который задается DNS. Если пользователи начинают жаловаться на возникновение случайных ошибок OWA, как определить, какой из серверов тому причиной? Файл hosts позволяет отказаться от услуг разрешения имен DNS и подставить требуемый адрес — для этого необходимо всего лишь внести в файл hosts значение, оно попадет в кэш и будет присутствовать там постоянно. Файл hosts имеет простой формат — в одной строке указываются IP-адрес и символьное имя. Служба разрешения имен обновляет значение в кэше автоматически при сохранении файла hosts, так что изменения вступают в силу немедленно.

О хостах

Хотя кэширование иногда мешает, оно может оказаться и весьма полезным. В кэше хранятся как копии найденных при разрешении имен адресов, так и статические элементы, которые определены в файле hosts на локальном компьютере. Файл hosts оказался весьма удобным средством поиска и устранения не-

Многосерверные/многоадаптерные конфигурации

Рассмотрим подробнее схему, приведенную на рис. 2. Мы рассмотре-

Управление положительным и отрицательным кэшированием

Кэширование в Windows выполняется в соответствии с установленными по умолчанию значениями, которые могут варьироваться в зависимости от используемой версии Windows и дополнительных настроек. Для управления кэшированием применяются два параметра реестра. Раздел HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNSCache\Parameters содержит параметры, управляющие продолжительностью хранения в кэше положительных и отрицательных ответов. Эти значения в версиях Windows Server 2003, Windows XP и Windows 2000 слегка отличаются.

Для положительного кэширования в Windows 2000 этот параметр называется MaxCacheEntryTtlLimit, в Window XP и 2003 он называется MaxCacheTtl. Оба параметра указывают максимальный срок, в течение которого положительные ответы могут храниться в кэше. Если этот параметр определен, по умолчанию его значение равно 86400 секундам (1 день). Это значение имеет преимущество перед всеми возможными значениями TTL, которые превышают данное значение. Поэтому, если оставить значение по умолчанию, Windows будет сохранять положительные ответы не более одного дня, даже если указанное значение TTL равно, скажем, пяти дням. Установив значение параметра равным одной секунде, можно практически предотвратить кэширование положительных ответов DNS.

Кэширование отрицательных ответов управляется параметром NegativeCacheTime в Windows 2000, а в Windows XP и 2003 — MaxNegativeCacheTtl. Значение по умолчанию составляет 300 секунд (5 минут) для Windows 2000 и 900 секунд (15 минут) для XP и 2003. Отрицательные ответы, возвращаемые сервером DNS, будут сохраняться в кэше именно такое время, так что, если после первой неудачной попытки сервер DNS получит нормальное разрешение имени, он все равно будет возвращать отказ на этот адрес до того момента, пока не закончится TTL отрицательного ответа. Если вы подключаете новые компьютеры, отрицательное кэширование действительно может вызвать проблемы в случае попытки найти компьютер до того, как запись о его присутствии будет распространена в сети.

Более подробные сведения об этих процедурах можно найти в статьях базы знаний Microsoft «How to Disable Client-Side DNS Caching in Windows 2000»(http://support.microsoft.com/default.aspx?scid=kb;en-us;245437) и «Disable Client-Side DNS Caching in Windows XP and Windows Server 2003» (http://support.microsoft.com/default.aspx?scid=kb;en-us;318803).

ли шаги, выполняемые в тех случаях, когда запрос может быть разрешен из локального кэша. Но если локальный кэш не позволяет выполнить разрешение запроса, то как дальше осуществляется процесс разрешения имени? Windows продолжает процесс разрешения имен, выдавая рекурсивные запросы DNS к серверам, указанным в качестве предпочтительных (настройка сервера DNS выполняется в параметрах протокола TCP/IP для каждого сетевого адаптера, как показано на экране 2). Если Windows не получает никакого ответа от предпочтительного сервера DNS в течение секунды, этот же запрос передается по остальным сетевым интерфейсам с интервалом ожидания 2 секунды. Если ответа по-прежнему нет, Windows выполняет три повторные попытки получить ответ на запрос. Каждый следующий раз устанавливается более длительный интервал ожидания (2, 4 и 8 секунд соответственно), после чего выполняется обращение ко всем остальным серверам DNS по всем имеющимся сетевым интерфейсам. Общее время разрешения адреса DNS не должно превышать 17 секунд.

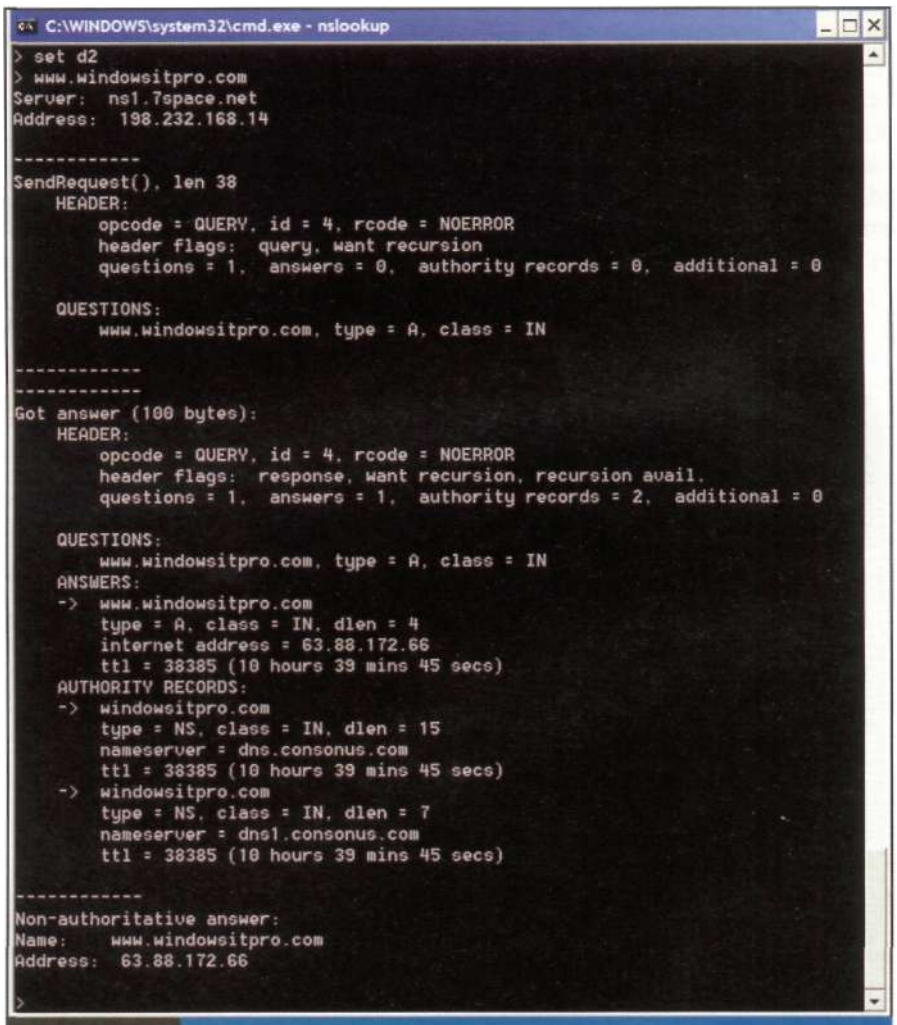
Каков механизм выбора предпочтительного и приемлемого сетевого адаптера (в Microsoft используют термин under consideration — «рассматриваемый»). Техническая документация Microsoft дает расплывчатые ответы в вопросах разрешения имен. Например, если все серверы DNS для определенного адаптера были опрошены и ни один из них не ответил, данный адаптер исключается из рассмотрения на 30 секунд. Можно предположить, что при этом адаптер временно исключается из категории «приемлемый» на указанный интервал времени, хотя в документации об этом не говорится. Кроме того, в документации Microsoft указано, что служба разрешения имен DNS запоминает время отклика серверов DNS и может выбирать предпочтительный сервер в зависимости от скорости получения ответа на запросы, — видимо, такой же подход используется и для определения предпочтительного адаптера.

Утверждение Microsoft о том, что служба разрешения имен может изменять порядок следования предпочтительных серверов DNS, противоречит настройкам, которые можно найти в расширенных окнах настроек DNS для сетевых адаптеров, где порядок следования определяется администратором при задании конфигурации. В большом количестве документов Microsoft дана другая информация. Поэтому я не очень доверяю сведениям о том, в каком порядке служба разрешения имен обращается к серверам DNS при разрешении имен. Когда мне приходится заниматься поиском и устранением неисправностей, я пользуюсь инструментами типа Network Grep (Ngrep) и WmDump для проверки отправляемых компьютером запросов DNS и серверов, которым эти запросы адресованы.

В следующей статье я планирую рассказать подробнее об этих инструментах, а также о программах, с которыми читатели, вероятнее всего, не знакомы. Некоторые полезные инструменты для работы с DNS описаны во врезке «Инструменты для поиска и устранения ошибок DNS».

Nslookup

Теперь, разобрав принципы выполнения запросов DNS и то, каким образом служба разрешения имен DNS направляет запросы DNS через установленные в компьютере сетевые интерфейсы, можно задействовать утилиту командной строки Nslookup, которая, безусловно, является одним из основных инструментов решения проблем с DNS и поиска и устранения неисправностей.



Экран 3 Пример выполнения запроса Nslookup

Nslookup может запускаться в неинтерактивном режиме и позволяет тестировать поиск и разрешение имен хостов с использованием стандартной службы разрешения имен Windows. Пример:

```
nslookup www.windowsitpro.com
```

С другой стороны, можно направить запрос DNS на конкретный сервер вместо тех, которые указаны на локальном компьютере. Для этого достаточно добавить в конце командной строки адрес данного сервера DNS:

```
nslookup www.windowsitpro.com 10.0.0.1
```

Это понадобится, если нужно убедиться, что получаемые ответы исходят именно от данного сервера DNS. Чтобы более детально вникнуть в процесс разрешения имен, можно запустить Nslookup в интерактивном режиме, который позволяет выбирать сервер, тип запроса (рекурсивный или итеративный) и детализацию отладочной информации. Рассмотрим для примера несколько сценариев обнаружения неисправностей.

Как уже упоминалось, в некоторых случаях процесс разрешения имен вынужден пройти всю цепочку до корневых серверов доменов Internet, если ни один другой сервер по пути прохождения запроса не располагает кэшированной информацией, имеющей заданный интервал TTL. Можно

Таблица

A.ROOT-SERVERS.NET	198.41.0.4
B.ROOT-SERVERS.NET.	128.9.0.107
C.ROOT-SERVERS.NET.	192.33.4.12
D.ROOT-SERVERS.NET.	128.8.10.90
E.ROOT-SERVERS.NET.	192.203.230.10
F.ROOT-SERVERS.NET.	192.5.5.241
G.ROOT-SERVERS.NET.	192.112.36.4
H.ROOT-SERVERS.NET.	128.63.2.53
I.ROOT-SERVERS.NET.	192.36.148.17
J.ROOT-SERVERS.NET.	192.58.128.30
K.ROOT-SERVERS.NET.	193.0.14.129
L.ROOT-SERVERS.NET.	198.32.64.12
M.ROOT-SERVERS.NET	202.12.27.33

выполнить полное прохождение цепочки, чтобы определить, где процесс прерывается. Для воспроизведения этого процесса с помощью Nslookup можно вызвать итеративный (нерекурсивный) запрос поиска для целевого домена, указав при этом один из корневых доменных серверов (список корневых доменов приведен в таблице) в качестве целевого сервера, а затем вручную проследовать по каждому направлению, которое возвращается до получения итогового результата.

Я выполнил поиск для полного доменного имени компьютера (FQDN) www.windowsitpro.com, настроив Nslookup для использования итеративных запросов. В приглашении я ввел параметр Set Norecurse, затем указал корневой сервер с помощью параметра Server и выполнил запрос. Следуя по адресам серверов, я проследил всю цепочку, указывая вручную целевой сервер при каждой итерации. Такой способ дает значительно больше информации для поиска и устранения неисправностей, чем выполнение стандартного запроса к локальному серверу DNS и анализ данных, которые приходят в ответ.

Если для решения задачи не требуется выполнять полный итеративный опрос, а просто нужна более подробная информация о прохождении запросов и возвращаемой информации, можно задействовать ключи Set Debug или Set D2 для отображения отладочной информации о выполнении запроса DNS. На экране 3 приведен результат исполнения примера запроса разрешения имени www.windowsitpro.com. Аналогично ключ Set Type позволяет использовать Nslookup для быстрого поиска определенных типов записей в домене по их типу. Для поиска почтовых серверов требуется указать ключ MX (Mail Exchange), а для серверов имен — NS (Name Server).

Добавим немного AD

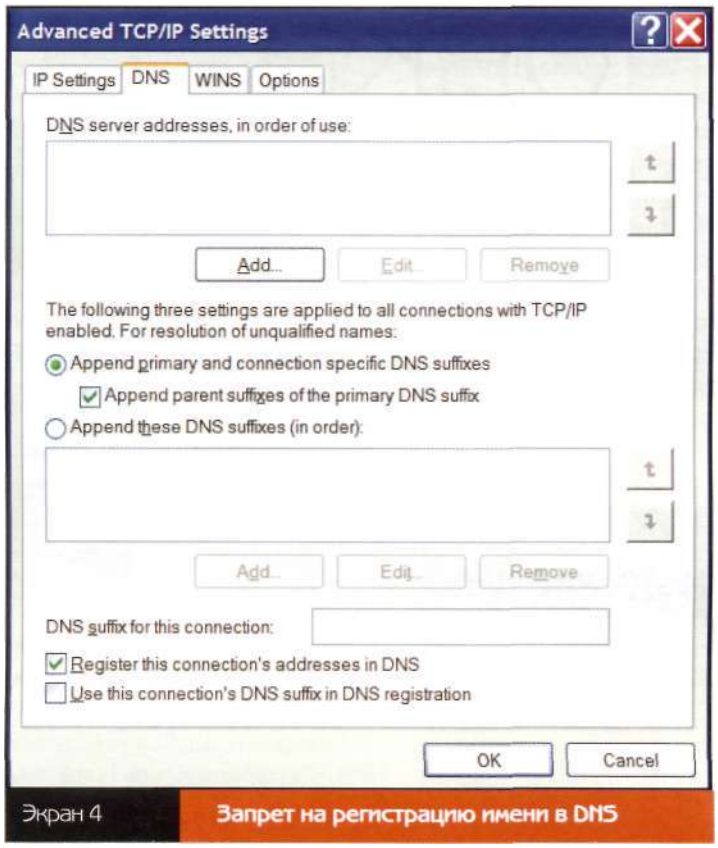
Теперь, когда мы познакомились с концепциями кэширования, последовательного и рекурсивного выполнения запросов, а также с приемами диагностики проблем разрешения имен в Internet, не составит большого труда разобраться с теми особенностями, которые привносит AD. Интеграция DNS и AD происходит на двух уровнях: во-первых, DNS является основным механизмом, с помощью которого компьютеры в сети находят другие хосты в среде AD, во-вторых, данные DNS — список существующих хостов и их адреса IP — реплицируются между серверами DNS через механизм репликации AD. Механизмы репликации AD обсуждались на страницах журнала достаточно подробно, так что рассмотрим дополнительную информацию, которая содержится в записях DNS в среде AD.

Записи AD содержат сведения о динамической регистрации, которые соз-

Инструменты для поиска и устранения ошибок DNS

В статье, посвященной поиску и устранению неисправностей в работе службы DNS, невозможно обойти вниманием сайт DNSstuff.com (http://www.dnsstuff.com). Этот сайт разработан и поддерживается Р. Скотт Пери. Здесь бесплатно предоставляются средства для работы с DNS, IP-адресами, доменами и т.д., предназначенные для простого и удобного поиска и устранения неисправностей с использованием Web-служб. Эти инструменты позволяют выполнить разрешение имен в IP-адреса, обратный поиск (reverse lookup), поиск WHOIS, а также проверку выбранных адресов IP на вхождение в базу адресов — известных источников спама. Я считаю DNSstuff.com чрезвычайно удобным инструментом для отладки DNS у клиентов. Примечательно, что предлагаемый этими средствами вариант поиска хоста позволяет автоматически выполнить итеративный запрос DNS, начиная с корневых серверов, и пройти весь путь до конечного имени хоста с использованием удобного и красивого Web-интерфейса. Это избавляет от необходимости выполнять данную процедуру вручную с помощью Nslookup и позволяет продемонстрировать клиентам результаты в гораздо более удобной и понятной форме. Вдобавок DNSstuff.com содержит функцию опроса основных Internet-провайдеров для проверки, не выдают ли они различные кэшированные ответы на один и тот же запрос DNS.

даются автоматически клиентскими компьютерами, серверами и рабочими станциями в среде AD и содержат имя компьютера и его адрес IP. Клиент службы DHCP выполняет процесс регистрации при запуске службы даже в том случае, если адрес присваивается статически. В соответствующих свойствах IP клиент службы DHCP регистрирует свой адрес на серверах DNS, для работы с которыми он настроен. Если вы установили дополнительные сетевые интерфейсы, предназначенные для выполнения специальных задач (например, выделенная сеть для выполнения резервирования на ленточные библиотеки), причем эти интерфейсы не должны отвечать на приходящие по ним запросы клиентов, процесс автоматической регистрации может создать проблемы с разрешением этих имен DNS.



Экран 4 Запрет на регистрацию имени в DNS

Например, эти специальные сетевые адаптеры могут быть зарегистрированы с адресами IP в DNS, в то время как было нежелательно, чтобы эти сетевые адреса выдавались в качестве возможных вариантов при разрешении имен. Если это все-таки случилось, можно отменить регистрацию сетевого интерфейса. Для этого необходимо выполнить редактирование дополнительных свойств DNS для данного интерфейса и снять флажок Register this connection's address in DNS («Зарегистрировать это соединение в DNS»), как показано на экране 4. В противном случае Windows обязательно попытается зарегистрировать в DNS все имеющиеся сетевые интерфейсы.

Помимо автоматической регистрации этих записей хостов (записи типа A), Windows выполняет для контроллеров доменов регистрацию дополнительных записей сервера (записи SRV). Запись SRV определяет тип участия компьютера в AD при обработке специальных задач аутентификации. Записи SRVНе являются уникальными для AD, напротив, это стандартный тип записей DNS, определяющий зарегистрированные в домене службы, хосты, на которых эти службы могут быть найдены, используемые порты и протоколы. Аналогично тому, как записи почтовой службы MX указывают, что служба SMTP может быть найдена на определенном порту (т. е. порт 25) на данном сервере, записи SRV предоставляют ссылку для любого типа служб на любой системе. Например, запись SRV, определяющая хост example.com как Web-сервер, может иметь следующий вид:

_http.Jcp.example.com SRV O O 80 www.example.com

Рассматривая этот пример, можно сделать следующие заключения: служба TCP, известная как HTTP, доступна в домене example.com; она доступна по порту 80 для хоста с именем www.example.com. В среде AD контроллер домена регистрирует четыре типа записей SRV на серверах DNS, на работу с которыми он настроен:

_ldap._tcp.example.com
SRV 0 0 389 dc.example.com
_kerberos._tcp.example.com
SRV 0 0 88 dc.example.com
_ldap._tcp.dc._msdcs.example.com
SRV 0 0 389 dc.example.com
_kerberos._tcp.dc._msdcs.example.com
SRV 0 0 88 dc.example.com

Эти записи позволяют клиентам AD определять, где найти службы LDAP и Kerberos, которые необходимы в домене example.com для обнаружения других ресурсов AD и аутентификации доступа к этим ресурсам. Эти четыре примера записей SRV сообщают зависящим от AD клиентам о контроллере домена dc.example.com (гипотетический контроллер домена example.com), который будет использоваться для всех видов аутентификации.

С помощью оснастки DNS MMC следует сделать эти записи доступными для серверов DNS. Необходимо также иметь возможность просматривать их с клиента с помощью Nslookup.

Знания — в жизнь

После применения Nslookup мне удалось быстро определить источник проблемы. Дело было в ошибке кэширования, связанной с ответами моего провайдера на некоторые запросы DNS. Для определения причины неполадок мне пришлось выполнить итеративный процесс разрешения адреса собственного компьютера. После этого я смог быстро настроить альтернативное разрешение внешних имен DNS, а провайдер занялся устранением собственных недоработок. Проблема была решена быстро, и мои клиенты снова смогли пользоваться полнофункциональным разрешением имен. Знание принципов работы DNS в сочетании с удобными средствами обнаружения ошибок позволяют без труда устранять большинство проблем с DNS.

Установка Exchange 2003 на кластере

Как обновить Exchange 2003 до уровня SP2 на кластере Windows 2003

Дарах Моррисси
Консультант группы Technology Leadership Group компании HP в Дублине. С ним можно связаться по адресу: daragh.morrissey@hp.com

В статье «Построение кластера Exchange 2003: планирование и подготовка», опубликованной по адресу (www.osp.ru/win2000/exchange/603_06_1.htm), я рассказал о задачах, которые администратору необходимо решить перед началом установки системы Exchange Server 2003 Service Pack 1 (SP1) в кластере Windows Server 2003 SP1. Будем исходить из того, что все подготовительные операции выполнены и можно приступать к установке Exchange 2003 на одном из серверов кластера. Установка Exchange в кластере не вызывает особых затруднений, однако операций она включает несколько больше, чем установка системы на одиночном сервере. Напомню, что кластер представляет собой активный/пассивный кластер, состоящий из двух узлов. Итак, приступаем к установке.

Перед тем как создавать новый кластер Exchange 2003, необходимо убедиться в том, что выполнены все требования, обеспечивающие возможность развертывания Exchange 2003. Прежде всего следует ознакомиться с руководством, опубликованным по адресу http://www.microsoft.com/exchange/evaluation/sysreqs/2003.mspx, и проверить, выполнены ли все операции, описанные ранее.

Напомню, что я уже рассказывал о формировании кластера на базе Windows 2003 SP1 и Exchange 2003 SP1. За время, прошедшее с момента публикации той статьи, корпорация Microsoft выпустила Exchange 2003 SP2. Для запуска этой системы необходимо до начала настройки Exchange установить на каждом узле кластера оперативный модуль коррекции Windows 2003 SP1. Этот модуль устраняет проблему, создаваемую системой Windows 2003 SP1 и состоящую в нарушении стабильности сетевых соединений между этой системой, с одной стороны, и другими серверами и клиентами — с другой. Сведения о рассматриваемой проблеме и о местах размещения доступного для загрузки оперативного модуля можно получить по адресу http://support.microsoft.com/?kbid=898060. После установки модуля коррекции соответствующий узел кластера необходимо перезагрузить. Следует иметь в виду, что упомянутая проблема сетевых соединений может коснуться и серверов, функционирующих под управлением Windows 2003 первоначальной версии RTM с дополнением MS015-019, обеспечивающим повышение уровня безопасности.

Создание Exchange Virtual Server

Итак, мы произвели настройку кластерной группы, задав имя кластера, а также ресурсы — IP-адрес и Microsoft Distributed Transaction Coordinator (MS DTC). Кроме того, мы выполнили настройку группы ресурсов Exchange, содержащей дисковые ресурсы, имя сети кластера и адрес IP виртуального сервера Exchange (Exchange Virtual Server, EVS). Следующая задача — установить Exchange 2003 на узлах кластера в соответствии с описанной ниже процедурой.

Процедуру установки нужно документировать: каждый шаг установки должен быть зафиксирован. Документация позволит другим администраторам получить представление о том, как вы строили сервер. Кроме того, она может пригодиться для восстановления данных при аварийных сбоях (иначе говоря, в случае, если придется вновь формировать кластер). Самый простой способ документирования таков. Открываем новый документ в WordPad или Microsoft Word. При выполнении каждого этапа установки, не покидая активного окна текстового редактора, делаем «моментальный снимок» экрана — для этого нужно нажимать комбинацию клавиш Alt+Print Screen. В результате изображение окна будет скопировано в буфер обмена. В меню Edit программы WordPad следует выбрать пункт Paste Special, а затем — пункт Device Independent Bitmap. Таким образом растровый рисунок будет сохранен в машинонезависимом формате, что обеспечивает уменьшение размера документа по сравнению с тем случаем, когда растр сохраняется с помощью стандартной команды Paste. Файл документации следует сохранить в безопасном месте (за пределами кластера).

Систему Exchange 2003 нужно установить на первом узле кластера. Затем следует зарегистрироваться на узле Node 1 под учетной записью, наделенной полномочиями уровня Exchange Full Administrator. Запустите программу установки Exchange 2003 (она находится на установочном компакт-диске Exchange 2003 в папке \setup\i386). На экране появится сообщение об ошибке: Exchange Server 2003 has a known compatibility issue with this version of Windows. Его можно проигнорировать; позднее мы устраним эту проблему с помощью пакета Exchange 2003 SP2. На экране приветствия нажимаем Next.

Теперь требуется принять условия лицензионного соглашения с конечным пользователем (End User License Agreement, EULA). Для этого необходимо нажать на кнопку I Agree. В меню Action выбираем пункт Typical. Перейдя в следующий экран, нужно принять условия соглашения о лицензировании «за рабочее место» (Per Seat Licensing Agreement). После этого начинается процесс установки; по его завершении на экране появляется соответствующее извещение.

Теперь следует установить Exchange 2003 на втором узле кластера. Установим Exchange 2003 на втором узле (Node 2), осуществляя при этом те же операции, которые выполняли на узле Node 1. Пока мы не можем модернизировать машинные команды до уровня Exchange 2003 SP2; SP2 можно будет устанавливать только после создания EVS.

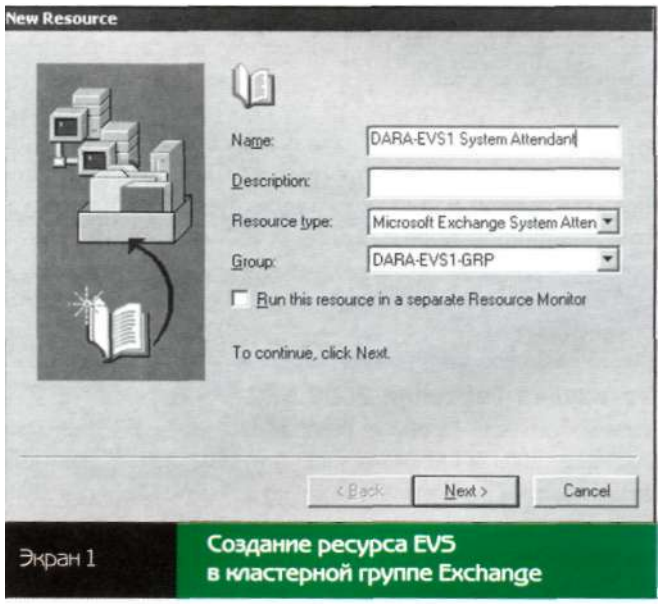
Создадим EVS. После установки двоичных файлов Exchange на узлах кластера можно приступать к созданию EVS. Этот сервер нужно создавать на активном узле (т.е. на узле, который является в данный момент владельцем EVS); дело в том, что программа установки размещает базы данных Exchange, файлы регистрации транзакций и другие компоненты в общую систему дисковой памяти — так, чтобы каждый узел имел к ним доступ.

Чтобы создать EVS, нужно зарегистрироваться на активном узле под учетной записью, наделенной полномочиями уровня Exchange Full Administrator. Откройте программу Cluster Administrator, в меню File выберите пункты New, Resource и Microsoft Exchange System Attendant. Создайте этот ресурс в группе кластера Exchange (Exchange cluster group); следует иметь в виду — это не то же самое, что группа кластера (cluster group). Как показано на экране 1, в нашем случае речь идет о группе DARA-EVS1-GRP. Нажмите Next.

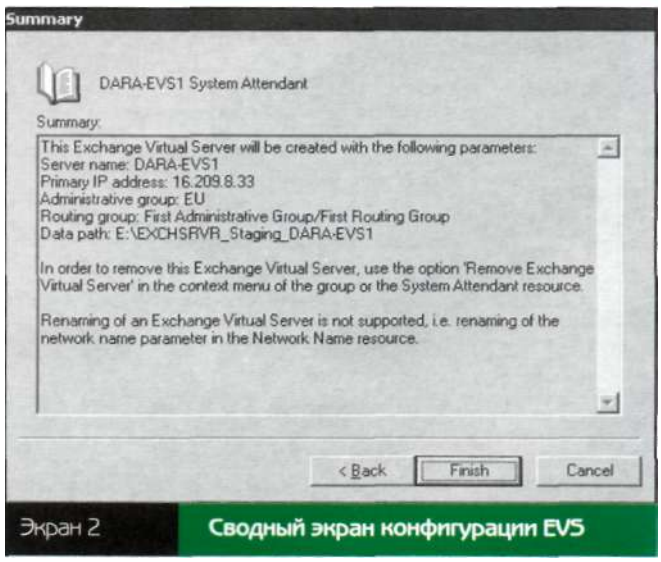
Система предложит указать узлы, которые могут быть владельцами данного ресурса. Оба узла необходимо включить в список владельцев по умолчанию. Чтобы продолжить процесс установки, нужно снова нажать Next. Далее система предложит указать ресурсы, зависимые от ресурса Exchange System Attendant. Выделяем все ресурсы, представленные в левой панели (IP address, network name и disk resources). Щелчком на кнопке Add следует ввести их в число ресурсов, необходимых для ресурса Exchange System Attendant. Нажимаем Next.

Теперь нужно выбрать административную группу для нового сервера EVS. Выбираем такую группу, нажимаем на кнопку Next. Выбираем для EVS группу маршрутизации и вновь нажимаем Next.

В следующем окне подсказки следует выбрать в совместно используемом хранилище папку, где будут храниться базы данных Exchange, журналы регистрации транзакций, папки SMTP, база данных полнотекстового индексирования и файлы регистрации трассировки сообщений. По умолчанию эта папка располагается в папке \exchsrvr на физическом ресурсе в группе ресурсов Exchange, создание которой описывалось ранее. Недостаток программы установки Exchange состоит в том, что в процессе установки она размещает все компоненты системы (такие, как ее базы данных) в одной и той же папке. После этого администратору приходится вручную перемещать их в нужные папки. Чтобы знать, какие компоненты Exchange программа установки размещает в процессе развертывания, я обычно использую для папки имя типа \exchsrvr_staging-EVSname. При создании тестового кластера в рамках подготовки статьи я дал папке имя \exchsrvr_staging_DARA-EVSl. Оно означает, что данная папка была создана во время установки указанного сервера EVS. Позднее я объясню, каким образом следует перемещать эти компоненты на другие накопители или в другие папки.



Экран 1 Создание ресурса EVS в кластерной группе Exchange



Экран 2 Сводный экран конфигурации EVS

Программа установки отображает сводный экран, где указаны все примененные параметры (см. экран 2). Примите сводку параметров установки — для этого нужно нажать на кнопку Finish. Программа установки Exchange автоматически создаст ресурсы для компонентов Exchange, такие как ресурсы, относящиеся к Information Store и протоколам IMAP и POP. По завершении этого процесса программа отобразит сообщение о том, что создание кластерного ресурса Exchange System Attendant успешно завершено.

На данном этапе в окне Cluster Administrator мы видим, что все ресурсы Exchange находятся в автономном режиме. Переведем все ресурсы в активный режим; для этого следует щелкнуть на каждом ресурсе правой кнопкой мыши и в контекстном меню выбрать пункт Bring Online. В окне Cluster Administrator появится перечень ресурсов, подобный представленному на экране 3.

Теперь следует убедиться в том, что EVS функционирует в активном режиме. Откроем диспетчер ESM (Exchange System Manager) и проверим административную группу. Сервер DARA-EVS1 будет отображен как входящий в состав кластера сервер, на котором выполняется Exchange 2003 RTM версии 6944.4.

