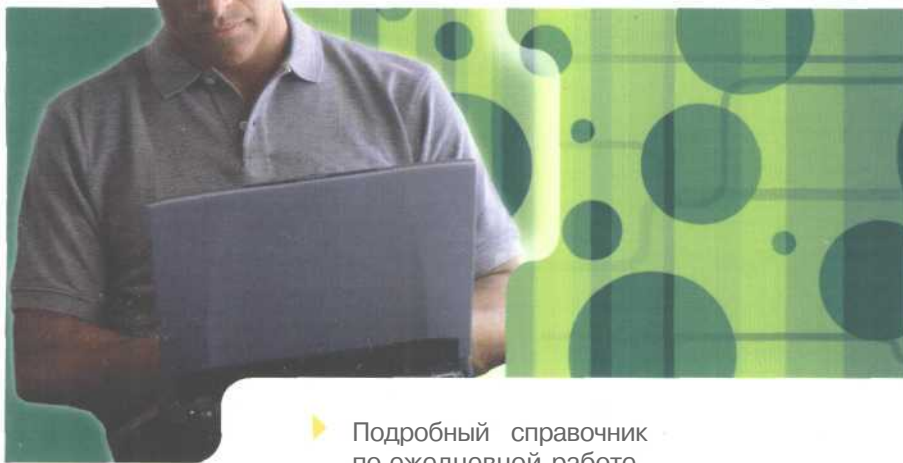


Уильям Р. Станек

Microsoft®

# Internet Information Services 5.0

Справочник администратора



- ▶ Подробный справочник по ежедневной работе с Microsoft Internet Information Services и Microsoft Indexing Services
- ▶ Таблицы, списки, пошаговые инструкции, подробный предметный указатель

**IT Professional**

И РУССКАЯ РЕДАКЦИЯ

**Microsoft®**





Уильям Р. Станек

Microsoft®

# Internet Information Services 5.0

Справочник администратора

Москва 2002

---

 РУССКАЯ РЕДАКЦИЯ

УДК 004.738.5  
ББК 32.973.202  
С76

**Уильям Р. Станек**

С76 Internet Information Services 5.0. Справочник администратора./  
Пер. с англ. — М.: Издательско-торговый дом «Русская Редакция», 2002. — 464 с.: ил.

**ISBN 5-7502-0188-0**

Данная книга — краткий и исчерпывающий справочник по всем основным вопросам, связанным с администрированием Web-, FTP-, NNTP- и SMTP-серверов под управлением Microsoft Internet Information Services, включая работу с фильтрами ISAPI, специальными HTTP-заголовками, установку серверных сертификатов и настройку протокола SSL, управление пользовательским доступом и работу с журналами сервера, а также управление службой Microsoft Indexing Services и устранение неполадок в работе IIS-серверов.

Книга адресована администраторам Web-решений на основе продуктов Microsoft, администраторам интрасетей/внешних сетей, администраторам, переходящим на Web-решения Microsoft, программистам, инженерам и специалистам службы поддержки, управляющим внутренними или тестовыми IIS-серверами.

Это богато иллюстрированное издание состоит из 12 глав и предметного указателя.

УДК 004.738.5  
ББК 32.973.202

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

Active Directory, BackOffice, FrontPage, JScript, Microsoft, Microsoft Press, MS-DOS, Visual Basic, Visual FoxPro, Windows и Windows NT являются товарными знаками или охраняемыми товарными знаками Microsoft Corporation. Все другие товарные знаки являются собственностью соответствующих фирм.

Если не оговорено иное, все названия компаний, организаций и продуктов, а также имена лиц, используемые в примерах, вымышлены и не имеют никакого отношения к реальным компаниям, организациям, продуктам и лицам.

(ID Оригинальное издание на английском языке. William R. Stanek, 2001

CO Перевод на русский язык,  
Microsoft Corporation, 2002

© Оформление и подготовка к изданию Издательско-торговый дом  
«Русская Редакция», 2002

**ISBN 0-7356-1024-x (англ)**  
**ISBN 5-7502-0188-0**

# Оглавление

Благодарности .....	XIV
<b>Введение</b> .....	<b>XV</b>
Кому адресована эта книга .....	XV
Структура книги .....	XVI
Условные обозначения .....	XVIII
Техническая поддержка .....	XVIII
<b>Часть I</b>	
<b>Основы Web-администрирования</b>	
<b>Microsoft Windows 2000</b> .....	<b>1</b>
Глава 1 <b>Обзор Web-служб Microsoft</b> .....	<b>2</b>
Подбор оборудования .....	4
Использование IIS .....	6
Установка компонентов IIS и узлов по умолчанию .....	6
Усовершенствования системы проверки подлинности .....	9
Установка служб Интернета и связанных с ними учетных записей .....	9
Методы и средства Web-администрирования .....	11
Управление ресурсами при помощи основных административных средств .....	11
Установка средств администрирования .....	12
Методы Web-администрирования .....	13
Глава 2 <b>Основы администрирования IIS</b> .....	<b>19</b>
Универсальные указатели ресурсов в IIS .....	19
Основы архитектуры IIS .....	20
Универсальные указатели ресурсов .....	22
Использование оснастки Internet Information Services .....	25
Запуск оснастки IIS и работа с ней .....	25
Подключение к другим серверам .....	28
Запуск, остановка и перезапуск всех служб Интернета .....	28
Запуск, остановка и приостановка отдельных ресурсов .....	31
Перезагрузка IIS-серверов .....	32
Управление службами IIS .....	33
Основные службы IIS .....	34

Запуск, остановка и приостановка служб IIS. . . . .	35
Настройка запуска службы. . . . .	36
Настройка восстановления службы. . . . .	37
Настройка резервного копирования и восстановления IIS . . .	38
Сохранение конфигурации сервера. . . . .	38
Создание резервных копий конфигурации IIS. . . . .	40
Восстановление IIS из резервной копии. . . . .	41
Восстановление поврежденных установок IIS. . . . .	42
Удаление резервных копий конфигурации IIS. . . . .	43
<b>Часть II</b>	
<b>Администрирование Web-сервера. . . . .</b>	<b>45</b>
Глава 3 Настройка Web-узлов и Web-серверов. . . . .	46
Именованное и идентификация Web-узлов. . . . .	46
IP-адреса и разрешение имен. . . . .	46
Идентификаторы Web-узла. . . . .	48
Размещение нескольких узлов на одном сервере. . . . .	49
Проверка имени компьютера и IP-адреса сервера. . . . .	52
Управление основными свойствами Web-службы. . . . .	54
Создание Web-узлов. . . . .	54
Управление свойствами Web-узла. . . . .	58
Задание домашнего каталога узла. . . . .	59
Изменение портов, IP-адреса и имени заголовка узла. . . .	60
Создание нескольких идентификаторов для одного Web-узла. . . . .	62
Ограничение числа входящих подключений и изменение времени ожидания соединения. . . . .	64
Поддержка пакетов HTTP Keep-Alive. . . . .	65
Управление каталогами. . . . .	66
Структура физических и виртуальных каталогов. . . . .	67
Создание физических каталогов. . . . .	67
Создание виртуальных каталогов. . . . .	68
Подключение IISAdmin, IISHelp и прочих системных каталогов. . . . .	70
Изменение свойств каталогов. . . . .	71
Переименование каталогов. . . . .	71
Удаление каталогов. . . . .	71
Управление Web-содержимым. . . . .	72
Открытие и просмотр файлов. . . . .	72
Изменение IIS-свойств файла. . . . .	72
Удаление файлов. . . . .	73
Перенаправление запросов браузера. . . . .	73

Перенаправление запросов к другим папкам или Web-узлам .	73
Перенаправление всех запросов на другой Web-узел . . . . .	75
Получение файлов из сетевых папок . . . . .	76
Перенаправление запросов приложениям . . . . .	77
<b>Глава 4 Настройка Internet Information Services . . . . .</b>	<b>81</b>
Основы использования приложений IIS . . . . .	81
Приложения ISAPI . . . . .	81
ASP-приложения . . . . .	84
Создание пользовательских приложений . . . . .	86
Использование и выполнение приложений . . . . .	88
Управление пользовательскими приложениями IIS . . . . .	93
Создание групповых и негрупповых приложений . . . . .	93
Настройка сопоставлений и кэширования . . . . .	95
Управление состоянием сеанса . . . . .	99
Управление буферизацией приложений . . . . .	101
Родительские пути, язык сценариев по умолчанию для ASP-страниц и время ожидания ASP-сценария . . . . .	102
Включение и отключение отладки приложений . . . . .	103
Настройка сообщений об ошибках приложения . . . . .	104
Выгрузка изолированных приложений . . . . .	105
Удаление IIS-приложений . . . . .	105
Управление пользовательскими фильтрами ISAPI . . . . .	106
Просмотр и настройка глобальных фильтров . . . . .	106
Просмотр и настройка локальных фильтров . . . . .	107
Изменение содержимого Web-узла и HTTP-заголовков . . . . .	109
Настройка документов по умолчанию . . . . .	109
Нижний колонтитул документа . . . . .	110
Срок хранения содержимого и запрет кэширования содержимого браузером . . . . .	111
Пользовательские HTTP-заголовки . . . . .	113
Системы оценки содержимого . . . . .	114
Настройка сообщений об ошибках Web-узла . . . . .	116
Коды состояния и сообщения об ошибках . . . . .	116
Дополнительные параметры обработки ошибок . . . . .	119
Использование существующих и создание собственных типов MIME . . . . .	122
Что такое MIME . . . . .	122
Просмотр и настройка MIME-типов для всех Web-узлов сервера . . . . .	125
Просмотр и настройка MIME-типов для отдельных узлов и папок . . . . .	126

Дополнительные сонеты по настройке .....	127
Управление простоями с помощью узлов обновления ....	127
Использование страниц переходов в рекламных целях ....	129
Обработка ошибок 404 и предупреждение тупиков. ....	130
<b>Глава 5 Управление безопасностью Web-сервера. ....</b>	<b>131</b>
Управление безопасностью Windows. ....	132
Учетные записи пользователей и групп. ....	132
Основные сведения об учетных записях пользователей и групп TIS. ....	132
Использование разрешений доступа к файлам и папкам ....	139
Работа с групповыми политиками. ....	144
Управление безопасностью IIS. ....	151
Настройка разрешений Web-сервера. ....	152
Настройка протокола WebDAV. ....	158
Выбор метода проверки подлинности. ....	160
Настройка ограничений доступа по IP-адресам и доменным именам. ....	166
Назначение операторов Web-узла. ....	169
Как повысить уровень безопасности Web-сервера. ....	172
Использование брандмауэров. ....	172
Переименование учетной записи Administrator. ....	173
Отключение Web-узла по умолчанию. ....	173
Отключение удаленного администрирования через Web ....	173
Запрет просмотра каталогов. ....	174
Создание уведомлений. ....	174
Установка сервисных пакетов, оперативных исправлений и шаблонов. ....	174
Удаление виртуального каталога IISADMPWD. ....	177
Проверка ввода в формах и строках запроса. ....	177
Удаление неиспользуемых сопоставлений приложений. ....	178
<b>Глава 6 Управление службой Microsoft Certificate Services и протоколом SSL. ....</b>	<b>180</b>
Протокол SSL. ....	180
SSL-шифрование. ....	181
SSL-сертификаты. ....	182
Стойкость шифра о протоколе SSL. ....	185
Служба Microsoft Certificate Services. ....	185
Общий обзор. ....	186
Установка службы Certificate Services. ....	187
Доступ к службе Certificate Services через Web-браузер. ....	191
Запуск и остановка службы Certificate Services ..	193

Архивирование и восстановление информации CA . . . . .	194
Удовлетворение и отклонение ожидающих запросов на сертификаты . . . . .	197
Генерирование сертификатов вручную с помощью оснастки Certification Authority . . . . .	198
Отзыв сертификатов . . . . .	199
Просмотр и обновление сертификата корневого CA . . . . .	200
Создание и установка сертификатов . . . . .	202
Создание запросов на сертификаты . . . . .	203
Передача запросов на сертификаты сторонним CA . . . . .	207
Передача запросов на сертификаты службе Certificate Services . . . . .	208
Обработка ожидающих запросов и установка сертификатов узлов . . . . .	211
Удаление ожидающих запросов на сертификаты . . . . .	212
Использование протокола SSL . . . . .	213
Настройка SSL-портов . . . . .	213
Установка сертификата корневого CA в хранилище клиентского браузера . . . . .	215
Проверка работоспособности SSL . . . . .	217
Устранение проблем с SSL . . . . .	218
Управление сертификатами узлов с помощью оснастки Internet Information Services . . . . .	219
Просмотр и внесение изменений в выданные сертификаты . . . . .	219
Обновление, удаление и замена сертификатов . . . . .	221
Игнорирование, принятие и требование клиентских сертификатов . . . . .	224
Требование SSL для всех подключений . . . . .	226
<b>Часть III</b>	
<b>Управление основными службами . . . . .</b>	<b>227</b>
Глава 7 Управление <b>FTP-серверами</b> . . . . .	228
Обзор протокола FTP . . . . .	228
Основы протокола FTP . . . . .	228
Управление доступом к FTP-серверу . . . . .	229
Использование FTP-сеансов . . . . .	231
Именованное и идентификация FTP-узлов . . . . .	233
Управление основными свойствами FTP-службы . . . . .	234
Создание FTP-узлов . . . . .	235
Управление FTP-узлами . . . . .	237
Задание домашнего каталога FTP-узла . . . . .	237

Изменение портов и IP-адресов узла . . . . .	239
Ограничение числа входящих подключений и изменение времени ожидания соединения . . . . .	240
Создание физических каталогов для FTP-узлов . . . . .	242
Создание виртуальных каталогов . . . . .	243
Перенаправление запросов к сетевым папкам . . . . .	244
Выбор способа отображения каталога . . . . .	244
Создание информационных сообщений . . . . .	245
Управление пользовательскими FTP-сеансами . . . . .	246
Просмотр пользовательских FTP-сеансов . . . . .	246
Просмотр общего числа подключенных пользователей . . . . .	247
Завершение пользовательских сеансов . . . . .	248
Управление безопасностью FTP-сервера . . . . .	248
Управление анонимными подключениями . . . . .	249
Конфигурирование анонимного доступа на глобальном уровне . . . . .	249
Конфигурирование анонимного доступа на уровне узла . . . . .	251
Использование разрешений Windows на FTP-серверах . . . . .	252
Конфигурирование разрешений FTP-сервера . . . . .	253
Настройка ограничений па доступ по IP-адресам и доменным именам . . . . .	256
Назначение операторов Web-узла . . . . .	258
<b>Глава 8 Настройка и поддержка службы SMTP . . . . .</b>	<b>260</b>
Использование SMTP . . . . .	261
Домены электронной почты . . . . .	261
Папка Mailroot . . . . .	262
Принципы обработки сообщений . . . . .	263
Основы управления службой SMTP . . . . .	265
Создание виртуальных SMTP-серверов . . . . .	265
Настройка портов и IP-адресов SMTP-серверов . . . . .	267
Создание нескольких идентификаторов для виртуального SMTP-сервера . . . . .	269
Мониторинг состояния виртуального SMTP-сервера . . . . .	270
Управление пользовательскими сеансами . . . . .	271
Настройка служебных доменов . . . . .	271
Просмотр служебных доменов . . . . .	271
Работа с локальными доменами . . . . .	272
Работа с удаленными доменами . . . . .	275
Настройка направляющего узла для удаленного домена . . . . .	282
Переименование и удаление служебных доменов . . . . .	282



Обработка входящих соединений. . . . .	283
Управление доступом на основе IP-адреса, подсети или домена. . . . .	283
Защищенные входящие соединения. . . . .	285
Проверка подлинности входящих соединений. . . . .	286
Управление числом входящих соединений и временем ожидания подключения. . . . .	288
Обработка исходящих соединений. . . . .	289
Безопасность исходящих соединений. . . . .	289
Управление исходящими соединениями. . . . .	291
Настройка ограничений на исходящие сообщения для SMTP. . . . .	292
Управление сообщениями, доставка которых невозможна. . . . .	294
Разрешение и запрет ретрансляции. . . . .	295
Управление доставкой сообщений. . . . .	297
Настройка параметров отправки сообщений. . . . .	297
Назначение числа пересылок сообщения. . . . .	299
Назначение параметров доменного имени. . . . .	300
Настройка обратного DNS-поиска. . . . .	302
Пересылка исходящих сообщений на направляющий узел. . . . .	302
<b>Глава 9 Администрирование службы Indexing Service . . .</b>	<b>304</b>
Основы работы со службой Indexing Service. . . . .	305
Использование службы Indexing Service. . . . .	305
Принципы работы службы Indexing Service. . . . .	309
Поиск в каталогах. . . . .	313
Основы администрирования службы Indexing Service . . . .	315
Назначение индексируемых Web-ресурсов. . . . .	315
Создание и просмотр каталогов. . . . .	316
Просмотр состояния индексирования. . . . .	318
Запуск, остановка и приостановка службы Indexing Service. . . . .	320
Настройка свойств службы Indexing Service. . . . .	320
Оптимизация производительности Indexing Service . . . . .	322
Управление каталогами. . . . .	326
Просмотр параметров каталога и индексируемых папок . . .	326
Добавление в каталог физических папок. . . . .	327
Принудительное полное и выборочное повторное сканирование папок. . . . .	328

Запуск, остановка и приостановка отдельных каталогов .....	329
Слияние каталогов .....	330
Включение в каталоги Web- или NNTP-узлов .....	331
Тестирование каталогов с помощью запросов .....	331
<b>Часть IV</b>	
<b>Производительность, оптимизация и поддержка .....</b>	<b>333</b>
Глава 10 Мониторинг и настройка производительности ..	334
Мониторинг производительности и активности IIS. ....	334
Зачем проводит мониторинг IIS? .....	335
Подготовка к мониторингу IIS .....	336
Средства мониторинга IIS .....	336
Выявление и устранение ошибок IIS. ....	337
Просмотр журналов доступа .....	338
Просмотр журналов событий .....	339
Мониторинг производительности IIS .....	343
Отбор наблюдаемых счетчиков .....	344
Создание и управление журналами Performance Monitor ....	352
Управление журналами производительности .....	353
Создание журналов счетчиков .....	354
Создание журналов трассировки .....	357
Воспроизведение журналов производительности .....	359
Создание оповещений для счетчиков производительности .....	359
Настройка производительности Web-сервера .....	363
Мониторинг и настройка использования памяти .....	363
Конфигурирование параметров производительности приложений .....	364
Оптимизация сервера для максимальной пропускной способности сетевых приложений .....	364
Контроль использования ОЗУ, кэширования и виртуальной памяти .....	365
Мониторинг и настройка использования процессора .....	366
Мониторинг и настройка дискового ввода-вывода .....	366
Мониторинг и настройка сетевых подключений и пропускной способности сети .....	367
Ограничение пропускной способности и числа подключений .....	375
Настройка HTTP-сжатия .....	376

William R. Stanek

# Microsoft® **Windows® 2000** **and IIS 5.0**

Administrator's Pocket Consultant

---

---

**Microsoft** Press

Оглавление

XIII

<b>Глава 11 Ведение журналов и контроль пользовательского доступа</b>	<b>378</b>
Статистика трассировки: общая картина	378
Стандартный формат файла журнала NCSA	380
Формат файла журнала Microsoft IIS	385
Расширенный формат файла журнала W3C	387
Формат журнала ODBC	391
О ведении журналов узлов	392
Включение ведения журналов для HTTP-, FTP- и SMTP-узлов	394
Конфигурирование стандартного формата файла журнала NCSA	394
Конфигурирование формата файла журнала Microsoft US	396
Конфигурирование расширенного формата файла журнала W3C	398
Конфигурирование журнала формата ODBC	400
Включение и конфигурирование ведения ODBC-формата в IIS	404
Выключение ведения журнала	405
<b>Глава 12 Оптимизация IIS и метабаза</b>	<b>406</b>
Методы повышения производительности IIS	406

## Благодарности

Работа над этой книгой доставила массу удовольствия, но вместе с тем потребовала предельного внимания. В ней описаны методики, которые я применяю ежедневно, и теперь не только я, но и все желающие смогут воспользоваться ими. Но я не всемогущ, а потому в работе над книгой мне помогало несколько человек, которых мне хотелось бы здесь упомянуть.

Как я уже писал в предыдущих книгах серии *«Справочник администратора»*, команда Microsoft Press просто великолепна. Я очень благодарен им за понимание моего практического потенциала и удачный подход к этой серии книг в целом. Джулиана Алдус (Juliana Aldous) помогла мне получить все необходимые инструменты. Карин Жалл (Karen Szall) и Джулия Миллер (Julie Miller) отлично руководили издательским процессом со стороны Microsoft Press, а

# Введение

«*Internet Information Services 5.0. Справочник администратора*» задуман как краткий и исчерпывающий источник для администраторов Web-администраторов, работающих со службами **Internet Information Services** и **Microsoft Indexing Services**. Это печатное руководство по ресурсам, которое вы захотите всегда иметь под рукой. В книге обсуждаются все основные задачи администрирования служб **Internet Information Services** и **Microsoft Indexing Services**. Поскольку наша цель — максимум пользы в книге карманного формата, вам не придется искать среди сотен страниц посторонней информации то, что вам нужно. Вы сразу найдете решение конкретной задачи.

Книга задумана как единый ресурс, к которому можно обращаться всякий раз, когда возникают вопросы по Web-администрированию служб **Internet Information Services** и **Microsoft Indexing Services**. Так что издание ориентировано на типичные процедуры администрирования, часто используемые задачи и документированные примеры. Одна из наших целей — сделать содержание сжатым, чтобы книга оставалась компактной, удобочитаемой и в то же время максимально информативной. Теперь вместо талмуда в 1 000 страниц или 100-страничной брошюры у вас есть ценное руководство по ресурсам, помогающее быстро и легко выполнять типичные задачи, решать проблемы и реализовывать такие технологии IIS, как перенаправление запросов, оптимизация метабазы и сценарии автоматизации.

## Кому адресована эта книга

В нашей книге речь идет о службах **Internet Information Services** и **Microsoft Indexing Services**. Книга адресована;

- нынешним администраторам Web-решений на основе продуктов Microsoft;
- администраторам интрасетей/внешних сетей;

- администраторам, переходящим на Web-решения Microsoft;
- программистам, инженерам и специалистам службы поддержки, управляющим внутренними или тестовыми IIS-серверами.

Чтобы сделать книгу максимально информативной, я исходил из того, что вы обладаете базовыми навыками сетевого администратора, в общих чертах знакомы с Web-серверами и на ваших системах уже установлены службы Internet Information Services и Microsoft Indexing Services. Так что я не посвящаю целые главы описанию Web-служб, работе со службами имен, созданию Web-узлов и установке IIS. Но я описываю конфигурирование, управление серверами предприятия, настройку производительности, оптимизацию, автоматизацию и многое другое.

Я также предполагаю, что вы хорошо знакомы с пользовательским интерфейсом Windows 2000 и умеете создавать сценарии. Если нам потребуется помощь, см. книги «*Microsoft Windows 2000. Справочник администратора*» издательства «Русская Редакция», 2002 г. и «*Microsoft Windows 2000 Scripting Bible*» издательства IDG Books, 2000 г.

## Структура книги

Книга задумана для использования в повседневном администрировании IIS, а потому организована на основе прикладных задач, а не функций IIS. Читая эту книгу, вы должны знать о связи между сериями «Справочник администратора» и «Руководство администратора». Обе задуманы как часть библиотеки администратора. Первая включает книги сугубо практической направленности, вторая — полные пособия и справочники, рассматривающие все аспекты использования продукта или технологии на предприятии.

Книга содержит подробное оглавление и большой предметный указатель для быстрого поиска решений, а также пошаговые инструкции, списки, таблицы и массу перекрестных ссылок. Книга разбита на части и главы. Каждая часть содержит вводный параграф о главах внутри нее.

Часть I описывает основные задачи администрирования IIS. В главе I дается обзор средств, способов и концепций ад-

министрирования IIS. В главе 2 рассматриваются задачи управления IIS. Вы также узнаете об административных компонентах, службах Windows, диспетчере Internet Services Manager и конфигурациях сервера.

Во второй части описаны важные задачи администрирования Web-серверов под управлением IIS. Глава 3 знакомит с управлением Web-серверами и поясняет, как создавать и управлять виртуальными каталогами. В главе 4 рассматривается настройка IIS: вы научитесь работать с фильтрами ISAPI, специальными HTTP-заголовками, нестандартными ошибками и т. д. В главе 5 обсуждается безопасность Web-серверов и объясняется, как создавать учетные записи пользователей, настраивать разрешения папок и назначать операторов. В главе 6 описаны серверные сертификаты и протокол SSL. Сертификаты обеспечивают безопасные Web-коммуникации, а SSL шифрует пересылаемые между клиентом и сервером данные.

Третья часть посвящена администрированию основных служб, постоянно развертываемых на Web-серверах. В главе 7 рассказывается об управлении FTP-серверами, включая их настройку, управление доступом к папкам, разрешение анонимных подключений и многое другое. В главе 8 рассматриваются настройка и поддержка SMTP. Вы научитесь конфигурировать SMTP-серверы, ставить сообщения в очередь на доставку и маршрутизировать их, задавать параметры доставки и организовывать безопасность SMTP-серверов. В главе 9 рассказывается о службе Indexing Service, включая новейшие способы индексирования, создание и управление каталогами, настройку производительности и создание форм запросов Indexing Service.

В заключительной части обсуждаются задачи настройки и поддержки IIS. В главе 10 описаны важные моменты мониторинга производительности Web-серверов и устранения проблем. Глава 11 начинается с руководства по контролю пользовательского доступа, затем рассматривается настройка журналов сервера. Глава 12 посвящена оптимизации IIS — обновлению связанных с IIS параметров реестра и работе с метабазой IIS.

## Условные обозначения

Я использовал множество элементов, чтобы текст был понятным и удобочитаемым. Коды и листинги набраны моноширинным шрифтом, кроме тех случаев, когда я явно говорю о вводе команды. В этом случае команда набирается полужирным начертанием. Когда я ввожу и определяю новый термин, я выделяю его *курсивом*.

**Примечание** описывает подробности акцентируемого момента.



**Совет** дает подсказку или дополнительную информацию.



**Внимание!** предупреждает о потенциальных проблемах.



Надеюсь, эта книга даст вам все необходимое для максимально быстрого и эффективного администрирования Windows 2000. Ваши комментарии автору присылайте по адресу [win2000-consulting@tppress.com](mailto:win2000-consulting@tppress.com). Спасибо.

## Техническая поддержка

Издательский коллектив приложил все усилия, чтобы обеспечить точность информации в книге. Microsoft Press принимает поправки к книге по адресу <http://mspress.microsoft.com/support>.

Если у вас есть комментарии, вопросы или идеи, связанные с этой книгой, присылайте их в Microsoft Press одним из следующих способов.

Обычной почтой:

Microsoft Press  
Attn: *Microsoft Windows 2000 and IIS 5.0*  
*Administrator's Pocket Consultant Editor*  
One Microsoft Way  
Redmond, WA 98052-6399

Электронной почтой:

MSPINPUT@MICROSOFT.COM

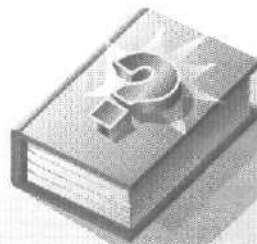
Учтите, что поддержка продукта не предоставляется по указанным адресам. Сведения о поддержке продуктов Microsoft см. по адресу <http://www.microsoft.com/support>.



## Часть I

# Основы Web-администрирования Microsoft Windows 2000

В первой части книги обсуждаются основные задачи Web-администрирования: в главе 1 — средства, методы и концепции Web-администрирования, глава 2 посвящена собственно Web-администрированию Microsoft Internet Information Services. Мы рассмотрим административные компоненты, конфигурации сервера и работу с диспетчером Internet Services Manager.



## Глава 1

# Обзор Web-служб Microsoft

Службы Microsoft Internet Information Services (IIS, Информационные службы Интернета) — средства разработки надежных и масштабируемых приложений, предназначенных для создания и управления узлами и серверами World Wide Web. Они позволяют публиковать информацию в интрасетях, внешних сетях и Интернете, а также предоставляют разнообразные взаимосвязанные службы, необходимые современным Web-узлам: File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Network News Transfer Protocol (NNTP) и др. В IIS имеется и дополнительная служба — Indexing Service (Служба индексирования). Она связана с перечисленными компонентами и служит для создания каталогов документов. Indexing Service, реализованная на Web-узле, позволяет производить поиск информации с помощью обычной HTML-формы.

IIS обладает множеством функций. Вот некоторые из них.

- **Протокол HTTP 1.1 и HTTP-сжатие** IIS полностью поддерживает протокол Hyper Text Transfer Protocol (HTTP) версии 1.1 и используемые им усовершенствованные алгоритмы сжатия. HTTP-сжатие позволяет сжимать статические и динамические результаты HTTP-запросов для передачи их клиентам, поддерживающим протокол HTTP 1.1.
- **Заголовки узлов** На компьютере с одним IP-адресом можно размещать несколько Web-узлов. Для определения запрошенного клиентом узла IIS использует имя компьютера, переданное в HTTP-заголовке.
- **Перезапуск FTP** При разрыве связи с FTP-узлом позволяет воспользоваться командой REST и продолжить загрузку файла с места разрыва.

- **Active Server Pages (ASP)** Этот язык сценариев предназначен для создания динамических интерактивных Web-приложений, выполняющихся на Web-сервере. ASP допускает использование HTML-кода, сценариев и COM-компонентов.
- **Защита приложения** ASP-приложения выполняются в отдельной области памяти. Приложения с низким уровнем защиты выполняются в процессе и разделяют ресурсы с IIS. Приложения со средним уровнем защиты — в групповом процессе, т. е. используют один и тот же процесс, отличный от обычных ресурсов IIS. Приложения с высоким уровнем защиты выполняются полностью вне процесса: они не разделяют какие-либо процессы, и их отказ не влияет на другие программы.
- **Аудит и регулирование процессов** Лудит предоставляет информацию об использовании ресурсов процессора отдельными Web-узлами; регулирование процессов позволяет ограничить обращение к процессору приложений, выполняющихся вне процессов, и тем самым повысить производительность.
- **Web Distributed Authoring and Versioning (WebDAV)** Этот протокол интегрирован в IIS и дополняет HTTP 1.1. WebDAV позволяет удаленным разработчикам создавать, перемещать или удалять файлы, свойства файлов, каталоги и свойства каталогов на сервере по HTTP-соединению.
- **SSL 3.0 и TLS** Эти протоколы предоставляют безопасный способ обмена информацией между клиентами и серверами. Кроме того, они позволяют задействовать клиентские сертификаты, считываемые серверными страницами ISAPI. Клиентские сертификаты сопоставляются учетным записям пользователей Windows и обеспечивают проверку их подлинности, а также управление доступом.
- **Краткая проверка подлинности** Этот механизм аутентификации позволяет осуществлять безопасную и надежную проверку подлинности учетных записей пользователей через прокси-серверы и брандмауэры.

Далее я буду называть администрирование IIS и службы Indexing Service просто Web-администрированием. Советую

вам обратить особое внимание взаимодействию IIS с оборудованием своего компьютера и с ОС семейства Windows, доступным административным средствам, методам управления и поддержки IIS.

## Подбор оборудования

Рекомендации по выбору оборудования для серверов Интернета значительно отличаются от рекомендаций для серверов других типов. Поставщик услуг Интернета может размещать Web-узлы своих клиентов на одном компьютере. Кроме того, он заключает соглашения о качестве обслуживания, определяющие уровень доступности и производительности. С другой стороны, коммерческие Web-узлы с большим числом клиентов иногда находятся на отдельном Web-сервере или даже на нескольких серверах с распределением нагрузки. Учитывая, что Интернет-серверы применяются в различных средах и могут быть как совместно используемыми, так и выделенными, хочу дать следующие рекомендации по выбору их компонентов.

- **Память** Ее необходимый объем зависит от различных факторов, включая требования сторонних служб, размер часто просматриваемого содержимого и требования Web-приложений к ОЗУ. На серверах с большим объемом дискового пространства должно быть не менее 512 Мб ОЗУ. ОЗУ большего размера позволит кэшировать больше файлов и уменьшить число запросов к диску. Подробнее об управлении памятью и настройке производительности см. главу 12.
- **Процессор** Тактовая частота процессора и размер шины данных определяют скорость перемещения информации между процессором, ПЗУ и системными шинами. Статичное содержимое, например, изображения и HTML-страницы, создают небольшую нагрузку на процессор, и обычным компьютерам, соответствующим рекомендованным аппаратным требованиям Windows 2000, она вполне по силам. Для увеличения предельной емкости Web-сервера, особенно с динамическим содержимым, лучше использовать один или несколько процессоров с высокой тактовой частотой.

- **Симметричная многопроцессорная обработка** IIS использует дополнительные процессоры для повышения производительности. Компьютерам, на которых выполняется только IIS и не применяется динамическое содержимое или шифрование, вполне достаточно одного процессора. Если же службы IIS выполняются параллельно с другими (типа Microsoft SQL Server или Microsoft Exchange Server), требуется несколько процессоров. На Web-узлах, где нужна высокая производительность, IIS практически линейно масштабируются до 4 процессоров.
- **Объем дискового пространства** Зависит от размера файлов содержимого и количества размещенных узлов. Места на диске должно хватать для хранения всех данных, рабочего пространства, системных файлов и виртуальной памяти. Почти так же, как и емкость дисков, важна производительность ввода-вывода. Однако она редко создает проблемы разработчикам общедоступных Web-узлов: обычно производительность ввода-вывода ограничивается полосой пропускания. Для Web-узлов с широкой полосой пропускания следует использовать аппаратные RAID-решения на основе оптоволоконных или медных SCSI-интерфейсов.
- **Защита данных** Если многочасовые простои для вас неприемлемы, в системе следует реализовать защиту от неожиданных отказов дисков, основанную на RAID-массивах. Конфигурация RAID-0 (чередование томов) обеспечивает оптимальную производительность чтения и записи, однако при отказе диска IIS сможет возобновить работу лишь после его замены. RAID-1 (зеркалирование дисков) создает идентичные копии данных на нескольких дисках, но для восстановления содержимого отказавшего диска из резервной копии работу IIS придется приостановить. Конфигурация RAID-5 (чередование томов с четностью) предоставляет отличную защиту в случае отказа отдельного диска, но имеет низкую производительность записи. Впрочем, при наличии избыточных серверов с распределением нагрузки RAID может и не понадобиться. Благодаря распределению нагрузки, дополнительные серверы обеспечивают нужный уровень отказоустойчивости.

- **Источник бесперебойного питания (ИБП)** ИБП позволяет нормально завершить работу системы при сбоях электросети, а также обеспечит целостность серверов, которые используют кэширующие контроллеры с отложенной записью без встроенной батарейной поддержки. Поставщики услуг Интернета, занимающиеся размещением Web-узлов, часто используют ИБП, способные неограниченно долго обеспечивать питание компьютеров в периоды отсутствия тока в сети.

## Использование IIS

В этом разделе описываются основы работы с IIS и службой Indexing Service, выполняющимися под управлением ОС Windows. В офисе эти службы следует устанавливать на серверах с Microsoft Windows 2000 Server/Advanced Server/Datacenter Server или новейших версий ОС Windows. Для личного использования их можно установить на компьютерах с Microsoft Windows 2000 Professional или новейшими версиями ОС Windows.

### Установка компонентов IIS и узлов по умолчанию

Службы IS и Indexing Service устанавливают или в составе ОС, или с помощью мастера Windows Components Wizard (Мастер компонентов Windows). Indexing Service устанавливается как отдельный компонент, а службы IIS включают массу подкомпонентов, которые можно в любое время удалить или установить. К ним относятся:

- **Common Files (Общие файлы)** — файлы, необходимые приложениям IIS;
- **Documentation (Документация)** — справочник по администрированию сервера и публикации содержимого узлов, доступен по адресу <http://localhost/IISHelp/iis/misc/>;
- **File Transfer Protocol Server (FTP-сервер)** используется для обмена файлами по протоколу FTP;
- **FrontPage 2000 Server Extensions (Серверные расширения FrontPage)** — расширения для разработки и администрирования Web-узлов с помощью FrontPage и Microsoft Visual InterDev;

- **Internet Information Services Snap-In (Оснастка IIS)** - основное средство администрирования IIS;
- **Internet Services Manager (Диспетчер служб Интернета)** — модификации административных утилит IIS на основе браузера;
- **Network News Transfer Protocol Service (Служба NNTP)** служит для создания групп новостей и управления ими;
- **Simple Mail Transfer Protocol Service (Служба SMTP)** служит для отправки почты с Web-сервера;
- **Visual InterDev RAD Remote Deployment Support (Поддержка удаленного развертывания Visual InterDev RAD)** – средство удаленного развертывания приложений на Web-серверах;
- **World Wide Web Server (Веб-сервер)** — Web-служба для публикации и управления Web-узлами.

При установке служб Интернета некоторые узлы создаются на компьютере по умолчанию. Изначально они отключены, но их можно запустить с помощью оснастки Internet Information Services. Для этого раскройте меню `Start\Programs\Administrative Tools` (Пуск\Программы\Администрирование) и выберите Internet Services Manager (Диспетчер служб Интернета). Следующие узлы создаются по умолчанию.

- **Default FTP site (FTP-узел по умолчанию)** предназначен для FTP-служб. По умолчанию к FTP-узлам разрешены анонимные подключения. Если вы не собираетесь обмениваться файлами по протоколу FTP, отключите эту службу.
- **Default Web site (Web-узел по умолчанию)** предназначен для Web-служб. По умолчанию к Web-узлам разрешены анонимные подключения. Если вы не хотите делать спой узел общедоступным, запретите анонимные подключения.
- **Administration Web site (Администрирование веб-узла)** предназначен для администрирования Web-серверов с помощью браузера. По умолчанию доступен только с локального компьютера. Если вы собираетесь использовать данную службу для удаленного администрирования, измените параметры IP-фильтрации.



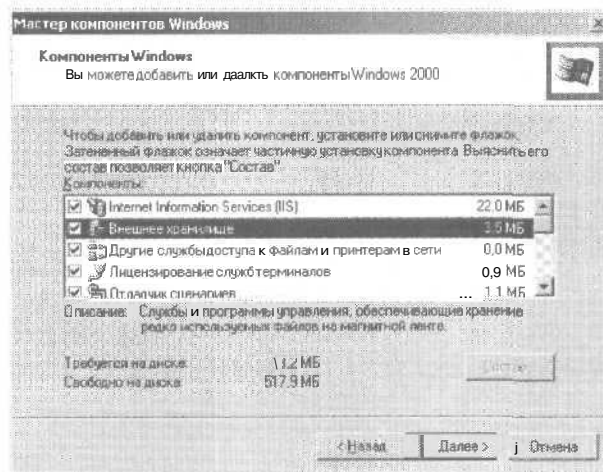
**Примечание** После останова Web-узла Administration управлять узлами с помощью диспетчера Internet Services Manager станет невозможно.

- **Default SMTP Virtual Server (Виртуальный SMTP-сервер по умолчанию)** предназначен для SMTP-служб. Если ваши страницы не генерируют сообщений электронной почты, запускать SMTP-серверы не следует. По умолчанию пересылать почту через сервер могут лишь серверы, прошедшие проверку подлинности в домене. Это предотвращает использование сервера в качестве точки рассылки нежелательных сообщений.
- **Default NNTP Virtual Server (Виртуальный NNTP-сервер по умолчанию)** предназначен для NNTP-служб. Конфигурация по умолчанию позволяет клиентам отправлять сообщения и принимать обновления групп новостей, а другим службам — получать статьи с сервера. Можете изменить эти параметры перед запуском NNTP-сервера.

Если какой-то из нужных вам компонентов IIS в оснастке Internet Information Services недоступен, его можно установить с помощью мастера Windows Components Wizard.

1. Зарегистрируйтесь в системе по учетной записи и паролю администратора.
2. Раскройте меню *Start\Settings* (Пуск\Настройка) и выберите *Control Panel* (Панель управления).
3. Дважды щелкните значок *Add/Remove Programs* (Установка и удаление программ). Откроется одноименное диалоговое окно.
4. В левой части окна щелкните значок *Add/Remove Windows Components* (Добавление и удаление компонентов Windows). Запустится мастер *Windows Components Wizard* (Мастер компонентов Windows) (рис. 1-1).
5. Выберите *Internet Information Services (IIS)* и щелкните *Details* (Состав), чтобы установить или удалить отдельные компоненты IIS.
6. Укажите устанавливаемые и удаляемые подкомпоненты.
7. Щелкните *Next* (Далее). Система установит (удалит) выбранные вами компоненты.





**Рис. 1-1.** Установка и удаление компонентов IIS с помощью мастера Windows Components Wizard (Мастер компонентов Windows)

### Усовершенствования системы проверки подлинности

Службы IIS полностью интегрированы с доменной системой безопасности Windows и обеспечивают аутентификацию на основе учетных записей пользователей и групп, а также обычной проверки подлинности. Эти методы значительно упрощают управление безопасностью и регистрацией в системе. Вы можете:

- применять проверку подлинности на основе учетных записей домена Windows, чтобы к серверу могли обращаться лишь пользователи, имеющие учетную запись домена;
- разрешить анонимный доступ к ресурсам без указания имени пользователя и пароля;
- реализовать ограниченный доступ на основе IP-адреса и доменного имени.

### Установка служб Интернета и связанных с ними учетных записей

При установке IIS и Indexing Service становятся доступны еще несколько служб. Их позволяют просмотреть утилита

Services (Службы) или оснастка Computer Management (Управление компьютером) из меню Administrative Tools. Вот они.

- FTP Publishing Service (Служба FTP-публикаций) позволяет обмениваться файлами по протоколу FTP и администрировать FTP-серверы с помощью оснастки Internet Information Services.
- IIS Admin Service (Служба IIS Admin) позволяет администрировать IIS с помощью оснастки Internet Information Services.
- Indexing Service (Служба индексирования) индексирует свойства и содержимое файлов, обеспечивая быстрый доступ к ним при помощи гибкого языка запросов.
- Network News Transport Protocol (NNTP) позволяет работать с группами новостей и администрировать NNTP-серверы из оснастки Internet Information Services.
- World Wide Web Publishing Service (Служба веб-публикаций) позволяет обмениваться файлами по протоколу HTTP и администрировать HTTP-серверы.

По умолчанию IIS и Indexing Service выполняются в контексте учетной записи локального компьютера и благодаря этому взаимодействуют с ОС. Кроме того, при установке IIS создаются следующие учетные записи.

- **IUSR\_имя\_компьютера** — гостевая, предназначена для анонимного доступа к узлам Интернета. Если она отключена или заблокирована, работа анонимных пользователей со службами Интернета невозможна.
- **IWAM\_имя\_компьютера** используется IIS для запуска приложений, выполняющихся вне процесса. Если она отключена или заблокирована, запуск упомянутых приложений невозможен.



**Совет** Учетные записи **IUSR\_имя\_компьютера** и **IWAM\_имя\_компьютера** относятся к группе Guests (Гости) и имеют запрещенный для изменения пользователем пароль с неограниченным сроком действия. И все же для них, как и для любых других учетных записей, можно задать произвольные пароли и таким образом управлять ими.

## Методы и средства Web-администрирования

Управлять IIS и службой Indexing Service можно различными способами, основные из которых описаны в этом разделе.

### Управление ресурсами при помощи основных административных средств

Для управления Web-, FTP-, SMTP- и NNTP-ресурсами, а также ресурсами индексирования существует множество утилит. Основные из них доступны из меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование).

- **Active Directory Users and Computers (Active Directory — пользователи и компьютеры)** управляет учетными записями пользователей, групп и компьютеров домена.
- **Computer Management (Управление компьютером)** управляет службами, дисками и приложениями. Узел Services and Applications (Службы и приложения) данной оснастки обеспечивает доступ к каталогам службы Indexing Service, а также к узлам и серверам IIS.
- **Data Sources (Источники данных ODBC)** настраивает драйверы и источники данных ODBC и управляет ими. Источники данных связывают Web-интерфейсы с базами данных.
- **DNS.** Любой общедоступный Web-узел должен иметь полное доменное имя, корректно разрешаемое браузером. Эта оснастка позволяет управлять DNS-конфигурацией работающих под управлением Windows 2000 DNS-серверов.
- **Event Viewer (Просмотр событий)** управляет событиями и системными журналами.
- **HTTP Monitoring tool** позволяет наблюдать за HTTP-активностью на сервере (подробнее см. главу 10).
- **IIS Administration Script Utility (ADSUTIL.VBS, Служебная программа администрирования IIS)** позволяет изменять конфигурацию IIS из командной строки. Предоставляет исполнимый файл и сценарий Microsoft VBScript, которые можно запускать из командной строки с помощью Windows Scripting Host (CSCRIPT.EXE).

- **Internet Services Manager (Диспетчер служб Интернета)** управляет Web- и FTP-серверами из браузера.
- **Performance (Производительность)** позволяет отслеживать производительность IIS, настраивать системные журналы событий и оповещения.
- **Server Extensions Administrator (Администратор серверных расширений)** управляет различными серверными расширениями, например, FrontPage и IIS.
- **Services (Службы)** позволяет просматривать информацию о службах, останавливать и запускать их, настраивать регистрацию служб в системе и параметры автоматического возобновления их работы.

Все эти утилиты позволяют управлять локальными и удаленными ресурсами. Так, с помощью оснастки Internet Information Services можно подключиться к новому компьютеру и управлять его узлами и службами с вашей системы.

### **Установка средств администрирования**

Со службами на сервер автоматически устанавливаются и утилиты для управления ими. Возможно, что при удаленном управлении серверами на рабочей станции не окажется нужных утилит — их можно установить на компьютер, с которого осуществляется удаленное администрирование.

Чтобы установить средства администрирования Windows 2000, сделайте следующее.

1. Зарегистрируйтесь в системе по учетной записи и паролю администратора.
2. Раскройте меню Start\Settings (Пуск\Настройка) и выберите Control Panel (Панель управления).
3. Дважды щелкните значок Add/Remove Programs (Установка и удаление программ).
4. Чтобы добавить или удалить административные утилиты, в левой части открывшегося окна щелкните значок Change or Remove Programs (Замена или удаление программ) и выберите Windows 2000 Administration Tools (Администрирование Windows 2000). Щелкните Change (Заменить).

5. Если вы устанавливаете административные средства впервые, щелкните CD or Floppy (CD или дискеты). Затем в диалоговом окне Run Installation Program (Запуск программы установки) щелкните Browse (Обзор). Вставьте компакт-диск Windows 2000 Server в привод CD-ROM. В диалоговом окне Browse (Обзор) выберите CD (Компакт-диск), дважды щелкните папку I386 и затем -- ADMINPAK.MSI. Щелкните Finish (Готово).
6. Запустится мастер Windows 2000 Administrative Tools Setup Wizard (Мастер установки Администрирование Windows 2000). Щелкните Next.
7. На компьютер будут установлены средства администрирования. Щелкните Finish, чтобы завершить установку.

### Методы Web-администрирования

Для управления IIS существует множество средств, включая оснастку Internet Information Services, диспетчер Internet Services Manager, административные объекты IIS, административные сценарии.

Стандартный интерфейс администрирования IIS — оснастка Internet Information Services (рис. 1-2). Чтобы запустить ее, раскройте меню Start\ Programs\ Administrative Tools (Пуск\Программы\Администрирование) и выберите Internet Services Manager (Диспетчер служб Интернета).

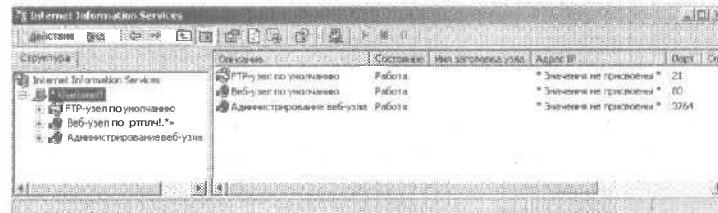


Рис. 1-2. Окно оснастки Internet Information Services

После запуска оснастка Internet Information Services автоматически подключается к локальной установке IIS (если таковая имеется). Если вы подсоединитесь к удаленным установкам IIS, при последующих запусках Internet Information Services будет автоматически подключаться и к ним тоже. Чтобы запретить это, отключитесь в оснастке от уда-

ленных серверов. Подробнее о работе с оснасткой Internet Information Services см. главу 3.

Для доступа к удаленным установкам IIS оснастка Internet Information Services использует Web-узел Administration (Администрирование веб-узла). Запуская или останавливая его, вы можете разрешать или запрещать удаленное управление Web-узлами из браузера. После установки IIS произвольно выбирает номер порта из диапазона от 2000 до 9999 и назначает его Web-узлу Administration. Узел реагирует на запросы браузеров ко всем разрешенным доменам, по администратор должен указать номер порта, поскольку тот отличается от номера порта протокола HTTP по умолчанию (80). Например, если доменное имя сервера — `primary.microsoft.com`, а номер административного порта — 9394, для подключения к административному Web-узлу в браузере нужно ввести адрес:

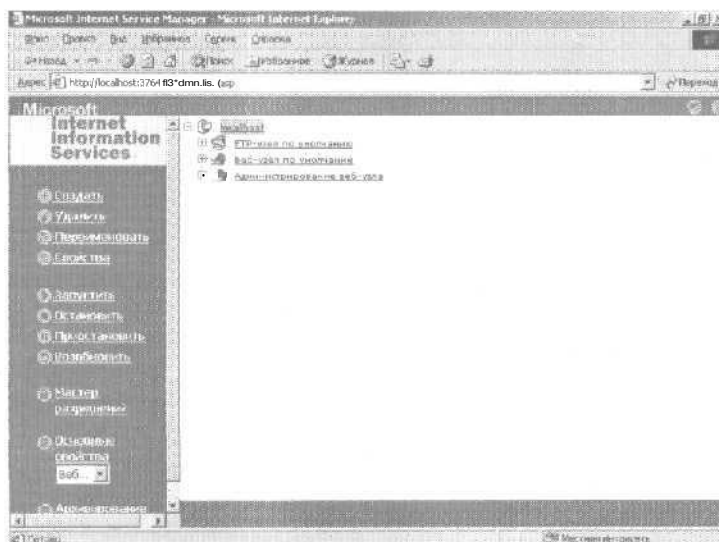
`http://primary.microsoft.com:9394/`

Ниже показано главное окно диспетчера Internet information Manager (рис. 1-3). По умолчанию включена лишь встроенная проверка подлинности Windows. Чтобы разрешить удаленное администрирование через Web-узел Administration, измените параметры IP-фильтрации в параметрах безопасности IIS и разрешите доступ внешних систем. Если при обращении к узлу проверка подлинности не осуществляется автоматически, вам предложат ввести имя пользователя и пароль. Если вы состоите в группе Administrators (Администраторы) ОС Windows и укажете соответствующие регистрационные реквизиты, то сможете удаленно администрировать IIS через Web-узел Administration.

Кроме того, правом удаленного администрирования IIS обладают члены группы операторов Web-узла — специальной группы пользователей, имеющих расширенные права на отдельных Web-узлах. Операторы Web-узла обладают меньшим набором прав, чем администраторы, и не имеют доступа к параметрам IIS, компьютера и сети. Узлы реагируют на посылаемые через браузер запросы операторов, если IIS передано имя домена узла, за которым следует `/iisadmin/`. Например, если доменное имя сервера — `primary.microsoft.com`,

для подключения к административному разделу Web-узла в браузере нужно ввести такой адрес:

<http://primary.microsoft.com/iisadmin/>



**Рис. 1-3.** Управление удаленными установками IIS с помощью диспетчера Internet Information Manager

Как и в случае с Web-узлом Administration, по умолчанию включена только встроенная проверка подлинности Windows. Чтобы разрешить удаленное администрирование, измените параметры IP-фильтрации в характеристиках безопасности IIS и разрешите доступ внешних систем. Если при обращении к узлу проверка подлинности не осуществляется автоматически, вам предложат ввести имя пользователя и пароль. Указав соответствующие регистрационные реквизиты, вы сможете удаленно администрировать Web-узел в качестве его оператора. Подробнее об операторах Web-узлов см. главу 5,

Кроме того, IIS можно управлять с помощью Windows Scripting Host (WSH), сервер сценариев Windows) и интерфейсов Active Directory Services Interface (ADSI). Windows Scripting Host предоставляет архитектуру для создания динамических

сценариев, состоящих из основной объектной модели, серверов сценариев и обработчиков сценариев. ADSI предоставляет набор интерфейсов для доступа к службе каталогов, интегрированной в Windows 2000 и более новые версии этой ОС. Например, поставщик Lightweight Directory Access Protocol (LDAP) модели ADSI предоставляет стандартный интерфейс для LDAP-совместимых служб и приложений, включая Windows 2000 Active Directory и Microsoft Exchange 2000.

Особо интересен поставщик IIS модели ADSI. Он определяет набор административных объектов, которые управляют метабазой IIS, содержащей определения различных элементов IIS и позволяющей изменять конфигурацию узлов и серверов IIS. Манипулируя административными объектами IIS, вы можете редактировать записи метабазы и изменять конфигурацию IIS.

Ключевые компоненты для работы с метабазой IIS — пути и имена разделов. Раздел — это область метабазы, аналогичная папке файловой системы. Путь метабазы представляет собой последовательность отделенных друг от друга косыми чертами (/) имен разделов, уникально идентифицирующей расположение раздела в метабазе. Пути метабазы служат для доступа к связанным с разделом административным объектам IIS (подробнее см. главу 12).

В папке `\Inetpub\Adminscripts` установки IIS несколько сценариев. Они содержат административные объекты для управления основными функциями IIS.

- **Change Access Restrictions (CHACCESS)** изменяет параметры доступа узла или сервера IIS. Может выполняться одновременно для нескольких ресурсов IIS и компьютеров.
- **Continue FTP Server (CONTFTP)** возобновляет работу одного или нескольких FTP-узлов на одном или нескольких компьютерах.
- **Continue Server (CONTSRV)** возобновляет работу одного или нескольких узлов IIS на одном или нескольких компьютерах.
- **Continue Web Server (CONTWEB)** возобновляет работу одного или нескольких Web-узлов на одном или нескольких компьютерах.



- **Create Virtual Directory (MKWEBDIR)** создает виртуальный каталог.
- **Create Web Site (MKW3SITE)** создает Web-узел.
- **Display Administrative Node (DISPNODE)** отображает конфигурационные параметры Web-узла,
- **Display Administrative Tree (DISPTREE)** отображает дерево административных объектов, начиная с заданного корневого узла или с вершины дерева IIS.
- **Find Web Site (FINDWEB)** ищет заданный Web-узел на указанном компьютере.
- **IIS Administration Script Utility (ADSUTIL)** получает и задает параметры IIS; создает, удаляет и копирует узлы и серверы IIS; получает сведения о состоянии приложений IIS; создает, выгружает и удаляет приложения IIS.
- **Pause FTP Server (PAUSEFTP)** приостанавливает работу одного или нескольких FTP-узлов на одном или нескольких компьютерах.
- **Pause Server (PAUSESRV)** приостанавливает работу одного или нескольких узлов IIS на одном или нескольких компьютерах.
- **Pause Web Server (PAUSEWEB)** приостанавливает работу одного или нескольких Web-узлов на одном или нескольких компьютерах.
- **Start FTP Server (STARTFTP)** запускает один или несколько FTP-узлов на одном или нескольких компьютерах.
- **Start Server (STARTSRV)** запускает один или несколько узлов IIS на одном или нескольких компьютерах.
- **Start Web Server (STARTWEB)** запускает один или несколько Web-узлов на одном или нескольких компьютерах.
- **Stop FTP Server (STOPFTP)** останавливает работу одного или нескольких FTP-узлов на одном или нескольких компьютерах.
- **Stop Server (STOPSRV)** останавливает работу одного или нескольких узлов IIS на одном или нескольких компьютерах.

- **Stop Web Server (STOPWEB)** останавливает работу одного или нескольких Web-узлов на одном или нескольких компьютерах.

Сценарии предназначены для работы с сервером сценариев Windows, выполняющимся из командной строки (CSCRIPT.EXE). На компьютере, где выполняются сценарии, данный сервер нужно зарегистрировать как сервер сценариев по умолчанию. Чтобы проверить, является ли CSCRIPT.EXE сервером сценариев по умолчанию, введите в окне MS-DOS команду:

```
cscript //H:cscript
```

Если вы находитесь в каталоге \Inetpub\Adminscripts, для запуска сценария достаточно ввести его название и параметры в командной строке, например:

```
dispnode -a IIS://localhost/w3svc
```

Для вывода справочной информации введите лишь имя сценария.

## Глава 2

# Основы администрирования IIS

К основным задачам администрирования IIS относится подключение к серверам, управление службами и сохранение конфигураций метабазы. Для подключения к отдельным серверам и управления их IIS-компонентами служат оснастка Internet Information Services и диспетчер Internet Services Manager. На одном IIS-сервере может размещаться несколько ресурсов. Ресурсы World Wide Web и File Transfer Protocol называются соответственно Web- и FTP-узлами, а ресурсы Simple Mail Transfer Protocol и Network News Transfer Protocol — виртуальными серверами SMTP и NNTP.

Узлы и виртуальные серверы — это процессы сервера с собственной конфигурационной информацией, включающей IP-адреса, номера портов и параметры проверки подлинности. Для администрирования серверов и узлов нужно зарегистрироваться на IIS-сервере по учетной записи администратора. Кроме того, управлять отдельными узлами и виртуальными серверами могут пользователи, не являющиеся администраторами, но назначенные операторами IIS. Подробнее о системе безопасности и операторах см. главу 5.

### Универсальные указатели ресурсов в IIS

Чтобы разобраться в принципах работы IIS, нужно изучить архитектуру и базовые методы доступа к документам Интернета. В этом разделе рассказывается об архитектуре IIS, а также обсуждается доступ к документам с помощью *универсальных указателей ресурсов* (uniform resource locator, URL).

## Основы архитектуры IIS

IIS можно рассматривать как надстройку ОС, требующую определенных действий перед выполнением задач IIS. Основные компоненты этой надстройки — папки и разрешения.

- Папки. Web-узлы, виртуальные серверы и прочие ресурсы используют структуру файлов и папок Microsoft Windows 2000. Перед созданием ресурсов IIS, например, узлов и виртуальных серверов убедитесь, что создали все нужные папки.
- Разрешения. Windows 2000 определяют права доступа пользователей к файлам и папкам. Прежде чем предоставить пользователям доступ к файлам и каталогам, убедитесь, что пользователи и группы имеют соответствующие разрешения ОС. После назначения разрешений уровня ОС требуется задать специфические для IIS разрешения безопасности.

Еще одна область, тесно интегрирующая Windows 2000 и IIS, — это процессы и службы Windows (рис. 2-1). Каждая служба IIS выполняется в экземпляре процесса SVCHOST.EXE. Он контролирует все выполняющиеся на сервере однотипные ресурсы, и поэтому Windows использует его для управления экземплярами конкретных ресурсов, например, Web- или FTP-узлов. Так, при останове или перезапуске службы World Wide Web Publishing Service вы управляете всеми выполняющимися на сервере Web-узлами через соответствующий процесс обработчика служб. Подробнее см. раздел «Управление службами IIS» этой главы.



Рис. 2-1. Архитектура IIS

Из-за многоуровневой структуры служб IIS останов или запуск виртуального сервера IIS не влияет напрямую на обработчик служб. Поэтому Windows управляет обработчиком через посредника — процесс InetInfo. Один экземпляр INETINFO.EXE управляет обработчиками служб, а также приложениями ISAPI, выполняющимися в контексте процесса IIS. При управлении отдельными службами Интернета Windows для взаимодействия с обработчиком служб также использует InetInfo. Кроме того, InetInfo позволяет управлять всеми выполняющимися на сервере IIS-ресурсами. Например, в оснастке Internet Information Services можно дать команду Restart (Перезапуск), полностью перезапускающую службы IIS (подробнее — в разделе «Запуск, останов и возобновление работы всех служб Интернета» этой главы).

Ключевая часть архитектуры IIS — серверные приложения ISAPI, выполняющиеся на Web-узлах IIS. Приложениями ISAPI, выполняющимися вне процесса, управляет обработчик DLL-серверов DLLHOST.EXE (рис. 2-2). Все приложения ISAPI, выполняющиеся в групповом процессе, используют один экземпляр DLLHOST.EXE. Изолированные же приложения ISAPI, напротив, выполняются в контексте отдельных процессов DLLHOST.EXE.

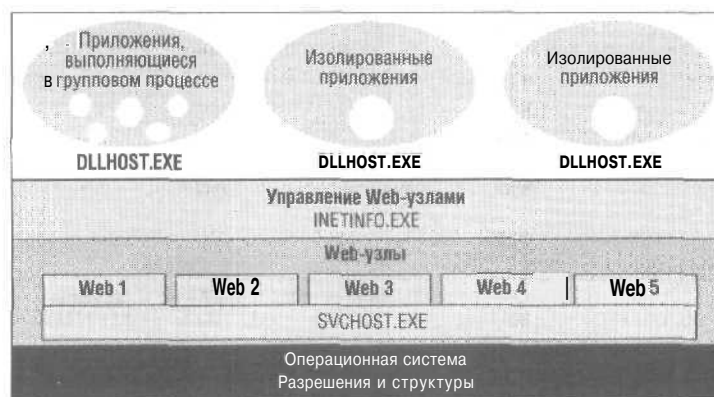


Рис. 2-2. Архитектура приложений IIS и ISAPI

### Универсальные указатели ресурсов

Для получения файлов с IIS-сервера клиент должен знать его адрес, местонахождение на нем требуемых файлов, а также протокол для доступа и загрузки файлов. Обычно все эти сведения передаются в виде универсального указателя ресурса (URL). URL — это универсальный способ идентификации ресурсов, доступных по протоколам Интернета. В основе такой универсальности лежит стандартная схема именования.

В URL указывается протокол для доступа и загрузки файла. По названию протокола клиент определяет формат следующей за ним информации. Обычно после названия протокола идут двоеточие и две косые черты. Формат следующей после них информации зависит от протокола, указанного в URL. Два самых распространенных формата таковы:

протокол://имя\_компьютера:порт/путь\_к\_ресурсу

и

протокол://имя\_пользователя:пароль@имя\_компьютера:порт/  
путь\_к\_ресурсу

Имя компьютера в URL определяет его адрес. Имена могут указываться в различной форме, включая имена NetBIOS, но самый распространенный формат — *полное доменное имя* (fully qualified domain name, FQDN). Обычно доменные имена Web-серверов начинаются с букв www. Например, URL `http://www.microsoft.com` указывает, что Web-сервер компании Microsoft относится к коммерческому домену. Существуют следующие типы доменов:

- **.com** — коммерческие узлы;
- **.edu** — узлы образовательных организаций;
- **.gov** — невоенные правительственные узлы;
- **.mil** — военные узлы;
- **.net** — сетевые узлы;
- **.org** — организационные узлы.

В URL также указывается номер порта, к которому производится подключение. При подключении к порту по умолчанию его номер указывать не требуется. Номер порта по умолчанию протокола HTTP — 80. Например, вы подключаетесь к серверу с помощью такого URL:

<http://www.microsoft.com/docs/my-yoyo.htm/>

Предполагается, что номер порта по умолчанию — 80. Если же требуется подключиться к порту 8080, укажите его номер в TJRL ресурса:

<http://www.microsoft.com:8080/docs/my-yoyo.htm/>

Номера портов по умолчанию для ресурсов IIS:

- FTP - 21;
- SMTP - 25;
- HTTP - 80;
- NNTP - 119;
- HTTPS - 443.