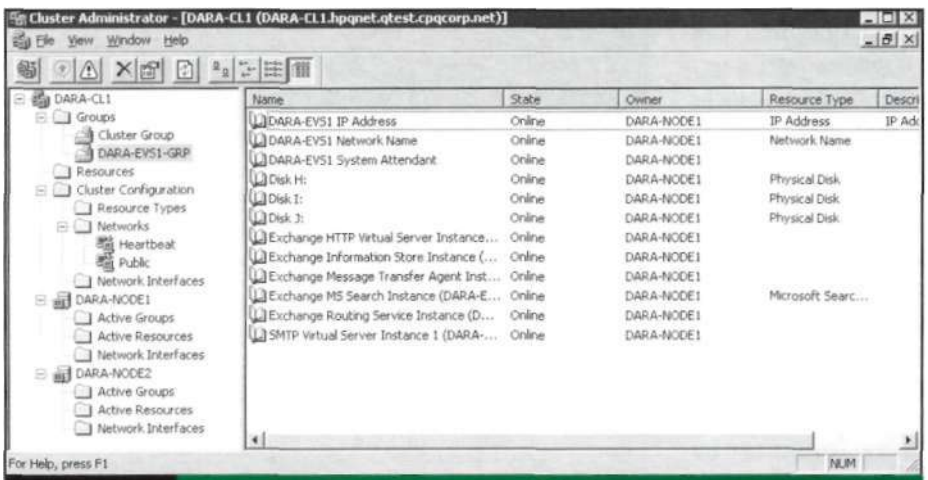
На данном этапе я рекомендую протестировать процедуру аварийного переключения на узел Node 2; необходимо убедиться в том, что сервер EVS способен функционировать на обоих узлах кластера. Чтобы осуществить аварийное переключение средствами программы Cluster Administrator, правой кнопкой мыши нужно щелкнуть на группе ресурсов, ассоциированной с сервером EVS (в данном случае с сервером DARA-EVS1) и выбрать Move Group. Тем самым мы запускаем процедуру аварийного переключения вновь созданного сервера EVS с Node 1 на Node 2.

Установка Exchange 2003 SP2

После того как процесс создания сервера EVS на базе Exchange 2003 RTM будет успешно завершен, я рекомендую модернизировать кластер до уровня Exchange 2003 SP2. Но перед тем как приступить к обновлению кластера до уровня Exchange 2003 SP2, следует позаботиться о том, чтобы все внешние серверы были доведены до уровня Exchange 2003 SP2. До начала модернизации внутренних серверов необходимо установить пакеты обновлений на внешних серверах. Специально для системы Exchange 2003 в Microsoft разработана новая процедура обновления Exchange. Эта процедура подробно описывается в статье «Кластеры Exchange 2003: технология последовательной модернизации» в пятом номере Windows IT Pro за 2005 год. Чтобы обновить систему до Exchange 2003 SP2, следует зарегистрироваться на узле Node 1 (сейчас он должен быть пассивным, ибо мы только что произвели аварийное переключение на узел Node 2) и установить Exchange 2003 SP2, запустив файл update.exe (он находится на компакт-диске Exchange 2003 SP2 в папке \setup\ i386). На экране Licensing Agreement нужно выбрать вариант I Agree (тем самым мы выражаем свое согласие с условиями лицензионного соглашения) и нажать Next. В столбце Action следует выбрать строку Update, как показано на экране 4. Выбираем операции по умолчанию (т. е. обновление всех компонентов, таких как ESM). Нужно иметь в виду, что по завершении процедуры обновления система может предложить выполнить операцию перезагрузки. Я получил такое предложение, потому что выполнял процедуру установки по удаленному соединению.

Чтобы завершить обновление, требуется перевести EVS в автономный режим, оставив в активном режиме сетевое имя, IP-адрес и ресурсы хранения данных, ассоциированные с этим сервером EVS. Для этого нужно правой кнопкой мыши щелкнуть на ресурсе System Attendant и в контекстном меню выбрать пункт Take Offline. В результате ресурсы Exchange, относящиеся к Store и протоколам IMAP и POP, будут переведены в автономный режим, поскольку все они могут находиться в активном режиме лишь в том случае, если в этом режиме находится Exchange System Attendant (т. е. сервер EVS).

Теперь необходимо переместить группу ресурсов Exchange с Node 2 на Node 1. Перемещение осуществляется с помощью аварийного переключения (правой кнопкой мыши следует щелкнуть на группе ресурсов Exchange и в контекстном меню выбрать пункт Move Group). Надо иметь в виду, что этот процесс нельзя осуществить, если программа Cluster Administrator выполняется на узле Node 2; дело в том, что файлы, необходимые для выполнения процедуры обновления, на Node 2 еще не установлены. До появления системы Exchange 2003 правило, в соответствии с которым дополнительная процедура модернизации для пакетов обновления Exchange осуществляется из программы Cluster Administrator, не применялось. Оно было впервые реализовано в процедуре модернизации кластера Exchange 2000 Server до уровня Exchange 2003. Эту же процедуру необходимо выполнять при модернизации кластера Exchange 2003 RTM до уровня Exchange 2003 SP1.

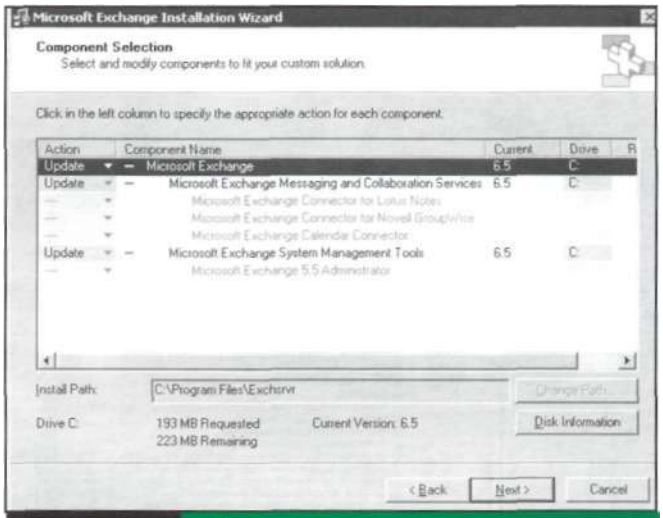


Экран 3 Просмотр состояния ресурсов Exchange в окне Cluster Administrator

Теперь программные файлы Exchange на Node 1 обновлены до уровня Exchange 2003 SP2. Чтобы завершить процесс модернизации, следует зарегистрироваться на Node 1. Правой кнопкой мыши нужно щелкнуть на ресурсе System Attendant для данного сервера EVS и в контекстном меню выбрать пункт Upgrade Exchange Virtual Server. По завершении процесса обновления на экране должно появиться сообщение The Exchange Virtual Server has been upgraded successfully.

На узле Node 2 выполняется система Exchange 2003 версии RTM. Запустив программу update.exe, нужно установить на этом узле систему Exchange 2003 SP2.

На экране Licensing Agreement следует выбрать вариант I Agree, выражая тем самым свое согласие с условиями лицензионного соглашения, и нажать Next. В столбце Action выберите строку Update. По завершении обновления узла Node 2 до уровня SP2 необходимо перезагрузить систему, если поступит такое предложение, и, когда Node 2 будет вновь инициализирован, удостовериться в том, что установка пакета обновлений SP2 завершилась корректно. Для этого требуется переместить группу ресурсов Exchange с Node 1 на Node 2; эту операцию мы уже проделывали раньше. В качестве финального теста я рекомендую провести перезагрузку одного узла за другим, начиная с Node 1. При этом сервер EVS должен «переместиться» с Node 1 на Node 2. Когда Node 1 вновь перейдет в активный режим и присоединится к кластеру, нужно перезагрузить Node 2, чтобы протестировать процесс аварийного переключения с Node 2 на Node 1. Эти тесты покажут, корректно ли настроен кластер Exchange. После завершения обоих аварийных переключений необходимо проверить файл Application log на наличие ошибок.



Экран 4 Модернизация кластера до уровня Exchange 2003 SP2

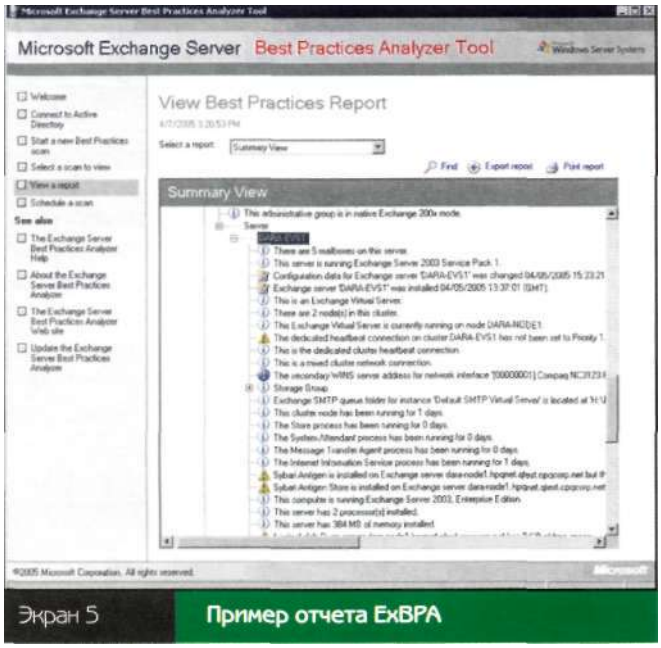
Действия после завершения установки

Примите поздравления: вы создали функционирующий кластер Exchange! Но не торопитесь размещать на EVS почтовые ящики. Сначала требуется выполнить ряд важных операций.

Нужно перераспределить компоненты Exchange по различным дисковым ресурсам. Программа Exchange cluster Setup размещает компоненты Exchange в папке \data directory. В процессе создания демонстрационного сервера EVS я разместил все компоненты в папке H:\exchsrvr_staging _DARA-EVS1. В нашей тестовой установке компоненты кластера Exchange помещены в следующие папки:

- папка E:\exchsrvr_staging_DAPvA-EVSl \mdbdata содержит файлы Exchange с расширением .edb, файлы потоковой базы данных (.stm), файл контрольных точек и журналы регистрации транзакций;
- в папке E:\exchsrvr_staging_DARAEVSl\mtadata размещается папка агента Message Transfer Agent (MTA);
- в папке E:\exchsrvr_staging_DARAEVS 1\ mailroot находятся структуры папок, которые использует SMTP Virtual Server;
- по адресу E:\exchsrvr_staging_DARAEVS 1\ exchange-serverservername размещается база данных полнотекстового индексирования, ассоциированная с EVS.
- в папке E:\exchsrvr_staging_DARAEVS 1\ servername.log хранятся файлы регистрации трассировки сообщений.

Журналы регистрации транзакций и базы данных Exchange желательно хранить на разных накопителях. Размещение указанных объектов на разных накопителях давно уже пропагандируется специалистами Microsoft, и я настоятельно рекомендую читателям следовать этой практике. Таким образом можно гарантированно повысить производительность сервера Exchange. Процесс Information



Экран 5 Пример отчета ExBPA

Store записывает каждую транзакцию в базу данных и в журнал регистрации транзакций; при разнесении этих ресурсов по разным физическим накопителям снижается нагрузка на систему хранения данных. Но еще важнее другое. Администратор, размещающий журналы регистрации транзакций и соответствующую базу данных на разных накопителях, получает возможность восстанавливать данные резервного копирования в случае утраты накопителя, на котором хранятся базы данных. О том, как разместить базы данных и журналы регистрации транзакций на отдельных накопителях, рассказано в статье Microsoft «How to move Exchange databases and logs in Exchange Server 2003» http://support.microsoft.com/7kbid =821915). Кроме того, рекомендую ознакомиться со статьей «Тонкая настройка Exchange 2000 Server», опубликованной по адресу: www.osp.ru/win2000/exchange/603_06_2.htm.

Затем необходимо переместить папки SMTP. При перемещении папок SMTP нужно следовать инструкции, приведенной в статье Microsoft «How to change the Exchange 2003 SMTP Mailroot folder location» (http://support. microsoft. com/?kbid=822933).

Также требуется переместить файлы индексов. При перемещении файлов полнотекстового индекса хранилища личных сообщений и журналов хранилища личных сообщений нужно следовать указаниям, опубликованным по адресу http://www.microsoft.com/technet/prodtechnol/exchange/guides/workinge2k3store/elea3634-a2c0-40e6-ad50-e9e988ae4728.mspx, а также содержащимся в статье Microsoft «XADM: Recommendations for Using Content Indexing Utilities (Pstoreutl or Catutil) in a Cluster Environment» (http:// support.microsoft.com/?kbid=294821). Для перемещения файлов индексирования используются две утилиты: pstoreutl.exe, которая позволяет перемещать на другой накопитель хранилище личных сообщений, и catutil.exe, которая обеспечивает перемещение каталога (индекса) на другой накопитель.

Кроме того, нужно сделать резервную копию содержимого кластера. Завершив перемещение необходимых компонентов, проведите полный сеанс резервного копирования содержимого кластера с помощью программы NTBackup. Следует скопировать данные накопителей локальной системы дисковой памяти, сведения о состоянии системы, а также провести полный сеанс резервного копирования баз данных Exchange.

Затем установите необходимые продукты от независимых поставщиков, такие как антивирусное программное обеспечение на базе анализа файлов, антивирусные программные средства, подходящие для работы в системе Exchange, а также программы, предназначенные для мониторинга. Примите меры к тому, чтобы из проверок, осуществляемых антивирусными программами на базе файлов, были исключены папки, содержащие базы данных Exchange и файлы регистрации транзакций, потому что такие антивирусные программы могут повредить базы данных Exchange. Более подробную информацию об этом можно найти в статье Microsoft «Overview of Exchange Server 2003 and antivirus software», опубликованной по адресу http://support.microsoft.com/?kbid=823166.

Обязательно проведите тестирование. Нужно создать в кластере тестовый почтовый ящик, а также профиль Microsoft Outlook, функционирующий в режиме Cached Exchange Mode. Следует протестировать процедуру аварийного переключения и зафиксировать время, необходимое для переключения EVS из автономного режима в активный между узлами кластера. Эти сведения пригодятся в дальнейшем при планировании мероприятий по обслуживанию кластера. По мере добавления к кластеру новых почтовых ящиков время аварийного переключения может возрастать из-за того, что у сервера EVS появятся новые каналы связи. Мне доводилось видеть производственные кластеры с подключенными к ним сотнями активных клиентов, на которых процедуры аварийного переключения выполнялись от 2 до 10 минут. Время аварийного переключения зависит от множества различных факторов, таких как характеристики аппаратных средств узлов кластера, производительность подсистемы дисковой памяти Exchange и число активных каналов связи.

Используйте пакет Exchange Server Best Practices Analyzer (ExBPA). Проверяйте корректность установки новых кластеров с помощью ExBPA. Эта программа, рассчитанная на эксплуатацию в кластерной конфигурации, обеспечивает анализ конфигурации кластера и EVS, а также генерирует отчеты, подобные изображенному на экране 5. Программу ExBPA можно загрузить по адресу http://www.microsoft.com/downloads/details. aspx?familyid=dbab201f-4bee-4943-ac22-e2ddbd258df3&displaylang=en.

Кластер Exchange готов к работе!

Следуя процедурам, описанным в данной статье, а также в статье «Построение кластера Exchange 2003: планирование и подготовка», можно успешно развернуть кластер Exchange. После запуска кластера нужно будет подумать о том, как обеспечить его безупречную эксплуатацию. Решить эту проблему поможет статья «Как улучшить работу кластера Exchange» из Windows IT Pro № 5 за 2004 год.

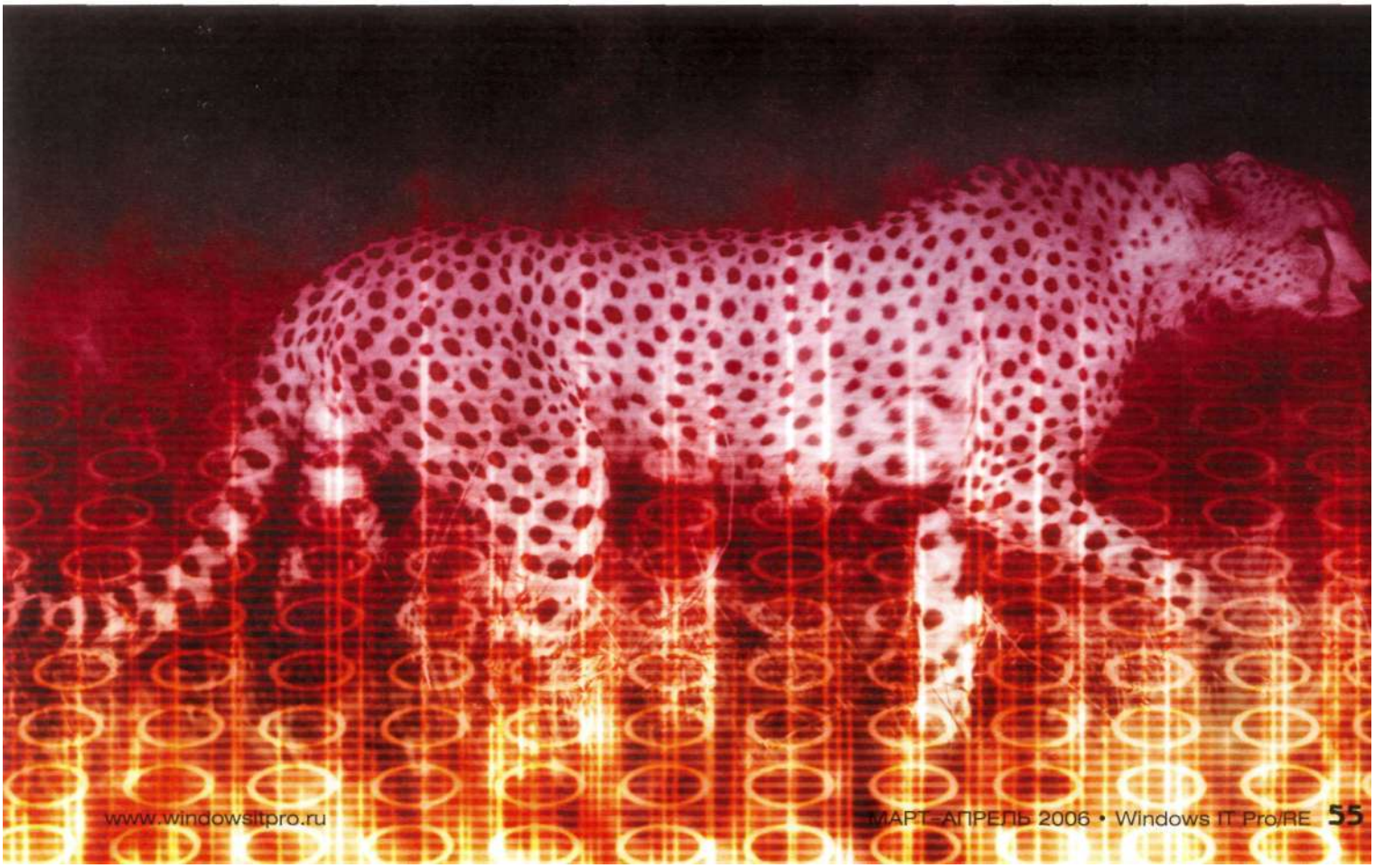
ADO.NET 2.0: умнее, быстрее, лучше

Новые возможности *решают* проблемы разработчиков

Вильям Воэн

Президент компании Beta V Corporation. Имеет звание Microsoft MVP. Работает в компьютерной индустрии с 1972 года.
billva@betav.com

Еще задолго до появления Visual Studio 2005 и SQL Server 2005 можно было наблюдать целый поток технических статей и маркетинговых материалов, превозносивших достоинства ADO.NET 2.0, новой версии ADO.NET, и тех инструментальных средств создания приложений, которые на нее ссылались. Во многих статьях просто приводился длинный список новых привлекательных возможностей ADO.NET 2.0. Но я думаю, что разработчиков больше интересует, как эти возможности помогут им в решении конкретных задач. Поэтому я собираюсь представить ADO.NET 2.0, перечислив некоторые важные проблемы и показав, насколько быстрее и эффективнее их решает новая версия.



Лучше управляет соединениями

Одна из самых досадных проблем в ADO.NET была связана с тем, как провайдеры данных обрабатывали (а скорее, не обрабатывали) пул соединений. К примеру, когда в ADO.NET 1.1 «умирало» соединение, механизм организации пула сохранял его экземпляр до тех пор, пока какое-нибудь ничего не подозревающее приложение не пыталось им повторно воспользоваться. И только тогда механизм организации пула «избавлялся от трупа». Однако при этом он оставлял другие отказавшие соединения, чтобы последующим вызовам Open было где поплутать. В ADO.NET 2.0 реализован новый подход: как только обнаруживается нарушение соединения, происходит немедленное вычищение из пула и его, и всех остальных неисправных соединений, что существенно облегчает задачу обработчиков исключений. Можно даже добавить код, стимулирующий очищение пула (или всех пулов). В ADO.NET 2.0 также заменены счетчики показателей пропускной способности соединения. Новые счетчики, кажется, работают (в отличие от старых), так что можно с большей точностью проводить мониторинг состояния пула соединений.

При работе с оболочкой Visual Studio в ходе создания нового соединения в Visual Studio 2003 предоставлялся выбор провайдеров OLE DB, но не провайдеров данных .NET Data. Для решения этой проблемы в ADO.NET 2.0 введен новый класс DbConnection StringBuilder, призванный помочь разработчикам строить настоящие строки соединения для провайдера данных в среде .NET, .NET Data Provider. Учитывая возможность использования новых интерфейсов приложений .NET Framework API для формирования списка провайдеров и серверов, создавать инструментальные средства построения диалоговых окон со строкой соединения Connection String станет заметно легче.

Некоторые приложения, особенно основанные на архитектуре JET, пытаются воспользоваться одним соединением для отправки обновлений в не до конца заполненные наборы строк и терпят неудачу. К примеру, разработчики могут, используя DataReader, выполнить предложение SELECT и при прохо-

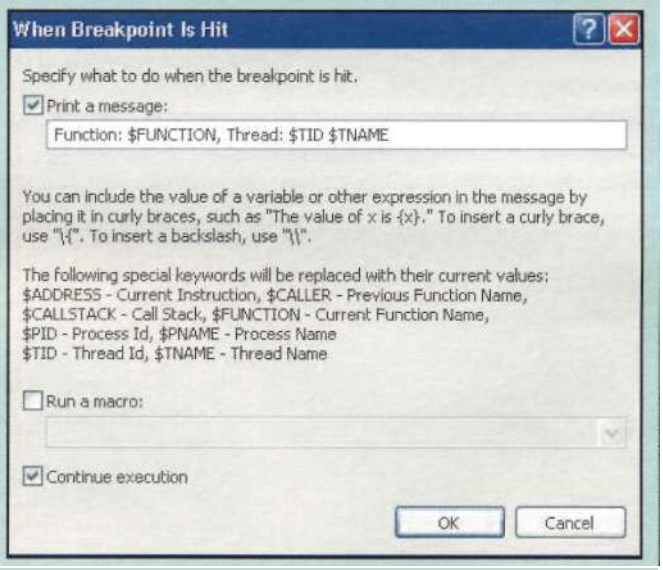
Отладка T-SQL в Visual Studio 2005

Для тех, кто занимается разработкой SQL Server, возможность работать с хранимыми процедурами дает заметный выигрыш в производительности. В предшествовавших версиям 2005 года выпусках Visual Basic и Visual Studio разработчикам приходилось быть весьма изобретательными, чтобы вообще заставить работать средства отладки T-SQL. Больше такое не повторится, ситуация исправлена. Отладчик не просто стал работать — специалисты Microsoft добавили превосходные возможности, которые облегчат отладку и настройку даже самых сложных хранимых процедур. В Visual Studio 2005 можно установить точки прерывания, которые будут срабатывать:

- на n-й раз. В этом случае можно выбрать разные варианты возникновения прерывания: когда показания счетчика будут равны, больше или равны и даже кратны заданному значению. Это значит, что можно вводить прерывания, когда известно, что за хранимой процедурой надо понаблюдать после того, как она вызывалась n раз.
- когда выполнены условия фильтра. Можно ограничить срабатывание точки прерывания только теми случаями, когда хранимую процедуру инициируют указанные процессы или потоки. Можно указывать название компьютера MachineName, идентификатор процесса ProcessID, название процесса ProcessName, идентификатор потока ThreadID, имя потока ThreadName, объединяя их в выражение операторами AND (&), OR (||) или NOT (!). К примеру, если SQL Server работает на группе серверов, то можно отлаживать хранимую процедуру, когда она запускается на определенном сервере из этой группы.

По-видимому, SQL Server 2005 не поддерживает условные точки прерывания SQL Server, так что выбрать эту возможность нельзя. Другая возможность позволяет указать, что сообщение должно появиться в отладочном окне при срабатывании точки прерывания, как показано на экране A.

Включение отладчика T-SQL также проще осуществить в Visual Studio 2005, чем в предыдущих версиях. Однако эта возможность не включена в Standard Edition, и, чтобы ею воспользоваться, понадобится Professional Edition или Team System Edition.



При отладке конкретной хранимой процедуры нужно задействовать Server Explorer, чтобы открыть эту хранимую процедуру и прийти к той ее строке, где надо прервать выполнение, точно так же, как это делается в Visual Studio 2003. Чтобы установить точку прерывания, следует щелкнуть правой кнопкой мыши на границе, как это делается для обычного кода в редакторе кода хранимой процедуры. Затем нужно открыть окно свойств приложения Application Properties (новинка Visual Studio 2005), открыть закладку Debug и выбрать режим включения отладчика Enable SQL Server debugging. Чтобы Visual Studio прервал исполнение, не надо подсоединяться к процессу, как это было в бета-версиях. При тестировании приложения Visual Studio показывает окно интерактивного редактора T-SQL, после того как хранимая процедура запущена и выполнены условия точки прерывания.

ждении по строкам попытаться исполнить предложение UPDATE через то же самое соединение. Теперь ADO.NET 2.0 и SQL Server 2005 поддерживают множественные активные результирующие наборы — Multiple Active Result Sets (MARS). Хотя мне еще только предстоит разобраться в этой возможности, видимо, специалисты Microsoft гордятся ею. MARS позволяет выполнять дополнительные операции по одному соединению (при принятии соответствующих мер предосторожности). Мне думается, что разумнее просто открыть дополнительное соединение, однако по умолчанию возможности MARS отключены, так что разработчикам предстоит самим решать, применять их или нет.

Быстрее обрабатывает данные

Справедливости ради замечу, что некоторым разработчикам действительно требуется предоставлять клиенту по 100 тыс. строк и возможность манипулировать ими в DataTable. Для таких задач специалисты Microsoft переделали способ конструирования, хранения и индексирования объектов DataTable и DataSet в ADO.NET Если в DataTable находится менее 10 тыс. строк, то разница в производительности будет не очень заметна. Но разработчики, строящие гигантские таблицы DataTable, почувствуют весьма существенное увеличение производительности — в 80 раз (так мне сказали в Microsoft). Подобное усовершенствование не должно побуждать вас загружать в оперативную память весь список абонентов МГТС. Существуют более быстрые и удобные способы обработки огромных объемов данных, такие как применение нового класса BulkCopy для импорта строк в таблицы на сервере и их обработки с помощью хранимой процедуры или даже новой процедуры на базе CLR.

Многие разработчики применяют DataReader для выборки данных, но впоследствии пользуются собственным кодом для загрузки данных в DataTable или DataSet. Сейчас в ADO.NET 2.0 классы DataTable и DataSet предоставляют метод загрузки Load, позволяющий разработчикам напрямую загружать данные в DataTable из DataReader. Можно также выделить поток Data-Reader из существующих DataSet или DataTable с помощью метода Create Reader. А это означает, что DataReader может возвращать множественные наборы строк посредством метода NextResult.

Однако предположим, что у вас спрашивают, как заставить быстрее работать приложение, предоставляющее клиенту 10 тыс. и более строк. Спрашивается, зачем? Так часто бывает, когда заказчик хочет выполнить массированную операцию, но не сознает этого. Как правило, запросы таких клиенты принимают одну из двух форм.

1. Заказчик просит произвести выборку миллиона строк, внести изменения и отправить строки обратно. Разумеется, заказчики могут не знать о существовании хранимых процедур, способных выполнить все изменения прямо на сервере за минимальное время. Таким клиентам я рекомендую почитать учебник по созданию корректных операций обновления UPDATE на сервере. Но ведь люди применяют те средства, с которыми им удобно работать.
2. Заказчик просит выбрать миллион строк из другой базы данных и переместить их в SQL Server. Иногда заказчики собираются произвести по ходу перемещения логическую обработку данных, но обычно они просто хотят импортировать множество строк из мэйнфрейма в свой офис. В прошлом я советовал в таких случаях воспользоваться DTS или программой копирования массивов (BCP). В ADO.NET 2.0 можно легко импортировать данные из любого источника с помощью класса SqlBulkCopy. Можно массированно копировать для дальнейшей обработки в SQL Server данные, демонстрируемые любым провайдером данных среды .NET: SqlClient, OLE DB, ODBC или провайдерами независимых фирм. Как только данные окажутся на сервере, клиенту стоит изменить или отфильтровать их на месте. То, что отнимало часы и даже дни с прежними версиями ADO, теперь занимает секунды или минуты с ADO.NET 2.0.

Чтобы проиллюстрировать последнее утверждение, я недавно написал приложение, применяющее MSDN Index CD, для поиска DVD в своей коллекции Universal. К сожалению, базирующемуся на Microsoft Internet Explorer (IE) поисковому механизму, который сопровождает Index CD, требуется несколько минут на самый простой поиск. Я загрузил данные MSDN Index с помощью класса ADO.NET 2.0 SqlBulkCopy, чтобы файлы .rs, неизменно базирующиеся на классическом варианте Advanced Data TableGram (ADTG), из Index CD попали в SQL Server. После того как данные были загружены, я создал подходящие индексы и смог снизить время обработки запроса с нескольких минут до менее чем пяти секунд. Операция BCP переместила около 450 тыс. строк менее чем за 30 секунд. Я также попробовал импортировать данные XML с CD, но результаты оказались неудовлетворительными — все происходило намного дольше. Похоже, XML представляет собой один из самых неэффективных (но зато самых гибких) механизмов хранения данных.

Еще одна возможность, которую никак нельзя упустить в ADO.NET 2.0, это адаптер таблиц TableAdapter. Лучше всего генерировать этот класс с помощью механизма перетаскивания интерфейса Visual Studio 2005. Класс TableAdapter спроектирован для показа новых функциональных возможностей объекта DataTable, который реализует многие методы DataSet. DataTable позволяет преобразовать в последовательную форму индивидуальный объект DataTable, применяя либо двоичный метод, либо метод XML. Добавим к этому новые механизмы связывания и элементы управления навигацией по наборам строк, и получим более мощный

инструмент построения интерактивных приложений. ASP.NET также получает поддержку от ADO.NET. К примеру, теперь можно автоматически обновлять наборы данных, которые строятся и связываются с применением новой «полностью дуплексной» технологии управления данными.

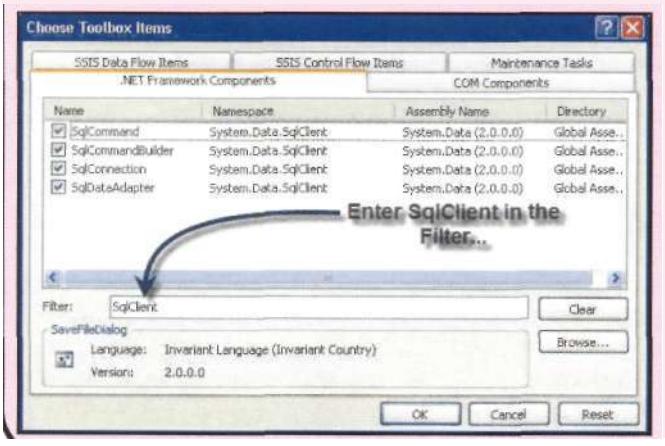
ADO.NET 2.0 может вести многозадачную обработку?

Поскольку я предвидел, что моему поисковому приложению MSDN Index иногда может требоваться много времени для выполнения сложного поиска, мне захотелось опробовать возможности нового асинхронного DataReader в ADO.NET 2.0 для вывода индикатора, показывающего прогресс при выполнении поиска. Хотя сделать это было несложно, предотвратить возникновение тупиковых ситуаций в ходе выполнения длительных запросов не удавалось. Ведь исполнение запроса и возврат набора строк образуют двухфазный процесс. При использовании в SqlClient.SqlCommand команды BeginExecuteReader для начала исполнения поискового запроса управление немедленно возвращается приложению. В этой точке можно показывать индикатор прогресса выполнения или делать что угодно для развлечения пользователей, чтобы они от скуки не нажали CTRL-ALT-DEL. Как только будет достигнуто состояние завершения IsCompleted, можно получить доступ к потоку DataReader, но ожидание на этом не заканчивается. Требуется еще возвратить найденные строки, на что может уйти значи-

Возвращение возможностей Visual Studio 2003

Microsoft заняла неожиданную позицию в отношении некоторых новых возможностей доступа к данным в Visual Studio 2005. По каким-то причинам разработчики Microsoft Visual Studio решили скрыть отдельные возможности Visual Studio, которыми многие привыкли пользоваться еще с первого выпуска Visual Studio. К примеру, в каждой книге, статье или учебном курсе по ADO.NET объясняется, как создать обновляемый набор данных DataSet с помощью мастера конфигурации адаптера данных DataAdapter Configuration Wizard (DACW). Но, запустив Visual Studio 2005, вы не найдете значка этого мастера на панели инструментов Toolbox, по крайней мере в предназначенной для просмотра членами сообщества июльской версии Community Technology Preview (CTP). Исчезли и значки мастеров команд Command и соединений Connection для каждого из провайдеров. Эти возможности в продукте по-прежнему имеются, но разработчики Microsoft скрыли их. Однако многие, как и я, по-прежнему находят применение этим средствам повышения производительности, особенно при обучении работе с ADO.NET. К счастью, их нетрудно вновь показать. Для этого нужно сделать следующее:

1. Запустить Visual Studio и создать проект Windows Forms. Проект можно создать на любом языке.
2. Зафиксировать закладку инструментария Toolbox, потому что мы собираемся создать новую закладку.
3. Щелкнуть правой кнопкой мыши ниже пунктов инструментария Toolbox и выбрать из выпадающего меню добавление закладки Add Tab. Затем нужно присвоить новой закладке какое-нибудь содержательное имя, например «Отверженные компоненты, которые Microsoft не дает мне применять»,
4. Щелкнуть правой кнопкой мыши на новой закладке, выбрать Choose Items, чтобы показать диалоговое окно выбора инструментов Choose Toolbox Items. Придется подождать, пока происходит ее инициализация,
5. Пролистать сведения в диалоговом окне до раздела провайдера доступа к данным. Для SQL Server необходимо добавить пункты из списка компонентов SqlClient. Если набрать S, указатель передвинется к первому S. Можно также ввести SqlClient в диалоговом окне фильтра Filter, чтобы найти все нужные компоненты, как показано на рис. Б. Надо просто проверить те компоненты, которые предполагается добавить в заказное меню,
6. Повторить этот процесс для компонентов ODBC и OLE DB, которые желательно показывать в инструментарии Toolbar.



Когда вы закончите, у вас должна появиться новая закладка Toolbox с компонентами ADO.NET, использованными в последних трех версиях, как показано на рис. С.

К сожалению, не все средства повышения продуктивности работы, к которым мы привыкли в Visual Studio 2003, остались в Visual Studio 2005. К примеру, когда надо было сделать быстрый вызов хранимой процедуры для построения коллекции параметров, Visual Studio 2003 позволял перетащить хранимую процедуру из Server Explorer в форму, а Visual Studio заботился об остальном. Этот метод в Visual Studio 2005 не работает. Но, как я понимаю, одно из новых добавлений может построить коллекцию параметров Parameters из хранимой процедуры, так что еще не все потеряно.

тельное время. ADO.NET не предоставляет асинхронные методы загрузки Load и заполнения Fill (что было бы прекрасно), так что придется прибегнуть к потокам BackgroundWorker. Хотя разобраться в этих потоках нетрудно, сам факт, что были опущены асинхронные Fill и Load, представляется мне досадной оплошностью. Кстати, эта новая возможность почти догоняет базирующуюся на COM версию ADO, которая также поддерживает асинхронный метод Connection Open.

Как ADO.NET 2.0 проводит обновления

В базирующемся на COM «классическом» ADO пакетные обновления были реализованы уже давно, и наконец-то в ADO.NET 2.0 тоже появилась такая возможность. Это означает, что можно будет вносить в DataTable десятки (или тысячи) изменений и при этом ADO.NET реализует эти изменения за гораздо меньшее число походов на сервер и обратно. Для поддержания этой возможности ADO.NET демонстрирует новый набор событий, которые обеспечивают высокую степень детализации при управлении операциями и возможными исключениями.

Если только от данной возможности не откажутся (а сейчас это под вопросом), ADO.NET 2.0 сможет улучшить метод, которым CommandBuilder строит исполняемые команды для выполнения параллельной обработки. Ввод нового свойства для обработки конфликтов ConflictOption в ADO.NET 2.0 позволяет выбирать между следующими вариантами: сравнением всех пригодных для поиска значений CompareAllSearchableValues (это текущая установка в ADO.NET 1.1), сравнением версий строк CompareRowVersion (эта установка проверяет версию строки и штамп времени для тестирования распараллеливания) и перезаписью изменений OverwriteChanges (она форсирует внесение изменений путем исключения оператора WHERE из предложения UPDATE). Такая дополнительная гибкость означает, что класс CommandBuilder может лучше соответствовать разным подходам управления распараллеливанием. Но трудно сказать, чем применение CommandBuilder лучше при работе со сложным синтаксисом SelectCommand.

Взаимодействие ADO.NET 2.0 и SQL Server

SQL Server 2005 Express представляет собой предложенную Microsoft замену версии MSDE. Одна из наиболее интересных возможностей ADO.NET — его способность открывать базы данных SQL Server (специально ориентированная на экземпляры SQL Server Express) простым указанием на файл .mdf базы данных SQL Server. Хотя доступ к базе данных через файлы .mdf поддерживался еще в версии ADO.NET 1.0, версия ADO.NET 2.0 теперь дает возможность в строку соединения ConnectionString помещать относительный путь к файлу .MDF, что позволяет применять эту строку вместе с настройками приложения. Кроме того, при использовании параметра User Instance=True SQL Server копирует базы данных master, model и tempdb, а также базу данных пользовательского приложения в частную область данных текущего пользователя. Подобное перемещение заметно упрощает доступ к базе данных и предотвращает повреждение совместно используемой базы данных master и других системных баз данных.

Хотя ADO.NET 2.0 все еще не поддерживает курсоры на стороне сервера, в нем реализована технология, которая гораздо лучше подошла бы многим приложениям. Представьте себе, что SQL Server инициирует возникновение события в приложении при изменении какой-либо строки в заданном наборе строк. Именно это и происходит в новом классе SqlNotificationRequest при работе со службами извещения SQL Server Notification Services. Такое мгновенное извещение позволит разработчикам обновлять данные в локальных кэшах при изменении данных на сервере. Эта технология может работать как с Windows Forms, так и с приложениями ASP.NET

ADO.NET также поддерживает все новые типы данных SQL Server, включая двоичные данные переменной длины varbinary(max), типы BLOB и CLOB, а также определенные на Common Language Runtime (CLR) пользовательские типы данных (UDT). Появился даже новый клиентский интерфейс SqlClient для применения в основанных на CLR хранимых процедурах, функциях, агрегатах и триггерах.

ADO.NET 2.0 больше не требуется стек MDAC

В прошлом разработчики и архитекторы делали глубокий вдох и надеялись на лучшее, когда объявляли о выходе новой версии стека MDAC. Они знали, что с большой вероятностью это могло разрушить некоторые из уже развернутых ими приложений. С ADO.N ET 2.0 больше не придется так беспокоиться о возможной поломке существующего кода, потому что стек MDAC (который содержит ADO на базе COM и избранные библиотеки netlib) для развертывания приложений ADO.NET не требуется. При построении приложений для среды .NET Framework исполняемые модули могут размещаться в одном каталоге, на который не оказывает влияния новый код, установленный после развертывания. Можно даже отметить избранные DLL, которые должны быть установлены и зарегистрированы в общих областях целевой системы или в кэше глобальной сборки Global Assembly Cache (GAC).

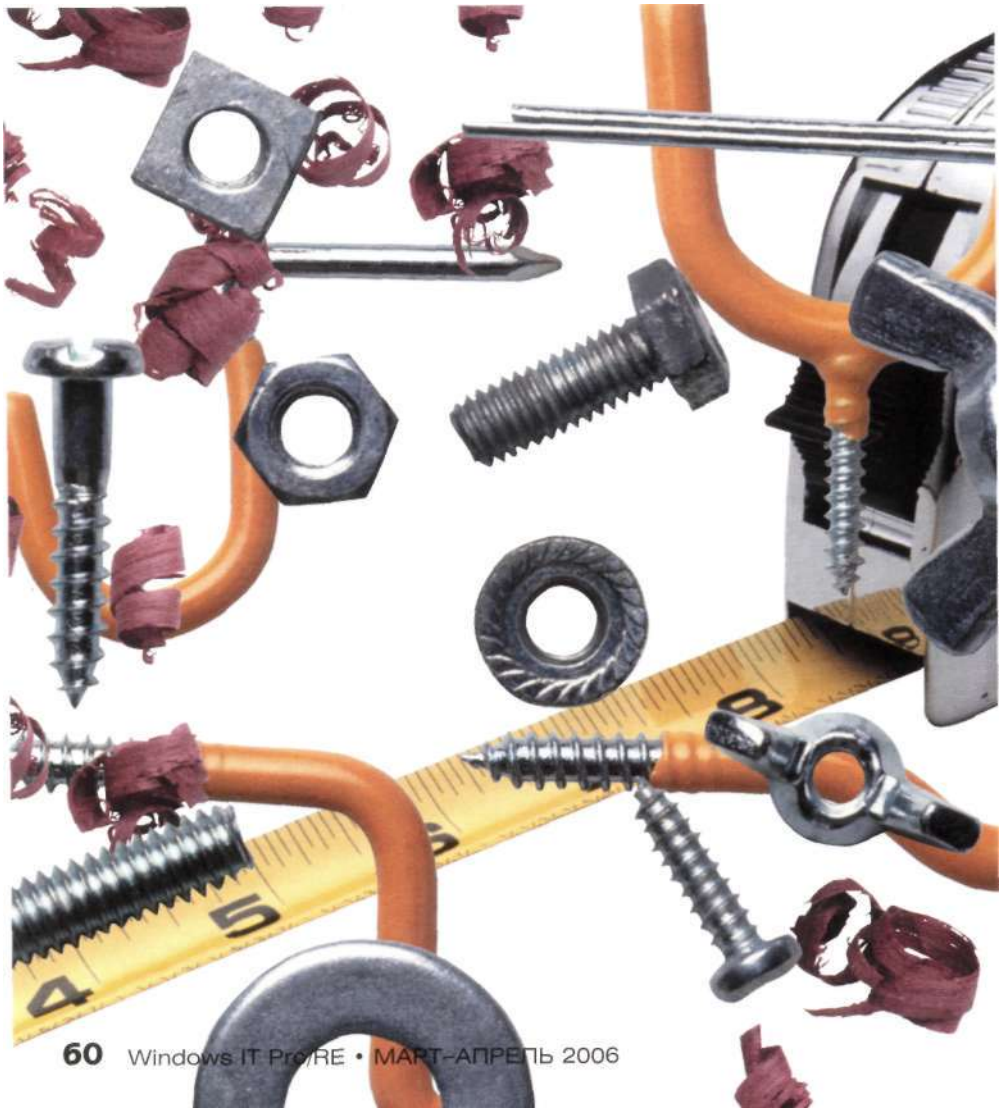
Очевидно, что специалисты Microsoft потратили немало времени на разработку новых возможностей ADO.NET 2.0 и на их интеграцию в Visual Studio и SQL Server 2005. Понятно также, что в Microsoft с особым вниманием относятся к сильно типизированным данным, связыванию данных и формированию отчетов. Эти новые возможности призваны помочь разработчикам реализовывать более эффективные, безопасные и быстродействующие проекты с меньшим объемом кода.

Легкое кодирование с SMO

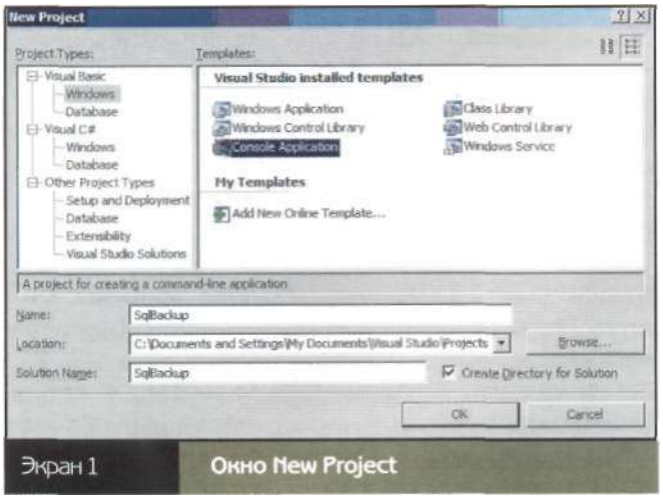
Упрощаем работу с помощью простой и эффективной модели программирования

Джон Пол Кук

Архитектор систем и баз данных из Хьюстона, Техас. Специализируется на помощи крупным компаниям и пользователям в работе с SQL Server, Oracle, и .NET Framework. Имеет несколько сертификатов Microsoft и Oracle. johnpaulcook@email.com



SQL Management Objects (далее SMO), новый программируемый уровень в SQL Server 2005, дополняет и заменяет SQL Distributed Management Objects (SQL-DMO). В этой статье я представлю SMO и покажу, как его использовать. Речь пойдет о применении Visual Studio 2005 и SMO для разработки управляемого кода и решения трех основных задач администрирования SQL Server 2005. Мы построим простое приложение для резервного копирования, доработаем его с целью облегчения использования, а затем создадим базу данных и таблицу. Основываясь на этом коде, читатели смогут задействовать его в качестве фундамента для обработки более сложных задач. SMO обеспечивает программный подход к полной объектной модели SQL Server. Любая работа, выполняемая на языке data definition language (далее DDL), теперь может выполняться на объектно-ориентированном языке управляемого кода для Common Language Runtime (CLR) (то есть .NET). Создавать приложения с помощью SMO и Visual Studio 2005 намного легче, чем



Экран 1 Окно New Project

в традиционных Notepad и SQL-DMO. Кроме того, в этой статье я покажу, каким образом возможности Visual Studio помогают уменьшить количество ошибок при программировании и повышают вероятность того, что решение правильно заработает с первого раза.

Enterprise Manager (и SQL Server Management Studio в SQL Server 2005) имеет все возможности для управления несколькими серверами, но администраторы баз данных, управляющие группой серверов, поняли, что решения, программные или на базе сценариев, при помощи SQL-DMO не только лучше выполняют работу, обеспечивая гарантию и повторяемость результатов, но и не требуют вмешательства оператора.

SMO предлагает большую производительность и масштабируемость, чем SQL-DMO. SQL-DMO остается в SQL Server 2005 только для обратной совместимости. SMO дает полный доступ ко всем свойствам SQL Server 2005. SMO можно использовать для управления SQL Server 2000 и SQL Server 7.0. К тому же, поскольку SMO выполнен как управляемый код CLR, можно легко и быстро разрабатывать устойчивые решения, использующие объектно-ориентированное программирование.

Несмотря на то что существует возможность использования любого текстового редактора для написания управляемого кода, Visual Studio 2005 предлагает высокопроизводительную среду для быстрого прикладного программирования. Visual Studio 2005 ускоряет разработку приложений SMO, поскольку располагает стандартными шаблонами, такими как шаблоны для приложений Windows Forms, для ASP.NET Web Form и Web-служб, консольных приложений и служб Windows. Если использовать шаблон для разработки приложений SMO, на кодирование тратится меньше усилий, потому что в шаблоне есть написанный заранее «примерный» код, который связывает части приложения друг с другом.

Я надеюсь, что читатели уже знакомы с какой-либо версией Visual Studio и SQL Server. Тем более неплохо было бы знать, как использовать Visual Studio для разработки простых приложений Windows. Примеры в этой статье созданы в Visual Basic .NET и C#, но если читатели раньше работали с Visual Basic, C++ или Java, все должно быть понятно.

Основы объектно-ориентированной модели программирования

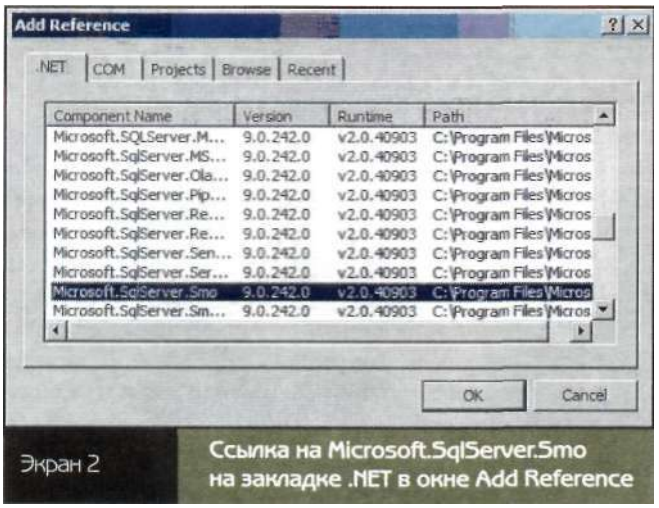
Прежде всего коротко рассмотрим некоторые определения в терминологии объектно-ориентированного программирования. Библиотека — это совокупность классов. Класс — описание объекта. Объект — экземпляр класса. Например, проект дома — это класс (абстракция), адом, построенный по проекту, — это объект. Почти так же, как и дом, объект «сделан из проекта». Объект должен обрабатываться (создаваться) из класса. Каждый объект — это определенный экземпляр класса. Класс имеет свойства, методы и события, которые доступны для использования объектами, создаваемыми из этого класса. Все свойства, методы и события объекта определены классом. Свойство — это признак, который определяет или описывает объект. Например, некоторые из многих свойств объекта базы данных — это имя, размер и дата создания. Методы, такие как create, alter, drop и grant, являются операциями, связанными с

Листинг 1 Код SqlBackup на Visual Basic .NET

```
Imports Microsoft.SqlServer.Management.Smo ' Allow shorthand notation
Module Module1
  Sub Main()
    Dim db As String = «AdventureWorks» ' Define and set a variable
    Dim bck As New Backup() ' Instantiate a Backup object
    bck.Action = BackupActionType.Database ' Set Action property
    bck.BackupSetName = db & «_BackupSet» ' Set BackupSetName property
    bck.Database = db ' Set Database name property
    bck.DeviceType = DeviceType.File ' Set DeviceType property
    ' Add method adds file to Devices collection
    bck.Devices.Add(«C:\» + db + «.bak»)
    Dim s2k5 As New Server() ' Instantiate a Server object
    bck.SqlBackup(s2k5) ' Invoke Backup object's SqlBackup method
  End Sub
End Module
```

Листинг 2 Код SqlBackup на C#

```
#region Using directives
using Microsoft.SqlServer.Management.Smo; // Allow shorthand notation
#endregion
namespace SqlBackup
{
 class Program
 {
  static void Main(string[] args)
  {
   string db = «AdventureWorks»; // Define and set a variable
   Backup bck = new Backup(); // Instantiate a Backup object
   bck.Action = BackupActionType.Database; // Set Action property
   bck.BackupSetName = db + «_BackupSet»; // Set BackupSetName property
   bck.Database = db; // Set Database name property
   bck.DeviceType = DeviceType.File; // Set DeviceType property
   // Add method adds file to Devices collection
   // Must escape the backslash in C#
   bck.Devices.Add(«C:\\» + db + «.bak»);
   // Instantiate a Server object and
   // invoke Backup object's SqlBackup method
   bck.SqlBackup(new Server());
  }
 }
}
```



Экран 2 Ссылка на Microsoft.SqlServer.Smo на закладке .NET в окне Add Reference

объектом. События — это случаи, которые перехватываются объектом и могут использоваться, чтобы вызвать действие. Например, щелчок по кнопке в форме Windows вызывает событие Button Click. Требуется написать собственный код, чтобы обработать событие и предпринять некоторое действие, например восстановление предшествующего состояния базы данных. Эти принципы объектно-ориентированного программирования можно будет видеть в примерах данной статьи. Я объясню некоторые концепции объектно-ориентированного программирования немного позже, а сейчас приступим к созданию приложения для резервного копирования.

Построение приложения при помощи SMO

Мы начнем с построения приложения для резервирования базы данных AdventureWorks, новой базы данных, содержащей примеры SQL Server 2005. При наличии разнообразных инструментов для администраторов баз данных и трехуровневых приложений для резервного копирования напрашивается вопрос: зачем тратить время на программирование приложения, резервирующего базу данных? Представим реальную ситуацию, которая включает требования по загрузке данных при операциях между компаниями. В случае сбоев при загрузке данных необходимо автоматически вернуть базу данных в то состояние, в котором она была непосредственно перед загрузкой. Дело осложняется тем, что нет возможности заранее спланировать копирование, так как данные могут поступать от деловых партнеров в любое время. SMO позволяет разработать полностью автоматизированное решение, которое резервирует базу данных немедленно, после того как получаемые данные будут загружены

Начнем с запуска Visual Studio 2005. Нужно открыть меню и выбрать File, New, Project. Когда появится диалоговое окно New Project, следует выбрать Project Type и Template, то есть шаблон для проекта, как показано на экране 1, затем щелкнуть OK. Для этого примера я выбрал шаблон Console Application (как и sqlcmd и osql, он запускается в командном окне), поскольку он требует минимального количества кода для демонстрации объектно-ориентированного программирования при использовании библиотеки классов .NET Framework 2.0 (SMO — это часть .NET Framework 2.0). В дальнейшем, когда приложение для резервирования базы данных будет усовершенствовано, будет использоваться шаблон Windows Application, так как потребуется пользовательский интерфейс с широкими возможностями. Шаблон Windows Service является подходящим вариантом в том случае, когда от приложения требуется работа в фоновом режиме, как службы.

Добавим ссылку на Microsoft.SqlServer.Smo, то есть на библиотеку классов CLR. Нужно зайти в меню Project и выбрать Add Reference. В диалоговом окне Add Reference, которое показано на экране 1, следует щелкнуть на закладке .NET, выбрать Microsoft.SQLServer.Smo, затем щелкнуть OK. Появится окно с несколькими строками кода, которые предоставляет шаблон Console Application. Необходимо удалить весь исходный код в окне, затем вставить код Visual Basic .NET, который показан в листинге 1, или код C# в листинге 2. Это весь код, необходимый для резервирования базы данных AdventureWorks. Все просто.

Заметим, что несохраненные изменения отмечены желтым цветом в крайнем левом поле окна кода. Можно сохранить изменения сейчас, но это не обязательно. При запуске приложения Visual Studio 2005 автоматически сохраняет изменения, и желтые отметки меняются

Листинг 3 Код VerifiedBackup на Visual Basic .NET

```
Imports Microsoft.SqlServer.Management.Smo
Public Class Form1
  Private Sub Form1_Load(ByVal sender As System.Object, _
          ByVal e As System.EventArgs) Handles MyBase.Load
    Dim s2k5 As New Server()
    For Each db As Database In s2k5.Databases ' Loop through the databases
      Databases.Items.Add(db.Name) ' Add database name to the ListBox
    Next
  End Sub
  Private Sub DoBackup_Click(ByVal sender As System.Object, _
          ByVal e As System.EventArgs) Handles DoBackup.Click
    ' Get database name from the ListBox
    Dim db As String = Databases.SelectedItem.ToString()
    Dim dbBck As String = «C:\» & db & «.bak»
    Dim bck As New Backup() ' Instantiate a Backup object
    bck.Action = BackupActionType.Database ' Set Action property
    bck.BackupSetName = db & «_BackupSet» ' Set BackupSetName property
    bck.Database = db ' Set Database name property
    bck.DeviceType = DeviceType.File ' Set DeviceType property
    ' Add method adds file to Devices collection
    bck.Devices.Add(dbBck)
    Dim s2k5 As New Server() ' Instantiate a Server object
    bck.SqlBackup(s2k5) ' Invoke Backup object's SqlBackup method
    Dim rst As New Restore() ' Instantiate a Restore object
    rst.DeviceType = DeviceType.File ' Set DeviceType property
    ' Add method adds file to Devices collection
    rst.Devices.Add(dbBck)
    If rst.SqlVerify(s2k5) Then ' Similar to VERIFY RESTOREONLY
      MessageBox.Show(db & « backup verified»)
    Else
      MessageBox.Show(db & « backup error»)
    End If
  End Sub
End Class
```

Экран 3 IntelliSense показывает детали объекта SqlBackup

на зеленые. Но перед запуском приложения SQLBackup я рекомендую сначала изучить и осмыслить код. Примеры в листингах 1 и 2 иллюстрируют несколько важных концепций объектно-ориентированного программирования.

Приложение в Visual Studio 2005 запускается так же, как запрос в SQL Server 2000 Query Analyzer. Запуск начинается со щелчка на значке Start (зеленый треугольник) или нажатия кнопки F5. Окно Console появляется при запуске приложения, и, когда оно исчезает (примерно через минуту), резервная копия базы данных готова.

Для подтверждения того, что резервный файл базы данных был создан с именем C:\AdventureWorks.bak, можно использовать Windows Explorer.

Некоторые разъяснения концепций

Мы начали с предложения Imports в тексте кода Visual Basic .NET в листинге 1 или с предложения using в коде C# в листинге 2. Добавление этих предложений в начало кода позволяет использовать укороченную нотацию. Несмотря на то что это предложение технически необязательное, оно рекомендуется для обеспечения скорости и аккуратности. Например, если предложение опустить, придется ввести строку BackupActionType.Database as Microsoft. SqlServer. Management.Smo.BackupActionType.Database.

Необходимо использовать конструктор объекта (метод New в Visual Basic .NET или новый метод в C#) для создания (инициализации) реального объекта как выделенного из абстрактного определения, которое имеется в библиотеке класса (такой, как библиотека классов SMO). Конструктор, имеющий более одной формы, называется перезагруженным. Каждая форма перезагруженного конструктора имеет свою сигнатуру, иначе говоря, каждый конструктор имеет уникальный набор параметров. Функция IntelliSense Visual Studio помогает решить, какую перезагрузку применить, показывая все варианты перезагрузки конструктора.

В объектно-ориентированном программировании после создания экземпляра объекта обычно задаются некоторые из свойств объекта. Это несложное приложение для резервирования базы данных устанавливает четыре свойства: тип резервирования, имя набора копирования, название базы данных для копирования и тип устройства резервирования. Нужно вызывать методы объекта, чтобы подвигнуть объект на совершение действия. Наше приложение использует метод Add объекта Backup для добавления полного имени резервного файла в набор элементов Backup. Объекту Server предписано установить соединение. Последний шаг вызывает метод SqlBackup объекта Backup, чтобы выполнить реальное копирование.

Преимущества Visual Studio 2005

Visual Studio обеспечивает две возможности, которые существенно повышают скорость и качество программирования: IntelliSense и контекстно-зависимая под-

Листинг 4 Код VerifiedBackup на C#

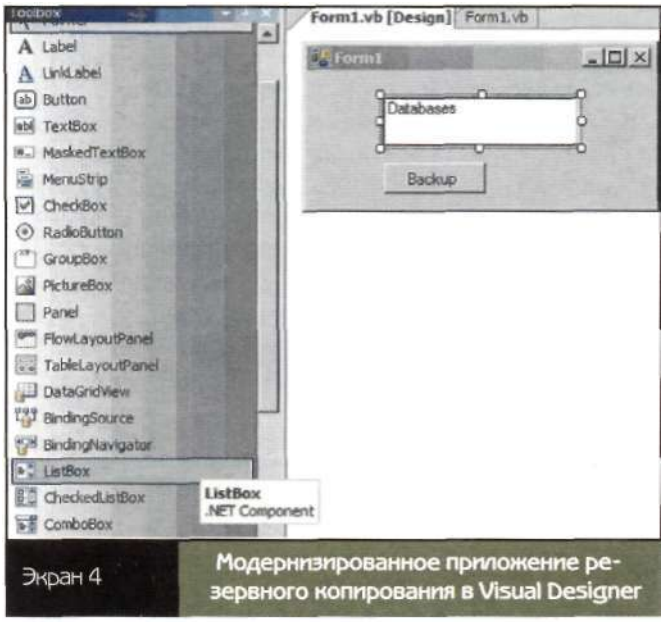
```
#region Using directives
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Windows.Forms;
using Microsoft.SqlServer.Management.Smo;
#endregion
namespace VerifiedBackup
{
 partial class Form1 : Form
 {
  public Form1()
  {
   InitializeComponent();
  }

  private void Form1_Load(object sender, EventArgs e)
  {
   Server s2k5 = new Server();
   foreach (Database db in s2k5.Databases) // Loop through the databases
   {
    Databases.Items.Add(db.Name); // Add database name to the ListBox
   }
  }
  private void DoBackup_Click(object sender, EventArgs e)
  {
   // Get database name from the ListBox
   string db = Databases.SelectedItem.ToString();
   string dbBck = «C:\\» + db + «.bak»; // Must escape the backslash in C#
   Backup bck = new Backup(); // Instantiate a Backup object
   bck.Action = BackupActionType.Database; // Set Action property
   bck.BackupSetName = db + «_BackupSet»; // Set BackupSetName property
   bck.Database = db; // Set Database name property
   bck.DeviceType = DeviceType.File; // Set DeviceType property
   // Add method adds file to Devices collection
   // Must escape the backslash in C#
   bck.Devices.Add(dbBck);
   // Instantiate a Server object and
   // invoke Backup object's SqlBackup method
   Server s2k5 = new Server();
   bck.SqlBackup(s2k5);
   Restore rst = new Restore(); // Instantiate a Restore object
   rst.DeviceType = DeviceType.File; // Set DeviceType property
   // Add method adds file to Devices collection
   rst.Devices.Add(dbBck);
   if (rst.SqlVerify(s2k5))
   { // Similar to VERIFY RESTOREONLY
    MessageBox.Show(db + « backup verified»);
   }
   else
   {
    MessageBox.Show(db + « backup error»);
   }
  }
 }
}
```

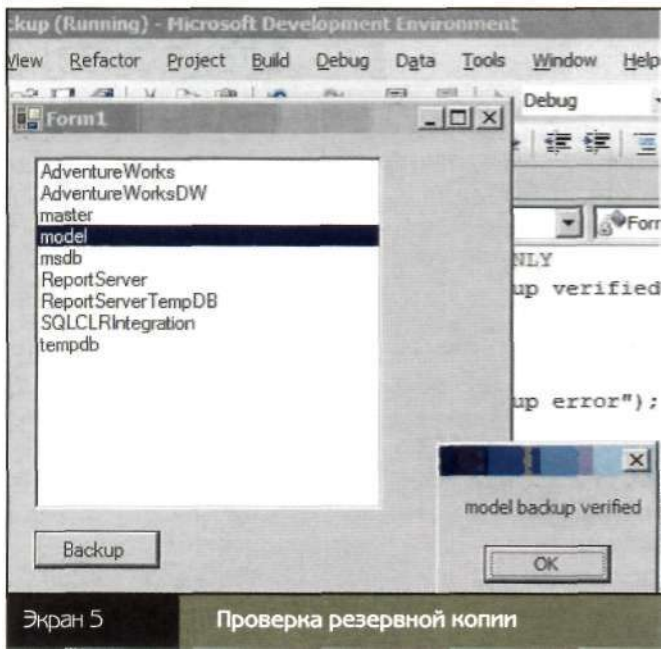
сказка. IntelliSense значительно упрощают разработку кода, если сравнивать с написанием сценариев SQLDMO в Notepad. В процессе кодирования текста IntelliSense обеспечивает перечень и краткое описание свойств и методов объекта SQLBackup, как показано на экране 3. Чтобы получить контекстную подсказку о коде, в котором находится курсор, нужно нажать клавишу F1.