Последняя часть URL — это путь к ресурсу. Обычно он соответствует структуре домашнего каталога сервера, на котором находится запрашиваемый ресурс.

URL FTP-узлов иногда также включают имя пользователя и пароль, благодаря чему на FTP-сервере можно регистрироваться по конкретной учетной записи. Например, следующий URL открывает соединение с FTP-сервером Microsoft и регистрируется на нем по указанной учетной записи:

[ftp://sysadmin:rad\\$4@ftp.microsoft.com/public/download](ftp://sysadmin:rad$4@ftp.microsoft.com/public/download)

Здесь *sysadmin* — имя регистрационной учетной записи, *rad\$4* — пароль, *ftp.microsoft.com* — сервер, *public/download* — запрошенный ресурс.

Если при подключении к FTP-серверу имя пользователя и пароль не указываются, FTP-клиент (Web-браузер) пытается установить анонимное соединение. При этом предполагается, что имя для входа в систему — *anonymous*, а пароль — адрес электронной почты пользователя.

В URL могут применяться заглавные и прописные буквы, числа от 0 до 9 и некоторые специальные символы:

- звездочка (\*);
- знак доллара (\$)
- восклицательный знак (!)
- знак переноса (-);
- круглые скобки (левая и правая);

- точка (.);
- знак «плюс» (+);
- одиночная кавычка (');
- символ подчеркивания (\_).

Прочие символы зарезервированы и имеют специальное назначение:

- **двоеточие (:)** отделяет название протокола от остальной части URL, имя узла от номера порта, и имя пользователя от пароля;
- **двойная косая черта (//)** указывает, что протокол использует формат, определенный *синтаксисом схем Интернета* (Common Internet Scheme Syntax);
- **косая черта (/)** отделяет путь от имени и номера порта узла;
- **знак процента (%)** позволяет задействовать в URL управляющие коды — специальные символы, в других случаях недопустимые или имеющие особое значение;
- **символ @** отделяет в URL имя и пароль пользователя от названия узла;
- **вопросительный знак (?)** в URL является началом строки запроса, передаваемой CGI-сценарию; вся информация после этого знака была отправлена пользователем и не является частью пути к ресурсу;
- **знак «плюс» (+)** соединяет слова строки запроса; браузер заменяет им пробелы между словами пользовательского запроса;
- **знак равенства (=)** отделяет в строках запроса ключ, назначенный автором, от значения, введенного пользователем;
- **амперсанд (&)** разделяет в строках запроса наборы ключей и значений;
- **знак карата (^)** зарезервирован для использования в будущем;
- **фигурные скобки ({} )** зарезервированы для использования в будущем;
- **квадратные скобки ([])** зарезервированы для использования в будущем.



Возможность применения управляющих кодов (специальных символов, в других ситуациях недопустимых или имеющих особое значение) повышает универсальность URL. Управляющий код состоит из знака процента (начало управляющего кода) и числового значения (собственно управляющий код). Управляющий код пробела — %20. Например, его можно использовать так:

<http://www.microsoft.com/docs/my%20party%20hat.htm>

## Использование оснастки Internet Information Services

IIS — это оснастка консоли MMC, предназначенная для управления ресурсами IIS в доменах Windows. С ее помощью вы будете выполнять рутинные задачи администрирования, например, запускать службы Интернета, отдельные узлы и удаленно запускать службы.



**Примечание** Диспетчер Internet Services Manager представляет основанный на браузере интерфейс для управления Web- и FTP-ресурсами и обладает большинством функций оснастки Internet Information Services. О работе с диспетчером см. раздел «Методы Web-администрирования» главы 1.

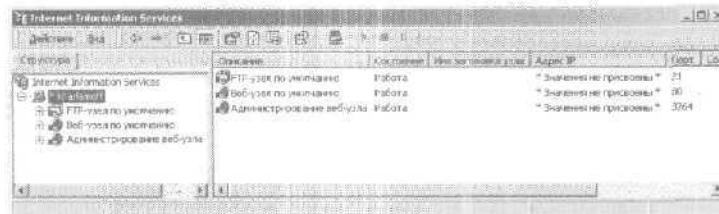
### Запуск оснастки IIS и работа с ней

Оснастка Internet Services Manager доступна в меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование), а также в оснастке Computer Management (Управление компьютером) консоли MMC. В левой панели окна Computer Management раскройте узел Services And Applications (Службы и приложения) и щелкните значок Internet Information Services (рис. 2-3).

Оснастка автоматически подключается к локальным службам IIS (если таковые имеются); кроме того, можно подключаться и к удаленным компьютерам. Компьютеры, к которым вы подключаетесь, представлены в виде отдельных узлов, позволяющих управлять их ресурсами.

После выбора узла в левой панели оснастки в правой панели отобразится информация о текущих подключениях компьютера:

- **Connection Type (Тип подключения)** — тип сетевого подключения: TCP/IP (Transmission Control Protocol/Internet Protocol) или UDP (User Datagram Protocol);
- **Status (Состояние)** — состояние компьютера: например, Unavailable (Недоступен) или Restarting (Перезапуск);
- **Computer (Компьютер)** — имя подключенного компьютера;
- **Local (Локальный)** указывает тип подключенной установки: локальная или удаленная; если значение этого поля — Yes (Да), вы подключены к локальной установке, и противном случае — работаете с удаленным компьютером.



**Рис. 2-3.** Оснастка Internet Information Services

После того, как в левой панели оснастки IIS будет выбран один из узлов компьютера, в правой панели отобразится информация о доступных на этой системе ресурсах IIS:

- **Description (Описание)** — краткое описание узла или виртуального сервера, задаваемое в диалоговом окне Properties (Свойства);
- **State (Состояние)** — состояние узла или виртуального сервера: например, Running (Работа), Stopped (Останов), Paused (Пауза) или Unknown (Нет сведений);
- **Host Header Name (Имя заголовка узла)** — в соответствующих случаях — имя узла, переданное в HTTP-заголовке клиенту;
- **IP Address (IP-адрес)** — IP-адрес узла или виртуального сервера; входящий IP-трафик сопоставляется по номеру порта и IP-адресу конкретному узлу или экземпляру виртуального сервера; значение All Unassigned (Все не назначенные) позволяет протоколам HTTP, FTP, SMTP

и NNTP использовать любые имеющиеся на сервере не назначенные IP-адреса;

- Port (Порт) — номер порта, прослушиваемого узлом или виртуальным сервером; по умолчанию для протоколов FTP, SMTP, HTTP и NNTP — 21, 25, 80 и 119 соответственно;
- Status (Состояние) — дополнительные сведения о состоянии узла или виртуального сервера.

Если вы открыли оснастку IIS из консоли Computer Management, ее интерфейс и модель поведения будут несколько отличаться от обычных (рис. 2-4). При первом запуске оснастка IIS автоматически подключается к локальным службам IIS (если таковые имеются); кроме того, можно подключаться и к удаленным компьютерам. Для этого щелкните узел Computer Management (Управление компьютером) правой кнопкой, выберите в контекстном меню команду Connect To Another Computer (Подключиться к другому компьютеру) и следуйте подсказкам.

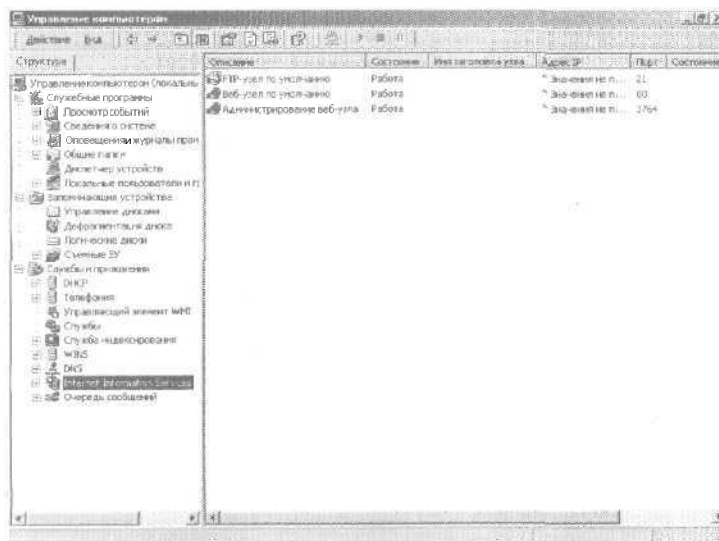


Рис. 2-4. Оснастки IIS и Indexing Service также доступны в оснастке Computer Management

### Подключение к другим серверам

Обычно администратор управляет службами IIS со своего компьютера, подключаясь к удаленным системам. Чтобы подключиться к удаленному компьютеру, сделайте следующее.

1. Запустите оснастку Internet Information Services.
2. В левой панели щелкните узел Internet Information Services правой кнопкой мыши и выберите в контекстном меню команду **Connect** (Подключение). Откроется диалоговое окно Connect to Computer (Подключение к компьютеру).
3. В поле Computer Name (Компьютер) введите имя компьютера и щелкните ОК. Кроме того, можете ввести IP-адрес или полное доменное имя сервера.

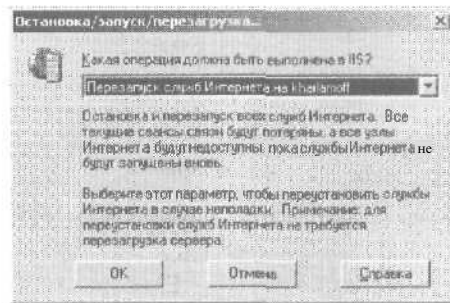
### Запуск, остановка и перезапуск всех служб Интернета

Как уже упоминалось, Windows 2000 управляет всеми службами IIS с помощью процесса INETINFO.EXE. InetInfo отслеживает все запущенные на компьютере ресурсы IIS и может отдавать им управляющие команды. Управляют InetInfo с помощью оснастки Internet Information Services или утилиты командной строки IISRESET.

Чтобы запустить, остановить или перезапустить все службы Интернета из оснастки Internet Information Services, сделайте следующее.

1. В оснастке Internet Information Services щелкните значок нужного компьютера. Если компьютер в оснастке не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» этой главы.
2. Из меню Action (Действие) выберите команду Restart IIS (Перезапуск IIS). Откроется диалоговое окно Stop/Start/Reboot (Остановка/запуск/перезагрузка) (рис. 2-5).
3. Выберите из списка команду:
  - **Start Internet Services** (Запуск служб Интернета) - запуск всех остановленных служб Интернета;
  - **Stop Internet Services** (Остановка служб Интернета) — остановка всех запущенных, приостановленных или находящихся в неизвестном состоянии служб Интернета;

- Reboot (Перезагрузка) — перезагрузка компьютера; команда аналогична команде Restart (Перезагрузка) из диалогового окна Windows Shutdown (Завершение работы Windows);
  - Restart Internet Services (Перезапуск служб Интернета) — остановка и перезапуск служб Интернета.
4. Щелкните ОК.



**Рис. 2-5.** Диалоговое окно Stop/Start/Reboot (Остановка/запуск/перезагрузка)

Важно понимать последовательность действий, выполняемых командой Restart Internet Services, которая:

1. останавливает все выполняющиеся на компьютере службы IIS, включая World Wide Web Publishing Service (Служба веб-публикаций), FTP Publishing Service (Служба FTP-публикаций), NNTP Service (Протокол Network News Transport Protocol), SMTP Service (Протокол Simple Mail Transfer Protocol) и IIS Admin Service (Служба IIS Admin);
2. пытается устранить проблемы с вышедшими из-под контроля процессами или зависшими приложениями, останавливая все процессы Dr. Watson (DRWTSN32.EXE), Microsoft Transaction Server (MTX.EXE) и обработчика DLL-серверов (DLLHOST.EXE);
3. запускает все службы IIS, а затем по мере необходимости — обработчики DLL-серверов.

Кроме того, запускать, останавливать и приостанавливать службы Интернета позволяет утилита командной строки

IISRESET. Для запуска всех остановленных на компьютере служб Интернета введите в окне MS-DOS команду *IISRESET /STOP*: она позволяет остановить все запущенные и приостановленные службы, а также службы, состояние которых неизвестно. Для управления службами IIS на удаленных компьютерах используется следующий синтаксис:

`IISRESET [ИМЯ_КОМПЬЮТЕРА] [КОМАНДА]`

Например, можно выполнить команду `IISRESET ENGSRV01 /RESTART`.

Подробнее о перезагрузке компьютеров см. раздел «Перезагрузка серверов IIS» этой главы. Параметры утилиты командной строки `IISRESET` таковы.

- **/DISABLE** запрещает перезапуск служб IIS на локальном компьютере.
- **/ENABLE** разрешает перезапуск служб IIS на локальном компьютере.
- **/NOFORCE** запрещает принудительное завершение работы служб IIS, если это не удалось сделать корректно.
- **/REBOOT** перезагружает локальный или указанный удаленный компьютер.
- **/REBOOTONERROR** перезагружает компьютер в случае ошибки при запуске, останове или приостановке служб IIS.
- **/RESTART** останавливает и перезапускает все службы IIS. Пытается устранить проблемы с вышедшими из-под контроля процессами и зависшими приложениями.
- **/START** запускает все остановленные службы IIS.
- **/STATUS** выводит сведения о состоянии служб IIS.
- **/STOP** останавливает все запущенные и приостановленные службы IIS, а также службы, состояние которых неизвестно.
- **/TIMEOUT:значение** задаст интервал ожидания (в секундах) удачного останова служб IIS. Если в командной строке был также передан параметр **/REBOOTONERROR**, по истечении заданного интервала компьютер перезагружается. Если же был передан параметр **/STOP** или **/RESTART**, возникает ошибка. Значения по умолчанию параметров

/RESTART - 20, /STOP - 60, /REBOOTONERROR -  
0 секунд.

### Запуск, остановка и приостановка отдельных ресурсов

Отдельными узлами и виртуальными серверами можно управлять точно так же, как и другими ресурсами сервера. Например, при изменении конфигурации узла или при выполнении других административных задач вам может потребоваться остановить узел, внести изменения и затем перезапустить его. Остановленный узел не работает и не принимает пользовательские соединения.

Узел или виртуальный сервер можно приостановить. После этого он перестанет принимать клиентские соединения, но уже подключенные клиенты смогут продолжить работу.

Для запуска, остановки или приостановки узла или виртуального сервера выполните следующее.

1. Запустите оснастку Internet Information Services.
2. В левой панели щелкните значок нужного компьютера. Если компьютер в оснастке не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» этой главы.
3. Щелкните нужный узел или виртуальный сервер правой кнопкой и выберите из контекстного меню команду:
  - **Start (Пуск)** — для запуска узла или виртуального сервера;
  - **Stop (Остановить)** — для остановки узла или виртуального сервера;
  - **Pause (Пауза)** — для приостановки узла или виртуального сервера (чтобы возобновить работу приостановленного узла или виртуального сервера, выберите в контекстном меню команду Pause повторно).



Примечание Для управления группами узлов и виртуальных серверов, выполняющихся в контексте одной службы IIS, используется их основной процесс. Например, основной процесс всех выполняющихся на компьютере виртуальных Web-серверов — служба World Wide Web Publishing Service. При остановке этой службы останавливаются все использующие ее Web-узлы, разрывая при этом клиентские соеди-

нения. После запуска службы World Wide Web Publishing Service запускаются все Web-узлы, которые были остановлены в результате ее остановки. Подробнее об управлении службами IIS см. соответствующий раздел этой главы.

### Перезагрузка IIS-серверов

Оснастка Internet Information Services и утилита IISRESET имеют расширения, позволяющие перезагружать локальные и удаленные компьютеры. Для работы с ними на компьютере должны быть установлены службы IIS, кроме того, вы должны состоять в группе, обладающей необходимыми разрешениями. Для перезагрузки локального компьютера требуется разрешение на завершение работы системы, для перезагрузки удаленной машины — разрешение на принудительное удаленное завершение работы компьютера. IIS-сервер следует перезагружать только при отказе команды Restart. Чтобы перезагрузить IIS-сервер с помощью оснастки IIS, сделайте следующее.

1. В оснастке Internet Information Services щелкните значок нужного компьютера. Если компьютер в оснастке не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» этой главы.
2. Из меню Action (Действие) выберите команду Restart IIS (Перезапуск IIS). Откроется диалоговое окно Stop/Start/Reboot (Остановка/запуск/перезагрузка) (рис. 2-5).
3. Выберите команду Reboot (Перезагрузка) и щелкните ОК.
4. Компьютер получит сообщение, что работа системы будет завершена через 30 секунд. После завершения работы компьютер перезагрузится.

Для перезагрузки компьютера с помощью утилиты IISRESET введите в окне MS-DOS команду *IISRESET [COMPUTERNAME] /REBOOT*.

Например, можно выполнить команду:

```
IISRESET ENGSR01 /REBOOT
```

Если задачи пользователя требуют корректного завершения, задайте интервал ожидания остановки служб и процессов.



По умолчанию он составляет 0 секунд, т. е. система сразу выключается и Windows 2000 не ожидает корректного завершения работы служб. Чтобы задать интервал ожидания в 60 секунд при перезагрузке компьютера engsvr01, выполните команду:

```
IISRESET ENGSR01 /REBOOT /TIMEOUT:60
```

## Управление службами IIS

Все IIS-серверы организации используют определенный набор служб для публикации страниц, обмена файлами и т. д. Управлять службами IIS можно из узла Services (Службы) оснастки Computer Management (Управление компьютером).

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и выберите Computer Management (Управление компьютером).
2. В дереве консоли щелкните значок Computer Management (Управление компьютером) правой кнопкой, выберите в контекстном меню команду Connect To Another Computer (Подключиться к другому компьютеру) и укажите в открывшемся диалоговом окне нужный IIS-сервер.
3. Раскрыв узел Services and Applications (Службы и приложения), щелкните значок Services (Службы) (рис. 2-6), где:
  - Name (Имя) — название службы;
  - Description (Описание) — краткое описание службы и ее назначения;
  - Status (Состояние) — состояние службы: Started (Работает), Paused (Приостановка) или Stopped (Остановлена; в этом случае поле Status отображается пустым);
  - Startup Type (Тип запуска) - тип запуска службы;



**Примечание** Автоматически запускаемые службы загружаются одновременно с ОС. Службы, запускаемые вручную, загружаются пользователем. Отключенные службы запустить нельзя.

- Log On As (Вход в систему) — учетная запись для входа в систему; обычно службы используют учетную запись LocalSystem.



- **Network News Transport Protocol (NNTP, Протокол Network News Transport Protocol (NNTP))** предоставляет службы групп новостей и позволяет администрировать NNTP-серверы из оснастки Internet Information Services.
- **Simple Mail Transfer Protocol (SMTP, Протокол Simple Mail Transfer Protocol (SMTP))** предоставляет службы обмена сообщениями и позволяет администрировать SMTP-серверы из оснастки Internet Information Services.
- **World Wide Web Publishing Service (Служба веб-публикаций)** позволяет обмениваться файлами по протоколу HTTP и администрировать HTTP-серверы.

### Запуск, остановка и приостановка служб IIS

Администратору часто приходится запускать, останавливать и приостанавливать службы IIS. Управляют службами IIS с помощью консоли Computer Management (Управление компьютером) и узла Services (Службы). На данном уровне управления любые действия затрагивают все использующие службу узлы и виртуальные серверы. Например, если на компьютере опубликовано три Web-узла, при остановке службы World Wide Web Publishing они прекратят работу и станут недоступны.

Для запуска, остановки и приостановки служб из консоли Computer Management выполните следующее.

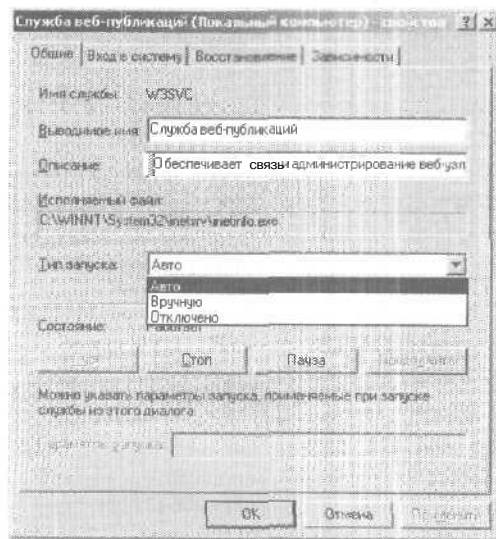
1. В дереве консоли щелкните значок Computer Management (Управление компьютером) правой кнопкой, выберите в контекстном меню команду Connect To Another Computer (Подключиться к другому компьютеру), и укажите в открывшемся диалоговом окне нужный IIS-сервер.
2. Раскройте узел Services and Applications (Службы и приложения) и щелкните значок Services (Службы).
3. Щелкните соответствующую службу правой кнопкой и выберите в контекстном меню команду Start (Пуск), Stop (Остановить) или Pause (Пауза). Остановить и после короткой паузы снова запустить службу позволяет команда Restart (Перезапуск). Чтобы возобновить работу приостановленной службы, можно также повторно выбрать из контекстного меню команду Pause.



**Совет** В случае ошибки при загрузке автоматически запускаемой службы поле Status отображается пустым, и ОС выводит соответствующее сообщение. Сообщения об отказах служб можно заносить в системный журнал событий. Windows 2000 позволяет настроить специальные действия (actions) для автоматической обработки отказов служб. Так, ОС может перезапускать за вас службу. Подробнее см. раздел «Настройка восстановления служб» данной главы.

### Настройка запуска службы

Основные службы IIS сконфигурированы для автоматического запуска, и без особых причин изменять этот порядок не следует. И все же вам может понадобиться запускать службу вручную. Кроме того, службу можно отключить, чтобы связанные с ней виртуальные серверы не запускались. Например, при перемещении виртуального SMTP-сервера на новый компьютер на исходном IIS-сервере отключают службу SMTP — она использоваться не будет, но при необходимости ее можно запустить.



**Рис. 2-7.** Вкладка General (Общие) диалогового окна свойств службы World Wide Web Publishing (Служба веб-публикаций)

Для настройки запуска службы выполните следующее.

1. В консоли Computer Management (Управление компьютером) подключитесь к нужному IIS-серверу.
2. Раскройте узел Services And Applications (Службы и приложения) и щелкните значок Services (Службы).
3. Щелкните значок нужной службы правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
4. На вкладке General (Общие) выберите из списка Startup Type (Тип запуска) тип запуска службы — Automatic (Авто), Manual (Вручную) или Disabled (Отключено) (рис. 2-7).
5. Щелкните ОК.

### Настройка восстановления службы

Службы Windows можно сконфигурировать для выполнения определенных действий в случае отказа. Например, попробовать перезапустить службу или перезагрузить сервер. Задайте параметры восстановления службы.

1. В консоли Computer Management (Управление компьютером) подключитесь к IIS-серверу.
2. Раскройте узел Services And Applications (Службы и приложения) и щелкните значок Services (Службы).
3. Щелкните значок нужной службы правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
4. На вкладке Recovery (Восстановление) задайте действия при первом, втором и последующих отказах службы (рис. 2-8):
  - Take No Action (Ничего не делать);
  - Restart The Service (Перезапуск службы);
  - Run A File (Выполнение программы);
  - Reboot The Computer (Перезагрузка компьютера).
5. В зависимости от заданных параметров может потребоваться изменить другие параметры перезапуска службы. Если вы выбрали перезапуск служб, задайте продолжительность задержки перед ним. Остановив службу, Windows 2000 ожидает в течение заданного интервала времени и затем перезапускает ее. Обычно достаточно задержки в 1-2 минуты.

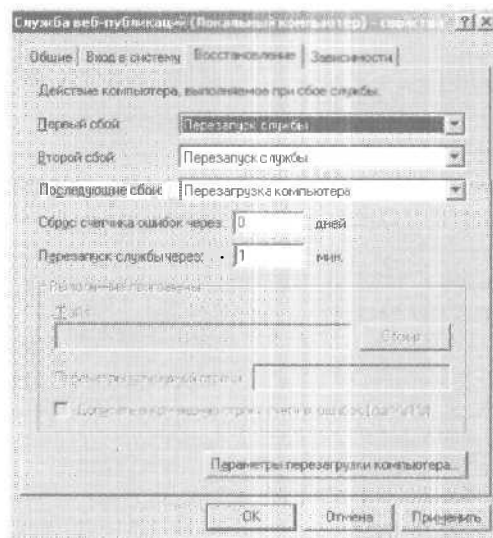


Рис. 2-8. Вкладка Recovery (Восстановление) диалогового окна свойств службы World Wide Web Publishing (Служба веб-публикации)

6. Щелкните OK.

Важные службы можно настроить для перезапуска при первом и втором отказах, и для перезагрузки сервера при третьем отказе.

## Настройка резервного копирования и восстановления IIS

Самые важные задачи Web-администратора — резервное копирование и восстановление IIS-серверов.

### Сохранение конфигурации сервера

При резервном копировании IIS-сервера обратите внимание на конфигурацию IIS и компьютера. Необходимо сохранять конфигурацию IIS в файл метабазы при любом изменении параметров служб IIS и в качестве дополнительной меры предосторожности хранить несколько резервных копий конфигурации.

Периодически архивируйте сервер (подробнее об этом см. книгу «Windows 2000. Справочник администратора»). На основе резервной копии вы сможете:

- восстановить конфигурационные параметры IIS для узлов и виртуальных серверов;
- восстановить поврежденную службу IIS, переустановить IIS;
- восстановить сервер, а также его файлы данных и конфигурацию IIS;
- провести выборочное восстановление и изменить поврежденные или уничтоженные файлы.

Резервные копии IIS содержат метаданные, описывающие конфигурационные параметры узлов и виртуальных серверов Интернета. IIS использует метаданные для восстановления значений всех свойств ресурсов, включая параметры безопасности, виртуальных каталогов и приложений ISAPI. Кроме того, эта информация нужна для поддержки рабочего состояния узлов и виртуальных серверов. Итак, если вы сохраните конфигурацию IIS, а позже восстановите ее, все значения параметров и ресурсы IIS вернутся в исходное состояние (Running, Paused, Stopped и т. д.).

Рекомендую архивировать конфигурацию IIS после внесения в нее любых мелких изменений, а также перед внесением крупных изменений, влияющих на доступность ресурсов. Резервные копии конфигураций IIS хранятся в виде файлов с расширением .md0 в папке %SystemRoot%\system32\inetsrv\MetaBack. Md0 указывает, что файл содержит метаданные. Обычно размер резервной копии составляет не более 200 Кб.

Резервные копии конфигураций IIS позволяют восстановить:

- удаленные ресурсы — хранятся ссылки на все выполнявшиеся на сервере экземпляры узлов и виртуальных серверов;
- значения параметров узла или сервера — хранятся все конфигурационные параметры узлов и виртуальных серверов;
- конфигурацию приложений ISAPI — хранятся все параметры приложений ISAPI, включая App Mappings, App Options, Process Options и App Debugging;

- **основные свойства Web- и FTP-служб** — хранятся все основные свойства, а также другие значения параметров IIS верхнего уровня (т. е. можно восстановить параметры по умолчанию новых Web- и FTP-узлов, параметры регулирования полосы пропускания, а также сопоставления типов MIME); восстановить основные свойства серверных расширений нельзя;
- **поврежденную установку IIS** — для этого потребуется удалить и повторно установить IIS, а затем восстановить значения параметров из последней резервной копии конфигурации IIS.

Подробнее см. раздел «Восстановление поврежденной установки IIS» этой главы.

Открыв файл резервной копии в текстовом редакторе, вы увидите, что он содержит разделы и пути **метабазы**, специфичные для текущего сервера. Это важно, потому что позволяет восстанавливать параметры IIS, хранящиеся в реестре, не работая с реестром напрямую. Параметры реестра специфичны для конкретного компьютера и экземпляра, т. е. восстановить **конфигурационные** параметры IIS на других компьютерах или после переустановки ОС нельзя,

### Создание резервных копий конфигурации IIS

Конфигурацию всех IIS-серверов следует периодически архивировать. Для этого сделайте следующее.

1. В оснастке Internet Information Services щелкните значок **нужного компьютера**. Если компьютер в оснастке не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам».
  2. Из меню Action (Действие) выберите команду Backup/Restore Configuration (Архивирование/восстановление конфигурации). Откроется **одноименное** диалоговое окно (рис. 2-9).
  3. Щелкните Create backup (Создать архив), а затем введите имя файла резервной копии и щелкните ОК. IIS создаст резервную копию конфигурации IIS. По умолчанию эти копии хранятся в папке %SystemRoot%\System32\Inet-srv\MetaBack.
- 1. Щелкните Close (Заккрыть).



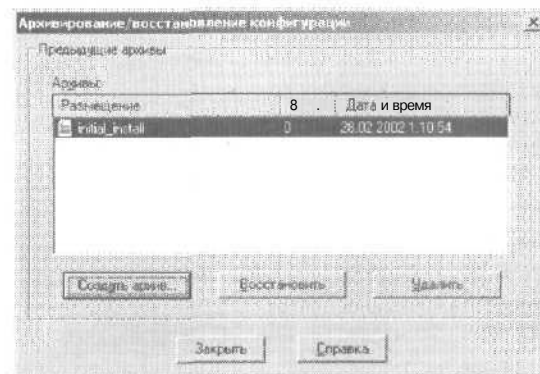


Рис. 2-9. Диалоговое окно Backup/Restore Configuration (Архивирование/восстановление конфигурации)

### Восстановление IIS из резервной копии

Службу IIS можно восстановить, используя файлы резервных копий конфигурации IIS. При этом будут восстановлены прежние значения параметров и состояние служб. Восстановление конфигурации не позволит наладить работу поврежденной установки IIS. Подробнее о восстановлении поврежденных установок см. одноименный раздел этой главы. При восстановлении IIS из резервной копии Windows 2000 останавливает и перезапускает службы IIS. Оповестив пользователей о недоступности ресурсов в течение следующих нескольких минут, сделайте так.

1. В оснастке Internet Information Services щелкните значок нужного компьютера. Если компьютер в оснастке не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам».
2. В меню Action (Действие) выберите команду Backup/Restore Configuration (Архивирование/восстановление конфигурации). Откроется одноименное диалоговое окно (рис. 2-9).
3. В панели Backup (Архивы) отображается список имеющихся на компьютере резервных копий конфигурации IIS. Выбрав нужный файл, щелкните Restore (Восстановить). Затем щелкните Yes, чтобы подтвердить восстановление конфигурационных параметров.

### Восстановление поврежденных установок MS

Поврежденная установка IIS может мешать работе узлов и виртуальных серверов IIS. Возможно, не будут работать ресурсы, IIS не среагирует на команды или зависнет. Для устранения этих проблем нужно восстановить установку IIS. Это занимает от 5 до 15 минут и требует полной остановки работы узлов и виртуальных серверов IIS.



**Внимание!** Резервные копии конфигурации IIS специфичны для конкретного компьютера и экземпляра, т. е. восстанавливать конфигурационные параметры IIS на других компьютерах или после переустановки ОС нельзя.

Чтобы восстановить поврежденную установку IIS, выполните следующие действия.

1. Локально зарегистрируйтесь на компьютере, где требуется восстановить IIS, используя учетную запись и пароль администратора.
2. Раскройте меню `Start\Settings` (Пуск\Настройки) и выберите `Control Panel` (Панель управления).
3. Дважды щелкните значок `Add\Remove Programs` (Установка и удаление программ). Откроется одноименное диалоговое окно.
4. Щелкните значок `Add/Remove Windows Components` (Установка и удаление компонентов Windows), чтобы запустить мастер `Windows Components Wizard` (Мастер компонентов Windows).
5. В списке `Components` (Компоненты) снимите флажок `Internet Information Services` и щелкните `Next` (Далее). После того как программа установки удалит службы IIS, щелкните `Next` (Далее), а затем — `Finish` (Готово).
6. В диалоговом окне `Add\Remove Programs` щелкните значок `Add/Remove Windows Components`. Запустится мастер `Windows Components Wizard`.
7. Пометьте флажок `Internet Information Services` для повторной установки служб IIS. При необходимости щелкните `Details` (Состав) и выберите нужные компоненты.
8. Щелкните `Next` (Далее). По завершении установки служб IIS щелкните `Next` и затем — `Finish` (Готово).

9. Щелкните Close (Закрыть), чтобы закрыть диалоговое окно Add/Remove Programs (Установка и удаление программ), и откройте оснастку Internet Information Services.
10. В дереве оснастки щелкните нужный компьютер правой кнопкой и выберите в контекстном меню команду Backup/Restore Configuration (Архивирование и восстановление конфигурации).
11. В открывшемся диалоговом окне выберите требуемую резервную копию IIS и щелкните Restore (Восстановить).
12. При запросе системы щелкните Yes (Да), чтобы подтвердить восстановление значений параметров. После восстановления конфигурации IIS щелкните Close (Закрыть), чтобы вернуться к оснастке Internet Information Services.

### Удаление резервных копий конфигурации IIS

Со временем число резервных копий IIS в папке MetaBack значительно увеличится. Ненужные файлы резервных копий позволяет удалить диалоговое окно Configuration Backup (Архивирование/восстановление конфигурации).

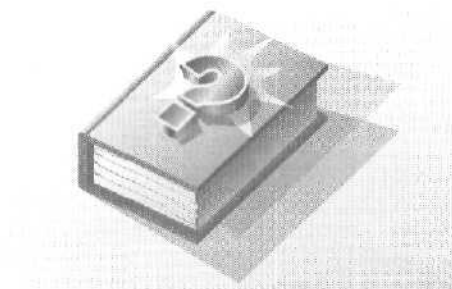
1. В оснастке Internet Information Services щелкните значок нужного компьютера. Если компьютер в оснастке не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам».
2. Из меню Action (Действие) выберите команду Backup/Restore Configuration (Архивирование/восстановление конфигурации). Откроется одноименное диалоговое окно.
3. В панели Backup (Архивы) отображается список имеющихся на компьютере резервных копий конфигурации IIS. Выбрав нужный файл, щелкните Delete (Удалить). Затем щелкните Yes (Да), чтобы подтвердить удаление файла.
4. Резервные копии навсегда удаляются с жесткого диска компьютера. Восстановить их из корзины невозможно.



## Часть II

# Администрирование Web-сервера

Во второй части книги рассмотрены основные задачи администрирования серверов **World Wide Web**, работающих под управлением **Internet Information Services**. Глава 3 посвящена управлению Web-узлами и серверами, а также созданию виртуальных каталогов и управлению ими. В главе 4 основное внимание уделено настройке **IIS**, обсуждаются также фильтры **ISAPI**, настраиваемые **HTTP**-заголовки, пользовательское содержимое, сообщения об ошибках сервера и типы **MIME**. В главе 5 рассказывается о безопасности Web-узлов и серверов. Для управления безопасностью сервера создаются учетные записи пользователей, настраиваются разрешения папок и назначаются операторы. Назначая привилегии операторов и разрешения, вы определяете свободу действий пользователя, а также доступные ему области Web-узла. В главе 6 обсуждаются сертификаты сервера и серверные расширения. Сертификаты обеспечивают безопасные Web-коммуникации, а серверные расширения применяются для администрирования и редактирования содержимого Web-узлов.



## Глава 3

# Настройка Web-узлов и Web-серверов

Глава посвящена настройке серверов и узлов World Wide Web. Мы рассмотрим составляющие этого процесса — именование и идентификацию Web-узлов, управление их основными свойствами, создание Web-узлов и др.

Свойства Web-узла идентифицируют его, задают конфигурационные параметры, а также определяют порядок доступа к документам. Свойства Web-узла по умолчанию можно задать на глобальном уровне, на уровне узла или папки.

Первые задаются в окне основных свойств Web-сервера и могут наследоваться всеми создаваемыми на нем узлами. Вторые — в диалоговом окне свойств Web-узла и распространяются только на данный Web-узел. Третьи — в диалоговом окне свойств папки и распространяются только на конкретную папку.

### Именование и идентификация Web-узлов

В этом разделе обсуждаются правила именования и идентификации Web-узлов. Независимо от типа все Web-узлы организации обладают уникальными характеристиками. Для узлов интрасети обычно используются имена компьютеров, разрешаемые локально, а также частные IP-адреса. Для узлов Интернета применяются полные доменные имена и общедоступные IP-адреса. Кроме того, узлы Интернета и интрасети могут использовать имена заголовков, позволяющие размещать несколько Web-узлов на компьютере с одним IP-адресом и портом.

#### IP-адреса и разрешение имен

Независимо от того, какой узел вы создаете — интрасети или Интернета, Web-серверу надо назначить уникальный IP-ад-

рес идентифицирующий компьютер в сети. IP-адрес — это числовой идентификатор компьютера. Схема IP-адресации зависит от конфигурации сети, но обычно IP-адреса назначаются из диапазона адресов конкретного сегмента сети. Так, если вы работаете в сегменте сети 192.55.10.0, вам будет доступен диапазон адресов 192.55.10.1 — 192.55.10.254.

Человеку сложнее, чем машине, запомнить числовые адреса, и поэтому компьютерам назначают простые текстовые имена. Существует два основных вида текстовых имен: для частных сетей — обычные имена компьютеров, а для общедоступных — имена Интернета.

Частными называются сети, подключенные к Интернету косвенно или полностью отключенные от него. В них применяются частные IP-адреса, недоступные из Интернета, включая:

- 10.0.0.1 - 10.255.255.254;
- 172.16.0.1 - 172.31.255.254;
- 192.168.0.1 - 192.168.255.254.

Частные сети, в которых применяются Интернет-технологии, называются интрасетями. Обмен информацией в них осуществляется с помощью привязок «IP-адрес — текстовое имя (NetBIOS-имя) компьютера». Windows-компоненты разрешают имена по протоколу NetBIOS, а TCP/IP-компоненты — используя Domain Name System (DNS, система доменных имен). В Microsoft Windows DNS-имя компьютера по умолчанию соответствует NetBIOS-имени. Скажем, если при установке сервера вы задали его имя как CorpServer, оно будет назначено в качестве NetBIOS- и DNS-имен по умолчанию.

Общедоступные сети напрямую подключены к Интернету. В них применяются IP-адреса, покупаемые или арендуемые для общественного использования. Обычно IP-адрес для общедоступного сервера можно получить у поставщика услуг Интернета (Internet Service Provider, ISP). ISP и другие организации приобретают группы IP-адресов у РосНИИРОС (Российский НИИ Развития Общественных Сетей).

В Интернете для разрешения текстовых имен в IP-адреса применяется DNS. Например, в таком DNS-имени, как *www.microsoft.com*, *www* — имя сервера, а *microsoft.com* — имя домена. Как и в случае с общедоступными IP-адресами, доменные имена арендуются или приобретаются. При-

обрести доменное имя можно в специализированном регистрационном бюро, например Сетевом Информационном Центре РосНИИРОС. Если клиентская система пытается подключиться к узлу по его доменному имени, запрос на подключение передается DNS-серверу. Тот возвращает IP-адрес, соответствующий имени компьютера, и клиентский запрос перенаправляется на соответствующий узел.

Не путайте открытую систему имен DNS, используемую в Интернете, и частные системы имен, применяемые в интрасетях. DNS-имена задаются на DNS-серверах, и перед обращением к узлу их нужно преобразовать в IP-адреса. Это позволяет серверу иметь несколько IP-адресов, каждому из которых соответствует уникальное DNS-имя. Так, серверу с именем *Gandolf* могут соответствовать IP-адреса 207.46.230.210, 207.46.230.211 и 207.46.230.212. Если на DNS-сервере эти IP-адреса сконфигурированы соответственно как *www.microsoft.com*, *services.microsoft.com* и *products.microsoft.com*, сервер сможет отвечать на запросы к данным доменным именам.

### Идентификаторы Web-узла

Все Web-узлы, развернутые в организации, обладают уникальными идентификаторами, позволяющими им принимать запросы и реагировать на них. Идентификатор включает имя компьютера или DNS-имя, IP-адрес, номер порта и необязательное имя заголовка узла.

Состав идентификатора зависит от того, где находится сервер, на котором размещен Web-узел, — в частной или общедоступной сети. Например, в частной сети компьютер с именем *CorpIntranet* имеет IP-адрес 10.0.0.52. Для доступа к Web-узлу на нем можно воспользоваться:

- **UNC-путем** (Uniform Naming Convention, универсальные правила именования) — `\\CorpIntranet` или `\\10.0.0.52`;
- **URL** (Uniform Resource Locator, универсальный указатель ресурса) — `http://CorpIntranet` или `http://10.0.0.52/`;
- **URL и номером порта** — `http://CorpIntranet:80` или `http://10.0.0.52:80/`.

Другой пример: в общедоступной сети компьютер с именем *Dingo* имеет DNS-имя *www.microsoft.com* и IP-адрес 207.46.230.210. Для доступа к Web-узлу на нем можно воспользоваться:



- URL - *http://www.microsoft.com/*или *http://207.46.230.210/*;
- URL и номером порта — *http://www.microsoft.com:80*или *http://207.46.230.210:80/*

### Размещение нескольких узлов на одном сервере

Используя различные комбинации IP-адресов, номеров портов и имен заголовков узлов, на одном компьютере можно размещать несколько узлов. Это дает определенные преимущества. Например, вместо настройки трех разных компьютеров для размещения Web-узлов *www.microsoft.com*, *support.microsoft.com* и *service.microsoft.com* вы размещаете их на одном компьютере.



Примечание На компьютерах с Windows 2000 Professional можно разместить лишь один Web-узел и один FTP-сервер. Чтобы разместить несколько Web- или FTP-узлов, обновите ОС до Windows 2000 Server.

Один из эффективных способов размещения нескольких узлов на одном сервере — назначить ему несколько IP-адресов (рис. 3-1).

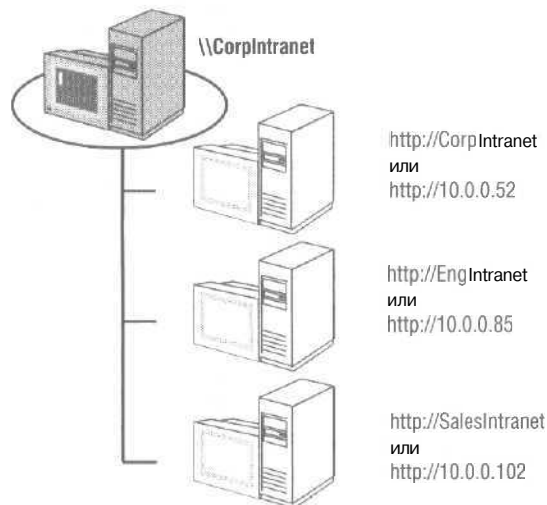


Рис. 3-1. Размещение нескольких Web-узлов на одном сервере путем назначения им разных IP-адресов

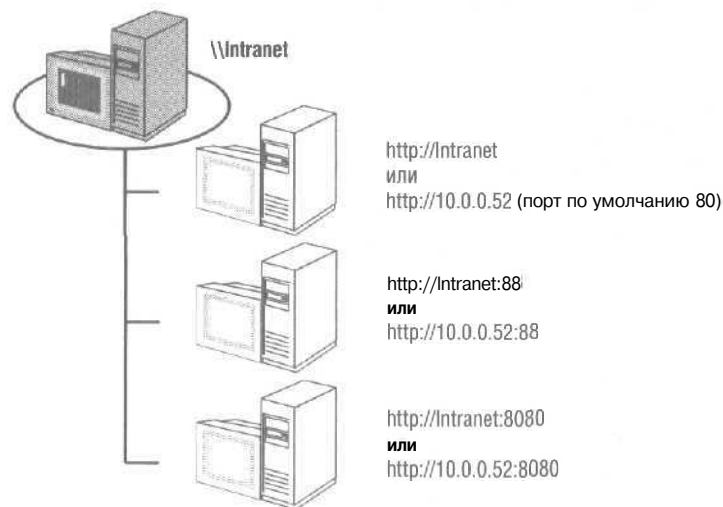
Для этого потребуется:

- сконфигурировать параметры TCP/IP сервера так, чтобы каждому из размещаемых узлов соответствовал один IP-адрес;
- настроить систему разрешения имен для разрешения имен узлов и соответствующих IP-адресов;
- настроить Web-узел для использования отдельного IP-адреса.

При этом пользователи смогут обращаться к нужным им узлам, вводя в браузере уникальное доменное имя или IP-адрес. Так, в обсуждаемом примере (рис. 3-1), для доступа к узлу SalesIntranet можно ввести *http://SalesIntranet* или *http://10.0.0.102/*.

Еще один метод размещения нескольких узлов на одном сервере — использовать один IP-адрес, но разные номера портов (рис. 3-2). Тогда пользователи смогут обращаться:

- к основному узлу, вводя в браузере текстовое имя или IP-адрес, например *http://Intranet* или *http://10.0.0.52/*.



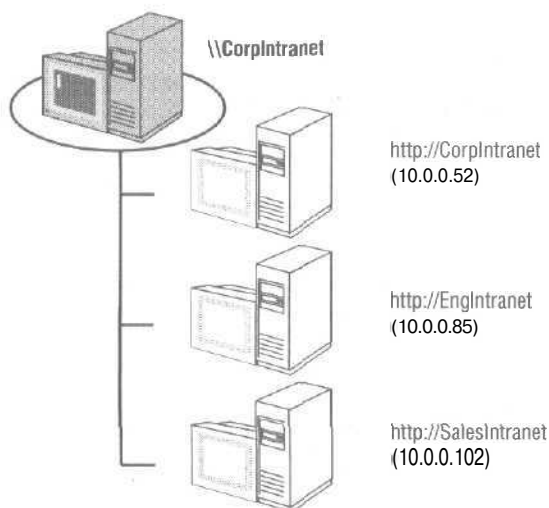
**Рис. 3-2.** Размещение нескольких Web-узлов на одном сервере путем назначения им разных номеров портов

- к другим виртуальным серверам, вводя в браузер доменное имя и или IP-адрес, а также номер порта, например `http://Intranet:88/` или `http://10.0.0.52:88/`.

Третий способ — воспользоваться заголовками узлов, они позволяют развернуть несколько узлов на компьютере с одним IP-адресом и номером порта. Этот метод основан на принципах назначения DNS-имен, которые задаются в системе разрешения имен и затем указываются в свойствах узла.

Допустим, на одном компьютере размещены узлы CorpIntranet, EngIntranet и SalesIntranet (рис. 3-3). Все они используют один и тот же IP-адрес и номер порта, но имеют разные DNS-имена. Чтобы задействовать заголовки узлов, потребуется настроить:

- систему разрешения имен для разрешения имен узлов и соответствующих IP-адресов;
- основной Web-узел для ответа на запросы к назначенным ему IP-адресу и номеру порта;
- дополнительные Web-узлы для использования одного IP-адреса и номера порта, а также назначенных заголовков узлов.



**Рис. 3-3.** Размещение нескольких Web-узлов на одном сервере с помощью заголовков узлов

Данный метод не лишен недостатков. Старые версии браузеров, не поддерживающие *протокол* HTTP 1.1, не могут возвращать имена заголовков узлов службам IIS. Так, браузеры Microsoft Internet Explorer версий *младше* 3.0 и Netscape Navigator версий *младше* 2.0 не поддерживают заголовки узлов, и их пользователи смогут просмотреть лишь основной *Web-узел*, которому соответствует данный IP-адрес. Еще один недостаток: заголовки узлов нельзя использовать совместно с протоколом Secure Sockets Layer (SSL). SSL шифрует HTTP-запросы, и поэтому определить нужный клиенту узел на основе имени *заголовка* узла из зашифрованного запроса невозможно.

### **Проверка имени компьютера и IP-адреса сервера**

*Перед* настройкой *Web-узлов* следует узнать имя компьютера и IP-адрес сервера. Для этого сделайте следующее.

1. На рабочем столе Windows щелкните правой кнопкой значок My Computer (Мой Компьютер) и выберите в контекстном меню команду Properties (Свойства). *Откроется* диалоговое окно System Properties (Свойства системы).
2. Перейдите на вкладку Network Identification (Сетевая идентификация), где отображаются полное доменное имя сервера и *домен*, к которому он относится. Полное доменное имя является *DNS-именем* компьютера.
3. DNS-имя обычно служит для *доступа* к IIS-ресурсам сервера. Например, если DNS-имя компьютера — www.microsoft.com и Web-узел использует порт 80, для доступа к компьютеру из Интернета следует ввести URL *http://www.microsoft.com/*.



**Совет** Чтобы изменить имя и членство компьютера в домене, щелкните Properties (Свойства) и введите новые значения. Если компьютер — контроллер домена, для изменения этих параметров потребуется переустановить ОС. Помните, что сведения на вкладке Network Identification (Сетевая идентификация) известны лишь конкретному компьютеру. Для корректного разрешения имен следует создать соответствующие записи на DNS-сервере.

Чтобы посмотреть IP-адрес и прочие параметры TCP/IP компьютера, сделайте так.

1. Раскройте меню Start\Settings (Пуск\Настройка) и выберите Network And Dial-Up Connections (Сеть и удаленный доступ к сети). Откроется одноименное диалоговое окно.
2. Щелкните значок Local Area Connection (Подключение по локальной сети) правой кнопкой и выберите в контекстном меню команду Properties (Свойства). Откроется соответствующее диалоговое окно.
3. Дважды щелкните Internet Protocol (TCP/IP). Откроется диалоговое окно Internet Protocol (TCP/IP) Properties (Свойства: TCP/IP). Или выделите Internet Protocol (TCP/IP) и щелкните Properties (Свойства).
4. Будут показаны параметры IP-адреса, а также прочие параметры протокола TCP/IP (рис. 3-4).

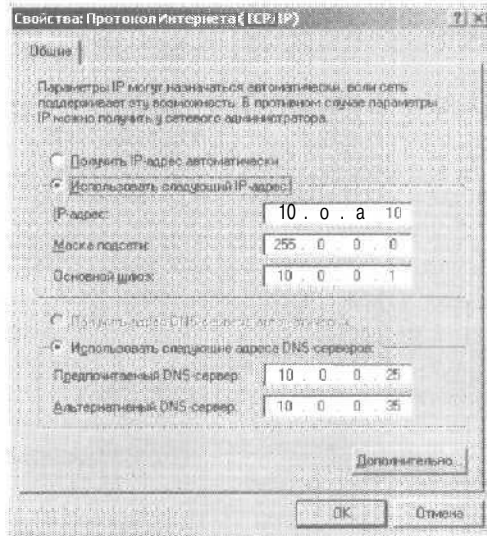


Рис. 3-4. Диалоговое окно Internet Protocol (TCP/IP) Properties (Свойства: TCP/IP)



**Совет** IIS-серверы должны использовать статические IP-адреса. Если компьютер получает IP-адрес автоматически, соответствующим образом измените параметры TCP/IP. Подробнее см. главу 15 книги «Microsoft Windows 2000. Справочник администратора».

## Управление основными свойствами Web-службы

Основные свойства Web-службы определяют значения по умолчанию свойств Web-узлов, создаваемых на сервере. Изменения глобальных свойств наследуются существующими Web-узлами. В некоторых ситуациях администратор может указать узлы и папки, которые должны наследовать изменения, в других — система автоматически применяет изменения ко всем существующим Web-узлам.

Чтобы изменить основные свойства Web-службы, сделайте следующее.

1. В оснастке Internet Information Services щелкните значок нужного компьютера правой кнопкой и выберите в контекстном меню команду Properties (Свойства). Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2.
2. В группе Master Properties (Основные свойства) выберите из раскрывающегося списка пункт WWW Service (WWW-служба) и щелкните Edit (Изменить). Откроется диалоговое окно WWW Service Master Properties (Основные свойства WWW-службы) для данного компьютера.
3. Внесите изменения и щелкните ОК.
4. Перед применением новых параметров IIS проверяет текущие значения всех характеристик вложенных узлов выбранного ресурса (при наличии таковых). Если параметры Web-узла или папки отличаются от предлагаемых, откроется диалоговое окно Inheritance Overrides (Переопределение наследования), позволяющее переопределить параметры отдельных узлов и папок. Щелкните ОК.

## Создание Web-узлов

При установке в составе IIS службы World Wide Web Publishing Service (Служба веб-публикаций) автоматически создается Web-узел по умолчанию. Изменять параметры сети, чтобы предоставить пользователям доступ к этому Web-узлу, не требуется. Достаточно лишь сообщить им URL, который следует вводить в поле Address (Адрес) браузера. Так, если DNS-имя компьютера — `www.microsoft.com` и узел использует порт 80, URL — `http://www.microsoft.com/`.

Web-узел по умолчанию предназначен для помощи начинающим администраторам и содержит массу папок с полезными приложениями и документацией.

- **IISHelp** — папка с интерактивной справочной документацией. По умолчанию находится в каталоге %SystemRoot%\Help\IisHelp и представляет собой групповое ISAPI-приложение IIS Help Application (Справочное приложение IIS).
- **IISAdmin** — папка с административными страницами Web-узла. Ее следует создать на каждом Web-узле, требующем удаленного администрирования. По умолчанию находится в каталоге %SystemRoot%\System32\Inetsrv\Iisadmin и представляет собой групповое ISAPI-приложение Administration Application (Приложение администрирования),
- **IISamples** — папка с примерами документов, полезных администраторам и разработчикам. По умолчанию находится в каталоге \Iisamples корневой папки IIS и представляет собой групповое ISAPI-приложение Sample Application (Учебное приложение).

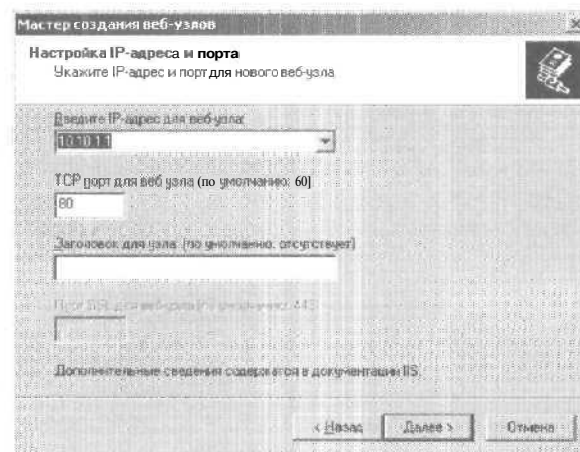
Хотя Web-узел по умолчанию полезен новичкам, он может стать источником многих проблем. Так, стандартные ISAPI-приложения занимают системные ресурсы, которым можно найти лучшее применение. Файлы приложений — легкая мишень для злоумышленников. Кроме того, папка \IISAdmin делает возможным удаленное администрирование, даже когда это нежелательно.

В связи с этим и по ряду других причин я рекомендую удалить Web-узел по умолчанию и создать вместо него новый. Затем по мере необходимости создавайте другие каталоги по умолчанию. Скажем, чтобы разрешить удаленное администрирование узла, создайте виртуальный каталог с именем \IISAdmin, ссылающийся на папку %SystemRoot%\System32\Inetsrv\Iisadmin. Подробнее см. ниже раздел «Подключение IISAdmin, IISHelp и прочих системных каталогов». Для создания дополнительных Web-узлов сделайте так.

1. Устанавливая Web-узел на новом сервере, убедитесь в наличии на нем службы World Wide Web Publishing Service.
2. Если Web-узел будет использовать новый IP-адрес, его нужно предварительно настроить. Подробнее см. главу 15

книги «Microsoft Windows 2000. Справочник администратора».

3. В оснастке Internet Information Services щелкните значок требуемого компьютера правой кнопкой и выберите в контекстном меню команду New\Web Site (Создать\Узел Web). Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2,
4. Запустится мастер Web Site Creation Wizard (Мастер создания Web-узлов). Щелкните Next (Далее). В поле Name (Описание) введите описательное имя Web-узла, например Corporate WWW Server. Снова щелкните Next.
5. В списке IP Address selection (Введите IP-адрес для веб-узла) можно выбрать доступный IP-адрес (рис. 3-5). Щелкните All Unassigned (Значения не присвоены), чтобы узел мог использовать все не назначенные IP-адреса сервера. Одному IP-адресу может соответствовать несколько Web-узлов, при условии, что они используют разные номера портов или имена заголовков узлов.



**Рис. 3-5.** Мастер Web Site Creation Wizard (Мастер создания веб-узлов)

6. Номер TCP-порта Web-узла автоматически задается как 80. В поле TCP Port (TCP-порт) можно ввести новый но-



мер порта. **Одному номеру порта может соответствовать несколько Web-узлов, при условии, что они используют разные IP-адреса или имена заголовков узлов.**

7. Если вы собираетесь использовать заголовки узлов, введите в соответствующее поле имя заголовка узла. В частной сети заголовком узла может быть имя компьютера, например `EngIntranet`. В общедоступной сети заголовком узла должно быть DNS-имя, например `services.microsoft.com`. Имя заголовка узла всегда должно быть уникальным.
8. По умолчанию Web-серверы **используют** для протокола SSL порт 443. Если на сервере установлен SSL-сертификат (подробнее — в главе 6 этой книги), будет доступен протокол SSL, и вы сможете изменить его порт, введя соответствующий номер в поле SSL Port (Порт SSL). Несколько узлов могут использовать один и тот же SSL-порт, при условии, что они задействуют разные IP-адреса.
9. В следующем диалоговом окне можно **задать** домашний каталог Web-узла. Для поиска уже созданной папки щелкните Browse (Обзор). Папку можно создать, используя Windows Explorer (Проводник). Щелкните Next (Далее).



**Совет** Рекомендую создать корневую папку, в которой будут храниться домашние каталоги, и затем — отдельную вложенную папку для каждого узла. Можно использовать корневую папку по умолчанию — `C:\inetpub` и создать в ней вложенные папки `CorpWWW`, `CorpServices` и `CorpProducts`, где будут храниться файлы Web-узлов `www.microsoft.com`, `services.microsoft.com` и `products.microsoft.com` соответственно,

10. Чтобы создать **безопасный** или **частный** Web-узел, снимите флажок **Allow Anonymous Access To This Web Site** (Разрешить к веб-узлу анонимный доступ). По умолчанию к новым Web-узлам **разрешен анонимный** доступ, т. е. пользователи могут подключаться к ним, не проходя проверку подлинности.
11. Теперь можно задать разрешения доступа к Web-узлу (рис. 3-6). Стандартные разрешения позволяют:
  - **Read (чтение)** — считывать документы, например HTML-файлы;

- Run Scripts (запуск сценариев) — запускать сценарии, например ASP-файлы (Active Server Page) или сценарии на Perl;
- Execute (выполнение) — выполнять программы, например ISAPI-приложения или исполнимые файлы;
- Write (запись) — загружать файлы на узел, например с помощью Microsoft FrontPage;
- Browse (обзор) — просматривать содержимое папки, если для нее не определен файл по умолчанию.

Обычно узлу рекомендуется назначить только разрешения Read и Run Scripts.

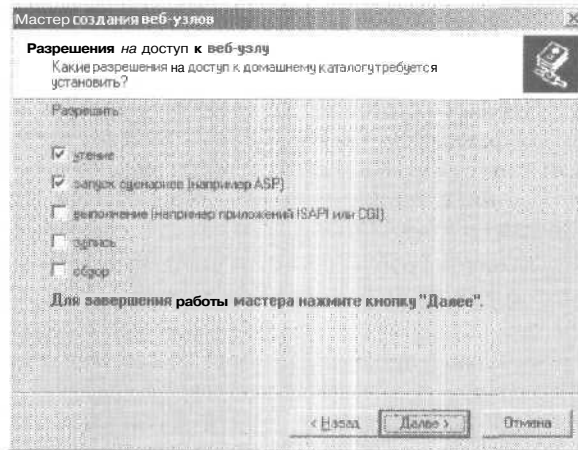


Рис. 3-6. Задание разрешений доступа к Web-узлу

12. Щелкните **Next** (Далее), и затем — **Finish** (Готово). Мастер создаст Web-узел, но не запустит его. Прежде чем запустить узел и предоставить к нему доступ, нужно завершить настройку его свойств.

## Управление свойствами Web-узла

Большинством свойств Web-узла можно управлять через диалоговое окно его свойств.

### Задание домашнего каталога узла

Любой развернутый на сервере Web-узел имеет домашний каталог — основную папку для всех его файлов, включая домашнюю страницу, связанную с другими страницами узла. Домашний каталог связан с доменным именем узла или именем сервера. Так, если DNS-имя узла — `www.microsoft.com` и домашний каталог — `C:\Inetpub\Wwwroot`, к файлам в домашнем каталоге узла браузеры будут обращаться по URL `http://www.microsoft.com/В` интрасети для доступа к документам в домашнем каталоге может применяться имя сервера. Так, если имя сервера — `CorpIntranet`, для обращения к файлам в домашнем каталоге узла браузеры будут использовать URL `http://CorpIntranet/`.

Чтобы просмотреть или изменить домашний каталог узла, сделайте так.

1. Запустите оснастку Internet Information Services и в левой панели раскройте узел нужного компьютера. Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2 этой книги.
2. Щелкните значок требуемого Web-узла правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
3. Перейдите на вкладку Home Directory (Домашний каталог) (рис. 3-7).
4. Если каталог находится на локальном компьютере, поставьте переключатель в положение A Directory Located On This Computer (каталог данного компьютера) и затем в поле Local Path (Локальный путь) введите путь к каталогу, например `C:\Inetpub\Wwwroot`. Для поиска каталога щелкните Browse (Обзор).
5. Если нужный каталог находится на другом компьютере и является сетевым ресурсом, поставьте переключатель в положение A Share Located On Another Computer (общая папка другого компьютера) и введите в поле Network Directory (Сетевой путь) UNC-путь к ресурсу. Путь должен иметь вид `\\ИмяСервера\ИмяРазделяемойПапки` например, `\\Gandolf\CorpWWW`. Затем щелкните Connect As

(Подключить как), введите имя пользователя и пароль для подключения к сетевому ресурсу.



**Примечание** Если имя пользователя и пароль опущены, пользователь Everyone (Все) должен обладать доступом к указанному сетевому ресурсу, иначе подключение к сетевому каталогу будет невозможно.

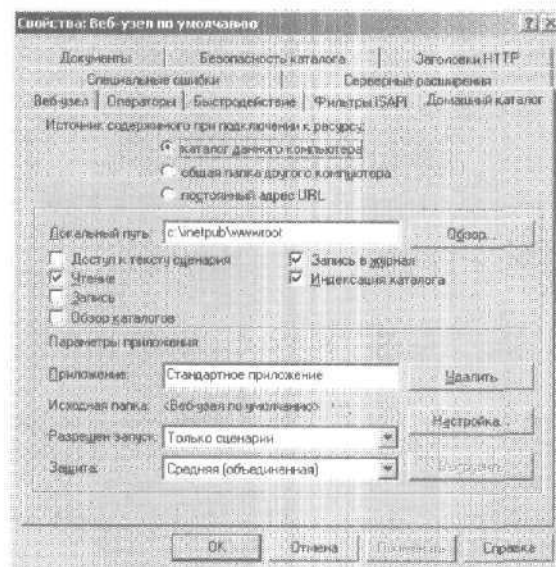


Рис. 3-7. Задание домашнего каталога узла

6. Для перенаправления пользователей к другому URL поставьте переключатель в положение A Redirection To A URL (постоянный адрес URL) и следуйте инструкциям раздела «Перенаправление запросов браузера» этой главы.
7. Щелкните OK.

### Изменение портов, IP-адреса и имени заголовка узла

Каждый Web-узел обладает уникальным идентификатором, состоящим из номера TCP-порта, номера SSL-порта, IP-адреса и заголовка узла. Номер TCP-порта по умолчанию – 80, SSL-порта — 443. В качестве IP-адреса по умолчанию используется любой доступный IP-адрес.