Модернизация SMO Backup

Наше приложение создает резервную копию базы данных, однако у него есть два явных недостатка: имя базы данных жестко запрограммировано и отсутствует возможность проверки резервной копии. Для устранения этих недостатков необходимо немного модернизировать приложение, предоставив пользователю возможность выбора имени базы данных из списка, и проверить резервную копию, создавая экземпляр объекта Restore и вызывая метод Verify.



Экран 4 Модернизированное приложение резервного копирования в Visual Designer



Экран 5 Проверка резервной копии

Освоив основы разработки приложения при помощи Visual Studio 2005, создадим приложение, которое имеет пользовательский интерфейс Windows. Приложения Windows требуют значительного большего объема кода, чем приложения консоли. При разработке нового проекта будет использоваться шаблон Windows Application. Visual Studio 2005 автоматически добавляет необходимый для проекта дополнительный код. В отличие от ранних версий Visual Studio, Visual Studio 2005 сохраняет автоматически разработанный код в отдельном от написанного пользователем кода файле. В Visual Basic .NET этот файл называется formname.Designer.vb. В C#, он носит название formname.Designer.cs. Файл по умолчанию скрыт. Чтобы увидеть файл в Solution Explorer, нужно выбрать режим Show All Files. Код в файле Designer не придется изменять вручную, он изменится автоматически, когда в форму добавятся новые элементы управления. Код, написанный пользователем, включен либо в файл fbrmname.vb, либо в formname, cs. Если оставить имя формы по умолчанию, Forml, файл с кодом будет называться Forml.vb или Forml.cs.

В Visual Studio 2005 в меню выберем File, New, Project. Затем нужно указать шаблон Windows Application для предпочитаемого языка. Выберем Verified Backup как имя проекта. Visual Designer появляется вместе с пустым объектом Form. Используя Toolbox, переместим элемент Button и элемент ListBox в форму. Используя окно Properties, присвоим элементу ListBox имя Databases, а элементу Button имя DoBackup с помощью свойства Text в Backup. Как и в предыдущем примере, добавим ссылку на Microsoft.SqlServer.Smo. Кроме того, нужно добавить ссылку на Microsoft.SqlServer.Connectionlnfb. Дважды щелкнем на элементе Button для создания программы обработки события для кнопки и для того, чтобы переключиться в режим просмотра кода Code View. Экран теперь должен выглядеть так, как показано на экране 4.

Затем можно создать более удобное приложение для резервного копирования, предоставив пользователю перечень имен баз данных для выбора. Улучшим приложение SqlBackup добавлением кода в обработчик события Form Load, который будет заполнять объект ListBox именами баз данных на сервере. При копировании базы данных теперь пользователь может просто выбрать базу данных из списка и нажать Backup. Наконец, для того чтобы проверить копию, добавим объект Restore, а чтобы предоставить пользователю возможность проверки состояния резервной копии — управляющий элемент MessageBox. В листингах 3 и 4 показано, как это сделать.

Как и ранее, можно заменить весь код в Forml.vb на код листинга 3 или заменить код в Forml .cs на код листинга 4. Сначала требуется дважды щелкнуть на управляющем элементе Form и управляющем элементе Button для регистрации обработчиков событий в файле

Листинг 5 Код CreateTable на Visual Basic .NET

```
Imports Microsoft.SqlServer.Management.Smo ' Allow shorthand notation
Module Module1
  Sub Main()
    Dim s2k5 As New Server() ' Instantiate a Server object
    ' Instantiate a Database object and set the database name
    Dim db As New Database(s2k5, «SqlMag»)
    db.Create() ' Create the database using the Create method
    Dim tab As New Table(db, «DemoTable»)
    ' Instantiate a Column object and set its name and datatype
    Dim col1 As New Column(tab, «Quantity», DataType.Int)
    col1.Nullable = False ' Make the column NOT NULL
    tab.Columns.Add(col1) ' Add the column to Columns collection
    Dim chk1 As New Check(tab, «DemoTable_Quantity_chk»)
    chk1.Text = «Quantity > 0» ' Allow only a quantity > 0
    tab.Checks.Add(chk1) ' Add check constraint to Checks collection
    Dim col2 As New Column(tab, «TypeCode», DataType.NChar(2))
    tab.Columns.Add(col2)
    tab.Create()
  End Sub
End Module
```

Листинг 6 Код CreateTable на C#.

```
#region Using directives
using Microsoft.SqlServer.Management.Smo; // Allow shorthand notation
#endregion
namespace CreateTable
{
 class Program
 {
  static void Main(string[] args)
  {
   Server s2k5 = new Server(); // Instantiate a Server object
   // Instantiate a Database object and set the database name
   Database db = new Database(s2k5, «SqlMag»);
   db.Create(); // Create the database using the Create method
   Table tab = new Table(db, «DemoTable»);
   // Instantiate a Column object and set its name and datatype
   Column col1 = new Column(tab, «Quantity», DataType.Int);
   col1.Nullable = false; // Make the column NOT NULL
   tab.Columns.Add(col1); // Add the column to Columns collection
   Check chk1 = new Check(tab, «DemoTable_Quantity_chk»);
   chk1.Text = «Quantity > 0»; // Allow only a quantity > 0
   tab.Checks.Add(chk1); // Add check constraint to Checks collection
   Column col2 = new Column(tab, «TypeCode», DataType.NChar(2));
   tab.Columns.Add(col2);
   tab.Create();
  }
 }
}
```

кода Visual Designer. Следует убедиться, что для Form, ListBox и Button используются управляющие имена Forml, Databases и DoBackup, в соответствии с текстом примеров этой статьи. Нельзя забывать и о том, что C# является языком, чувствительным к регистру, поэтому doBackup и DoBackup представляют различные объекты.

Для упрощения кодирования и для того, чтобы избежать ошибок, можно загрузить готовое решение и работать с ним. После загрузки кода следует дважды щелкнуть на файлах vbproj или csproj для загрузки в Visual Studio 2005. В установках файла могут появиться сообщения об ошибке, такие как The automatically saved settings file '%user_documents%\visualstudio\settings\visualstudio\8.0\currentsettings.vssettings' cannot be found. Нужно нажать OK. Эти сообщения можно игнорировать, так как Visual Studio создает данные установки, когда проект загружается в Visual Studio.

Теперь запустим модернизированное приложение для резервного копирования. Следует нажать F5 или значок Start (зеленый треугольник). Выберите базу данных, затем щелкните Backup. Как показано на экране 5, когда копия готова, появляется окно, показывающее статус копии. В третьем примере будет показано, как, используя SMO, создать базу данных и таблицу.

Разработка базы данных и таблицы с помощью SMQ

Много лет разработчики баз данных использовали программный код для автоматического создания таблиц. Общий подход заключался в создании строки, состоящей из предложения T-SQL, CREATE TABLE, которое посылается на исполнение серверу базы данных. SMO предлагает более ясный, удобный объектно-ориентированный способ разработки объектов баз данных прямо в тексте программы, без использования в качестве посредника T-SQL.

В листингах 5 и 6 показано, как создать новую базу данных и таблицу полностью в тексте программы, без написания каких-либо предложений на T-SQL. Мы используем объект Database для создания базы данных и объект Table — для составления таблицы. Чтобы сохранить простоту программирования, следует выбрать шаблон Console Application и назвать его CreateTable. Можно добавить код к другим шаблонам, в зависимости от типа выбираемого пользовательского интерфейса. Затем добавим ссылки на Microsoft. Sql Server. Smo и на Microsoft.SqlServer.Connectionlnfo. Теперь запустим приложение. Необходимо использовать SQL Server Management Studio для проверки вновь созданных баз данных и таблиц. Если SQL Server Management Studio уже запущен, возможно, понадобится сначала щелкнуть на значке Refresh в Object Explorer.

Используйте преимущества SM0

Как было показано на трех примерах, программировать при помощи SMO и Visual Studio 2005 просто и удобно. SMO и Visual Studio 2005 предлагают администраторам баз данных и разработчикам непревзойденную гибкость при создании многочисленных приложений для работы с базой данных, а кроме того, обеспечивают снижение сложности и времени разработки с более высокой производительностью, лучшей масштабируемостью и большим количеством свойств, чем SQL-DMO. SMO в SQL Server 2005 также имеет обратную совместимость с SQL Server 2000 и SQL Server 7.0.

Аутентификация доступа в Internet с использованием сервера ISA

Защита и разграничение клиентского доступа в *Internet*

Леон Брагинский
Технический руководитель Microsoft Developer Support. Соавтор книги Microsoft Internet Information Server и автор статей в MSDN Magazine.
leonbrag@braginski.com

Наиболее известной проблемой обеспечения безопасности при работе с Internet является защита сети от вторжений извне. Для этого используется контролируемый доступ в Internet. Чтобы предоставить определенным пользовательским учетным записям доступ в Internet через proxy-сервер, можно задействовать Microsoft Internet Security and Acceleration (ISA) Server 2000. Сервер ISA не только помогает защитить внутренних клиентов от внешних атак, но и предоставляет возможность контроля и управления активностью пользователей в Internet. Сервер ISA поддерживает доступ к внутренним серверам извне (reverse proxy), но в этой статье такая возможность не рассматривается.

Для иллюстрации затронутых в статье вопросов я использовал упрощенную сетевую топологию. Она включает один сервер Windows 2000 с Service Pack 3 (SP3) с установленным на нем ISA Server Enterprise Edition. Он обеспечивает функции proxy-сервера и сетевого экрана (брандмауэра). Такая конфигурация предпочтительна для сети небольшого офиса. На рис. 1 изображена подобная сеть, состоящая из сервера ISA (ISA-Leon), клиентской системы (Alpha, IP-адрес 10.0.0.2) и внешнего Web/FTP сервера (Leonbr-Hm, IP-адрес 192.168.154.1). Система, на которой работает сервер ISA, имеет два сетевых интерфейса, один из них (IP-адрес 10.0.0.1) подключен к внутренней сети, а другой (IP-адрес 192.168.154.20) — к внешней, т. е. к Internet.

Версии и режимы

Сервер ISA выпускается в двух версиях: корпоративной и стандартной (enterprise и standard). ISA Server Enterprise Edition позволяет запускать сервер ISA как в режиме выделенного (standalone) сервера, так и в режиме логического объединения нескольких серверов ISA в один массив (создать массив можно и на одном компьютере, но это не даст каких-либо преимуществ). Конфигурация в виде массива поддерживает корпоративные административные политики, т. е. изменения, сделанные на одной из систем массива, распространяются на все системы массива, так что отпадает необходимость вносить такие же изменения на каждой системе. Можно создать несколько массивов для поддержки многоуровневых политик и прав доступа. Кроме того, можно передавать право управления массивами другим пользователям и группам. Enterprise Edition интегрируется с Active Directory (AD) и сохраняет конфигурационные данные массива серверов ISA в AD, в отличие от выделенного сервера ISA, конфигурация которого сохраняется в системном реестре. Когда Enterprise Edition устанавливается в сети, где отсутствует AD, сервер ISA становится выделенным сервером. Enterprise Edition масштабируется на любое число процессоров. ISA Server Standard Edition поддерживает не более четырех процессоров. Для упрощения я использую в тестовой сети ISA Server в режиме выделенного сервера, не интегрированного в AD.

Клиенты

Сервер ISA поддерживает три типа клиентов: Secure Network Address Translation (SecureNAT) — клиент, обеспечивающий трансляцию сетевых адресов; клиент брандмауэра и клиент Web Proxy. Я настроил для теста клиента брандмауэра и Web Proxy. Рассмотрим свойства каждого из клиентов более подробно.

Клиент SecureNAT

Для клиентов SecureNAT сервер ISA играет роль устройства NAT, т. е. устройства, принимающего пакеты из внутренней сети и выполняющего трансляцию сетевых адресов при их передаче вовне. В пакетах, предназначенных для передачи за пределы внутренней сети, сервер ISA изменяет IP-адрес системы-отправителя на внешний IP-адрес сервера ISA. Например, если я настрою свою учебную сеть на поддержку клиентов SecureNAT, то, когда система Alpha будет посылать запрос Leonbr-Hm, тот идентифицирует запрос как пришедший с IP-адреса 192.168.154.20 (т. е. адреса внешнего сетевого интерфейса сервера ISA Leon). Весь процесс незаметен для клиента и не требует какого-либо дополнительного программного обеспечения на клиентской системе. По этой причине такой клиент работает на системах с любыми типами сетевых операционных систем. Единственное требование — необходимо настроить на клиентской системе адрес шлюза по умолчанию так, чтобы это был адрес внутреннего сетевого интерфейса сервера ISA. Если клиенты настроены на получение IP-адреса через DHCP, то можно настроить DHCP-сервер на выдачу клиентам корректного адреса шлюза по умолчанию. Если внутренняя сеть имеет множество подсетей, связанных маршрутизаторами, необходимо в конфигурации оконечного маршрутизатора указать адрес шлюза по умолчанию, соответствующий адресу внутреннего сетевого интерфейса сервера ISA.

Клиенты SecureNAT ответственны за разрешение имен, поэтому во внутренней сети должен быть доступен сервер DNS для разрешения адресов Internet. Можно указать внутренним клиентам внешний сервер DNS и создать на системе с сервером ISA специальные правила, разрешающие DNS-запросам проходить к внешнему серверу DNS и получать от него ответы. Но если клиентам необходимо разрешать как внутренние, так и внешние адреса, требуется установить локальный сервер DNS, который будет разрешать внутренние адреса и передавать запросы к внешним адресам на внешние серверы DNS.

Клиент SecureNAT не запускает какого-либо специального программного обеспечения, и поэтому сервер ISA не может определить, какие пользователи запрашивают внешние соединения, так что вы не сможете применять на сервере ISA политики безопасности, основанные на именах пользователей. Если настроить сервер ISA так, чтобы он требовал авторизации, все запросы клиентов SecureNAT будут запрещены. Также, если протокол уровня приложений, например FTP, требует создания вторичного соединения, придется использовать специальный прикладной фильтр. Сервер ISA поставляется с набором таких фильтров, но администратору, возможно, понадобится написать фильтр, если протокол, который требует открытия вторичного соединения, не попадает в этот список. И, поскольку пакеты не содержат IP-адреса источника, приложения, например Distributed COM (DCOM), базирующиеся на корректном IP-адресе источника, не будут работать с клиентом SecureNAT.

Клиент брандмауэра

Клиент брандмауэра должен запускать специальное программное обеспечение, ISA Server Firewall Client. Во время установки сервера ISA создается каталог \%program-files%\microsoft isa server\clients, содержащий все программные и конфигурационные файлы, необходимые для установки клиента. Для настройки клиента брандмауэра используется оснастка ISA Management\Client Configuration, запускаемая из Microsoft Management Console (MMC). ISA Server распространяет эти установки на все системы, использующие клиента брандмауэра. Это программное обеспечение сервер ISA использует в качестве провайдера уровня сокетов Windows (Winsock Layered Service Provider). Клиент принимает все запросы от приложений, использующих сокеты, и передает их на систему с запущенным на ней сервером ISA. В результате все приложения во внутренней сети, использующие сокеты, работают так, как будто они непосредственно подключены к Internet.

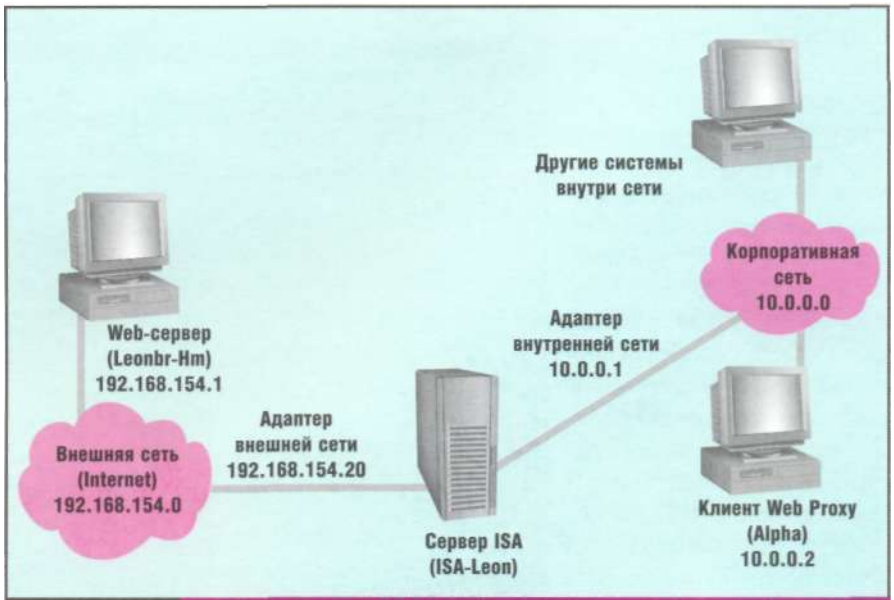
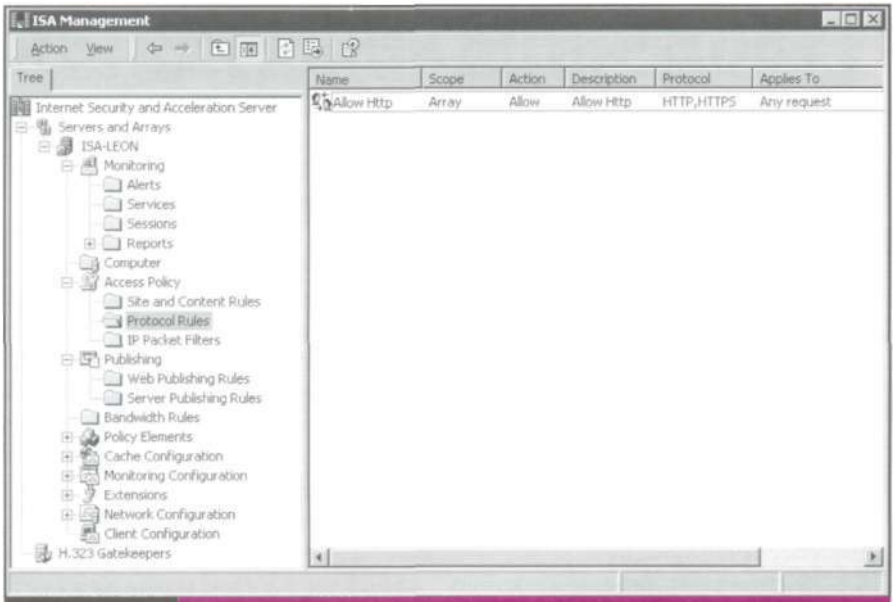


Рисунок 1 Пример сети с ISA Server



Экран 1 Консоль ISA Management в режиме Advanced

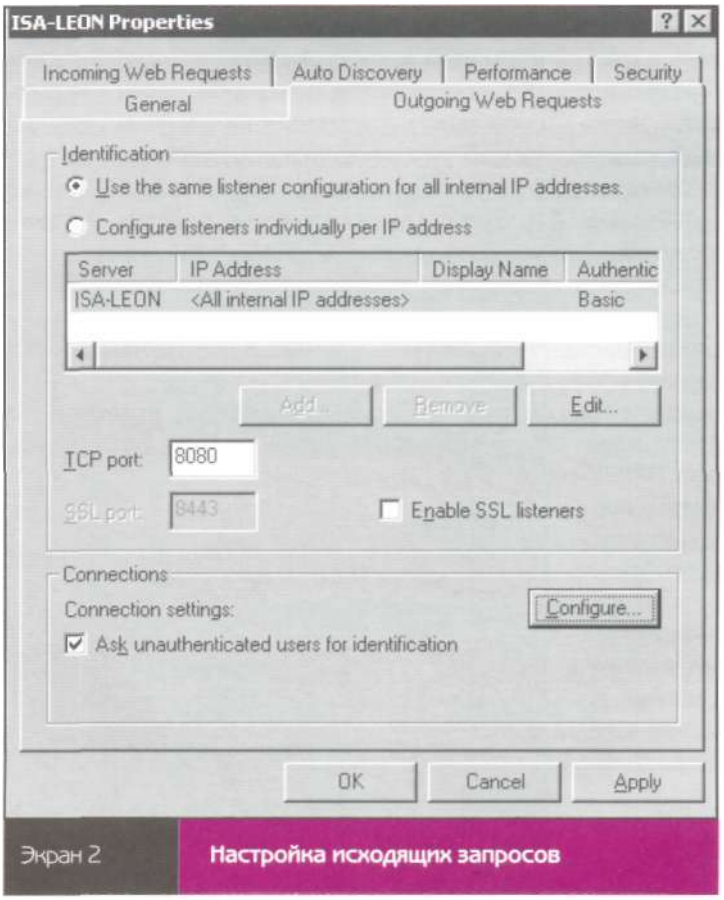
После установки этого программного обеспечения на клиентских системах пользователи, в частности, смогут запускать ftp.exe из командной строки и получать доступ к внешним FTP-сайтам.

У клиента брандмауэра разрешение имен устроено просто. По умолчанию ISA Server разрешает все имена, содержащие точки (например, www.braginski.com); имена без точек разрешаются локально. Для изменения настроек разрешения имен можно задействовать оснастку ISA Management.

Запрос клиента брандмауэра содержит имена пользователей, поэтому можно применять политики доступа, базирующиеся на именах пользователей. Однако запросы выполняются в контексте текущего пользователя, и клиентское программное обеспечение не имеет механизма для запроса у пользователей другого имени и пароля, если имя и пароль зарегистрированного пользователя неправильны. Поэтому, если запретить пользователю выход за пределы сетевого экрана, попытка выйти в Internet приведет к ошибке без предложения ввести другое имя и пароль.

Клиент Web Proxy

Использование клиента Web Proxy — наиболее простой путь обеспечить пользователям доступ в Internet. Чтобы его настроить, необходимо в настройках Web-браузера пользователя в качестве proxy-сервера указать адрес или имя сервера ISA. Клиент Web Proxy не может применять FTP-приложения командной строки. Чтобы преодолеть это ограничение, можно настроить клиента Web Proxy на использование клиента брандмауэра, который поддерживает все сетевые приложения. Как и сервер ISA, он имеет соответствующие фильтры приложений, которые поддерживают необходимые вторичные соединения. Клиенты в моем примере сконфигурированы как клиенты Web Proxy и брандмауэра.



Экран 2 Настройка исходящих запросов

Установка

При установке сервера ISA самое главное — определить, какой сетевой интерфейс находится во внутренней сети. Сервер ISA основывает все свои решения (например, предоставить ли клиенту доступ к внутренним системам либо обеспечить доступ за пределами внутренней сети) на локальной таблице адресов, Local Address Table (LAT), которая определена для внутреннего сетевого интерфейса. Во время установки можно выбрать диапазон IP-адресов внутренней сети. Проще всего выбрать режим создания таблицы, Construct Table, который открывает диалоговое окно Local Address Table. После того как администратор выберет сетевой интерфейс, подключенный к внутренней сети, и нажмет OK, программа установки сервера ISA извлекает информацию об IP-адресах из таблицы маршрутизации Windows 2000 и заполняет LAT из диапазона внутренних IP-адресов. Впоследствии можно доба-

вить или удалить IP-адреса из этого диапазона.

Управление

Сервер ISA управляется через оснастку ISA Management, которая поддерживает окна управления двух типов: Taskpad View (представление панели задач) и Advanced View (расширенное представление). Я предпочитаю расширенное представление, показанное на экране 1. Оно логически организует все компоненты сервера ISA в соответствующих папках, находящихся под системным объектом «сервер ISA». Назначение этих папок описано во врезке «Папки управления сервером ISA».

Настройка

Настройка сервера ISA для выделенных систем и для систем, являющихся частью массива, похожа. Для конфигурирования сервера ISA требуется открыть диалоговое окно

Листинг Сценарий для вывода заголовков запросов

```
<%@ LANGUAGE=»VBSCRIPT» %>
<HTML>
<h2> Client from
<%= Request.ServerVariables («REMOTE_ADDR») %>,
 welcome to
<i><%= Request.ServerVariables(«SERVER_NAME»)%></i></h2>
<pre>
<%= Request.ServerVariables («ALL_HTTP») %>
</pre>
</HTML>
```

лотового окна Outgoing Web Requests («Исходящие Web-запросы»), показанная на экране 2, управляет обработкой исходящих запросов сервером ISA. На этой закладке можно изменить порт, который сервер ISA использует для исходящих соединений (например, 8080). Чтобы разрешить доступ в Internet через proxy-сервер только зарегистрированным пользователям, следует установить флажок Ask unauthenticated users for identification («Запрашивать идентификацию у незарегистрированных пользователей»). Когда вы настроите клиентов на использование сервера ISA в качестве proxy-сервера, этот режим будет вызывать появление у клиента при обращении в Internet через браузер приглашение ввести имя и пароль для авторизации на proxy-сервере.

Подобно Microsoft IIS, сервер ISA поддерживает различные методы регистрации. Чтобы выбрать схему регистрации, которую клиент будет использовать для проверки имени и пароля на proxy-сервере, нужно выбрать сервер ISA в секции идентификации и нажать Edit, чтобы открыть диалоговое окно Add/Edit Listeners (добавить/редактировать слушателей). Я рекомендую выбрать встроенную (Integrated) аутентификацию, которая предписывает клиенту использовать аутентификацию по протоколу Kerberos (когда сервер ISA и клиенты являются членами домена AD) или по протоколу NT LAN Manager (NTLM). В том случае когда выбирается встроенная аутен-

Папки управления сервером ISA

Для управления Microsoft Internet Security and Acceleration (ISA) Server 2000 используется консоль Microsoft Management Console (MMC) и оснастка ISA Management. Оснастка ISA Management поддерживает расширенный режим (Advanced view), который группирует параметры сервера в папки, находящиеся под каждым системным объектом ISA Server. Данный режим упрощает управление сервером ISA. Рассмотрим подробнее эти папки и их назначение.

Папка Monitoring содержит несколько вложенных папок. Во вложенной папке Alerts хранятся короткие сообщения и предупреждения, которые появляются в системном журнале службы Firewall Service в ответ на те или иные события. Вложенная папка Services содержит информацию о запущенных службах и позволяет останавливать и запускать их. Вложенная папка Sessions помогает следить за текущей активностью сервера ISA. Вложенная папка Reports содержит задания на создание отчетов сервером ISA (например, отчетов об использовании Web), которые можно запускать по расписанию.

Папка Computer содержит список компьютеров, на которых установлена система ISA и которые являются членами массивов наряду с выбранной системой.

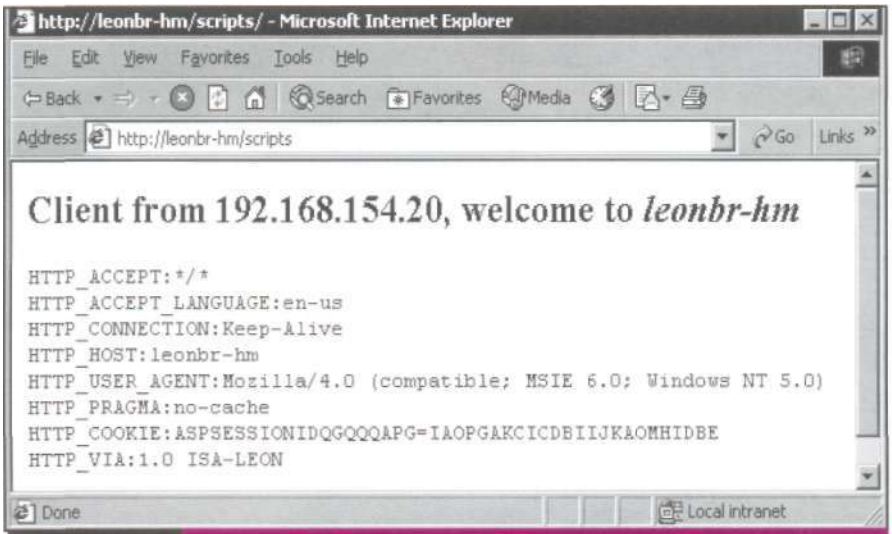
Папка Access Policy содержит три вложенные папки: Site and Content Rules, Protocol Rules и IP Packet Filters. Сервер ISA использует комбинацию этих правил для обеспечения защиты доступа в Internet.

Папка Publishing позволяет обеспечить безопасную публикацию ресурсов внутренних серверов для внешних клиентов. Папка Bandwidth Rules позволяет управлять полосой пропускания в зависимости от протокола, целевого адреса и других факторов. Папка Policy Elements хранит предварительно созданные наборы информации, такие как списки IP-адресов, списки адресов-приемников, расписания (например, Work Hours определяет часы рабочего времени пользователей). Можно комбинировать политики доступа и элементы политик для создания гибких обязательных политик доступа в Internet. Например, можно создать список существующих сайтов, таких как amazon.com или bn.com, и составить расписание с именем Lunch Time (обеденное время), которое определит часы обеденного времени пользователей. Затем можно будет использовать эти установки для предоставления доступа к сайтам из списка только в обеденное время.

Папка Cache Configuration позволяет настраивать функцию кэширования сервера ISA (т. е. какое содержимое и в течение какого времени должно храниться в кэше сервера ISA). Папка Monitoring Configuration позволяет определить, какое действие должен выполнить сервер ISA в ответ на определенное событие (например, послать по электронной почте сообщение администратору в случае остановки какой-либо службы). Папка Extensions может пригодиться для работы с динамическими библиотеками, которые расширяют функциональность сервера ISA (для написания таких библиотек следует использовать ISA Server SDK). Папка Network Configuration управляет тем, как сервер ISA маршрутизирует запросы и тем, как ISA перенаправляет их на другие proxy-серверы. Папка Client Configuration содержит настройки клиента брандмауэра ISA Server Firewall Client.

J

тификация, браузер клиента сначала пытается задействовать имя и пароль зарегистрированного пользователя. Если имя или пароль не подходят, браузер выдает приглашение ввести имя и пароль заново. Поэтому большинство пользователей домена применяют встроенную аутентификацию. В режиме аутентификации Basic with this domain «Базовая в текущем домене») имя и пароль посылаются по сети открытым текстом. Такая аутентификация безопасна только в случае использования приложениями соединений Secure Sockets Layer (SSL). Режим Digest with this domain («В соответствии с правилами домена») работает подобно NTLM, а вариант Client certificate («Сертификат клиента») работает только с соединениями SSL.



Экран 3 Подсоединение к proxy-серверу

Папка Monitoring\ervices консоли управления ISA Management содержит три службы: Firewall Service, Web Proxy Service и Scheduled Content Download. Служба Firewall Service необходима для работы клиентов SecureNAT и брандмауэра. Служба Web Proxy, помимо обеспечения функций сервера-посредника, ускоряет работу с Internet для внутренних клиентов Web Proxy, используя кэш, находящийся на сервере ISA. Если необходимо, чтобы клиенты SecureNAT и брандмауэра могли воспользоваться преимуществами такого ускорения, сервер ISA должен перенаправлять их запросы на Web Proxy. Фильтр HTTP Redirector Filter, обеспечивающий такое перенаправление, находится в папке Extensions\Application Filters консоли управления ISA Management. Настройка параметров перенаправления доступна из контекстного меню фильтра. В своем примере я могу остановить службу Web Proxy без запрещения доступа в Internet для клиентов SecureNAT и брандмауэра. Я также могу остановить службу Firewall Service, после чего доступ в Internet смогут получить только клиенты Web Proxy. Служба Scheduled Content Download наполняет кэш содержимым наиболее часто используемых адресов Internet и не влияет на работу служб Firewall Service и Web Proxy.

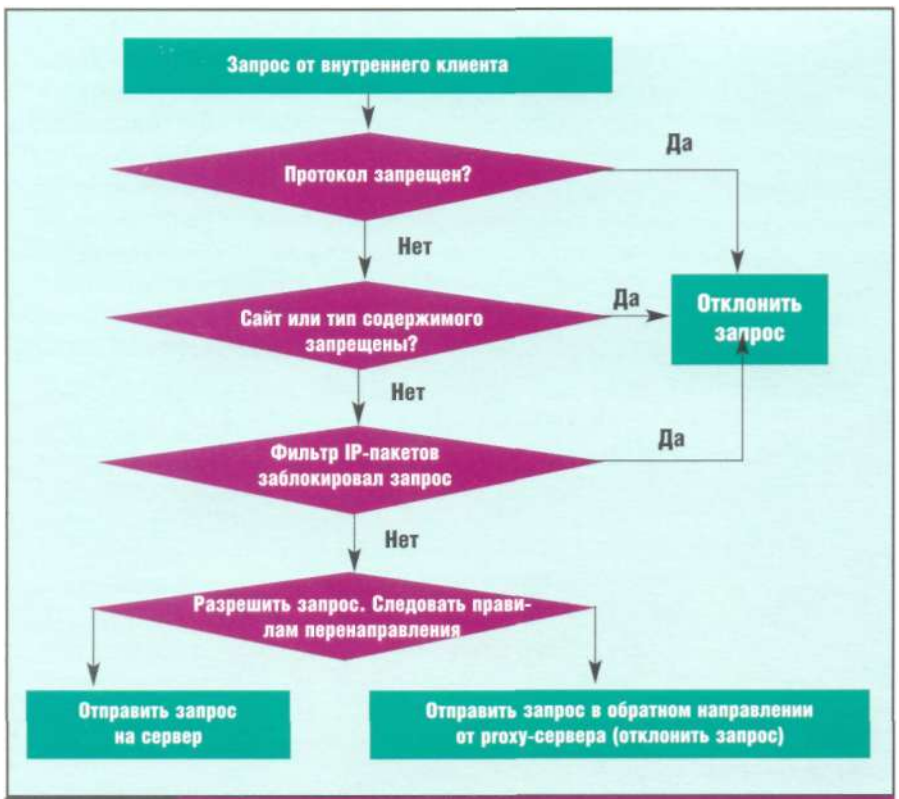


Рисунок 2 Упрощенный алгоритм проверки доступа

По умолчанию после установки сервера ISA его алгоритм управления доступом (на рис. 2 показана упрощенная версия) предотвращает доступ внутренних клиентов ко всем внешним системам. Для каждого исходящего запроса служба Firewall Service определяет, имеются ли явно заданные текущие разрешения доступа или запреты на каждый из запрашиваемых протоколов, сайтов или тип содержимого. Можно назначать специальные правила для сайтов и их содержимого, которые будут определять, какой сайт или какой тип содержимого будет доступен тем или иным пользователям. ISA Server запрещает все внешние запросы до тех пор, пока администратор явно не разрешит их. Он

также проверяет все пакеты, проходящие через proxy-сервер на предмет явного запрещения запросов каким-нибудь пакетным фильтром IP. Сервер ISA не использует каких-либо запрещающих фильтров по умолчанию. Например, внешние системы не смогут получать ответы от сервера ISA на команду ping до тех пор, пока администратор не создаст соответствующий пакетный IP-фильтр, явно разрешающий прохождение пакетов протокола Internal Control Message Protocol (ICMP), который использует команда ping. Поэтому первой задачей администратора в обеспечении доступа клиентов в Internet будет добавление в список разрешенных протоколов HTTP и HTTP Secure (HTTPS).

Для настройки правил и фильтров можно использовать папки Access Policy Site and Content Rules (правила доступа к сайтам и содержимому), Protocol Rules (правила использования протоколов), и IP Packet Filters (фильтры пакетов IP) консоли управления ISA Management. Для создания правила использования протоколов следует щелкнуть правой кнопкой мыши на папке Protocol Rules, затем выбрать New Rule для запуска мастера New Rule Wizard. Следуя указаниям мастера, создайте правило, разрешающее использование протоколов HTTP и HTTPS. В своем примере я назвал это правило Http Allow (разрешение HTTP). Нажмите Next, затем выберите Allow. На следующем экране нужно выбрать из списка Selected Protocols протоколы HTTP и HTTPS. На всех последующих экранах нажимаем Next для принятия установок по умолчанию. После закрытия мастера следует перезапустить службы Firewall Service и Web Proxy, выбирая в контекстном меню каждой службы (в папке Monitoring\Services) пункт Stop, затем остается выбрать Start для перезапуска служб.

Политики использования протоколов и политики управления доступом

Теперь давайте рассмотрим работу proxy-сервера ISA-Leon и настроим клиента Alpha для доступа к Leonbr-Hm. Откроем Microsoft Internet Explorer (IE) и выберем Tools, Internet Options из строки меню. Далее требуется выбрать закладку Connections («Соединения»), затем нажать кнопку LAN Settings («Настройка сети»). В открывшемся окне Local Area Network (LAN) Settings («Настройка локальной сети») нужно установить флажок Use a proxy server for your LAN («Использовать proxy-сервер для вашей сети»). Для модемных и VPN-соединений эти установки недоступны. В поле Address следует ввести ISA-Leon, в поле Port — 8080. Для проверки возможности доступа в Internet через локальную сеть я поместил небольшой сценарий, показанный в листинге, в папку \inetpub\scripts на Leonbr-Hm. Кроме того, я настроил сервер ISA так, чтобы он проводил идентификацию для незарегистрированных в домене пользователей. На сервере ISA используется метод базовой аутентификации (Basic authentication method), поэтому я всегда смогу просмотреть результаты своего теста.

Когда я регистрируюсь на Alpha и перехожу по адресу http://leonbr-hm/script, браузер Alpha выводит приглашение ввести имя и пароль для proxy-сервера. Когда я введу имя и пароль пользователя, который имеет доступ к серверу ISA (например, для учетной записи администратора на ISA-Leon), proxy-сервер разрешит соединение. Браузер на клиенте Alpha выведет страницу, показанную на экране 3. Обратите внимание на заголовок HTTP_VIA в приведенном запросе. Proxy-сервер добавляет этот заголовок, чтобы показать, что ISA-Leon перенаправил данный запрос. Если бы я выбрал встроенный (Integrated) тип аутентификации, браузер пытался бы задействовать имя и пароль пользователя, зарегистрированного в данный момент в системе. В этом случае сервер ISA не стал бы выводить приглашение для ввода имени и пароля, если бы учетная запись, под которой я зарегистрировался на клиенте, не имела достаточных прав для доступа к proxy-серверу.

Аутентификация соединения с proxy-сервером позволяет идентифицировать пользователя и отслеживать использование Internet-ресурсов. Поскольку proxy-сервер записывает в журнал учетные данные пользователей, можно предписать серверу ISA вести наблюдение за доступом к различным сайтам и записывать результаты в журнал. Сервер ISA создает журнал в папке \%programfiles%\microsoft isa server\isalogs. Образец журнала показан на экране 4 (для простоты я удалил большинство полей). В журнале показаны IP-адреса систем, имена пользователей, типы запросов и запрашиваемые адреса (URL). Например, можно просматривать эти журналы на предмет посещения пользователями запрещенных сайтов. Если потребовать авторизации на proxy-сервере (установив флажок Ask unauthenticated users for identification в диалоговом окне Properties сервера), можно будет определить, кто из пользователей нарушал правила (если не выбирать этот параметр, сервер ISA все соединения будет считать анонимными).

Использование сервера ISA в качестве сетевого экрана и сервера-посредника поможет защитить сеть от внешних атак за счет возможности управления внешним доступом. Кроме того, proxy-сервер позволяет управлять доступом внутренних клиентов в Internet.

```
#Software: Microsoft(R) Internet Security and Acceleration Server 2000
#Version: 1.0
#Date: 2002-12-16 03:02:55
#Fields: c-ip  cs-username          s-operation  cs-uri
10.0.0.2 anonymous   GET           http://leonbr-hm/scripts/
10.0.0.2 ISA-LEON\Administrator  GET  http://leonbr-hm/scripts/
```

Экран 4 Пример журнала ISA Server

Повышение производительности с помощью нестандартных решений

Расширяемость SQL Server 2005 Integration Services позволяет решать необычные задачи

Дуглас Макдауэлл
Преподаватель, менеджер проектов по Business Intelligence в Solid Quality Learning. Имеет звания MCSE, MCDBA и MCT.
douglas@SolidQualityLearning.com

Джей Хэкни
Старший консультант в Intellinet, занимается проектированием решений BI на базе технологий SQL Server 2005 и Microsoft .NET. Имеет сертификаты MCDBA и MCSD.
jayh@intellinet.co

В версии SQL Server 2005 самым существенным изменениям подверглись службы Data Transformation Services (DTS), ныне переименованные в SQL Server 2005 Integration Services (SSIS). Как мощное средство извлечения, преобразования и загрузки данных, SSIS обладает высокой производительностью, большим каталогом динамических компонентов, продуманной моделью развертывания, а также гибкостью и расширяемостью. Расширяемость является отличительной чертой продуктов Microsoft, и компания остается верна стратегии построения надежных платформ, отвечающих основным потребностям пользователей, с возможностью расширения для решения более специализированных задач. Если вы вплотную подошли к оценке перспектив развертывания SQL Server 2005, и в частности SSIS, на своем предприятии, то вам следует знать, о какой расширяемости платформы здесь идет речь.

В этой статье мы на конкретном примере рассмотрим процесс создания, установки и тестирования нестандартного соединения для работы с исходными данными в SSIS, который может осуществлять разбор данных файлов журнала Internet Information Server (IIS). Благодаря нестандартному компоненту пакет SSIS рассматривает файл журнала IIS в качестве источника данных, поэтому преобразует, а затем перенаправляет его содержимое в место назначения. Причем этот нестандартный компонент для работы с исходными данными создать на удивление легко.

Нужно иметь в виду, что, когда мы разрабатывали и тестировали приведенный в статье пример, последней версией SQL Server 2005 была Beta 2 October Community Technology Preview (IDW9). Эта стадия разработки характеризуется почти полной готовностью продукта, за исключением некоторых деталей, таких как объекты со старыми именами DTS, которые к моменту выпуска финальной версии еще могут измениться. И хотя наш пример будет компилироваться и исполняться на последующих бета-версиях и в финальном продукте, скорее всего, некоторые существенные изменения, вносимые Microsoft, могут проявить себя неожиданным образом, как это было в SSIS между Beta 1 и Beta 2.

Нестандартный источник данных

Источник данных — это адаптер SSIS, который загружает информацию в процесс обработки данных. SSIS позволяет разработать нестандартный компонент, который можно подключить к уникальному источнику или целевому файлу, а также использовать для выполнения специфических задач по преобразованию данных. Можно разработать нестандартный компонент для подсоединения к источнику данных, к которому нельзя получить доступ посредством существующих адаптеров данных или выполнить разбор данных и реализовать логику в сценарии на этапе извлечения данных.

В последнее время Microsoft придерживается такой тактики совершенствования продуктов, при которой сами пользователи и независимые разработчики имеют возможность расширять базовый продукт за счет собственных новаций. Несмотря на то что нестандартные компоненты можно было создавать и в DTS, это было непросто. Более того, большинство пакетов основывалось на объемных сценариях, выполняющих сложные операции. При наличии SSIS создавать нестандартные компоненты становится проще, необходимость написания сценариев сокращается радикально, а производительность и надежность построенных решений возрастают.

Создаем компонент

Наш пример нестандартного соединения выполняет разбор по столбцам содержимого журнала IIS по умолчанию, с использованием выходного буфера SSIS, что дает пакету возможность отправить журнал в базу дан-

ных, Excel или любой другой целевой компонент. Согласно настройкам по умолчанию, в журнале IIS фигурируют имена различных полей — время запроса, искомый IP-адрес, метод, единый индикатор ресурса (Uniform Resource Indicator, URI) и код статуса — в четвертой строке файла. Те, кто пытался разобраться в журнале, используя стандартный текстовый адаптер, знают, насколько неуклюжим может быть форматирование, поскольку информация разделена пробелами, а данные в строке URI непредсказуемы. Хотя осуществить разбор данных в журнале можно с помощью других средств, этот тип файлов подходит для нашего примера.

Нестандартный компонент создается в виде сборки .NET, которая является дочерней по отношению к базовому классу Microsoft. Sql Server. DTS. Pipeline. PipelineComponent. Этот базовый класс определяет методы, к которым будет обращаться SSIS для управления задачей Data Flow. В дополнительном компоненте предусмотрена безопасная замена (и игнорирование) любых методов, необходимых для выполнения задачи. Базовый класс PipelineComponent устроен так, что при отсутствии замены метода вызовы обрабатываются его механизмами по умолчанию.

В интерфейсе PipelineComponent создаются компонент источника, компонент преобразования и компонент назначения. Несмотря на то что компоненты играют разные роли в Data Flow, они выглядят одинаково; отличие заключается в функциях, выбираемых для реализации. У компонента источника (компонента для работы с исходными данными) есть выходные данные, у компонента назначения есть входные данные, а у компонента преобразования есть и то и другое плюс логика преобразования данных между вводом и выводом. Нужно только указать SSIS, к какому этапу обработки относится компонент.

Этап подготовки мы начнем с создания в Visual Studio 2005 нового проекта Class Library. Поскольку имя проекта будет именем по умолчанию для создаваемой сборки, следует выбрать имя, которое отражает сущность компонента. По неписаному правилу в конец имени компонента добавляется Src (исходный) или Dest (целевой), в зависимости от функции компонента. В нашем примере создается проект с именем IisLogFileSrc.

Листинг 1. Применение предложения using

```
using System;
using System.IO;

using Microsoft.SqlServer.Dts.Pipeline;
using Microsoft.SqlServer.Dts.Pipeline.Wrapper;
using Microsoft.SqlServer.Dts.Runtime;
using Microsoft.SqlServer.Dts.Runtime.Wrapper;

namespace IisLogFileSrc
{
  [DtsPipelineComponent(
DisplayName="IIS LogFile Source",
ComponentType=ComponentType.SourceAdapter
)]
  public class MyClass : PipelineComponent
  {
    [...]
  }
}
```

Следующий шаг — добавление в проект ссылок, указывающих Visual Studio, где искать объекты SQL Server, с которыми мы будем работать. На вкладке .NET результирующего диалогового окна следует выбрать четыре компонента: Microsoft. Sql Server. DTS Pipeline Wrap, Microsoft. SQLServer. DTSRuntimeWrap, Microsoft.SQLServer.ManagedDTS и Microsoft.SqlServer.PipelineHost.

Когда запускается проект, Visual Studio автоматически создает начальный класс (возможно, с именем Class 1 — имя класса не имеет значения). Сначала, чтобы указать компилятору, какие будут использоваться ссылки, мы задействуем простое для запоминания предложение using, как показано в коде на C# в листинге 1. Необходимо применить предложение using для вышеназванных компонентов Pipeline и Runtime, и, поскольку мы будем считывать данные из файла, следует добавить System.IO.

Также мы должны немного изменить файл Assemblylnfo. Этот файл, как можно догадаться по его имени, дает компилятору дополнительную информацию о сборке через атрибуты. По умолчанию каждый раз, когда мы строим компонент, Visual Studio создает его новую версию. Но нам это не нужно, так как компонент регистрируется в SSIS с конкретной версией,

Листинг 2. Описание компонента проектировщику пакетов

```
private IDTSOutputColumn90 CreateOutputColumn(IDTSOutput90 output, string
strColumnName, DataType intDataType, int intLength)
{
  IDTSOutputColumn90 outputColumn = output.OutputColumnCollection.New();
  outputColumn.Name = strColumnName;
  outputColumn.SetDataTypeProperties(intDataType, intLength, 0, 0, 0);
  return outputColumn;
}
private void AddColumnsToOutput(IDTSOutput90 Output)
{
  CreateOutputColumn(Output, "Time", DataType.DT_WSTR, 50);
  CreateOutputColumn(Output, "IP", DataType.DT_WSTR, 50);
  CreateOutputColumn(Output, "Method", DataType.DT_WSTR, 50);
  CreateOutputColumn(Output, "URI", DataType.DT_WSTR, 200);
  CreateOutputColumn(Output, "Status", DataType.DT_WSTR, 50);
}
public override void ProvideComponentProperties()
{
  base.RemoveAllInputsOutputsAndCustomProperties();
  ComponentMetaData.RuntimeConnectionCollection.RemoveAll();

  IDTSOutput90 output = ComponentMetaData.OutputCollection.New();
  output.Name = "Output";

  AddColumnsToOutput(output);

  IDTSRuntimeConnection90 conn = ComponentMetaData.RuntimeConnectionCollection.New();
  conn.Name = "File Connection";
}
```

Листинг 3 Код для обращения к менеджеру соединений

```
private TextReader textReader = null;
public override void AcquireConnections(object transaction)
{
  if (ComponentMetaData.RuntimeConnectionCollection[0].ConnectionManager != null)
  {
    ConnectionManager cm = DtsConvert.ToConnectionManager(
      ComponentMetaData.RuntimeConnectionCollection[0].ConnectionManager);
    ConnectionManagerFile cmFile = cm.InnerObject as ConnectionManagerFile;

    string fileConnection = cmFile.AcquireConnection(transaction) as string;
    textReader = File.OpenText(fileConnection);
  }
}
public override void ReleaseConnections()
{
  if (textReader != null)
  {
    textReader.Close();
    textReader = null;
  }
}
```

поэтому мы заменяем значение по умолчанию атрибута AssemblyVersion (1.0.?) на конкретную версию, например 1.0.0.0.

Наконец, желательно добавить наш нестандартный компонент для работы с исходными данными в глобальный кэш сборок (Global Assembly Cache, GAC), для чего необходимо присвоить ему полноценное имя. Проще всего это сделать с помощью утилиты .NET Framework 2.0 SDK Strong Name Utility (sn.exe). Переключатель -k позволяет создать ключевой файл, который становится частью проекта и должен быть помещен в папку проекта. Чтобы передать компилятору имя ключевого файла, следует использовать атрибут AssemblyKeyFile.

Возвращаясь к классу Class1, мы должны создать атрибут класса, который сообщает Business Intelligence Development Studio о нашем компоненте. В листинге 1 атрибут содержит минимальную информацию: имя компонента и тип компонента. Эту информацию можно пополнить, в том числе добавив пиктограмму, которая будет появляться в панели инструментов Development Studio.

В заключительных строках кода листинга 1 объявляется о том, что наш класс является дочерним для класса PipelineComponent. Это избавляет нас от необходимости реализовывать каждый метод, как того требует интерфейс, и все вызовы, которые мы не обрабатываем, будет получать базовый класс. Базовый класс также позволяет нам воспользоваться IntelliSense, которая автоматически создает сигнатуры для выбираемых нами методов.

На старт! Теперь мы начинаем добавлять в наш класс методы, которые будут перехватывать вызовы от SSIS Data Flow. Первый метод, ProvideComponentProperties (см. листинг 2), описывает наш компонент дизайнеру пакетов SSIS. В листинге 2 показан вызов от дизайнера, в котором запрашивается, какие входные данные, выходные данные, соединения и другие свойства необходимы компоненту для выполнения работы. Дизайнер пакетов SSIS добавляет поля на страницы свойств компонента, предоставляя пользователю возможность вводить эту информацию. Ввиду простоты нашего компонента нам понадобятся только данные о соединении и данные, относящиеся к выводу.

В соответствии с кодом листинга 2 SSIS не сохраняет предыдущую информацию о компоненте. В целях предосторожности на этом шаге стирается вся предыдущая информация, относящаяся к выводу и соединениям, а также предотвращается дублирование данных, если компонент уже инициализировался. Далее в набор данных, относящихся к выводу, добавляется выходной объект. Поскольку в нашем примере только один выходной объект, мы можем назвать его Output. Чтобы определить в SSIS внешний вид выходного объекта, код добавляет в объект столбцы, представляющие столбцы по умолчанию файла журнала IIS, который мы будем разбирать. Для простоты все поля в примере имеют строковый тип.

В заключительной части кода в SSIS передается информация о том, что компоненту необходимо соединение. Компоненту требуется файловое соединение с журналом, который мы будем читать, однако, как ни странно, в SSIS не предусмотрен способ задания типа соединения, необходимого компоненту. Мы назовем его File Connection. При желании получить более надежную реализацию проекта мы должны были бы убедиться, что соединение, которое компонент устанавливает в процессе работы, имеет подходящий тип.

Внимание! Второй этап в создании компонента состоит в формировании запросов SSIS на установление соединения перед исполнением пакета и на освобождение соединения в процессе очистки после исполнения. Как показано в листинге 3, запрос на установление соединения и получение запрошенного файлового соединения осуществляется путем обращения к менеджеру соединений. В коде содержится пара строк, которые позволяют ему найти нужный объект, поэтому мы получаем простое имя файла, которое пользователь указал в дизайнере пакетов. Для открытия файла используется метод AcquireConnections, а для закрытия — метод ReleaseConnections, при этом мы сохраняем в частной переменной дескриптор файла, чтобы тот был доступен на этапе исполнения.

Марш! На третьем и заключительном этапе мы обеспечиваем все, что связано с выводом данных, применяя метод PrimeOutput, как показано в листинге 4. К этому моменту SSIS создает буфер для каждого канала вывода, который мы установили ранее, и теперь передает эти буферы в PrimeOutput в виде массива. Пос-

кольку в нашем примере выходные данные генерируются только по одному каналу, в массиве имеется только один буферный элемент. Метод PrimeOutput заполняет буфер данными и закрывает его.

Поскольку на предыдущем этапе мы воспользовались дескриптором файла, компоненту остается только считать каждую строку файла и произвести разбор нужной информации. Вверху файла журнала IIS предусмотрена секция заголовков, поэтому мы пропускаем все строки, начинающиеся с символа #, который обозначает заголовок. Поля данных в строках, которые являются записями в журнале, разделены пробелами, что способствует более легкому разбору. Если пробелы отсутствуют, разбор данных невозможен, но с тестовыми файлами, которые мы использовали в этом примере, затруднений не возникло.

Как только компонент разобрал данные и готов добавить их в буфер, он вызывает метод AddRow и задает каждое значение. В листинге 4 показана мера предосторожности, состоящая в обрезании данных поля по определенной ширине столбца выходных данных. Таким образом предотвращается переполнение, которое может привести к ошибке во время исполнения пакета. Ввиду того что администраторы иногда заполняют журналы дополнительной информацией (а строка URI может быть очень длинной), этот прием повышает надежность проекта даже тогда, когда вы абсолютно уверены в форматах своих файлов.

Наконец, когда код листинга 4 достигает конца файла журнала и все данные записаны в буфер, код применяет к буферу метод SetEndOfRowset, сообщая SSIS, что работа закончена. Теперь код может закрыть компонент и очистить буфер.

Скрытые препятствия. Несмотря на простоту нашего примера, чтобы привести его в рабочее состояние, потребуются еще некоторые усилия. По сведениям Microsoft, на этапе метода PrimeOutput нельзя быть уверенным, что столбцы идут в том же порядке, в каком вы расположили их на этапе использования ProvideComponentProperties. Дело в том, что у менеджера буфера есть право вставлять заполнители вместо лишних столбцов, которые в процессе преобразования данных могут сливаться. Созданный компонент может и «не знать» об этих дополнительных заполнителях. Кроме того, менеджер буфера в состоянии изменить порядок столбцов для лучшей компоновки страниц памяти. Microsoft предлагает не надеяться на то, что порядок столбцов будет таким, каким вы его определили, а применить метод PreExecute и использовать метод менеджера буфера FindColumnByLineageID для уточнения местонахождения столбцов, построив массив, который можно применять в методе PrimeOutput для поиска индекса столбца по имени. Мы так и делали, но в целях простоты и экономии места в примере этого не приводим.

Устанавливаем компонент

Компонент легко устанавливается для дальнейшего использования Business Intelligence Development Studio. Сначала требуется скопировать созданную сборку в ту папку, где хранятся конвейерные компоненты SSIS. Затем нужно добавить сборку в глобальный кэш GAC. Напоследок можно добавить компонент в панель инструментов Development Studio, где его сможет выбирать пользователь. Каждый раз, когда в компонент вносятся изменения, следует скопировать файл,

Листинг 4. Код, реализующий метод PrimeOutput

```
private string Truncate(string Value, int MaxLength)
{
  return Value.Substring(0, Math.Min(MaxLength, Value.Length));
}
public override void PrimeOutput(
  int outputs, int[] outputIDs, PipelineBuffer[] buffers)
{
  string line = "";
  PipelineBuffer buffer = buffers[0];

  while (line != null)
  {
    line = textReader.ReadLine();
    if (line != null)
    {
      if (line.Substring(0, 1) != "#")
      {
        string[] values = line.Split(new char[] {' '});

        buffer.AddRow();
        buffer.SetString(0, Truncate(values[0], 50));
        buffer.SetString(1, Truncate(values[1], 50));
        buffer.SetString(2, Truncate(values[2], 50));
        buffer.SetString(3, Truncate(values[3], 200));
        buffer.SetString(4, Truncate(values[4], 50));
      }
    }
  }
  buffer.SetEndOfRowset();
}
```

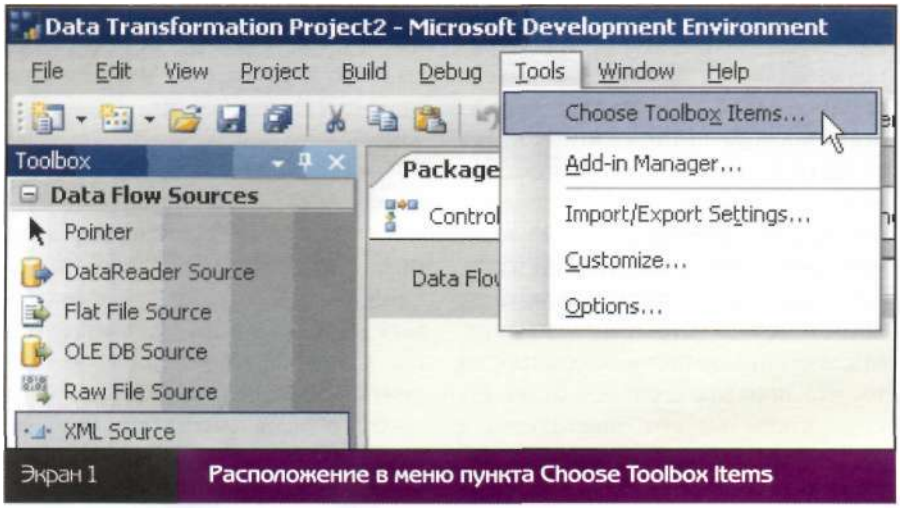
Листинг 5. Пример пакетного файла для внесения изменений в компонент

```
copy bin\Debug\lisLogFileSrc.dll "C:\Program Files\Microsoft SQL Server\90\DTS\PipelineComponents"

"C:\Program Files\Microsoft Visual Studio 8\SDK\v2.0\Bin\gacutil" /u lisLogFileSrc

"C:\Program Files\Microsoft Visual Studio 8\SDK\v2.0\Bin\gacutil" /i "C:\Program Files\Microsoft SQL
Server\90\DTS\PipelineComponents\lisLogFileSrc.dll"

pause
```



удалить предыдущую версию из GAC и установить в GAC новую версию компонента, поэтому мы рекомендуем для всех этих действий создать пакетный файл. В листинге 5 показан пример такого пакетного файла, который использовался в процессе работы.

Чтобы добавить компонент в панель инструментов, нужно открыть меню Tools и выделить пункт Choose Toolbox Items. Откроется диалоговое окно, изображенное на экране 1. Компонент должен появиться на вкладке Data Flow Items, как показано на экране 2. Необходимо выделить компонент и щелкнуть OK, после чего он появится в списке инструментов в секции Data Flow Sources.

Для обновления компонента после модернизации нужно закрыть все использующие его приложения, снова запустить установочный пакетный файл и открыть то же приложение. Данное приложение должно автоматически получить новую версию компонента. Сбой при выполнении этой процедуры у нас возник только однажды — когда мы изменили имя класса компонента. В силу этого изменения Business Intelligence Development Studio воспринял наш компонент как совершенно другой (хотя и с тем же именем). Нам пришлось удалить старый компонент из панели инструментов и добавить новый. Кроме того, потребовалось удалить компонент из всех проектов и добавить его заново.

Создаем тестовый пакет

Для того чтобы протестировать образец, нужно создать новый проект типа Data Transformation Project в Business Intelligence Development

Первый нестандартный компонент для работы с источником данных

Дуглас Макдауэлл

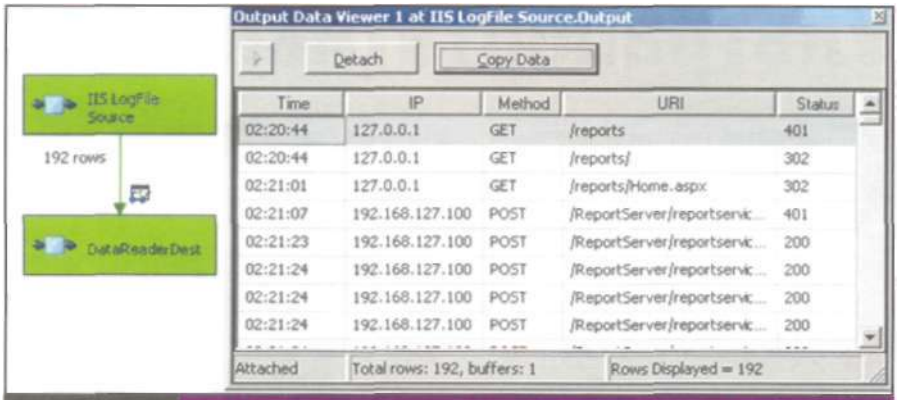
На этапе начального бета-тестирования SQL Server 2005 команда разработчиков SQL Server 2005 Integration Services (SSIS) подыскивала сложные проблемы, с помощью которых можно было бы протестировать SSIS. И вот вместе с нашим коллегой Эриком Веерманом мы предоставили команде в качестве источника данных чрезвычайно мудреный текстовый файл. Это был журнальный файл телефонного узла размером около 5 Мбайт, имевший более пяти форматов многострочной записи. В нашем приложении, построенном на основе SQL Server 2000 Data Transformation Services (DTS), эти журнальные файлы импортировались в одну консолидированную таблицу, которая содержала более 100 столбцов и использовала для разбора записей сценарий ActiveX, состоящий из 500 строк. Три механизма разбивали данные на выделенные таблицы, в зависимости от типа записей. Обработка одного файла и отправка его в базу данных занимала 40 секунд, и мы применяли нестандартный процесс, чтобы справиться с количеством текстовых файлов в исходной папке. Рабочая нагрузка доходила до 1000 файлов в день.

Специалисты команды SSIS тщательно исследовали файловый формат телефонного узла и пришли к выводу, что он не подходит ни к одному из существующих адаптеров данных. Таким образом, мы познакомились с концепцией нестандартного соединения для работы с исходными данными. Команда работала над этой проблемой в отсутствие документации, поэтому одному из главных членов команды, Джиму Хоуи, пришлось повозиться с идеями и деталями компонента, и со своей задачей он успешно справился. В результате появилось превосходное решение для импорта и разбора журнальных файлов. Более того, команда разработчиков SSIS предусмотрела возможность использования встроенного цикла ForEach для массовой обработки журнальных файлов, содержащихся в папке, без утомительного написания сценариев.

Мы переместили сложную логику разбора данных из ActiveX в готовый .NET-компонент и таким образом сохранили вложенные при декодировании файла усилия, обеспечив их использование на более высоком уровне. Применяя логику разбора, компонент для работы с исходными данными различал три типа записей и создавал три выходных потока, так что данные могли непосредственно вставляться в три целевые таблицы, минуя дорогостоящий промежуточный шаг, необходимый в DTS. В итоге число операций импорта сократилось в 12 раз на один файл и в 17 раз при одновременном импорте многих файлов. Это впечатляющее достижение имело место до выпуска первой бета-версии SSIS и до того, как команда закончила все настройки производительности продукта. Поначалу мы были даже несколько ошеломлены таким ростом производительности, но позже, оглядываясь назад, поняли, в чем дело. В дополнительном компоненте для работы с исходными данными произошел существенный сдвиг в архитектуре, при котором логика преобразования данных переместилась в скомпилированный компонент, не имеющий дополнительных издержек, связанных с созданием сценариев ActiveX. Кроме того, сближение преобразования данных с источником данных сократило количество обращений к данным. Сочетание высокой производительности с гибкостью решения делает нестандартный компонент для работы с исходными данными весьма эффективным средством.

Studio. Сначала на экране появляется чистый лист Control Flow, в который требуется добавить задачу Data Flow Task. Нужно дважды щелкнуть на этой задаче — откроется чистый лист Data Flow. Теперь следует захватить новый компонент для работы с исходными данными в панели инструментов и перенести его на пустое место.