Чтобы изменить идентификатор Web-узла, сделайте следующее.

1. Если Web-узел будет использовать новый IP-адрес, его необходимо предварительно настроить. Подробнее — в главе 15 книги «Microsoft Windows 2000. Справочник администратора».
2. Запустите оснастку Internet Information Services и в левой панели раскройте узел нужного компьютера. Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2.
3. Щелкните значок Web-узла правой кнопкой и выберите в контекстном меню команду Properties (Свойства). Откроется одноименное диалоговое окно (рис. 3-8).

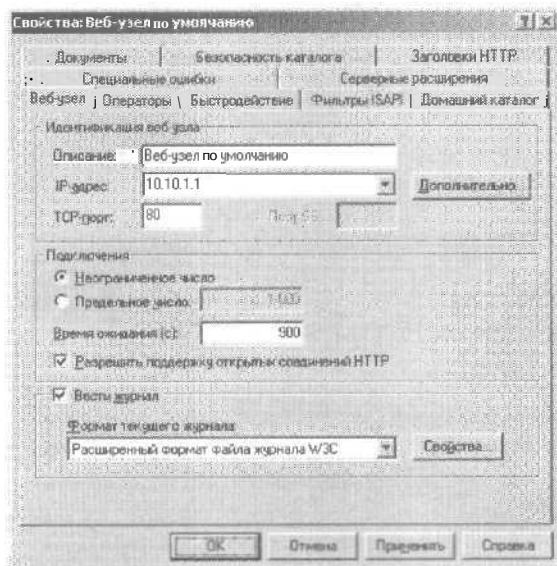


Рис. 3-8. Диалоговое окно свойств Web-узла

4. Поле Description (Описание) содержит описательное имя Web-узла, которое отображается в оснастке Internet Information Services и для других целей не используется. Чтобы изменить его, введите в поле Description новое имя.

5. В списке IP Address selection (IP-адрес) можно выбрать доступный IP-адрес. Щелкните (All Unassigned) [(Значения не присвоены)], чтобы узел мог использовать все неназначенные IP-адреса сервера. Одному IP-адресу может соответствовать несколько Web-узлов, при условии, что они используют разные номера портов или имена заголовков узлов.
6. Номер TCP-порта Web-узла автоматически задается как 80. В поле TCP Port (TCP-порт) можно ввести новый номер порта. Одному номеру порта может соответствовать несколько Web-узлов, при условии, что они используют разные IP-адреса или имена заголовков узлов.
7. Если вы собираетесь использовать заголовки узлов, введите в соответствующее поле имя заголовка узла. В частной сети заголовком узла может быть имя компьютера, например EngIntranet. В общедоступной сети заголовком узла должно быть DNS-имя, например, services.microsoft.com. Имя заголовка узла всегда должно быть уникальным.
8. По умолчанию Web-серверы используют для протокола SSL порт 443. Если на сервере установлен SSL-сертификат (подробнее — в главе 6 этой книги), доступен протокол SSL и вы вправе изменить его порт, введя требуемый номер в поле SSL Port (Порт SSL). Несколько узлов могут использовать один и тот же SSL-порт, при условии, что задействуют разные IP-адреса.
9. Щелкните ОК.

#### **Создание нескольких идентификаторов для одного Web-узла**

Ранее мы рассматривали способы размещения нескольких Web-узлов на одном сервере, уделяя основное внимание созданию уникального идентификатора для каждого узла. Но вам может понадобиться сопоставить один Web-узел нескольким доменным именам. Такой узел публикует одинаковое содержимое для различных групп пользователей. Допустим, в целях безопасности ваша фирма зарегистрировала в InterNIC доменные имена domain.com, domain.org и domain.net. Тогда, вместо того чтобы публиковать идентичное содержимое на нескольких узлах, разместите его

на одном узле, реагирующем на запросы к этим доменным именам.

Правила, предусматривающие уникальные комбинации портов, IP-адресов и заголовков, применяются и к узлам с несколькими идентификаторами. Таким образом, каждый идентификатор узла должен быть уникальным, т. е. включать уникальный IP-адрес, порт или заголовок узла.

Чтобы создать для одного Web-узла несколько идентификаторов, сделайте следующее.

1. Если Web-узел использует несколько IP-адресов, их необходимо предварительно настроить. Подробнее — в главе 15 книги «Microsoft Windows 2000. Справочник администратора».
2. **Запустите оснастку Internet Information Services** и в левой панели **раскройте** узел нужного **компьютера**. Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2.
3. Щелкните значок требуемого Web-узла правой кнопкой и выберите в контекстном меню команду Properties (Свойства). Откроется одноименное диалоговое окно (рис. 3-8).
4. На вкладке Web Site (Web-узел) щелкните Advanced (Дополнительно). Откроется диалоговое окно Advanced Multiple Web Site Configuration (Дополнительная настройка Web-узлов), в котором можно задать идентификаторы данного узла (рис. 3-9).
5. Кнопки группы Multiple Identities For This Web Site (Удостоверения данного веб-узла) позволяют:
  - Add (Добавить) — добавить новый идентификатор: щелкните ее, выберите требуемый IP-адрес, введите номер TCP-порта и укажите имя заголовка узла, щелкните ОК;
  - Edit (Изменить) — изменять выбранный идентификатор;
  - Remove (Удалить) — удалить выбранный идентификатор.
6. Группа Multiple SSL Identities For This Web Site (SSL удостоверения данного узла) позволяет управлять пара-

метрами портов. Чтобы добавить новую запись, щелкните Add (Добавить), изменить или удалить существующую — Edit (Изменить) или Remove (Удалить).

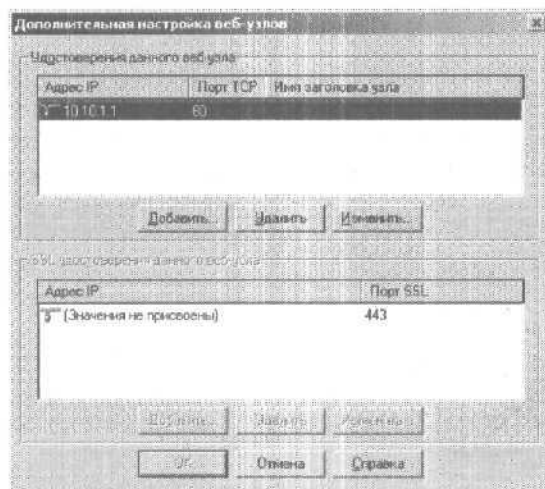


Рис. 3-9. Web-узел может иметь несколько идентификаторов

7. Дважды щелкните ОК, чтобы вернуться к оснастке Internet Information Services.

### Ограничение числа входящих подключений и изменение времени ожидания соединения

Для управления входящими подключениями Web-узла можно ограничить число параллельных подключений и задать время ожидания соединения.

Обычно Web-узел принимает неограниченное число подключений, и это оптимально для большинства сред. Одного при большом числе подключений производительность Web-узла может заметно снизиться, порой настолько, что к узлу невозможно обратиться. Во избежание этого администраторы ограничивают число параллельных подключений. Если узел просматривает максимально допустимое число клиентов, новым посетителям придется ждать, пока не отключится кто-нибудь. Подключенные же в данный момент посетители могут без проблем работать со страницами узла.



Когда время ожидания соединения истекает, сервер отключает простаивающий пользовательский сеанс. Для Web-узла по умолчанию время ожидания сеанса — 900 секунд (15 минут). Это гарантирует отсутствие открытых соединений, некорректно закрытых браузером.

Чтобы изменить допустимое число параллельных подключений или задать время ожидания соединения, сделайте следующее.

1. В оснастке Internet Information Services щелкните правой кнопкой значок требуемого компьютера и выберите в контекстном меню команду Properties (Свойства). Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2.
2. Щелкните нужный Web-узел правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
3. Чтобы снять ограничения на число подключений, поставьте переключатель в группе Connections (Подключения) в положение Unlimited (Неограниченное число). Чтобы ограничить число подключений к узлу, поставьте переключатель в положение Limit To Number Of Connections (Предельное число) и введите в соответствующее поле нужное значение.
4. В поле Connection Timeout (Время ожидания) задается время ожидания соединения. Если необходимо, введите новое значение.
5. Щелкните ОК.

#### Поддержка пакетов HTTP Keep-Alives

В оригинальной архитектуре протокола HTTP для загрузки нескольких файлов с Web-сервера открывается соответствующее число соединений. Соединение поддерживается открытым не дольше, чем необходимо, и по завершении транзакции перестает занимать системные ресурсы. Недостаток такой архитектуры — при запросе дополнительных данных клиенту приходится повторно открывать соединение, создавая дополнительный трафик и задержки.

Рассмотрим обычную Web-страницу, состоящую из основного HTML-документа и десяти изображений. При использо-

вании HTTP 1.0 клиент запрашивает каждый файл по отдельному соединению. Он подключается к серверу, запрашивает файл документа, получает ответ и отключается. Этот процесс повторяется для каждого изображения в документе. Web-серверы, совместимые с протоколом HTTP 1.1, поддерживают пакеты HTTP Keep-Alives, позволяющие клиентам поддерживать открытое соединение с Web-сервером, а не открывать его повторно для каждого запроса. По умолчанию на новых Web-узлах используются пакеты HTTP Keep-Alives, и обычно это дает клиентам заметный выигрыш в производительности. Но поддержка соединений требует системных ресурсов тем больше, чем больше соединений открыто. Во избежание падения производительности сервера из-за большого числа открытых соединений можно ограничить число параллельных подключений, уменьшить время ожидания соединения, или и то, и другое. Подробнее об управлении соединениями — в разделе «Ограничение числа входящих подключений и изменение времени ожидания соединения» этой главы.

Чтобы включить или отключить использование пакетов HTTP Keep-Alives, сделайте так.

1. В оснастке Internet Information Services щелкните значок требуемого компьютера правой кнопкой и выберите в контекстном меню команду Properties (Свойства). Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2.
2. Щелкните нужный Web-узел правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
3. Чтобы включить использование пакетов HTTP Keep-Alives, пометьте флажок HTTP Keep-Alives Enabled (Разрешить поддержку открытых соединений HTTP). Чтобы отключить — снимите его.
4. Щелкните ОК.

## Управление каталогами

Структура каталогов IIS основана преимущественно на файловой системе Windows 2000, но предоставляет пользователям расширенную функциональность и гибкость.

## Структура физических и виртуальных каталогов

В предыдущих разделах мы обсуждали домашние каталоги и их использование. Помимо домашних каталогов, Web-узлы на основе продуктов Microsoft также используют физические и виртуальные каталоги. Разница между ними очень важна. Физический каталог — это часть файловой системы, и чтобы к нему можно было обращаться через IIS, он должен находиться в домашнем каталоге узла. Виртуальный каталог может располагаться и вне домашнего каталога, но всегда доступен клиентам через псевдоним. Создавать и управлять физическими и виртуальными каталогами можно из оснастки Internet Information Services. Физическим каталогам соответствует обычный значок папки, а виртуальным каталогам — значок папки с глобусом в углу.

Для создания физического каталога нужно создать вложенную папку в домашнем каталоге узла. Обращаться к этим вложенным папкам можно, добавляя имя папки к DNS-имени Web-узла. Например, вы создали Web-узел с DNS-именем `products.microsoft.com`. Пользователи могут обращаться к нему с помощью URL `http://www.microsoft.com/`. Затем вы создали в домашнем каталоге папку `search`. Для доступа к ней нужен URL `http://www.microsoft.com/search/`.

Размещение файлов и папок содержимого в домашнем каталоге упрощает управление Web-узлом, но можно использовать и виртуальные каталоги — указатели на папки, расположенные вне домашнего каталога узла. Для доступа к виртуальному каталогу следует добавить его псевдоним к DNS-имени узла. Например, если домашний каталог узла — `D:\Inetpub\Wwwroot` и вы храните документы Microsoft Word в папке `E:\Worddocs`, можно создать виртуальный каталог, указывающий фактическое расположение этой папки. Если псевдоним папки `E:\Worddocs` — `docs`, посетители Web-узла `www.microsoft.com` смогут обратиться к ней при помощи URL `http://www.microsoft.com/docs/`.

### Создание физических каталогов

Вы упростите организацию документов узла, создав в его домашнем каталоге вложенные папки. Для этого сделайте так.

1. Раскройте меню Start\Programs\Accessories (Пуск\Программы\Стандартные) и выберите Windows Explorer (Проводник).
2. В левой панели щелкните домашний каталог нужного Web-узла.
3. В правой панели щелкните правой кнопкой и выберите в контекстном меню команду New\Folder (Создать\Папку). Система создаст новую папку и предложит вам изменить ее имя по умолчанию — New Folder (Новая папка).
4. Введите новое имя и нажмите клавишу Enter. Каталогам рекомендуется задавать краткие и информативные имена: например, Images, WodDocs или Downloads.



Совет Использовать пробелы в именах каталогов IIS не рекомендуется: официально они недопустимы в URL и должны заменяться управляющей последовательностью %20. В новых версиях браузеров реализована автоматическая замена пробелов кодом %20, но в старых версиях ее может не быть, и в результате пользователь не обратится к странице.

5. Новая папка наследует разрешения по умолчанию домашнего каталога и IIS-разрешения Web-узла. Подробнее о просмотре и изменении разрешений см. главу 5 этой книги.



Совет Оснастка Internet Information Services не отображает новые папки автоматически. Возможно, потребуется щелкнуть кнопку Refresh (Обновить) на панели инструментов.

### Создание виртуальных каталогов

Виртуальные каталоги создаются в два этапа. Сначала следует создать физическую папку (обычно вне домашнего каталога узла), затем виртуальный каталог, связанный с физической папкой. Виртуальный каталог создастся так.

1. Запустите оснастку Internet Information Services и в левой панели раскройте узел нужного компьютера. Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2.

2. Правой кнопкой щелкните нужный Web-узел и выберите в контекстном меню команду *New\Virtual Directory* (Создать\Виртуальный каталог). Запустится мастер Virtual Directory Creation Wizard (Мастер создания виртуальных каталогов). Щелкните Next (Далее).
3. В поле Alias (Псевдоним) введите имя для доступа к виртуальному каталогу. Рекомендуется сделать его кратким и информативным, как и имя обычной папки.
4. В следующем диалоговом окне задайте домашний каталог Web-узла. Для поиска уже созданной папки щелкните Browse (Обзор). При необходимости создайте папку с помощью Windows Explorer (Проводник).
5. Задайте разрешения на доступ к виртуальному каталогу. Обычно достаточно разрешений Read (Чтение) и Run Script (Запуск сценариев). Стандартные разрешения позволяют:
  - Read (чтение) — считывать документы: например, HTML-файлы;
  - Run Scripts (запуск сценариев) — запускать сценарии: например, ASP-файлы (Active Server Page) или сценарии на Perl;
  - Execute (выполнение) — выполнять программы: например, ISAPI-приложения или исполнимые файлы;
  - Write (запись) — загружать файлы на узел, например, с помощью Microsoft FrontPage;
  - Browse (обзор) — просматривать содержимое папки, если для нее не определен файл по умолчанию.
6. Щелкните Next (Далее) и затем — Finish (Готово). Система создаст виртуальный каталог.



**Примечание** По умолчанию новый виртуальный каталог создается как одноименное групповое приложение ISAPI. В связи с этим виртуальным каталогам соответствует значок с документом и глобусом. Подробнее о приложениях ISAPI см. главу 4 этой книги.

### Подключение IISAdmin, IISHelp и прочих системных каталогов

IISAdmin, IISHelp и другие системные каталоги служат для исполнения специфических задач. IISAdmin позволяет Web-операторам контролировать узел. IISHelp показывает вспомогательную документацию. По умолчанию эти каталоги не настроены для использования новым узлом, который вы создаете. Чтобы сделать их доступными, создайте виртуальный каталог, сопоставляющий псевдоним его физическому размещению.

1. Запустите оснастку Internet Information Services и в левой панели раскройте узел нужного компьютера. Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2.
2. Правой кнопкой щелкните нужный Web-узел и выберите в контекстном меню команду **New\Virtual Directory (Создать\Виртуальный каталог)**. Запустится мастер Virtual Directory Creation Wizard (Мастер создания виртуальных каталогов). Щелкните **Next (Далее)**.
3. В поле **Alias (Псевдоним)** введите имя для доступа к виртуальному каталогу: например, **IISAdmin**.
4. В следующем диалоговом окне можно указать путь к физической папке, где хранится содержимое узла. Для поиска нужной системной папки щелкните **Browse (Обзор)**. Каталог **IISHelp** по умолчанию находится в папке `%SystemRoot%\Help\Iishelp`, а каталог **IISAdmin** — в папке `%SystemRoot%\System32\Inetsrv\Iisadmin`.
5. Щелкните **Next (Далее)** и задайте разрешения на доступ. Каталогам **IISAdmin**, **IISHelp** и **IISamples** назначьте разрешения **Read (чтение)** и **Run Scripts (запуск сценариев)**, а каталогу **MSADC** — разрешения **Read (чтение)**, **Run Scripts (запуск сценариев)** и **Execute (выполнение)**.
6. Щелкните **Next (Далее)** и затем — **Finish (Готово)**. Виртуальный каталог создай и сопоставлен системному каталогу, на который ссылается.

### Изменение свойств каталогов

Параметры физических и виртуальных каталогов можно в любое время **изменить**. Разрешения и основные свойства каталога задаются в Windows Explorer (Проводник), разрешения и свойства IIS — в диалоговом окне свойств каталога. В оснастке Internet Information Services щелкните нужный каталог правой кнопкой и выберите в контекстном меню команду Properties (Свойства).

### Переименование каталогов

Физические и виртуальные каталоги можно **переименовать** с помощью оснастки Internet Information Services. При переименовании физического каталога изменяется фактическое имя папки в файловой системе, виртуального — только псевдоним каталога, имя соответствующей физической папки остается **неизменным**.

Чтобы переименовать физический или виртуальный каталог, сделайте так.

1. В оснастке Internet Information Services раскройте узел нужного Web-узла.
2. Щелкните каталог правой кнопкой и выберите в контекстном меню команду Rename (Переименовать).
3. Введите новое имя каталога и нажмите клавишу Enter.



**Внимание!** Браузеры хранят пути к файлам и каталогам в закладках. При изменении имени каталога любой ссылающийся на него URL становится **недействительным**, и пользователь, повторно обращающийся к странице, может столкнуться с ошибкой «404 — File Not Found». Чтобы этого не случилось, перенаправляйте запросы браузера к новым ресурсам (подробнее см. раздел «Перенаправление запросов браузера» этой главы).

### Удаление каталогов

Удалить физические и виртуальные каталоги можно из оснастки Internet Information Services. При удалении физического каталога он и его **содержимое** помещаются в Recycle Bin (Корзина). При удалении виртуального каталога удаляется только его псевдоним, содержимое **соответствующей** физической папки не затрагивается.

Чтобы удалить физический или виртуальный каталог, сделайте следующее.

1. В оснастке Internet Information Services раскройте узел нужного Web-узла.
2. Щелкните каталог правой кнопкой и выберите в контекстном меню команду **Delete** (Удалить). При запросе системы подтвердите свои действия, щелкнув **Yes** (Да).

## Управление Web-содержимым

Фактически опубликование документов на Web-узле представляет собой копирование файлов в домашние, вложенные и виртуальные каталоги. Документы наследуют свойства узла по умолчанию, а также разрешения по умолчанию папки Windows, в которой находятся. Эти свойства и разрешения можно изменять как для отдельных документов, так и для всех сразу.



**Внимание!** Как уже говорилось, браузеры хранят пути к файлам и каталогам в закладках. Во избежание ошибок, связанных с переименованием или удалением файлов, перенаправляйте запросы браузера к новым ресурсам (подробнее см. раздел «Перенаправление запросов браузера» этой главы).

### Открытие и просмотр файлов

Открывать файлы в браузере можно прямо из оснастки Internet Information Services. Щелкните нужный файл правой кнопкой и выберите в контекстном меню команду **Open** (Открыть). Файл будет открыт с использованием пути папки, например `D:\Inetpub\Wwwroot\DEFAULT.HTM`.

Большинство файлов открываются в браузере по умолчанию. Тем не менее, если запущен Web-узел и файл является .asp-документом или другим файлом динамического содержимого, система не откроет его. Чтобы просмотреть такой файл в Internet Explorer, щелкните файл правой кнопкой и выберите в контекстном меню команду **Browse** (Обзор документа).

### Изменение IIS-свойств файла

Свойства Web-файла можно в любое время изменить. Разрешения и основные свойства файла задают в Windows Explorer (Проводник), разрешения и свойства IIS — в диало-



говом окне свойств каталога. В оснастке Internet Information Services щелкните нужный файл правой кнопкой и выберите в контекстном меню команду Properties (Свойства).

#### Переименование каталогов

Переименовать файлы можно из оснастки Internet Information Services.

1. В оснастке Internet Information Services раскройте узел нужного Web-узла.
2. Щелкните требуемый файл правой кнопкой и выберите в контекстном меню команду Rename (Переименовать).
3. Введите новое имя файла и нажмите клавишу Enter.

#### Удаление файлов

Удалять файлы можно из оснастки Internet Information Services.

1. В оснастке Internet Information Services раскройте узел нужного Web-узла.
2. Щелкните требуемый файл правой кнопкой и выберите в контекстном меню команду Delete (Удалить). При запросе системы подтвердите свои действия, щелкнув Yes (Да).

#### Перенаправление запросов браузера

Перенаправление запросов — один из способов профилактики ошибок при переименовании или удалении содержимого Web-узла. Браузер можно перенаправить к файлам в другой папке, на другом Web-узле, на другом компьютере, а также к конкретному файлу вместо набора и для запуска ISAPI-приложения вместо обращения к запрашиваемым файлам.

Подробнее об этих способах перенаправления см. следующие разделы. Советы по созданию собственных процедур перенаправления см. в разделе «Изменение параметров перенаправления браузера» данной главы.

#### Перенаправление запросов к другим папкам или Web-узлам

Если вы переименовали или удалили папку, запросы к ее файлам можно перенаправлять к другой папке или Web-узлу. Когда браузер обращается к файлу по его старому адресу,

Web-сервер указывает ему запросить страницу по новому адресу. Для перенаправления запросов к другим каталогам или Web-узлам сделайте следующее.

1. В оснастке Internet Information Services щелкните значок (+) напротив соответствующего Web-узла.
2. Щелкните нужную папку правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
3. Перейдите соответственно на вкладку Virtual Directory (Виртуальный каталог) или Directory (Каталог) и поставьте переключатель в положение Redirection To A URL (постоянный адрес URL) (рис. 3-10).

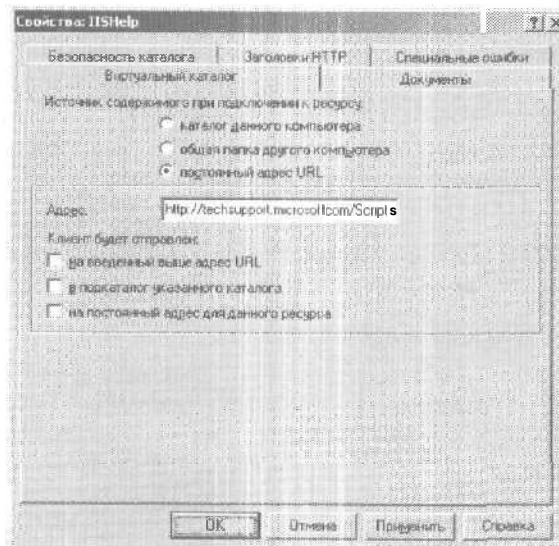


Рис. 3-Ю. Перенаправление запросов на файлы одной папки к другой

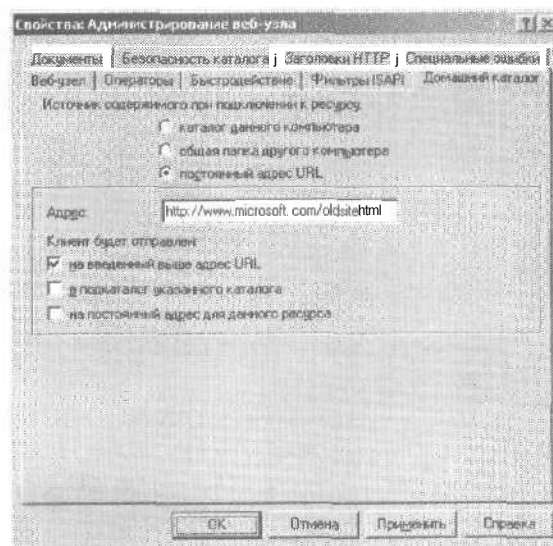
4. В поле Redirect To (Адрес) введите URL конечной папки или Web-узла. Например, для перенаправления всех запросов на файлы папки /Docs к папке /CorpDocs надо ввести /CorpDocs. Чтобы перенаправить все запросы на файлы папки [www.microsoft.com/Docs](http://www.microsoft.com/Docs) к папке [techsupport.microsoft.com/CorpDocs](http://techsupport.microsoft.com/CorpDocs), введите <http://techsupport.microsoft.com/CorpDocs>.

- Щелкните ОК. Теперь все запросы на файлы старой папки будут перенаправляться к новой. Так, если браузер запросил файл по адресу <http://www.microsoft.com/Docs/adminguide.doc> и вы перенаправляете все запросы на адрес <http://techsupport.microsoft.com/CorpDocs/>, браузер получит файл <http://techsupport.microsoft.com/CorpDocs/adminguide.doc>.

### Перенаправление всех запросов на другой Web-узел

Если вы закрыли существовавший Web-узел, и не хотите, чтобы при обращении к нему пользователи попадали в тупик, перенаправьте все запросы на файлы старого Web-узла к определенной странице нового. Для этого сделайте так.

- В оснастке Internet Information Services щелкните значок нужного Web-узла правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
- Перейдите на вкладку Home Directory (Домашний каталог) и поставьте переключатель в положение A Redirection To A URL (постоянный адрес URL) (рис. 3-11).



**Рис. 3-11.** Перенаправление всех запросов на файлы к определенной странице другого Web-узла

3. В поле Redirect To (Адрес) введите полный URL страницы нового узла, например *http://www.microsoft.com/oldsite.htm*.
4. Пометьте флажок The Exact URL Entered Above (на указанный выше адрес) и щелкните ОК. Теперь все запросы на файлы старого узла будут перенаправляться к заданной вами странице нового Web-узла.

### Получение файлов из сетевых папок

Службы IIS могут получать не только файлы, находящиеся на локальном жестком диске, но и файлы из сетевых папок. Чтобы сконфигурировать IIS для получения файлов из сетевых папок, сделайте следующее.

1. В оснастке Internet Information Services щелкните нужный Web-узел правой кнопкой и выберите в контекстном меню команду Properties (Свойства).

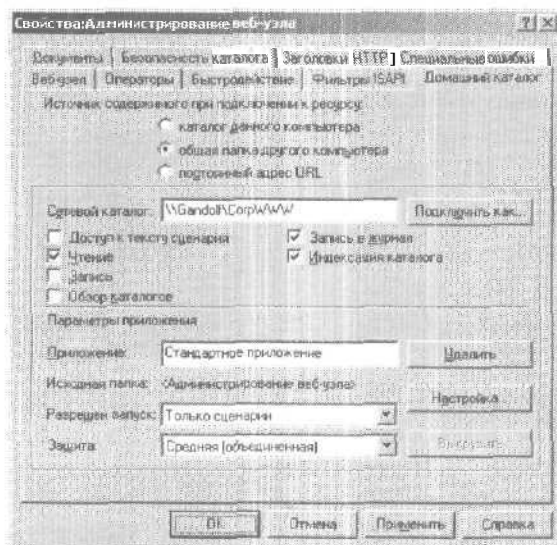


Рис. 3-12. Источником содержимого могут быть сетевые папки, подключаемые посредством перенаправления

2. Перейдите на вкладку Home Directory (Домашний каталог) и поставьте переключатель в положение A Share

Located On Another Computer (общая папка другого компьютера) (рис. 3-12).

3. В поле Network Directory (Сетевой каталог) введите UNC-путь к сетевой папке. Он должен иметь вид \\Имя-Сервера\ИмяСетевойПапки, например, \\Gandolf\Corp-WWW. Затем щелкните Connect As (Подключить как) и в открывшемся диалоговом окне введите имя пользователя и пароль для подключения к сетевой папке.
4. Щелкните ОК. Теперь все файловые запросы к Web-узлу будут перенаправлены на файлы другого сетевого ресурса.

### Перенаправление запросов приложениям

Все запросы на файлы конкретной папки (узла), а также параметры из URL можно перенаправлять специально созданному приложению.

1. В оснастке Internet Information Services щелкните нужный Web-узел правой кнопкой.
2. Щелкните папку правой кнопкой и выберите в контекстном меню команду Properties (Свойства). Для перенаправления всех запросов на файлы узла щелкните его значок правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
3. Перейдите соответственно на вкладку Home Directory (Домашний каталог), Virtual Directory (Виртуальный каталог) или Directory (Каталог) и поставьте переключатель в положение A Redirection To A URL (постоянный адрес URL).
4. В поле Redirection To (Адрес) введите URL приложения, включая все переменные, необходимые для передачи параметров программе. Например, /CorpApps/Login.exe?URL=\$V+PARAMS=\$P, где \$V и \$P - переменные перенаправления. Полный список переменных перенаправления см. в табл. 3-1.
5. Пометьте флажок The Exact URL Entered Above (на введенный выше адрес URL) и щелкните ОК. Теперь все запросы на файлы указанной папки будут перенаправляться приложению.

**Табл. 3-1.** Переменные перенаправления, используемые в IIS

Переменная	Описание	Пример
<b>\$S</b>	Перелает совпавший суффикс из запрошенного URL, сервер автоматически подставляет этот суффикс в конечный URL. Используется только совместно с другими переменными.	Если запросы на файлы папки /Corrapps перенаправляются к папке /Apps и исходный запрос — /Corrapps/LOGIN.EXE, суффиксом будет /LOGIN.EXE.
<b>\$P</b>	Передаёт параметры исходного URL, опуская знак вопроса, указывающий на начало строки запроса.	Если исходный URL — /Scripts/COUNT.ASP?valA=1&valB=2, в конечный URL добавляется строка valA=1&valB=2.
<b>\$Q</b>	Полностью передаёт строку запроса в конечный URL.	Если исходный URL — /Scripts/COUNT.ASP?valA=1&valB=2, в конечный URL добавляется строка ?valA=1&valB=2.
<b>\$V</b>	Передаёт запрошенный путь без имени сервера.	Если исходный URL — //Gandolf/Apps/COUNT.ASP, в конечный URL добавляется строка /Apps/COUNT.ASP.
<b>\$0-\$9</b>	Передаёт часть запрошенного URL, совпадающую с указанным шаблоном.	
<b>!</b>	Блокирует перенаправление запросов на определённую папку или файл.	

### Изменение параметров перенаправления браузера

Рассмотрим теперь дополнительные параметры перенаправления, доступные, если переключатель находится в положении **A Redirection To A URL (постоянный адрес URL)**. Ранее при этом в группе **The Client Will Be Sent To (Клиент будет отправлен)** становились доступны дополнительные параметры перенаправления. Вы не изменяли их, и все запросы на файлы старого узла автоматически перенаправля-

лись к новому. Между тем переключатели группы The Client Will Be Sent To (Клиент будет отправлен) позволяют следующее.

- **The Exact URL Entered Above (на введенный выше адрес URL)** — перенаправлять поступающие запросы по указанному URL, не добавляя каких-либо частей исходного URL. При этом все запросы на файлы старого узла или папки перенаправляются к одному файлу. Так, чтобы отсылать все запросы на каталог /Downloads к файлу DOWNLOAD.HTM из домашней папки нового узла, пометьте данный флажок и в поле Redirect To (Адрес) введите /DOWNLOAD.HTM.
- **A Directory Below This One (в подкаталог указанного каталога)** — перенаправлять запросы к родительской папке в дочернюю. Так, для перенаправления запросов на файлы родительской папки (обозначается косой чертой «/») к дочерней папке с именем /Current пометьте данный флажок и в поле Redirect To (Адрес) введите /Current.
- **A Permanent Redirection For This Resource (на постоянный адрес для данного ресурса)** — возвращать клиенту сообщение «301 — Permanent Redirect». Если данный флажок снят, перенаправление считается временным, и клиентскому браузеру возвращается сообщение «302 — Temporary Redirect». Некоторые браузеры могут на основе сообщения «301 — Permanent Redirect» изменять URL-страницы, хранящиеся в кэше или закладках.

Кроме того, для более точной настройки перенаправления можно задействовать соответствующие переменные (табл. 3-1). Переменные перенаправления позволяют передавать части исходного URL в конечный путь, а также блокировать перенаправление запросов на определенную папку или файл. Еще один способ перенаправления — использовать шаблоны, которые позволяют отсылать запросы на файлы конкретного типа к определенному файлу на новом узле. Так, шаблоны перенаправления позволяют отсылать запросы на любые .htm-файлы к файлу DEFAULT.HTM и запросы на любые .asp-файлы к файлу DEFAULT.ASP. Синтаксис шаблонов перенаправления таков:

```
*; *.EXT; FILENAME.EXT[; *.EXT; FILENAME.EXT...]
```

Здесь *.EXT* — расширение файлов, запросы к которым требуется перенаправлять, а *FILENAME.EXT* — имя файла, к которому шаблоны отсылаются. Конечный URL нужно начинать со звездочки и точки с запятой; пары «шаблон — конечный URL» разделяются точками с запятой. Убедитесь, что указаны все типы документов, к которым может напрямую обратиться пользователь: например, *.htm*, *.html* и *.asp*. **Вы можете использовать шаблоны перенаправления, сделав следующее.**

1. В оснастке Internet Information Services щелкните нужный Web-узел правой кнопкой.
2. Щелкните папку правой кнопкой и выберите в контекстном меню команду Properties (Свойства). Для перенаправления всех запросов на файлы узла щелкните его значок правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
3. Перейдите соответственно на вкладку Home Directory (Домашний каталог), Virtual Directory (Виртуальный каталог) или Directory (Каталог) и щелкните A Redirection To A URL (постоянный адрес URL).
4. В поле Redirection To (Адрес) введите шаблоны перенаправления. Например, для перенаправления запросов на любые *.htm*-файлы к файлу *DEFAULT.HTM* и запросов на любые *.asp*-файлы к файлу *DEFAULT.ASP* введите:  
`*;*.htm;DEFAULT.HTM;*.*.asp;DEFAULT.ASP`
5. Поставьте флажок The Exact URL Entered Above (на указанный выше адрес) и щелкните ОК. Теперь все запросы на файлы папки или узла будут по возможности перенаправляться с использованием шаблонов.



## Глава 4

# Настройка Internet Information Services

Службы IIS предоставляют среду с широкими возможностями для разработки пользовательских приложений. Чтобы управлять такими приложениями, Web-администратор должен хорошо ориентироваться в этой среде. Функциональность таких приложений основана преимущественно на интерфейсе ISAPI.

Можно *настраивать* и другие компоненты IIS. Технология Microsoft Active Server Pages позволяет создавать пользовательские приложения, изолированные от внешних процессов. Пользовательские фильтры ISAPI позволяют изменить функциональность IIS и добавить новые возможности, например поддержку Java Servlet Pages. Можно также создавать пользовательские заголовки, сообщения об ошибках и типы MIME, разрабатывать узлы обновлений, страницы переходов и т. д.

### Основы использования приложений IIS

Интерфейсы ISAPI расширяют функциональность IIS. Это своеобразная надстройка над IIS, которую вы вправе дополнять приложениями ISAPI, ASP-приложениями и расширениями сторонних производителей (рис. 4-1). Мы подробно рассмотрим ASP- и ISAPI-приложения. Расширения IIS сторонних производителей работают почти так же, как приложения ISAPI, и потому отдельно останавливаться на них мы не будем.

#### Приложения ISAPI

Приложения ISAPI делятся на две категории: фильтры и расширения. И те, и другие изменяют функциональность IIS.



Рис. 4-1. Архитектура Web-приложения в IIS

Фильтры ISAPI — это динамически подключаемые библиотеки (DLL) или исполнимые файлы, загружаемые в память при запуске службы World Wide Web Publishing Service (Служба веб-публикаций) и остающиеся там до завершения работы IIS-сервера. Фильтры ISAPI активизируются при наступлении на IIS-сервере определенных событий. Например, можно создать фильтр, который при наступлении события Read заносит тип клиентского браузера в базу данных. Фильтры ISAPI могут применяться глобально или локально. Глобальные фильтры влияют на все Web-узлы IIS и загружаются в память при запуске World Wide Web Publishing Service. После добавления нового или изменения параметров существующего глобального фильтра World Wide Web Publishing Service требуется остановить и перезапустить. Локальные фильтры влияют на отдельный Web-узел IIS и могут при их добавлении или изменении динамически загружаться в память, при условии, что запущены World Wide Web Publishing Service и Web-узел.

Если для реакции на одно событие сконфигурировано несколько фильтров, они выполняются по очереди. Для управления последовательностью выполнения фильтрам назначаются приоритеты. Первыми выполняются фильтры с самым высоким приоритетом. При одинаковом приоритете сначала

ла выполняются фильтры глобального уровня, заданные в основных свойствах WWW-службы, затем — фильтры уровня узла, определенные в свойствах Web-узла. Фильтры одного уровня с одинаковым приоритетом выполняются в порядке загрузки в память. При возникновении конфликтов порядок загрузки фильтров в память можно изменить.

Расширения ISAPI — это тоже динамически подключаемые библиотеки (DLL) или исполнимые файлы. В отличие от фильтров, загружаемых при запуске World Wide Web Publishing Service, расширения ISAPI загружаются по требованию и выполняются в ответ на запрос клиента. Обычно ISAPI-расширения применяются для обработки данных, полученных в результате запроса на определенный тип файла. Например, если клиент запрашивает .asp-файл, IIS с помощью расширения ISAPI под названием ASP.DLL обрабатывает содержимое ASP-страницы и возвращает результаты клиенту.

Одновременно с IIS устанавливается множество стандартных расширений ISAPI, которые сконфигурированы для реакции на HTTP-запросы конкретного типа или на любые HTTP-запросы, требующие возврата файла с определенным расширением. Вот основные типы HTTP-запросов:

- **DELETE** — на удаление ресурса, обычно выполняется пользователями, обладающими на данном Web-узле специальными разрешениями;
- **GET** — на обращение к ресурсу (стандартный запрос для получения файлов);
- **HEAD** — на получение HTTP-заголовка, ответ не содержит тела сообщения;
- **OPTIONS** — на получение сведений о параметрах связи;
- **POST** — на передачу информации в виде подчиненного объекта данного ресурса, обычно используется для отправки данных формы;
- **PUT** — на сохранение прилагающихся данных с указанным идентификатором ресурса, обычно используется при загрузке файлов по протоколу HTTP;
- **TRACE** — на отслеживание передачи данных клиентом, используется в целях тестирования и отладки.

Расширения ISAPI загружаются по требованию, и поэтому их можно добавлять в любое время без перезагрузки IIS.

И все же, чтобы изменения параметров уже загруженного в память расширения ISAPI вступили в силу, нужно остановить и перезапустить World Wide Web Publishing Service. Как и в случае с фильтрами ISAPI, контекст расширений ISAPI может быть глобальным и локальным. Расширения ISAPI, заданные в основных свойствах WWW-службы, доступны всем Web-узлам сервера, а указанные в окне свойств конкретного узла — только данному узлу.

У расширений ISAPI нет приоритетов, и поэтому настраивать несколько расширений для обработки однотипного содержимого не следует. Кроме того, расширения ISAPI всегда выполняются в одном процессе сервера — используемом IIS, групповом для нескольких приложений или изолированном.

### ASP-приложения

ASP — это серверная среда обработки сценариев, предназначенная для создания динамических Web-приложений. ASP-приложение представляет собой набор логически сгруппированных файлов ресурсов и компонентов. Логическая группировка позволяет службам IIS совместно использовать данные в приложении и запускать приложение в разделяемом, групповом или изолированном процессе. На одном Web-узле может быть несколько приложений с разными параметрами.

К файлам ресурсов IIS относятся ASP- и HTML-страницы, изображения в форматах GIF и JPEG, а также прочие Web-документы. ASP-страница — это файл с расширением .asp, включающий HTML-код, комбинацию HTML-кода и сценариев или только сценарии. Сценарии ASP-страниц обрабатываются или клиентским браузером, или сервером. Последние называются серверными сценариями и могут быть написаны на Visual Basic Scripting Edition (VBScript), JScript или любом другом языке сценариев, поддерживаемом сервером.

ASP предоставляет разработчикам объектно-ориентированную среду сценариев. Для выполнения распространенных задач, таких как слежение за состоянием сеанса, обработка ошибок, чтение передаваемых клиентами HTTP-запросов, серверные сценарии используют встроенные объекты ASP. Вот полный список этих объектов:

- **Application** обеспечивает обмен информацией между всеми пользователями ASP-приложения;
- **ASPError** отслеживает сведения об условиях возникновения ошибок сценариев в ASP-страницах;
- **ObjectContext** поддерживает сведения об экземплярах компонента приложения и предоставляет доступ к встроенным объектам ASP, а также методы и события для подтверждения и прерывания транзакции;
- **Request** получает значения, переданные в HTTP-запросе клиентским браузером;
- **Response** передает HTTP-ответ клиентскому браузеру;
- **ScriptingContext** предоставляет доступ к встроенным объектам (поддерживается только для обратной совместимости, вместо этого объекта рекомендуется использовать ObjectContext);
- **Server** используется для выполнения серверных задач, таких как выполнение файлов, передача сведений о состоянии сеанса другой ASP-странице и создание экземпляров серверных компонентов;
- **Session** хранит сведения о сеансе конкретного пользователя (при условии, что у клиентского браузера имеется и включена поддержка файлов cookie).

В ASP-сценариях также могут использоваться IIS-компоненты — исполнимые программы, взаимодействующие с IIS при помощи служб Component Services (Службы компонентов) и технологии COM. Стандартная установка IIS включает несколько встроенных компонентов, которые можно применять в ASP-приложениях. Они размещаются в папке %SystemRoot%\Inetsrv IIS-сервера, и, если удалить их отсюда, ASP-приложения не смогут работать с ними. Вот эти компоненты:

- **Ad Rotator (ADROT.DLL)** выводит на Web-страницах рекламные баннеры по заданному расписанию;
- **Browser Capabilities (BROWSERCAP.DLL)** определяет возможности, тип и версию браузеров, обращающихся к Web-узлу;
- **Content Linking (NEXTLINK.DLL)** генерирует оглавление Web-страницы, а также создает ссылки для перекода к предыдущей или последующей странице;

- **Content Rotator (CONTROT.DLL)** меняет HTML-содержимое Web-страницы по заданному расписанию;
- **Counters (COUNTERS.DLL)** создает счетчик обращений к Web-узлу и отдельным страницам;
- **Database Access (MSADO20.DLL)** при помощи ActiveX Data Objects обеспечивает доступ к БД и структурированным файлам данных;
- **File Access Component (FSCFG.DLL)** взаимодействует с объектом FileSystemObject библиотеки SCRRUN.DLL, позволяющим управлять объектами файловой системы;
- **Logging Utility (LOGSCRIPT.DLL)** позволяет приложениям считывать журналы HTTP-активности, генерируемые IIS;
- **MyInfo (MYINFO.DLL)** отслеживает личную информацию об узле и его разработчике;
- **Page Counter (PAGECNT.DLL)** ведет и отображает счетчик посещений Web-страницы;
- **Permission Checker (PERMCHK.DLL)** на основе протоколов проверки подлинности, используемых IIS, определяет наличие у клиента разрешений на чтение файла;
- **Status (STATUS.DLL)** возвращает сведения о состоянии сервера Personal Web Server for Macintosh;
- **Tools (TOOLS.DLL)** предоставляет функции для проверки наличия файлов, установления принадлежности сайта, поиска подключаемых модулей (только на компьютерах Macintosh), обработки данных HTML-форм и генерации случайных целых чисел.

### Создание пользовательских приложений

Создавать пользовательские приложения поможет оснастка IIS, а управлять COM-компонентами — оснастка Component Services (Службы компонентов). В процессе установки IIS на Web-узлах создаются стандартные приложения, позволяющие запускать пользовательские программы без изменения параметров рабочей среды. Например, можно скопировать ASP-файлы в базовую папку узла и затем запускать их, не создавая отдельного приложения. В этом случае созданное вами ASF-приложение будет выполняться в контексте стандартного.



**Совет** Зачастую начинающие администраторы удаляют приложение по умолчанию, не понимая его назначения, а потом удивляются странному поведению других приложений. Например, не удастся обмениваться сведениями о состоянии сеанса между ASP-страницами. А дело в том, что ASP-приложения и прочие файлы, использовавшие приложение по умолчанию, потеряли его контекст и, как следствие, все связанные параметры приложения.

Приложение по умолчанию позволяет запускать приложения IIS независимо от их расположения в структуре папок узла, если у этих папок имеются соответствующие разрешения на выполнение [Scripts Only (Только сценарии) или Scripts And Executables (Сценарии и исполняемые файлы)]. Чтобы удалить приложение по умолчанию, создайте для всех приложений, которые собираетесь использовать, специфические контексты.

Для тонкого управления назначьте основным приложениям отдельные контексты, т. е. настройте основные и дополнительные параметры приложения. Вот основные параметры:

- **Application Name (Приложение)** — описательное имя приложения;
- **Starting Point (Исходная папка)** задает основной каталог приложения, все его файлы и вложенные папки считаются частью приложения;
- **Execute Permissions (Разрешен запуск)** задает разрешенный уровень выполнения приложения;
- **Application Protection (Защита)** определяет, как выполняется приложение и какие ресурсы оно использует совместно с IIS и другими программами.

Дополнительные параметры:

- **Application Mappings (Отображение приложений)** определяет параметры кэширования приложения и сопоставляет расширения файлов DLL-библиотекам;
- **Application Options (Параметры приложений)** определяет порядок выполнения приложения, включая время ожидания, буферизацию и язык сценариев по умолчанию;
- **Application Debugging (Отладка приложений)** управляет отладкой и выводом сообщений об ошибках сценариев.

Настроечные параметры создают контекст, в котором выполняется приложение. При отсутствии контекста пользовательские страницы выполняются как отдельные файлы и не могут задействовать основные функции IIS, включая буферизацию, состояние сеанса и кэширование. Контекст приложения определяется на уровне папки. Все файлы и вложенные папки основного каталога приложения считаются частью приложения. Поэтому для создания приложения рекомендуется сделать так.

1. В Windows Explorer (Проводник) создайте папку, которая станет начальной точкой приложения, и назначьте ей соответствующие разрешения доступа Windows.
2. При необходимости из оснастки IIS создайте виртуальный каталог и сопоставьте его созданной папке.
3. Настройте для папки параметры приложения в соответствии с инструкциями раздела «Создание групповых и негрупповых приложений» этой главы.

### Использование и выполнение приложений

У каждого приложения есть начальная точка, которая задает его логическое пространство имен, т. е. определяет относящиеся к приложению файлы и папки. Все файлы и папки в начальной точке считаются частью приложения.

Начальную точку приложения можно определить для всего узла, для папки или для виртуального каталога. Если вы создаете приложение уровня узла, все файлы во всех вложенных папках Web-сайта будут считаться его частью. При создании приложения уровня обычного или виртуального каталога его частью будут считаться все файлы во всех вложенных папках данного каталога.

Как уже говорилось, начальная точка приложения задает его пространство имен — метод привязки области памяти к легко запоминаемому имени, объединяющему группу файлов и компонентов. Область памяти приложения определяет параметры его защиты. Перечислю возможные варианты.

- Low (Низкая) — приложения с низким уровнем защиты, выполняются в процессе и разделяют ресурсы с IIS. Это обеспечивает максимальную производительность, но позволяет приложению-вирусу аварийно завершить работу IIS.



- **Medium** (Средняя) — приложения со средним уровнем защиты, выполняются в групповом процессе, т. е. используют один и тот же процесс, отличный от обычных ресурсов IIS. Отказ одного приложения повлияет на работу других приложений со средним уровнем защиты, но не нарушит работу IIS.
- **High** (Высокая) — приложения с высоким уровнем защиты, выполняются полностью вне процесса. Они не разделяют какие-либо процессы, и их отказ не влияет на другие программы.

При использовании среднего и **высокого** уровней защиты IIS может изолировать приложение в отдельный процесс, что позволяет защитить World Wide Web Publishing Service от сбоев, ведущих к аварийному завершению работы или зависанию Web-сервера. Кроме того, изоляция процесса позволяет автоматически перезагружать приложения и завершать их процессы в случае фатальной ошибки.

Параметры защиты приложений влияют на доступ к памяти. Приложения, выполняющиеся в одном процессе с IIS, используют одну область памяти и могут вызывать друг друга, практически не создавая нагрузки. Изолированным приложениям и приложениям, выполняющимся в групповом процессе, для выполнения запросов между процессами приходится прибегать к маршалингу. Маршалинг необходим для любого взаимодействия приложения со службами IIS или другими приложениями. Маршалированные вызовы выполняются медленнее, чем вызовы в пределах одного процесса, и поэтому производительность изолированных и групповых приложений ниже производительности приложений, разделяющих один процесс IIS.

Внепроцессные приложения и компоненты, включая расширения ISAPI, по умолчанию не имеют доступа к свойствам метабазы, что предотвращает несанкционированное изменение последних. Чтобы предоставить внепроцессным приложениям доступ к метабазе, измените реквизиты контекста внепроцессного приложения на конкретную учетную запись пользователя и назначьте ей разрешения на доступ к метабазе.



**Совет** Задать параметры проверки подлинности для компонентов приложения можно из оснастки Component Services: запустив ее, раскройте узел Component Services\Computers\My Computer\COM+ Applications (Службы компонентов\Компьютеры\My Computer\Приложения COM+). Затем щелкните правой кнопкой значок IIS Out-Of-Process Pooled Applications, выберите в контекстном меню команду Properties (Свойства) и перейдите на вкладку Identity (Удостоверение). Учетная запись пользователя, назначаемая приложению, должна обладать нужными разрешениями на доступ к метабазе. Чтобы просмотреть разрешения файловой системы, щелкните в Windows Explorer (Проводник) файл метабазы (Inetsrv\METABASE.BIN) правой кнопкой, выберите в контекстном меню команду Properties и перейдите на вкладку Security (Безопасность).

Сопоставления позволяют указать доступные приложениям CGI-программы и расширения ISAPI. Web-узел наследует сопоставления от основных свойств WWW-службы при своем создании. Папка наследует сопоставления от свойств узла, после того, как она создана и доступна службам IIS. Любое сопоставление приложения состоит из трех частей.

- **Extension** (Расширение) — расширение файла, сопоставленное расширению ISAPI или CGI-программе. Не обязательно должно быть зарегистрировано в ОС и может включать более трех символов.
- **Executable Path** (Путь к исполняемому файлу) — путь к расширению ISAPI или CGI-программе. IIS на основе пути определяют, какое расширение ISAPI или CGI-программу следует загрузить. Соответствующая DLL-библиотека или EXE-файл должны находиться в папке, доступной IIS. Обычно это папки %SystemRoot% или %SystemRoot%\Inetsrv.
- **Verbs** (Команды) — типы HTTP-запросов, используемые расширением ISAPI или CGI-программой (подробный список типов HTTP-запросов — в разделе «Приложения ISAPI» этой главы).

Получив запрос на файл с определенным расширением, IIS динамически загружают в память соответствующее расширение ISAPI или CGI-программу и по завершении обработ-

ки выгружают их. Если разрешить кэширование приложений, службы IIS будут хранить загруженную DLL-библиотеку или исполняемый файл в памяти.

Параметры кэширования и защиты приложения определяют порядок использования ОЗУ IIS-сервера. При запуске новых приложений и загрузке новых программ в память ОС подвергается дополнительной нагрузке, размер которой зависит от настроечных параметров приложений. В качестве примера рассмотрим следующую ситуацию.

На IIS-сервере — три Web-узла (корпоративный, служебный и административный) и SMTP-сервер. В обычной конфигурации на сервере выполняются следующие процессы IIS:

- **INETINFO.EXE** управляет обработчиками служб и приложениями ISAPI, выполняющимися в контексте процесса IIS;
- **SVCHOST.EXE** — эти три процесса управляют Web- и SMTP-ресурсами и собственно установкой IIS;
- **DLLHOST.EXE** управляет процессами IIS (а также всеми запущенными приложениями, выполняющимися в групповом или отдельном процессе), изначально на сервере нет приложений, выполняющихся вне процесса или в групповом процессе.

Эти основные процессы занимают 27 848 Кб ОЗУ сервера (табл. 4-1). Чтобы продемонстрировать, как обработка приложений влияет на сервер, я создал дополнительные приложения, выполняющиеся:

- групповое приложение 1 — со средним уровнем защиты;
- групповое приложение 2 — со средним уровнем защиты;
- изолированное приложение 1 — с высоким уровнем защиты;
- изолированное приложение 2 — с высоким уровнем защиты.

Создание приложений с отличием от их запуска практически не влияет на занимаемый объем памяти. При запуске группового приложения 1, выполняющегося в групповом процессе, создается новый процесс DLLHOST.EXE, и занимаемый объем ОЗУ увеличивается до 34 109 Кб. Этот дополнительный процесс DLLHOST.EXE будет использоваться

для управления всеми приложениями такого типа, так что при запуске группового приложения 2 новый процесс не создается и занимаемый объем ОЗУ растет незначительно.

**Табл. 4-1.** Нагрузка на IIS-сервер, создаваемая приложениями

Процесс	Основные процессы IIS	Используется			
		Групповое Изолиро- ванное прило- жение 1	Групповое Изолиро- ванное прило- жение 2	Групповое Изолиро- ванное прило- жение 1	Групповое Изолиро- ванное прило- жение 2
INETINFO.EXE	7568	8360	8388	8440	8472
DLLHOST.EXE	4968	4968	4968	4960	4960
DLLHOST.EXE	—	5436	5492	5080	5080
DLLHOST.EXE	—	—	—	5460	5460
DLLHOST.EXE	—	—	—	—	5248
SVCHOST.EXE	3060	3080	3080	3084	3100
SVCHOST.EXE	9908	9920	9920	9920	9920
SVCHOST.EXE	2344	2344	2344	2344	2344
Занимаемый объем памяти, Кб	27848	34109	34194	39289	44586

А вот при каждом запуске нового изолированного приложения создается новый процесс DLLHOST.EXE, и занимаемый объем памяти заметно растет. При запуске изолированного приложения 1 создается третий процесс DLLHOST.EXE, и используемый объем ОЗУ вырастает до 39 289 Кб. При запуске изолированного приложения 2 создается четвертый процесс DLLHOST.EXE, и используемый объем памяти достигает 44 586 Кб.

В нашем примере каждый обслуживающий процесс DLLHOST.EXE использует около 5 000 Кб памяти, и IIS в целом занимает примерно 45 000 Кб ОЗУ сервера. Хотя это и не много, более сложные приложения могут задействовать гораздо больший объем памяти, особенно загружаемые в память дополнительные расширения ISAPI и CGI-программы. Кроме того, серверы кэшируют Web-документы, и часть ОЗУ всегда резервируется под файловый кэш.

## Управление пользовательскими приложениями IIS

Для создания и управления пользовательскими приложениями IIS служит диалоговое окно свойств Web-узла. При установке IIS на всех стандартных Web-узлах создается приложение по умолчанию, начальной точкой которого является корневой каталог Web-узла. Приложения по умолчанию позволяют создавать пользовательские приложения, в которых применяются стандартные параметры настройки. Изменять при этом какие-либо характеристики рабочей среды не нужно. Для более тонкого управления можно создавать приложения с более узкой областью действия.

### Создание групповых и негрупповых приложений

IIS приложения — это набор файлов ресурсов и компонентов, сгруппированных вместе для использования таких основных функций IIS, как буферизация, состояние сеанса и кэширование. Чтобы создать приложение IIS, сделайте так.

1. В оснастке IIS щелкните правой кнопкой папку, которая станет начальной точкой приложения, и выберите в контекстном меню команду Properties (Свойства). Затем перейдите на вкладку Home Directory (Домашний каталог), Directory (Каталог) или Virtual Directory (Виртуальный каталог). Откроется диалоговое окно свойств Web-узла (рис. 4-2).
2. Поля группы Application Settings (Параметры приложения) позволяют сконфигурировать приложение. Если поля Application Name (Приложение) и Application Protection (Защита) выделены серым цветом, значит, данный каталог уже используется в контексте другого приложения. Это нормально, и вы по-прежнему можете создать свое приложение. И все же помните, что при этом вы удалите данный каталог и все его вложенные папки из контекста текущего приложения.
3. Для создания приложения щелкните Create (Создать). При необходимости удалите приложение по умолчанию, щелкнув Remove (Удалить).
4. В поле Application Name (Приложение) задается описательное имя приложения, по умолчанию соответствующее

щес имени каталога. Вы можете ввести любое подходящее имя,

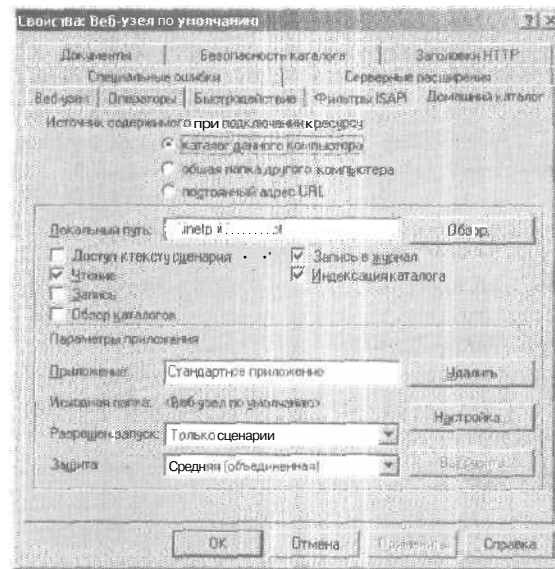


Рис. 4-2. Диалоговое окно свойств Web-узла

5. Список Execute Permission (Разрешен запуск) позволяет задать уровень выполнения приложения:
  - None (Нет) — доступ только к статичным файлам, например, HTML- и GIF-;
  - **Scripts Only** (Только сценарии) — выполняются только сценарии, например ASP-сценарии;
  - **Scripts And Executables** (Сценарии и исполняемые файлы) — просмотр и выполнение всех файлов.
6. Список Application Protection (Защита) позволяет задать область памяти, занимаемую приложением:
  - **Low (IIS Process)** [Низкая (процесс IIS)] — приложения с низким уровнем защиты выполняются в одном экземпляре процесса и разделяют ресурсы с IIS;
  - **Medium (Pooled)** [Средняя (объединенная)] — приложения со средним уровнем защиты выполняются в

групповом процессе, т. е. используют один и тот же процесс, отличный от обычных ресурсов IIS;

- **High (Isolated)** [Высокая (изолированная)] — приложения с высоким уровнем защиты выполняются полностью вне процесса: они не разделяют какие-либо процессы, и их отказ не влияет на другие программы.
7. Щелкните **Apply (Применить)**, чтобы создать приложение. Для настройки дополнительных параметров щелкните **Configuration (Настройка)**.

### Настройка сопоставлений и кэширования

Сопоставления приложений и параметры кэширования определяют, какие компоненты доступны IIS-приложениям и как они организованы в памяти. Для управления сопоставлениями и кэшированием служит вкладка Application Mappings (Отображение приложений) диалогового окна Application Configuration (Настройка приложения) (рис. 4-3).



**Рис. 4-3.** Вкладка Application Mappings (Отображение приложений) диалогового окна Application Configuration (Настройка приложения)

Чтобы открыть ее, сделайте следующее.

1. В оснастке IIS щелкните правой кнопкой папку, являющуюся начальной точкой приложения, и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите соответственно на вкладку Home Directory (Домашний каталог), Directory (Каталог) или Virtual Directory (Виртуальный каталог) и щелкните Configuration (Настройка).
3. Чтобы включить кэширование приложений, пометьте флажок Cache ISAPI Applications (Помещать приложения ISAPI в кэш), чтобы отключить — снимите его.



Примечание Кэширование приложений рекомендуется применять во всех случаях, кроме отладки, или устранения проблем, или когда требуется принудительная перезагрузка компонентов, используемых службами IIS.

4. В группе Application Mappings (Сопоставление приложений) отображаются текущие сопоставления расширений ISAPI и CGI-программ. Все сопоставления включают расширение файла, путь к исполняемому файлу и перечень действий.

#### Добавление сопоставлений приложения

Сопоставление приложения добавляется так.

1. На вкладке App Mappings (Отображение приложений) окна свойств приложения щелкните Add (Добавить). Откроется диалоговое окно Add/Edit Application Extension Mapping (Добавление или изменение сопоставления расширений) (рис. 4-4).
2. В текстовое поле Executable (Исполняемый файл) введите путь к требуемому расширению ISAPI или CGI-программе. Путь должен оканчиваться на .EXE или .DLL, например C:\Windows\System32\Inetsrv\ASP.DLL. Если путь неизвестен, щелкните Browse (Обзор) и выберите нужный файл в диалоговом окне Open (Открыть).



Примечание DLL-библиотека или исполняемый файл должны находиться на локальном жестком диске. Обычно они располагаются в папке %SystemRoot% или %SystemRoot%\Inetsrv.



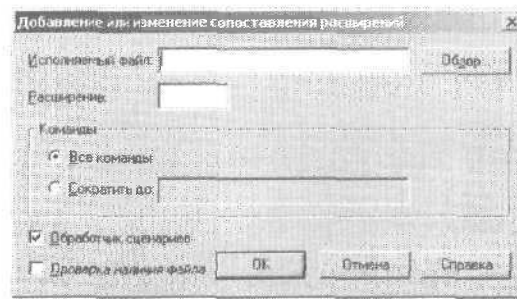


Рис. 4-4. Диалоговое окно Add/Edit Application Extension Mapping (Добавление или изменение сопоставления расширений)

3. В поле Extension (Расширение) введите расширение имени файла, которое нужно связать с расширением ISAPI или CGI-программой. Не забудьте указать перед расширением точку (.), например .HTML.



**Совет** Чтобы расширение ISAPI или CGI-программа обрабатывала запросы ко всем типам файлов, введите в поле Extension звездочку (\*). При этом файловые запросы в пределах данного приложения будут передаваться указанному компоненту, независимо от расширения файла. Помните также, что файловые запросы должны соответствовать параметрам, заданным в группе Verbs.

4. В группе Verbs (Команды) задайте список действий для данного сопоставления. Чтобы все запросы, включающие заданное расширение, передавались приложению, поставьте переключатель в положение All Verbs (Все команды). Если вы поставите переключатель в положение Limit To (Сократить до), укажите конкретные типы запросов, разделив их запятыми.



**Примечание** Список Verbs (Команды) определяет типы запросов, передаваемые приложению. Например, можно создать одно сопоставление для обработки запросов GET, HEAD и POST на HTM-файлы и другое — для обработки запросов PUT, TRACE и DELETE на HTM-файлы.

5. Приложения могут выполняться в каталогах с разрешением Scripts Only (Только сценарии) или Scripts And Exe-

cutables (Сценарии и исполняемые файлы). Если надо, чтобы расширение ISAPI или CGI-программа выполнялись в каталоге с разрешением Scripts Only (Только сценарии), пометьте флажок Script Engine (Обработчик сценариев). Если нет — снимите флажок, и компонент будет выполняться только в каталогах с разрешением Scripts And Executables (Сценарии и исполняемые файлы).