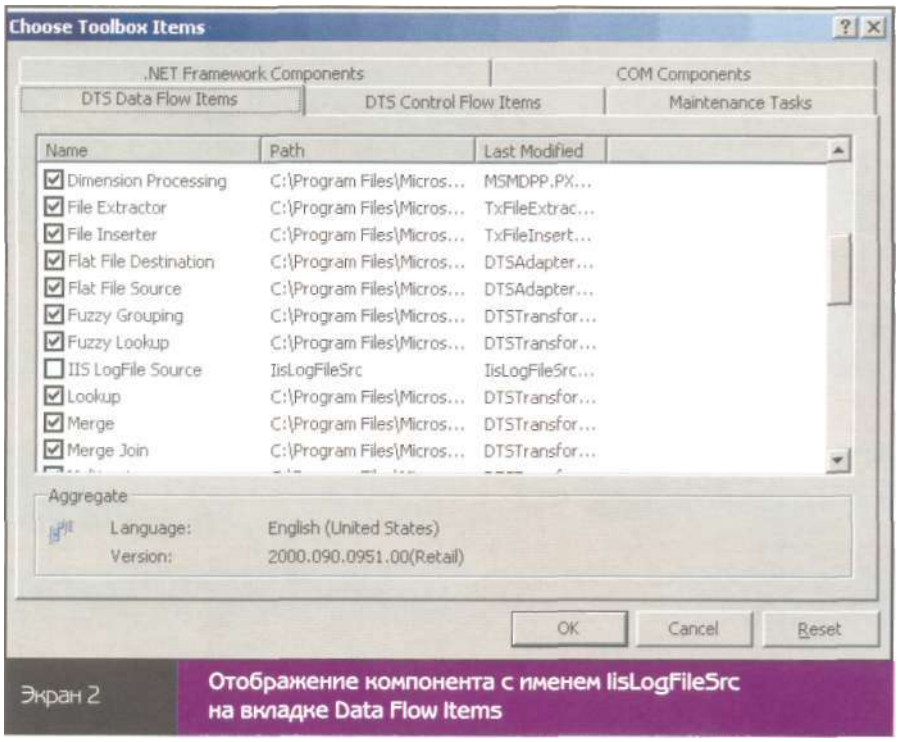
Затем File Connection должен сообщить компоненту, где искать файл журнала, который предстоит импортировать. Нужно дважды щелкнуть на секции Connections внизу листа Data Flow и выделить New File Connection. Будьте внимательны, чтобы невзначай не воспользоваться пунктом New Flat File Connection: это соединение другого типа, предназначенное для компонента Flat File Source. Для файлового соединения в нашем примере тип использования следует установить в значение Existing File. После этого можно добавить импортируемый файл журнала IIS. Обычно журнальные файлы IIS расположены в папке C:\WINDOWS\system32\Logfiles на той системе, где установлен IIS. Ясно, что Web-сервер должен иметь какой-то контент и трафик, чтобы сгенерировать журналы. Если ничего такого нет, можно сформировать несколько файлов на основе описанного выше формата.



Экран 3 Добавленное к компоненту средство просмотра данных показывает, что все работает

Теперь требуется добавить в компонент новое соединение. Нужно щелкнуть правой кнопкой на компоненте и выделить Edit в контекстном меню. На экране появится редактор, и первая вкладка должна называться Connection Managers. Соединение, которое компонент запросил в методе ProvideComponentProperties, должно на ней отобразиться, а в поле со списком можно будет выбрать вновь созданное файловое соединение.

Последний шаг — объект назначения. Тестируя компоненты с исходными данными, мы пользовались DataReader Destination, средством аккумулирования выходных данных, которое позволяет легко протестировать компонент. Конечно, можно было бы направить выходные данные в SQL Server, Excel или в какое-нибудь другое целевое приложение, но нужно иметь в виду, что, как правило, другие целевые приложения требуют дополнительной настройки. Чтобы воспользоваться DataReader Destination, необходимо просто захватить выходной объект источника и перенести его на целевой объект. Затем нужно отредактировать целевой объект и выбрать столбцы, соответствующие имеющимся выходным данным, чтобы не вызвать ошибок SSIS из-за неиспользуемых столбцов. Рекомендуется также добавить к соединению средство просмотра данных Data Viewer, как показано на экране 3, чтобы иметь возможность убедиться, что источник данных работает. Для этого следует щелкнуть правой кнопкой на соединении, выделить Data Viewers и добавить источник данных.



Экран 2 Отображение компонента с именем IisLogFileSrc на вкладке Data Flow Items

Теперь пакет должен быть полностью готов к исполнению. После того как мы щелкнем зеленую стрелку для компиляции и исполнения в отладчике, должен появиться Data Viewer и отобразить данные файла журнала IIS в виде таблицы с сеткой. Более подробную информацию о разработке дополнительных компонентов для работы с исходными данными можно найти в разделе «Creating a Source Component» в SQL Server 2005 Books Online.

Ультрапортативные компьютеры

Джейсон Бовберг

Старший редактор журналов Windows IT Pro и SQL Server Magazine.
jbovberg@windowsitpro.com

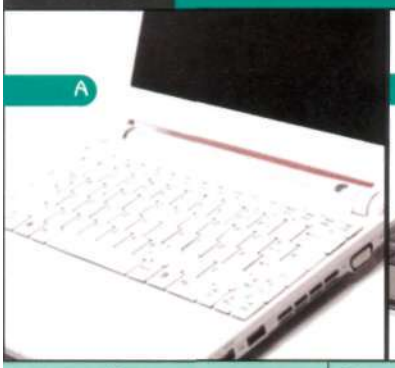
Существует определенная категория пользователей, которые живут в постоянном движении. Как говорил капитан Немо: «Подвижное в подвижном». Путешествия занимают все их время, они не отрывают пальцев от клавиатуры, перемещаясь из страны в страну, с конференции в региональное представительство... Такие люди наверняка не раз проклинали громоздкий ноутбук, особенно когда приходилось таскать тяжеленный чемодан по аэропортам и гостиницам.

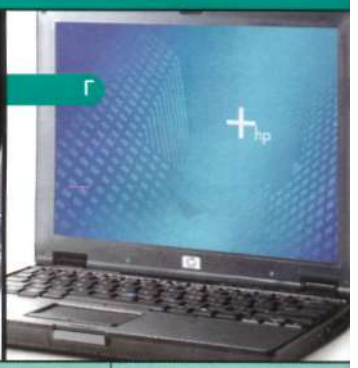
В таком случае ультрапортативный ноутбук — именно то, что нужно. Эти устройства такие легкие, что, кажется, могут плавать, и в то же время легко справляются с выполнением типичных бизнес-задач, обладая дополнительными возможностями, которые могут сделать путешествие менее утомительным. В этом выпуске мы рассмотрим самые выдающиеся продукты в классе ультрапортативных ноутбуков.

Достоинства этих ноутбуков становятся очевидны, как только берешь их в руки, — они просто невесомы! В процессе подготовки этого обзора я работал на одном из них, и все окружающие завидовали мне черной завистью. Довольно яркий широкоэкранный дисплей наводит на мысли о приятном просмотре любимого фильма, и клавиатура тоже весьма удобна, хоть и невелика.

Особенное впечатление производит то, что такое устройство выступает на равных, если не даст сто очков вперед обычным настольным компьютерам. Процессор с частотой от 1,1 до 1,73 МГц, диск — от 30 до 80 Гбайт, оперативная память — от стандартных 256 Мбайт до 2 Гбайт. Компьютер с такими характеристиками способен решать вычислительные задачи любой сложности. Все современные ноутбуки обеспечивают беспроводную связь стандарта 802.1 lb/g. В общем, достойная машина для «странствующего рыцаря». Время независимой работы от батарей достаточное, но не выдающееся. Со стандартной батареей можно работать от 3 до 7 часов, некоторые модели предлагают дополнительную резервную батарею для удвоения времени автономной работы.

Таблица **Ультрапортативные компьютеры**





	Контактная информация	Продукт	Базовая цена, долл.	Вес, кг	Размеры, мм	Размер и тип экрана	Время работы от батарей, ч
А	Averatec, http://www.averatec.com	1000 Series AV1050-EB1	1379	1,18	266x202x35	AveraBrite, 10.6" WXGA	До 5 часов со стандартной батареей
Б	Dell, http://www.dell.com	Latitude X1	1693	1,13	286x196x25	12,1" WXGA	3
В	Fujitsu Siemens, http://www.fujitsusiemens.com	LIFEBOOK S Series	2299	1,75	306x247x32	14,1" TFT-XGA (1024x768)	5
Г	HP, http://www.hp.com	HP Compaq nc4200 Notebook PC	1693	1,77	285x235x30	12,1" XGA	4
Д	IBM/Lenovo	ThinkPad X Series	1499	1,45	267x211x21	12,1" TFT-XGA	7
Е	Sharp	Sharp M4000	1799	1,68	312x226x37	13,3" WXGA	6
Ж	Sony	Sony VAIO T Series	1899	1,38	272x206x34	10,6" WXGA	5
З	Toshiba	Portege R200	2099	1,29	286x229x8	12,1" Diagonal Polysilicon XGA (1024x768)	5

Примечание редактора. Некоторые поставщики сообщили, что у них нет продуктов, соответствующих требованиям обзора, или не предоставили продукты для тестирования. В руководстве поку-

Однако, если вы решились на ультрапортативную модель, будьте готовы чем-то пожертвовать. Ограничение размера экрана придется не по вкусу опытным пользователям и системным администраторам, которым требуется иметь дело одновременно с большим количеством рабочих столов и приложений. Можно найти более яркие дисплеи в более громоздких ноутбуках, но следует признать, что ультрапортативные ноутбуки справляются с любой задачей, если только идеально четкое изображение не является главным критерием.

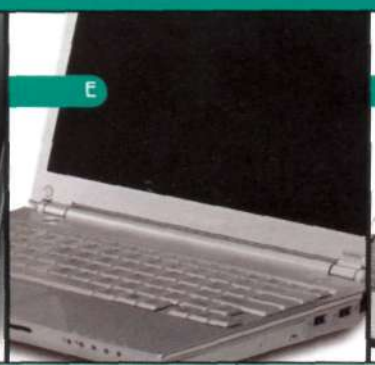
Чтобы вес системы не превышал четырех фунтов (примерно 1,8 кг), многие ноутбуки были лишены встроенного оптического привода. Если вам часто приходится работать с контентом на носителях DVD, постоянно подключать и отключать внешний накопитель быстро надоест.

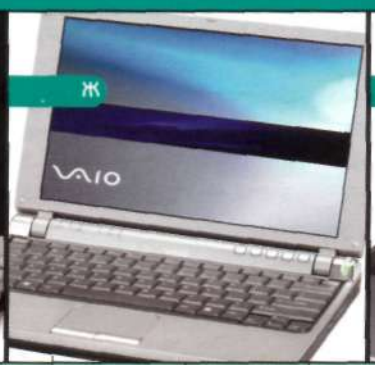
Для тестирования внешнего привода DVD, который входил в комплект моей тестовой системы, я запустил свой любимый фильм. Изображение было отличное, но встроенные колонки выдавали слабоватый звук, так что для нормального просмотра фильмов потребуются наушники. Вообще это не лучший видеопроигрыватель, учитывая небольшой размер экрана и явно недостаточную звуковую систему. С другой стороны, такие ноутбуки имеют более удобный экран, чем большинство портативных DVD-плейеров, так что все равно мобильным пользователям они пригодятся для просмотра кино.

Наконец, хотя клавиатура вполне удобна, длительное ее использование для набора текста вызывает ощущение дискомфорта — пространство слишком ограничено. Стоит заметить, что для самых миниатюрных из рассматриваемых ноутбуков можно дополнительно приобрести док-станцию, которая позволит, находясь в офисе, использовать нормальные клавиатуру, мышь и монитор.

В целом все рассмотренные ноутбуки исключительно портативные и мощные. Носить этот тестовый компьютер из офиса домой и обратно было просто удовольствием. Технология стремительно развивается, и, хотя многие производители предлагают внешний DVD-привод, некоторые сумели интегрировать этот важный компонент в миниатюрную систему.

Решающим остается вопрос, является ли миниатюрность и небольшой вес достаточным основанием раскошелиться? А если принять во внимание размеры экрана и клавиатуры? Каждый сам определяет, какие возможности и качества ноутбука являются для него решающими. Советую исходить из того, насколько часто вам приходится носить ноутбук с собой, не беря в расчет второстепенные факторы, такие как скорость процессора, объем памяти и дисковое пространство.





Тип указателя	Оптические накопители	Процессор	Объем оперативной памяти	Жесткий диск	Беспроводной адаптер 802.11	Bluetooth/ИК-порт	Графический адаптер, слоты
Touchpad	Интегрированный DVD, CD-RW	1,1 ГГц Intel Pentium M Ultralow Voltage (ULV) 733	512 Мбайт Double Data Rate (DDR)	80 Гбайт	802.11g	Нет/нет	Intel Extreme Graphics 2 с динамическим выделением видеопамяти
Touchpad	DVD+/-RW	1,1 ГГц Intel Pentium M ULV 733	256 Мбайт - 1,28 Гбайт	30 или 60 Гбайт	802.11b/g	Да/нет	Слоты CompactFlash (CF) и Secure Digital (SD), порт IEEE 1394, Transaction Processing Monitor (TPM)
Touchpad/ touchstick	Дополнительное устройство	1,6 ГГц Intel Pentium M 755	256 Мбайт - 2 Гбайт	40 или 80 Гбайт	802.11b/g	Да/да	Intel 855GME
DualPoint (Touchpad и PointStick)	Дополнительное устройство MultiBay II с DVD/CD-RW (за $169)	1,73 ГГц Intel Pentium M 740	512 Мбайт 400MHz DDR II SDRAM	60 Гбайт	802.11b/g	Да/нет	Intel Graphics Media Accelerator 900
TrackPoint	Не данных	1,1 ГГц Intel Pentium M ULV 733	256 Мбайт - 1,25 Гбайт	30 Гбайт	802.11b/g	Нет/да	Intel Extreme Graphics 2
Touchpad	CD-RW/DVD	Информация у производителя	512 Мбайт - 1,5 Гбайт	80 Гбайт	802.11b/g	Нет/нет	Intel 915GM с 128 Мбайт разделяемой памяти
Touchpad	DVD+/-RW/CD-RW	1,2 ГГц Intel Pentium M ULV 753	512 Мбайт - 1 Гбайт	60 Гбайт	802.11b/g	Да/нет	Intel 855GME
Touchpad	Дополнительное устройство	Intel Pentium M ULV 753	512 Мбайт - 1,28 Гбайт	60 Гбайт	802.11b/g	Да/нет	Intel Graphics Media Accelerator 900

пателя приведены сведения, предоставленные производителями.

Защита беспроводной сети

Корректная настройка устройств и отслеживание *ложных узлов - залог* безопасности

Джон Хоуп
Менеджер центра Microsoft Security Center of Excellence. Имеет сертификаты CISSP, CISM и CISA.
jhowie@microsoft.com

Беспроводные сети широко применяются в компаниях любого масштаба. Благодаря низкой цене и простоте развертывания беспроводные сети могут иметь преимущество перед проводными на малых и средних предприятиях. В крупных учреждениях беспроводные сети обеспечивают сетевые соединения, необходимые для делового общения сотрудников в рабочих помещениях или комнатах отдыха.

Чтобы можно было воспользоваться преимуществами беспроводных сетей, их необходимо защитить. Незащищенные беспроводные сети открывают практически неограниченный доступ к корпоративной сети для хакеров и других злоумышленников, которые нередко стремятся лишь получить бесплатный доступ в Internet. В крупных учреждениях иногда существуют несанкционированные беспроводные сети — члены рабочих групп или конечные пользователи подчас игнорируют корпоративную политику и устанавливают точки доступа (Access Points, AP), и это таит в себе большую опасность для предприятия. Опытные спамеры и мошенники используют незащищенные беспроводные сети для массовой рассылки сообщений электронной почты. Они разъезжают по городам и промышленным зонам в поисках уязвимых беспроводных сетей, а когда находят, настраивают свои мобильные компьютеры для подключения к сети, получают через DHCP действительный IP-адрес, DNS и стандартную информацию о шлюзе, а затем передают свои сообщения. Пользователям таких продуктов, как NetStumbler, или встроенного инструментария управления беспроводной сетью, имеющегося в большинстве ноутбуков и PDA, вероятно, приходилось обнаруживать незащищенные беспроводные сети в своих жилых районах, по соседству или внутри своего предприятия.

Владельцы незащищенных сетей должны быть готовы и к снижению пропускной способности Internet-соединения, и к проникновению вирусов и червей, и даже к несению уголовной или гражданской ответственности за использование незащищенных сетей для осуществления атак против третьих лиц. В данной статье рассматриваются практические меры, которые можно предпринять для защиты беспроводных сетей, методы автоматизированного развертывания параметров и инструменты для анализа незащищенных и неавторизованных беспроводных сетей.

Экран 1 Настройка беспроводных параметров в XP

Основы беспроводных сетей

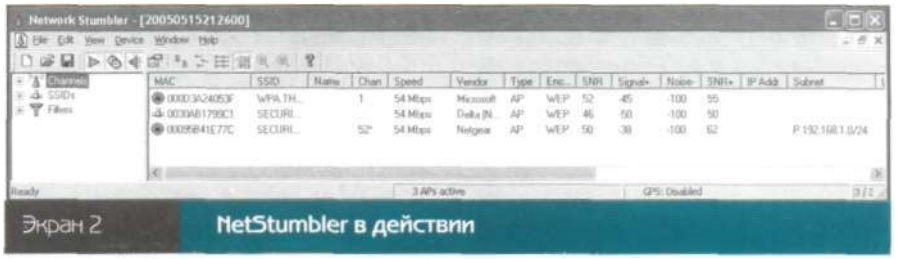
Прежде чем приступать к защите беспроводной сети, необходимо понять основные принципы ее организации. Как правило, беспроводные сети состоят из узлов доступа и клиентов с беспроводными адаптерами. Узлы доступа и беспроводные адаптеры оснащаются приемопередатчиками для обмена данными друг с другом. Каждому AP и беспроводному адаптеру назначается 48-разрядный адрес MAC, который функционально эквивалентен адресу Ethernet. Узлы доступа связывают беспроводные и проводные сети, обеспечивая беспроводным клиентам доступ к проводным сетям. Связь между беспроводными клиентами в одноранговых сетях возможна без AP, но этот метод редко применяется в учреждениях. Каждая беспроводная сеть идентифицируется назначаемым администратором идентификатором SSID (Service Set Identifier). Связь беспроводных клиентов с AP возможна, если они распознают SSID узла доступа. Если в беспроводной сети имеется несколько узлов доступа с одним SSID (и одинаковыми параметрами аутентификации и шифрования), то возможно переключение между ними мобильных беспроводных клиентов.

Наиболее распространенные беспроводные стандарты — 802.11 и его усовершенствованные варианты. В спецификации 802.11 определены характеристики сети, работающей со скоростями до 2 Мбит/с. В усовершенствованных вариантах предусмотрены более высокие скорости. Первый, 802.11b, распространен наиболее широко, но быстро замещается стандартом 802.1 lg. Беспроводные сети 802.11b работают в 2,4-ГГц диапазоне и обеспечивают скорость передачи данных до 11 Мбит/с. Усовершенствованный

вариант, 802.11a, был ратифицирован раньше, чем 802.1 lb, но появился на рынке позднее. Устройства этого стандарта работают в диапазоне 5,8 ГГц с типовой скоростью 54 Мбит/с, но некоторые поставщики предлагают более высокие скорости, до 108 Мбит/с, в турборежиме. Третий, усовершенствованный вариант, 802.1 lg, работает в диапазоне 2,4 ГГц, как и 802.1 lb, со стандартной скоростью 54 Мбит/с и с более высокой (до 108 Мбит/с) в турборежиме. Большинство беспроводных сетей 802.1lg способно работать с клиентами 802.11b благодаря обратной совместимости, заложенной в стандарте 802.1lg, но практическая совместимость зависит от конкретной реализации поставщика. Основная часть современного беспроводного оборудования поддерживает два или более вариантов 802.11. Новый беспроводной стандарт, 802.16, именуемый WiMAX, проектируется с конкретной целью обеспечить беспроводной доступ для предприятий и жилых домов через станции, аналогичные станциям сотовой связи. Эта технология в данной статье не рассматривается.

Реальная дальность связи AP зависит от многих факторов, в том числе варианта 802.11 и рабочей частоты оборудования, изготовителя, мощности, антенны, внешних и внутренних стен и особенностей топологии сети. Однако беспроводной адаптер с узконаправленной антенной с большим коэффициентом усиления может обеспечить связь с AP и беспроводной сетью на значительном расстоянии, примерно до полутора километров в зависимости от условий.

Из-за общедоступного характера радиоспектра возникают уникальные проблемы с безопасностью, отсутствующие в проводных сетях. Например, чтобы подслушивать сообщения в проводной сети, необходим физический доступ к такому сетевому компоненту, как точка подсоединения устройства к локальной сети, коммутатор, маршрутизатор, брандмауэр или хост-компьютер. Для беспроводной сети нужен только приемник, такой как обычный сканер частот. Из-за открытости беспроводных сетей разработчики стандарта подготовили спе-



Экран 2 NetStumbler в действии

цификацию Wired Equivalent Privacy (WEP), но сделали ее использование необязательным. В WEP применяется общий ключ, известный беспроводным клиентам и узлам доступа, с которыми они обмениваются информацией. Ключ можно использовать как для аутентификации, так и для шифрования. В WEP применяется алгоритм шифрования RC4. 64-разрядный ключ состоит из 40 разрядов, определяемых пользователем, и 24-разрядного вектора инициализации. Пытаясь повысить безопасность беспроводных сетей, некоторые изготовители оборудования разработали расширенные алгоритмы со 128-разрядными и более длинными ключами WEP, состоящими из 104-разрядной и более длинной пользовательской части и вектора инициализации. WEP применяется с 802.11a, 802.11b- и 802.1 lg-совместимым оборудованием. Однако, несмотря на увеличенную длину ключа, изъяны WEP (в частности, слабые механизмы аутентификации и ключи шифрования, которые можно раскрыть методами криптоанализа) хорошо документированы, и сегодня WEP не считается надежным алгоритмом.

В ответ на недостатки WEP отраслевая ассоциация Wi-Fi Alliance, насчитывающая более 200 членов, среди которых Apple Computer, Cisco Systems, Dell, IBM и Microsoft, приняла решение разработать стандарт Wi-Fi Protected Access (WPA). WPA превосходит WEP благодаря добавлению протокола TKIP (Temporal Key Integrity Protocol) и надежному механизму аутентификации на базе 802.1x и протокола EAP (Extensible Authentication Protocol). Предполагалось, что WPA станет рабочим стандартом, который можно будет представить для одобрения комитету IEEE в качестве расширения для стандартов 802.11. Расширение, 802. 11i, было ратифицировано в 2004 г., а WPA обновлен до WPA2 в целях совместимости с Advanced Encryption Standard (AES) вместо WEP и TKIP. WPA2 обратно совместим и может применяться совместно с WPA. WPA был предназначен для сетей предприятий с инфраструктурой аутентификации RADIUS (Remote Authentication Dial-In User Service — служба дистанционной аутентификации пользователей по коммутируемым линиям), но версия WPA, именуемая WPA Pre-Shared Key (WPAPSK), получила поддержку некоторых изготовителей и готовится к применению на небольших предприятиях. Как и WEP, WPAPSK работает с общим ключом, но WPAPSK надежнее WEP.

У многих складывается неверное представление о 802.1x. Стандарт используется для управления доступом к портам в коммутаторах проводных сетей и узлам доступа в AP беспроводных сетей. В 802.1x не задан метод аутентификации (например, можно использовать версию 3 спецификации X.509 или Kerberos) и нет механизма шифрования или обязательного требования шифровать данные.

Три шага к безопасности

Существует три механизма защиты беспроводной сети: настроить клиент и AP на использование одного (не выбираемого по умолчанию) SSID, разрешить AP связь только с клиентами, MAC-адреса которых известны AP, и настроить клиенты на аутентификацию в AP и шифрование трафика. Большинство AP настраиваются на работу с выбираемым по умолчанию SSID, без ведения списка разрешенных MAC-адресов клиентов и с известным общим ключом для аутентификации и шифрования (или вообще без аутентификации и шифрования). Обычно эти параметры документированы в оперативной справочной системе на Web-узле изгото-

вителя. Благодаря этим параметрам неопытный пользователь может без труда организовать беспроводную сеть и начать работать с ней, но одновременно они упрощают хакерам задачу проникновения в сеть. Положение усугубляется тем, что большинство узлов доступа настроено на широковещательную передачу SSID. Поэтому взломщик может отыскать уязвимые сети по стандартным SSID.

Первый шаг к безопасной беспроводной сети — изменить выбираемый по умолчанию SSID узла доступа. Кроме того, следует изменить данный параметр на клиенте, чтобы обеспечить связь с AP. Удобно назначить SSID, имеющий смысл для администратора и пользователей предприятия, но не явно идентифицирующий данную беспроводную сеть среди других SSID, перехватываемых посторонними лицами.

Следующий шаг — при возможности блокировать широковещательную передачу SSID узлом доступа. В результате взломщику становится сложнее (хотя возможность такая сохраняется) обнаружить присутствие беспроводной сети и SSID. В некоторых AP отменить широковещательную передачу SSID нельзя. В таких случаях следует максимально увеличить интервал широковещательной передачи. Кроме того, некоторые клиенты могут устанавливать связь только при условии широковещательной передачи SSID узлом доступа. Таким образом, возможно, придется провести эксперименты с этим параметром, чтобы выбрать режим, подходящий в конкретной ситуации.

После этого можно разрешить обращение к узлам доступа только от беспроводных клиентов с известными MAC-адресами. Такая мера едва ли уместна в крупной организации, но на малом предприятии с небольшим числом беспроводных клиентов это надежная дополнительная линия обороны. Взломщикам потребуется выяснить MAC-адреса, которым разрешено подключаться к AP предприятия, и заменить MAC-адрес собственного беспроводного адаптера разрешенным (в некоторых моделях адаптеров MAC-адрес можно изменить).

Выбор параметров аутентификации и шифрования может оказаться самой сложной операцией защиты беспроводной сети. Прежде чем назначить параметры, необходимо провести инвентаризацию узлов доступа и беспроводных адаптеров, чтобы установить поддерживаемые ими протоколы безопасности, особенно если беспроводная сеть уже организована с использованием разнообразного оборудования от различных поставщиков. Некоторые устройства, особенно старые AP и беспроводные адаптеры, могут быть несовместимы с WPA, WPA2 или ключами WEP увеличенной длины.

Еще одна ситуация, о которой следует помнить, — необходимость ввода пользователями некоторых старых устройств шестнадцатеричного числа, представляющего ключ, а в других старых AP и беспроводных адаптерах требуется ввести фразу-пароль, преобразуемую в ключ. В результате трудно добиться применения одного ключа всем оборудованием. Владельцы подобного оборудования могут использовать такие ресурсы, как WEP Key Generator (http://www.andrewscompanies.com/tools/wep.asp), для генерации случайных ключей WEP и преобразования фраз-паролей в шестнадцатеричные числа.

В целом WEP следует применять лишь в случаях крайней необходимости. Если использование WEP обязательно, стоит выбирать ключи максимальной длины и настроить сеть на режим Open вместо Shared. В режиме Open в сети аутентификация клиентов не выполняется, и установить соединение с узлами доступа может каждый. Эти подготовительные соединения частично загружают беспроводной канал связи, но злоумышленники, установившие соединение в AP, не смогут продолжать обмен данными, так как не знают ключа шифрования WEP Можно блокировать даже предварительные соединения, настроив AP на прием соединений только от известных MAC-адресов. В отличие от Open, в режиме Shared узел доступа использует ключ WEP для аутентификации беспроводных клиентов в процедуре запрос-отклик, и взломщик может расшифровать последовательность и определить ключ шифрования WEP

Если можно применить WPA, то необходимо выбрать между WPA, WPA2 и WPA-PSK. Главным фактором при выборе WPA или WPA2, с одной стороны, и WPA-PSK — с другой, является возможность развернуть инфраструктуру, необходимую WPA и WPA2 для аутентификации пользователей. Для WPA и WPA2 требуется развернуть серверы RADIUS и, возможно, Public Key Infrastructure (PKI). WPA-PSK, как и WEP, работает с общим ключом, известным беспроводному клиенту и AP. WPA-PSK можно смело использовать общий ключ WPA-PSK для аутентификации и шифрования, так как ему не присущ недостаток WEP (возможность узнать ключ шифрования методом криптоанализа процедуры аутентификации).

Естественно, в узлах доступа различных поставщиков применяются свои пользовательские интерфейсы и методы настройки конфигурации, поэтому невозможно представить единый список подробных инструкций для всех устройств. Но приведенная выше информация будет полезна при настройке узлов доступа.

Настройка клиента Windows

Windows Server 2003 и Windows XP облегчают настройку клиента для работы в беспроводных сетях, особенно в сетях с WE P. Компания Microsoft организовала службу Wireless Zero Configuration в XP и назвала ее Wireless Configuration service в Windows 2003. Запущенная служба выполняет мониторинг беспроводных адаптеров для приема широковещательных посылок SSID от узлов доступа. Если принята широковещательная передача известного SSID и имеется достаточно информации для конфигурации, то Windows автоматически подключается к сети (если настроена на соединение). Служба беспроводной настройки выдает стандартное диалоговое окно для настройки параметров беспроводной сети независимо от установленного беспроводного адаптера. К сожалению, служба не работает со всеми беспроводными адаптерами; если она не работает с конкретной платой, необходимо блокировать ее и задействовать драйвер и инструменталь-

ный комплект для настройки, поставляемый вместе с сетевым адаптером. Чтобы использовать службу настройки, следует открыть утилиту Network Connections в панели управления, щелкнуть правой кнопкой мыши на значке беспроводного адаптера, выбрать пункт Properties и перейти к вкладке Wireless Networks. Необходимо убедиться, что режим Use Windows to configure my wireless network settings активизирован, и щелкнуть на кнопке Add, чтобы настроить беспроводную сеть. На экране 1 показано диалоговое окно для ввода параметров беспроводной сети. Затем следует ввести SSID для беспроводной сети, с которой нужно установить соединение, выбрать метод для Network Authentication. Если выбрать Open или Shared, то в поле Data encryption можно указать одно из значений — WEP или Disabled. Если выбраны WPA или WPA-PSK, то можно применять алгоритмы шифрования TKIPmmAES.

При использовании WPA или WPA-PSK для аутентификации или шифрования можно ввести ключ аутентификации или шифрования (чтобы активизировать поле Network key и поле Confirm network key, требуется отменить режим The key is provided for me automatically). Если существует более одного ключа, следует выбрать номер ключа, или индекс. В некоторых узлах доступа и беспроводных адаптерах можно хранить и использовать до четырех ключей в целях повышения гибкости. Например, ключи можно менять еженедельно, вручную выбирая ключ из списка каждый понедельник утром.

Обнаружение несанкционированных узлов доступа

Как отмечалось выше, ложные узлы доступа могут представлять огромную опасность для предприятия. Но из-за преимуществ и простоты установки AP (особенно если используются выбираемые по умолчанию параметры) очень вероятно, что кто-то в один прекрасный момент установит узел доступа в сети предприятия. Отыскать несанкционированные узлы доступа может быть сложно, но это необходимо для надежной защиты. В Windows 2003 появилась новая оснастка консоли Microsoft Management Console (MMC), называемая Wireless Network Monitor, с помощью которой можно протоколировать активность сетевых клиентов и находить узлы доступа. Однако устанавливать Windows 2003 в ноутбуках только ради оснастки MMC неудобно, дорого и вообще необязательно. Большинство ноутбуков и PDA со встроенными беспроводными адаптерами располагают инструментарием, пригодным для поиска несанкционированных AP.