6. Пометьте флажок Check That File Exists (Проверка наличия файла), чтобы IIS перед запуском расширения ISAPI или CGI-программы проверяла, существует ли запрашиваемый файл и имеет ли пользователь соответствующие разрешения на доступ. При отсутствии файла или разрешений браузеру возвращается предупреждение, и компонент не выполняется.



**Примечание** Функция Check That File Exists полезна при использовании сценариев, которые связаны с исполнимыми файлами, не отсылающими CGI-ответ в случае недоступности сценария. В качестве примера здесь можно привести сценарии на языке Perl. Check That File Exists может вызвать падение производительности перегруженного сервера, поскольку файл открывается дважды: службами IIS и соответствующим компонентом.

7. Трижды щелкните ОК, чтобы вернуться к оснастке IIS.

#### Редактирование сопоставлений приложений

Существующие сопоставления приложений можно изменить.

1. На вкладке App Mappings (Отображение приложений) окна свойств приложения щелкните Edit (Изменить). Откроется диалоговое окно Add/Edit Application Extension Mapping (Добавление или изменение сопоставления расширений) (рис. 4-4).
2. Внесите необходимые изменения и дважды щелкните ОК.
3. При следующей загрузке исполнимого файла или соответствующей DLL в память будут использоваться новые параметры. Если включено кэширование ISAPI, для вступления изменений в силу остановите и перезапустите Web-узел.

### Удаление сопоставлений приложений

Чтобы удалить сопоставления приложений, сделайте следующее.

1. В окне свойств App Mappings (Отображение приложений) приложения щелкните Remove (Удалить).
2. Щелкните Yes (Да) в ответ на запрос системы,
3. Щелкните OK. При следующей загрузке исполнимого файла или соответствующей DLL в память будут задействованы новые параметры. Если включено кэширование ISAPI, для вступления изменений в силу остановите и перезапустите Web-узел.

### Управление состоянием сеанса

Состояние сеанса существенно влияет на производительность IIS и использование ресурсов. Если состояние сеанса включено, IIS создает отдельный сеанс для каждого обращающегося к ASP-приложению пользователя. Сведения о сеансе позволяют отслеживать работу пользователя с приложением, а также обмениваться пользовательской информацией между страницами. Например, отслеживать ASP-параметры пользователей, работающих с приложением.

Принцип работы сеанса прост — при первом обращении пользователя к одной из ASP-страниц указанного приложения службы IIS генерируют:

- **объект Session** — содержит все параметры пользовательского сеанса, включая идентификатор кодовой страницы, который применяется для вывода динамического содержимого, идентификатор расположения, идентификатор сеанса и значение времени ожидания,  
или
- **набор Session.Collection** — содержит все элементы, значения которых были изменены приложением на протяжении сеанса (кроме объектов, созданных в файле GLOBAL.ASA приложения),  
или
- **набор Session.StaticObjects** — содержит статические объекты, определенные в файле GLOBAL.ASA.

Объект Session и связанные с ним свойства хранятся в памяти сервера. Идентификатор пользовательского сеанса передается клиентскому браузеру в виде файла cookie. Если браузер принимает такие файлы, при последующих запросах идентификатор сеанса передается обратно серверу. Это верно, даже если пользователь обращается к одной из страниц другого приложения. Использование одного и того же идентификатора позволяет уменьшить число файлов cookie, передаваемых браузеру. Помните: если браузер не принимает cookie, идентификаторы сеанса не поддерживаются, и IIS не может отслеживать с их помощью пользовательские сеансы.

По умолчанию сеансы включены для всех IIS-приложений, и время ожидания сеанса составляет 20 минут. Таким образом, если пользователь не обращается к странице в течение 20 минут, сеанс заканчивается, и IIS удаляет из памяти соответствующий объект Session. Задать время ожидания по умолчанию можно в поле Session Timeout (Время ожидания сеанса) вкладки Application Options (Параметры приложений).

Понятно, что для отслеживания сеансов нужны значительные ресурсы системы. Чтобы уменьшить их объем, сократите срок ожидания или вообще отключите отслеживание сеансов. В первом случае сеансы будут заканчиваться быстрее, чем обычно. Во втором — IIS не будет автоматически создавать сеансы. Вы сможете открывать их вручную из приложения, добавив в код соответствующей ASP-страницы директиву `<%@ENABLESESSIONSTATE = True%>`.

Все имеющиеся на сервере приложения используют собственные параметры управления состоянием сеанса. Чтобы изменить их, сделайте следующее.

1. В оснастке IIS щелкните правой кнопкой каталог, являющийся начальной точкой приложения, и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите соответственно на вкладку Home Directory (Домашний каталог). Directory (Каталог) или Virtual Directory (Виртуальный каталог), затем щелкните Configuration (Настройка).
3. Чтобы разрешить автоматическое создание сеансов, пометьте на вкладке App Options (Параметры приложений) флажок Enable Session State (Включить состояние сеанса), чтобы запретить - снимите флажок.

4. Если вы разрешили поддержку сеансов, введите в поле Session Timeout (Время ожидания сеанса) время ожидания сеанса. Для интенсивно используемого приложения, в котором клиенты быстро перемешаются от одной страницы к другой, следует задать небольшое время ожидания, например 15 минут. Но если вам требуется поддерживать пользовательский сеанс до завершения транзакции, задайте более длительный интервал ожидания, например 60 минут.

5. Дважды щелкните ОК.



**Совет** Сегодня большинство крупномасштабных коммерческих Web-узлов размещают параллельно на нескольких серверах. При этом применяется специальный компонент, распределяющий обращения к Web-узлу между доступными в данный момент серверами. Для управления ASP-сеансами на Web-узле с распределением нагрузки необходимо, чтобы все запросы конкретного клиента обрабатывались одним сервером. Способ реализации этого зависит от компонента — распределителя нагрузки.

### Управление буферизацией приложений

Буферизация также влияет на производительность и использование ресурсов сервера. Если буферизация включена, IIS полностью обрабатывает страницы перед передачей их содержимого клиентскому браузеру. При отключенной буферизации IIS передаст содержимое клиентскому браузеру по мере обработки страницы. Буферизация позволяет динамически реагировать на события, возникающие при обработке страницы. Вы можете прервать отправку страницы или отослать пользователя к другой странице, очистить буфер и передать пользователю другое содержимое, изменить информацию HTTP-заголовка из любого места ASP-сценария.

Недостаток буферизации: пользователь может просмотреть содержимое лишь после того, как сервер полностью закончит обработку сценария. Если сценарий длинный или сложный, ждать придется довольно долго. Для устранения таких задержек разработчики часто вставляют в ключевые строки сценария операторы Flush. При этом генерируются дополнительные запросы на клиент-серверные соединения, что может привести к падению производительности.

Как и отслеживание сеансов, буферизация по умолчанию включена для всех приложений. Для управления буферизацией сделайте следующее.

1. В оснастке IIS щелкните правой кнопкой каталог, являющийся начальной точкой приложения, и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите соответственно на вкладку Home Directory (Домашний каталог), Directory (Каталог) или Virtual Directory (Виртуальный каталог), затем щелкните Configuration (Панель).
3. Чтобы разрешить автоматическое создание сеансов, пометьте на вкладке App Options (Параметры приложения) флажок Enable Buffering (Включить буферизацию). Чтобы запретить, снимите флажок.



**Совет** Чтобы включить буферизацию на уровне отдельных страниц приложения, добавьте в их код оператор `Response.Buffer = True`.

4. Дважды щелкните ОК.

#### **Родительские пути, язык сценариев по умолчанию для ASP-страниц и время ожидания ASP-сценария**

Дополнительные параметры приложения — это родительские пути, язык сценариев по умолчанию для ASP-страниц и время ожидания ASP-сценария. Флажок Enable Parent Paths (Включить пути к родительским каталогам) позволяет ASP-страницам задействовать относительные пути для доступа к родительскому каталогу текущей папки. Например, сценарий может ссылаться на файл `../BUILD.HTM`, где «`..`» — родительский каталог текущей папки. Использование родительских путей разрешено по умолчанию.

Поле Default ASP Language (Язык ASP по умолчанию) определяет язык сценариев по умолчанию для ASP-страниц. При обычной установке служб IIS на компьютер копируются два обработчика сценариев: Microsoft Visual Basic Scripting Edition (VBScript) и Microsoft JScript. Для ссылки на них служат значения VBScript и JScript соответственно. В обычной установке IIS язык сценариев по умолчанию — VBScript, но это можно в любое время изменить. Переопределить в сценарии язык по умолчанию позволяет директива `<%@LANGUAGE%>`.

В поле **ASP Script Timeout** (Время ожидания сценария ASP) задается срок, в течение которого система ожидает завершения выполнения сценария. Если по завершении этого срока сценарий не закончит выполняться, службы IIS остановят его и занесут сообщение об ошибке в журнал событий приложения. Время ожидания по умолчанию — 90 секунд. Переопределить время ожидания по умолчанию в коде ASP-страницы позволяет метод `Server.ScriptTimeout`.

Сделайте следующее.

1. В оснастке IIS щелкните правой кнопкой папку, являющуюся начальной точкой приложения, и выберите в контекстном меню команду **Properties** (Свойства).
2. Перейдите соответственно на вкладку **Note Directory** (Домашний каталог), **Directory** (Каталог) или **Virtual Directory** (Виртуальный каталог), затем щелкните **Configuration** (Настройка). Перейдите на вкладку **App Options** (Параметры приложений).
3. Чтобы разрешить сценариям использовать относительные пути для доступа к родительскому каталогу, пометьте флажок **Enable Parent Paths** (Включить пути к родительским каталогам). Чтобы запретить, снимите флажок.
4. Язык сценариев по умолчанию — **VBScript**. Чтобы изменить это, введите в поле **Default ASP Language** (Язык ASP по умолчанию) имя нужного языка.
5. По умолчанию время ожидания ASP-сценария — 90 секунд. Чтобы изменить это, введите в поле **ASP Script Timeout** (Время ожидания сценария ASP) требуемое значение.
6. Дважды щелкните **OK**.

#### **Включение и отключение отладки приложений**

Отладка — один из лучших методов локализации ошибок в IIS-приложении. Для утравления отладкой используются серверные и клиентские конфигурационные параметры. При отладке на стороне сервера службы IIS в процессе обработки ASP-страниц отбрасывают ошибки и выводят сообщения с предложением о запуске **Microsoft Script Debugger**. Затем пользователь может с помощью отладчика изучить код ASP-страницы. Отладка на стороне клиента включает передачу

клиентскому браузеру отладочной информации, позволяющей выявить источник проблем с IIS и соответствующими ASP-страницами.

Чтобы включить отладку на стороне сервера или клиента, сделайте так.

1. В оснастке IIS щелкните правой кнопкой папку, которая является начальной точкой приложения, и выберите в контекстном меню команду **Properties** (Свойства).
2. Перейдите соответственно на вкладку **Home Directory** (Домашний каталог), **Directory** (Каталог) или **Virtual Directory** (Виртуальный каталог), затем щелкните **Configuration** (Настройка). Перейдите на вкладку **App Debugging** (Отладка приложений).
3. Чтобы разрешить отладку на стороне сервера, пометьте флажок **Enable ASP Server-Side Script Debugging** (Включить серверную отладку сценариев ASP). Чтобы запретить, снимите флажок.



**Примечание** Серверная отладка ASP-приложений предназначена для тестовых, а не производственных серверов. Включив серверную отладку на производственном сервере, вы заметите падение производительности соответствующего приложения, поскольку ASP будет работать в однопоточном режиме.

4. Чтобы разрешить отладку на стороне сервера, пометьте флажок **Enable ASP Client-Side Script Debugging** (Включить клиентскую отладку сценариев ASP), чтобы запретить — снимите его.

#### Настройка сообщений об ошибках приложения

По умолчанию приложения передают клиентам подробные сообщения об ошибках, включающие имя файла, текст сообщения и номер строки, в которой произошла ошибка. Эти сведения полезны для локализации ошибок в коде. Однако их вовсе не обязательно выводить пользователям и можно заменить кратким текстовым сообщением.

Чтобы изменить параметры вывода сообщений об ошибках приложения, сделайте следующее.



1. В оснастке IIS щелкните правой кнопкой папку, которая является начальной точкой приложения, и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите соответственно на вкладку Home Directory (Домашний каталог), Directory (Каталог) или Virtual Directory (Виртуальный каталог), и затем щелкните Configuration (Настройка). Перейдите на вкладку App Debugging (Отладка приложений).
3. Для вывода подробных сообщений об ошибках пометьте флажок Send Detailed ASP Error Messages To Client (Отправлять подробные сообщения об ошибках ASP клиенту). Или пометьте флажок Send Text Error Message To Client (Отправлять текст сообщения клиенту) и введите текст сообщения, которое будет появляться при возникновении ошибки.

### Выгрузка изолированных приложений

Изолированные приложения выполняются в отдельной области памяти и отдельном процессе DLLHOST.EXE. Для принудительного удаления приложения из памяти можно выгрузить его. Таким образом, при следующем обращении пользователя к приложению службы IIS повторно загрузят приложение в память и создадут новый процесс DLLHOST.EXE.

Чтобы выгрузить изолированное приложение, сделайте следующее.

1. В оснастке IIS щелкните правой кнопкой папку, которая является начальной точкой приложения, и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите соответственно на вкладку Home Directory (Домашний каталог), Directory (Каталог) или Virtual Directory (Виртуальный каталог).
3. Щелкните Unload (Выгрузить), затем — ОК.

### Удаление IIS-приложений

Ненужные приложения рекомендуется удалить, чтобы освободить занимаемые ими ресурсы. Чтобы удалить приложение, сделайте так.

1. В оснастке IIS щелкните правой кнопкой папку, которая является начальной точкой приложения, и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите соответственно на вкладку Home Directory (Домашний каталог), Directory (Каталог) или Virtual Directory (Виртуальный каталог).
3. Щелкните Remove (Удалить), затем — OK.

## Управление пользовательскими фильтрами ISAPI

Фильтры ISAPI — это IIS-приложения, которые обрабатывают запросы на конкретные типы событий, например Read или Write. При наступлении соответствующего события фильтр выполняет ряд действий. Фильтры ISAPI могут быть как глобальными, так и локальными. Глобальные фильтры действуют для всех узлов, а локальные — только для конкретного Web-узла.

### Просмотр и настройка глобальных фильтров

Глобальные фильтры влияют на все Web-узлы IIS и загружаются в память при запуске World Wide Web Publishing Service. После добавления или изменения параметров существующего глобального фильтра эту службу нужно остановить и перезапустить. Чтобы просмотреть или изменить параметры глобальных фильтров, сделайте так.

1. В оснастке IIS щелкните значок компьютера правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. В группе Master Properties (Основные свойства) щелкните Edit (Изменить) и затем перейдите на вкладку ISAPI Filters (Фильтры ISAPI).
3. Появится список имеющихся глобальных фильтров. Фильтры в списке действуют для всех Web-узлов сервера и выполняются в соответствии со своим приоритетом.
4. Список фильтров включает такие поля:
  - **Status** (Состояние) — состояние загрузки фильтра: успешно загруженные в память фильтры отмечены зеленой стрелкой, направленной вверх, незагруженные — красной, направленной вниз;

- Filter Name (Имя фильтра) — описательное имя фильтра, задаваемое при его установке;
- Priority (Приоритет) — приоритет фильтра, указанный в исходном коде; первыми выполняются фильтры с самым высоким приоритетом.



**Примечание** Щелкнув фильтр, можно просмотреть путь к его исполняемому файлу.

5. Настроить глобальные фильтры позволяют кнопки:
  - Add (Добавить) — добавление фильтра: щелкнув эту кнопку, введите имя фильтра и путь к его исполняемому файлу; если путь неизвестен, щелкните Browse (Обзор) и выберите требуемый файл в диалоговом окне Open (Открыть);
  - Remove (Удалить) — удаление фильтра: выберите глобальный фильтр и щелкните Remove;
  - Edit (Изменить) — изменение параметров фильтра: единственный параметр, который можно изменить — путь к исполняемому файлу фильтра; выберите фильтр и щелкните Edit, в диалоговом окне свойств введите новый путь и щелкните OK.
6. Если для реакции на одно событие сконфигурировано несколько фильтров, они выполняются по очереди, и соответствии со своим приоритетом. При одинаковом приоритете сначала выполняются глобальные фильтры, а затем — фильтры уровня узла. Чтобы изменить порядок выполнения фильтров с одинаковым приоритетом, используйте зеленые стрелки «вверх» и «вниз».
7. Добавив новый или изменив параметр существующего глобального фильтра, остановите и перезапустите World Wide Web Publishing Service. В результате службы IIS загрузят новые фильтры в память.

#### Просмотр и настройка локальных фильтров

Локальные фильтры влияют на отдельный Web-узел IIS и могут при добавлении или изменении динамически загружаться в память при условии, что запущены World Wide Web Publishing Service и Web-узел. Таким образом, останавливать и перезапускать World Wide Web Publishing Service после изменения или добавления локального фильтра не требуется.

Чтобы просмотреть или изменить параметры локальных фильтров, сделайте следующее.

1. В оснастке IIS щелкните значок Web-узла кнопкой мыши и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите на вкладку ISAPI Filters (Фильтры ISAPI). Появится список локальных узлов для данного Web-узла.



**Примечание** В этом списке показаны только фильтры, назначенные для конкретного Web-узла. В нем нет глобальных фильтров, заданных в основных свойствах WWW-службы, даже если выполняются оба типа фильтров. Некоторые глобальные фильтры установлены по умолчанию, локальные — всегда создает администратор.

3. Список фильтров включает следующие поля:
  - Status (Состояние) — состояние загрузки фильтра; успешно загруженные в память фильтры отмечены зеленой стрелкой, направленной вверх; фильтры, не загруженные в память, — красной, направленной вниз;
  - Filter Name (Имя фильтра) — описательное имя фильтра, задаваемое при его установке;
  - Priority (Приоритет) — приоритет фильтра, указанный в исходном коде; первыми выполняются фильтры с самым высоким приоритетом.



**Примечание** Щелкнув фильтр, можно просмотреть путь к его исполняемому файлу.

4. Настроить локальные фильтры позволяют кнопки:
  - Add (Добавить) — добавление фильтра; щелкнув эту кнопку, введите имя фильтра и путь к его исполняемому файлу; если путь неизвестен, щелкните Browse (Обзор) и выберите файл в диалоговом окне Open (Открыть);
  - Remove (Удалить) — удаление фильтра; выберите глобальный фильтр и щелкните Remove;
  - Edit (Изменить) — изменение параметров фильтра; единственный параметр, который можно изменить — путь к исполняемому файлу фильтра; выберите фильтр

и щелкните Edit, в диалоговом окне свойств введите новый путь и щелкните ОК.

5. Если для реакции на одно событие сконфигурировано несколько фильтров, они выполняются по очереди, в соответствии со своим приоритетом. При одинаковом приоритете сначала выполняются глобальные фильтры, а затем — фильтры уровня узла. Изменить порядок выполнения фильтров с одинаковым приоритетом позволяют зеленые стрелки «вверх» и «вниз».

## Изменение содержимого Web-узла и HTTP-заголовков

Службы IIS используют для документов и HTTP-заголовков значения по умолчанию, которые можно изменять на уровне узла, папки или файла.

### Настройка документов по умолчанию

Параметры документа по умолчанию определяют, как IIS обрабатывает запросы, не содержащие имени документа. Клиентские запросы, в которых путь к каталогу оканчивается не именем файла, а именем папки или косой чертой (/), обрабатываются в соответствии с параметрами документа по умолчанию. Если обработка документов по умолчанию включена, службы IIS ищут документы в порядке перечисления их в списке и возвращают первый найденный документ по умолчанию. Если документы не найдены, IIS проверяют наличие разрешения Directory Browsing (Просмотр каталогов) и, если оно имеется, возвращают содержимое папки. Если нет — сообщается об ошибке «404 — File Not Found» (Файл не найден).

Параметры документа по умолчанию можно изменять как на уровне узла, так и на уровне папки, т. е. параметры документа по умолчанию для отдельных папок могут отличаться от соответствующих параметров узла. Стандартные имена документов по умолчанию — DEFAULT.HTM, DEFAULT.ASP, INDEX.HTM и INDEX.HTML.

Чтобы просмотреть или изменить текущие параметры документа по умолчанию, сделайте так.

1. В оснастке IIS щелкните правой кнопкой нужный Web-узел, папку или виртуальный каталог и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите на вкладку Documents (Документы). Если хотите разрешить обработку документов по умолчанию, пометьте флажок Enable Default Document (Задать документ, используемый по умолчанию). Если нет — снимите его.
3. Чтобы добавить новый документ по умолчанию, щелкните Add (Добавить). Затем введите имя документа, например INDEX.HTML, и щелкните OK.
4. Чтобы удалить документ по умолчанию, выберите его в списке и щелкните Remove (Удалить).
5. Чтобы изменить порядок поиска, выберите документ и измените его положение в списке с помощью стрелок «вверх» и «вниз».
6. Щелкните OK.

#### Нижний колонтитул документа

Службы IIS можно настроить для автоматической вставки во все отсылаемые документы нижнего колонтитула в формате HTTP. Нижний колонтитул может включать информацию об авторских правах, логотип и пр. Как и документы по умолчанию, колонтитулы можно определить на уровне узла или отдельной папки.

#### Автоматическая вставка нижних колонтитулов

Чтобы создать автоматически вставляемый нижний колонтитул, сделайте так.

1. Создайте документ в формате HTML и сохраните его в папке на локальном жестком диске сервера. Нижний колонтитул должен быть не законченной HTML-страницей, а включать лишь HTML-теги с необходимым содержанием.
2. В оснастке IIS щелкните правой кнопкой нужный Web-узел, папку или виртуальный каталог и выберите в контекстном меню команду Properties (Свойства).
3. Перейдите на вкладку Documents (Документы) и пометьте флажок Enable Document Footer (Включить примечание документа).

4. В текстовое поле введите путь к файлу нижнего колонтитула или щелкните **Browse (Обзор)** и выберите файл в диалоговом окне **Open (Открыть)**.
5. Щелкните **ОК**.

**Отключение автоматической вставки нижних колонтитулов**

Автоматическая вставка нижнего колонтитула *отключается* так.

1. В оснастке IIS щелкните правой кнопкой нужный **Web-узел**, папку или виртуальный каталог и выберите в контекстном меню команду **Properties (Свойства)**.
2. Перейдите на вкладку **Documents (Документы)** и снимите флажок **Enable Document Footer (Включить примечание документа)**.
3. Щелкните **ОК**.

**Срок хранения содержимого и запрет кэширования содержимого браузером**

Большинство браузеров помещает просмотренные документы в кэш, для дальнейшего их просмотра пользователями без загрузки с Web-сервера. Управлять кэшированием можно при помощи срока хранения содержимого. Если этот параметр задействован, при передаче пользователю HTTP-ответов IIS включают в них сведения о сроке хранения содержимого. Таким образом, при последующих обращениях к документу браузер может определить: считать его из кэша или загрузить с Web-узла.

Срок хранения содержимого можно задать на уровне узла, папки или файла. Параметры уровня узла влияют на все его страницы, уровня папки — на все файлы вложенных каталогов, а уровня файла — на конкретный файл. Есть три срока хранения содержимого.

- **Expire Immediately (Немедленно)** — срок хранения истекает немедленно, т. е. браузер не может считать файл из кэша. Используйте это значение, если нужно, чтобы браузер показывал новейшую версию динамически генерируемой страницы.
- **Expire After (Через)** — срок хранения в минутах, часах или днях, до истечения которого браузер может считы-

вать файл из кэша. Задайте это значение, если нужно, чтобы браузер по истечении определенного времени заново загружал файл с Web-узла.

- **Expire On Date At Time (На)** — конкретные дата и время окончания срока хранения, до наступления которых браузер может считывать файл из кэша. Используйте это значение для данных, устаревающих после определенной даты, например для специальных предложений или уведомлений.



**Совет** Для управления сроком хранения содержимого при работе с ASP-страницами следует добавить в HTTP-заголовков запись `Response.Expires`. Если присвоить ей нулевое значение (`Response.Expires = 0`), срок хранения содержимого будет истекать немедленно. Помните: HTTP-заголовки должны передаваться браузеру до содержимого страницы.

#### Задание срока хранения содержимого

Срок хранения содержимого можно задать на уровне узла, папки или файла. Параметры уровня файла и папки определяют параметры уровня узла. Таким образом, при возникновении проблем стоит проверить параметры соответствующего файла или папки.

Срок хранения содержимого на уровне узла, папки или файла задается так.

1. В оснастке IIS щелкните правой кнопкой нужный Web-узел, папку или виртуальный каталог и выберите в контекстном меню команду **Properties** (Свойства).
2. Перейдите на вкладку **HTTP Headers** (Заголовки HTTP) и пометьте флажок **Enable Content Expiration** (Включить срок действия содержимого).
3. Чтобы срок хранения содержимого истекал немедленно, поставьте переключатель в положение **Expire Immediately** (Немедленно).
4. Чтобы задать конкретный срок хранения в минутах, часах или днях, поставьте переключатель в положение **Expire After** (Через) и введите требуемые значения в соответствующих полях.



5. Чтобы задать конкретные дату и время окончания срока хранения, щелкните переключатель Expire On (На) и введите значения в соответствующие поля.
6. Щелкните ОК.

#### Отключение срока хранения содержимого

Срок хранения содержимого на уровне узла, папки или файла можно отключить.

1. В оснастке IIS щелкните правой кнопкой нужный Web-узел, папку или виртуальный каталог и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите на вкладку HTTP Headers (Заголовки HTTP) и снимите флажок Enable Content Expiration (Включить срок действия содержимого).
3. Щелкните ОК.

#### Пользовательские HTTP-заголовки

Если браузер запрашивает документ с Web-узла под управлением IIS, тот обычно передается ему вместе с заголовком ответа. Возможно, вам потребуется изменить стандартный или создать собственный заголовок. Например, чтобы задействовать преимущества HTTP-заголовков, которые предусмотрены протоколом HTTP, но которыми нельзя управлять из IIS. Или же предоставить клиенту информацию, которую можно передать лишь в пользовательских HTTP-заголовках.

Пользовательские HTTP-заголовки содержат сведения, которые требуется включить в заголовок ответа документа. Записи пользовательского заголовка представляют собой пары «имя — значение». «Имя» определяет значение, на которое вы ссылаетесь, «значение» — содержимое, передаваемое клиентскому браузеру.

Обычно пользовательские заголовки содержат инструкции по обработке документов или дополнительную информацию. Например, поле Cache-Control HTTP-заголовка позволяет контролировать кэширование страницы прокси-сервером. Значение Public данного поля указывает прокси-серверу, что кэширование разрешено, а значение Private — что запрещено. Просмотреть или изменить пользовательские HTTP-заголовки для узла, папки или файла можно следующим образом.

1. В оснастке IIS щелкните нужный Web-узел, виртуальный каталог или папку правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите на вкладку HTTP Headers (Заголовки HTTP). В списке Custom HTTP Headers (Специальные заголовки HTTP) отображаются имеющиеся заголовки в формате «имя: значение».
3. Управление заголовками осуществляется при помощи кнопок:
  - Add (Добавить) — добавление пользовательского HTTP-заголовка; щелкните эту кнопку, введите имя и значение заголовка и щелкните ОК;
  - Remove (Удалить) - удаление пользовательского HTTP-заголовка: выберите заголовок и щелкните Remove (Удалить);
  - Edit (Изменить) - изменение пользовательского HTTP-заголовка: выберите заголовок и щелкните Edit (Изменить), в открывшемся диалоговом окне свойств произведите нужные изменения и щелкните ОК.
4. Щелчком ОК закройте диалоговое окно свойств текущего узла, папки или файла.

### Системы оценки содержимого

IIS включает встроенную систему оценки содержимого, основанную на системе PICS (Platform for Internet Content Selection). Система PICS разработана Наблюдательным советом по развлекательному ПО (Recreational Software Advisory Council, RSAC) и базируется на исследованиях доктора Дональда Робертса (Donald Roberts), работающего в Стэнфордском университете. Согласно PICS содержимое можно оценивать по наличию в нем таких категорий, как насилие, секс, обнаженная натура и нецензурные выражения. Оценка каждой категории может изменяться от 0 (элементы указанной категории отсутствуют) до 4 (элементы указанной категории представлены очень широко).

Задать оценки содержимого можно на уровне узла, папок или файлов. Вам потребуется предварительно заполнить анкету RSAC, чтобы получить рекомендуемые оценки для содержимого вашего Web-узла.

**Оценка содержимого**

Чтобы оценить содержимое своего Web-узла, сделайте следующее.

1. В оснастке IIS щелкните нужный Web-узел, виртуальный каталог или папку правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите на вкладку HTTP Headers (Заголовки HTTP) и затем в группе Content Ratings (Оценка содержимого) щелкните Edit Ratings (Изменить).
3. Щелкните Rating Questionnaire (Опрос) и следуйте инструкциям RSAC.
4. Заполнив анкету, закройте браузер и дважды щелкните ОК.

**Включение оценок содержимого**

Оценки содержимого для узла, папки или файла настраиваются так.

1. В оснастке IIS щелкните нужный Web-узел, виртуальный каталог или папку правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите на вкладку HTTP Headers (Заголовки HTTP), в группе Content Ratings (Оценка содержимого) щелкните Edit Ratings (Изменить).
3. Перейдите на вкладку Ratings (Оценки) и пометьте флажок Enable Ratings For This Resource (Включить оценки для данного ресурса).
4. В списке Category (Категория) выберите нужную категорию оценок. С помощью ползунка задайте уровень присутствия элементов этой категории в оцениваемом содержимом. Для каждого положения ползунка выводится описание.
5. Введите в поле Email Name Of Person Rating This Content (Введите адрес электронной почты лица, оценивающего содержимое) свой адрес электронной почты и затем в списке Expire On (Срок действия) укажите дату, после которой оценки содержимого станут недействительными.
6. Дважды щелкните ОК.

Отключение **оценок** содержимого

Оценки содержимого можно и отключить.

1. В оснастке IIS щелкните нужный Web-узел, виртуальный каталог или папку правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите на вкладку HTTP Headers (Заголовки HTTP). В группе Content Ratings (Оценка содержимого) щелкните Edit Ratings (Изменить).
3. Перейдите на вкладку Ratings (Оценка) и снимите флажок Enable Ratings For This Resource (Включить оценки для данного ресурса).
4. Дважды щелкните ОК.

## **Настройка сообщений об ошибках Web-узла**

При возникновении ошибок на Web-узле службы IIS генерируют HTTP-сообщения об ошибках. Обычно ошибки связаны с некорректными клиентскими запросами, проблемами проверки подлинности и внутренними ошибками сервера. Администратор полностью управляет передачей сообщений об ошибках клиенту. Так, вы можете настроить IIS для возврата клиенту обычных HTTP-сообщений об ошибках, файлов по умолчанию, содержащих подробные сообщения об ошибках, а также созданных вами файлов с такими сообщениями.

### **Коды состояния и сообщения об ошибках**

Код состояния и сообщения об ошибках работают параллельно. При запросе пользователем файла сервер генерирует специальный код, определяющий состояние пользовательского запроса. Если запрос выполнен успешно, код состояния регистрирует это, и запрашиваемый файл передается браузеру. При невозможности выполнить запрос код состояния регистрирует причину. На основе данного кода сервер генерирует соответствующее сообщение об ошибке, возвращаемое браузеру вместо запрашиваемого файла.

Код состояния — это трехзначное число, которое может включать цифровой суффикс. Первая цифра определяет его класс, две следующих — категорию ошибки, а суффикс (если

есть) — конкретную ошибку. Например, код состояния 403 указывает на проблемы доступа. К этой категории относятся несколько ошибок, например 403.1 (запрещен доступ для выполнения), 403.2 (запрещен доступ для чтения), 403.3 (запрещен доступ для записи).

Просматривая журналы Web-сервера или получив код ошибки при локализации какой-либо проблемы, обратите внимание на коды состояния. Вот список их основных классов:

- 1XX — продолжение работы (смена протокола);
- 2XX — успешное выполнение;
- 3XX — переадресация;
- 4XX — ошибка (сбой) на стороне клиента;
- 5XX — ошибка сервера.

Как видно, первая цифра кода указывает, что же на самом деле произошло. Коды состояния, начинающиеся с 1, 2 или 3, являются обычными и, как правило, не означают какой-либо ошибки. Коды состояния, начинающиеся с 4 или 5, указывают на ошибку или потенциальную проблему, которую требуется устранить.

При просмотре файлов журнала или отчетов о компиляции, устранении проблем или отладке полезно, а порой и необходимо знать, к какому классу относится ошибка. В следующем списке приведены поддерживаемые службами IIS обычные HTTP-сообщения (соответствуют протоколу HTTP 1.1).

- 400 — Bad request (Ошибочный запрос);
- 401.1 — Logon failed (Сбой входа в систему);
- 401.2 — Logon failed due to server configuration (Сбой входа в систему из-за конфигурации сервера);
- 401.3 — Unauthorized due to access control list (ACL) on resource (Нет доступа из-за таблицы управления доступом на ресурсе);
- 401.4 — Authorization failed by filter (Отказ при проверке прав доступа на фильтре);
- 401.5 — Authorization failed by ISAPI/CGI application (Отказ при проверке прав доступа к приложению ISAPI/CGI);
- 403.1 — Execute access forbidden (Запрещен доступ на выполнение);

- **403.2** — Read access forbidden (Запрещен доступ на чтение);
- **403.3** — Write access forbidden (Запрещен доступ на запись);
- **403.4** — SSL required (Требуется SSL);
- **403.5** - SSL 128 required (Требуется SSL 128);
- **403.6** — IP address rejected (Отказ для IP-адреса);
- **403.7** — Client certificate required (Требуется клиентский сертификат);
- **403.8** — Site access denied (Нет доступа к узлу);
- **403.9** — Too many users (Слишком много пользователей);
- **403.10** — Invalid configuration (Недопустимая конфигурация);
- **403.11** — Password change (Смена пароля);
- **403.12** — Mapper denied access (Доступ запрещен средством сопоставления);
- **403.13** — Client certificate revoked (Клиентский сертификат отозван);
- **403.14** — Directory listing denied (Просмотр каталога запрещен);
- **403.15** — Client Access Licenses exceeded (Достигнуто максимально разрешенное число подключений);
- **403.16** — Client certificate untrusted or invalid (Клиентский сертификат не вызывает доверия или недействителен);
- **403.17** — Client certificate has expired or is not yet valid (Клиентский сертификат устарел или еще не начал действовать);
- **404** — Not found (Объект не найден);
- **404.1** — Site not found (Узел не найден);
- **405** — Method not allowed (Метод не поддерживается);
- **406** — Not acceptable (Недопустимый объект);
- **407** — Proxy authentication required (Требуется проверка подлинности прокси-сервером);
- **412** — Precondition Failed (Сбой подготовки начальных условий);

- 414 — Request-URI too long (Слишком длинный запрос URI);
- 500 — Internal server error (Внутренняя ошибка сервера);
- 500.12 — Application restarting (Приложение в состоянии перезапуска);
- 500.13 — Server too busy (Сервер перегружен);
- 500.15 - Requests for GLOBAL.ASA not allowed (Запросы на файл GLOBAL.ASA недопустимы);
- 500-100.ASP - ASP error (Ошибка ASP);
- 501 — Not implemented (Не реализовано);
- 502 — Bad gateway (Неверный шлюз).

### Дополнительные параметры обработки ошибок

Вы вправе определить порядок обработки любой стандартной ошибки. Порядок может задаваться на уровне файлов, папок и узлов, причем параметры обработки для файла переопределяют соответствующие параметры уровня каталога, а те в свою очередь — аналогичные параметры уровня узла. Существует три метода обработки ошибок:

- **Default** (По умолчанию) — клиенту возвращается стандартное сообщение IIS об ошибке;
- **File** (Файл) — клиенту возвращается указанный файл с сообщением об ошибке (применяется для статического содержимого);
- **URL** (Адрес URL) — клиенту возвращается сообщение, переадресующее его на конкретный URL (применяется для динамического содержимого).

Большинство HTTP-ошибок обрабатывается при помощи файлов сообщений, которые при обычной установке IIS находятся в папке % System Root %\Help\Iishelp\Comtop. Можно и редактировать файлы сообщений об ошибках по умолчанию, и создавать *собственные* файлы. Помните; метод File можно использовать только для статического содержимого (например, HTML-страниц), а метод URL — для динамического содержимого (например, ASP-страниц). Иначе вы рискуете получить неожиданные результаты.



**Совет** Если для обработки ошибок используется ASP-файл, код ошибки и URL исходной страницы передаются ему в виде параметров запроса. ASP-файл следует сконфигурировать так, чтобы он считывал параметры из URL и соответствующим образом изменял код состояния. Например, если страница NOTFOUND.ASP обрабатывает ошибки 404 и пользователь пытается открыть страницу при помощи URL `http://www.microsoft.com/data.htm/`, вызов ASP-страницы должен осуществляться посредством URL `http://www.microsoft.com/NotFound.asp?404;http://www.microsoft.com/data.htm/`. Затем эта страница извлекает из переданного ей URL параметры 404 и `http://www.microsoft.com/data.htm/`.



**Примечание** Если Internet Explorer считает, что пользовательское сообщение об ошибке слишком мало и не содержит полезной информации, он заменяет его собственным HTTP-сообщением. Оценка полезности сообщения осуществляется на основе размера последнего. Так, если размер сообщения об ошибке 403, 405 или 410 меньше 256 байт или размер сообщения об ошибке 400, 404, 406, 408, 409, 500, 500.12, 500.13, 500.15, 501 или 505 меньше 512 байт, Internet Explorer заменит пользовательское сообщение об ошибке, возвращаемое службами IIS, на собственное сообщение.

#### Просмотр параметров сообщений об ошибках

Чтобы просмотреть параметры сообщений об ошибках, сделайте следующее.

1. В оснастке IIS щелкните нужный Web-узел, виртуальный каталог или панку правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите на вкладку Custom Errors (Специальные ошибки) (рис. 4-5). Появится список стандартных HTTP-ошибок, включающий следующие поля:
  - **HTTP Error (Ошибка HTTP)** — HTTP-код состояния для данной ошибки; может включать суффикс;
  - **Type (Тип)** — метод обработки ошибки (default, file или URL);
  - **Contents (Содержание)** — текст сообщения, путь или URL файла, содержащего описание данной ошибки.



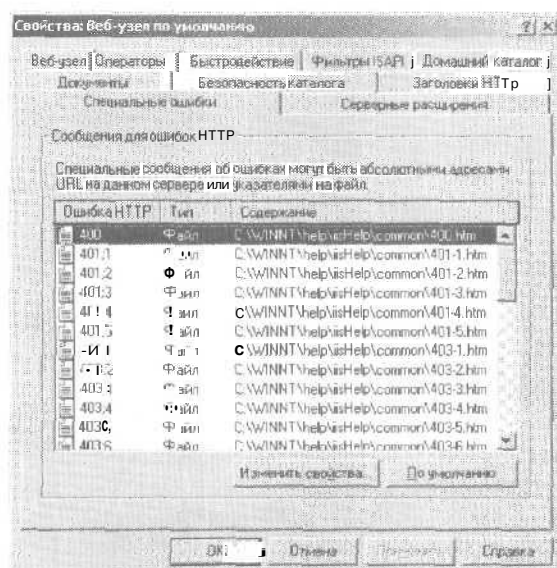


Рис. 4-5. Вкладка Custom Errors (Специальные ошибки) диалогового окна свойств Web-узла

3. Просмотрев параметры ошибок, щелкните ОК.

#### Изменение параметров сообщений об ошибках

Чтобы изменить параметры сообщений об ошибках, сделайте следующее.

1. В оснастке IIS щелкните нужный Web-узел, виртуальный каталог или папку правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите на вкладку Custom Errors (Специальные ошибки). Появится список стандартных HTTP-ошибок и методов их обработки.
3. Дважды щелкните запись ошибки или выделите ее и щелкните Edit Properties (Изменить свойства). Откроется диалоговое окно Error Mapping Properties (Свойства сопоставления ошибок) (рис. 4-6).
4. В списке Message Type (Тип сообщения) выберите метод обработки ошибки. Доступные методы зависят от типа ошибки, при этом клиенту возвращается:

- **Default** (По умолчанию) — сообщение об ошибке, созданное на основе информации из полей Error Code, Sub Error Code и Default Text;
- **File** (Файл) — указанный вами файл (введите полный путь к файлу или щелкните Browse (Обзор) и выберите нужный файл);
- **URL** (Адрес URL) — указанный URL (для файлов па других серверах следует ввести абсолютный URL, на текущем сервере — относительный URL).

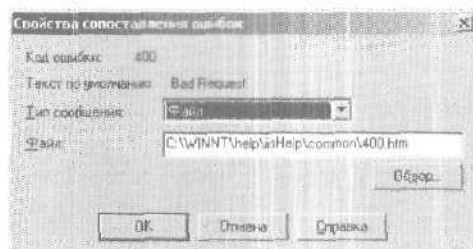


Рис. 4-6. Диалоговое окно Error Mapping Properties (Свойства сопоставления ошибок)

5. Дважды щелкните OK.

## Использование существующих и создание собственных типов MIME

У всех файлов, передаваемых между IIS и клиентским браузером, есть указатель типа данных, представленный типом MIME. IIS полностью поддерживает MIME.

### Что такое MIME

Вспомните, как осуществляется передача файлов по HTTP — многоцелевому протоколу для передачи файлов различных типов, видеофильмов кинематографического качества, звуковых стереозаписей, изображения с высоким разрешением и прочих видов мультимедийной информации. Передача мультимедийных файлов без стандарта MIME была бы невозможна. С помощью MIME Web-серверы определяют тип передаваемого объекта. Типы объектов указываются в HTTP-заголовке, который передается перед основными данными, что позволяет Web-клиенту соответствующим образом обрабатывать файл объекта.

Web-серверы задают тип MIME с помощью директивы `Content_Type`, которая является частью HTTP-заголовка, передаваемого клиентскому браузеру. Типы MIME делятся на несколько категорий, каждая из которых имеет связанный с ней основной *подтип*. Вот стандартные типы MIME:

- **application** — двоичные данные, могут быть выполнены или использованы с другим приложением;
- **audio** — звуковой файл, для воспроизведения требуется специальное устройство вывода;
- **image** — изображение, для просмотра требуется специальное устройство вывода;
- **message** — инкапсулированное почтовое сообщение;
- **multipart** — данные, состоящие из нескольких частей и, возможно, относящиеся к разным типам;
- **text** — текстовые данные, можно представить с помощью любого набора символов и языка форматирования;
- **video** — видеофайл, для просмотра требуется специальное устройство вывода;
- **x-world** — экспериментальный тип данных для файлов виртуального мира.

Существует три категории подтипов MIME:

- **основная** — типы данных, принятые для использования в качестве типов содержимого MIME;
- **дополнительная** — подтипы, официально приняты для использования в качестве типов содержимого MIME;
- **экспериментальная** — подтипы, пока не приняты официально для использования в качестве типов содержимого MIME.

Отличить экспериментальные подтипы очень легко — их название включает префикс «x-». Ниже перечислены основные типы и подтипы MIME (табл. 4-2).

Сотни типов MIME создаются с использованием сопоставлений «расширение файла — тип файла». Такие сопоставления позволяют службам IIS обрабатывать практически любые типы файлов, необходимые приложению или утилите на конечном компьютере. Если файл имеет неизвестное расширение, он передается с использованием типа MIME по умолчанию, подразумевающего, что файл содержит данные приложения. Обычно использование типа MIME по умолчанию

означает, что клиент не может обработать файл или запустить нужные для этого утилиты. Чтобы клиент корректно обработал файл нового типа, создайте сопоставление «расширение файла — тип файла».

Табл. 4-2. Основные типы MIME

Тип	Подтип	Описание
application	mac-binhex40	Двоичные данные в формате Macintosh
msword		Документ Microsoft Word
octet-stream		Двоичные данные, которые можно выполнить или использовать в другом приложении
pdf		Документ Acrobat PDF
postscript		Данные в формате Postscript
rtf		Документ RTF
x-compress		Данные, сжатые с использованием UNIX-утилиты compress
x-gzip		Данные, сжатые с использованием UNIX-утилиты gzip
x-tar		Данные заархивированные с использованием UNIX-утилиты Tar
x-zip-compressed		Данные, сжатые с использованием утилиты PKZip или WinZip
audio	basic	Звук в неопределенном формате
x-aiff		Звук в формате Apple AIFF
x-wav		Звук в формате Microsoft WAV
image	gif	Изображение в формате GIF
jpeg		Изображение в формате JPEG
tiff		Изображение в формате TIFF
Lext	html	Текст в формате HTML
plain		Простой текст без HTML-форматирования
video	mpeg	Видеоизображение в формате MPEG
quicktime		Видеоизображение в формате Apple QuickTime
x-msvideo		Видеоизображение в формате the Microsoft AVI
x-world	x-vrml	Файл VRML

Сопоставления типов MIME, заданные в основных свойствах, распространяются на все Web-узлы сервера. В диалоговом окне основных свойств можно изменять существующие, настраивать дополнительные и удалять ненужные типы MIME. При следующем запуске IIS изменения вступят в действие для всех Web-узлов. Кроме того, можно создавать дополнительные сопоставления типов MIME для отдельных узлов и папок. Они будут действовать только в пределах этих конкретных объектов.

#### Просмотр и настройка MIME-типов для всех Web-узлов сервера

Просмотреть или изменить параметры типов MIME для всех Web-узлов сервера можно так.

1. В оснастке IIS щелкните значок компьютера правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. В группе Computer MIME Map (Настройка типов MIME компьютера) щелкните Edit (Изменить). Откроется окно со списком имеющихся на компьютере типов MIME (рис. 4-7). Они действительны для всех Web-узлов сервера.

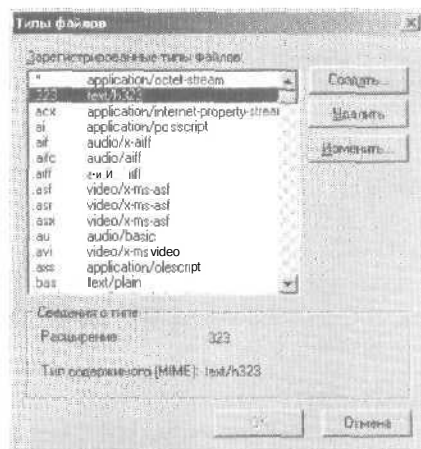


Рис. 4-7. Диалоговое окно File Types (Типы файлов)

3. Управление типами MIME осуществляется с помощью следующих кнопок:

- **New Type (Создать)** — добавление нового типа MIME; введите в поле Association Extension (Связанное расширение) расширение файла, например `.HTML`, затем в поле Content MIME Type [Тип содержимого (MIME)] — тип MIME, например `text/html`; щелкните OK;
- **Remove (Удалить)** — удаление типа MIME; выберите тип и щелкните Remove;
- **Edit (Изменить)** — изменение параметров типа MIME; выберите тип и щелкните Edit; затем в диалоговом окне File Type (Тип файла) введите новое расширение файла и тип содержимого MIME.

4. Дважды щелкните OK.

#### **Просмотр и настройка MIME-типов для отдельных узлов и папок**

На уровне узла или папки можно ограничить доступность пользовательских MIME-типов. При работе с параметрами MIME на этом уровне будут выводиться только значения, заданные вами.

Просмотреть или изменить параметры типов MIME на уровне узла или папки можно так.

1. В оснастке IIS щелкните нужный Web-узел правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке HTTP Headers (Заголовки HTTP) щелкните File Types (Типы файлов). Откроется одноименное диалоговое окно.
3. Управление типами MIME осуществляется с помощью следующих кнопок:
  - **New Type (Создать)** — добавление нового типа MIME: введите в поле Association Extension (Связанное расширение) расширение файла, например `.HTML`; затем в поле Content MIME Type [Тип содержимого (MIME)] — тип MIME, например `text/html`; щелкните OK.
  - **Remove (Удалить)** — удаление типа MIME: выберите тип и щелкните Remove (Удалить).

- **Edit (Изменить)** — изменение параметров типа MIME: выберите тип и щелкните **Edit (Изменить)**; затем в диалоговом окне **File Type (Тип файла)** введите новое расширение файла и тип содержимого MIME.

**4. Дважды щелкните ОК.**



**Примечание** Типы MIME, наследуемые из основных свойств Web-узла, не отображаются. Список включает только типы MIME, сконфигурированные для текущего узла или папки, хотя действуют оба набора типов MIME.

## Дополнительные советы по настройке

Для дополнительной настройки Web-узлов под управлением IIS можно также задействовать узлы обновлений, страницы перехода и перенаправление со страниц ошибок.

### Управление простоями с помощью узлов обновления

Узлы обновления позволяют управлять простоями и отображать альтернативное содержимое, если основные Web-узлы отключены от сети. Вместо отсутствующего содержимого и сообщения об ошибке пользователь увидит сообщение с информацией о причинах простоя и др.

Каждый опубликованный вами Web-узел должен включать узел обновления. Чтобы создать узел обновления, сделайте следующее.

1. Попросите Web-разработчиков создать отображаемую при простоях узлов Web-страницу, которая объясняла бы, что в данный момент осуществляется техническое обслуживание и скоро работа узла будет восстановлена. Можно также включить в код страницы ссылки на другие Web-узлы вашей компании.
2. В Windows Explorer (Проводник) создайте папку для узла обновления. Лучше расположить ее на локальном диске Web-сервера. Скопируйте в эту папку файлы содержимого, созданные Web-разработчиками.



**Совет** Рекомендую создать корневую папку, в которой будут храниться домашние каталоги, а затем — отдельную вложенную папку для каждого узла обновления. Например, корневую папку D:\UpdateSites и вложенные папки WWWUp-

date, ServicesUpdate и ProductsUpdate, где будут храниться файлы Web-узлов www.microsoft.com, services.microsoft.com и products.microsoft.com соответственно.

3. Запустите оснастку IIS и раскройте в левой панели узел нужного компьютера. Если компьютер не отображается, подключитесь к нему. Появится список Web-узлов, сконфигурированных на сервере.
4. Щелкните в дереве консоли значок компьютера и просмотрите сведения о заголовке узла, IP-адресе и портах основного узла, который требуется подменять при простое.
5. Создайте новый узел с этими конфигурационными параметрами. Назовите узел так, чтобы было понятно, что это узел обновления, но не запускайте его.
6. Настройте свойства нового узла. Для этого щелкните значок узла правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
7. На вкладке Documents (Документы) можно:
  - включить использование документов по умолчанию;
  - удалить существующие документы по умолчанию;
  - добавить документ по умолчанию и задать ему имя страницы, созданной на случай простоев.
8. Перейдите на вкладку Custom Errors (Специальные ошибки). Измените параметры обработки ошибок 400, 404 и 500: выберите в списке Message Type (Тип сообщения) пункт File (Файл) и введите путь к странице на случай простоев.
9. При необходимости измените другие свойства узла. Затем щелкните ОК, чтобы закрыть диалоговое окно свойств.

Чтобы запустить созданный узел обновления, сделайте так.

1. Прежде чем начать техническое обслуживание основного узла, остановите его из оснастки IIS и запустите соответствующий узел обновления,
2. Убедитесь, что этот узел работает, открыв его в Web-браузере. Если узел настроен правильно, при попытке открыть какой-либо файл клиент увидит страницу на случай простоев.



3. Выполните на основном узле технические работы. Завершив их, остановите узел обновления и запустите основной узел.
4. Убедитесь, что основной узел работает, открыв его в Web-браузере.

### Использование страниц переходов в рекламных целях

Страницы переходов перенаправляют пользователя к другим ресурсам и позволяют отслеживать переходы посетителей по рекламным баннерам, а также обращения к узлу, инициированные рекламой.

Страница перехода гарантирует, что клиент сначала посетит одну из страниц вашего узла и лишь затем перейдет к Web-узлу рекламодателя, разместившего баннер. Таким образом, вы можете отслеживать эффективность рекламы на своем Web-узле. Вот как это работает.

На одной из страниц Web-узла размещен рекламный баннер. Он ссылается на страницу перехода, которая размещена на том же узле. Пользователь щелкает баннер. Открывается страница перехода. Web-сервер отслеживает все обращения к ней и заносит их в файл журнала. Страница перехода отправляет пользователя к определенной странице Web-узла.

Страница перехода позволяет также оценить эффективность вашей рекламной кампании в Интернете. Это происходит так. В обычных рекламных материалах, например, брошюре, упоминается URL вашего Web-узла, точнее, URL соответствующей страницы перехода. Пользователь вводит URL в браузере и открывает страницу перехода. Web-сервер отслеживает все обращения к ней и заносит их в файл журнала. Страница перехода отправляет пользователя к странице вашего Web-узла, посвященной рекламируемому продукту.

Каждая страница перехода должна быть уникальной; можно также создать динамическую страницу, считывающую код из URL и отправляющую пользователя к соответствующей странице узла. Например, создать страницу перехода под названием JUMP.ASP, принимающую первый переданный сценарию параметр как код рекламы. Затем создается ссылка в баннере, включающая URL и соответствующий код рекламы, например JUMP.ASP?4408.

**Обработка ошибок 404 и предупреждение тупиков**

Пользователи очень не любят тупики, одним из которых является ошибка 404. Вместо вывода на дисплей бессмысленного сообщения «404 — File not found» можно заменить файл ошибок по умолчанию файлом, содержащим полезные сведения и ссылки или перенаправлять все ошибки 404 на домашнюю страницу вашего Web-узла. Это сделает навигацию по узлу более удобной и выгодно выделит его из множества ему подобных.

## Глава 5

# Управление безопасностью Web-сервера

В этой главе рассказывается об управлении безопасностью Web-сервера. Требования к безопасности Web-серверов отличаются от тех, что предъявляются к обычным серверам Microsoft Windows. Web-сервер предоставляет два уровня безопасности: на *уровне безопасности Windows* создают учетные записи пользователей, назначают права доступа к файлам и каталогам, а также настраивают политику безопасности, на *уровне безопасности IIS* настраивают разрешения доступа к содержимому, *компоненты* проверки подлинности, а также привилегии оператора.

Оба уровня можно использовать параллельно. Интегрированная модель безопасности позволит осуществлять проверку подлинности учетных записей пользователей и групп, а также обычную проверку подлинности на основе Интернета. Кроме того, многоуровневая система разрешений даст вам возможность определять права и разрешения на доступ к содержимому Web-узла. Чтобы пользователи обращались к файлам и папкам, соответствующим учетным записям должны быть назначены необходимые разрешения на уровне ОС. Затем нужно задать разрешения системы безопасности IIS, предоставляющие доступ к содержимому Web-узла.

Рассматриваемый в этой главе круг вопросов — вступление к дальнейшему обсуждению безопасности ресурсов IIS, включая File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) и Network News Transfer Protocol (NNTP). Материал по этой теме имеется и в следующих главах.

### Управление безопасностью Windows

Перед настройкой разрешений безопасности IIS задаются разрешения безопасности ОС Windows, которые позволяют создавать учетные записи пользователей и групп и управлять ими, задавать разрешения на доступ к файлам и папкам, настраивать политики групп.

### Учетные записи пользователей и групп

В Microsoft Windows 2000 имеются учетные записи пользователей и групп, определяющие их права и привилегии.

### Основные сведения об учетных записях пользователей и групп IIS

Учетные записи пользователей и групп можно создавать на уровне локального компьютера или на уровне домена. Локальные учетные записи специфичны для конкретного компьютера и не действуют на других компьютерах, если им не предоставить соответствующие разрешения. Доменные учетные записи действуют в пределах домена, т. е. с их помощью можно предоставить доступ ко всем его ресурсам.

- В разных ситуациях используются определенные типы учетных записей. Локальные учетные записи применяют, когда IIS-серверы не входят в домен или требуется ограничить доступ к определенному компьютеру. Доменные учетные записи следует задействовать, если серверы являются частью домена Windows, и пользователи должны обращаться ко всем его ресурсам.

Среди учетных записей IIS-серверов наиболее важны следующие.

- **LocalSystem** (Системная учетная запись) — по умолчанию все пользователи служб IIS и Indexing Service регистрируются в системе по этой учетной записи, благодаря чему службы могут взаимодействовать с ОС.
- **IUSR\_имя\_компьютера** — гостевая учетная запись для анонимного доступа к узлам Интернета. Если она отключена или заблокирована, работа анонимных пользователей со службами Интернета невозможна.
- **IWAM\_имя\_компьютера** — используется IIS для запуска приложений, выполняющихся вне процесса. Если она

отключена или заблокирована, запуск таких приложений невозможен.

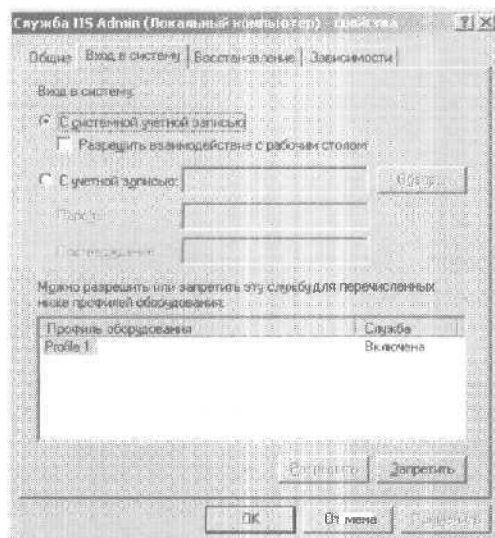
Учетные записи `IUSR_имя_компьютера` и `IWAM_имя_компьютера` относятся к группе Guests (Гости) и имеют запрещенный для изменения пользователем пароль с неограниченным сроком действия. Однако вы можете изменять параметры этих записей. В целях безопасности лучше сконфигурировать IIS под учетные записи, отличные от принятых по умолчанию. Кроме того, вы вправе создать дополнительные учетные записи.

#### Управление учетными записями служб MS и Indexing Service для входа в систему

Службы IIS и Indexing Service регистрируются на сервере под системной учетной записью, что позволяет им выполнять системные процессы и задачи. Изменять этот порядок, кроме специфических случаев или необходимости полного контроля над правами и привилегиями регистрационной учетной записи IIS, не следует. Чтобы назначить службам IIS и Indexing Server другую учетную запись для входа в систему, сделайте так.

1. Раскройте меню `Start\Programs\Administrative Tools` (Пуск\Программы\Администрирование) и выберите `Computer Management` (Управление компьютером).
2. В консоли `Computer Management` подключитесь к нужному компьютеру.
3. Раскройте узел `Services And Applications` (Службы и приложения), затем щелкните значок `Services` (Службы).
4. Щелкните интересующую вас службу правой кнопкой и выберите в контекстном меню команду `Properties` (Свойства).
5. Перейдите на вкладку `Log On` (Вход в систему) (рис. 5-1).
6. Щелкните переключатель `Local System Account` (С системной учетной записью), чтобы служба регистрировалась в системе по системной учетной записи (как и происходит по умолчанию для большинства служб).
7. Щелкните `This Account` (С учетной записью), чтобы служба регистрировалась под конкретной учетной записью. Не забудьте ввести имя и пароль пользователя в

соответствующие поля. Для поиска учетной записи щелкните кнопку Browse (Обзор).



**Рис. 5-1.** Выбор регистрационной учетной записи службы на вкладке Log On (Вход в систему)

8. Щелкните ОК.



**Примечание** Если системная учетная запись не используется, предоставьте права и разрешения на вход в систему своей учетной записи. Подробнее — в главе 3 книги «Microsoft Windows 2000. Справочник администратора».

#### Управление гостевой учетной записью Интернета

Управлять гостевой учетной записью Интернета можно как на уровне безопасности IIS, так и на уровне безопасности Windows.

На уровне безопасности IIS задают учетную запись для анонимного доступа. Обычно управление анонимным доступом осуществляется на уровне узла, и все вложенные файлы и папки наследуют параметры анонимного доступа к этому узлу. Но вы можете переопределить параметры отдельных файлов и папок.

На этом же уровне указывают, кто управляет паролем учетной записи анонимного пользователя: вы или IIS. Вам нужно лишь синхронизировать пароли учетных записей анонимных пользователей, которые определены локально. Если учетная запись задана на другом компьютере, паролем необходимо управлять самостоятельно.

Чтобы изменить параметры учетной записи для анонимного доступа к Web-узлам и папкам Web-сервера, сделайте так.

1. В оснастке Internet Information Services щелкните правой кнопкой значок нужного компьютера и выберите в контекстном меню команду Properties (Свойства). Откроется диалоговое окно свойств.
2. Из раскрывающегося списка Master Properties (Основные свойства) выберите WWW Service (WWW-служба) и щелкните Edit (Изменить). Откроется диалоговое окно WWW Service Master Properties (Основные свойства WWW-службы) для данного компьютера.
3. Перейдите на вкладку Directory Security (Безопасность каталога) или File Security (Безопасность файла) и в группе Anonymous Access And Authentication Control (Анонимный доступ и проверка подлинности) щелкните Edit.



**Примечание** Если разрешен анонимный доступ, указывать имя пользователя и пароль для работы с ресурсом не требуется. IIS автоматически регистрирует пользователя под учетной записью для анонимного доступа к данному ресурсу. Если анонимный доступ запрещен, пользователю придется указать свое имя и пароль. Чтобы разрешить анонимный доступ, пометьте флажок Anonymous Access (Анонимный доступ). Но вы должны быть твердо уверены, что ресурсу не требуется защита.

4. В поле Username (Пользователь) указывают учетную запись для анонимного доступа к ресурсу. Имя учетной записи можно ввести вручную или щелкнуть кнопку Browse (Обзор) и выбрать его в диалоговом окне Select User (Выбор: Пользователь).
5. Флажок Allow IIS To Control Password (Разрешить управление паролем из IIS) определяет, разрешено ли управ-

ление паролем учетной записи анонимного доступа из IIS. Рекомендуется, чтобы учетной записью анонимного доступа, определенной на локальном компьютере, управляли службы IIS. Если вы согласны с этим, пометьте данный флажок, если нет -- снимите его и введите пароль учетной записи для анонимного доступа.

6. Трижды щелкните ОК, чтобы сохранить сделанные изменения,

Конфигурация учетной записи анонимного пользователя на уровне узла, папки или файла **изменяется так**,

1. В оснастке Internet Information Services щелкните правой кнопкой нужный Web-узел, папку или файл, и выберите в контекстном меню команду Properties (Свойства).
2. Выполните пп. 3-6 предыдущей инструкции.

На уровне безопасности Windows выполняются все прочие задачи управления учетными записями, включая активизацию и отключение учетных записей, снятие блокировки с заблокированной учетной записи, изменение состава групп.

Подробнее о работе с учетными записями пользователей и групп см. главы 7, 8, 9 книги «Microsoft Windows 2000. Справочник администратора».

#### **Управление учетными записями Web-приложений**

Управление учетными записями Web-приложений осуществляется только на уровне безопасности IIS и на уровне безопасности Windows. На уровне безопасности IIS из оснастки Component Services (Службы компонентов) указывают учетную запись для приложений, выполняющихся в групповом потоке, а также для изолированных приложений. Приложения первого типа используют одну, а приложения второго типа — разные учетные записи.

Оснастка Component Services (Службы компонентов) открывается так.

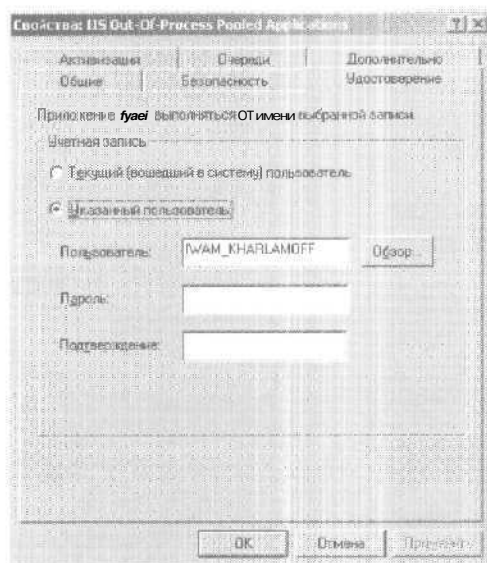
1. Раскройте меню Start (Пуск) и выберите Run (Выполнить). Откроется одноименное диалоговое окно.
2. В поле Open (Открыть) введите MMC и щелкните ОК. Запустится консоль управления MMC.



3. В меню Console (Консоль) консоли MMC выберите команду Add/Remove Snap-In (Добавить/удалить оснастку). Откроется одноименное диалоговое окно.
4. На вкладке Standalone (Изолированная оснастка) щелкните Add (Добавить).
5. В диалоговом окне Add Standalone Snap-In (Добавить изолированную оснастку) выберите Component Services (Службы компонентов) и щелкните Add (Добавить).
6. Щелкните Close (Заккрыть) и затем ОК, чтобы закрыть диалоговое окно Add Standalone Snap-In (Добавить изолированную оснастку).

Для управления учетной записью приложений, выполняющихся в групповом потоке, сделайте следующее.

1. Раскройте узел Component Services (Службы компонентов) — отобразится вложенный узел Computers (Компьютеры).
2. Чтобы подключиться к удаленному компьютеру, щелкните узел Computers правой кнопкой и выберите в контекстном меню команду New\Computer (Создать\Компьютер). Введите имя компьютера и щелкните ОК. Если имя компьютера неизвестно, вызовите диалоговое окно Select Computer (Выбор: Компьютер), щелкнув кнопку Browse (Обзор).
3. Раскройте узел компьютера и щелкните папку COM+ Applications (Приложения COM+).
4. Щелкните правой кнопкой узел IIS Out-Of-Process Pooled Applications, выберите в контекстном меню команду Properties (Свойства) и перейдите на вкладку Identity (Удостоверение).
5. Щелкните переключатель This User (Указанный пользователь) (рис. 5-2) и затем в поле User (Пользователь) введите имя требуемой учетной записи. Можно также щелкнуть кнопку Browse (Обзор) и выбрать учетную запись в диалоговом окне Select User (Выбор: Пользователь).
6. В полях Password (Пароль) и Confirm Password (Подтверждение) введите пароль учетной записи.
7. Щелкните ОК.



**Рис. 5-2.** Выбор учетной записи Web-приложения в оснастке Component Services (Службы компонентов)

Управление учетными записями изолированных приложений осуществляется почти так же. Единственное отличие: вы будете работать не с узлом IIS Out-Of-Process Pooled Applications, а с записью конкретного изолированного приложения. Все записи изолированных приложений в метабазе начинаются с префикса IIS-. Скажем, запись изолированного приложения, созданного в папке /Apps/Data Web-узла по умолчанию, его в метабазе будет называться IIS-{Default Web Site//Root/Apps/Data}-

На уровне безопасности Windows выполняются все прочие задачи управления учетными записями, включая активизацию и отключение учетных записей, снятие блокировки с заблокированной учетной записи, изменение состава групп.

Подробнее о работе с учетными записями пользователей и групп см. главы 7, 8, 9 книги «Microsoft Windows 2000. Справочник администратора».

## Использование разрешений доступа к файлам и папкам

Все папки и файлы IIS могут иметь разные разрешения доступа, назначенные на уровне безопасности Windows.

### Основные разрешения доступа к файлам и папкам

Основные разрешения доступа к файлам и папкам состоят из набора специальных разрешений доступа, например, на просмотр содержимого папки и на выполнение файла (табл. 5-1). Для тонкого управления доступом к файлам или папкам можно выборочно назначать учетным записям отдельные специальные разрешения. Подробнее см. главу 13 книги «Microsoft Windows 2000. Справочник администратора».

**Табл. 5-1.** Основные разрешения доступа к файлам и папкам Windows 2000

	Разрешает (для папок)	Разрешает (для файлов)
Read (Чтение)	Просмотр файлов и вложенных папок	Просмотр или доступ к содержимому файла
Write (Запись)	Добавление файлов и вложенных папок	Запись в файл
Read & Execute (Чтение и выполнение)	Просмотр файлов и вложенных папок, а также выполнение файлов; наследуется файлами и папками	Просмотр и доступ к содержимому файла, а также его выполнение
List Folder Contents (Просмотр содержимого папки)	Просмотр файлов и вложенных папок, а также выполнение файлов; наследуется только папками	—
Modify (Изменить)	Чтение и запись файлов и вложенных папок, удаление папки	Чтение, запись и удаление файла
Full Control (Полный доступ)	Чтение, запись, изменение и удаление файлов и вложенных папок	Чтение, запись, изменение и удаление файла

Помните, что:

- для выполнения сценариев необходимо только разрешение Read (Чтение), разрешение Execute (Выполнение) распространяется только на исполнимые файлы;

- для доступа к ярлыку и файлу, на который он ссылается, требуется разрешение **Read**;
- пользователь, обладающий разрешением на запись файла и не имеющий разрешения на его удаление, может стереть содержимое этого файла;
- пользователь с полным доступом к папке может удалять файлы в ней независимо от их разрешений.

При настройке доступа к файлам и папкам IIS использует следующие учетные записи, предоставляющие:

- **Administrators** (Администраторы) — административный доступ к ресурсам IIS;
- **Creator Owner** (Создатель-владелец) — создателю ресурса доступ к этому ресурсу;
- **System** (Система) — локальной системе доступ к ресурсу;
- **Everyone** (Все) — интерактивным, удаленным, сетевым и аутентифицированным пользователям доступ к содержимому (IIS использует эту группу, если Web-узел входит в домен Windows);
- **Users** (Пользователи) — указанным учетным записям пользователей (включая гостевую учетную запись Интернета и учетные записи Web-приложений) доступ к ресурсу.

Если назначить любому из пользователей и групп разрешение **Read** (Чтение), все клиенты с доступом к данному узлу Интернета или интрасети смогут просматривать файлы и папки. Чтобы ограничить доступ к определенным файлам и папкам, выборочно задайте соответствующие разрешения пользователям и включите аутентифицированный доступ к ресурсам. При аутентифицированном доступе IIS проверяет подлинность учетной записи пользователя и на основе разрешений Windows определяет, какие файлы и папки ему доступны.

Вот какие разрешения доступа можно назначить папкам и файлам IIS (табл. 5-2):

**Табл. 5-2.** Рекомендации по назначению разрешений доступа различным типам содержимого

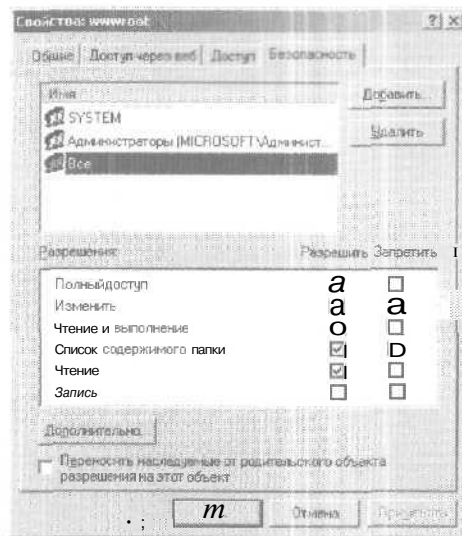
Тип файла	Расширение файла	Разрешения
Сценарии CGI и исполнимые файлы	.exe, .DLL, .cmd	Everyone (Execute) Administrators (Full Control) System (Full Control)
Динамическое содержимое	.asp, .vbs, .js, .pl	Everyone (Read) Administrators (Full Control) System (Full Control)
Файлы включений	.inc, .shtm, .shtml, .stm	Everyone (Read) Administrators (Full Control) System (Full Control)
Статичное содержимое	.Lxt, .rtf, .gif, .jpg, .jpeg, .htm, .html, .doc, .ppt, .xls	Everyone (Read) Administrators (Full Control) System (Full Control)

Лучше не назначать разрешения отдельным файлам, а помещать однотипное содержимое в один каталог. Например, для Web-узла со сценариями, статичным и динамическим содержимым можно создать подпапки WebScripts, WebStatic и WebDynamic, поместить в них файлы соответствующего типа, а затем назначить папкам нужные разрешения.

#### Просмотр разрешений доступа к файлам и папкам

Разрешения доступа к файлам и папкам можно просмотреть.

1. В Windows Explorer (Проводник) щелкните правой кнопкой файл или папку.
2. В контекстном меню выберите команду Properties (Свойства). Затем в открывшемся диалоговом окне перейдите на вкладку Security (Безопасность) (рис. 5-3).
3. В списке Name (Имя) выберите имя пользователя, контакт, компьютер или группу. Флажки разрешений, выделенные серым цветом, означают, что разрешения наследуются от родительского объекта.



**Рис. 5-3.** Вкладка Security (Безопасность) диалогового окна Properties (Свойства)

### Назначение разрешений доступа к файлам и папкам

Разрешения доступа к файлам и папкам назначаются так.

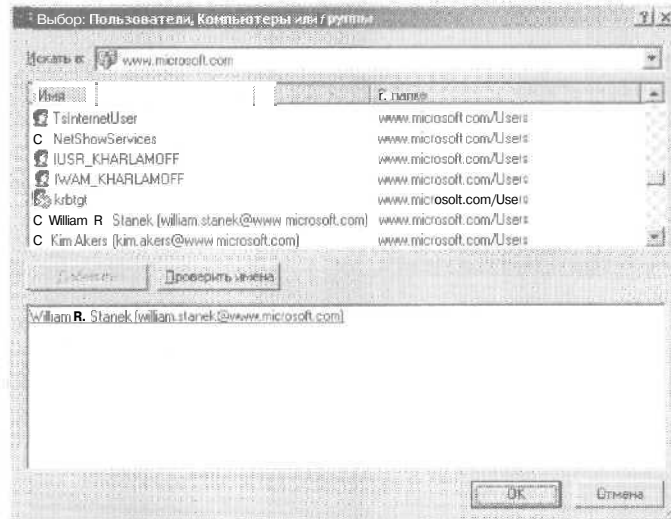
1. В Windows Explorer (Проводник) щелкните правой кнопкой файл или папку.
2. В контекстном меню выберите команду Properties (Свойства). Затем в открывшемся диалоговом окне перейдите на вкладку Security (Безопасность).
3. В списке Name перечислены пользователи или группы, обладающие доступом к файлу (папке). Чтобы изменить разрешения этих пользователей и групп, выберите пользователя или группу и внесите необходимые изменения в список Permissions.



**Примечание** Наследуемые права выделены серым цветом. Чтобы переопределить их, пометьте соответствующий флажок.

4. Щелкните Add, чтобы настроить разрешения на доступ для дополнительных пользователей, контактов, компью-

геров и групп. Откроется диалоговое окно Select Users, Computers, Or Groups (рис. 5-4).



**Рис. 5-4.** Выбор пользователей, компьютеров и групп, которым предоставляются разрешения на доступ

5. Выберите пользователей, компьютеры или группы:
  - список Look In (Искать в) содержит список доменов и прочих ресурсов, учетные записи которых можно просмотреть; для просмотра учетных записей всех ресурсов и доменов выберите Entire Directory (Весь каталог);
  - в поле Name (Имя) отображаются доступные учетные записи текущего домена или ресурса;
  - кнопка Add (Добавить) добавляет выбранные учетные записи в список;
  - кнопка Check Names (Проверить имена) проверяет имена пользователей и групп (это полезно, если вы вводили имена вручную и хотите убедиться в их доступности).
- fi. В списке Name выберите имя пользователя, компьютер или группу, и затем назначьте разрешения в поле Permis-

sions. Повторите эту операцию для других пользователей, компьютеров или групп.

7. Завершив назначать разрешения, щелкните ОК.

### Работа с групповыми политиками

Групповые политики — еще один аспект безопасности Windows, понимание которого важно для успешной работы. Они позволяют автоматизировать ключевые задачи безопасности и эффективнее управлять ресурсами ИС.

#### Основы групповых политик

Политика — это набор правил, распространяющихся на компьютеры и пользователей. Групповые политики обеспечивают централизованное управление привилегиями, разрешениями и возможностями пользователей и компьютеров. Компьютеры могут состоять в более крупных группах, и тогда на них распространяется действие нескольких политик. Порядок применения политик чрезвычайно важен и определяет, какие правила будут действовать, а какие — нет.

При наличии нескольких политик они применяются в следующем порядке.

1. Политики Microsoft Windows NT 4.0 из файлов NTCONFIG.POL.
2. Локальные групповые политики, распространяющиеся только на локальный компьютер.
9. Групповые политики уровня узла, влияющие на все компьютеры конкретного узла, который может включать несколько доменов.
3. Политики уровня домена, распространяющиеся на все компьютеры в определенном домене.
4. Политики организационных единиц (organizational unit, OU), влияющие на все компьютеры в OU.
5. Политики дочерних организационных единиц, распространяющиеся на все компьютеры в каком-либо подразделении OU.

В результате последовательного применения правила предыдущих политик переопределяются правилами текущей политики. Например, приоритет доменной политики выше приоритета локальной групповой политики. Исключения позво-



ляют блокировать, переопределять и отключать параметры политик.

Параметры политик делятся на две большие категории — пользовательские и компьютерные. Компьютерные параметры применяются при загрузке системы, пользовательские — при входе в систему. Для управления политиками служит оснастка Group Policy (Групповые политики).

1. Для узлов запустите оснастку Group Policy из консоли Active Directory Sites And Services (Active Directory — сайты и службы). Откройте консоль Active Directory Sites And Services.
2. Для доменов и организационных единиц запустите оснастку Group Policy из консоли Active Directory Users And Computers (Active Directory — пользователи и компьютеры). Откройте консоль Active Directory Users And Computers.
3. В корне консоли щелкните узел, домен или организационную единицу правой кнопкой и выберите в контекстном меню команду Properties (Свойства). Откроется одноименное диалоговое окно.
4. Перейдите на вкладку Group Policy (Групповая политика). В списке Group Policy Object Links (Ссылки текущего объекта групповой политики) перечислены существующие политики (рис. 5-5).
5. Для создания новой или редактирования уже существующей политики щелкните New (Создать).
6. Для редактирования существующей политики выберите ее и щелкните Edit (Изменить).
7. Для изменения приоритета политики измените ее положение в списке Group Policy Object Links (Ссылки текущего объекта групповой политики), пользуясь кнопками Up (Вверх) и Down (Вниз).

Для управления локальными групповыми политиками отдельного компьютера сделайте следующее.

1. Раскройте меню Start (Пуск) и выберите команду Run (Выполнить). Откроется одноименное диалоговое окно.
2. В поле Open введите MMC и щелкните ОК. Откроется консоль Microsoft Management Console (MMC).



Рис. 5-5. Создание и редактирование политик на вкладке Group Policy (Групповая политика)

3. В меню Console (Консоль) выберите команду Add/Remove Snap-In (Добавить/удалить оснастку). Откроется одноименное диалоговое окно.
4. На вкладке Standalone щелкните Add (Добавить).
5. В диалоговом окне Add Snap-In (Изолированная оснастка) выберите Group Policy (Групповая политика) и затем щелкните Add (Добавить). Откроется диалоговое окно Select Group Policy Object (Выбор объекта групповой политики).
6. Выберите Local Computer (Локальный компьютер) для редактирования групповой политики локального компьютера или щелкните Browse, чтобы выбрать локальную политику другого компьютера.
7. Щелкните Finish (Готово) и затем — Close (Заккрыть).
8. Щелкните OK. Теперь вы можете управлять локальной политикой выбранного компьютера.

Групповые политики паролей, блокировки учетных записей и аудита — основа безопасности вашего Web-узла. Советую:

- задать минимальный срок действия пароля для всех учетных записей: например, 2-3 дня;
- задать максимальный срок действия пароля для всех учетных записей, например 30 дней;
- задать минимальную длину пароля: например, 8 символов;
- использовать безопасные пароли, активизировав политику, отвечающую за их сложность;
- включить журнал паролей и хранить в нем не менее пяти паролей.

Рекомендации по блокировке учетных записей таковы:

- включите счетчик блокировки — обычно учетную запись блокируют после пяти неудачных попыток входа в систему;
- задайте длительность блокировки учетной записи — лучше блокировать учетные записи на неопределенный срок;
- сбрасывайте счетчик блокировки через 30-60 минут.

Рекомендую вести аудит:

- успешного и неудачного завершения системных событий;
- успешного и неудачного завершения событий входа в систему;
- неудачных попыток доступа к объектам;
- успешных и неудачных попыток редактирования политики;
- успешных и неудачных попыток управления учетными записями;
- успешных и неудачных попыток входа в систему.

#### Настройка политик учетных записей для IIS-серверов

Подробнее об управлении этими групповыми политиками рассказывается в главе 4 книги «Microsoft Windows 2000. Справочник администратора», а мы поговорим об этом вкратце. Политики учетных записей настраиваются так.

1. Раскройте узел Computer Configuration\Windows Settings\Security Settings\Account Policies (Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики учетных записей) и выберите контейнер групповой политики. Для управления политика-

ми учетных записей доступны узлы Password Policy (Политика паролей), Account Lockout Policy (Политика блокировки учетной записи) и Kerberos Policy (Политика Kerberos) (рис. 5-6).

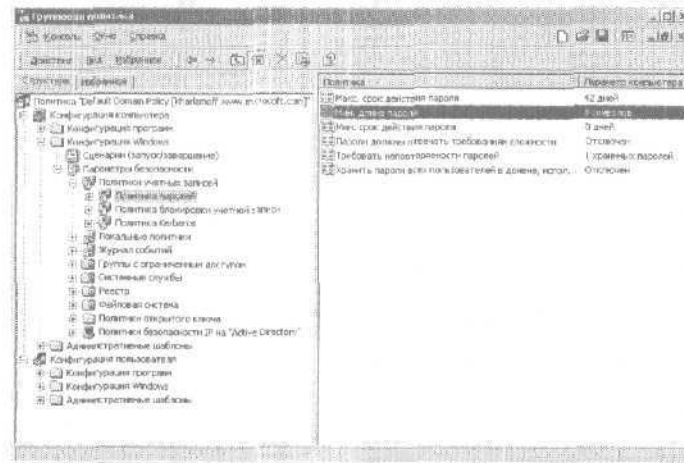


Рис. 5-6. Окно оснастки Group Policy (Групповая политика)

2. Чтобы настроить политику, дважды щелкните ее значок. Либо щелкните значок правой кнопкой и выберите в контекстном меню команду Security (Безопасность). Откроется диалоговое окно свойств данной политики (рис. 5-7), отображающее параметры текущей политики компьютера, изменить которые нельзя, а также изменяемые параметры локальной политики. Пропустите оставшиеся этапы — они касаются только глобальных групповых политик.

Для узла, домена или организационного подразделения диалоговое окно свойств имеет иной вид (рис. 5-8).

Политика может быть определена или не определена, т. е. применяться или нет на данном компьютере. Политики, не определенные в текущем контейнере, могут наследоваться из другого контейнера. Используется ли политика, показывает флажок Define This Policy Setting (Определить следующий параметр политики).

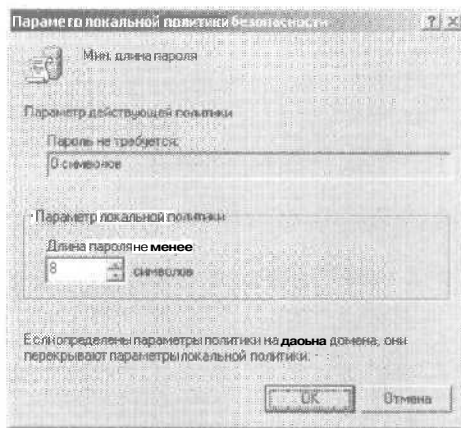


Рис. 5-7. Диалоговое окно свойств локальной политики

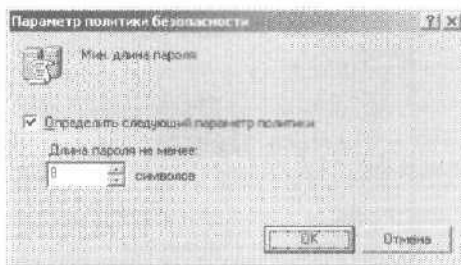


Рис. 5-8. Диалоговое окно свойств глобальной групповой политики

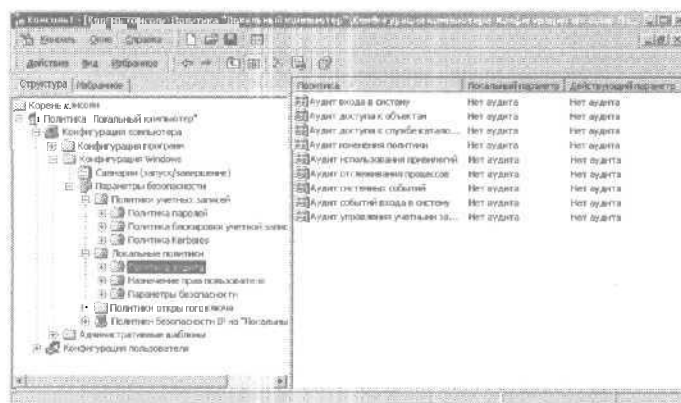
Политики могут иметь дополнительные конфигурационные параметры: например, переключатели *Enabled* (политика включена) и *Disabled* (политика отключена).

#### Настройка политик аудита

Аудит — лучший способ отслеживать события ИС-сервера. Он позволяет собирать сведения об использовании ресурсов, например, о доступе к файлам, входе в систему и изменении ее конфигурации. Записи обо всех отслеживаемых действиях заносятся в системный журнал безопасности, который можно просмотреть с помощью утилиты Event Viewer (Просмотр событий).

Политики аудита настраиваются так.

1. Раскройте узел Computer Configuration\Windows Settings\Security Settings\Local Policies (Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики) и выберите контейнер Audit Policy (Политика аудита) (рис. 5-9).



**Рис. 5-9.** Узел Audit Policy (Политика аудита) консоли Group Policy (Групповая политика)

- I. Теперь можно настроить параметры аудита, которые отслеживают:
  - **Audit Account Logon Events (Аудит событий входа в систему)** — события, связанные со входом и выходом пользователя из системы;
  - \* **Audit Account Management (Аудит управления учетными записями)** — управление учетными записями (события генерируются при создании, изменении или удалении учетных записей пользователей, компьютеров и групп);
  - **Audit Directory Service Access (Аудит доступа к службе каталогов)** — доступ к Active Directory (события генерируются при обращении пользователей и компьютеров к Active Directory);
  - \* **Audit Logon Events (Аудит входа в систему)** — события, связанные со входом, выходом и удаленным подключением пользователя к компьютерам сети;

- **Audit Object Access (Аудит доступа к объектам)** – доступ к файлам, каталогам, общим ресурсам, принтерам и объектам Active Directory;
  - **Audit Policy Change (Аудит изменения политики)** – изменения прав пользователей, аудита и доверительных отношений;
  - **Audit Privilege Use (Аудит использования привилегий)** — использование разрешений, например, на резервное копирование файлов и каталогов (вход и вход из системы не отслеживаются);
  - **Audit Process Tracking (Аудит отслеживания процессов)** — системные процессы и используемые ими ресурсы;
  - **Audit System Events (Аудит системных событий)** — запуск, завершение работы и перезагрузку системы, а также действия, влияющие на безопасность или журнал безопасности.
3. Чтобы настроить политику, дважды щелкните ее значок. Можно также щелкнуть значок политик правой кнопкой и выбрать в контекстном меню команду Security (Безопасность). Откроется диалоговое окно свойств данной политики.
  4. Щелкните переключатель Define These Policy Settings и затем пометьте флажок Success (Успех), флажок Failure (Отказ) или оба этих флажка.
  5. Завершив настройку, щелкните OK.

## Управление безопасностью IIS

Настроив систему безопасности Windows, сконфигурируйте в системе безопасности IIS;

- разрешения на доступ к Web-серверу и выполнение содержимого;
- протокол WebDAV;
- методы проверки подлинности;
  - доступ по IP-адресам или доменным именам Интернета;
  - разрешения операторов Web-узлов.

### Настройка разрешений Web-сервера

Помимо разрешений безопасности Windows, узлы, папки и файлы обладают разрешениями IIS, которые **одинаковы** для всех пользователей. Это означает, что **назначить** разные права доступа разным **пользователям** на уровне Web-узла нельзя. Однако вы можете создать защищенные области Web-узла и управлять доступом к ним с **помощью** разрешений файловой системы Windows.

#### Основы разрешений Web-сервера

Разрешения, назначаемые Web-содержимому, применяются **совместно** с методами проверки подлинности и ограничениями доступа, уже используемыми для **ресурса**. Это значит, что для выполнения пользовательские запросы должны соответствовать требованиям подсистемы **разрешений**, подсистемы проверки подлинности и подсистемы контроля доступа. Все папки и файлы узла **наследуют** заданные на уровне узла разрешения, но для **отдельных** файлов и папок эти разрешения можно **переопределить**.

Разрешения Web-сервера также **определяют** круг действий, которые можно выполнять по протоколу Web Distributed Authoring and Versioning (WebDAV). WebDAV позволяет удаленным пользователям **публиковать** и блокировать ресурсы, а также управлять ими на Web-узле через HTTP-соединение. Windows 2000, Microsoft Office 2000, Internet Explorer 5.0 и более **новые** версии этих продуктов поддерживают WebDAV. Если у вас есть приложения с **поддержкой** WebDAV, можно посредством разрешений Web-сервера определить круг допустимых действий этих приложений и их пользователей. Подробнее об этом см. раздел «Настройка протокола WebDAV» данной главы.

Разрешения Web-сервера можно задать двумя способами.

*Глобальные разрешения* задают в диалоговом окне WWW Server Master Properties (Основные свойства WWW-службы). При настройке разрешений Web-сервера надо указать, как эти свойства наследуются. Если вы изменили разрешения и возник конфликт с существующими параметрами сайта или папки, IIS предложит переопределить разрешения сайта (папки) и **заменить** их глобальными разрешениями.



После переопределения на сайт (папку) и его (ее) содержимое будут распространяться глобальные разрешения; если этого не сделать — старые разрешения сайта или папки.

*Локальные разрешения* задаются на уровне сайта, папки или файла. Как и глобальные, локальные разрешения сайтов и узлов тоже могут наследоваться. Поэтому, если при изменении разрешения возникнет конфликт с существующими параметрами сайта или папки, IIS предложит переопределить разрешения сайта (папки) и заменить их глобальными разрешениями. После переопределения на сайт (папку) и его (ее) содержимое будут распространяться глобальные разрешения; если этого не сделать — старые разрешения сайта или папки.

Поскольку IIS управляет наследованием разрешений на уровне узла, папка верхнего уровня и прочие папки сайта рассматриваются как отдельные узлы. Изменения разрешений узла сайта распространяются только на корневую папку и ее файлы. На вложенные папки, если этого специально не указать, они распространяться не будут.

#### **Настройка глобальных разрешений Web-сервера**

Для управления глобальными разрешениями Web-сервера сделайте так.

1. В оснастке Internet Information Services щелкните правой кнопкой значок нужного компьютера и выберите в контекстном меню команду Properties (Свойства). Откроется диалоговое окно свойств.
2. Из списка Master Properties (Основные свойства) выберите WWW Service (WWW-служба) и щелкните Edit (Изменить). Откроется диалоговое окно WWW Service Master Properties (Основные свойства WWW-службы) для данного компьютера.
3. Перейдите на вкладку Home Directory (Домашний каталог) (рис. 5-10) и задайте разрешения Web-сервера, которые будут наследоваться сайтами и папками, с помощью следующих флажков:
  - Directory Browsing (Обзор каталогов) позволяет пользователю просматривать список файлов и вложенных папок данной папки;

- **Index This Resource (Индексация каталога)** позволяет службе Index Service индексировать данный ресурс, благодаря чему пользователи могут искать нужную информацию по ключевым словам;
- **Log Visits (Запись в журнал)** используется совместно с системой аудита сервера для регистрации обращений к ресурсу;
- **Read (Чтение)** позволяет пользователю обращаться к каталогу или просматривать и выводить содержимое файла;
- **Script Source Access (Доступ к тексту сценария)** предоставляет пользователям доступ к исходному коду, включая ASP-сценарии; если также помечен флажок Read (Чтение), пользователи могут считывать файл исходного кода, а при наличии разрешения Write (Запись) — изменять его;

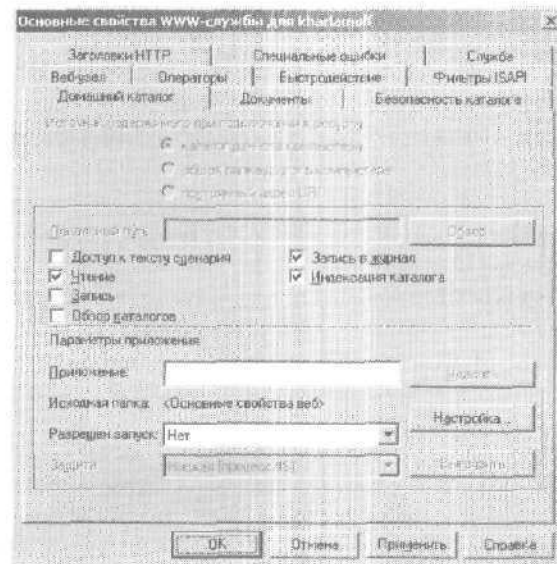


Рис. 5-10. Настройка разрешений Web-сервера



Внимание! Назначая разрешение Script Source Access на общедоступных из Интернета производственных серверах, будьте особенно осторожны. Такое решение позволит всем клиентам читать исходный код сценариев и может сделать сервер уязвимым для атак злоумышленников. Данное разрешение рекомендуется назначать лишь каталогу, требующему прохождения проверки подлинности.

- **Write (Запись)** позволяет пользователю изменять содержимое файла или создавать и публиковать файлы каталога.



Внимание! Разрешение Write следует назначать ограниченному числу ресурсов. По возможности создайте специальные каталоги для перезаписываемых файлов или назначайте это разрешение отдельным файлам, а не целым каталогам. Для выполнения приложений нужно назначить разрешение Read всем используемым ими файлам или сайту (папке), где эти файлы хранятся. Если приложение записывает содержимое в один из файлов сайта, назначьте также разрешение Write (но лишь для отдельного файла или каталога).

4. Если выбранный ресурс является частью IIS-приложения, можно в списке Execute Permission (Разрешен запуск) задать уровень выполнения:
  - None (Нет) — доступ только к статичным файлам: например, HTML- и GIF-;
  - Scripts Only (Только сценарии) — выполняются только сценарии: например ASP-;
  - Scripts And Executables (Сценарии и исполняемые файлы) - просматриваются и выполняются все файлы.
5. Щелкните Apply (Применить). Прежде чем применить изменения, IIS проверяет текущие параметры всех Web-узлов и их папок. Если на Web-узле действуют другие разрешения, открывается диалоговое окно Inheritance Overrides (Переопределение наследования). Отметьте в нем узлы, к которым следует применить новые разрешения, и щелкните ОК.

**Настройка локальных разрешений Web-сервера**

Чтобы назначить содержимому Web-узла, каталога или файла права доступа, сделайте следующее.

1. В оснастке Internet Information Services щелкните правой кнопкой значок нужного компьютера и выберите в контекстном меню команду Properties (Свойства). Откроется диалоговое окно свойств.
2. Перейдите на вкладку Home Directory (Домашний каталог), Directory (Каталог) (рис. 5-11) или Virtual Directory (Виртуальный каталог) и задайте разрешения Web-сервера, которые будут наследоваться сайтами и папками, с помощью следующих флажков:

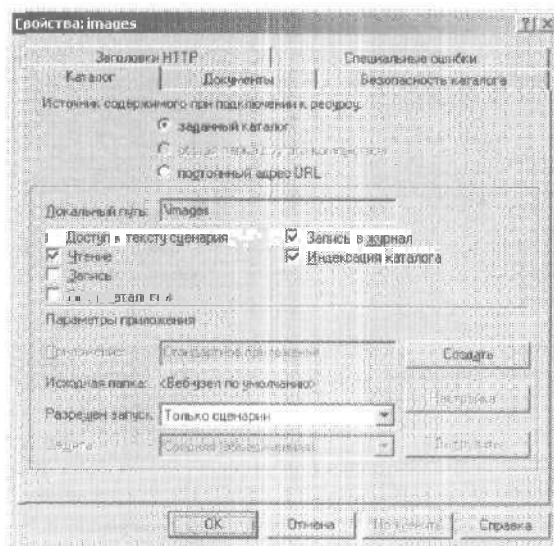


Рис. 5-11. Настройка разрешений Web-сервера

- Directory Browsing (Обзор каталогов) позволяет пользователю просматривать список файлов и вложенных папок данной папки;
- Index This Resource (Индексация каталога) позволяет службе Index Service индексировать данный ресурс, благодаря чему пользователи могут искать нужную информацию по ключевым словам;

- Log Visits (Запись в журнал) используется совместно с системой аудита сервера для регистрации обращений к ресурсу;
- Read (Чтение) позволяет пользователю обращаться к каталогу или просматривать и выводить содержимое файла;
- Script Source Access (Доступ к тексту сценария) предоставляет пользователям доступ к исходному коду, включая ASP-сценарии; если также помечен флажок Read (Чтение), пользователи могут считывать файл исходного кода, а при наличии разрешения Write (Запись) — изменять его;



**Внимание!** Назначая разрешение Script Source Access на общедоступных из Интернета производственных серверах, будьте особенно осторожны. Такое решение позволит всем клиентам читать исходный код сценариев и может сделать сервер уязвимым для атак злоумышленников. Данное разрешение рекомендуется назначать лишь каталогу, требующему прохождения проверки на подлинность.

- Write (Запись) позволяет пользователю изменять содержимое файла или создавать и публиковать файлы каталога.



**Внимание!** Разрешение Write следует назначать ограниченному числу ресурсов. По возможности создайте специальные каталоги для перезаписываемых файлов или назначьте это разрешение отдельным файлам, а не целым каталогам. Для выполнения приложений необходимо назначить разрешение Read всем используемым ими файлам или сайту (папке), где эти файлы хранятся. Если приложение записывает содержимое в один из файлов сайта, следует также назначить разрешение Write (но лишь для отдельного файла или каталога).

3. Если выбранный ресурс является частью IIS-приложения, можно с помощью списка Execute Permission (Разрешен запуск) задать уровень выполнения:
  - None (Нет) — доступ только к статичным файлам: например, HTML- и GIF-;

- **Scripts Only (Только сценарии)** — выполняются только сценарии: например, ASP-;
  - **Scripts And Executables (Сценарии и исполняемые файлы)** — просматриваются и выполняются все файлы.
4. Щелкните Apply. Прежде, чем применить изменения, IIS проверяет текущие параметры всех Web-узлов и их папок. Если на узле действуют другие разрешения, открывается диалоговое окно **Inheritance Overrides**. Отметьте в нем узлы, к которым надо применить новые разрешения, и щелкните OK.

### Настройка протокола WebDAV

Протокол WebDAV дополняет HTTP 1.1 и позволяет удаленным пользователям управлять ресурсами Web-сервера, т. е.:

- выполнять обычные файловые операции: например, вырезать, копировать и вставлять файлы;
- создавать и редактировать файлы и их свойства на уровне ОС;
- создавать и редактировать каталоги и их свойства на уровне ОС;
- блокировать ресурсы, чтобы при одновременном просмотре лишь один из пользователей мог редактировать ресурс, а также снимать блокировку;
- вести поиск по содержанию и свойствам файлов определенной папки.

WebDAV интегрирован в US, и поэтому все папки Web-узлов IIS-сервера доступны для распределенного редактирования и проверки версий. Это упрощает доступ и публикацию документов на IIS-сервере.

### Разрешения WebDAV-приложений

Для управления допустимыми действиями WebDAV-приложений используются обычные разрешения Web-сервера,

- **Directory Browsing (Обзор каталогов)** позволяет клиентам WebDAV просматривать содержимое каталогов.
- **Index This Resource (Индексация каталога)** — если на Web-сервере выполняется служба Indexing Service, клиенты WebDAV могут искать нужную информацию в папке с помощью специальных поисковых утилит.

- **Read (Чтение)** позволяет клиентам WebDAV просматривать вложенные папки и выполнять файлы в папке WebDAV.
- **Script Source Access (Доступ к тексту сценария)** позволяет клиентам WebDAV загружать файлы исходного кода сценариев.
- **Write (Запись)** позволяет клиентам WebDAV просматривать вложенные папки и перезаписывать файлы.

Для публикации файла и просмотра списка файлов в каталоге пользователь должен обладать разрешениями Read (Чтение), Write (Запись) и Directory Browsing (Обзор каталогов). Для редактирования исходного кода сценариев необходимо разрешение Script Source Access (Доступ к тексту сценария). В целях защиты Web-содержимого данные разрешения следует назначать только папкам, требующим прохождения проверки на подлинность. Например, можно создать папку For-Publishing, запретить к ней анонимный доступ и назначить ей разрешения Read, Write и Directory Browsing, необходимые WebDAV-приложениям.

Предоставляя доступ к исходным кодам сценариев, убедитесь, что исходный код и исполнимые файлы надежно защищены. Все расширения файлов, указанные на вкладке Application Mappings (Отображение приложений) диалогового окна свойств сайта, считаются расширениями файлов сценариев. Файлы, расширения которых не сопоставлены какому-либо приложению, обрабатываются как статичные HTML- или текстовые файлы. Файлы с расширениями .DLL и .exe, которым не задано разрешение Scripts And Executables (Сценарии и исполняемые файлы), позволяющее перезаписывать их даже при отсутствии у клиента разрешения Script Source Access (Доступ к тексту сценария), также считаются статичными HTML-файлами. Если же им назначено разрешение Scripts And Executables, они обрабатываются как исполнимые файлы и могут быть перезаписаны только при наличии у пользователя разрешения Script Source Access.

Доступ к документам и их публикация с помощью **WebDAV**

Windows 2000 и Office 2000 поддерживают WebDAV, и поэтому подключиться к Web-папкам на IIS-серверах не составляет труда. В Windows 2000 это делается так.

1. На рабочем столе Windows дважды щелкните значок My Network Places (Мое сетевое окружение), а затем — значок Add Network Place (Новое место в сетевом окружении). Запустится мастер Add Network Place Wizard (Добавление в сетевое окружение).
2. В окно мастера введите URL требуемой папки: например <http://www.microsoft.com/data/>.
3. Щелкните Next (Далее) и введите описание папки.
4. После того как вы щелкнете Finish (Готово), Windows 2000 автоматически подключится к папке. Для повторного обращения к папке дважды щелкните на рабочем столе значок My Network Places (Мое сетевое окружение) и затем — значок папки.

Создав новое место в сетевом окружении для папки WebDAV, можно легко и просто публиковать в ней документы из Microsoft Office 2000.

1. В меню File (Файл) выберите команду Save As (Сохранить как), затем в левой части диалогового окна Save As (Сохранение документа) щелкните значок My Network Places (Мое сетевое окружение).
2. Щелкните значок нужной папки WebDAV или введите ее URL и щелкните ОК.

Вы также можете подключаться к каталогам WebDAV через Internet Explorer 5.0 в ОС Microsoft Windows 95/98/NT 4.0/2000.

1. Запустите Internet Explorer версии 5.0 или более новой и выберите из меню File (Файл) команду Open (Открыть). Откроется одноименное диалоговое окно.
2. В диалоговом окне Open (Открыть) введите URL требуемой папки WebDAV: например <http://www.microsoft.com/data/>.
3. Пометьте флажок Open As Web Folder (Открыть как Web-папку) и щелкните ОК.

#### Выбор метода проверки подлинности

Методы проверки подлинности управляют доступом к ресурсам IIS. Проверка позволяет реализовать анонимный доступ к общедоступным узлам, а также создавать защищенные



области Web-узлов и Web-узлы с контролируемым доступом. Если проверка подлинности включена, IIS на основе реквизитов пользователя определяет его права и разрешения доступа к ресурсу.

Основы **проверки** подлинности

Доступны четыре режима проверки подлинности.

- **Anonymous Authentication (Анонимная проверка подлинности)** IIS автоматически регистрирует пользователей под анонимной или гостевой учетной записью, что позволяет получить доступ без указания имени пользователя и пароля.
- **Basic Authentication (Обычная проверка подлинности)** IIS запрашивает имя пользователя и пароль, которые передаются по сети незашифрованными. Если вы сконфигурировали на сервере безопасные коммуникации в соответствии с инструкциями раздела «Использование SSL» главы 6, можете требовать от клиентов применения протокола Secure Sockets Layer (SSL). При совместном использовании SSL и обычной проверки подлинности регистрационные реквизиты перед передачей их серверу шифруются.
- **Integrated Windows Authentication (Встроенная проверка подлинности Windows)** IIS проверяет личность пользователя с помощью обычной системы безопасности Windows. Вместо предоставления имени пользователя и пароля клиенты пересылают IIS-серверу регистрационные реквизиты, указываемые пользователями при входе в Windows. Передаваемые сведения полностью зашифрованы, не требуют использования SSL и включают имя пользователя и пароль, необходимые для входа в сеть. Встроенную проверку подлинности Windows поддерживают только браузеры семейства Internet Explorer.
- **Digest Authentication (Краткая проверка подлинности)** Осуществляется безопасный обмен реквизитами пользователя между клиентами и серверами. Краткая проверка подлинности является одной из возможностей протокола HTTP 1.1 и использует методы, усложняющие перехват и расшифровку информации посторонними. Данная возможность доступна, только если IIS-сервер является

контроллером домена и запрос поступает от Internet Explorer версии 5.0 или более новой.

По умолчанию для ресурсов IIS включены как анонимная, так и обычная проверка подлинности средствами Windows, и поэтому процесс проверки подлинности происходит следующим образом.

1. IIS пытается обратиться к ресурсу, используя гостевую учетную запись Интернета. Если она обладает достаточными разрешениями, пользователю предоставляется доступ к ресурсу.
2. Если проверка регистрационных реквизитов прошла неудачно или учетная запись заблокирована (отключена), IIS переключается на текущие регистрационные реквизиты пользователя. Если реквизиты успешно проходят проверку и пользователь обладает нужными разрешениями, ему будет предоставлен доступ к ресурсу.
3. Если проверка завершилась неудачно или у пользователя нет достаточных прав на доступ, ему будет отказано в доступе к ресурсу.

Как и в случае с разрешениями Web-сервера, проверку подлинности можно настроить глобально или локально. Глобальные методы проверки подлинности задают в диалоговом окне основных свойств WWW-службы. Локальные методы настраивают в окне свойств сайта, папки или файла. Если изменения конфликтуют с текущими настройками ресурсов, IIS выводит диалоговое окно, позволяющее указать, какие ресурсы будут наследовать новые параметры.

Помните следующее.

- **При совместном использовании анонимного доступа и доступа с проверкой подлинности пользователи** получают полный доступ к ресурсам, предоставляемый гостевой учетной записью Интернета. Если у данной учетной записи нет доступа к ресурсу, IIS пробует проверить ее подлинность с помощью указанных вами методов проверки. Если проверка завершится неудачно, пользователю будет отказано в доступе.
- Если анонимный доступ запрещен, службы IIS проверяют все пользовательские запросы с помощью указанных вами методов проверки подлинности. После того как

пользователь пройдет проверку, IIS на основе его учетной записи определяет его права доступа.

- **При совместном использовании** обычной и встроенной или краткой **проверки подлинности** Internet Explorer сначала использует один из последних методов проверки. Это означает, что пользователям, прошедшим проверку с регистрационными реквизитами текущей учетной записи, не будет предложено ввести имя и пароль.

Кроме того, перед использованием краткой проверки подлинности надо включить двустороннее шифрование паролей для учетных записей всех пользователей, которые будут подключаться к серверу с помощью данного метода проверки. Двустороннее шифрование позволяет IIS и Web-браузеру обеспечить защищенную передачу и расшифровку пользовательской информации. Чтобы включить двустороннее шифрование, сделайте так.

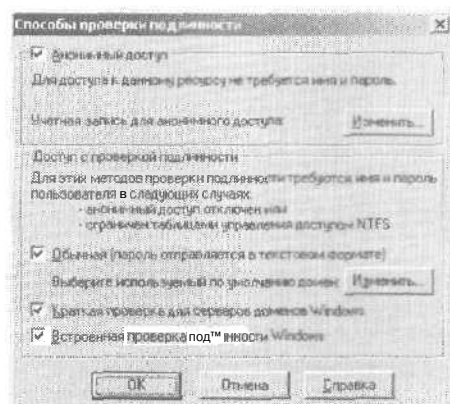
1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и выберите Active Directory Users And Computers (Active Directory – пользователи и компьютеры). Запустится одноименная оснастка.
2. Дважды щелкните учетную запись, которая должна использовать краткую проверку подлинности.
3. В диалоговом окне Account Options (Учетная запись) пометьте флажок Store Password Using Reversible Encryption (Хранить пароль, используя обратимое шифрование).
4. Щелкните ОК. Повторите пп. 1-4 для всех учетных записей пользователей.

#### Включение и отключение проверки подлинности

Включать и отключать анонимный доступ можно на уровне сервера, сайта, каталога или файла. Если анонимный доступ включен, пользователи будут обращаться к ресурсам без прохождения проверки подлинности (при условии, что это допускается разрешениями безопасности Windows данного ресурса). При отключенном анонимном доступе для обращения к ресурсу пользователи должны пройти проверку подлинности, автоматически или вручную (в зависимости от используемого браузера и реквизитов учетной записи).

Проверка подлинности на уровне сервера включается/отключается так.

1. В оснастке Internet Information Services щелкните правой кнопкой значок нужного компьютера и выберите в контекстном меню команду *Properties* (Свойства). Откроется одноименное диалоговое окно.
2. В раскрывающемся списке *Master Properties* (Основные свойства) выберите *WWW Service* (WWW-служба) и щелкните *Edit* (Изменить). Откроется диалоговое окно *WWW Service Master Properties* (Основные свойства WWW-службы) для данного компьютера.
3. Перейдите на вкладку *Directory Security* (Безопасность каталога) и в группе *Anonymous Access And Authentication Control* (Анонимный доступ и проверка подлинности) щелкните *Edit* (Изменить). Откроется диалоговое окно *Authentication Methods* (Способы проверки подлинности) (рис. 5-12). Его элементы:
  - **Anonymous Access** (Анонимный доступ) управляет анонимной проверкой подлинности;
  - **Basic Authentication** [Обычная (пароль отправляется в текстовом формате)] управляет обычной проверкой подлинности; отключая ее, помните, что в результате некоторые клиенты не смогут удаленно обращаться к ресурсам, так как поддерживаемый ими метод проверки не будет включен на сервере;
  - **домен по умолчанию** автоматически не определяется; если при регистрации в системе не предоставлено сведений о домене, при включении обычной проверки подлинности его можно задать — это позволит гарантировать корректное прохождение проверки клиентами;
  - **Digest Authentication** (Краткая проверка для серверов Windows) управляет краткой проверкой подлинности; если используемый вами компьютер не является контроллером домена, данный флажок недоступен;
  - **Integrated Windows Authentication** (Встроенная проверка подлинности Windows) управляет встроенной проверкой подлинности Windows.



**Рис. 5-12.** Диалоговое окно Authentication Methods (Способы проверки подлинности)

4. Щелкните ОК. Прежде чем применить изменения, IIS проверит текущие параметры всех дочерних узлов выбранного ресурса. Если на дочернем узле применяются иные методы проверки подлинности, откроется диалоговое окно *Inheritance Overrides* (Переопределение наследования). Отметьте в нем узлы, к которым следует применить новые разрешения, и щелкните ОК.

Проверка подлинности на уровне узла, каталога или файла включается/отключается так.

1. В оснастке Internet Information Services щелкните правой кнопкой значок нужного компьютера и выберите в контекстном меню команду *Properties* (Свойства). Откроется одноименное диалоговое окно.
2. Перейдите на вкладку *Directory Security* (Безопасность каталога) и в группе *Anonymous Access And Authentication Control* (Анонимный доступ и проверка подлинности) щелкните *Edit* (Изменить). Откроется диалоговое окно *Authentication Methods* (Способы проверки подлинности) (рис. 5-12). Его элементы:
  - **Anonymous Access** (Анонимный доступ) управляет анонимной проверкой подлинности;
  - **Basic Authentication** [Обычная (пароль отправляется в текстовом формате)] управляет обычной провер-

кой подлинности; отключая ее, помните, что в результате некоторые клиенты не смогут удаленно обращаться к ресурсам, так как поддерживаемый ими метод проверки не будет включен на сервере;

- **домен по умолчанию** автоматически не определяется; если при регистрации в системе не предоставлено сведений о домене, при включении обычной проверки подлинности его можно задать — это позволит гарантировать корректное прохождение проверки клиентами;
  - **Digest Authentication (Краткая проверка для серверов Windows)** управляет краткой проверкой подлинности; если используемый вами компьютер не является контроллером домена, данный флажок недоступен;
  - **Integrated Windows Authentication (Встроенная проверка подлинности Windows)** управляет встроенной проверкой подлинности Windows.
3. Щелкните ОК. Прежде чем применить изменения, IIS проверит текущие параметры всех дочерних узлов выбранного ресурса. Если на дочернем узле применяются иные методы проверки подлинности, откроется диалоговое окно **Inheritance Overrides** (Переопределение наследования). Отметьте в нем узлы, к которым следует применить новые разрешения, и щелкните ОК.

#### **Настройка ограничений доступа по IP-адресам и доменным именам**

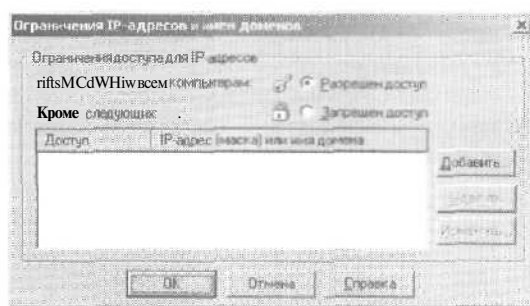
По умолчанию ресурсы IIS доступны всем компьютерам и доменам, а также с любого IP-адреса, и это создает опасность некорректного использования сервера. Для управления использованием ресурсов можно предоставлять или блокировать доступ по IP-адресам, сетевым идентификаторам и доменам. Как и любые другие параметры Web-сервера, ограничения доступа можно задать на уровне сервера или на уровне отдельных сайтов, папок и файлов.

Предоставление доступа позволяет компьютеру запрашивать ресурсы, но не обязательно — работать с ними. Если включена проверка подлинности, пользователи должны ее пройти. Отказ в доступе запрещает компьютеру обращаться к ресурсам. Следовательно, пользователи данного компьютера не

могут работать с ресурсами даже при успешном прохождении проверки подлинности.

Ограничения доступа на уровне сервера включаются/отключаются так.

1. В оснастке Internet Information Services щелкните правой кнопкой значок нужного компьютера и выберите в контекстном меню команду Properties (Свойства). Откроется одноименное диалоговое окно.
2. В раскрывающемся списке Master Properties (Основные свойства) выберите WWW Service (WWW-служба) и щелкните Edit (Изменить). Откроется диалоговое окно WWW Service Master Properties (Основные свойства WWW-службы) для данного компьютера.
3. Перейдите на вкладку Directory Security (Безопасность каталога) и в группе IP Address And Name Restrictions (Ограничения IP-адресов и имен доменов) щелкните Edit (Изменить). Откроется одноименное диалоговое окно (рис. 5-13).



**Рис. 5-13.** Диалоговое окно IP Address And Name Restrictions (Ограничения IP-адресов и имен доменов)

4. Щелкните переключатель Granted Access (Разрешен доступ), чтобы предоставить доступ определенным и запретить доступ остальным компьютерам.
5. Щелкните переключатель Denied Access (Запрещен доступ), чтобы запретить доступ определенным и предоставить доступ остальным компьютерам.
6. Создайте список доступа. Для этого щелкните Add (Добавить) и затем в открывшемся диалоговом окне — Single

Computer (Один компьютер), Group Of Computers (Группа компьютеров) или Domain (Имя домена). Введите:

- для отдельного компьютера — его IP-адрес: например 192.168.5.50;
- для группы компьютеров — адрес их подсети: например, 192.168.0.0, или маску подсети: например, 255.255.0.0;
- для домена — его полное имя: например, eng.domain.com.




Внимание! После предоставления/запрета доступа отдельному домену IIS должны будут выполнять по всем входящим соединениям обратный DNS-поиск, чтобы определить их исходный домен. Это значительно увеличит время отклика на первый запрос любого пользователя к Web-узлу.

7. Чтобы удалить запись из списка доступа, выделите ее в списке Computers (Кроме следующих) и щелкните Remove (Удалить).
8. Щелкните Apply (Применить). Прежде чем применить изменения, IIS проверит текущие параметры всех Web-узлов и их папок. Если на Web-узле используются другие значения параметров, откроется диалоговое окно Inheritance Overrides (Переопределение наследования). Отметьте в нем узлы, к которым следует применить новые значения, и щелкните ОК.

Ограничения доступа на уровне сайта, папки или файла включаются/отключаются так.

1. В оснастке Internet Information Services щелкните правой кнопкой значок нужного компьютера и выберите в контекстном меню команду Properties (Свойства). Откроется одноименное диалоговое окно.
2. Перейдите на вкладку Directory Security (Безопасность каталога) и в группе IP Address And Name Restrictions (Ограничения IP-адресов и имен доменов) щелкните Edit (Изменить). Откроется одноименное диалоговое окно (рис. 5-13).
3. Щелкните переключатель Granted Access (Разрешен доступ), чтобы предоставить доступ определенным и запретить доступ остальным компьютерам.



4. Щелкните переключатель Denied Access (Запрещен доступ), чтобы запретить доступ определенным и предоставить доступ остальным компьютерам.
  5. Создайте список доступа. Для этого щелкните Add (Добавить) и затем в открывшемся диалоговом окне — Single Computer (Один компьютер), Group Of Computers (Группа компьютеров) или Domain (Имя домена). Введите:
    - для отдельного компьютера — его IP-адрес: например, 192.168.5.50;
    - для группы компьютеров — адрес их подсети: например, 192.168.0.0, или маску подсети: например, 255.255.0.0;
    - для домена — его полное имя: например, eng.domain.com.
-  **Внимание!** После предоставления/запрета доступа отдельному домену IIS должны будут выполнять по всем входящим соединениям обратный DNS-поиск, чтобы определить их исходный домен. Это значительно увеличит время отклика на первый запрос любого пользователя к Web-узлу.
6. Чтобы удалить запись из списка доступа, выделите ее в списке Computers (Кроме следующих) и щелкните Remove (Удалить).
  7. Щелкните Apply (Применить). Прежде, чем применить изменения, IIS проверит текущие параметры всех Web-узлов и их папок. Если на Web-узле используются другие значения параметров, откроется диалоговое окно Inheritance Overrides (Переопределение наследования). Отметьте в нем узлы, к которым следует применить новые значения, и щелкните ОК.

#### Назначение операторов Web-узла

Всем Web-узлам сервера можно назначить операторов, которые будут управлять ими удаленно.

#### Операторы Web-узлов

Операторы Web-узла — это специальная группа пользователей, обладающих разрешениями на:

- создание, переименование и удаление каталогов Web-узла;

- управление свойствами папок, включая разрешения доступа, документы по умолчанию, безопасность каталогов, HTTP-заголовки и сообщения об ошибках;
- управление свойствами сайта, включая разрешения сайта, назначение операторов, производительность, фильтры ISAPI, свойства домашнего каталога, документы по умолчанию, безопасность каталога, HTTP-заголовки и сообщения об ошибках.

Операторы не могут изменять свойства, влияющие на работу IIS обслуживающего компьютера или сети. Такое ограничение наложено в целях повышения уровня безопасности.



**Примечание** Привилегии операторов не распространяются на Web-узел Administration (Администрирование Web-узла). Для удаленного управления IIS через данный Web-узел пользователь должен состоять в группе Administrators (Администраторы).

Удаленное администрирование делают возможным сценарии, компоненты и приложения, находящиеся в каталоге IISAdmin. Для каждого Web-узла, требующего удаленного управления операторами, следует создать такой каталог. Путь к этому каталогу по умолчанию — `\\%Systemroot%\System32\Inet-srv\Iisadmin`.

Для подключения к требуемому Web-узлу операторы используют обычный браузер, например Internet Explorer 5.0. Вводимый администратором URL состоит из доменного имени узла, за которым следует имя виртуального административного каталога. Например, если доменное имя сервера — `dev.microsoft.com`, а административного каталога — `ops`, для подключения к административному разделу Web-узла в браузере нужно ввести адрес:

`http://dev.microsoft.com/ops/`

Метод проверки подлинности реквизитов оператора Web-узла зависит от методов проверки, включенных для административного каталога. Ни в коем случае не разрешайте анонимный доступ к административному каталогу.

Задать учетные записи, обладающие привилегиями оператора Web-узла, можно глобально или локально. Глобальное назначение операторов автоматически распространяется на

все Web-узлы сервера. Локальное назначение операторов влияет только на отдельный Web-узел.

#### Разрешение администрирования Web-узла оператором

Чтобы разрешить администрирование Web-узла операторами, сделайте так.

1. Создайте виртуальный каталог и сопоставьте его физическому расположению папки IISAdmin.
2. Создайте групповое IS-приложение и сделайте начальной его точкой созданный каталог. Групповое IS-приложение изолирует административные задачи от основных процессов IS.
3. Из списка Execute Permission (Разрешен запуск) выберите для административной папки уровень выполнения; Scripts Only (Только сценарии) или Scripts And Executables (Сценарии и исполняемые файлы).

#### Назначение операторов всем Web-узлам сервера

Чтобы назначить операторов всем Web-узлам сервера, сделайте так.

1. В оснастке Internet Information Services щелкните правой кнопкой значок нужного компьютера и выберите в контекстном меню команду Properties (Свойства). Откроется одноименное диалоговое окно.
2. В раскрывающемся списке Master Properties (Основные свойства) выберите WWW Service (WWW-служба) и щелкните Edit (Изменить). Откроется диалоговое окно WWW Service Master Properties (Основные свойства WWW-службы) для данного компьютера.
3. Перейдите на вкладку Operators (Операторы). В списке Operators (Операторы) отображаются операторы, назначенные Web-узлу. По умолчанию оператором Web-узла является только глобальная группа Administrators (Администраторы).
4. Чтобы добавить оператора, щелкните Add (Добавить). Откроется диалоговое окно Select Users Or Groups (Выбор: Пользователи или Группы), где можно выбрать пользователей и группы.

5. Чтобы удалить оператора, выберите его в списке Operators (Операторы) и щелкните Remove (Удалить).
6. Трижды щелкните ОК, чтобы завершить назначение операторов.

#### Назначение операторов отдельным Web-узлам

Операторы определенному Web-узлу назначаются так.

1. В оснастке Internet Information Services щелкните правой кнопкой значок нужного компьютера и выберите в контекстном меню команду Properties (Свойства). Откроется одноименное диалоговое окно.
2. Перейдите на вкладку Operators (Операторы). В списке Operators (Операторы) отобразятся назначенные Web-узлу операторы. По умолчанию оператором Web-узла является только глобальная группа Administrators (Администраторы).
3. Чтобы добавить оператора, щелкните Add (Добавить). Откроется диалоговое окно Select Users Or Groups (Выбор: Пользователи или Группы), где можно выбрать пользователей и группы.
4. Чтобы удалить оператора, выберите его в списке Operators (Операторы) и щелкните Remove (Удалить).
5. Дважды щелкните ОК, чтобы завершить назначение операторов.

### Как повысить уровень безопасности Web-сервера

Ваш Web-сервер будет безопасен ровно настолько, насколько вы этого захотите, и я предлагаю вам несколько советов.

#### Использование брандмауэров

Обеспечение безопасности Web-сервера — непрерывная задача, требующая постоянной бдительности. Для защиты от атак вам потребуется брандмауэр, например, Microsoft Internet Security and Acceleration Server или Cisco PIX 515 Firewall. При установке брандмауэра следует закрыть все незадействованные порты. Их перечень зависит от используемых ресурсов IIS. Протокол FTP использует порты 21 и 23;

SMTP — порт 25 и иногда — порт 53 для разрешения доменных имен; HTTP - порты 80 и 443, а NNTP - 119 и 563.

### Переименование учетной записи Administrator

Общезвестная учетная запись Administrator обладает на Web-сервере расширенными привилегиями. Злоумышленники часто выбирают ее мишенью своих атак в попытке получить контроль над сервером. Чтобы их отпугнуть, переименуйте учетную запись Administrator в оснастке Active Directory Users And Computers (Active Directory — пользователи и компьютеры). Только не забудьте сообщить другим администраторам компании новое название учетной записи администратора.

### Отключение Web-узла по умолчанию

Web-узел по умолчанию использовать не рекомендуется. На нем множество сконфигурированных приложений, обращающихся к системным ресурсам и позволяющих выполнять связанные сценарии и исполнимые файлы. Кроме того, данный узел автоматически разрешает удаленное администрирование через хорошо известный всем каталог. Все это делает Web-узел уязвимым для атак, и его лучше отключить.

1. В оснастке Internet Information Service щелкните правой кнопкой Web-узел по умолчанию и выберите в контекстном меню команду Stop (Остановить).
2. Закройте оснастку IIS, чтобы сохранить изменения конфигурации.
3. Запустив оснастку IIS снова, вы увидите, что Web-узел по умолчанию остановлен.



**Примечание** Во избежание использования его в будущем Web-узел по умолчанию можно удалить.

### Отключение удаленного администрирования через Web

Как уже говорилось, Web-узлами можно управлять удаленно через браузер. Для управления отдельным узлом оператор подключается к его папке IISAdmin, а для управления IIS — к Web-узлу Administration (Администрирование Web-узла). Для четкого управления доступом к серверу отклю-

чите удаленное администрирование через Web и разрешите доступ к серверу только через оснастку IIS.

Итак, отключим удаленное администрирование через Web.

1. Остановите Web-узел Administration (Администрирование Web-узла).
2. Удалите административную папку (обычно — IISAdmin) или выберите в списке Execute Permission (Разрешен запуск) уровень выполнения None (Нет).

### Запрет просмотра каталогов

Возможность просматривать содержимое каталогов большинству пользователей не нужна, поэтому вы можете глобально запретить просмотр каталогов. Снимите соответствующий флажок в диалоговом окне Master WWW Service Properties (Основные свойства WWW-службы).

### Создание уведомлений

Всем пользователям, входящим на Web-сервер локально или с помощью утилиты telnet, должно выводиться сообщение о том, что сервер является частной компьютерной системой и предназначен только для авторизованных пользователей. Уведомление состоит из заголовка и собственно текста. Заголовков можно задать в разделе HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption реестра, а текст — в разделе HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText реестра.

Оба раздела создают и изменяют с помощью Registry Editor (Редактор реестра) или сценария Windows. При создании разделов убедитесь, что тип их значений — REG\_SZ. Данный тип соответствует строковому значению, содержащему последовательность символов. Задавая значение раздела, введите 1 и затем заголовок или текст уведомления, например:

1, This is a private system. Use of this system is restricted to authorized personnel only.