Если ноутбук или PDA поставляются без такого инструмента или необходимы передовые функции, например GPS (глобальная система позиционирования в сочетании с двунаправленной антенной и компасом позволяет вычислить методом триангуляции местоположение несанкционированного AP), то предпочтительным может оказаться такой бесплатный инструмент, как NetStumbler. По адресу http://www.netstumbler.com/downloads можно получить две версии: одну для Windows 2000 и более поздних версий и одну для устройств на базе Windows CE, называемую MiniStumbler. На экране 2 показан NetStumbler, работающий на ноутбуке Dell с пакетом XP Service Pack 2 (SP2) и Dell TrueMobile 1400, одним из многих беспроводных адаптеров, совместимых с NetStumbler.

С помощью NetStumbler можно обнаружить несанкционированные AP, просто запустив программу на портативном компьютере и пройдя по территории предприятия с ноутбуком. Обнаруженные узлы доступа отображаются на экране. Таким образом можно получить информацию о MAC-адресе узла доступа, прослушиваемом канале, шифровании и поставщике. Кроме того, NetStumbler показывает отношение сигнал-шум для радиосигнала. Чем выше число, тем меньше расстояние до AP.

Прежде чем удастся обнаружить несанкционированные узлы доступа, необходимо выяснить MAC-адрес и SSID каждого законно установленного AP на предприятии. Развертывая узлы доступа, следует записывать их MAC-адреса, SSID и местоположение. Делая обход с NetStumbler, следует искать узлы доступа с незнакомыми SSID и неизвестными MAC-адресами. Обнаружив незаконные устройства, следует записать их местоположение, затем пройти в разных направлениях и отметить то направление, в котором показатель SNR увеличивается. Если продолжать идти в эту сторону, рано или поздно будет обнаружена AP или по крайней мере очерчена примерная область ее местонахождения для более полного исследования в будущем. Следует учитывать, что AP может находиться на полу или на потолке.

Особенно важно отметить, что опытный хакер может установить AP с таким же SSID, который имеется в сети, в надежде застать врасплох ничего не подозревающих пользователей. Подключившись к несанкционированному AP, пользователи попытаются обратиться к сетевым ресурсам, таким как почтовый сервер и приложения, размещенные в Web. Им не удастся получить доступ к ресурсам через AP взломщика, но пока это выяснится, они могут раскрыть свои пароли и имена. Следует научить сотрудников службы поддержки отслеживать вызовы, связанные с проблемами беспроводной сети, которые могут свидетельствовать о незаконных узлах доступа, и попросить пользователей сообщать об их местонахождении. По поступающим сигналам следует проводить расследование с использованием NetStumbler или других инструментов и проверять MAC-адреса всех AP в этом районе, чтобы убедиться в законности их установки.

Дополнительную информацию о защите беспроводной сети для предприятий любых размеров и даже домашних пользователей можно почерпнуть в превосходной книге Джозефа Дэвиса Deploying Secure 802.11 Wireless Networks with Microsoft Windows (издательство Microsoft Press, 2003). По адресу http://www.microsoft.com/mspress/books/6749.asp можно получить сведения о книге и о том, как ее приобрести, а также найти ссылку на дополнительные материалы. Отличный оперативный ресурс — http://www.microsoft.com/windowsserver2003/technologies/networking/wifi/default.mspx. Данная страница находится в разделе Windows 2003 Web-узла Microsoft.

Безопасность сетей 802.11g — это просто

С новейшими беспроводными точками *доступа атаки хакеров* не *страшны*

Джеф Феллинг

Директор по информационной безопасности компании Quantive. Автор книги IT Administrator's Top 10 Introductory Scripts for Windows (издательство Charles River Media). jeff@blackstatic.com

добство беспроводных сетей неоспоримо: они обеспечивают связь и доступ в Internet за пределами нашего рабочего места или офиса. Стоимость беспроводной точки доступа (Access Point, AP) начального уровня — менее 75 долл., поэтому они стали одними из наиболее популярных периферийных устройств после плейера iPod. Кроме того, достаточно подключить эти устройства к электрической сети, чтобы Wi-Fi-совместимые ноутбуки смогли устанавливать сетевые соединения без проводов. С другой стороны, удобный сетевой доступ связан с огромным риском для сети и данных, так как в выбираемом по умолчанию режиме многих недорогих беспроводных AP злоумышленники могут легко подключиться к сети и похитить данные. К счастью, большинство беспроводных AP располагает простыми процедурами настройки, благодаря которым резко повышается уровень защиты устройств. Выполнив шесть несложных операций, можно надежно защитить небольшую беспроводную сеть с недорогим оборудованием 802.11g.

802.11g — стандарт комитета IEEE, но большинство поставщиков снабжают свои беспроводные AP многочисленными дополнительными возможностями. Однако меры безопасности, как правило, одни и те же, хотя названия похожих функций у разных поставщиков различаются. В примере процедуры настройки в качестве точки доступа используется Linksys WRT54G. Недорогая модель WRT54G широко применяется в малых офисах, домашних офисах и даже лабораториях более крупных компаний. Эта и аналогичные AP не располагают функциональностью корпоративного уровня, как продукты семейств Proxim ORiNOCO или Cisco Systems Aronet; в данной статье рассматриваются способы защиты простых точек доступа начального уровня.

Ненадежная стандартная конфигурация

Недостаток многих недорогих беспроводных AP — акцент на простоту установки в ущерб безопасности. Например, если распаковать и подключить к сети такое устройство, то после активизации беспроводного сетевого адаптера в компьютере с Windows XP Service Pack 2 (SP2) Windows выдаст сообщение об обнаружении новой беспроводной AP и спросит, нужно ли установить соединение с нею. Соединение с сетью после положительного ответа устанавливается моментально.

Производители совершенствуют свои решения: новейшая (пятая) версия распространенной точки доступа Linksys WRT54G располагает мастером SecureEasySetup, в котором объединены аппаратные и программные шаги, необходимые для безопасной настройки AP. В приложении к руководству можно найти ответы даже на сложные вопросы по беспроводной безопасности, которые нередко возникают у пользователя. Однако владельцам более ранних моделей точек доступа Linksys следует проверить процедуру установки, так как в этих моделях многие описанные в статье параметры изначально отключены.

Незащищенная конфигурация выбрана специально; в руководстве для первых моделей Linksys неоднократно указывалось, что маршрутизатор должен корректно функциони-

ровать после подключения к сети. После подключения компьютер может установить соединение с любым другим компьютером сети и даже использовать Internet-соединение. Благодаря функциям беспроводной настройки XP установить соединение с незащищенной AP очень просто. К сожалению, те самые функции, которые облегчают подключение к сети, упрощают задачу любого постороннего владельца Wi-Fi-устройства в радиусе нескольких десятков метров, желающего проникнуть в сеть компании.

В следующих двух разделах будут описаны этапы организации защиты простой беспроводной AP. Изменения в параметрах просты — их может использовать любой администратор беспроводной сети. В описываемой конфигурации применяется чуть более старая модель Linksys WRT54G и предполагается, что читателю известно, как обратиться к экранам настройки AP Старая модель была выбрана по двум причинам: во-первых, многие из этих устройств встречаются в общедоступных местах; во-вторых, в новом устройстве Linksys WRT54G применяется фирменный мастер, тогда как экраны настройки в старых моделях более типичны, и мои рекомендации проще применить к другим продуктам. Даже владельцам новейших моделей любых AP полезно сверить конфигурацию своего устройства с простой процедурой, описанной в данной статье.

Этап 1. Защита AP Administration Page

Первый шаг — изменить выбираемый по умолчанию пароль на вкладке Administration Web-интерфейса точки доступа Linksys. Если беспроводная точка доступа одновременно выполняет функции широкополосного маршрутизатора, необходимо убедиться в возможности управления устройством только с внутреннего интерфейса, а не непосредственно из Internet. Нежелательно, чтобы кто-то установил Web-соединение с общедоступным Internet-адресом через внешний интерфейс беспроводной точки доступа и изменил параметры этого интерфейса, чтобы завладеть AP.

Этап 2. Изменение SSID и запрет широковещательной передачи SSID

В результате изменения или блокировки SSID беспроводной AP случайным взломщикам становится труднее отыскать сеть, но это препятствие не отпугнет даже начинающего хакера. Каждый владелец беспроводного анализатора, такого как NetStumbler (http://www.netstumbler.com), может обнаружить точку доступа и определить ее нестандартный SSID. Узнав SSID точки доступа, взломщик может установить соединение с AP. Тем не менее лучше изменить выбираемое по умолчанию значение SSID, чем открывать его любому обладателю беспроводной точки AP данной модели.

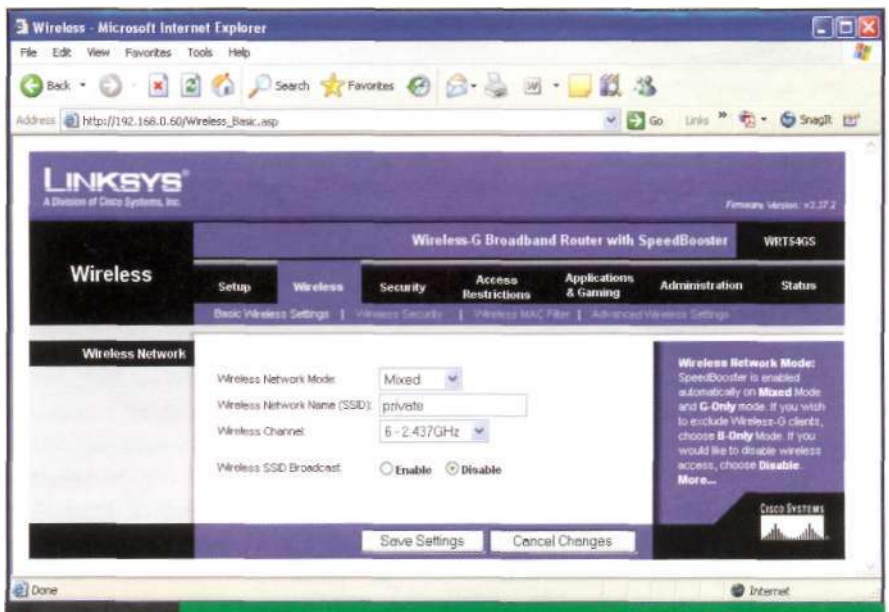
Чтобы изменить SSID, следует перейти в область Basic Wireless Settings вкладки Wireless встроенной программы настройки Linksys и изменить значение Wireless Network Name (SSID), как показано на экране 1. Рекомендуется выбрать неброское имя; например, не стоит использовать название компании или слово Finance. Эти имена могут заинтересовать взломщиков.

На той же странице встроенной программы Linksys следует выбрать режим Disable, чтобы блокировать широковещательную передачу SSID по беспроводной сети (экран 1). После изменения имени SSID и блокировки широковещательной передачи SSID необходимо вручную указать на беспроводных клиентах значение SSID, чтобы установить связь с AP. Шаги для клиента будут описаны ниже.

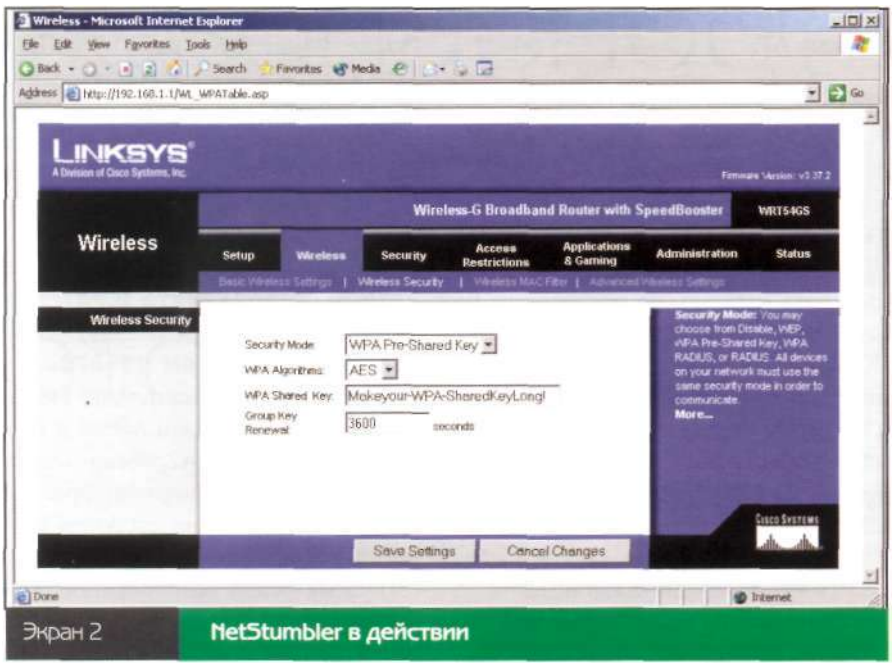
Этап 3. Используйте WPA, если можно, но WEP — все же лучше, чем ничего

Протоколы Wired Equivalent Privacy (WEP), Wi-Fi Protected Access и продолжение WPA, WPA2, обеспечивают общую для поставщиков инфраструктуру для управления доступом и защиты и шифрования данных, пересылаемых между беспроводной AP и беспроводным клиентом. На каждой точке доступа необходимо активизировать WEP или WPA. При возможности выбора между тремя технологиями WPA2 предпочтительнее WPA, а WPA предпочтительнее WEP. В структуре и реализации WEP имеются серьезные недостатки, а разгадать ключ шифрования и взломать защиту WEP можно с помощью целого ряда инструментов.

В основе протокола WPA, который пришел на смену WEP, лежит подмножество стандарта IEEE 802.Hi, а WPA2 основан на окончательной редакции стандарта IEEE 802.11i. В WPA применяется несколько способов и алгоритмов, в частности



Экран 1 Настройка параметров беспроводной сети в XP



Экран 2 NetStumbler в действии

Temporal Key Integrity Protocol (TKIP) и Advanced Encryption Standard (AES), для совершенствования методов управления ключом и шифрования. Большинство современных беспроводных AP совместимы с WPA, а в некоторых старых моделях можно обновить встроенное программное обеспечение, дополнив его функциями WPA, — по этому вопросу необходимо проконсультироваться у поставщика. Но следует помнить, что выбор WPA возможен, только если точка доступа и все клиенты совместимы с WPA.

WEP и WPA шифруют данные, пересылаемые между AP и удаленными клиентами. Говоря простым языком, ключ (строка символов), известный как беспроводной AP, так и клиенту, используется для шифрования и восстановления данных, пересылаемых между этими устройствами. Взломщик, завладевший ключом, может расшифровать данные, пересылаемые между беспроводными AP и клиентом, или установить соединение с беспроводной AP.

Существенный недостаток WEP — необходимость вручную вводить ключ, используемый для шифрования как в беспроводной AP, так и на клиенте. Это трудоемкий процесс, и большинство пользователей вводят ключ один раз и никогда не меняют его. Из-за других недостатков WEP целеустремленные хакеры могут взломать ключ, а затем использовать его для доступа к беспроводной AP или дешифрации данных, передаваемых между беспроводной точкой доступа и клиентами. Поскольку ключ автоматически не изменяется, взломщики могут получить доступ к данным на длительное время, пока кто-нибудь не изменит ключ.

Для устранения этого недостатка протокол WPA дополнен функциями управления ключом. Как и в WEP, ключ здесь используется для шифрования данных. Однако он вводится один раз, а впоследствии с помощью этого ключа WPA генерирует настоящий ключ для шифрования данных. WPA периодически меняет ключ. Следовательно, даже если взломщику повезет и он разгадает ключ шифрования, тот будет полезен только до тех пор, пока беспроводная AP и клиент автоматически не изменят его. По умолчанию ключ шифрования в беспроводных точках доступа Linksys меняется один раз в час.

В старых моделях точек доступа Linksys меры беспроводной безопасности отключены. Чтобы активизировать их, следует нажать на кнопку Wireless Security во вкладке Wireless встроенной программы Linksys. В раскрывающемся окне Security Mode следует выбрать предпочтительный режим беспроводной защиты. В старых моделях Linksys AP реализованы режимы с именами WPA Pre-Shared Key, WPA RADIUS, RADIUS и WEP. В новейшей модели WPA Pre-Shared Key и WPA RADIUS переименованы соответственно в WPA Personal и WPA Enterprise и добавлен протокол WPA2. Большинство поставщиков используют те же технологии, но могут дать им другие имена.

Оптимальный режим для пользователей малого или домашнего офиса — WPA Pre-Shared Key (WPA-PSK) или WPA Personal, который обеспечивает надежную защиту WPA и прост в настройке. Для средних и крупных предприятий предпочтителен режим WPA RADIUS (WPA Enterprise) устройств Linksys с обязательным сервером RADIUS (Remote Authentication Dial-In User Service — служба дистанционной аутентификации пользователей по коммутируемым линиям), хотя такие пользователи, вероятно, пожелают приобрести AP корпоративного класса вместо модели начального уровня, рассматриваемой в данной статье. Более подробно о WPA RADIUS рассказано во врезке «Более тщательная аутентификация». Режим RADIUS в устройствах Linksys, как и WEP, применяется в основном в унаследованных решениях, поэтому его следует выбирать только при наличии беспроводных клиентов, несовместимых с WPA.

Для настройки Linksys для использования режима WPA-PSK нужно выбрать параметр WPA Pre-Shared Key (экран 2). В точках доступа Linksys реализованы два алгоритма WPA: TKIP и AES. TKIP - промежуточная мера, предназначенная для того, чтобы устранить многочисленные проблемы WEP до широкого распространения протокола следующего поколения WPA (WPA2). В TKIP используется тот же алгоритм шифрования, что и в WEP, но многие изъяны WEP устранены благодаря динамической смене ключа шифрования данных, шифрованию данных настройки, пред-

ставленных обычным текстом в WEP, и проверке целостности сообщений. AES — новый, исключительно надежный алгоритм шифрования, используемый в стандарте 802.11i и WPA2. Однако он пока не реализован во всех аппаратных средствах и программном обеспечении. По возможности следует выбирать AES.

Затем вводится ключ WPA Shared Key. Необходимо ввести один и тот же ключ на всех клиентах, которые устанавливают связь с точкой доступа Linksys. Следует выбирать длинный, трудно разгадываемый ключ. В устройствах Linksys его длина может составлять 63 символа, а рекомендуемая длина ключа — не менее 20 символов.

В поле Group Key Renewal указывается, как часто изменяется автоматически генерируемый ключ (в секундах). Как отмечалось выше, выбираемое по умолчанию значение Group Key Renewal — 1 час, что приемлемо для большинства сетей малых и домашних офисов.

Если клиенты несовместимы с WPA, лучше использовать WEP, чем вовсе отказаться от защиты. Для настройки WEP в Linksys WRT54G следует указать режим безопасности (Security Mode) WEP, выбрать ключ для использования в качестве стандартного ключа передачи (ключ с номером от 1 до 4) и тип шифрования WEP, как правило 64- или 128-разрядный (чем больше, тем лучше) с представлением в шестнадцатеричном или ASCII-формате. Ключ следует ввести в поле Key, которое соответствует выбранному стандартному ключу передачи. Например, если выбран 64-разрядный шестнадцатеричный ключ, то можно ввести строку из десяти шестнадцатеричных цифр, такую как af592del29. Эту конфигурацию WEP-ключа необходимо повторить во всех клиентах, поэтому следует выбирать вариант, приемлемый для всех устройств.

Процедура настройки WEP различается между продуктами разных поставщиков в большей степени, чем настройка WPA, поэтому рекомендации по WEP труднее адаптировать к конкретной ситуации.

Этап 4. Для самых малых сетей — фильтрация MAC-адресов

Для дополнительной защиты небольших сетей можно использовать фильтрацию адресов MAC (media access control), которая реализована в большинстве беспроводных AP. Все беспроводные сетевые адаптеры имеют уникальный MAC-адрес. Чтобы узнать MAC-адрес адаптера клиента, достаточно ввести в командной строке клиента следующую команду:

```
ipconfig /all
```

MAC-адреса всех клиентов, которым предстоит обращаться к беспроводной AP, следует ввести в фильтр MAC Address (экран 3). Обратиться к этой странице можно из вкладки Wireless встроенной программы точки доступа Linksys. Только указанные в списке фильтра адаптеры смогут устанавливать связь с AP.

Некоторые программы могут подделывать MAC-адреса, а пользователи иногда меняют свои Wi-Fi-адаптеры, поэтому, хотя с помощью фильтрации MAC-адресов можно остановить случайных взломщиков, метод не так безопасен, как более надежные механизмы аутентификации, в частности WPA RADIUS на базе 802.1x. Своевременно обновлять список MAC-адресов трудно для любых сетей, кроме действительно очень небольших. Однако фильтрация MAC-адресов поможет остановить злоумышленника, получившего общий ключ WPA от сотрудника предприятия, хотя опытный хакер может обойти и MAC-фильтр.

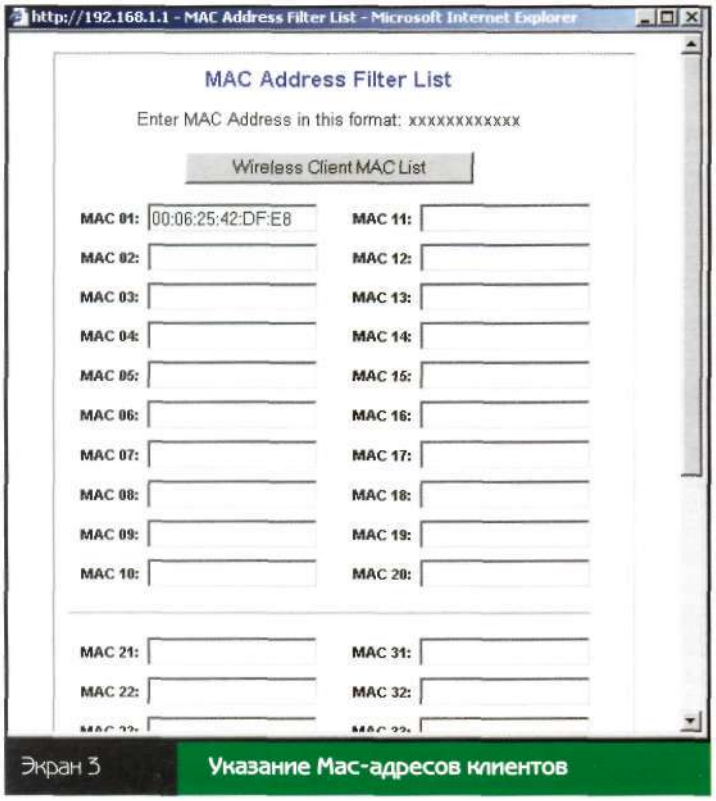
Более тщательная аутентификация

В режиме WPA Pre-Shared Key (WPA-PSK) любое клиентское устройство с корректным общим ключом может получить доступ к сети, связанной с беспроводной точкой доступа. Общий ключ легко назначить, но у него есть ряд недостатков. Во-первых, сетевой администратор должен вручную ввести верный общий ключ на каждом беспроводном клиенте. Кроме того, общий ключ не гарантирует авторизации или одобрения всех подключенных устройств. Например, если один пользователь сообщает такой ключ другому пользователю, то оба устройства успешно устанавливают соединение с беспроводной AP.

Чтобы решить данную проблему, необходимо аутентифицировать всех пользователей или устройства, подключенные к беспроводной AP. Функция WPA RADIUS устройства Linksys WRT54G (называется WPA Enterprise в новейшей версии продукта) обеспечивает ряд дополнительных возможностей аутентификации входящих клиентов.

Стандарт аутентификации IEEE 802.1x используется в WPA RADIUS для проверки всех новых беспроводных устройств на удаленном сервере RADIUS. После того как настроенный сервер RADIUS успешно аутентифицирует клиента, соединение будет одобрено и беспроводная AP разрешит устройству подключиться к сети. Компания Microsoft поставляет сервер RADIUS — службу Internet Authentication Service (IAS) — в составе Windows Server 2003. Благодаря серверу RADIUS возможности аутентификации значительно расширяются, в частности можно потребовать у клиентов использования доменного пароля и имени пользователя, смарт-карт или сертификатов, прежде чем разрешить им соединение с беспроводной AP.

Чтобы активизировать WPA RADIUS или WPA Enterprise в точке доступа Linksys WRT54G, требуется ввести IP-адрес сервера RADIUS и общий ключ RADIUS. Необходимо также настроить сервер RADIUS, такой как Windows 2003, с запущенной службой IAS. На Web-узле Microsoft TechNet представлено несколько руководств для настройки сертификатов, RADIUS и беспроводных сетей. Более подробно о 802.1x рассказано в статье «Безопасная беспроводная сеть», опубликованной в Windows IT Pro/RE № 4 за 2004 год, и в статье «Как защитить WLAN с помощью сертификатов» из № 3 за 2005 год. Настроить WPA RADIUS несложно, но процедура несколько более трудоемкая; для пользователей малых и домашних офисов WPA-PSK обеспечивает хороший баланс безопасности и простоты управления.



Экран 3 Указание Mac-адресов клиентов

Экран 4 Настройка параметров безопасности в XP SP2

Этап 5. Изоляция беспроводной точки доступа

Следует обратить внимание на место соединения беспроводной AP с сетью. Точка доступа Linksys оснащается сетевым экраном, и большинство пользователей задействуют устройство не только как беспроводную AP, но и в качестве Internet-шлюза. Если доверие к беспроводной сети меньше, чем к проводной, то для передачи конфиденциальной информации рекомендуется подключить беспроводную AP между брандмауэром проводной сети и Internet. Устанавливая беспроводную AP на периметре сети, можно еще более сузить круг компьютеров внутренней сети, к которым могут обращаться беспроводные клиенты.

Этап 6. Настройка конфигурации клиентов

Защита беспроводной AP — лишь одна часть уравнения. Необходимо еще настроить параметры безопасности беспроводных клиентов. Чтобы максимально расширить возможности защиты, следует установить на клиентах операционную систему XP SP2 и новейшие драйверы беспроводных сетевых адаптеров. По возможности следует выбрать беспроводные платы, совместимые с WPA или WPA2. Текущие модели беспроводного адаптера Linksys с новейшим программным обеспечением во встроенной постоянной памяти и драйверами поддерживают как WPA и WPA2, так и алгоритмы шифрования TKIP и AES.

Чтобы назначить беспроводному клиенту такие же параметры шифрования, как в AP, следует щелкнуть на Start, Connect To, Wireless Network Connection, View Available Wireless Networks, Change Advanced Settings. Затем требуется перейти на вкладку Wireless Networks и щелкнуть на кнопке Add в разделе Preferred networks, чтобы открыть диалоговое окно свойств беспроводной сети. Другой способ — щелкнуть правой кнопкой мыши на адаптере беспроводной сети, а затем на пункте Properties. Следует выбрать вкладку Association (экран 4).

Чтобы настроить клиентов на соединение с беспроводной AP с нестандартным SSID, необходимо ввести имя сети (т. е. SSID) беспроводной AP, в данном случае private. Если беспроводная AP и другие беспроводные клиенты поддерживают WPA-PSK и AES, нужно выбрать эти значения для полей Network Authentication и Network Authentication соответственно. Затем требуется ввести общий ключ, назначенный для беспроводной AP. На этом завершаются настройки, которые необходимо выполнить в данном диалоговом окне. Если приходится работать с WEP, то необходимо поменять режим Network Authentication на открытый или совместный, изменить тип шифрования на WEP и ввести индекс и ключ, точно соответствующие конфигурации ключа точки доступа. После того как параметры клиента будут точно соответствовать параметрам беспроводной AP, клиент должен автоматически установить соединение и может безопасно обмениваться данными с беспроводной AP.

Защищаем конфиденциальные данные

Сфера применения беспроводных сетей расширяется, в чем легко убедиться, если просто пройтись по любому городу с Wi-Fi-ноутбуком или PDA. По пути вам встретится немало открытых беспроводных AP, подключиться к которым не составляет труда. Так что самое время защитить свою сеть от любопытных глаз с помощью простых мер безопасности.

Использование и настройка резервирования в Outlook

Автоматическое *резервирование ресурсов* при *помощи Outlook*

Джозеф Ньюбауэр
Старший технический консультант HP, специалист по Windows и Microsoft Exchange Server.
joseph.neubauer@hp.com

Совместное использование возможностей Exchange Server и Outlook предоставляет мощные средства планирования расходования ресурсов. Если в сети у всех пользователей в качестве почтового клиента установлен Outlook 2000 или старше, можно реализовать возможность, которую в Microsoft называют прямым резервированием (direct booking). В данном обзоре я объясню, как настроить прямое резервирование, приведу некоторые предостережения относительно использования и несколько советов, которые помогут сделать работу с данным средством более удобной для пользователя.

Прямое резервирование ресурса

До появления Exchange и Outlook, если требовалось использовать какой-либо ресурс, например комнату для конференций или аудиооборудование, приходилось связываться с отвечающим за это сотрудником, который сверялся с расписанием и говорил, когда данный ресурс будет доступен. Механизм прямого резервирования избавляет от необходимости контактировать с другим лицом с целью проверки доступности ресурса и резервирования времени для его использования; технология прямого резервирования позволяет планировать встречи непосредственно из приложения Outlook Calendar.

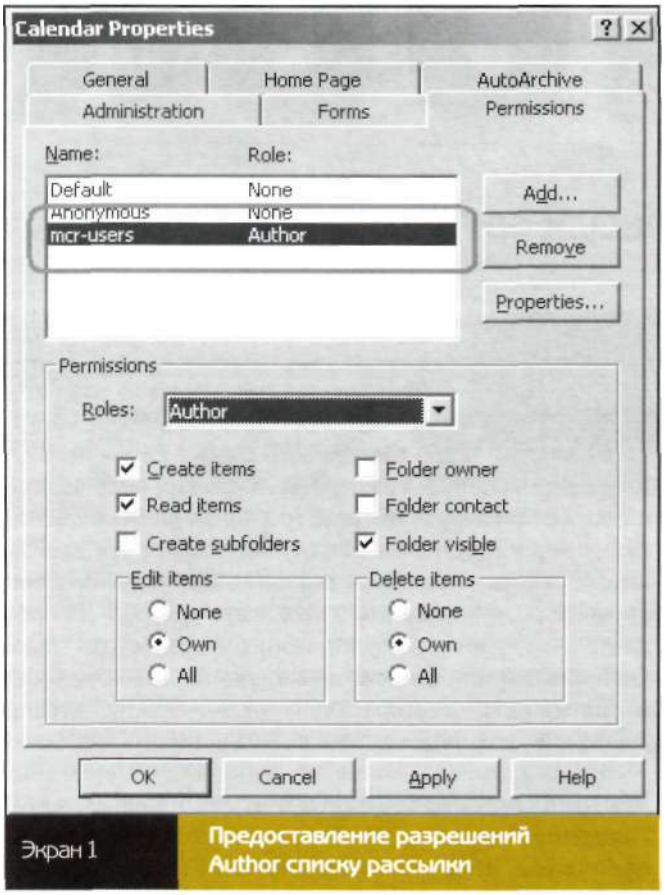
Начиная с пакета Outlook 97 можно реализовать элементарную форму прямого резервирования, настроив почтовый ящик клиента, отвечающего за ресурс, на автоматическое утверждение запросов о сетевых встречах. Так как клиент Outlook обрабатывает входящие запросы календаря аналогично входящим запросам о совещаниях, приходится поддерживать почтовый клиент в запущенном состоянии для проверки ресурсов и конфликтов. В версии Outlook 2000 специалисты Microsoft расширили возможности пакета Outlook в отношении данных задач резервирования. Удерживать Outlook в активном состоянии и писать сценарии для сервера больше не требуется. Outlook пользователя, организующего встречу, выполняет все необходимые задачи, такие как поиск конфликтов и запись времени резервирования в календарь ресурса. Для реализации прямого резервирования понадобится пакет Outlook 2000 или выше и правильно настроенный почтовый ящик на сервере Exchange Server 5.5, Exchange 2000 Server или старше.