### Установка сервисных пакетов, оперативных исправлений и шаблонов

Microsoft регулярно выпускает сервисные пакеты и оперативные исправления для ОС Windows. Для обеспечения

безопасности серверов эти пакеты и исправления необходимо разворачивать как можно скорее, предварительно протестировав их на машинах с аналогичной конфигурацией.

Кроме того, корпорация публикует шаблоны безопасности для Web-серверов. Шаблоны безопасности доступны во всех системах с ОС Windows 2000 Server. Просмотреть существующие и создать собственные шаблоны безопасности поможет оснастка Security Templates (Шаблоны безопасности). Для применения и анализа ограничений безопасности, налагаемых шаблоном, служит оснастка Security Configuration And Analysis (Анализ и настройка безопасности). Эти оснастки запускаются так.

1. Раскройте меню Start (Пуск) и выберите команду Run (Выполнить). Откроется одноименное диалоговое окно,
2. В поле Open (Открыть) введите MMC и щелкните ОК. Запустится консоль MMC.
3. В меню Console (Консоль) выберите команду Add/Remove Snap-In (Добавить/удалить оснастку). Откроется одноименное диалоговое окно.
4. На вкладке Standalone (Изолированная оснастка) щелкните Add (Добавить).
5. В диалоговом окне Add Standalone Snap-In (Добавить изолированную оснастку) выберите Security Templates (Шаблоны безопасности) и щелкните Add (Добавить).
6. Выберите Security Configuration And Analysis (Анализ и настройка безопасности) и щелкните Add (Добавить).
7. Щелкните Close (Закрыть) и затем ОК, чтобы закрыть диалоговое окно Add Standalone Snap-In (Добавить изолированную оснастку).

Для Web-серверов, требующих надежной защиты, рекомендуется шаблон securews, а для серверов, требующих системы безопасности повышенной надежности — hisecws (рис. 5-14). Данные шаблоны определяют значения параметров:

- политик паролей, блокировки учетных записей и Kerberos;
- политик аудита, назначения прав пользователям и безопасности;
- журналов событий, системных служб, а также разрешения файловой системы;

- реестра для локальной машины и текущего пользователя.

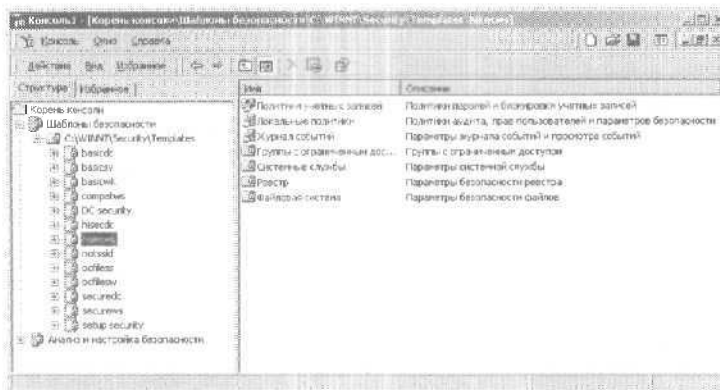


Рис. 5-14. Оснастка Security Templates (Шаблоны безопасности)

Выбрав шаблон, просмотрите его параметры и попробуйте оценить, как они повлияют на вашу рабочую среду. Если какой-то параметр никак не влияет на нее, удалите или измените его. Просмотреть/изменить параметры можно так.

1. Запустите оснастку Security Configuration And Analysis (Анализ и настройка безопасности).
2. Щелкните узел Security Configuration And Analysis правой кнопкой и выберите в контекстном меню команду Open Database (Открыть базу данных). Откроется одноименное диалоговое окно.
3. Введите в поле File Name (Имя файла) имя новой базы данных и щелкните Open (Открыть).
4. Откроется диалоговое окно Import Template (Импортировать шаблон). Выберите шаблон безопасности и щелкните Open (Открыть).
5. Щелкните узел Security Configuration And Analysis (Анализ и настройка безопасности) правой кнопкой и выберите в контекстном меню команду Analyze Computer Now (Анализ компьютера). В ответ на предложение указать путь к журналу ошибок щелкните ОК. Путь по умолчанию вполне подойдет.
6. Дождитесь, пока оснастка закончит анализ шаблона. Затем просмотрите результаты и при необходимости обно-



вите шаблон. Чтобы просмотреть журнал ошибок, щелкните правой кнопкой узел Security Configuration And Analysis (Анализ и настройка безопасности) и выберите в контекстном меню команду View Error Log file (Просмотр файла журнала).

7. Чтобы применить шаблон, щелкните правой кнопкой узел Security Configuration And Analysis (Анализ и настройка безопасности) и выберите в контекстном меню команду Configure Computer Now (Настроить компьютер). В ответ на предложение указать путь к журналу ошибок щелкните ОК, выбрав путь по умолчанию.
8. Просмотрите журнал ошибок, щелкнув правой кнопкой узел Security Configuration And Analysis (Анализ и настройка безопасности) и выбрав в контекстном меню команду View Error Log file (Просмотр файла журнала). Выявите проблемы (если таковые будут) и примите соответствующие меры для их устранения.

### Удаление виртуального каталога IISADMPWD

Виртуальный каталог IISADMPWD позволяет сбрасывать пароли Windows NT и Windows 2000. Он разрабатывался для интрасетей и не устанавливается в составе IIS версии 5.0 или более новой. И все же после обновления с IIS 4.0 данный каталог по-прежнему может присутствовать на вашем сервере. На Web-серверах, доступных из Интернета, его следует удалить.

### Проверка ввода в формах и строках запроса

Вводимый пользователями в формах текст может содержать символы, способные вызвать определенные проблемы в работе сервера. Если передать их непосредственно сценарию или ASP-странице, злонамеренный пользователь сможет получить доступ к системе. Чтобы избежать этого, нужно проверять все вводимые пользователями символы перед передачей их сценарию или ASP-странице.

Чтобы убедиться, что ввод содержит только текст и числа, удалите все символы, не являющиеся алфавитно-цифровыми. Сделать это поможет код на VBScript:

```
'Начинаем обычное выражение  
Set reg = New RegExp
```

```
'Проверяем наличие символов, отличных от 0-9, a-z, A-Z и '_'
reg.Pattern = "\W+"
```

```
'Удаляем из строки ввода недопустимые символы
goodString = reg.Replace(inputString, "")
```

Если вы хотите разрешить пользователям ввод знаков пунктуации и одновременно исключить злонамеренный ввод, выявляйте и удаляйте символ конвейеризации (`()`). Он объединяет команды, предоставляя тем самым пользователю возможность выполнять команды на сервере. Следующий код удаляет из строки ввода символ конвейера и весь стоящий за ним текст;

```
'Начинаем обычное выражение
Set reg = New RegExp
```

```
'Проверяем наличие символа конвейеризации
reg.Pattern = "^(.+)\|(.+)"
```

```
'Удаляем символ конвейеризации и все прочие символы, следующие за ним
goodString = reg.Replace(inputString, "$1")
```

Существует масса других методов проверки ввода пользователя. Подробнее — на Web-узле Microsoft TechNet по адресу <http://www.microsoft.com/technet/>.

### **Удаление неиспользуемых сопоставлений приложений**

Сопоставления позволяют указать доступные приложениям CGI-программы и расширения ISAPI. Службы IIS сконфигурированы для поддержки многих распространенных приложений ISAPI, включая ASP, Internet Database Connector и Index Server. Если какие-то из этих приложений на Web-сервере не используются, для повышения безопасности можно удалить соответствующие сопоставления, включая те, что используются:

- `.httr` — для сброса пароля через Web;
- `.htw`, `.ida`, `.idq` — Index Server;
- `.idc` — Internet Database Connector;
- `.printer` — Internet Printing;
- `.stm`, `.shtm`, `.shtml` — для включений на стороне сервера.

Чтобы полностью удалить для всех Web-узлов сервера сопоставления приложений, сделайте так.

1. В оснастке Internet Information Services щелкните правой кнопкой значок нужного компьютера и выберите в контекстном меню команду Properties (Свойства). Откроется одноименное диалоговое окно.
2. В раскрывающемся списке Master Properties (Основные свойства) выберите WWW Service (WWW-служба) и щелкните Edit (Изменить). Откроется диалоговое окно WWW Service Master Properties (Основные свойства WWW-службы) данного компьютера.
3. Перейдите на вкладку Home Directory (Домашний каталог) и в группе Application Settings (Параметры приложения) щелкните Configuration (Настройка). Откроется диалоговое окно Application Configuration (Настройка приложения).
4. На вкладке App Mappings (Отображение приложений) выберите сопоставление и щелкните Remove (Удалить). Затем щелкните Yes (Да), чтобы подтвердить удаление.
5. Щелкните Apply (Применить). Прежде чем применить эти значения параметров, IIS проверит текущие параметры всех Web-узлов и их папок. Если на Web-узле используются другие параметры, откроется диалоговое окно Inheritance Overrides (Переопределение наследования). Отметьте в нем узлы и папки, которые будут использовать новые сопоставления, и щелкните OK.

## Глава 6

# Управление службой Microsoft Certificate Services и протоколом SSL

В предыдущей главе мы рассмотрели безопасность Web-сервера, а сейчас обсудим службу Microsoft Certificate Services (Службы сертификации) и протокол SSL, создающие дополнительный уровень защиты.

Certificate Services и SSL защищают важную информацию, например пароли, номера кредитных карт и сведения об оплате, шифруя данные, пересылаемые между клиентом и сервером. Шифрование — это процесс кодирования информации по математическому алгоритму, затрудняющему считывание исходных данных сторонними лицами.

Службы Internet Information Services передают зашифрованные данные клиентскому браузеру по протоколу SSL, при этом серверы и/или клиенты предварительно подтверждают свою подлинность, используя сертификаты, а после установки соединения обмениваются информацией по защищенному каналу SSL. Информация шифруется методом, позволяющим клиенту и серверу получить исходные данные.

## Протокол SSL

IIS поддерживают протокол SSL версии 3.0, обеспечивающий обмен зашифрованными данными между Web-серверами и клиентскими браузерами. Рассмотрим архитектуру и использование SSL.

### SSL-шифрование

В алгоритме для шифрования применяется математическое значение, называемое *ключом*, без которого прочесть исходные данные невозможно.

Существует множество методов шифрования для обмена информацией. Одни применяют открытый (общего пользования) и закрытый (секретный) ключи, другие — секретные ключи общего пользования, распространяемые между прошедшими проверку подлинности системами. В протоколе SSL реализовано шифрование открытого ключа, объединяющее ключи:

- открытый, доступный любому запросившему его лицу;
- закрытый, известный лишь владельцу;
- секретный общего пользования (ключ сеанса), создаваемый на основе данных открытого и закрытого ключей.

Для установления соединения между клиентом и сервером IIS применяют компонент шифрования открытого ключа, имеющийся в протоколе SSL. Используйте этот протокол всегда, когда хотите обеспечить дополнительную защиту клиент-серверного обмена информацией. Службу Certificate Services и протокол SSL рекомендуется использовать:

- для удаленного администрирования Web-сервера с помощью Web-узла Administration (Администрирование Web-узла) или страниц администратора;
- при наличии на Web-узле защищенных областей с важными документами;
- при наличии на Web-узле страниц, собирающих важные личные или финансовые сведения о посетителях;
- если на Web-узле принимаются заказы на товары и услуги и собираются сведения о кредитных картах клиентов.

По протоколу SSL клиент подключается к Web-странице, используя URL, начинающийся с *https://*. Обозначение *https* указывает, что браузер пытается установить защищенное соединение с IIS. По умолчанию для SSL-подключений предназначен порт 443, но это можно изменить. Настроившись на работу с SSL, помните, что невозможно использовать заголовки узлов. SSL шифрует HTTP-запросы и поэтому не

позволяет определить нужный клиенту узел на основе имени заголовка узла из зашифрованного запроса.

После того как клиентский браузер подключится к серверу с помощью безопасного URL, сервер перелает ему свой открытый ключ и сертификат. Затем клиент и сервер согласуют уровень шифрования для безопасной связи. Сервер всегда пытается задействовать наивысший поддерживаемый им уровень шифрования. После согласования уровня шифрования клиентский браузер создаст ключ сеанса и с помощью открытого ключа шифрует его для передачи. Прочитать перехваченное в этот момент сообщение нельзя — извлечь исходные данные позволяет лишь закрытый ключ сервера.

IIS-сервер расшифровывает клиентское сообщение своим закрытым ключом, и в результате создается SSL-соединение между клиентом и сервером. Теперь для шифрования пересылаемых между клиентом и сервером данных будет использоваться ключ сеанса.

Итак, SSL-подключение устанавливается в такой последовательности.

1. Клиентский браузер обращается к серверу с помощью безопасного URL.
2. IIS-сервер передает браузеру свой открытый ключ и сертификат.
3. Клиент и сервер согласуют уровень шифрования для обмена информацией.
4. Клиентский браузер шифрует ключ сеанса открытым ключом сервера и передает зашифрованные данные серверу.
5. IIS-сервер расшифровывает клиентское сообщение своим закрытым ключом. В итоге создается SSL-соединение между клиентом и сервером.
6. Для шифрования пересылаемых между клиентом и сервером данных применяется ключ сеанса.

### SSL-сертификаты

Сертификат можно рассматривать как удостоверение с информацией для идентификации приложения в сети. Сертификаты позволяют пользователям и Web-серверам подтверждать свою подлинность перед установлением соединения.

Кроме того, сертификаты содержат ключи, необходимые для установки SSL-сеансов между сервером и клиентом.

Сертификаты, используемые IIS, Web-браузерами и службами Component Services, обычно соответствуют стандарту X.509, и потому называются сертификатами X.509. Существует несколько версий стандарта X.509, время от времени дополняемых и совершенствуемых. При установке соединения используется два типа сертификатов X.509: клиентские (с идентификационной информацией клиента) и серверные (с идентификационной информацией сервера).

Центр сертификации (Certificate Authority, CA) уполномочен выдавать сертификаты обоих типов и представляет собой доверенный орган, проверяющий личности пользователей, организаций и их серверов, и выдающий сертификаты, которые удостоверяют их личность. Перед выдачей клиентского сертификата CA требует предоставить сведения, идентифицирующие пользователя, организацию и клиентское приложение. Для выдачи серверного сертификата CA требует предоставить сведения, идентифицирующие организацию и ее сервер.

В этом разделе основное внимание уделено серверным сертификатам. Их можно получить у одного из нескольких CA. Если вы используете Certificate Services, организация вправе сама выступать в качестве CA. Поддержка SSL на Web-сервере в этом случае включается так.

1. Установите службу Certificate Services на одном из серверов домена и сгенерируйте сертификат корневого CA.
2. Сгенерируйте файлы запроса сертификата для всех размещенных на ваших серверах Web-узлов с уникальными именами. Затем с помощью этих файлов создайте для Web-узлов серверные сертификаты.
3. Установите сертификаты и включите SSL на всех требующих этого Web-узлах.
4. Чтобы клиентские браузеры опознавали сертификат корневого CA и доверяли ему, пользователи должны установить этот сертификат в хранилище сертификатов браузера.
5. Для установки SSL-соединения используйте URL, начинающиеся с *https://*.

Кроме того, можно обратиться к сторонним СА. Они подтвердят вашу подлинность, и в браузерах уже предустановлены сертификаты множества доверенных СА. Просмотреть список доверенных центров к Microsoft Internet Explorer 5.0 можно так,

1. В меню Tools (Сервис) выберите команду Internet Options (Свойства обозревателя). Откроется одноименное диалоговое окно.
2. Перейдите на вкладку Content (Содержание) и щелкните Certificates (Сертификатов). Откроется диалоговое окно Certificates (Сертификаты).
3. Перейдите на вкладку Trusted Root Certification Authorities (Доверенные корневые центры сертификации), где содержится список доверенных корневых СА.

Поддержка SSL на Web-узле при работе со сторонним СА включается так.

1. Сгенерируйте файлы запроса сертификата для всех размещенных на ваших серверах Web-узлов с уникальным именем.
2. Передайте эти файлы в доверенный сторонний СА, например Entrust, Equifax, Valicert или Verisign. СА обрабатывает запросы и вернет вам сертификаты.
3. Установите сертификаты и включите SSL на всех требующих этого Web-узлах.
4. Теперь для установки SSL-соединений клиенты смогут задействовать URL, начинающиеся с *https://*.

Независимо от типа используемого СА серверными сертификатами управляют вручную с помощью Certificate Services. Срок действия серверного сертификата может закончиться, кроме того, сертификат могут отозвать. Например, организация — поставщик услуг Интернета, выдающая собственные сертификаты, вправе выдавать клиентам сертификаты, действительные в течение года. Это заставит клиентов хотя бы раз в год обновлять сведения сертификата. Кроме того, когда клиент отказывается от услуг, его сертификат отзывается.



### Стойкость шифра в протоколе SSL

Стойкость шифра SSL-сеанса прямо пропорциональна числу разрядов в ключе сеанса. Иначе говоря, считается, что ключи с большим числом разрядов безопаснее — их труднее взломать.

Для SSL-сеансов обычно применяются 40- и 128-разрядный уровни шифрования. Первый вариант подходит для большинства ситуаций, включая электронную коммерцию, а второй — обеспечивает дополнительную защиту важных личных и финансовых сведений клиента. В версиях Microsoft Windows для США реализовано 128-, а в экспортных версиях — 40-разрядное шифрование. Чтобы обновить сервер для 128-разрядного шифрования, установите специальный пакет обновления, распространяемый Microsoft.

Не путайте уровень шифрования SSL-сеансов (стойкость ключа сеанса, выраженная в разрядах) и уровень шифрования SSL-сертификатов (стойкость открытого и закрытого ключей сертификата, выраженная в разрядах). Обычно длина ключа шифрования, открытого или закрытого, составляет 512 или 1 024 разряда. Внутренние американские и экспортные версии большинства приложений и ОС поддерживают ключи шифрования длиной 512 разрядов. Ключи длиной 1 024 и более разрядов во многих случаях не поддерживаются.

Когда пользователь пытается установить SSL-соединение с Web-сервером, клиентский браузер и сервер на основе своих ключей шифрования определяют максимально возможный уровень шифрования. Если длина ключей шифрования 512 разрядов, используется 40-разрядное, если 1 024 — 128-разрядное шифрование. Также доступны другие длины ключей и уровни шифрования.

### Служба Microsoft Certificate Services

Служба Microsoft Certificate Services позволяет предоставлять и отзывать цифровые сертификаты, с помощью которых можно создавать SSL-сеансы и подтверждать подлинность узла интрасети, внешней сети, а также Интернета.

### Общий обзор

Certificate Services — это служба Windows, выполняющаяся на выделенном сервере сертификатов. Вот список возможных серверов:


- корневой СА предприятия находится в корне иерархии домена Windows, этот наиболее доверенный СА в пределах предприятия должен обладать доступом к службе Active Directory;
- дочерний СА предприятия состоит в иерархии имеющегося СА, может выдавать сертификаты, но должен получить собственный сертификат СА у корневого СА предприятия;
- автономный корневой СА находится в корне иерархии, не связанной с предприятием; он наиболее доверенный в иерархии и не требует доступа к Active Directory;
- автономный дочерний СА состоит в не связанной с предприятием иерархии, может выдавать сертификаты, но должен получить собственный сертификат СА у автономного корневого СА своей иерархии.

На сервере сертификатов не обязательно должна выполняться только Certificate Services, на нем вполне можно публиковать Web-узлы. Однако в домене рекомендуется выделить специальные серверы сертификатов, не используемые для иных целей. Переименовать компьютер, на котором установлена служба Certificate Services, нельзя. Нельзя изменить и его членство в домене.

Для управления Certificate Services служат оснастка Certification Authority (Центр сертификации) и Web-приложение на основе ASP-страниц, которое можно открыть в обычном браузере. Оснастка позволяет полностью управлять службой Certificate Services, а Web-приложение — получать списки отозванных сертификатов (certificate revocation lists, CRL), отправлять запросы и проверять наличие поступивших запросов на сертификаты.

Рассмотрим главное окно оснастки Certification Authority (Центр сертификации) (рис. 6-1). Узел корневого СА содержит 4 вложенных узла, в которых хранятся:

- **Revoked Certificates** (Отозванные сертификаты) — все отозванные сертификаты;
- **Issued Certificates** (Выданные сертификаты) — все сертификаты, утвержденные и выданные администратором службы Certificate Services;
- **Pending Requests** (Запросы в ожидании) — ожидающие своей очереди запросы на сертификаты, поступившие в данный CA; чтобы удовлетворить запрос, щелкните его значок правой кнопкой и выберите в контекстном меню команду **Issue** (Выдать);
- **Failed Requests** (Неудачные запросы) — все отклоненные запросы на сертификаты, поступившие в данный CA; чтобы отклонить запрос, щелкните его значок правой кнопкой и выберите в контекстном меню команду **Deny** (Запретить).

 **Примечание** Метка корневого узла в оснастке соответствует имени CA. В нашем примере это Corporate Root CA.

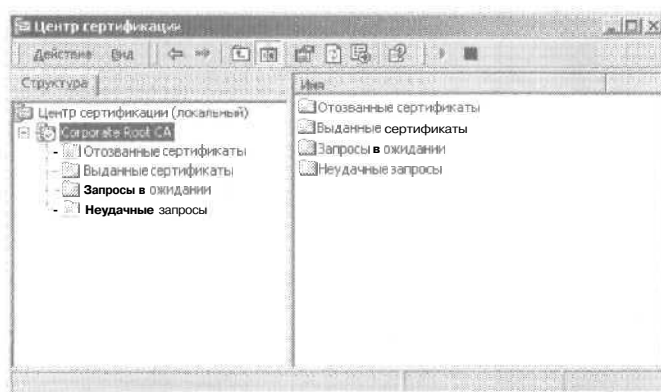


Рис. 6-1. Оснастка Certification Authority (Центр сертификации)

### Установка службы Certificate Services

Установка включает несколько этапов. Прежде всего нужно создать папку для хранения сертификатов и конфигурационных файлов. Она должна располагаться на том же компьютере, что и Certificate Services. Ей следует назначить разрешение **Read** (Чтение) для встроенной группы **Everyone**

(Все), чтобы пользователи смогли обращаться к папке и устанавливать сертификаты из нее. Если на сервере не выполняется IIS и вам требуется получать CRL для запрашивания сертификатов или проверки наличия ожидающих запросов на сертификаты с помощью браузера, установите па сервере сертификатов службы IIS.

Создав папку сертификатов и установив IIS, установите Certificate Services.

1. Зарегистрируйтесь на сервере сертификатов, используя учетную запись с привилегиями администратора (при создании CA предприятия — учетную запись с привилегиями администратора домена).
2. Раскройте меню Start\Settings (Пуск\Настройка) и выберите Control Panel (Панель управления).
3. Дважды щелкните значок Add/Remove Programs (Установка и удаление программ). Откроется одноименное диалоговое окно.
4. Щелкнув Add/Remove Windows Components, запустите мастер Windows Components Wizard (Мастер компонентов Windows).
5. Поставьте флажок Certificate Services (Службы сертификации). При необходимости подтвердите свои действия, щелкнув Yes (Да). Затем щелкните Next (Далее).
6. Выберите тип CA (рис. 6-2):
  - Enterprise Root CA (корневой ЦС предприятия) — корневой CA домена Active Directory, переключатель доступен, только если сервер состоит в домене;
  - Enterprise Subordinate CA (подчиненный ЦС предприятия) — дочерний CA, который станет членом существующей иерархии; переключатель также требует наличия службы Active Directory;
  - Stand-Alone Root CA (изолированный ЦС предприятия) — автономный корневой СЛ, наличие Active Directory не требуется;
  - Stand-Alone Subordinate CA (изолированный подчиненный ЦС) — дочерний CA, который станет членом существующей иерархии; наличие Active Directory не требуется.



**Примечание** Для выбора поставщика услуг шифрования и алгоритмов хеширования, используемых при создании ключей, пометьте флажок **Advanced Options** (Дополнительные возможности). В большинстве ситуаций будут приемлемы значения по умолчанию.

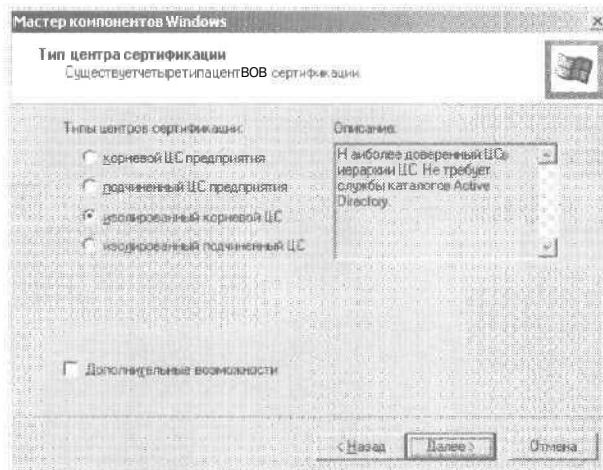


Рис. 6-2. Выбор типа CA

7. Вам предложат предоставить сведения, идентифицирующие CA, и указать дату окончания сертификата (рис. 6-3). В поле введите:
  - **CA Name** (Имя ЦС) — имя CA: например, *Microsoft Corporation Root CA*;
  - **Organization** (Организация) — официальное наименование вашей организации: например, *Microsoft Corporation*;
  - **Organizational Unit** (Подразделение) — подразделение организации, отвечающее за CA: например, *Technology Department*;
  - **City** (Город) — город или местность, в которой расположена организация;
  - **State or Province** (Область) — штат или область, в которой расположена организация;

- **Country/Region** (Страна/регион) — страна или регион, в котором расположена организация;
- **E-Mail** (Электронная почта) — адрес электронной почты администратора сервера сертификатов;
- **CA Description** (Описание ЦС) — описание CA<sup>1</sup>;
- **Valid For** (Срок действия) — дата и время окончания сертификата корневого CA (этот сертификат генерируется при установке CA).

**Рис. 6-3.** Идентификационная информация и дата **окончания** сертификата CA

8. Укажите папку для хранения конфигурационных сведений, Б.И. и журнала. По умолчанию Б.И. и Журнал сертификатов помещаются в папку `\\%SystemRoot%\System32\CertLog`. Также в группе Shared Folder (Сетевая папка) укажите расположение ранее созданной папки сертификатов. Можете щелкнуть Browse (Обзор) и выбрать папку в открывшемся диалоговом окне.
9. Щелкните. Next (Далее). Если на сервере сертификатов выполняются IIS, Windows потребует завершить их работу. Щелкните OK в ответ на запрос системы. Мастер

<sup>1</sup> Все поля, кроме этого, рекомендуется заполнять на английском языке. — *Прим. перев.*

Windows Components Wizard начнет установку и конфигурирование Certificate Services.

10. Щелкните Finish (Готово). Если вы установили службу Certificate Services на компьютер с IIS, то теперь сможете сконфигурировать ее для доступа через Web.

### Доступ к службе Certificate Services через Web-браузер

После установки на компьютер с IIS службы Certificate Services ОС обновляет Web-узел по умолчанию (основной Web-узел), позволяя получать CRL, запрашивать сертификаты и проверять наличие ожидающих запросов на сертификаты через Web-браузер.

Управление на основе Web-браузера реализовано с помощью файлов из трех папок.

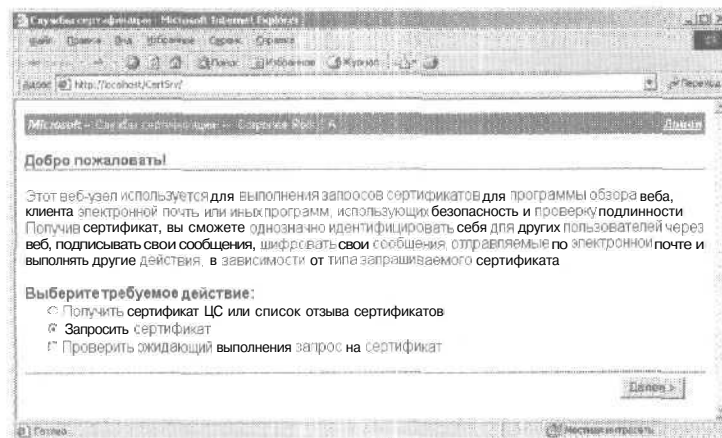
- **CertSrv** служит для Web-доступа к Certificate Services. Расположение по умолчанию — `\\%SystemRoot%\System32\CertSrv`. По умолчанию эта папка сконфигурирована в качестве ISAPI-приложения с именем CertSrv, выполняющегося в процессе.
- **CertControl** предназначена для управления службой Certificate Services. Расположение по умолчанию — `\\%SystemRoot%\System32\CertControl`.
- **CertEnroll** служит для управления службой Certificate Services. Расположение по умолчанию -- `\\%SystemRoot%\System32\CertEnroll`.

Если эти папки почему-либо недоступны, можно создать виртуальные каталоги, которые свяжут псевдонимы с их физическим местоположением. Для этого сделайте так.

1. Запустите оснастку Internet Information Services и в левой панели раскройте узел нужного компьютера. Если компьютер не отображается, подсоединитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2.
2. Щелкните правой кнопкой Web-узел, к которому требуется подключить системный каталог, и выберите в контекстном меню команду **New\Virtual Directory** (Создать\Виртуальный каталог). Запустится мастер Virtual Directory Creation Wizard (Мастер создания виртуальных каталогов). Щелкните Next (Далее).

3. В поле Alias (Псевдоним) введите имя для доступа к системной папке, например *CertSrv*.
4. В следующем диалоговом окне вам предложат указать путь к физической папке с содержимым. Щелкните Browse (Обзор) и выберите в открывшемся окне системную папку.
5. Щелкните Next (Далее) и задайте разрешения на доступ и выполнение. Папкам CertSrv, CertControl и CertEnroll задайте разрешения Read (чтение) и Scripts Only (запуск сценариев).
6. Щелкните Next (Далее), затем — Finish (Готово), Будет создан виртуальный каталог, связанный с указанной вами физической папкой. Сконфигурируйте каталог CertSrv как ISAPI-приложение, начальная точка которого указывает на его базовую папку. CertControl и CertEnroll будут частью приложения; делать их отдельными приложениями не требуется.

Теперь для Web-доступа к службе Certificate Services можно использовать URL *http://hostname/certsrv*. Здесь hostname — DNS- или NetBIOS-имя обслуживающего сервера, например *sa.microsoft.com* или *CASrv*. Ниже показана основная страница Certificate Services (рис. 6-4).



**Рис. 6-4.** Web-интерфейс управления службой Certificate Services (Службы сертификатов)



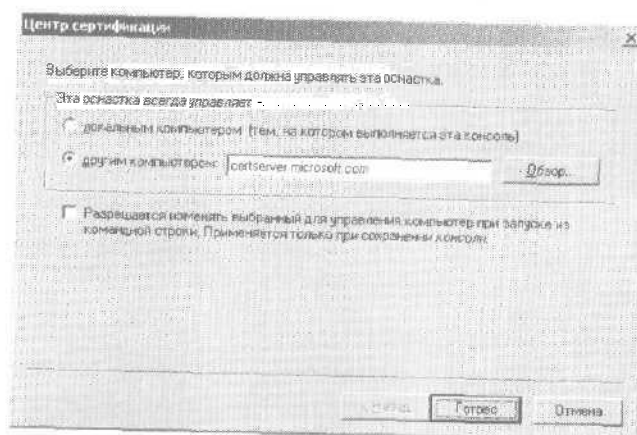
### Запуск и остановка службы Certificate Services

Microsoft Certificate Services выполняется на сервере как служба Windows. Остановить/запустить ее можно так.

1. Запустите оснастку Certification Authority (Центр сертификации), щелкните корневой узел CA (Root CA) правой кнопкой и выберите в контекстном меню команду All Tasks (Все задачи).
2. Для остановки Certificate Services выберите Stop (Остановить службу), а для запуска - Start (Запуск службы).

На удаленном компьютере Certificate Services останавливают/запускают так.

1. Запустите оснастку Certification Authority и щелкните корневой узел CA (Root CA) правой кнопкой.
2. Выберите в контекстном меню команду Retarget Certification Authority (Перенацелить центр сертификации). Откроется диалоговое окно Certification Authority (Центр сертификации).
3. Поставьте переключатель в положение Another Computer (Другим компьютером) (рис. 6-5), введите имя компьютера и щелкните Finish (Готово). Можно также ввести IP-адрес или полное доменное имя сервера.



**Рис. 6-5.** Диалоговое окно Certification Authority (Центр сертификации)

4. В оснастке Certification Authority щелкните правой кнопкой корневой узел **CA (Root CA)** и выберите в контекстном меню команду **All Tasks (Все задачи)**.
5. Для остановки Certificate Services выберите **Stop (Остановить службу)**, а для запуска — **Start (Запуск службы)**.

### Архивирование и восстановление информации CA

При наличии в организации собственного CA следует периодически архивировать его информацию. Это гарантирует восстановление важных данных CA, включая закрытый ключ и сертификат, конфигурационные сведения, журнал и очередь ожидающих запросов.

Возможно архивирование двух видов:

- **обычное** — создание *полной* копии журналов сертификатов и очередей ожидающих запросов;
- **добавочное** — создание *частичной* копии журналов сертификатов и очередей ожидающих запросов, содержащей изменения с момента последнего обычного архивирования.

Если CA очень большой, можно проводить также добавочное архивирование журналов и очередей командой **Perform Incremental Backups (Выполнить добавочную архивацию)**.

1. Произведите обычное архивирование информации CA.
2. Затем производите добавочное архивирование.

При добавочном архивировании восстанавливать информацию следует также по частям.

1. Остановите службу Certificate Services.
2. Восстановите *последнюю* обычную резервную копию.
3. Поочередно восстановите все добавочные *резервные* копии.
4. Запустите Certificate Services.

### Архивирование информации CA

Информация CA на сервере сертификатов архивируется так.

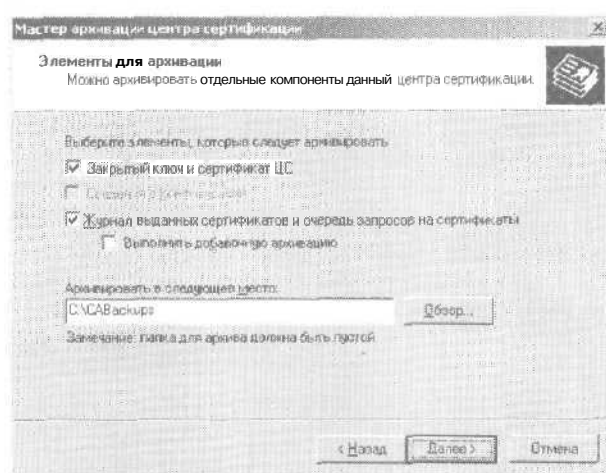
1. Создайте папку, где служба Certificate Services будет хранить резервные копии. Эта папка должна быть пустой и находиться на одном компьютере с Certificate Services (Службы сертификации).

2. Запустите оснастку Certification Authority (Центр сертификации), щелкните правой кнопкой **корневой узел CA (Root CA)** и выберите в контекстном меню команду **All Tasks\Backup CA (Все задачи\Архивация ЦС)**. Запустится мастер Certification Authority Backup Wizard (Мастер архивации центра сертификации).



**Примечание** При резервном копировании информации CA должна быть запущена Certificate Services. Если служба остановлена, вам будет предложено ее запустить — щелкните OK.

3. Щелкните **Next (Далее)** и выберите объекты для архивирования (рис. 6-6):



**Рис. 6-6.** Мастер Certification Authority Backup Wizard (Мастер архивации центра сертификации)

- Private Key And CA Certificate (Закрытый ключ и сертификат ЦС);
- Configuration Information (Сведения о конфигурации);
- Issued Certificate Log And Pending Certificate Request Queue (Журнал выданных сертификатов и очередь запросов на сертификаты),

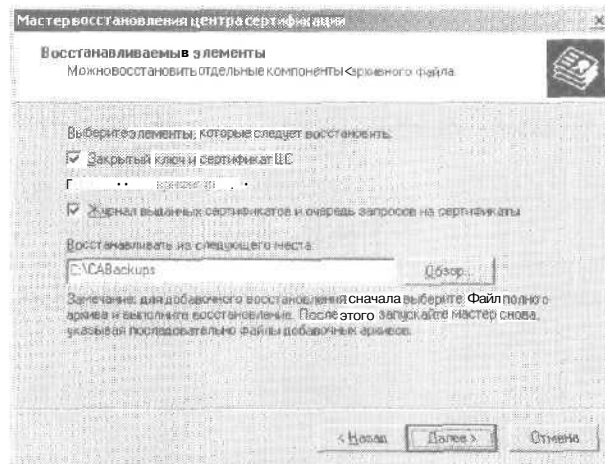
4. Если *это* добавочное архивирование, пометьте флажок Perform Incremental Backup (Выполнить добавочное архивирование).
5. В поле Back Up To This Location (Архивировать в следующее место) введите путь к папке для резервного копирования или щелкните Browse (Обзор) и выберите папку в открывшемся диалоговом окне. Если указанной вами папки нет, система предложит создать ее.
6. Щелкните Next (Далее). Введите и подтвердите пароль для защиты файлов закрытого ключа и сертификата CA.
7. Щелкните Next (Далее), затем Finish (Готово). Мастер создаст резервную копию указанных данных.

#### Восстановление информации CA

Данные CA восстанавливаются так.

1. Certificate Services (Службы сертификатов) должна быть остановлена: в оснастке Certification Authority (Центр сертификации) щелкните правой кнопкой корневой узел CA (Root CA) и выберите в контекстном меню команду All Tasks\Stop Service (Все задачи\Остановить службу).
2. Снова щелкните корневой узел CA (Root CA) правой кнопкой и выберите в контекстном меню команду All Tasks\Restore CA (Все задачи\Восстановление ЦС). Запустится мастер Certification Authority Restore Wizard (Мастер восстановления центра сертификации).
3. Щелкните Next (Далее) и выберите объекты для восстановления (рис. 6-7):
  - Private Key And CA Certificate (Закрытый ключ и сертификат ЦС);
  - Configuration Information (Сведения о конфигурации);
  - Issued Certificate Log And Pending Certificate Request Queue (Журнал выданных сертификатов и очередь запросов на сертификаты).
4. В поле Back Up From This Location (Восстанавливать из следующего места) введите путь к папке с резервными копиями или щелкните Browse (Обзор) и выберите папку в открывшемся диалоговом окне. Перед восстано-

нием добавочных копий всегда восстанавливайте самую новую обычную резервную копию.



**Рис. 6-7.** Мастер Certification Authority Restore Wizard (Мастер восстановления центра сертификации)

5. Щелкните Next (Далее). Введите пароль, защищающий файлы закрытого ключа и сертификата CA.
6. Щелкните Finish (Готово). Мастер восстановит выбранные данные. После этого вам будет предложено запустить Certificate Services. Если восстанавливать добавочные копии не надо, щелкните Yes (Да). В противном случае щелкните No (Нет) и восстановите добавочные копии,

#### **Удовлетворение и отклонение ожидающих запросов на сертификаты**

Просмотреть ожидающие запросов на сертификаты можно в узле Pending Requests (Запросы в ожидании) оснастки Certification Authority (Центр сертификации).

Чтобы удовлетворить ожидающий запрос на сертификат, сделайте так.

1. Запустите оснастку Certification Authority (Центр сертификации) и раскройте узел Pending Requests (Запросы в ожидании). Появится список ожидающих запросов.

- Щелкните нужный запрос правой кнопкой и выберите в контекстном меню команду `All Tasks\Issue` (Все задачи\Выдать).
- Certificate Services сгенерирует основанный на запросе сертификат и поместит его к очередь Issued Certificates (Выданные сертификаты). Срок действия сертификата — один год, после этого его нужно обновить.

Отклонить ожидающий запрос на сертификат можно так.

- Запустите оснастку Certification Authority (Центр сертификации) и раскройте узел Pending Requests (Запросы в ожидании). Появится список ожидающих запросов.
- Щелкнув нужный запрос правой кнопкой, выберите в контекстном меню команду `All Tasks\Deny` (Все задачи\Запретить).
- При запросе системы подтвердите свои действия, щелкнув Yes (Да),
- Отклоненные запросы помещаются в очередь Failed Requests (Неудачные запросы), и их невозможно восстановить. Пользователю потребуется отправить новый запрос.

### **Генерирование сертификатов вручную с помощью оснастки Certification Authority**

Выдав сертификат, можно вручную создать файл сертификата для установки на Web-узле.

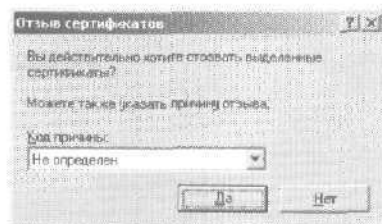
- Запустите оснастку Certificate Authority (Центр сертификации) и выделите узел Issued Certificates (Выданные сертификаты). Появится список сертификатов, выданных этим корневым СА,
- Щелкните нужный сертификат правой кнопкой и выберите в контекстном меню команду `Open` (Открыть). Откроется диалоговое окно Certificates (Сертификат).
- Перейдите на вкладку Details (Состав) и щелкните `Copy To File` (Копировать в файл). Запустится мастер Certificate Export Wizard (Мастер экспорта сертификатов). Щелкните Next (Далее).
- Щелкните переключатель Base-64 Encoded X.509 (Файлы в Base64-кодировке X.509) и затем — Next.

5. Укажите имя экспортируемого файла. Не забудьте ввести .cer в качестве расширения. Чтобы для указания имени и места сохранения файла вызвать диалоговое окно Save As (Сохранить как), щелкните Browse (Обзор).
6. Щелкните Next (Далее) и затем — Finish (Готово). После того как мастер Certificate Export Wizard подтвердит успешное экспортирование сертификата, щелкните ОК. Теперь файл сертификата можно установить на Web-узле (подробнее см. раздел «Обработка ожидающих запросов и установка сертификатов узлов» этой главы).

### Отзыв сертификатов

Если изменяется состояние узла или клиент отказывается от ваших услуг, сертификаты серверов можно отозвать.

1. Запустите оснастку Certificate Authority (Центр сертификации) и выделите узел Issued Certificates (Выданные сертификаты). Появится список сертификатов, выданных этим корневым СА.
2. Щелкните сертификат правой кнопкой и выберите в контекстном меню команду All Tasks\Revoke Certificate (Все задачи\Отзыв сертификата). Откроется диалоговое окно Certificate Revocation (Отзыв сертификатов) (рис. 6-8).



**Рис. 6-8.** Диалоговое окно Certificate Revocation (Отзыв сертификатов)

3. В списке Reason code (Код причины) укажите причину отзыва сертификата и щелкните Yes (Да).
4. СА пометит сертификат как отозванный и переместит его в очередь Revoked Certificates (Отозванные сертификаты).

По умолчанию СА публикуют CLR еженедельно, но это можно изменить в диалоговом окне *Revoked Certificates Properties* (Свойства: Отозванные сертификаты).

1. Запустите оснастку Certificate Authority (Центр сертификации), щелкните узел *Revoked Certificates* правой кнопкой и выберите в контекстном меню команду *Properties* (Свойства).
2. С помощью полей *Publication Interval* (Интервал публикации) задайте новый интервал публикации CRL (рис. 6-9).

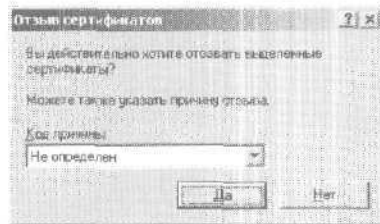


Рис. 6-9. Диалоговое окно *Revoked Certificates Properties* (Свойства: Отозванные сертификаты)

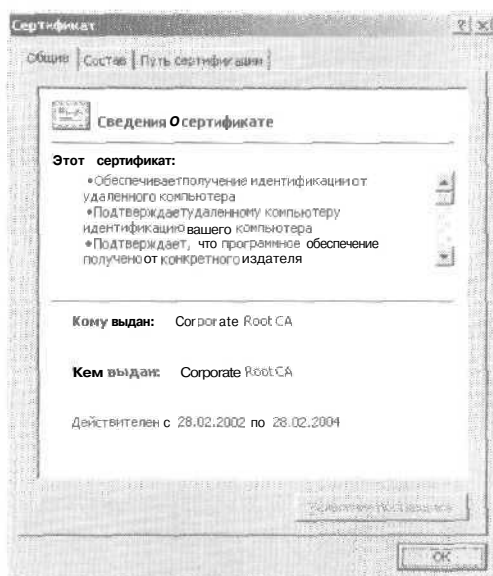
3. Щелкните ОК.

### Просмотр и обновление сертификата корневого СА

Сертификат корневого СЛ действителен в течение периода, указанного при его создании. Просмотреть дату окончания или другие свойства сертификата несложно.

1. В оснастке *Certification Authority* (Центр сертификации) щелкните корневой узел *CA (Root CA)* правой кнопкой и выберите в контекстном меню команду *Properties* (Свойства). Откроется диалоговое окно *Root CA Properties* (Свойства: Root CA).
2. На вкладке *General* (Общие) щелкните *View Certificate* (Просмотр сертификата).
3. Диалоговое окно *Certificate* (Сертификат) позволяет просмотреть свойства сертификата, включая дату начала и дату окончания срока действия (рис. 6-10).





**Рис. 6-10.** Диалоговое окно Certificate (Сертификат)

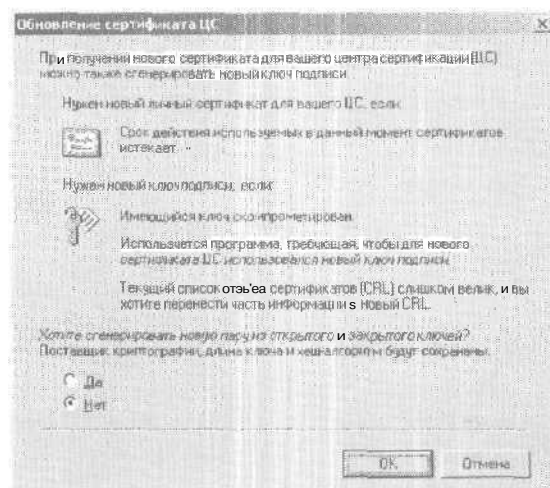
Обычно срок действия сертификата корневого СА — два года. Если он кончается, сертификат надо обновить. Кроме того, обновить сертификат корневого СА рекомендуется, если:

- скомпрометирован ключ, которым подписан сертификат;
- программа требует использовать с новым сертификатом новый ключ подписания;
- текущий CRL слишком велик и требуется перенести часть информации в новый.

Вот как обновить сертификат корневого СА,

1. Служба Certificate Services должна быть остановлена. В оснастке Certification Authority (Центр сертификации) (Центр сертификации) щелкните правой кнопкой корневой узел СА (Root CA) и выберите в контекстном меню команду All Tasks\Stop Service (Все задачи\Остановить службу).
2. Щелкните корневой узел СА (Root CA) правой кнопкой и выберите в контекстном меню команду All Tasks\Renew CA Certificate (Все задачи\Обновить сертификат ЦС).

Откроется диалоговое окно Renew CA Certificate (Обновление сертификата ЦС) (рис. 6-11).



**РИС. 6-11.** Диалоговое окно Renew CA Certificate (Обновление сертификата ЦС)

3. Если нужно создать новую пару «открытый - закрытый ключ», щелкните Yes (Да), если нет — No (Нет).
4. Щелкните ОК. Certificate Services автоматически перезапустится, и будет выдан новый сертификат.

## Создание и установка сертификатов

Создавать и устанавливать сертификаты можно с помощью собственной Certificate Services или сторонней доверенной организации. В первом случае созданием, сроком действия и отзывом сертификатов управляете непосредственно вы, а во втором — доверенная организация. В любом случае для создания и установки сертификата сделайте так.

1. Создайте запрос на сертификат.
2. Передайте его выбранному вами или вашему собственному корневому СА.
3. Получив ответ от СА, обработайте ожидающий запрос и установите сертификат.

4. Убедитесь, что включена поддержка SSL и сконфигурированы безопасные коммуникации.

### Создание запросов на сертификаты

Для корректной работы SSL каждому размещенному на сервере Web-узлу необходим отдельный сертификат. Первый этап его создания — создание запроса на сертификат.

1. В оснастке Internet Information Services щелкните правой кнопкой значок узла и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке Directory Security (Безопасность каталога) щелкните Server Certificate (Сертификат). Запустится мастер Web Server Certificate Wizard (Мастер сертификатов веб-сервера). Щелкните Next (Далее).



**Примечание** Если для узла уже создавался запрос на сертификат, откроется диалоговое окно Pending Certificate Request (Отложенный запрос сертификата) (рис. 6-17). Для продолжения работы вам придется обработать или удалить имеющийся запрос. Подробнее об этом см. разделы «Обработка ожидающих запросов» и «Установка сертификатов узлов» и «Удовлетворение и отклонение ожидающих запросов на сертификаты» данной главы.

3. Щелкните Create A New Certificate (Создание нового сертификата) (рис. 6-12) и затем — Next (Далее).
4. Щелкните Prepare The Request Now (Подготовить запрос сейчас), чтобы подготовить запрос и вручную передать его CA. После этого щелкните Next (Далее).
5. Вам предложат указать имя сертификата и длину ключа (рис. 6-13). Имя должно быть описательным и легко запоминающимся, длина — определяет уровень шифрования открытого и закрытого ключей. Обычно рекомендуется выбирать максимально возможную длину ключа.



**Совет** Если вы захотите создать SGC-сертификат (Server Gated Cryptography), пометьте флажок Server Gated Cryptography (SGC) Certificate (Серверный сертификат SGC). Это не означает, что вы автоматически получите SGC-сертификат, — придется предварительно пройти проверку SGC в доверенной организации.

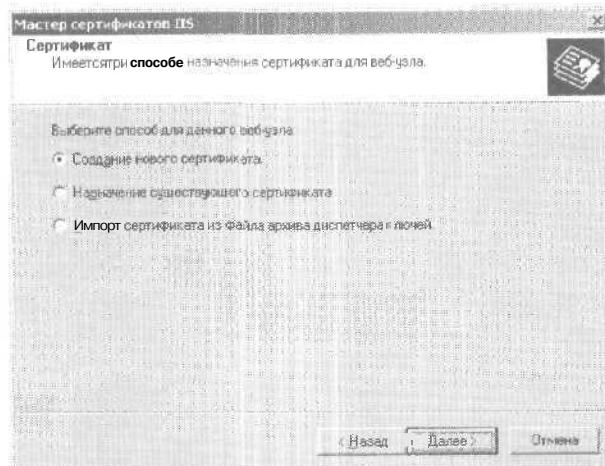


Рис. 6-12. Создание нового сертификата

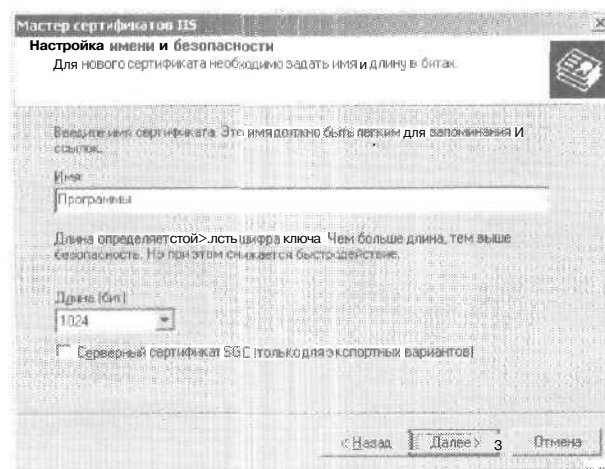


Рис. 6-13. Ввод имени сертификата и указание длины ключа



**Внимание!** При использовании SSL-соединений высокий уровень шифрования может снизить производительность приложения, требовательного к ресурсам процессора. Если ASP-приложения широко используют SSL и счетчики показывают высокую загрузку процессора Web-сервера,

поэкспериментируйте с уровнями шифрования и найдите компромисс между защитой и производительностью.

6. Щелкните Next (Далее). Вы создали открытый и закрытый ключи, которые локально хранятся на Web-сервере. Теперь нужно создать *запрос на подписание сертификата* (certificate-signing request, CSR). Представленные в нем сведения идентифицируют владельца ключа и отображаются в сертификате. CSR применяется лишь для запроса сертификата. Во избежание проблем с работоспособностью сертификата исключите из полей CSR символы:

! @ # \$ % ^ \* ( ) ~ ? > < & / \

7. Предоставьте сведения о своей организации. Введите в поля:

- Organization (Организация) — официальное наименование организации: например, *Microsoft Corporation*;
- Organizational Unit (Подразделение) — название подразделения организации, отвечающего за СА: например, *Technology Department*.



**Примечание** Сторонние СА используют указанное вами имя организации, имя узла и информацию о географическом расположении для проверки запроса на сертификат. Если информация неверна, сертификата вы не получите.

8. Щелкните Next (Далее) и введите имя Web-узла. Если сертификат будет использоваться в интрасети, именем может быть одно слово, а также NetBIOS-имя сервера, например *CorpIntranet*. Если сертификат предназначен для Интернета, именем должно быть действительное DNS-имя, например *www.domain.com*. Щелкните Next (Далее).



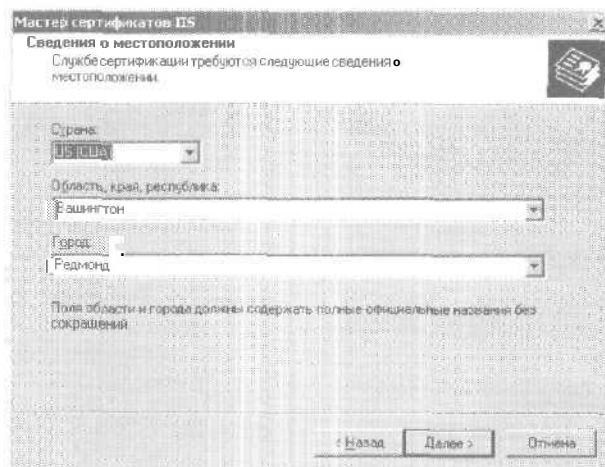
**Совет** Обычно имя узла состоит из имени обслуживающего компьютера и доменного имени, например, *www.domain.com* или *products.microsoft.com*. Сертификат может использоваться только для доступа к тому узлу, на имя которого был выдан. Имя должно быть таким же, как и Web-адрес, используемый для подключения к защищенным узлам. Например, при доступе к узлу *www.domain.com* или *services.domain.com* с использованием сертификата домена *domain.com* будет сгенерировано сообщение об ошибке, поскольку адреса

www.domain.com и services.domain.com отличаются от domain.com. Вам потребуется создать сертификат для соответствующего имени узла.

9. Предоставьте информацию о географическом расположении своей организации (рис. 6-14). В поле укажите:

- **Country/Region** (Страна) — страну или регион;
- **State/Province** (Область, край, республика) — штат или область;
- **City/Locality** (Город) — город или местность.

Щелкните **Next** (Далее).



**Рис. 6-14.** Ввод информации о географическом расположении организации



**Внимание!** Не *используйте* аббревиатуры географических названий. Некоторые СА не приемлют этого, и вам потребуется повторно отсылать запрос.

10. Укажите имя и путь к файлу запроса сертификата. По умолчанию они заданы как **CA\CERTREQ.TXT**. Введите новый путь или щелкните **Browse** и выберите путь и имя файла в диалоговом окне **Save As** (Сохранить как).
11. Дважды щелкните **Next** (Далее) и **затем** **Finish** (Готово), чтобы завершить создание запроса.

## Передача запросов на сертификаты сторонним СА

Созданный CSR можно передать стороннему СА, например Entrust, Equifax, Valicert или Verisign. Запрос на сертификат хранится как ASCII-текст в указанном вами файле (см. раздел «Создание запросов на сертификаты»). Этот файл содержит открытый ключ и идентификационные сведения вашего узла. Открыв файл, вы увидите зашифрованное содержимое запроса:

```
--BEGIN NEW CERTIFICATE REQUEST--
MIXCCDCCAnECAQAwczERMA8GA1UEAxMIZW5nc3ZyMDExEzARBgNVBAStC1RlY2hu
b2xvZ3kxEzARBgNVBAoTCkRvbWVpbi5Db20xEjAQBgNVBAcTCVZhbmdvdXZlcjET
MBEGA3UECBMKV2FzaGluz3RvbjELMAkGA1UEBhMCVVMwZ8wDQYJKoZIhvcNAQEB
BQADgY0ANIGJAoGBALElbrvIZNR8+gvkdcf9b7tNns24h82Jgp5BhKi4NXc/twR7
C+GuDnyTqRs+C2AnNHgb9oQkpiVqQNKH2+N18bKU3PEZUzXH0pxxjhaiT8aMFJhi
3bFvD+gTCQrw5BWoV9/Ff5Ud3EF5TRQ2WJZ+JluQQewo/mXv5ZnbHsM+aLy3AgMB
AAGgggFTMBGcisGAQQBgjcNAgMxDBYKNS4wLjIxOTUuMjA1BgorBgEEAYI3AgE0
MScwJTA0BgNVHQ8BAf8EBAMCBPAwEwYDVR01BAwwCgYIKwYWWQUHAWewgf0GcisG
AQQBgjcNAgIxge4wgesCAQEewgBNAGkAYwByAG8AcwBvAGYAdAAgAFIAUwBBACAA
UwBDAGgAYQBuAG4AZQBsACAAQwByAHkAcAB0AG8AZwByAGEAcABoAGkAYwAgAFAA
cgBvAHYAaQBkAGUAcg0BiQBfE24DPqBwFp1R15/xZDY8Cugoxbyymtwq/tAPZ6dz
Pr9Zy3MnNkKQbKcsbLR/4t9/tWJIMmrFhZonrx12q8fICoiKUXreSK890ILrLEto
1frm/dycoXhHstSsZdm25vszv827FKKk5bRW/vIIEBqfKnePJHOnoiG6UscvgA8Q
fgAAAAAVVAAAOGCSqGSIb3DQEBAQUAA4GBAFZc6K4S04BMUnR/80w3J/MS3Tyi
HAvFuxnjG0CefTq8SakzVq+uazU03waBqHxZ1f32qGr7karoD+fq8dX27nmh0zpp
Rz1DXrxR35mMC/yP/fpLmLb5lsx0t1379PdS4trvWUfKfy93/CkUi+nrQt/uZHY3
NOSTHxf73VkfbsE3
--END NEW CERTIFICATE REQUEST--
```

Многие СА предлагают передать запрос на сертификат как часть формального процесса регистрации узла по электронной почте или через интерактивную форму. В первом случае файл следует просто вложить в сообщение электронной почты и отослать его. Во втором — скопировать весь текст запроса, включая операторы BEGIN и END, в буфер обмена и вставить его в соответствующее поле формы. Это можно сделать посредством Microsoft Notepad (Блокнот).

Изучив ваш запрос на сертификат, СА удовлетворит или отклонит его. Если запрос будет удовлетворен, вы получите сообщение с вложенным подписанным сертификатом или с указанием адреса, по которому можно получить этот сертификат. Сертификат представляет собой текстовый ASCII-файл. Его можно просмотреть в Notepad, но расшифровать —

лишь созданным ранее закрытым ключом. Как и ранее, содержимое файла закодировано и включает операторы BEGIN и END:

```
--BEGIN CERTIFICATE--
MXXCWjCCAgQCEd1pyIenknxBt43eUZ7JF9YwDQYJKoZIhvcNAQEEBQAwgaxFjAU
BgNERAoTDVZ1cm1TaWduLCBjb2MxRzBFBgNVBAsTPnd3dy52ZXJpc2lnbi5jb20v
cmVwb3NpdG9yeS90ZXN0Q1BTIEIuY29ycC4gQnkgUmVmLiBMaWFiLiBMVEQuMUWw
RAYDVQQLZz1G45IgVmVyaVNPZ24gYXV0aG9yaXplZCB0ZXN0aW5nIG9ubHkuIeev
IGFzc3VyYW5jZXMgKEM345MxOTk3MB4XDTAwMTEwNzAwMDAwMFoXDTAwMTEyMTIz
NTk1OVowczELMAkGA1UEBhMCVVMxEzARBgNVBAGTC1dhc2hpbmd0b24xEjAQBgNV
BAcUCVZhbWVudXZlcjETMBEGA1UEChQKRg9tYW1uLkNvbTETMBEGA1UECmVGVGVj
aG5vbG9neTERMA8GA1UEAxQIZW5nc3ZyQWEwgZ8wDQYJKoZIhvcNAQEBBQADgYOA
MIGJAoGBALE1brvIZNRB+gvkdcf9b7tNns24hB2Jgp5BhKi4NXc/twR7C+GuDnyT
qRs+C2AnNHgb9oQkpivqQNKh2+N18bKU3PEZUzXH0prtyhaiT8aMFJhi3bFvD+gT
CQrw5BWoV9/Ff5Ud3EF5TRQ2WJZ+JluQQewo/mXnTZnbHsM+aLy3AgMBAAEwDQYJ
KoZIhvcNAQEEBQADQCCQIrhq5UmsPYzwzKVHIiLDNkYunbhUpSNaBfUSYdv1AU1
Ic/370rdN/E1Zm0ut0MbCWIXKr0Jk5q8F6T1bqwe
--END CERTIFICATE--
```

Сохраните файл сертификата в папку, доступную оснастке Internet Information Services. Не забудьте, что расширением имени файла должно быть .cer. Обработайте и установите сертификат, следуя инструкциям раздела «Обработка ожидающих запросов и установка сертификатов узлов» этой главы.

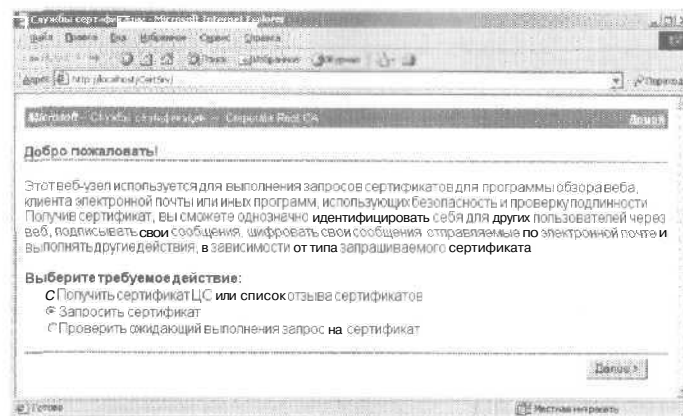
### Передача запросов на сертификаты службе Certificate Services

Созданный CSR можно через Web-интерфейс передать службе Certificate Services.

1. Откройте файл с ASCII-текстом сертификата в Notepad и скопируйте весь текст запроса, включая операторы BEGIN и END, в буфер обмена (воспользуйтесь комбинацией клавиш Ctrl+A и затем — Ctrl+C).
2. Теперь запрос можно передать службе Certificate Services. Запустите Web-браузер и введите URL службы, например, <http://ca.microsoft.com/certsrv/>. Откроется основная страница Certificate Services (рис. 6-15).
3. Поставьте переключатель в положение Request A Certificate (Запросить сертификат) и щелкните Next.

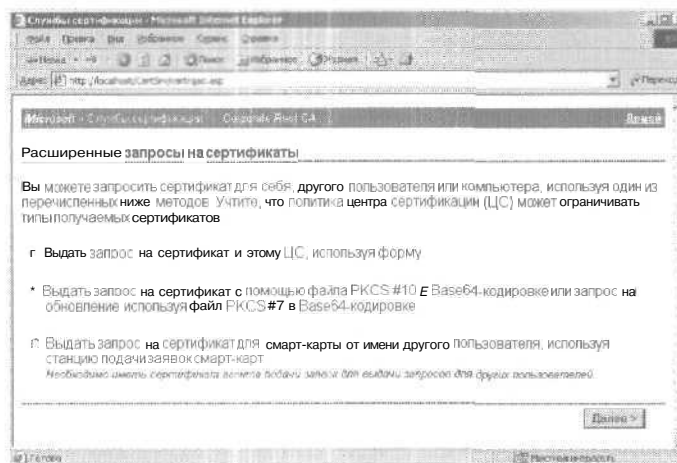


4. На странице Choose Request Type (Выбор типа запроса) щелкните Advanced Request (Расширенный запрос) и затем — Next.



**Рис. 6-15.** Web-интерфейс управления службой Certificate Services (Службы сертификации)

5. На странице Advanced Certificate Requests (Расширенные запросы на сертификаты) щелкните второй переключатель (рис. 6-16) и затем — Next. Тем самым вы сообщите Certificate Services, что собираетесь передать запрос в кодировке base-64.
6. Вставьте текст запроса в поле Saved Request (Сохраненный запрос) и щелкните Submit (Выдать запрос).
7. Если вы все сделали правильно, откроется итоговая страница с сообщением, что запрос получен и ожидает рассмотрения CA. В случае проблем откроется страница с предложением обратиться к администратору. Для просмотра дополнительной информации об ошибке щелкните Details (Подробности). Возможно, вам потребуется повторно создать запрос на сертификат или вернуться и убедиться, что в тексте запроса нет случайно вставленных пробелов и символов.
8. Если у вас собственный CA, запрос можно обработать в оснастке Certification Authority (Центр сертификации). Подробнее см. раздел «Удовлетворение и отклонение ожидающих запросов на сертификаты» этой главы.



**Рис. 6-16.** Страница Advanced Certificate Requests (Расширенные запросы на сертификаты)

Если запрос удовлетворен, вы получите подписанный сертификат с помощью Web-интерфейса, сделав следующее.

1. Запустите Web-браузер и введите URL службы, например, <http://ca.microsoft.com/certsrv/>.
2. В группе Select a task (Выберите требуемое действие) щелкните Check On Pending Certificate (Проверить ожидающий выполнения запрос на сертификат) и затем — Next (Далее).
3. Полнится список ожидающих запросов, которые включают описание и метку времени. Выберите требуемый запрос и щелкните Next.



**Примечание** Если файл сертификата через Web-интерфейс недоступен, попросите администратора СА сгенерировать сертификат вручную. Подробнее см. раздел «Создание сертификатов вручную с помощью оснастки Certification Authority» этой главы.

4. Если на запрос выдан сертификат, откроется страница с соответствующим сообщением. На ней щелкните Base 64 Encoded (в Base64-кодировке) и затем — Download CA Certificate (Загрузить сертификат ЦС).

5. Откроется диалоговое окно File Download (Загрузка файла). Поставьте переключатель в положение Save This File To Disk (Сохранить этот файл на диске) и щелкните ОК.
6. В диалоговом окне Save As (Сохранить как) укажите папку, куда следует поместить файл сертификата, и щелкните Save (Сохранить). Используйте расширение .cer. Обработайте и установите сертификат, следуя инструкциям раздела «Обработка ожидающих запросов и установка сертификатов узлов» этой главы.



**Совет** Рекомендуется поместить все файлы сертификатов в одну папку локального диска Web-сервера. Предоставьте к ней доступ только администраторам.

### Обработка ожидающих запросов и установка сертификатов узлов

Чтобы установить полученный от СЛ сертификат, сделайте так.

1. В оснастке Internet Information Services щелкните значок узла правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке Directory Security (Безопасность каталога) щелкните Server Certificate (Сертификат). Запустится мастер Web Server Certificate Wizard (Мастер сертификатов веб-сервера). Щелкните Next (Далее).
3. Поставьте переключатель в положение Process The Pending Request And Install The Certificate (Обработать отложенный запрос и установить сертификат) (рис. 6-17) и щелкните Next.
4. Введите имя и путь к файлу сертификата или щелкните Browse (Обзор) и выберите файл в открывшемся диалоговом окне. Щелкните Next (Далее).
5. Откроется страница с информацией о сертификате. Если это тот сертификат, щелкните Next и затем — Finish (Готово), чтобы завершить установку. В противном случае щелкните Back (Назад) и повторите пп. 4-5.
6. Сконфигурируйте SSL и управляйте сертификатом, следуя инструкциям разделов «Использование протокола SSL» и «Управление сертификатами узлов с помощью оснастки Internet Information Services» этой главы.

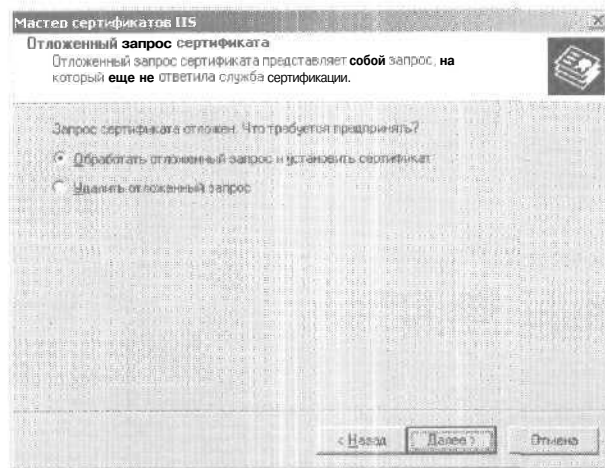


Рис. 6-17. Обработка ожидающего запроса и установка файла сертификата

### Удаление ожидающих запросов на сертификаты

Если в уже сгенерированном запросе на сертификат вы указали неверные сведения, единственный способ исправить это — удалить запрос и создать новый. Ожидающий запрос на сертификат удаляется так.

1. В оснастке Internet Information Services щелкните значок узла правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке Directory Security (Безопасность каталога) щелкните Server Certificate (Сертификат). Запустится мастер Web Server Certificate Wizard (Мастер сертификатов веб-сервера). Щелкните Next (Далее).
3. Поставьте переключатель в положение Delete The Pending Request (Удалить отложенный запрос) (рис. 6-18), и щелкните Next.
4. Щелкните Next и затем — Finish (Готово). При этом будет удалена только привязка запроса в IIS; сам файл запроса останется нетронутым. Он содержит открытый ключ узла и его необходимо обязательно удалить.

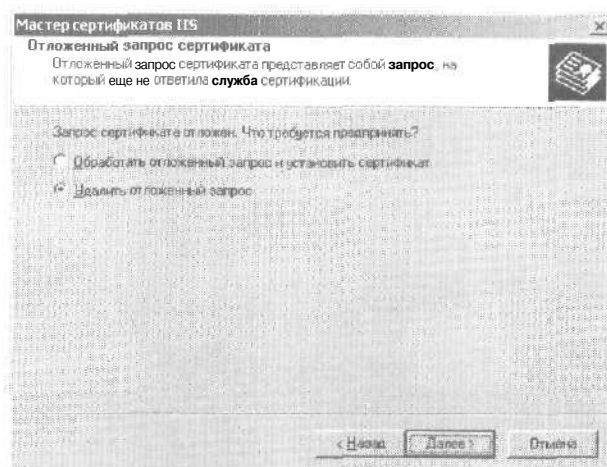


Рис. 6-18. Удаление ожидающего запроса на сертификат

## Использование протокола SSL

При установке сертификата узла автоматически включается поддержка протокола SSL; и все же вам может понадобиться изменить параметры по умолчанию. Сконфигурируйте SSL и устраняйте проблемы по мере их возникновения.

### Настройка SSL-портов

Установив сертификат на Web-узел, можно изменить SSL-порт последнего. SSL-порт применяется для безопасных коммуникаций с клиентскими браузерами. Чтобы просмотреть или изменить SSL-порт, сделайте так.

1. В оснастке Internet Information Services щелкните значок узла правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. В поле SSL Port (Порт SSL) вкладки Web Site (Веб-узел) отображается текущий номер SSL-порта (если таковой имеется).
3. При необходимости введите в этом поле новое значение (рис. 6-19). Несколько узлов могут использовать один порт SSL, при условии, что им назначены разные IP-адреса.

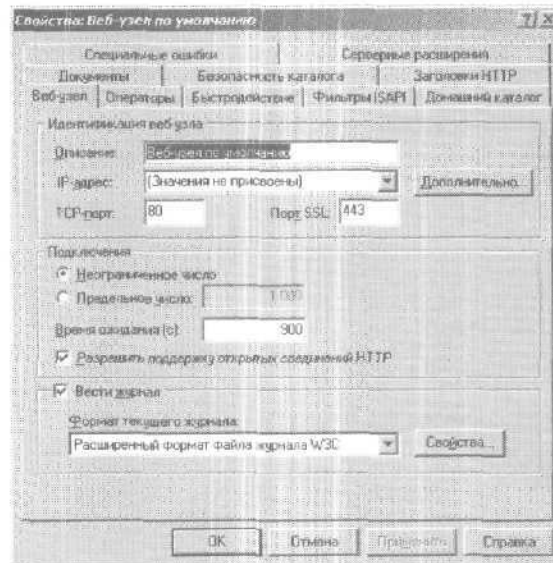


Рис. 6-19. Изменение номера SSL-порта

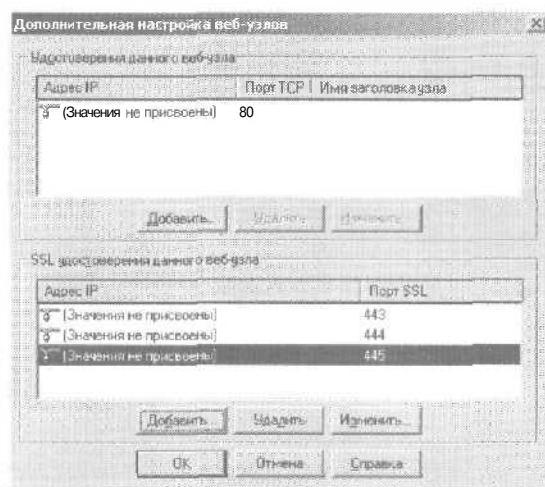
#### 4. Щелкните OK.

Узел также может обладать несколькими SSL-удостоверениями (использовать несколько разных SSL-портов). SSL-порт, указанный на вкладке Web Site (Веб-узел), задействован по умолчанию. Все прочие порты следует указывать в запросе браузера. Например, если определить для протокола SSL порты 443, 444 и 445, запрос <https://yoursite> будет автоматически обработан портом 443, но прочие порты следует указывать явно, например <https://yoursite:445/>.

Вы можете сконфигурировать несколько SSL-удостоверений для Web-узла.

1. В оснастке Internet Information Services щелкните значок узла правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке Web Site (Веб-узел) щелкните Advanced (Дополнительно). Откроется диалоговое окно Advanced Multiple Web Site Configuration (Дополнительная настройка веб-узлов).

3. Для управления удостоверениями SSL служат следующие кнопки (рис. 6-20):



**Рис. 6-20.** Диалоговое окно Advanced Multiple Web Site Configuration (Дополнительная настройка веб-узлов)

- Add (Добавить) — добавление удостоверения SSL; щелкнув эту кнопку, выберите нужный IP-адрес, выберите номер SSL-порта, и затем — OK;
  - Remove (Удалить) — удаление удостоверения SSL;
  - Edit (Изменить) — изменение удостоверения SSL.
4. Дважды щелкните OK, чтобы сохранить изменения.

#### **Установка сертификата корневого СА в хранилище клиентского браузера**

Большинство сертификатов корневых СА, выдаваемые сторонними СА, конфигурируются в Web-браузерах как доверенные СА. Однако, если вы сами себе СА, браузеры не будут опознавать сертификат вашего корневого СА и доверять ему. Чтобы добиться опознания сертификата клиентскими браузерами, пользователям следует установить его в хранилище сертификатов браузера, выполнив следующие действия.

1. Подключитесь к вашему узлу с помощью безопасного URL, начинающегося с *https://*.

2. Появится сообщение о проблемах с сертификатом безопасности узла (рис. 6-21).

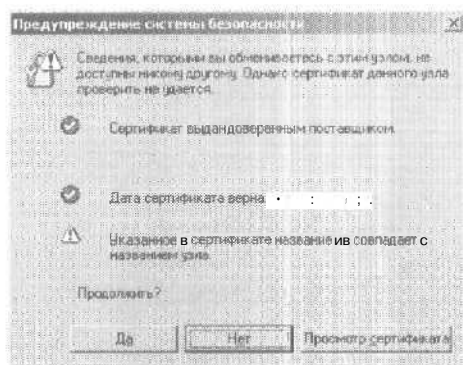
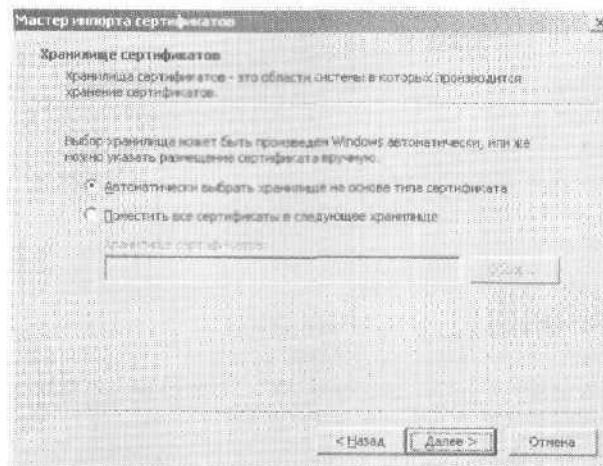


Рис. 6-21. Сообщение о проблемах с сертификатом безопасности узла

Сообщение вызвано тем, что пользователь не доверяет вашему корневому СА. Сейчас он может продолжить подключение, щелкнув Yes (Да), прервать его, щелкнув No (Нет), или просмотреть сертификат корневого СА, щелкнув View Certificate (Просмотр сертификата).

3. Щелкните View Certificate (Просмотр сертификата). Откроется диалоговое окно Certificate (Сертификат).
4. На вкладке General (Общие) будет указано, что данный сертификат ненадежен. Чтобы установить доверие, щелкните Install Certificate (Установить сертификат).
5. Запустится мастер Certificate Import Wizard (Мастер импорта сертификатов). Щелкните Next.
6. Поставьте переключатель в положение Automatically Select The Certificate Store Based On The Type Of Certificate (Автоматически выбрать хранилище на основе типа сертификата) (рис. 6-22) и щелкните Next.
7. Щелкните Finish (Готово). Параметры по умолчанию позволяют браузеру выбрать хранилище для сертификата, основываясь на типе последнего.
8. Щелкните ОК и затем — Yes (Да), чтобы продолжить работу. Предупреждение о проблемах безопасности больше выводиться не будет.





**Рис. 6-22.** Мастер Certificate Import Wizard (Мастер импорта сертификатов)

### Проверка работоспособности SSL

Соединения безопасны, только если браузер подключается к серверу при помощи безопасного URL, начинающегося с *https://*. Если какое-либо вложенное содержимое (например, изображения) загружается с защищенной Web-страницы по обычному соединению, браузер сообщает пользователю, что часть содержимого небезопасна, и спрашивает, продолжить ли загрузку.

Включив SSL на сервере, убедитесь, что протокол работает и уровень шифрования задан правильно.

1. Обратитесь к своему Web-узлу по безопасному URL, начинающемуся с *https://*. Значок замка на панели в нижней части окна Internet Explorer указывает, что создан SSL-сеанс. Если значка нет — SSL-сеанс не создан.
2. Щелкните в любом месте страницы правой кнопкой и выберите в контекстном меню команду Properties (Свойства). Откроется одноименное диалоговое окно с информацией о Web-странице.
3. Щелкните Certificates (Сертификаты), перейдите на вкладку Details (Состав) и просмотрите сведения о сертификате и используемом уровне шифрования.

Проверить, работает ли SSL в Netscape Navigator, можно так.

1. Обратитесь к **своему** Web-узлу по безопасному URL, начинающемуся с *https://*. На панели в нижней части окна Netscape Navigator должен отображаться значок закрытого замка, указывая, что создан SSL-сеанс.
2. **Щелкните** значок замка. **Откроется** Netscape Personal Security Manager, отображающий используемый уровень шифрования.

### Устранение проблем с SSL

Если протокол SSL не работает, убедитесь, что сервер сертификатов установлен на **правильном** Web-узле и что на этом узле включена поддержка SSL. Это поможет вам **устранить** проблемы SSL, **связанные** с сервером.

В случае проблем с уровнем шифрования убедитесь, что браузер поддерживает **используемый** вами уровень. Если браузер поддерживает 128-разрядное шифрование, а в его диалоговом окне свойств сконфигурировано 40-разрядное, нужно обновить сертификат сервера для 128-разрядного шифрования.

Поддерживаемый уровень шифрования в Internet Explorer проверяется так.

1. В меню Help (Справка) **выберите** команду About Internet Explorer (О программе).
2. В поле Cipher Strength (Стойкость шифра) отображается поддерживаемый уровень шифрования. Для создания 128-разрядного сеанса браузер должен поддерживать 128-разрядное **шифрование**. Щелкните OK.
3. В меню Tools (Сервис) выберите команду Internet Options (Свойства обозревателя) и перейдите на вкладку Advanced (Дополнительно).
4. Прокрутите содержимое окна до заголовка Security (Безопасность). **Убедитесь**, что помечены флажки Use SSL 2.0 (SSL 2.0) и Use SSL 3.0 (SSL 3.0). Щелкните OK.

Поддерживаемый уровень шифрования в Netscape Navigator проверяется так.

1. Щелкните значок замка на панели в нижней части окна Netscape Navigator. Откроется Netscape Personal Security

Manager, отображающий используемый уровень шифрования.

2. Перейдите на вкладку **Advanced** и щелкните **Options**. Вы увидите три флажка, которые по умолчанию должны быть помечены **Enable SSL Version 2**, **Enable SSL Version 3** и **Enable TLS**. Убедитесь, что выбраны минимум два первых флажка.
3. Щелкните **Close**, чтобы сохранить изменения.

## Управление сертификатами узлов с помощью оснастки Internet Information Services

Рассмотрим управление установленным сертификатом Web-узла из оснастки Internet Information Services.

### Просмотр и внесение изменений в выданные сертификаты

Сертификат содержит идентификационные и географические сведения, передававшиеся в оригинальном запросе на него. У него также имеется ряд свойств, задаваемых CA. Они описывают сертификат, область его допустимого использования, а также узел, для которого сертификат действителен. Вы также можете обновить дружественное имя, заданное при создании сертификата, ввести подробное описание сертификата и изменить область его применения.

Просмотреть или изменить сертификат узла можно так.

1. В оснастке Internet Information Services щелкните правой кнопкой значок узла и выберите в контекстном меню команду **Properties** (Свойства).
2. На вкладке **Directory Security** (Безопасность каталога) щелкните **View Certificate** (Просмотр). Откроется диалоговое окно **Certificate** (Сертификат) (рис. 6-23).
3. Для просмотра свойств, определенных при выдаче сертификата, перейдите на вкладку **Details** (Состав). В поле отображается:
  - **Version** (Версия) — версия X.509, использовавшаяся при создании сертификата;
  - **Serial Number** (Серийный номер) — уникальный серийный номер сертификата;

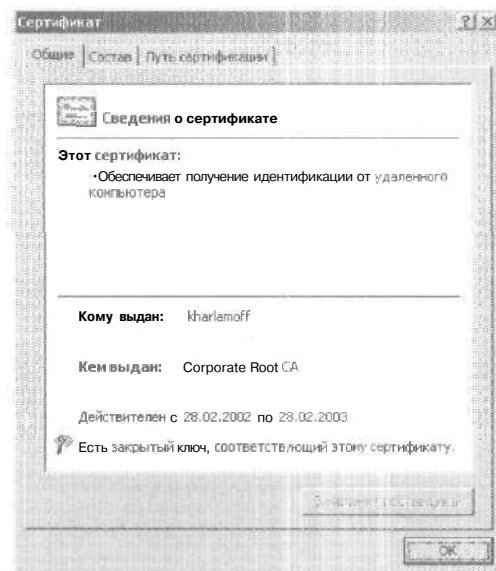
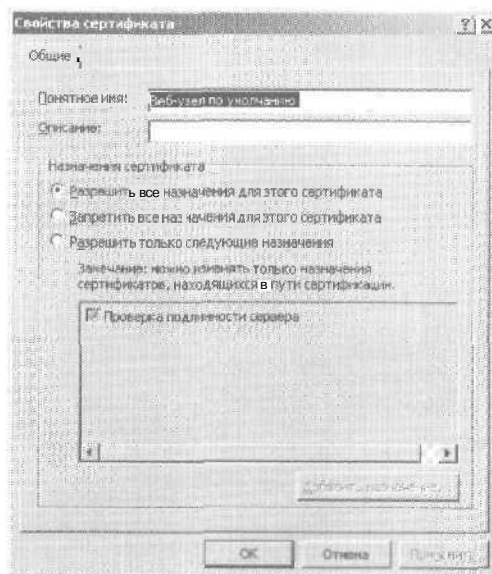


Рис. 6-23. Диалоговое окно Certificate (Сертификат)

- **Signature Algorithm** (Алгоритм подписи) — алгоритм шифрования, использовавшийся для создания подписи сертификата;
- **Issuer** (Поставщик) — организация, выдавшая сертификат;
- **Valid From** (Действителен с) — срок начала действия сертификата;
- **Valid To** (Действителен по) — срок окончания действия сертификата;
- **Subject** (Субъект) - владелец сертификата (обычно — идентификационные и географические сведения);
- **Public Key** (Открытый ключ) — зашифрованный открытый ключ сертификата;
- **Thumbprint Algorithm** (Алгоритм печати) — алгоритм шифрования, использовавшийся для создания образца сертификата;
- **Thumbprint** (Печать) - зашифрованный образец подписи;

- **Friendly Name** (Понятное имя) — описательное имя сертификата,
4. Чтобы просмотреть или изменить список применений сертификата, на вкладке Details (Состав) щелкните Edit Properties (Свойства). Откроется диалоговое окно Certificate Properties (Свойства сертификата) (рис. 6-24).



**Рис. 6-24.** Диалоговое окно Certificate Properties (Свойства сертификата)

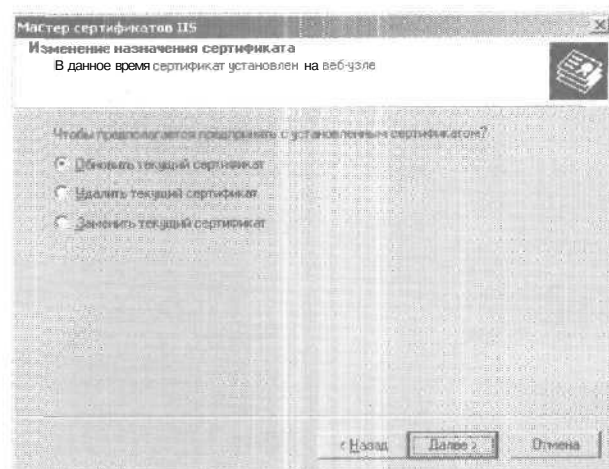
### Обновление, удаление и замена сертификатов

Как вы помните, сертификаты надо ежегодно обновлять. Кроме того, при необходимости сертификаты можно заменять и удалять. Чтобы обновить/удалить/заменить сертификат, сделайте так.

1. В оснастке Internet Information Services щелкните значок узла правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите на вкладку Directory Security (Безопасность каталога) и в группе Secure Communications (Безопасные

подключения) щелкните Server Certificate (Сертификат). Запустится мастер Web Server Certificate Wizard (Мастер сертификатов веб-сервера). Щелкните Next.

3. Вам будет предложено обновить, удалить или заменить имеющийся сертификат (рис. 6-25). Поставьте переключатель в нужное положение и продолжите работу с мастером.



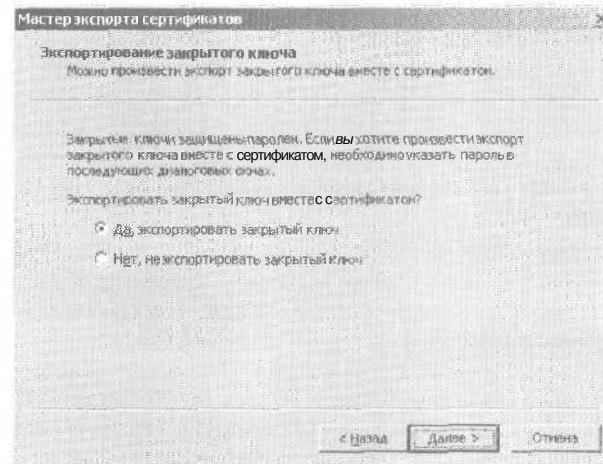
**Рис. 6-25.** Обновление, удаление или замена сертификата с помощью мастера Web Server Certificate Wizard (Мастер сертификатов веб-сервера)

#### Экспорт сертификатов узла

Сертификаты узла можно экспортировать в файл.

1. В оснастке Internet Information Services щелкните значок узла правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке Directory Security (Безопасность каталога) щелкните View Certificate (Просмотр). Откроется диалоговое окно Certificate (Сертификат) (рис. 6-23).
3. Перейдите на вкладку Details (Состав) и щелкните Copy To File (Копировать в файл). Запустится мастер Certificate Export Wizard (Мастер экспорта сертификатов). Щелкните Next.

4. Вам будет предложено экспортировать файл сертификата вместе с соответствующим закрытым ключом или без него (рис. 6-26). Чтобы экспортировать закрытый ключ, щелкните Yes (Да); в противном случае — No (Нет). Щелкните Next.



**Рис. 6-26.** Мастер Certificate Export Wizard (Мастер экспорта сертификатов)

5. В следующем окне будет предложено выбрать формат экспортируемого файла. Формат по умолчанию вполне подойдет; запомните его и щелкните Next.
6. При экспортировании закрытого ключа вам потребуется задать пароль для файла сертификата. Введите в соответствующие поля пароль и его подтверждение, затем щелкните Next (Далее).
7. Укажите имя экспортируемого файла. Кроме того, можно щелкнуть Browse (Обзор) и задать путь и имя файла R в диалоговом окне Save As (Сохранить как).
8. Щелкните Next и затем — Finish (Готово). Щелкните OK, чтобы подтвердить успешное экспортирование сертификата. Дважды щелкните OK, чтобы вернуться к оснастке Internet Information Services.

### Игнорирование, принятие и требование клиентских сертификатов

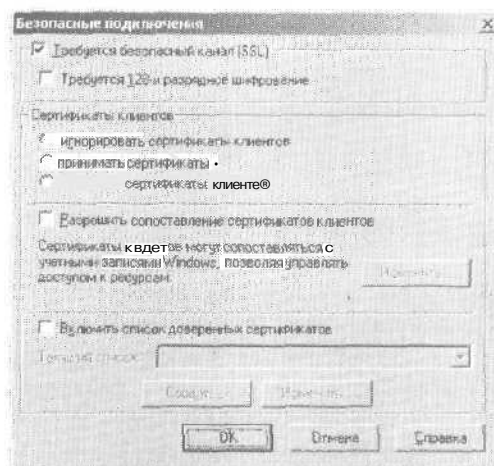
Клиентские сертификаты позволяют пользователям подтверждать свою подлинность с помощью Web-браузера. Такие сертификаты можно применять при наличии внешнего защищенного Web-узла, например в случае со внешней сетью. Если Web-узел принимает или требует клиентские сертификаты, можно сконфигурировать сопоставления, обеспечивающие управление доступом к ресурсам на основе клиентских сертификатов. Клиентский сертификат может сопоставляться конкретной учетной записи Windows методом «один к одному» или в соответствии с заданными администратором правилами.

По умолчанию IIS не принимает и не требует клиентских сертификатов, но это можно изменить. Помните: принятие клиентских сертификатов не то же самое, что требование их предоставления. Если узел требует предоставлять клиентские сертификаты, к нему можно обращаться только по защищенным SSL-подключениям, обычный HTTP-доступ невозможен. Если же узел лишь принимает, но не требует клиентские сертификаты, к нему можно обращаться как по протоколу HTTP, так и по HTTPS.

Политика узла в отношении клиентских сертификатов определяется так.

1. В оснастке Internet Information Services щелкните значок Web-узла правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите на вкладку Directory Security (Безопасность каталога) и в группе Secure Communications (Безопасные подключения) щелкните Edit (Изменить). Откроется диалоговое окно Secure Communications (Безопасные подключения) (рис. 6-27).
3. Чтобы потребовать применение SSL (и исключить использование незащищенных подключений), пометьте флажок Require Secure Channel (Требуется безопасный канал). Если на сервере установлена и включена поддержка 128-разрядного шифрования, можно также пометить флажок Require 128-bit Encryption (Требуется 128-и разрядное шифрование).





**Рис. 6-27.** Диалоговое окно Secure Communications (Безопасные подключения)

4. В группе Client Certificates (Сертификаты клиентов) поставьте переключатель в нужное положение — Ignore client certificates (игнорировать сертификаты клиентов), Accept client certificates (принимать сертификаты) или Require client certificates (требовать сертификаты клиентов).



**Примечание** Требовать клиентские сертификаты можно, только если сервер также требует использования безопасных SSL-подключений. В связи с этим следует пометить и флажок Require Secure Channel (Требуется безопасный канал).

5. Для сопоставления клиентских сертификатов учетным записям пользователей Windows пометьте флажок Enable Client Certificate Mapping (Разрешить сопоставление сертификатов клиентов) и щелкните Edit (Изменить). В открывшемся диалоговом окне Account Mappings (Сопоставление с учетными записями) сконфигурируйте сопоставление сертификатов.
6. Чтобы принимать лишь клиентские сертификаты, выданные определенными CA, пометьте флажок Enable Certificate Trust List (Включить список доверенных сертификатов) и щелкните New (Создать). Запустится мастер

Certificate Trust List Wizard (Мастер списков доверия сертификатов), позволяющий задать доверенные сертификаты корневых СА. Узел будет принимать сертификаты, выданные доверенными корневыми СА; прочие сертификаты приниматься не будут.

7. Дважды щелкните ОК.

#### **Требование SSL для всех подключений**

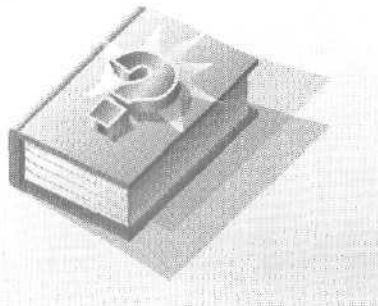
Иногда необходимо создавать узлы, принимающие лишь защищенные подключения. Для этого потребуйте использования SSL и исключите незащищенные подключения.

1. В оснастке Internet Information Services щелкните значок Web-узла правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите на вкладку Directory Security (Безопасность каталога) и в группе Secure Communications (Безопасные подключения) щелкните Edit (Изменить). Откроется диалоговое окно Secure Communications (Безопасные подключения) (рис. 6-27).
3. Чтобы потребовать использования SSL и исключить незащищенные подключения, пометьте флажок Require Secure Channel (Требуется безопасный канал).
4. Если на сервере установлена и включена поддержка 128-разрядного шифрования, также пометьте флажок Require 128-bit Encryption (Требуется 128-и разрядное шифрование).
5. Дважды щелкните ОК.

## Часть III

# Управление основными службами

В этой части обсуждается администрирование ключевых служб IIS, постоянно развертываемых на Web-узлах. Глава 7 посвящена управлению службой File Transfer Protocol: конфигурированию FTP-серверов, управлению доступом к каталогам и пользовательскими сеансами, обеспечению безопасности FTP-серверов. В главе 8 рассматриваются конфигурирование и поддержка протокола Simple Mail Transfer Protocol. Я расскажу, как конфигурировать SMTP-серверы, организовать и маршрутизировать сообщения для доставки, задавать параметры доставки и обеспечивать безопасность SMTP-серверов. В главе 9 мы обсудим использование службы Indexing Service (Служба индексирования), включая создание и управление каталогами, оптимизацию производительности и проверку параметров индексирования.



## Глава 7

# Управление FTP-серверами

Протокол FTP применяется для передачи файлов между компьютерами. Управление FTP-серверами аналогично управлению WWW-узлами и серверами. FTP-узлы могут использоваться как в Интернете, так и в корпоративных интрасетях. FTP-узлам для Интернета обычно назначают полные доменные имена и общедоступные IP-адреса, а FTP-узлам для интрасетей — частные IP-адреса и локально разрешаемые имена.

Как и в случае с Web-узлами, свойства FTP-узла идентифицируют его, задают конфигурационные параметры и определяют порядок доступа к документам. Свойства по умолчанию Web-узла можно задать на разных уровнях: глобальном, на уровне узла или папки.

Глобальные свойства по умолчанию задаются в окне *основных свойств FTP-службы* и наследуются всеми новыми FTP-узлами. На уровне узла они задаются в диалоговом окне *свойств FTP-узла* и распространяются только на данный FTP-узел. Свойства папок по умолчанию задаются в диалоговом окне *свойств папки* и распространяются только на конкретную папку.

### Обзор протокола FTP

В этом разделе обсуждается использование протокола FTP, включая передачу файлов, доступ к FTP-серверам и создание FTP-сеансов.

#### Основы протокола FTP

FTP — это клиент-серверный протокол для передачи файлов. Он позволяет подключиться к FTP-узлу, найти нужный файл в структуре папок и загрузить его. Кроме того, по FTP можно закачивать файлы на FTP-сервер. Разница между

загрузкой и закачкой файла существенна. При загрузке файла сервер передает данные клиенту, а при закачке — наоборот.

Из-за возрастающей популярности HTTP протокол FTP используют все реже. Между тем, хотя HTTP и позаимствовал некоторые функции FTP, последний остается лучшим средством создания удобного в применении и поддержке ресурса для обмена файлами. Как и HTTP, FTP использует в качестве транспортного протокола Transmission Control Protocol (TCP), FTP в отличие от HTTP ориентирован на сеансы, т. е. FTP-подключения являются постоянными. Соединение с FTP-сервером остается открытым даже после завершения передачи файлов.

На поддержку постоянных подключений нужны системные ресурсы, и производительность сервера с большим числом клиентов может заметно снизиться. В связи с этим число и продолжительность сеансов на многих FTP-серверах ограничены. По умолчанию время ожидания сеанса для FTP-узла — 900 секунд (15 минут).

Поскольку FTP — клиент-серверный протокол, успешная передача файлов зависит от нескольких факторов. На компьютере-сервере должно выполняться серверное ПО FTP, например Internet Information Services. На компьютере-клиенте — клиентское ПО FTP, например, Microsoft Internet Explorer 5.0 или FTP-утилита командной строки, имеющаяся в Microsoft Windows 2000.

Передача файлов может осуществляться в ASCII- или двоичном режиме. Используйте ASCII-передачу, когда работаете с текстовыми документами и хотите сохранить указатели конца строки, а передачу в двоичном формате — при операциях с исполнимыми файлами. Передача в двоичном формате целесообразна и для других типов файлов.

### Управление доступом к FTP-серверу

Большинство FTP-клиентов и серверов допускают анонимную передачу файлов, т. е. анонимное подключение клиента к серверу и последующий обмен файлами. Как следует из названия, цель анонимной передачи — позволить всем подключаться к серверам и обмениваться файлами. Обычно при работе с Internet Explorer или другим FTP- клиен-

том анонимная передача файлов может начинаться автоматически.

Так, для подключения к FTP-серверу Microsoft введите в поле Address (Адрес) своего браузера URL `ftp://ftp.microsoft.com/public/`. Здесь `ftp://` — обозначение протокола FTP, `ftp.microsoft.com` — адрес сервера, к которому осуществляется подключение, и `public` — имя папки на сервере. FTP-клиент автоматически предоставляет необходимые имя пользователя и пароль. При анонимном FTP-подключении ими будут имя `anonymous` и пароль в виде вашего адреса электронной почты или пустой строки. Если клиент не может автоматически заполнить нужные поля, введите `anonymous` как имя пользователя и адрес электронной почты — в качестве пароля.

Доступ к FTP-серверу может быть ограничен, и тогда к нему будут обращаться лишь пользователи, прошедшие проверку подлинности. При подключении к серверу клиенту будет предложено ввести имя и пароль. Это должны быть имя и пароль учетной записи, имеющейся на локальном компьютере или в домене, где состоит данная система.

Имя и пароль можно указывать к URL для доступа к серверу в формате:

```
ftp://имя_пользователя:пароль@имя_сервера:порт/путь_к_ресурсу
```

Здесь `ftp://` — обозначение протокола FTP, `имя_пользователя` — имя учетной записи, и `пароль` — соответствующий пароль. Если имя пользователя — `wrstanek`, а пароль — `mydingo123`, надо ввести:

```
ftp://wrstanek:mydingo123@ftp.microsoft.com/public/
```

Получив доступ к серверу, анонимно или посредством проверки подлинности, пользователь не обязательно сможет загружать или закачивать файлы. Диапазон допустимости его действий зависит от параметров безопасности. Как говорилось в главе 5 «Управление безопасностью Web-сервера», параметры безопасности задаются на двух уровнях: Windows и IIS. На уровне Windows создаются учетные записи пользователей и групп, определяются разрешения на доступ к файлам и папкам, а также конфигурируется групповая

политика. На уровне ИС определяются разрешения FTP-сервера, конфигурируется система проверки подлинности и задаются TCP/IP-ограничения доступа.

### Использование FTP-сеансов

После того как клиент получит доступ к FTP-серверу (анонимно или пройдя проверку подлинности), создается TCP-подключение, остающееся открытым даже по завершении пользовательского сеанса или истечении срока ожидания на стороне сервера. FTP-клиент и сервер устанавливают соединение путем трехэтапного обмена подтверждающими сигналами. В этом обмене участвуют два выделенных TCP-порта FTP-сервера и два динамически назначаемых TCP-порта клиентской системы, сопоставляемые выделенным портам сервера.



**Примечание** TCP/IP-соединения тоже создаются на сетевом уровне модели OSI путем трехэтапного обмена подтверждающими сигналами. FTP-подключения создаются на прикладном уровне этой модели.

По умолчанию FTP-сервер использует порты 20 и 21. Порт 20 применяется для обмена FTP-данных и открыт лишь при приеме-передаче информации. Порт 21 служит для обмена управляющей информацией FTP, на нем ведется прослушивание клиентов, пытающихся установить соединение. После создания FTP-сеанса подключение к порту 21 остается открытым, пока не будет завершен пользовательский сеанс.

Два порта клиентской системы динамически назначаются из диапазона 1024-5000. При создании FTP-сеанса клиент открывает через управляющий порт соединение с портом 21 сервера, применяемое для управления FTP-сеансом. Подключение к порту данных сервера осуществляется не автоматически, а лишь когда начинается клиент-серверный обмен данными. Для передачи данных клиент открывает новый порт данных и подключается к порту данных сервера (по умолчанию — порт 20). Завершив передачу, клиент освобождает порт. В следующий раз для передачи информации клиент откроет новый порт, номер которого обычно отличается от ранее использовавшегося.



**Примечание** Номера динамически назначаемых портов находятся вне диапазонов, зарезервированных для прочих TCP- и UDP-служб. Поскольку порты 0-1023 зарезервированы для TCP- и UDP-служб, протокол FTP использует порты 1024-5000 (этот диапазон задается в реестре Windows и теоретически его верхний предел — 65 535). Полный перечень используемых TCP- и UDP-портов см. в разделе `\%SystemRoot%\System32\Drivers\Etc\Services` реестра.

Как же создаются и используются при передаче данных FTP-сеансы?

1. FTP-сервер прослушивает запросы клиентов на выделенном управляющем порте. Номер этого порта по умолчанию — 21.
2. При запросе пользователем ресурсов FTP-сервера FTP-клиент динамически назначает управляющий порт и связывает его с управляющим портом сервера. Например, порт 1025, связанный с портом 20 сервера.
3. После установления соединения клиент и сервер могут взаимодействовать через управляющий порт.
4. Перед передачей данных клиент динамически назначает порт данных и связывает его с портом данных сервера. При каждой передаче файла клиент открывает и затем закрывает новый порт данных. Например, передает первый файл через порт 1057, второй — через порт 1058 и т. д.
5. FTP-сеанс остается открытым, пока не будет завершен или пока не истечет время ожидания на стороне сервера.

Для мониторинга FTP-сеансов на серверах и клиентских компьютерах можно воспользоваться утилитой командной строки Netstat, отображающей состояние сетевых подключений. При вызове Netstat укажите, что требуется просматривать список TCP-подключений с обновлением информации через определенный интервал времени. В следующем примере Netstat будет обновлять статистику подключений каждые 15 секунд:

```
netstat -p tcp 15
```

Запустив Netstat на клиентской системе, вы сможете наблюдать за FTP-активностью компьютера. Например, после ус-



тановления связи с FTP-сервером выводится сообщение наподобие этого:

Активные подключения

```
Имя Локальный адрес Внешний адрес Состояние
TCP engsvr01:ftp engsvr01:1043 ESTABLISHED
TCP engsvr01:1043 engsvr01:ftp ESTABLISHED
```

Здесь FTP-соединение установлено через порт 1043, связанный с управляющим портом FTP. При получении данных с сервера клиент открывает и сопоставляет порт данных. По завершении передачи этот порт переходит в состояние `TIME_WAIT` и пребывает в нем, пока не истечет срок ожидания и он не будет закрыт. Управляющий порт находится в состоянии `ESTABLISHED` все время, пока открыто соединение. Состояния портов отображаются так:

Активные подключения

```
Имя Локальный адрес Внешний адрес Состояние
TCP engsvr01:ftp-data engsvr01:1045 TIME_WAIT
TCP engsvr01:ftp engsvr01:1043 ESTABLISHED
TCP engsvr01:1043 engsvr01:ftp ESTABLISHED
```

После закрытия соединения с FTP-сервером остается лишь запись о сопоставлении управляющих портов клиента и сервера. Сопоставление переходит в состояние `TIME_WAIT` и остается в нем до истечения срока ожидания сеанса:

Активные подключения

```
Имя Локальный адрес Внешний адрес Состояние
TCP engsvr01:1043 engsvr01:ftp TIME_WAIT
```



**Примечание** Помните: клиент может открыть несколько соединений с сервером. При этом на наблюдаемой клиентской системе будет отображаться несколько записей о состоянии задействованных управляющих портов и портов данных.

### Именованное и идентификация FTP-узлов

Все FTP-узлы, развернутые в организации, обладают уникальными идентификаторами, позволяющими принимать запросы и реагировать на них. Идентификатор включает имя компьютера или DNS-имя, IP-адрес и номер порта.

Состав идентификатора зависит от того, где находится сервер, на котором размещен FTP-узел, — в частной или общедоступной сети. Например, в частной *сети* компьютер с именем CorpFTP имеет IP-адрес 10.0.0.25. Для доступа к FTP-узлу на нем можно задействовать:

- **UNC-путь** (Uniform Naming Convention, универсальные правила именования) — \\CorpFTP или \\10.0.0.25;
- **URL** (Uniform Resource Locator, универсальный указатель ресурса) — ftp://CorpFTP/ или ftp://10.0.0.25/;
- **URL и номер порта** — ftp://CorpFTP:21/ или ftp://10.0.0.25:21/.

Другой пример: в общедоступной сети компьютер с именем MoonShot имеет DNS-имя ftp.microsoft.com и IP-адрес 207.46.230.210. Для доступа к FTP-узлу на нем можно использовать:

- **URL** - ftp://ftp.microsoft.com/ или ftp://207.46.230.210/;
- **URL и номер порта** — ftp://ftp.microsoft.com:21/ или ftp://207.46.230.210:21/.

Используя различные комбинации IP-адресов, номеров портов и имен заголовков узлов, на одном компьютере можно размещать несколько узлов. Это дает некоторые преимущества. Например, вместо настройки трех разных компьютеров для размещения FTP-узлов ftp.microsoft.com, ftp.msn.com и ftp.adatum.com вы размещаете их на одном компьютере.



**Примечание** На компьютерах с Windows 2000 Professional можно разместить лишь один Web-узел и один FTP-сервер. Чтобы разместить несколько Web- или FTP-узлов, обновите ОС до Windows 2000 Server.

## Управление основными свойствами FTP-службы

Основные свойства FTP-службы определяют значения по умолчанию свойств FTP-узлов, создаваемых на сервере. Изменения глобальных свойств наследуются существующими FTP-узлами. На необязательной основе наследуются лишь изменения разрешений па доступ — вам будет предложено указать, какие узлы и папки должны наследовать их.

Основные свойства FTP-службы изменяются так.

1. В оснастке Internet Information Services щелкните правой кнопкой значок компьютера и выберите в контекстном меню команду Properties (Свойства). Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2.
2. В группе Master Properties (Основные свойства) выберите из раскрывающегося списка пункт FTP Service (FTP-служба) и щелкните Edit (Изменить). Откроется диалоговое окно FTP Service Master Properties (Основные свойства FTP-службы) для данного компьютера.
3. Внесите изменения и дважды щелкните ОК.

### Создание FTP-узлов

При установке в составе IIS службы FTP Publishing Service (Служба FTP-публикаций) автоматически создается FTP-узел по умолчанию. Его расположение по умолчанию — Inetpub\Ftproot. Вложенные папки этого каталога составляют структуру FTP-узла, а файлы — его содержимое. Для доступа к FTP-узлу клиент может применить имя FTP-сервера или ввести в поле Address (Адрес) браузера соответствующий URL.

Дополнительные FTP-узлы создаются так.

1. Убедитесь в наличии на FTP-узле службы FTP Publishing Service (Служба FTP-публикаций).
2. Если FTP-узел будет использовать новый IP-адрес, его нужно предварительно настроить. Подробнее см. главу 15 книги «Microsoft Windows 2000. Справочник администратора».
3. В оснастке Internet Information Services щелкните значок компьютера правой кнопкой и выберите в контекстном меню команду New\FTP Site (Создать\Узел FTP). Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2.
4. Запустится мастер FTP Site Creation Wizard (Мастер создания FTP-узла). Щелкните Next (Далее). В поле Name

- (Описание) введите описательное имя FTP-узла, например *Corporate FTP Server*. Снова щелкните Next.
5. В списке IP Address selection (IP-адрес) можно выбрать доступный IP-адрес (рис. 7-1). Щелкните (All Unassigned) [(Значения не присвоены)], чтобы узел мог использовать все неназначенные IP-адреса сервера. Один IP-адрес может использоваться несколькими FTP-узлами, при условии, что им назначены разные номера портов.

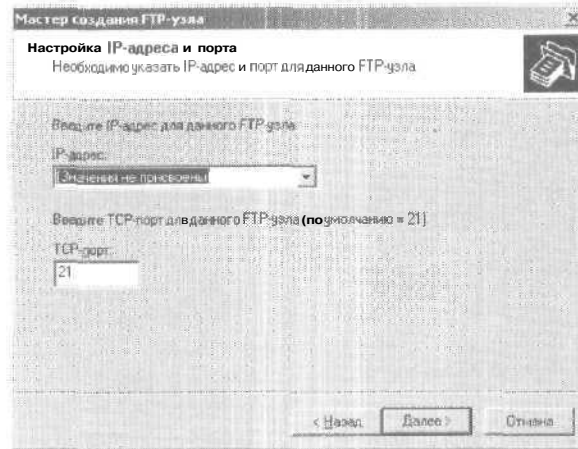



Рис. 7-1. Мастер FTP Site Creation Wizard  
(Мастер создания FTP-узла)

-  **Примечание** В FTP нет аналога заголовков узлов, используемых протоколом HTTP, т. е. для FTP-узлов нельзя использовать имена заголовков узлов.
6. Номер TCP-порта FTP-узла автоматически задается как 21. При необходимости в поле TCP Port (TCP-порт) можно ввести новый номер порта. Один номер порта может использоваться несколькими FTP-узлами, при условии, что им назначены разные IP-адреса.
7. В следующем диалоговом окне задают домашний каталог FTP-узла. Для поиска уже созданной папки щелкните Browse (Обзор). Папку можно создать с помощью Windows Explorer (Проводник). Щелкните Next.

8. Теперь можно задать разрешения доступа к FTP-узлу (рис. 7-2). Стандартные разрешения позволяют:
- Read (чтение) — загружать документы с узла;
  - Write (запись) — закидывать файлы на узел.
- Обычно рекомендуется назначить узлу только разрешение Read (чтение).

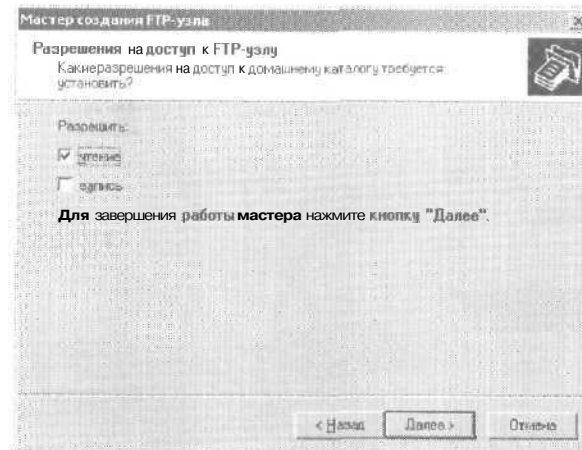


Рис. 7-2. Задание разрешений доступа к FTP-узлу

9. Щелкните Next, затем — Finish (Готово). Мастер создаст FTP-узел, но не запустит его. Прежде чем запустить узел и предоставить к нему доступ, нужно завершить настройку его свойств.

## Управление FTP-узлами

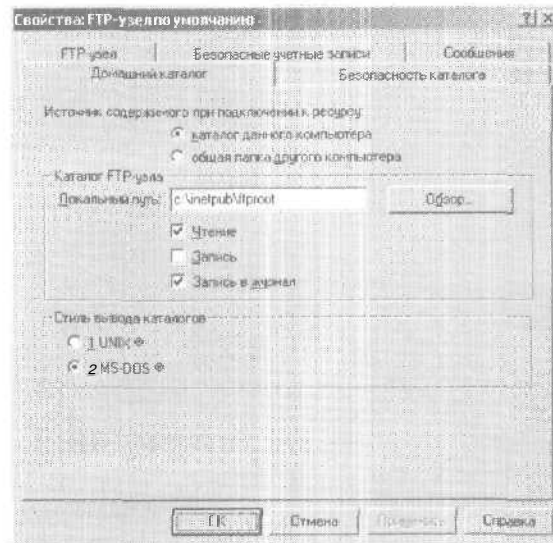
Большинством свойств Web-узла можно управлять из оснастки Internet Information Services.

### Задание домашнего каталога FTP-узла

Любой развернутый на сервере FTP-узел имеет домашний каталог — основную папку для обмена файлами. Домашний каталог связан с доменным именем узла или именем сервера. По умолчанию клиенты подключаются к узлу и попадают в этот каталог.

Домашний каталог узла можно просмотреть/изменить.

1. Запустите оснастку Internet Information Services и в левой панели раскройте узел нужного компьютера. Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2.
2. Щелкните значок FTP-узла правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
3. Перейдите на вкладку **Note Directory (Домашний каталог)** (рис. 7-3).



**Рис. 7-3.** Задание домашнего каталога узла

4. Если каталог находится на локальном компьютере, поставьте переключатель в положение **A Directory Located On This Computer** (каталог данного компьютера), и затем в поле **Local Path (Локальный путь)** введите путь к каталогу, например **C:\inetpub\ftproot**. Для поиска каталога щелкните **Browse (Обзор)**.
5. Если нужный каталог находится на другом компьютере и является сетевым ресурсом, поставьте переключатель в положение **A Share Located On Another Computer** (общая папка другого компьютера) и введите в поле **Network**

Directory (Сетевой путь) UNC-путь к ресурсу. Путь должен иметь вид \\ИмяСервера\ИмяРазделяемойПапки: например, \\Gandolf\CorpFTP. Затем щелкните Connect As (Подключить как), введите имя пользователя и пароль для подключения к сетевому ресурсу.



**Примечание** Если имя пользователя и пароль опущены, пользователь Everyone (Все) должен обладать доступом к указанному сетевому ресурсу. Иначе подключиться к нему будет невозможно.

6. Щелкните ОК.

### Изменение портов и IP-адресов узла

Каждый Web-узел обладает уникальным идентификатором, состоящим из номера TCP-порта, номера SSL-порта, IP-адреса и заголовка узла. Номер TCP-порта по умолчанию — 80, SSL-порта — 443. В качестве IP-адреса по умолчанию используется любой доступный IP-адрес.

Идентификатор Web-узла можно изменить.

1. Если FTP-узел будет использовать новый IP-адрес, его нужно предварительно настроить. Подробнее см. главу 15 книги «Microsoft Windows 2000. Справочник администратора».
2. Запустите оснастку Internet Information Services и в левой панели раскройте узел нужного компьютера. Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2.
3. Щелкните правой кнопкой значок FTP-узла и выберите в контекстном меню команду Properties (Свойства). Откроется одноименное диалоговое окно (рис. 7-4).
4. Поле Description (Описание) содержит описательное имя FTP-узла, которое отображается в оснастке Internet Information Services и для других целей не используется. Чтобы изменить его, введите в поле Description новое имя.
5. В списке IP Address selection (IP-адрес) можно выбрать доступный IP-адрес. Щелкните (All Unassigned) [(Значения не присвоены)], чтобы узел мог задействовать все неназначенные IP-адреса сервера. Один IP-адрес могут

использовать несколько **Web-узлов**, при условии, что им назначены разные номера портов.

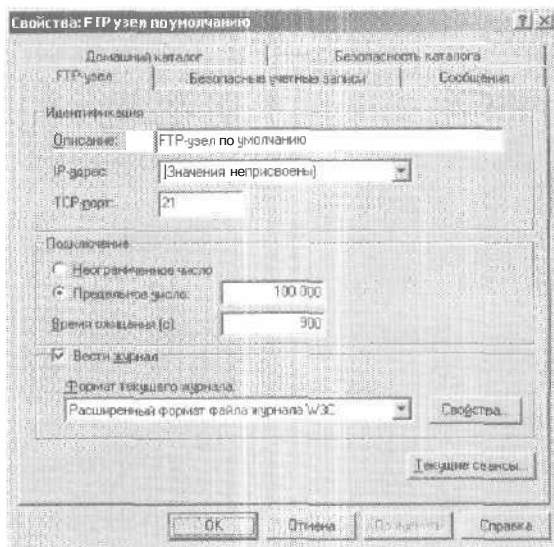


Рис. 7-4. Диалоговое окно свойств FTP-узла

6. Номер TCP-порта FTP-узла автоматически задается как 21. В поле TCP Port (TCP-порт) можно ввести и новый номер порта. Один номер порта могут задействовать несколько FTP-узлов, при условии, что им назначены разные IP-адреса.
7. Щелкните ОК.

#### **Ограничение числа входящих подключений и изменение времени ожидания соединения**

Для управления входящими подключениями FTP-узла можно ограничить число параллельных подключений и задать время ожидания соединения. Обычно FTP-узел принимает 100 000 подключений и имеет срок ожидания 900 секунд (15 минут). Если ресурсов сервера не хватает, можно ограничить число входящих подключений. Помните: если узел просматривает максимально допустимое число клиентов, новым посетителям придется ждать, пока не отключится кто-нибудь.



Когда время ожидания соединения истечет, сервер отключит простаивающий пользовательский сеанс. Время, определенное для FTP-узла по умолчанию (900 секунд) оптимально для большинства FTP-узлов. Если пользователи жалуются на слишком быстрое отключение простаивающих сеансов, увеличьте срок ожидания.

Чтобы изменить допустимое число параллельных подключений или задать время ожидания соединения, сделайте так.

1. В оснастке Internet Information Services щелкните правой кнопкой значок компьютера и выберите в контекстном меню команду Properties (Свойства). Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2. Затем правой же кнопкой щелкните нужный FTP-узел и выберите в контекстном меню команду Properties (Свойства).
2. Чтобы снять ограничения на число подключений, поставьте переключатель в группе Connections (Подключения) в положение Unlimited (Неограниченное число). Но учтите: делать это не рекомендуется. Чтобы ограничить число подключений к узлу, поставьте переключатель в положение Limit To Number Of Connections (Предельное число) и введите в соответствующее поле нужное значение.
3. В поле Connection Timeout (Время ожидания) задается время ожидания соединения. Если нужно, введите новое значение.
4. Щелкните ОК.



**Примечание** На поддержку подключений FTP-серверу требуются системные ресурсы. Чтобы снизить утечку ресурсов, ограничьте число подключений к серверу. Допустимое число подключений по умолчанию — 100 000 — оптимально для сервера среднего размера. Если же ресурсы сервера ограничены или он используется для других целей (скажем, на нем опубликован Web-узел), это число лучше уменьшить. Для выделенного FTP-сервера или сервера организации допустимое число подключений можно увеличить.

### Создание физических каталогов для FTP-узлов

Для загрузки и закачки файлов на FTP-узлах используют отдельные каталоги. Такая структура позволяет четко отличать файлы, опубликованные организацией, от файлов, закачанных пользователями. Вот типичное дерево каталогов FTP-узла:

- **C:\Inetpub\FTProot** — базовый каталог узла;
- **C:\Inetpub\FTProot\Public\** — базовый каталог для загрузки файлов;
- **C:\Inetpub\FTProot\Upload\** — базовый каталог для закачки файлов.

Имеющуюся структуру базовых каталогов можно дополнять вложенными папками. Например, компания-разработчик ПО может создать в каталоге **C:\Inetpub\FTProot\Public\** папки для;

- **Documentation** — документации;
- **Patches** — программных заплат;
- **Service\_Packs** — пакетов обновлений.



**Совет** Чтобы упростить посетителям понимание структуры папок узла, создайте приветственное сообщение, содержащее рекомендации по работе с узлом и карту папок — текстовый файл с подробным описанием имеющихся папок и их назначения. Сохраните карту папок в виде **.txt-файла** в базовом каталоге узла.

Для загрузки и закачки файлов можно сконфигурировать отдельные FTP-узлы. Папкам узла для загрузки следует назначить разрешения только на доступ, а папкам узла для закачки — только на запись. Таким образом, посетители смогут выполнять на конкретном узле лишь одно действие, и работа администратора упростится.

Физические каталоги FTP-узлов создаются в Windows Explorer (Проводник). Вложенные папки в домашнем каталоге FTP-узла создаются так.

1. Раскройте меню **Start\Programs\Accessories (Пуск\Программы\Стандартные)** и выберите **Windows Explorer**.
2. В левой части окна выделите домашний каталог FTP-узла.

3. В правой части окна щелкните правой кнопкой этот каталог и выберите в контекстном меню команду *New\Folder* (Создать\Папку). Система создаст новую папку и предложит изменить имя по умолчанию — *New Folder* (Новая папка).
4. Введите новое имя и нажмите клавишу *Enter*. Каталогам рекомендуется задавать краткие и информативные имена, например, *Documentation*, *Service\_Packs* или *Patches*.
5. Новая папка наследует разрешения по умолчанию домашнего каталога и *IS*-разрешения FTP-узла.



**Совет** Оснастка *Internet Information Services* не отображает новые папки автоматически. Возможно, потребуется щелкнуть кнопку *Refresh* (Обновить) на панели инструментов.

### Создание виртуальных каталогов

Виртуальные каталоги создаются в два этапа. Сначала надо создать физическую папку, а затем — связанный с ней виртуальный каталог. Виртуальные каталоги FTP-узлов могут допускать загрузку файлов, загрузку файлов или и то, и другое. Управлять передачей файлов очень просто. Папкам назначаются разрешения:

- для загрузки файлов — *Read* (чтение);
- для загрузки файлов - *Write* (запись);
- для загрузки и загрузки файлов — *Read* (чтение) и *Write* (запись).

Круг допустимых действий пользователя также определяется разрешениями, заданными на уровне файлов и папок. При анонимном подключении учетная запись *Internet Guest* (гостевая учетная запись Интернета) должна обладать необходимыми разрешениями уровня папки. При подключении с проверкой подлинности такими разрешениями должен обладать пользователь или группа, к которой он относится.

Виртуальный каталог создается так.

1. Запустите оснастку *Internet Information Services* и в левой панели раскройте узел нужного компьютера.
2. Правой кнопкой щелкните нужный FTP-узел и выберите в контекстном меню команду *New\Virtual Directory* (Создать\Виртуальный каталог). Запустится мастер *Vir-*

- tual Directory Creation Wizard (Мастер создания виртуальных каталогов). Щелкните Next (Далее).
3. В поле Alias (Псевдоним) введите имя для доступа к виртуальному каталогу. Рекомендуется сделать его кратким и информативным, как и имя обычной папки.
  4. В следующем диалоговом окне задайте домашний каталог FTP-узла. Для поиска уже созданной папки щелкните Browse (Обзор). При необходимости создайте папку с помощью Windows Explorer (Проводник).
  5. Задайте разрешения на доступ к виртуальному каталогу. Разрешение Read (чтение) позволяет загружать, а разрешение Write (запись) — закачивать файлы.
  6. Щелкните Next и затем — Finish (Готово). Система создаст виртуальный каталог.

### Перенаправление запросов к сетевым папкам

Если у вас имеются подключаемые к сети накопители или выделенный сервер для обмена данными, вы можете перенаправлять запросы к файлам узла на сетевые папки.

1. В оснастке Internet Information Services щелкните правой кнопкой нужный FTP-узел и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите на вкладку Home Directory (Домашний каталог) и поставьте переключатель в положение A Share Located On Another Computer (общая папка другого компьютера).
3. В поле Network Directory (Сетевой каталог) введите UNC-путь к сетевой папке. Он должен иметь вид \\ИмяСервера\ИмяСетевойПапки: например, \\Gandolf\CorpFTP. Затем щелкните Connect As (Подключить как) и в открывшемся диалоговом окне введите имя пользователя и пароль для подключения к сетевой папке.
4. Щелкните ОК. Теперь все файловые запросы к FTP-узлу будут перенаправлены на файлы указанного сетевого ресурса.

### Выбор способа отображения каталога

При обращении к FTP-серверу FTP-клиент автоматически получает список содержимого каталога, который может отображаться в стиле MS-DOS или UNIX.

Отображение в стиле MS-DOS более удобно и упрощает перемещение по каталогам. Отображение в стиле UNIX совместимо со старыми версиями браузеров, которые могут не поддерживать отображение в формате MS-DOS. Способ отображения каталогов задается на уровне узла.

1. В оснастке Internet Information Services щелкните правой кнопкой нужный FTP-узел и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите на вкладку Home Directory (Домашний каталог) и в группе Directory Listing Style (Стиль вывода каталогов) щелкните переключатель UNIX или MS-DOS.
3. Щелкните ОК.

### Создание информационных сообщений

FTP-узлы под управлением IIS могут выводить приветственное и завершающее сообщения, а также сообщение о максимальном числе подключений. Эти сообщения называются информационными и создаются на уровне узла. Для всех размещенных на сервере FTP-узлов можно определить разные наборы информационных сообщений.

- **Приветственные сообщения** отображаются при подключении клиента к FTP-серверу и содержат информацию о назначении узла, правилах его использования, расположении зеркальных узлов, администраторе и т. д. Рекомендуется сделать приветственное сообщение максимально информативным — 8-10 строк текста. Чтобы выделить сообщение на экране, заключите его, например, в строки звездочек.
- **Завершающие сообщения** выводятся клиенту при отключении от узла, но только если пользователь завершил активный сеанс с помощью FTP-команды QUIT. Если FTP-сеанс был завершен иначе, например щелчком кнопки Close в браузере, сообщение не выводится. Максимальный размер завершающего сообщения — одна строка.
- **Сообщения о максимальном числе подключений** выводятся при достижении максимально допустимого числа подключений к серверу. (Помните: максимально допустимое число подключений можно изменять, подробнее см. раздел «Ограничение числа входящих подключений и изменение времени ожидания соединения» этой главы.)