Настройка ресурса: три шага

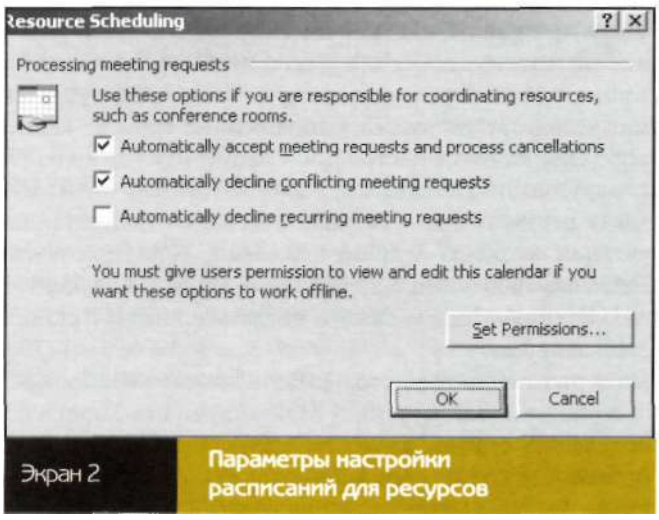
Первым шагом в настройке ресурса, который требуется сделать доступным для пользователей (например, простой ресурс Main Conference Room, использовавшийся мною при работе над данной статьей), является создание почтового ящика для хранения календаря ресурса. Кроме предоставления самому себе прав доступа, администратору не нужно выполнять на сервере какие-либо специальные настройки. Следует иметь в виду, что в окружении Exchange 5.5 можно связать почтовый ящик ресурса Main Conference Room с существующей учетной записью Windows. Однако, если применять Exchange 2000 и выше, необходимо создать новую учетную запись Windows 2000 и связать почтовый ящик с этой записью.

На втором шаге требуется создать профиль Outlook для доступа к почтовому ящику Main Conference Room и использовать его при запуске Outlook. Следует щелкнуть правой кнопкой мыши на папке Calendar, выбрать пункт Properties, потом выбрать закладку Permissions.

Также можно изменить роль пользователя, заданного по умолчанию, или добавить список рассылки (DL), состоящий из пользователей, которым необходимо разрешение для резервирования ресурса. Добавлять DL обычно предпочтительнее, чем изменять разрешения, заданные по умолчанию, так как DL обеспечивает более полный контроль над использованием ресурса. Как показано на экране 1, я добавил DL, названный mcr-users, и присвоил ему роль Author. Получение разрешений категории Author дает возможность пользователям, указанным в списке DL, резервировать ресурс и изменять свои заказы, но запрещает изменение заказов, сделанных другими пользователями. Указав в качестве роли значение Author, следует закрыть диалоговое окно Properties нажатием кнопки OK.



Экран 1 Предоставление разрешений Author списку рассылки



Экран 2 Параметры настройки расписаний для ресурсов

И наконец, третий шаг: выбор пункта Options в меню Tools в Outlook. Выбрав пункт Preferences, следует нажать на вкладке Calendar Options. В результате нажатия кнопки Resource Scheduling на экране появится три поля (см. экран 2). Необходимо установить флажки для первых двух полей Automatically accept meeting requests and process cancellations и Automatically decline conflicting meeting requests. Последний флажок, Automatically decline recurring meeting requests, надо оставить пустым, если вы не хотите, чтобы пользователи заказывали повторное использование данного ресурса.

Далее следует трижды нажать OK, чтобы выйти из окна Options, после чего закрыть Outlook. Теперь почтовый ящик ресурса готов принимать заказы.

Резервирование ресурса

Чтобы зарезервировать ресурс, нужно просто создать запрос о встрече, указывая в соответствующих полях обязательных и желательных участников и требуемый ресурс (т. е. Main Conference Room) в поле Resources, как показано на экране 3. Нажмите кнопку OK, и Outlook попытается зарезервировать ресурс. Если запрашиваемое время свободно, на экране появится подтверждающее сообщение (см. экран 4), а Outlook разошлет участникам приглашения. Если ресурс занят, система выдаст сообщение с отказом, а Outlook не будет рассылать приглашения — вместо этого он предложит изменить запрос. Поскольку Outlook не рассылает приглашения, ничто не мешает вам послать один или несколько обновленных запросов о встрече, пытаясь найти временное «окно». Участникам тоже не придется отзываться на многочисленные обновления времени встречи и выяснять, когда точно вы хотите провести мероприятие, что часто случается, когда отправляется множество обновленных запросов о встрече.

Принцип работы прямого резервирования

Когда организатор встречи указывает почтовый ящик как ресурс в запросе о собрании, Outlook выполняет несколько шагов в случае, если кто-то из пользователей отправляет запрос. Прежде всего Outlook считывает информацию о настройках из указанного почтового ящика, чтобы определить, нужно ли пытаться осуществить прямое резервирование. Вы задаете эту информацию, когда устанавливаете флаги в различные поля в диалоговом окне Resource Scheduling. Если не поставить флаг в поле Automatically accept meeting requests and process cancellations, Outlook посылает запрос о собрании на почтовый ящик ресурса, как будто он является одним из участников. Если выбрано это поле, клиент Outlook организатора встречи заказывает ресурс следующим образом: если вдобавок к первому полю выбран пункт Automatically decline conflicting meeting requests, Outlook считывает информацию о занятости в календаре почтового ящика и с ее помощью определяет, свободен ли ресурс в запрашиваемое время. Если ресурс свободен,

Outlook заносит напоминание прямо в календарь ресурса. Если выбрано поле Automatically decline recurring meeting requests, Outlook будет отклонять повторяющиеся запросы.

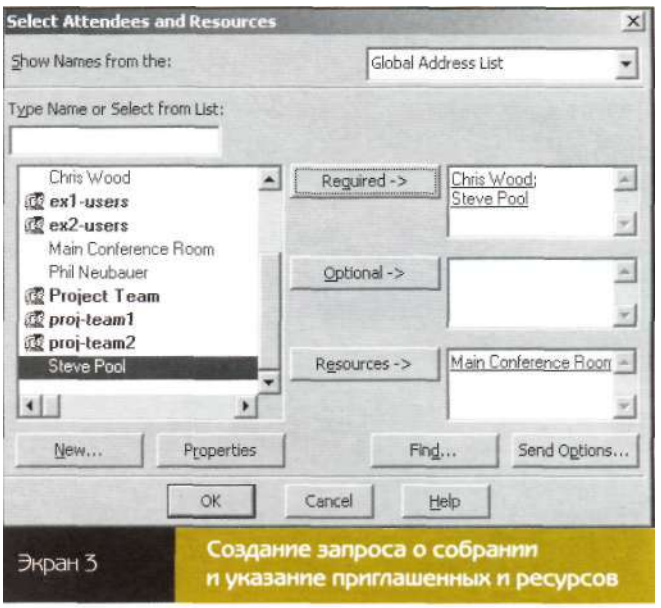
Если запрашиваемые для встречи часы свободны, вы получаете подтверждение того, что ресурс заказан, а Outlook рассылает приглашения обязательным и желательным участникам. Он не посылает приглашение на почтовый ящик ресурса, так как Outlook уже включил напоминание в календарь. Если пользователь, не обладающий хотя бы разрешением класса Author, попытается осуществить прямое резервирование ресурса, он получит уведомление о том, что его прав недостаточно.

Ловушки прямого резервирования

Настройка прямого резервирования является относительно простой задачей. Однако я считаю необходимым рассказать о некоторых ловушках, перед тем как вы начнете практическое использование функции прямого резервирования.

Доступность информации о занятости. Технология прямого резервирования использует информацию о занятости, чтобы определить доступность ресурса. Система Exchange хранит в скрытой общей папке информацию о занятости почтовых ящиков на 12 месяцев: текущий месяц, прошлый месяц и до 10 месяцев в будущем. Например, если сегодня 15 марта 2006 года, система будет хранить информацию с 1 февраля 2006 года по 31 января 2007 года. Хотя половина марта уже позади, система хранит информацию о занятости только до 31 января и не будет содержать информацию на период с 1 по 14 февраля 2007 года, пока не наступит 1 апреля 2006 года. Когда используется прямое резервирование ресурса за границей периода хранения информации о занятости в будущем, система не способна обнаружить конфликт, который может возникнуть при наложении встреч. Например, когда до наступления 1 апреля 2006 года два организатора назначают встречу на 14:00 17 февраля 2007 года. Каждый из организаторов будет считать, что он успешно зарезервировал ресурс для встречи в будущем году.

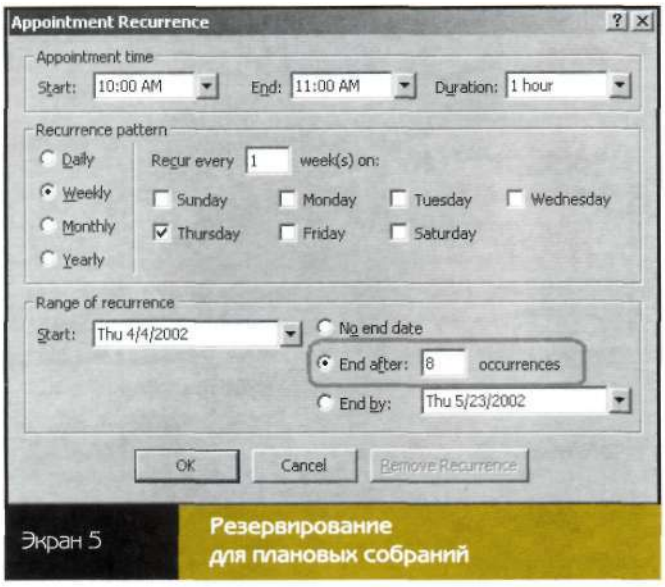
Информация о занятости в Outlook. Другой ловушкой прямого резервирования является количество информации о занятости, публикуемое каждым клиентом Outlook. Так как функции прямого резервирования зависят отданных о занятости, вы хотите публиковать максимальное количество информации. По умолчанию клиенты Outlook публикуют данные о занятости за два месяца (текущий и следующий). Настройки данных о занятости не только определяют, какое количество информации Outlook публикует для календаря отдельного пользователя, но и влияют на то, какой объем информации Outlook публикует при обновлении данных о занятости ресурса. Это означает, что клиент Outlook организатора встречи обновляет данные о занятости учетной записи ресурса, когда система успешно осуществляет заказ. Необходимо настроить все клиенты Outlook так, чтобы они публиковали информацию за 12 месяцев (максимальный период), тогда функция прямого резервирования сможет пресекать максимальное число конфликтов.



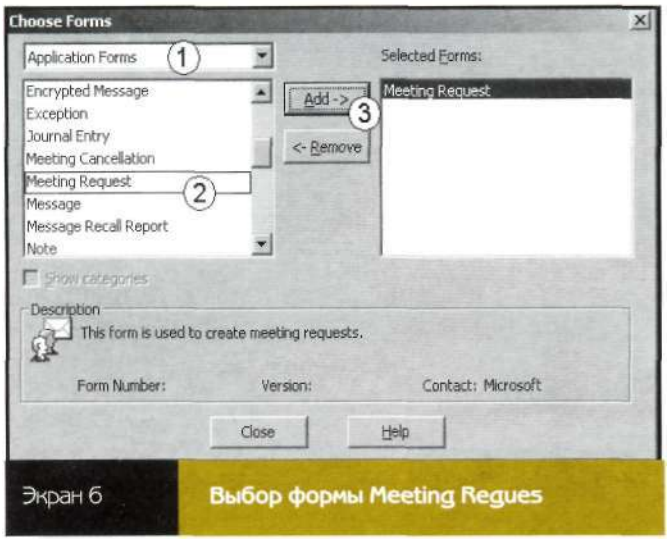
Экран 3 Создание запроса о собрании и указание приглашенных и ресурсов

Экран 4 Сообщение об успешном резервировании

Проблема, связанная с информацией о занятости, заключается в том, как система хранит данные о занятости в общей папке и управляет ими и как клиенты Outlook обновляют эту информацию. Exchange хранит данные о занятости календаря каждого почтового ящика в отдельных записях в общей папке. Когда кто-то планирует напоминание, система не добавляет новую информацию к существующей. Вместо этого клиент Outlook планировщика повторно генерирует время занятости и переписывает набор данных. Такой метод допустим, если вы настроили все свои клиенты на публикацию одинакового количества данных о занятости. Однако зачастую один или более клиентов настроены на публикацию данных менее чем за 12 месяцев. Так как Outlook по умолчанию публикует данные о занятости за 2 месяца, существующий набор данных будет содержать информацию о занятости либо за 2, либо за 12 месяцев. В зависимости от этого срока клиент Outlook создает последние запросы о встрече и обновляет данные о занятости. Если обновленный набор данных имеет временной диапазон менее 12 месяцев, функции



Экран 5 Резервирование для плановых собраний



Экран 6 Выбор формы Meeting Regues

прямого резервирования могут не иметь достаточной информации для обнаружения конфликтов при планировании.

Рекуррентные запросы. Рекуррентные запросы о встречах, которые я рассматриваю как ошибки, возникают, когда кто-либо обновляет рекуррентный запрос с целью продлить период его действия. Скажем, один сотрудник удачно заказывает комнату для конференций на 4 недели, начиная с первого четверга апреля, с 10:00 до 11:00, для проведения серии лекций (4, 11, 18 и 25 апреля). Другой сотрудник резервирует комнату с первого четверга мая (2 мая) также с 10:00 до 11:00. Первый сотрудник принимает решение расширить серию лекций до 8 недель и обновить рекуррентные настройки в серии встреч, добавив 4 недели в мае (2, 9, 16 и 23 мая), как показано на экране 5. Нажав кнопку Send Update в своем запросе, он получает отказ, так как возникает конфликт во встречах 2 мая. Этот отказ вполне понятен, но Outlook также удаляет его изначально зарезервированные часы встреч в апреле из календаря комнаты для конференций, и у первого сотрудника больше нет зарезервированного времени. Функция прямого резервирования не рассматривает его действия как изменение. Вместо этого она считает, что данное расширение представляет собой первую попытку резервирования ресурса. Единственным способом восстановить бронь и сохранить ее связь с запросом о встрече — снова изменить период действия запроса и нажать кнопку Send Update. К сожалению, этот метод в результате отправляет уведомление об обновлении времени встречи всем участникам.

Делегирование. Следующая ловушка касается делегирования (т. е. ассистентов, уполномоченных запланировать встречи для своих менеджеров). Если ассистент отправляет запрос о встрече от имени менеджера и удачно резервирует ресурс с помощью прямого резервирования, запросы прибудут в ящики участников от менеджера. Но так как разрешения класса Author привязаны к календарю ресурса, именно ассистент, а не менеджер резервирует время в календаре. Если менеджер попытается обновить запрос о встрече (например, изменить время встречи), он получит сообщение об ошибке, связанной с отсутствием необходимых прав. Нужно иметь в виду, что роль Author дает право изменять свои заказы, но не заказы, созданные другими людьми.

Поле Resources. Ловушка, связанная с полем ресурсов, возникает из-за того, что клиент Outlook лучше, чем Exchange, выполняет функции прямого резервирования. Единственный способ приказать Outlook попробовать осуществить прямое резервирование ресурса — указать ресурс в поле Resources в форме запроса на встречу. Многие по ошибке определяют ресурс как обязательного или желательного участника, прописывая его в поле To. После этого Outlook отсылает запрос в папку входящих сообщений ресурса, где он и будет лежать без ответа. В этом случае люди ошибочно предполагают, что зарезервировали ресурс, так как не получили отказа.

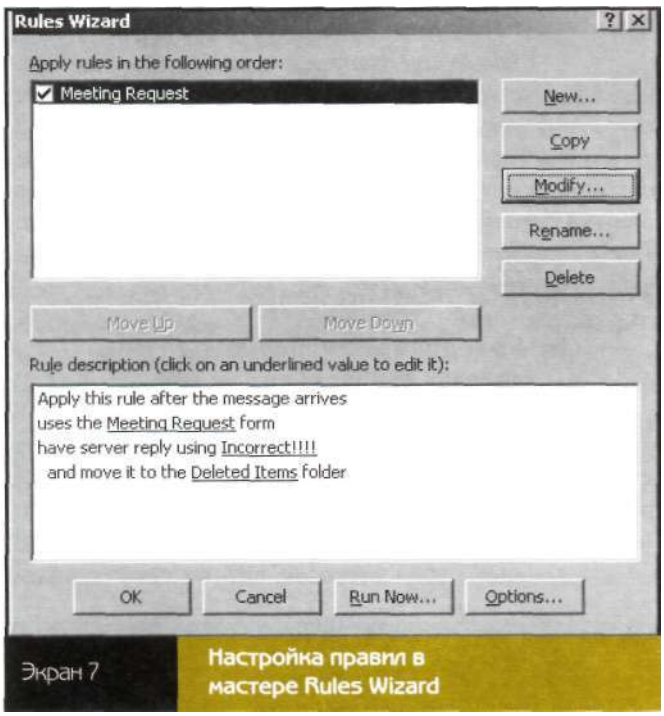
Меры по улучшению

Некоторые описанные ловушки устраняются только через обновления Outlook. Сотрудники, которые будут резервировать ресурсы, должны разбираться в ограничениях прямого резервирования (например, ограничение в 12 месяцев при хранении информации о занятости) и работать в рамках этих ограничений. Другие проблемы, например с клиентами, настроенными на публикацию данных менее чем за 12 месяцев, и такие, как ошибочное указание ресурса в качестве участника, решаются достаточно просто.

Чтобы убедиться, что каждый клиент публикует информацию о занятости за 12 месяцев, нужно запустить редактор реестра и открыть раздел реестра HKEY_CURRENT_USER\Software\Microsoft\Office\<version>\Outlook\Preferences\FBPublishRange, где для Outlook XP параметр version имеет значение 10.0, а Outlook 2003 — 11.0. Этот параметр содержит шестнадцатеричное значение, так что для публикации данных за 12 месяцев следует установить значение параметра в «c». Таблица 1 отображает шест-

надцатеричные эквиваленты номеров месяцев, данные по которым требуется публиковать. Простейший способ убедиться в том, что все клиенты публикуют максимальное количество информации о занятности, — использовать системную политику или сценарий регистрации для проверки корректности установки значения этого параметра. Дополнительную информацию можно найти в статье Microsoft XCLN: How to Configure Default Free/Busy Options (http://support.microsoft, com/default. aspx?scid=kb;en-us;ql97712).

Для того чтобы предупредить людей, что они по ошибке указали ресурс в качестве участника, можно создать на сервере правило, подразумевающее отправление организатору встречи электронного письма с сообщением об ошибке. Для настройки этой возможности следует открыть почтовый ящик ресурса, используя профиль службы Outlook, с помощью которого выполнялась изначальная настройка функции прямого резервирования (в три этапа). Необходимо открыть папку Inbox и выбрать пункт Rules Wizard в меню Tools в Outlook. Затем нужно нажать кнопку New для создания правила. Поставьте флажок Check messages when they arrive и щелкните Next для отображения состояний, инициирующих правило. Если используется Outlook 2002, режимом, устанавливаемым по умолчанию для нового правила, является режим Start creating a rule from a template; требуется выбрать возможность Start from a blank rule option для отображения состояния Check messages when they arrive. Выберите состояние Uses the form name form. В секции описания правила нужно нажать на поле form name, чтобы отобразить диалоговое окно Choose Forms. Поменяйте в списке Personal Forms на Application Forms, потом выберите форму Meeting Request из списка и нажмите кнопку Add, как показано на экране 6.



Экран 7 Настройка правил в мастере Rules Wizard

Таблица Номера месяцев в шестнадцатеричной системе

Номера месяцев	Шестнадцатеричные числа
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	a
11	b
12	c

Теперь требуется нажать кнопку Close в диалоговом окне Choose Forms, затем — кнопку Next в мастере Rules Wizard, чтобы указать действие. Выберите действия move it to the specified folder и have server reply using a specific message. В секции описания правила следует нажать на подчеркнутое слово specified, выбрать папку Deleted Items Folder из списка папок и нажать OK. Также в секции описания правила нужно щелкнуть на фразе a specific message для отображения окна структуры нового сообщения. В качестве предметной строки следует ввести You incorrectly attempted to reserve a resource, установить приоритет сообщения в значение High и ввести в тело сообщения текст, объясняющий, что организатор встречи получил это сообщение, так как ошибочно указал ресурс в качестве участника. Необходимо указать, что организатор не имеет подтвержденной брони на использование ресурса, и описать шаги, которые следует предпринять для исправления ошибки (т. е. указать ресурс в поле Resources). После того как вы создали сообщение, нажмите кнопку Save, а потом — Close. Вернувшись в окно мастера Rules Wizard, щелкните Next дважды, чтобы отобразить последнюю страницу мастера. На этой странице требуется указать имя правила и установить флаг в поле Turn on this rale. Нажмите Finish. Должно появиться описание правила, которое выглядит примерно так, как показано на экране 7. Если организатор встречи непреднамеренно указал ресурс в качестве участника, он получит электронное сообщение, информирующее об ошибке.

Сделай сам

Прямое резервирование в Outlook может иметь некоторые ограничения, но в общем реализовать его несложно. Я обнаружил, что организации тяжело привыкают к другим решениям, базирующимся на сценариях или кодах событий, так как не имеют компетентного персонала для внедрения и отладки этих решений. Устранив необходимость вручную утверждать и отвергать ресурс, прямое резервирование в Outlook позволяет сотрудникам резервировать ресурсы быстро и эффективно.

Команда управления энергопотреблением компьютера

Марк Минаси

Редактор Windows NT Magazine MCSE и автор книги Mastering Windows NT Server 4.0 (издательство Sybex). С ним можно связаться по адресу: mark@minasi.com

Я уже не раз писал о новых полезных функциях Windows XP SP2, и теперь пришло время рассказать о возможностях команды Powercfg, предназначенной для управления режимами энергопотребления. Команда Powercfg действует почти так же, как приложение «Электропитание» в панели управления, обеспечивая при этом более детальные средства настройки электропитания. Утилита Powercfg включена в состав Windows Server 2003, а в XP SP1 вошла версия с ограниченными возможностями.

Из всего множества параметров командной строки утилиты Powercfg я рассмотрю только две возможности — управление яркостью ЖК-панели ноутбука и снижение скорости центрального процессора в энергосберегающем режиме.

Уменьшение яркости экрана

В последние два года ноутбуки продавались значительно лучше, чем настольные компьютеры. Одна из главных особенностей ноутбуков в том, что блок управления электропитанием является важнейшим элементом их конструкции, вокруг которого строятся другие функции. Управление электропитанием помогает экономить энергию и повышает мобильность, но оно же может приводить к нежелательным эффектам. Как-то мой приятель пожаловался, что у его нового ноутбука неожиданно уменьшается яркость экрана и даже при максимальной яркости становится трудно читать информацию на экране. Я занялся решением этой проблемы.

У многих ноутбуков есть функциональные клавиши, которые позволяют контролировать яркость экрана, однако ни эти клавиши, ни панель управления не помогают настроить постоянную яркость. Для устранения эффекта снижения яркости я предлагаю воспользоваться следующей командой:

```
powercfg /g off /option videodim
```

Параметр /g является глобальным, он включает помимо параметра videodim еще четыре параметра: wakeonring, batteryicon, multibattery и resumepassword. Рассмотрим их подробнее. Параметр wakeonring в панели управления отсутствует. Как следует из названия, он включает или выключает возможность запуска компьютера из режима ожидания или «спячки», когда на какие-то аппаратные устройства воздействует внешний сигнал (например, входящий звонок на модем). Можно настроить и остальные три глобальные параметра — batteryicon (показывает значок батареи на системной панели), multibattery (показывает столько значков батареек, сколько их находится в ноутбуке) и параметр resumepassword (запрос пароля в случае возобновления работы из режима ожидания или «спячки»).

Замедление скорости работы процессора

Случалось ли вам при запуске тестов скорости работы процессора обнаружить, что процессор ноутбука 1,5 ГГц Pentium работает всего на 700 МГц? В этом и заключается управление электропитанием. Windows включает несколько стандартных схем управле-

ния питанием. Эти схемы определяют настройки отдельных параметров в различных режимах — интервалы простоя до выключения монитора и жесткого диска, время до переключения в режим ожидания/«спячки» и т. д. Вроде бы в панели управления все это есть. Но там нет «пятого элемента» — processor throttle для управления процессором. Этот элемент управления позволяет Windows замедлять скорость процессора для более экономичного режима расхода энергии. Параметр processor throttle может принимать четыре значения: none, constant, degrade и adaptive.

None. Значение none не разрешает компьютеру замедлять скорость процессора даже в том случае, когда он не выполняет полезной работы и батарейка «выдохлась».

Constant. Значение constant предписывает процессору работать на самой низкой скорости. И эта скорость может действительно быть низкой. В системе, которой я сейчас пользуюсь, в режиме constant скорость процессора понижается с 1,7 ГГц до 600 МГц. Это минимальная тактовая частота, или, в терминах управления питанием, минимальное быстродействие, заданное изготовителем процессора.

Degrade. Значение degrade переводит систему на самую низкую допустимую тактовую частоту (как в режиме constant), и для большего замедления и экономии энергии использует функцию пропускания тактов stop clock throttling (или линейного уменьшения быстродействия linear performance reduction). Диаграммы stop clock throttling, которые я просматривал, наводят на мысль, что в этом режиме на короткое время глушится сигнал от генератора тактовой частоты процессора. В этом случае процессор сохраняет минимальную тактовую частоту — для моего ноутбука Pentium это 600 МГц. Работа процессора на самой низкой скорости сокращает энергопотребление еще больше, но это означает, что процессор функционирует не в допустимой области тактовых частот, заданной изготовителем. Однако такая процедура с постоянными пропусками тактов, а не просто понижением тактовой частоты приводит к тому, что процессор считает, что он получает минимально приемлемую тактовую частоту на входе, хотя на самом деле в этот момент работает даже медленнее, чем при минимальной тактовой частоте. И в результате достигается еще меньшее потребление энергии.

Adaptive. При использовании параметра adaptive сначала определяется, какая мощность процессора необходима системе, а затем процессор запускается с максимально низкой возможной скоростью для выполнения процессов. По-видимому, параметр adaptive обеспечивает самую гибкую настройку ускорения процессора, однако то, как процессор использует эту настройку, зависит от его типа. Каждая микросхема имеет свой драйвер для управления мощностью.

Итак, для уменьшения скорости процессора и увеличения времени автономной работы используется четыре параметра: none, adaptive, constant и degrade. Для настройки значения мощности процессора применяется команда:

```
powercfg /x <имя схемы питания>
 /processor-throttle-ac <регулировка>
```

где <имя схемы питания> принимает значения portable/ laptop, max battery, home/office desk или любой профиль пользователя для управления электропитанием, а параметр <регулировка> принимает значения none, adaptive, constant или degrade. Эта команда установит электропитание при включении системы в розетку, при изменении значения processor-throttle-ac на processor-throttle-dc будет осуществлен переход на автономное питание. Например, для задания профиля управления электропитанием home/office desk на моей системе, чтобы использовать адаптивное управление процессором, я ввожу две команды:

```
powercfg /x «home/office desk»
 /processor-throttle-ac adaptive
powercfg /x «home/office desk»
 /processor-throttle-dc adaptive
```

При желании узнать, как влияют настройки мощности на реальную тактовую частоту процессоров Pentium, можно воспользоваться утилитой идентификации процессора Intel Processor Identification Utility (http://www.intel.com/support/processors/tools/piu), которая покажет номинальную скорость микросхемы и реальную ее скорость в данный момент. Для процессоров AMD существуют специальные утилиты для тестирования тактовой частоты. Полезная программа PowerNow! Dashboard для процессоров AMD (http://www.amd.com/usen/Processors/ComputingSolutions/0,30_288_1276_964,00.html) покажет скорость процессора ноутбука в любой момент работы.

К моему удивлению, на моем втором ноутбуке с Turion при установке мощности в режим adaptive оказалось, что тактовая частота процессора постоянно плавает. Возможно, что без утилиты для AMD я бы никогда не узнал, что скорость работы процессора может меняться так часто. Другими словами, просто удивительно, как часто мы все еще работаем в диапазоне частот до 1ГГц и не испытываем при этом никаких неудобств. Возможности команды Powercfg гораздо шире, но я очень доволен, что с ее помощью могу избавиться от эффекта уменьшения яркости экрана, она помогла мне лучше контролировать снижение скорости процессора для экономии электричества. Мой следующий проект будет посвящен созданию командного файла, который можно использовать для установки настроек электропитания системы из командной строки — ее возможности существенно облегчат работу при настройке новых серверов и рабочих станций.

Советы по повышению производительности VM

Технология виртуальных машин, Virtual Machine (VM), обеспечивает отличную гибкость в работе, но за счет снижения производительности. Конечно, новые процессоры помогут повысить производительность VM, но пока имеет смысл использовать подручные средства оптимизации как для VM-продуктов Microsoft, так и для VMware.

Майкл Отп

Старший технический редактор Windows IT Pro и президент компании TECA. С ним можно связаться по адресу: mikeo@teca.com

10 Устанавливайте специальные утилиты. Не забывайте устанавливать утилиты, которые идут в комплекте с VM; они повышают производительность видео и упрощают манипулирование мышью за счет оптимизации работы видеодрайвера SVGA.

9 Используйте достаточное дисковое пространство. Каждая VM требует от 4 до 50 Гбайт (иногда больше) места на диске. Производительность может падать, если свободного места недостаточно. На устройстве, где размещаются образы виртуальных дисков, следует иметь по крайней мере 20% свободного дискового пространства.

8 Отключайте визуальные эффекты в гостевых операционных системах. Визуальные эффекты гостевых систем расходуют ресурсы процессора и памяти. Чтобы отключить ненужные эффекты в Windows XP, следует открыть контекстное меню рабочего стола гостевой операционной системы, выбрать Properties, Appearance, Effects и убрать флажок «Use transition effects for menus». В Windows 2000 выполняется аналогичная процедура.

7 Заранее выделяйте место для виртуального жесткого диска. По умолчанию виртуальные жесткие диски от большинства производителей VM настроены на динамическое расширение в случае необходимости. Динамическое расширение экономит дисковое пространство, но снижает производительность гостевой операционной системы. Чтобы устранить это снижение, следует отказаться от динамического расширения при создании виртуального диска.

6 Используйте связанные (Raw или Linked) виртуальные диски. Применение Raw- или Linked-дисков (терминология у разных производителей различна) позволяет VM напрямую читать с диска и писать на диск. В результате можно избежать непроизводительных издержек при использовании других типов дисков. Эта техника может ускорить работу приложений, для которых производительность дисковой подсистемы критически важна.

5 Используйте полноэкранный режим Full Screen Mode. Запуск VM в полноэкранном режиме по сравнению с оконным режимом дает около 10% роста производительности за счет сокращения числа видеоопераций хоста.

4 Создавайте виртуальные диски на отдельных накопителях. Создание виртуального жесткого диска на отдельном накопителе, отличном от того, на котором установлена операционная система хоста, уменьшает число конфликтов операций ввода-вывода и повышает производительность VM в целом. Если запускается несколько VM, лучше размещать каждую VM на своем диске.

3 Проводите дефрагментацию жестких дисков VM. Фрагментация диска возникает как в гостевой операционной системе, так и в системе хоста, поэтому процесс дефрагментации в данном случае следует проводить на нескольких уровнях. Сначала выполняется дефрагментация диска гостевой операционной системы. Некоторые версии продуктов VMware позволяют выполнять дефрагментацию виртуального диска в отключенном состоянии VM. После этого дефрагментируется физический диск операционной системы хоста.

2 Используйте быстрые диски. Производительность дисковой подсистемы — это один из главных факторов, влияющих на скорость работы VM. Чем быстрее устройство, тем выше и производительность VM. Для ноутбуков число оборотов диска в минуту должно быть не менее 5400, для настольной системы — не менее 7200. При консолидации серверов этот показатель должен быть не ниже 10 000.

1 Устанавливайте максимальный объем оперативной памяти. Объем физической памяти — вероятно, самый критичный фактор, влияющий на производительность VM. Необходимо выделять достаточный объем оперативной памяти для гостевой операционной системы — по меньшей мере 128 Мбайт для рабочих станций и 256 Мбайт для сервера. Если в каждый момент времени работает только одна VM, следует рассмотреть вопрос о выделении ей до половины памяти хоста. Виртуальные машины могут использовать только физическую память. Во всех современных VM-продуктах поддерживается до 3,6 Гбайт памяти в расчете на одну VM, поэтому максимизация оперативной памяти хоста — вопрос не академический. W