Информационные сообщения создаются так.

1. В оснастке Internet Information Services щелкните правой кнопкой нужный FTP-узел и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите на вкладку Messages (Сообщения).
3. В поле Welcome (Приветствие) введите приветственное сообщение.



**Примечание** Каждая строка текста должна заканчиваться вводом (символами возврата каретки и перевода строки). В противном случае сообщение может некорректно отображаться в FTP-клиенте браузера Internet Explorer.

4. В поле Exit (Выход) введите завершающее сообщение.
5. В поле Maximum Connections (Предельное число подключений) введите сообщение о максимальном числе подключений.
6. Щелкните ОК.

## Управление пользовательскими FTP-сеансами

Поддержка подключений к FTP-узлу требует ресурсов FTP-сервера. В целях упрощения мониторинга ресурсов IIS позволяет просматривать статистику пользовательских сеансов отдельно для каждого FTP-узла.

### Просмотр пользовательских FTP-сеансов

Пользовательские сеансы FTP-узла можно просмотреть.

1. В оснастке Internet Information Services щелкните нужный FTP-узел правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке FTP Site (FTP-узел) щелкните Current Sessions (Текущие сеансы). Откроется диалоговое окно FTP User Sessions (FTP-сеансы) (рис. 7-5). Его поля содержат:
  - Connected Users (Подключено пользователей) — имена учетных записей пользователей, прошедших проверку подлинности, и пароли анонимных пользователей;



**Совет** Помните: анонимному пользователю предлагается ввести в качестве пароля свой адрес электронной почты. Отличить прошедшего проверку пользователя от анонимного можно по значку. В первом случае отображается обычный значок пользователя, а во втором — значок с красным знаком вопроса.

- **From (От)** — IP-адреса или DNS-имена подключенных компьютеров;
- **Time (Время)** — время, прошедшее с начала сеанса в формате ЧЧ:ММ:СС.

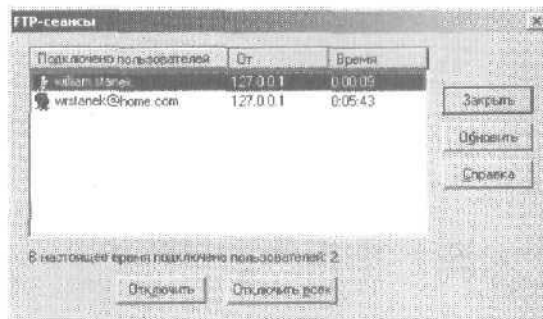


Рис. 7-5. Диалоговое окно FTP User Sessions (FTP-сеансы)

3. Щелкните Refresh (Обновить), чтобы обновить статистику сеансов, или Close (Закреть), чтобы закрыть диалоговое окно FTP User Sessions (FTP-сеансы),

### Просмотр общего числа подключенных пользователей

IIS отображает общее число подключенных к FTP-узлу пользователей в левом нижнем углу диалогового окна FTP User Sessions. Чтобы открыть его и просмотреть общее число подключенных пользователей, сделайте так,

1. В оснастке Internet Information Services щелкните нужный FTP-узел правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке FTP Site (FTP-узел) щелкните Current Sessions (Текущие сеансы). Откроется диалоговое окно FTP User Sessions (FTP-сеансы).

3. Общее число подключенных к FTP-узлу пользователей отображается в левом нижнем углу этого окна. Щелкните Refresh (Обновить), чтобы обновить статистику.

### Завершение пользовательских сеансов

На FTP-узле можно завершать отдельные или все активные пользовательские сеансы. Обычно к этому прибегают, если продолжительность сеанса чересчур велика или возникли проблемы с ресурсами сервера. Если в момент завершения сеанса пользователь закачивает или загружает файл, передача данных будет немедленно прекращена, а пользователь увидит сообщение о разрыве соединения удаленным узлом.

Отдельный пользовательский сеанс завершается так

1. В оснастке Internet Information Services щелкните правой кнопкой нужный FTP-узел и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке FTP Site (FTP-узел) щелкните Current Sessions (Текущие сеансы).
3. Выделите сеанс и щелкните Disconnect (Отключить).
4. При запросе системы подтвердите свои действия, щелкнув Yes (Да).
5. Дважды щелкните OK, чтобы вернуться к оснастке Internet Information Services.

Все пользовательские сеансы на FTP-узле завершаются так,

1. В оснастке Internet Information Services щелкните нужный FTP-узел правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке FTP Site (FTP-узел) щелкните Current Sessions (Текущие сеансы).
3. Щелкните Disconnect All (Отключить всех), и при запросе системы подтвердите свои действия, щелкнув Yes.
4. Дважды щелкните OK, чтобы вернуться к оснастке Internet Information Services.

### Управление безопасностью FTP-сервера

Управление безопасностью FTP-сервера во многом похоже на управление безопасностью Web-сервера и осуществляется на двух уровнях: Windows и IIS. На первом создают учет-



ные записи пользователей и групп, определяют разрешения на доступ к файлам и папкам, а также конфигурируют политики, на втором — разрешения на доступ к содержимому, конфигурируют систему проверки подлинности и задают привилегии операторов.



**Примечание** Большинство задач управления безопасностью FTP-узла аналогичны соответствующим задачам Web-сервера, и поэтому в данном разделе рассматриваются только специфические вопросы. Подробнее о безопасности IIS см. главу 5 этой книги.

### Управление анонимными подключениями

Управлять анонимными подключениями позволяет поименованная учетная запись, обладающая нужными разрешениями на доступ к папкам и файлам, доступным для загрузки и загрузки. По умолчанию для анонимного доступа применяется гостевая учетная запись Интернета *IUSR\_ИмяКомпьютера* (см. главу 5).

Если разрешен анонимный доступ, клиентам не нужно указывать имя пользователя и пароль. IIS автоматически регистрирует пользователя с применением сконфигурированной для ресурса учетной записи анонимного доступа. Если анонимный доступ запрещен, клиенты должны предоставлять реквизиты своих учетных записей. В отличие от Web-узлов управлять анонимным доступом можно только на глобальном уровне или на уровне узла. Управлять анонимным доступом на уровне пайки или файла невозможно.

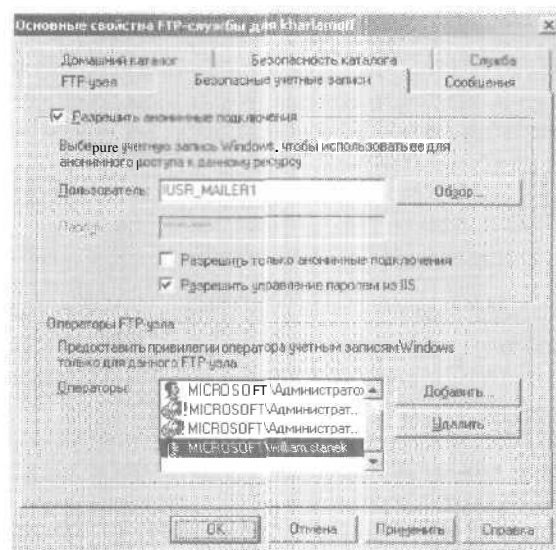
### Конфигурирование анонимного доступа на глобальном уровне

Параметры анонимного доступа ко всем FTP-узлам сервера конфигурируются так.

1. В оснастке Internet Information Services щелкните правой кнопкой значок нужного компьютера и выберите в контекстном меню команду Properties (Свойства).
2. В списке Master Properties (Основные свойства) выберите пункт FTP Service (FTP-служба) и щелкните Edit (Изменить). Откроется диалоговое окно FTP Service Master

Properties (Основные свойства FTP-службы) для данного компьютера.

3. Перейдите на вкладку Security Accounts (Безопасные учетные записи) (рис. 7-6).



**Рис. 7-6.** Вкладка Security Accounts (Безопасные учетные записи) диалогового окна FTP Service Master Properties (Основные свойства FTP-службы)

4. Чтобы разрешить анонимный доступ, пометьте флажок Allow Anonymous Access (Разрешить анонимные подключения) и перейдите к п. 5. Для запрещения анонимного доступа снимите флажок Allow Anonymous Access и перейдите к п. 6. При этом к узлу смогут обращаться только прошедшие проверку подлинности пользователи.
5. Сконфигурируйте локальные учетные записи или учетные записи домена для доступа к FTP-узлам сервера:
  - поле Username (Пользователь) содержит имя учетной записи для анонимного доступа к ресурсу; его можно изменить или, щелкнув Browse (Обзор), выбрать учетную запись в диалоговом окне Find User (Выбор: Пользователь);

- флажок Allow Only Anonymous Connections (Разрешить только анонимные подключения) запрещает пользователям подключаться к узлу с указанием имени и пароля; пометьте его, если нужен только анонимный доступ к узлу, если нет — снимите;
  - флажок Allow IIS To Control Password (Разрешить управление паролем из IIS) определяет, разрешено ли управление паролем учетной записи анонимного доступа из IIS; обычно это то, что нужно, — пометьте флажок; или снимите его и введите пароль учетной записи для анонимного доступа.
6. Дважды щелкните ОК. Произведенные изменения будут автоматически унаследованы всеми FTP-узлами сервера.

### Конфигурирование анонимного доступа на уровне узла

Параметры анонимного доступа к отдельному FTP-узлу конфигурируются так.

1. В оснастке Internet Information Services щелкните значок нужного FTP-узла правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите на вкладку Security Accounts (Безопасные учетные записи).
3. Чтобы разрешить анонимный доступ, пометьте флажок Allow Anonymous Access (Разрешить анонимные подключения) и перейдите к п. 4. Для запрещения — снимите флажок Allow Anonymous Access и перейдите к п. 8. При этом к узлу смогут обращаться только прошедшие проверку подлинности пользователи.
4. Вам потребуется сконфигурировать локальные учетные записи или учетные записи домена для доступа к FTP-узлам сервера:
  - поле Username (Пользователь) содержит имя учетной записи для анонимного доступа к ресурсу; его можно изменить или, щелкнув Browse (Обзор), выбрать учетную запись в диалоговом окне Find User (Выбор: Пользователь);
  - флажок Allow Only Anonymous Connections (Разрешить только анонимные подключения) запрещает пользователям подключаться к узлу с указанием имени и

пароля; пометьте его, если нужен только анонимный доступ к узлу, если нет — снимите;

- флажок Allow IIS To Control Password (Разрешить управление паролем из IIS) определяет, разрешено ли управление паролем учетной записи анонимного доступа из IIS; обычно это то, что нужно, — пометьте флажок; или снимите его и введите пароль учетной записи для анонимного доступа.

5. Дважды щелкните ОК. Изменения будут автоматически унаследованы всеми FTP-узлами сервера.

### Использование разрешений Windows на FTP-серверах

Все папки и файлы IIS могут иметь разные разрешения на доступ, назначенные на уровне безопасности Windows. Помните, что полным доступом к файлам и папкам (т. е. правом создавать, переименовывать и удалять ресурсы) обладают только администраторы.

Пользователям, прошедшим проверку на подлинность, следует назначать специфические разрешения в зависимости от выполняемых ими задач. Предоставьте пользователям, загружающим файлы, разрешение Read (чтение), а пользователям, закачивающим файлы, — Write (запись) для соответствующих ресурсов. Если пользователям второго типа нужно просматривать содержимое каталогов, назначьте им и разрешение Read.

Специальная группа Everyone (Все) и гостевая учетная запись Интернета должны обладать неявными разрешениями. FTP-узел по умолчанию наследует разрешения папки Inetpub, к которой группа Everyone обладает полным доступом. Это создает угрозу безопасности, которую нужно предотвратить: задайте папкам и файлам для загрузки разрешение Read, а папкам для закладки — Write и Read (если хотите, чтобы пользователь просматривал их содержимое).



**Совет** Чтобы сконфигурировать разрешения на доступ к отдельной папке после изменения свойств базового каталога FTP-узла по умолчанию, снимите в окне свойств последнего флажок Allow Inheritable Permissions (Переносить наследуемые от родительского объекта разрешения на этот объект).

### Конфигурирование разрешений FTP-сервера

Помимо разрешений безопасности Windows, FTP-узлы и папки обладают разрешениями IIS, одинаковыми для всех пользователей. Это означает, что задать разные права на доступ разным пользователям на уровне IIS нельзя. И все же вы можете создать специфические папки, допускающие только загрузку или только закачку файлов, или и то, и другое.

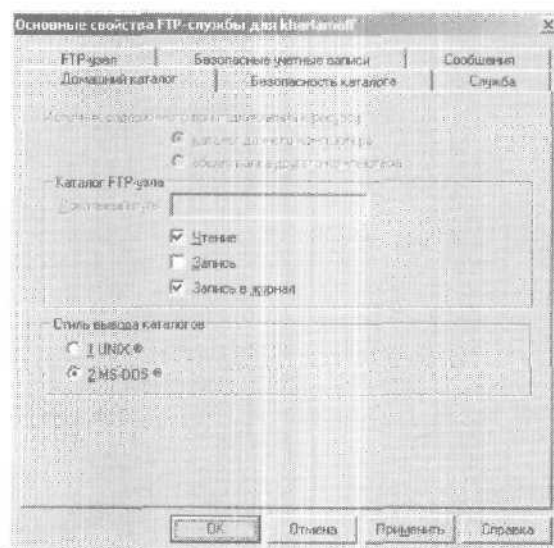
Разрешения FTP можно задавать глобально или локально, на уровне узлов и папок. Глобальные разрешения задают в диалоговом окне FTP Service Master Properties (Основные свойства FTP-службы). При настройке разрешений FTP нужно также указать, как они наследуются. Если вы изменили разрешения и возник конфликт с существующими параметрами узла или папки, IIS предложит заменить разрешения узла (папки) глобальными разрешениями. Точно так же в случае конфликтов при изменении разрешений узла (папки) вам предложат заменить их локальными разрешениями.

#### Конфигурирование глобальных разрешений FTP

Для управления глобальными разрешениями FTP сделайте так.

1. В оснастке Internet Information Services щелкните правой кнопкой значок компьютера и выберите в контекстном меню команду Properties (Свойства). Откроется диалоговое окно свойств.
2. Из списка Master Properties (Основные свойства) выберите FTP Service (FTP-служба) и щелкните Edit (Изменить). Откроется диалоговое окно FTP Service Master Properties (Основные свойства FTP-службы) для данного компьютера.
3. Перейдите на вкладку Home Directory (Домашний каталог) и с помощью следующих флажков задайте разрешения Web-сервера, которые будут наследоваться узлами и папками (рис. 7-7):
  - Read (Чтение) — позволяет пользователю считывать и загружать файлы из каталога;
  - Write (Запись) — позволяет пользователю закачивать файлы в каталог;

- Log Visits (Запись в журнал) — используется совместно с системой аудита сервера для регистрации обращений к ресурсу.



**Рис. 7-7.** Настройка глобальных разрешений FTP

4. Щелкните **Apply** (Применить). Прежде чем применить изменения, IIS проверит текущие настройки всех FTP-узлов и их панок. Если на FTP-узле используются другие разрешения, откроется диалоговое окно **Inheritance Overrides** (Изменение наследования). Отметьте в нем узлы, к которым нужно применить новые разрешения, и щелкните **OK**.

#### Конфигурирование локальных разрешений FTP

Разрешения FTP для отдельного узла или папки конфигурируются так.

1. В оснастке **Internet Information Services** щелкните правой кнопкой значок узла или папки и выберите в контекстном меню команду **Properties** (Свойства).
2. Перейдите соответственно на вкладку **Home Directory** (Домашний каталог), **Directory** (Каталог) или **Virtual Di-**

rectory (Виртуальный каталог) (рис. 7-8) и с помощью следующих флажков задайте разрешения Web-сервера, которые будут наследоваться узлами и папками:

- Read (Чтение) — позволяет пользователю считывать и загружать файлы из каталога;
- Write (Запись) — позволяет пользователю закачивать файлы в каталог;
- Log Visits (Запись в журнал) — используется совместно с системой аудита сервера для регистрации обращений к ресурсу.

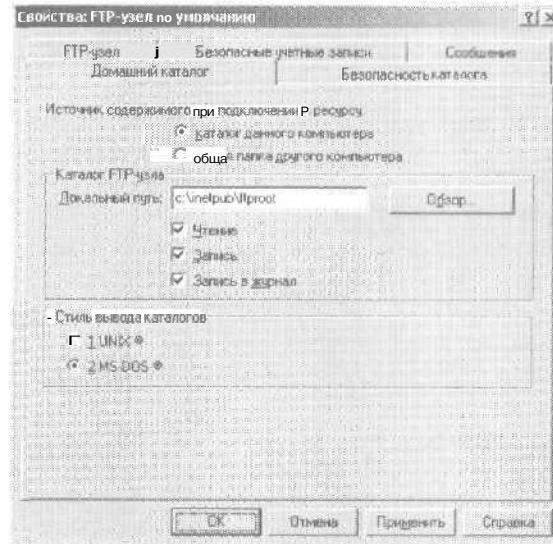


Рис. 7-8. Настройка локальных разрешений FTP

3. Щелкните Apply (Применить). Прежде чем применить изменения, IIS проверит текущие настройки всех FTP-узлов и их папок. Если на FTP-узле используются другие разрешения, откроется диалоговое окно Inheritance Overrides (Изменение наследования). Отметьте в нем узлы, к которым следует применить новые разрешения, и щелкните OK.

### Настройка ограничений на доступ по IP-адресам и доменным именам

По умолчанию FTP-ресурсы доступны всем компьютерам и доменам, а также с любого IP-адреса, что создает опасность некорректного использования сервера. Для управления ресурсами можно предоставлять или блокировать доступ по IP-адресам, сетевым идентификаторам и доменам. Как и любые другие параметры FTP-сервера, ограничения на доступ можно задать на уровне сервера или отдельных узлов, папок и файлов.

Предоставление доступа позволяет компьютеру запрашивать ресурсы, но не дает пользователям гарантии на работу с ними. Если включена проверка на подлинность, пользователи должны ее пройти,

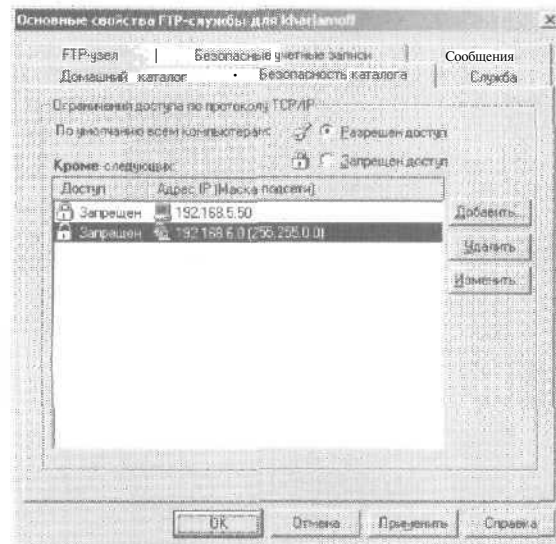
Отказ в доступе запрещает компьютеру обращаться к ресурсам. Следовательно, пользователи данного компьютера не смогут работать с ресурсами, даже если бы у них была возможность успешно пройти проверку на подлинность.

Ограничения на доступ на уровне сервера включаются/отключаются так.

1. В оснастке Internet Information Services щелкните правой кнопкой значок компьютера и выберите в контекстном меню команду **Properties** (Свойства). Откроется одноименное диалоговое окно.
2. Из раскрывающегося списка **Master Properties** (Основные свойства) выберите **FTP Service** (FTP-служба) и щелкните **Edit**. Откроется диалоговое окно **FTP Service Master Properties** (Основные свойства FTP-службы) для данного компьютера.
3. Перейдите на вкладку **Directory Security** (Безопасность каталога) (рис. 7-9). Поставьте переключатель в положение **Granted Access** (Разрешен доступ), чтобы предоставить доступ определенным и запретить доступ остальным компьютерам, или в положение **Denied Access** (Запрещен доступ), чтобы запретить доступ определенным и предоставить доступ остальным компьютерам.
4. Создайте список доступа. Для этого щелкните **Add** (Добавить) и затем в диалоговом окне **Computer** (Запрещение доступа к узлу) — **Single Computer** (Один компью-



тер) или Group Of Computers (Группа компьютеров). Для отдельного компьютера введите его IP-адрес, например 192.168.5.50, для группы компьютеров — адрес их подсети, например 192.168.0.0, или маску подсети, например 255.255.0.0.



**Рис. 7-9.** Вкладка Directory Security (Безопасность каталога) диалогового окна FTP Service Master Properties (Основные свойства FTP-службы)

5. Чтобы удалить запись из списка доступа, выделите ее в списке Computers (Кроме следующих) и щелкните Remove (Удалить).
6. Щелкните Apply (Применить). Прежде чем применить изменения, IIS проверяет текущие параметры всех FTP-узлов и их папок. Если на FTP-узле используются другие параметры, откроется диалоговое окно Inheritance Overrides (Изменение наследования). Отметьте в нем узлы, к которым следует применить новые значения, и щелкните OK.

Ограничения доступа на уровне узла, папки или файла включаются/отключаются так.

1. В оснастке Internet Information Services щелкните правой кнопкой значок узла или папки и выберите в контекстном меню команду Properties (Свойства). Откроется одноименное диалоговое окно.
2. Перейдите на вкладку Directory Security (Безопасность каталога). Поставьте переключатель в положение Granted Access (Разрешен доступ), чтобы предоставить доступ определенным и запретить доступ остальным компьютерам, или в Denied Access (Запрещен доступ), чтобы запретить доступ определенным и предоставить доступ остальным компьютерам.
3. Создайте список доступа. Для этого щелкните Add (Добавить) и затем в диалоговом окне Computer (Запрещение доступа к узлу) — Single Computer (Один компьютер) или Group Of Computers (Группа компьютеров). Для отдельного компьютера введите его IP-адрес, например 192.168.5.50, для группы компьютеров — адрес их подсети, например 192.168.0.0, или маску подсети, например 255.255.0.0.
4. Чтобы удалить запись из списка доступа, выделите ее в списке Computers (Кроме следующих) и щелкните Remove (Удалить).
5. Щелкните Apply (Применить). Прежде чем применить изменения, IIS проверит текущие параметры всех FTP-узлов и их папок. Если на FTP-узле используются другие значения, откроется диалоговое окно Inheritance Overrides (Изменение наследования). Отметьте в нем узлы, к которым следует применить новые параметры, и щелкните ОК.

### Назначение операторов Web-узла

Всем FTP-узлам сервера можно назначить операторов, которые будут управлять ими удаленно. Операторы FTP-узла — это специальная группа пользователей, обладающих ограниченными административными привилегиями.

Всем FTP-узлам сервера операторы назначаются так.

1. В оснастке Internet Information Services щелкните правой кнопкой значок компьютера и выберите в контекстном

меню команду Properties (Свойства). Откроется одноименное диалоговое окно.

2. Из раскрывающегося списка Master Properties (Основные свойства) выберите FTP Service (FTP-служба) и щелкните Edit (Изменить). Откроется диалоговое окно FTP Service Master Properties (Основные свойства FTP-службы) для данного компьютера.
3. Перейдите на вкладку Security Accounts (Безопасные учетные записи). В списке Operators (Операторы) отображаются назначенные операторы. По умолчанию оператором является только глобальная группа Administrators (Администраторы).
4. Чтобы добавить оператора, щелкните Add (Добавить). Откроется диалоговое окно Select Users Or Groups (Выбор: Пользователи или Группы), где можно выбрать пользователей и группы.
5. Чтобы удалить оператора, выберите его в списке Operators (Операторы) и щелкните Remove (Удалить).
6. Трижды щелкните ОК, чтобы завершить назначение операторов.

Отдельному FTP-узлу операторы назначаются так.

1. В оснастке Internet Information Services щелкните правой кнопкой значок узла и выберите в контекстном меню команду Properties (Свойства). Откроется одноименное диалоговое окно.
2. Перейдите на вкладку Operators (Операторы). В списке Operators отображаются назначенные FTP-узлу операторы. По умолчанию оператором является только глобальная группа Administrators (Администраторы).
3. Чтобы добавить оператора, щелкните Add (Добавить). Откроется диалоговое окно Select Users Or Groups (Выбор: Пользователи или Группы), где можно выбрать пользователей и группы.
4. Чтобы удалить оператора, выберите его в списке Operators (Операторы) и щелкните Remove (Удалить).
5. Щелкните ОК или Apply (Применить), чтобы завершить назначение операторов.

## Глава 8

# Настройка и поддержка службы SMTP

Протокол SMTP позволяет обмениваться сообщениями по Интернету. Он и разрабатывался для того, чтобы дать WWW-серверам возможность получать такие сообщения. Однако большинство организаций используют службу SMTP, входящую в состав IIS, в основном для отправки сообщений электронной почты. Создавать почтовый Интернет-сервер общего назначения для корпоративной сети или поставщика услуг Интернета на основе службы SMTP из состава IIS нецелесообразно. Для этого лучше задействовать полнофункциональный сервер сообщений, например Microsoft Exchange 2000 Server.

При установке службы SMTP в процессе установки IIS создается виртуальный SMTP-сервер по умолчанию. Он настроен так, что обрабатывает и доставляет лишь локально созданные сообщения. Отправка сообщений, созданных удаленными пользователями, включая гостевую учетную запись Интернета и других именованных пользователей Web-сервера, запрещена. Кроме того, не разрешается ретрансляция электронной почты через виртуальный SMTP-сервер. Такая конфигурация позволяет использовать виртуальный сервер по умолчанию в большинстве сред без изменения каких-либо параметров. Но иногда вам все же потребуется модифицировать конфигурационные параметры, чтобы привести их в соответствие требованиям конкретной рабочей среды.

Управление службой SMTP довольно сильно отличается от других задач Web-администратора. Вы будете управлять не содержимым или передачей файлов, а тем, как обрабатываются и доставляются сообщения электронной почты.

Прежде чем перейти к основным задачам администрирования, рассмотрим основы SMTP.

## Использование SMTP

Служба SMTP предоставляет одному или нескольким доменам простые службы обмена сообщениями и имеет множество конфигурационных параметров. Управление конфигурацией SMTP осуществляется с помощью виртуальных серверов. При этом надо четко понимать, как используются домены электронной почты и папка Mailroot, а также как обрабатываются SMTP-сообщения.

### Домены электронной почты

Служба SMTP обрабатывает сообщения электронной почты, основываясь на адресах, указанных в полях To (Кому), Cc (Копия), Bcc (Скрытая копия) и From (От) письма. Первые три определяют адресатов, последнее — отправителя сообщения.

Электронные адреса, например `williams@tech.microsoft.com`, состоят из трех частей:

- имени учетной записи электронной почты (здесь — `williams`);
- символа `@`, отделяющего имя учетной записи от имени домена;
- имени домена электронной почты (здесь — `tech.microsoft.com`).

Порядок обработки сообщений SMTP-сервером определяется доменом электронной почты или служебным доменом. Последний может быть как локальным, так и удаленным. Локальный служебный домен — это DNS-домен (Domain Name System, система доменных имен), обслуживаемый SMTP-сервером локально. Удаленный — это DNS-домен, обслуживаемый другим SMTP-сервером или почтовым шлюзом.

Любое сообщение с именем локального домена в полях To (Кому), Cc (Копия) или Bcc (Скрытая копия) доставляется локально. Локальный домен можно назначить доменом по умолчанию или доменом-псевдонимом. Домен по умолчанию служит для всех сообщений, пересылаемых в домен или из него. Сообщения, отправляемые в домен по умолчанию, по-

мещаются в папку Dгор виртуального сервера. Для исходящих сообщений, в которых не задан домен в поле From (От), в качестве домена происхождения используется домен по умолчанию. У виртуального SMTP-сервера может быть только один домен по умолчанию.

Любые другие создаваемые на сервере локальные домены будут назначены доменами-псевдонимами. Домены-псевдонимы позволяют создавать вторичные домены, указывающие на домен по умолчанию и использующие его параметры. Помните, что любые передаваемые домену-псевдониму сообщения помечаются именем домена по умолчанию. Это значит, что домен-псевдоним использует те же конфигурационные параметры и ту же папку Dгор, что и домен по умолчанию. Так, доменом по умолчанию виртуального SMTP-сервера может быть `tech.microsoft.com`, а доменом-псевдонимом — `dev.microsoft.com`. Все сообщения, в которых указан любой из этих доменов, локально обрабатываются виртуальным SMTP-сервером, помечаящим их именем домена по умолчанию и заполняющим служебные поля.

Все сообщения, в полях To, Cc или Bcc которых указан домен, не являющийся локальным, помещаются в очередь для отправки на удаленный сервер. Если для конкретного удаленного домена предусмотрены особые требования доставки, можно добавить этот домен к SMTP-серверу и настроить его параметры для соответствующей обработки сообщений. Скажем, задать для удаленного домена индивидуальные параметры безопасности, требующие шифрования сообщений. Кроме того, вы вправе переслать сообщения для удаленного домена через конкретный почтовый сервер, являющийся направляющим узлом.

#### Папка Mailroot

При установке SMTP со стандартными параметрами автоматически создается виртуальный сервер по умолчанию, управляющий отправкой и доставкой сообщений через папку `Inetpub\Mailroot`. Можно создать и дополнительные виртуальные SMTP-серверы, у каждого из которых будет отдельная папка Mailroot, расположенная в указанной вами папке файловой системы.

В каждой папке Mailroot семь вложенных папок.

- **Badmail** хранит сообщения, которые невозможно и доставить, и вернуть отправителю. Каждому из таких сообщений сопоставлено сообщение об ошибке, позволяющее выявить источник проблемы. Чтобы гарантировать корректную обработку сообщений системой, периодически просматривайте содержимое папки.
- **Drop** хранит все входящие сообщения, предназначенные адресатам на данном сервере, например почтмейстеру виртуального сервера. Служба SMTP перемещает сюда из папки Queue все входящие сообщения, адресованные локальным получателям.
- **Mailbox** хранит почтовые ящики.
- **Pickup** — любое помещенное в эту папку сообщение служба SMTP забирает и перемещает в папку Queue для дальнейшей обработки и доставки. SMTP постоянно проверяет наличие в этой папке новых сообщений.
- **Queue** хранит подготовленные к обработке и доставке сообщения: получаемые службой SMTP, а также из папки Pickup. Кроме того, папка содержит сообщения, доставка которых временно невозможна из-за отказов соединений или большой загруженности конечных серверов. Если же SMTP сочтет, что эти сообщения не смогут быть доставлены, они будут перемещены в папку Badmail.
- **Route** хранит временные данные, нужные для пересылки сообщений по конкретному маршруту. Обычно папка используется при настройке маршрутного домена для виртуального SMTP-сервера.
- **SortTemp** используется в качестве временной папки для сортировки сообщений. Здесь создаются временные файлы, удаляемые после сортировки и постановки сообщений в очередь на отправку.

После установки службы SMTP на сервере периодически просматривайте содержимое папок Badmail и Queue — эти папки лучший индикатор сбоев SMTP.

#### Принципы обработки сообщений

Служба SMTP обрабатывает сообщения по четкой схеме. Источником сообщения может быть папка Pickup. Файлы сообщений помещаются в эту папку приложениями (напри-

мер, ASP-страницей) или пользователем (например, администратором). Другой источник — служба SMTP, при этом файлы сообщений принимаются по протоколу SMTP.

Сообщение, скопированное в папку Pickup или поступившее по протоколу SMTP, помещается для обработки и доставки в папку Queue. Дальнейшая судьба сообщения зависит от типа адресата. Адресаты могут быть локальными, т. е. их домен электронной почты обслуживается SMTP-сервером локально. К ним относятся домен по умолчанию и все установленные на сервере домены-псевдонимы. Почтовые сообщения для локальных адресатов обрабатываются локально.

Адресаты также могут быть удаленными, их домен электронной почты обслуживается SMTP-сервером удаленно. Почтовые сообщения для удаленных адресатов пересылаются напрямую, маршрутизируются с использованием DNS или отсылаются на указанный почтовый шлюз.



**Примечание** Имя домена в адресе электронной почты расположено справа от знака @. Например, имя домена в адресе `williams@tech.microsoft.com` — `tech.microsoft.com`.

Сообщения для локальных адресатов перемещаются из папки Queue в папку Drop, заданную для домена по умолчанию. После этого обработка сообщения службой SMTP считается завершенной. Расположение папки Drop по умолчанию — `Inetpub\Mailroot\Drop`. Этот путь можно изменить в диалоговом окне свойств домена по умолчанию.

Если сообщение предназначено удаленным адресатам, те сортируются по именам доменов. Это позволяет службе SMTP доставлять сообщения удаленным адресатам как группе и передавать за один сеанс связи несколько сообщений. После сортировки сообщения обрабатываются в порядке очередности поступления. Чтобы отправить сообщение, SMTP пытается подключиться к конечному почтовому серверу. После установки связи проверяются адресаты, отсылается сообщение, и конечный почтовый сервер при необходимости подтверждает его получение. Если конечный сервер не отвечает или не может принять сообщение, оно остается в очереди, и SMTP повторно пытается доставить его через заданные интервалы времени, в течение которых обрабатываются сообщения с более низким приоритетом.



Если по истечении **определенного срока** сообщение так и не удалось доставить, SMTP помечает его и генерирует соответствующий отчет. В нем говорится, почему доставка сообщения не представляется возможной, и приводится его текст. Затем служба пытается доставить отчет отправителю исходного сообщения.

Процесс доставки отчета аналогичен процессу доставки любого другого сообщения — служба SMTP помещает его в папку Queue. Дальнейшая обработка зависит от того, является ли отправитель исходного сообщения локальным или удаленным адресатом. Если же отчет доставить невозможно, он помещается в папку Badmail, и на этом обработка данного сообщения заканчивается.

## Основы управления службой SMTP

Управление SMTP-сервером включает создание виртуальных SMTP-серверов, **конфигурирование** порта и IP-адреса сервера, а также мониторинг пользовательских сеансов и состояния сервера.

### Создание виртуальных SMTP-серверов

При установке SMTP-сервера автоматически создается виртуальный SMTP-сервер по умолчанию, осуществляющий доставку сообщений для домена по **умолчанию** и прочих сконфигурированных вами доменов. Если на вашем компьютере несколько доменов или вам нужны два и более доменов по умолчанию, создайте для их обслуживания дополнительные виртуальные SMTP-серверы. Сделайте это также, если для всех размещаемых доменов нужно настроить отдельные ограничения на обмен сообщениями.

Дополнительный виртуальный SMTP-сервер создается так.

1. При установке виртуального SMTP-сервера на новый сервер убедитесь, что на нем уже установлена служба SMTP.
2. Если виртуальный сервер будет использовать **новый IP-адрес**, его необходимо предварительно сконфигурировать. Подробнее об этом см. главу 15 книги «Microsoft Windows 2000. Справочник Администратора».
3. В оснастке Internet Information Services щелкните правой кнопкой значок нужного компьютера и выберите в контекстном меню команду New\SMTP Virtual Server (Co-

здать\Виртуальный SMTP-сервер). Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2 этой книги.

4. Запустится мастер SMTP Virtual Server Wizard (Мастер создания виртуального SMTP-сервера) (рис. 8-1). В поле Description (Описание виртуального SMTP-сервера) введите описательное имя Web-узла, например TechNet SMTP Server, и щелкните Next (Далее).

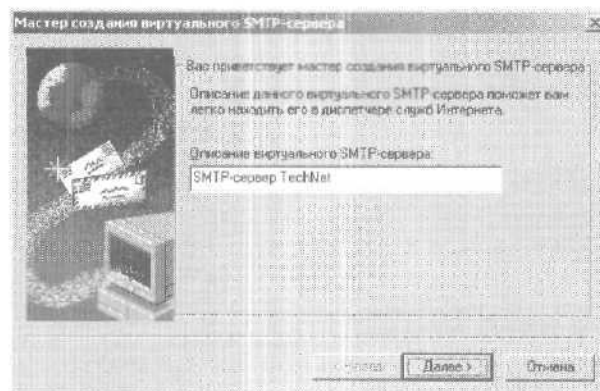


Рис. 8-1. Мастер SMTP Virtual Server Wizard (Мастер создания виртуального SMTP-сервера)

5. В списке IP Address selection (Выбор IP-адреса) выберите доступный IP-адрес. Щелкните (All Unassigned (все не назначенные)), чтобы виртуальный SMTP-сервер использовал все неназначенные IP-адреса сервера. Номер порта протокола TCP автоматически задается как 25. Щелкните Next (Далее).



**Примечание** Каждый виртуальный сервер должен использовать уникальную комбинацию «TCP-порт + IP-адрес». Несколько виртуальных SMTP-серверов могут работать с одним и тем же портом, при условии, что используют разные IP-адреса.

6. В следующем диалоговом окне задайте домашнюю папку виртуального сервера. Для поиска уже созданной папки щелкните Browse (Обзор). При необходимости папку

можно создать с помощью Windows Explorer (Проводник). Щелкните Next.



**Совет** Для корректной работы службы SMTP предоставьте группе Everyone (Все) полный доступ к домашней папке и всем ее файлам и вложенным папкам.

7. Укажите домен по умолчанию для виртуального сервера — это DNS-домен, обслуживаемый SMTP-сервером локально. Обычно доменом по умолчанию является домен, указанный на вкладке DNS диалогового окна TCP/IP Properties [Свойства: Протокол Интернета (TCP/IP)] сервера.
8. Щелкните Finish (Готово), чтобы создать виртуальный сервер. Если служба SMTP по умолчанию настроена для автоматического запуска, новый виртуальный SMTP-сервер также будет запускаться автоматически. Если же при создании сервера вы указали уже занятую комбинацию «TCP-порт + IP-адрес», новый сервер не запустится, и вам потребуется изменить его IP-адрес или TCP-порт.
9. Настройте виртуальный сервер в соответствии с инструкциями разделов «Управление входящими соединениями», «Управление исходящими соединениями» и «Управление доставкой сообщений» данной главы.

### Настройка портов и IP-адресов SMTP-серверов

Каждый виртуальный SMTP-сервер обладает уникальным идентификатором, включающим его IP-адрес (по умолчанию — все неназначенные адреса) и номер TCP-порта (по умолчанию — 25). Идентификатор виртуального SMTP-сервера можно изменить.

1. Если виртуальный сервер будет использовать новый IP-адрес, его необходимо предварительно сконфигурировать. Подробнее об этом см. главу 15 книги «Microsoft Windows 2000. Справочник Администратора».
2. Запустите оснастку Internet Information Services и затем в левой части ее окна (Console Root) (корень консоли) раскройте узел нужного компьютера. Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2 этой книги.

- Щелкните виртуальный SMTP-сервер правой кнопкой и выберите в контекстном меню команду Properties (Свойства). Откроется одноименное диалоговое окно (рис. 8-2).

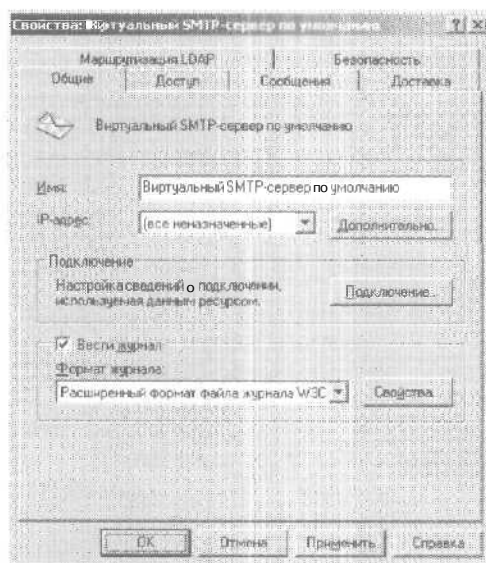


Рис. 8-2. Окно свойств виртуального SMTP-сервера

- В поле Name (Имя) содержится описательное имя виртуального SMTP-сервера, отображаемое в оснастке Internet Information Services. Для других целей оно не используется, и его можно редактировать.
- В разделе IP Address selection (IP-адрес) отображается текущий IP-адрес виртуального SMTP-сервера. Чтобы изменить его, выберите любой другой доступный IP-адрес или щелкните (All Unassigned) (все неназначенные), чтобы SMTP-сервер использовал все неназначенные IP-адреса. Несколько виртуальных SMTP-серверов могут работать с одним и тем же IP-адресом, при условии, что они используют разные порты.
- Номер TCP-порта виртуального SMTP-сервера автоматически задается как 25. Чтобы изменить это, щелкните Advanced (Дополнительно). В открывшемся диалоговом окне выберите IP-адрес, порт для которого нужно изме-

нить, и щелкните Edit (Изменить). Введите в поле TCP Port (Порт TCP) новый номер порта и щелкните OK. Еще раз щелкните OK, чтобы сохранить изменения. Несколько FTP-серверов могут работать с одним и тем же портом, при условии, что у них разные IP-адреса.

7. Щелкните OK, чтобы закрыть диалоговое окно Properties (Свойства).

### Создание нескольких идентификаторов для виртуального SMTP-сервера

Виртуальный SMTP-сервер может обрабатывать входящие сообщения по нескольким IP-адресам и портам, и поэтому иногда ему нужно несколько идентификаторов. Например, можно сконфигурировать сервер для получения почты по нескольким TCP-портам.

Несколько идентификаторов виртуальному SMTP-серверу можно назначить так.

1. В оснастке Internet Information Services щелкните правой кнопкой виртуальный SMTP-сервер и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке General (**Общие**) щелкните Advanced (Дополнительно) и в открывшемся диалоговом окне (рис. 8-3) задайте новый IP-адрес и TCP-порт сервера. Следующие кнопки позволяют:

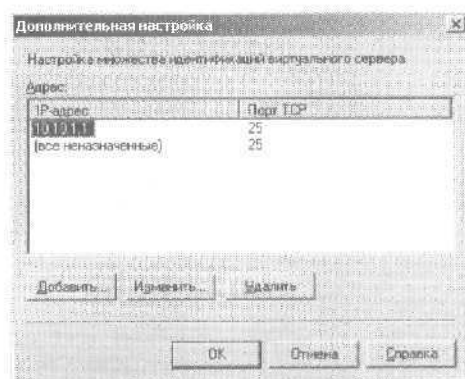


Рис. 8-3. Диалоговое окно Advanced (Дополнительная настройка)

- **Add** (Добавить) — добавить новый идентификатор (щелкните эту кнопку, укажите нужный IP-адрес и введите номер TCP-порта, затем щелкните ОК);
- **Edit** (Изменить) — редактировать запись, выбранную в списке **Address** (Адрес);
- **Remove** (Удалить) — удалить запись, выбранную в списке **Address** (Адрес).

3. Дважды щелкните ОК, чтобы сохранить изменения.

### Мониторинг состояния виртуального SMTP-сервера

Как уже говорилось, после установки службы SMTP на сервере следует периодически просматривать содержимое вложенных папок папки **Mailroot** (подробнее — в разделе «Папка **Mailroot**» этой главы). Рекомендую вам наблюдать за папками и в случае проблем предпринять следующие действия.

- **Badmail** — если число сообщений в этой папке увеличивается, возможны проблемы с доступом почтового сервера к сети или с доставкой почты. Попробуйте опросить узлы внешней сети или проблемные серверы с помощью команды **ping**.
- **Drop** — прочитайте входящие сообщения, предназначенные адресатам на данном сервере, и при необходимости перешлите их другим сотрудникам.
- **Queue** — если число сообщений в этой папке увеличивается, возможны проблемы с доступом почтового сервера к сети или с доставкой почты. Опросите узлы внешней сети или проблемные серверы с помощью команды **ping**.
- **Pickup** — сообщения не должны задерживаться в этой папке. Если это не так, то, возможно, что они нечитаемы или возникли проблемы в работе SMTP. Например, вы могли задать папке **Pickup** разрешения, не позволяющие службе SMTP считывать ее содержимое. Проверьте разрешения и состояние службы SMTP.



**Внимание!** У каждого виртуального SMTP-сервера — отдельная папка **Mailroot**, расположение которой было указано при его установке. Заметьте, что на вкладке **Messages** диалогового окна свойств виртуального SMTP-сервера можно также настроить дополнительные папки **Badmail**.

### Управление пользовательскими сеансами

После подключения пользователя к виртуальному серверу создается пользовательский сеанс, длительность которого равна продолжительности подключения. Все виртуальные серверы отслеживают пользовательские сеансы независимо. Просматривая текущие сеансы, вы можете определить текущую загрузку сервера, подключенных к серверу пользователей и длительность их подключения. Если к серверу подключен неавторизованный пользователь, завершите соответствующий сеанс, тем самым немедленно отключив его. Вы можете отключить от сервера и всех пользователей.

Просмотреть/завершить пользовательские сеансы можно так.

1. Запустите оснастку Internet Information Services и дважды щелкните значок виртуального сервера.
2. В левой части окна появится узел Current Sessions (Текущие сеансы). Щелкнув его, вы увидите в правой части список текущих сеансов.
3. Чтобы отключить отдельного пользователя, щелкните в правой части окна его запись правой кнопкой и выберите в контекстном меню команду Terminate (Прервать).
4. Чтобы отключить всех пользователей, щелкните в правой части окна запись любого пользователя правой кнопкой и выберите в контекстном меню команду Terminate All (Прервать все).

### Настройка служебных доменов

Виртуальные SMTP-серверы сконфигурированы для поддержки определенных служебных доменов. Вы можете создать только два типа служебных доменов: домены-псевдонимы и удаленные домены. При установке виртуального сервера автоматически создается домен по умолчанию. Вы вправе сделать доменом по умолчанию и домен-псевдоним.

#### Просмотр служебных доменов

Перед созданием дополнительных служебных доменов надо проверить домены, уже обслуживаемые установленными на Web-сервере виртуальными SMTP-серверами. У каждого виртуального сервера есть собственные служебные домены. Чтобы просмотреть служебные домены, сделайте так.

1. Запустите оснастку Internet Information Services и дважды щелкните значок виртуального сервера.
2. В левой части окна появится узел Domains (Домены). Щелкнув его, в правой части вы увидите список имеющихся служебных доменов (рис. 8-4). Запись домена включает два поля:
  - **Domain Name** (Имя домена) — DNS-имя служебного домена: например `microsoft.com`;
  - **Type** (Тип) — тип служебного домена: например `Local (Default)` [Локальный (по умолчанию)], `Local (Alias)` [Локальный (псевдоним)] или `Remote` (Удаленный).

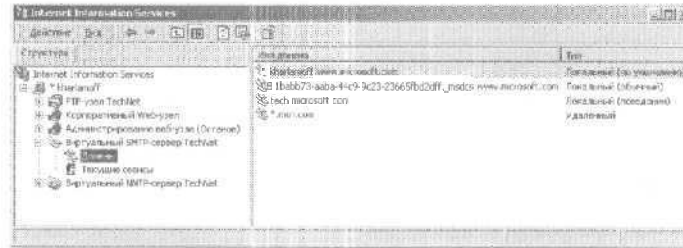


Рис. 8-4. Просмотр служебных доменов в оснастке Internet Information Services

3. Чтобы просмотреть свойства служебного домена, щелкните правой кнопкой его значок и выберите в контекстном меню команду **Properties** (Свойства).

#### Работа с локальными доменами

Локальные служебные домены — это домены, обслуживаемые SMTP-сервером локально. Они могут быть двух типов: домен по умолчанию и домен-псевдоним. Первый по умолчанию используется для обработки входящих и исходящих сообщений, второй позволяет создавать дополнительные домены, указывающие на домен по умолчанию и использующие его параметры. Сообщения, адресованные домену по умолчанию и всем связанным с ним доменам-псевдонимам, хранятся в папке `Dtop` виртуального сервера. Исходящие сообщения используют в качестве домена происхождения домен по умолчанию.



При работе с локальными доменами администратор может создавать домены-псевдонимы, делать существующий домен-псевдоним доменом по умолчанию, изменять расположение папки Drop и параметры квот.

#### Создание доменов-псевдонимов

Домены-псевдонимы позволяют создавать вторичные домены, которые указывают на домен по умолчанию, и используют его параметры и папку Drop. Домен-псевдоним создается так.

1. Запустите оснастку Internet Information Services и дважды щелкните значок виртуального сервера.
2. Щелкните узел Domains (Домены) правой кнопкой и выберите в контекстном меню команду New\Domain (Создать\Домен). Запустится мастер New SMTP Domain Wizard (Мастер создания домена SMTP).
3. Задайте тип домена как Alias (Псевдоним) и щелкните Next (Далее).
4. Введите в поле Name (Имя) DNS-имя домена. Использовать символы подстановки в имени домена нельзя. Так, имя tech.microsoft.com допустимо, а \*.microsoft.com — нет.
5. Щелкните Finish (Готово).

#### Назначение домена по умолчанию

Домен по умолчанию служит для обработки всех сообщений, пересылаемых в домен или из него. Адресованные ему сообщения хранятся в папке Drop виртуального сервера. Для исходящих сообщений, в поле From (От) которых не задан домен, в качестве домена происхождения используется домен по умолчанию. У виртуального SMTP-сервера может быть только один домен по умолчанию.

Имя домена по умолчанию задается автоматически при установке виртуального SMTP-сервера. Чтобы задать новый служебный домен по умолчанию, создайте домен-псевдоним и назначьте его служебным доменом по умолчанию.

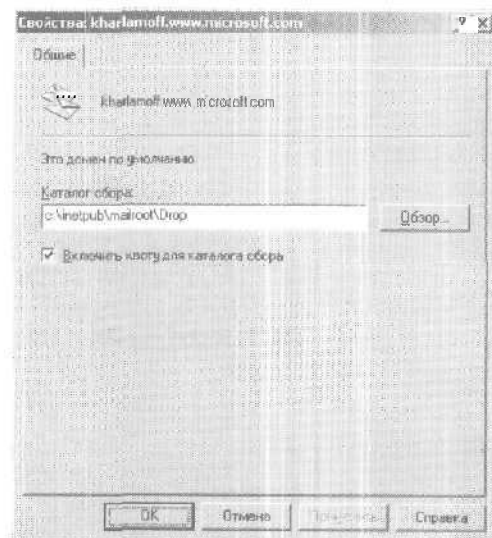
1. Запустите оснастку Internet Information Services и дважды щелкните значок требуемого сервера.
2. В левой части окна щелкните узел Domains (Домены). Отобразится список сконфигурированных на сервере служебных доменов.

3. Щелкните правой кнопкой домен-псевдоним и выберите в контекстном меню команду **Set As Default** (Использовать по умолчанию).

**Изменение** конфигурационных параметров **папки Drop домена** по умолчанию

Все входящие сообщения, адресованные локальному домену и доменам-псевдонимам, перемещаются из папки Queue в папку Drop. Расположение папки Drop по умолчанию – `Inetpub\Mailroot\Drop`. Чтобы изменить его, сделайте так.

1. Запустите оснастку **Internet Information Services** и дважды щелкните значок виртуального сервера.
2. Укажите узел **Domains (Домены)** в левой части окна. Появится список служебных доменов, установленных на сервере.
3. Щелкните правой кнопкой домен по умолчанию и выберите в контекстном меню команду **Properties (Свойства)**. Откроется одноименное диалоговое окно (рис. 8-5).



**Рис. 8-5.** Изменение параметров папки Drop в окне свойств домена

4. Введите новый путь к папке Drop. Для поиска уже созданной папки щелкните Browse (Обзор). Вы также можете создать папку с помощью Windows Explorer (Проводник).
5. Пометив флажок Enable Drop Directory Quota (Включить квоту для каталога сбора), включите для папки Drop политику квот. Если этого не надо, сбросьте флажок,



**Совет** Квоты позволяют ограничить общий размер сообщений в папке Drop и реализуются в соответствии с политикой квот, заданной владельцем папки. Подробнее об этом см. книгу «Microsoft Windows 2000. Справочник Администратора».

6. Щелкните ОК.

### Работа с удаленными доменами

Все сообщения, в полях To (Кому), Cc (Копия) или Bcc (Скрытая копия) которых указан домен, не являющийся локальным, помещаются в очередь для отправки на удаленный сервер. По умолчанию служба SMTP пересылает сообщения напрямую конечным серверам, как указано в таблицах DNS. Если для удаленного домена имеются особые требования доставки, добавьте его к SMTP-серверу, настроив его параметры для соответствующей обработки сообщений.

При работе с удаленными доменами администратор может задать ограничения на ретрансляцию, настроить поддержку протоколов ESMTP (Extension to SMTP) или SMTP, задать параметры проверки подлинности и доступа к внешним доменам, поставить сообщения в очередь для удаленно запускаемой доставки, указать направляющие узлы для маршрутных доменов.

### Создание удаленных доменов

Удаленные домены позволяют настраивать пути доставки и маршрутизации сообщений к другим SMTP-серверам и почтовым шлюзам. Обычно их создают для доменов, с которыми часто осуществляется обмен сообщениями. Каждому удаленному домену можно задать свои параметры доставки сообщений и требовать от него прохождения проверки подлинности перед доставкой почты.

Удаленный домен создается так.

1. Запустите оснастку Internet Information Services и дважды щелкните значок виртуального сервера.
2. Щелкните правой кнопкой узел Domains (Домены) и выберите в контекстном меню команду New\Domain (Создать\Домен). Запустится мастер New SMTP Domain Wizard (Мастер создания домена SMTP).
3. Задайте тип домена как Remote (Удаленный) и щелкните Next (Далее).
4. Задайте адресное пространство домена — обычно это DNS-имя удаленного домена.



Совет Чтобы задать однотипным доменам одинаковые параметры, укажите имя домена так: *\*.остальная\_часть\_имени*. Например, \*.com — для всех доменов .com или \*.microsoft.com - - для всех доменов, оканчивающихся на microsoft.com.

5. Щелкните Finish (Готово), чтобы создать удаленный домен. В левой части окна оснастки Internet Information Services щелкните узел Domains (Домены). В правой части окна щелкните правой кнопкой запись удаленного домена и выберите в контекстном меню команду Properties (Свойства). В открывшемся диалоговом окне задайте параметры маршрутизации и безопасной доставки сообщений удаленному домену. Щелкните ОК.

#### Настройка ограничений на ретрансляцию для удаленных доменов

Ретрансляция позволяет внешним пользователям отправлять через вашу почтовую систему сообщения в другие организации. В стандартной конфигурации службы SMTP ретрансляция сообщений запрещена, чтобы предотвратить рассылку нежелательной почты через ваш сервер. Если вы все же хотите разрешить пользователям пересылку почты на определенные почтовые шлюзы, создайте удаленный домен, представляющий конечный служебный домен и позволяющий ретранслировать в него сообщения.

Ограничения на ретрансляцию задаются/удаляются так.

1. Запустите оснастку Internet Information Services и дважды щелкните значок виртуального сервера.

2. Из левой части окна щелкните узел Domains (Домены). Появится список имеющихся на сервере служебных доменов.
3. Щелкните правой кнопкой удаленный домен и выберите в контекстном меню команду Properties (Свойства). Откроется одноименное диалоговое окно (рис. 8-6).

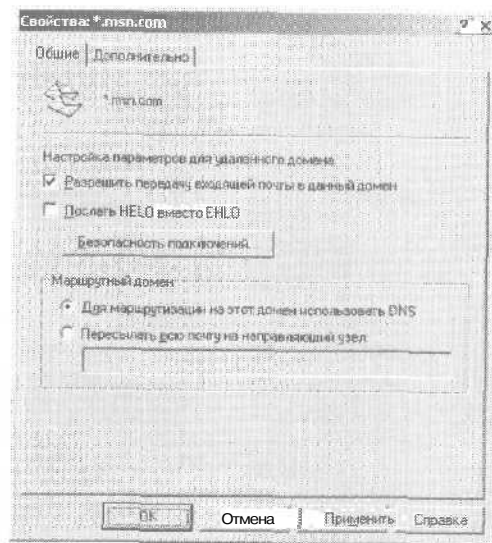


Рис. 8-6. Диалоговое окно свойств удаленного домена

4. Чтобы разрешить ретрансляцию почты на удаленный домен, пометьте флажок Allow Incoming Mail To Be Relayed To This Domain (Разрешить передачу входящей почты в данный домен).
5. Чтобы запретить ретрансляцию почты на удаленный домен, снимите флажок Allow Incoming Mail To Be Relayed To This Domain.
6. Щелкните ОК.

#### Переключение режима SMTP для удаленного домена

Служба SMTP поддерживает обычный протокол SMTP и его усовершенствованную версию — ESMTP. ESMTP эффективнее и надежнее SMTP, но иногда удаленные домены конфи-

гурируют под SMTP. Например, если система электронной почты удаленного домена не поддерживает ESMTP, при попытке установить ESMTP-сеанс связи вы получите сообщение об ошибке.

По умолчанию виртуальный SMTP-сервер пытается установить ESMTP-сеанс связи с другим почтовым сервером при помощи команды EHLO. Ее можно заменить более распространенной командой HELO.

Режим SMTP изменяется так.

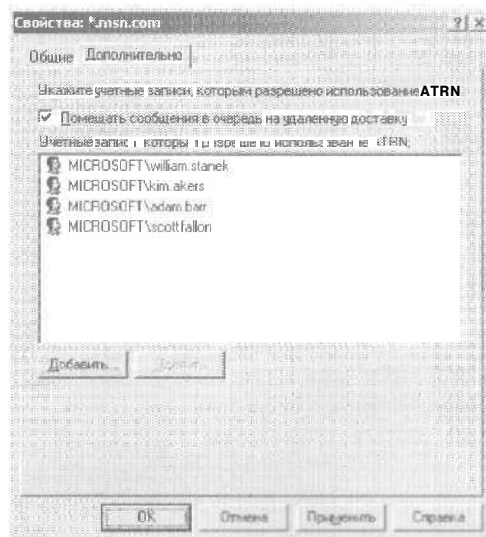
1. Запустите оснастку Internet Information Services и дважды щелкните значок виртуального сервера.
2. В левой части окна выберите узел Domains (Домены). Появится список имеющихся на сервере служебных доменов.
3. Щелкните правой кнопкой требуемый удаленный домен и выберите в контекстном меню команду Properties (Свойства). Откроется одноименное диалоговое окно (рис. 8-6).
4. Чтобы SMTP-сервер использовал протокол SMTP, пометьте флажок Send HELO Instead Of EHLO (Посылать HELO вместо EHLO). Для использования ESMTP (по умолчанию) снимите этот флажок.
5. Щелкните ОК.

#### **Постановка сообщений в очередь для удаленно запускаемой доставки**

Служба SMTP может хранить почту для клиентов и почтовых шлюзов, периодически подключающихся к виртуальному серверу и загружающих ее. При этом клиент запускает доставку посредством команды ATRN, указывая службе SMTP начать передачу сообщений в удаленный домен. Настроив удаленно запускаемую доставку, назначьте конкретные учетные записи домена, для которых она разрешена, для чего включите эти учетные записи в список авторизации.

1. Запустите оснастку Internet Information Services и дважды щелкните значок виртуального сервера.
2. В левой части окна выберите узел Domains (Домены). Появится список имеющихся на сервере служебных доменов.

3. Щелкните правой кнопкой удаленный домен и выберите в контекстном меню команду Properties (Свойства).
4. Перейдите на вкладку Advanced (Дополнительно) (рис. 8-7).



**Рис. 8-7.** Вкладка Advanced (Дополнительно) диалогового окна свойств удаленного домена

5. Чтобы включить удаленно запускаемую доставку, пометьте флажок Queue Messages For Remote Triggered Delivery (Помещать сообщения в очередь на удаленную доставку).
6. Чтобы добавить авторизованную учетную запись, щелкните Add (Добавить). В открывшемся диалоговом окне Select Users Or Groups (Выбор: Пользователи или Группы) выберите пользователей и группы из текущего дерева или леса доменов Active Directory.
7. Чтобы удалить авторизованную учетную запись, выберите ее в списке Accounts Authorized (Учетные записи, которым разрешено использование ATRN) и щелкните Remove (Удалить).
8. Щелкните OK.

**Настройка параметров проверки подлинности для удаленного домена**

Служба SMTP по умолчанию не проверяет подключения к удаленным доменам, т. е. пользователь может анонимно рассылать через них сообщения. Однако виртуальный SMTP-сервер можно настроить для передачи удаленным доменам регистрационных реквизитов. Это понадобится для отсылки сообщений в удаленный домен, требующий проверки подлинности, или если для доступа к удаленному домену нужно пройти определенный уровень проверки подлинности.

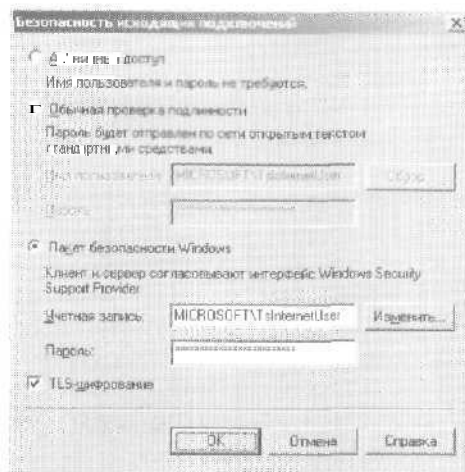
Существует несколько режимов проверки подлинности.

- Basic (Обычная проверка подлинности) — обычная проверка подлинности с широкой совместимостью. Имя пользователя и пароль передаются удаленному домену незашифрованным текстом.
- Windows Security Package (Пакет безопасности Windows) — безопасная проверка подлинности для Windows-совместимых доменов. Имя пользователя и пароль передаются удаленному домену в зашифрованном виде с применением системы безопасности Windows.
- Transport Layer Security (TLS) Encryption (TLS-шифрование) — проверка подлинности с применением шифрования. Предназначена для серверов, поддерживающих смарт-карты или сертификаты стандарта X.509. Используется совместно с обычной проверкой подлинности или проверкой подлинности Windows.

Параметры доступа к внешним доменам настраиваются так.

1. Запустите оснастку Internet Information Services и дважды щелкните значок виртуального сервера.
2. В левой части окна выберите узел Domains (Домены). Появится список имеющихся на сервере служебных доменов.
3. Щелкните правой кнопкой удаленный домен и выберите в контекстном меню команду Properties (Свойства).
- Л. На вкладке General (Общие) щелкните Outbound Security (Безопасность подключений). Откроется одноименное диалоговое окно (рис. 8-8).





**Рис. 8-8.** Диалоговое окно Outbound Security (Безопасность исходящих подключений)

5. Включите обычную проверку подлинности, обеспечивающую широкую совместимость, щелкнув переключатель Basic Authentication (Обычная проверка подлинности).
6. Включите безопасную проверку подлинности для Windows-совместимых доменов, щелкнув Windows Security Package (Пакет безопасности Windows).
7. Укажите регистрационные реквизиты пользователя в полях User Name (Имя пользователя) и Password (Пароль) (они имеются для каждого режима проверки подлинности). Если удаленный домен располагается на том же дереве или в лесу доменов Active Directory, можете щелкнуть Browse (Обзор), найти соответствующую учетную запись в окне Select User (Выбор: Пользователь) и ввести пароль.
8. Пометьте флажок TLS Encryption (TLS-шифрование), если нужно шифровать пересылаемые сообщения и конечные серверы удаленного домена поддерживают смарт-карты или сертификаты X.509.
9. Щелкните OK.



**Примечание** Если помечен флажок TLS Encryption, конечные серверы удаленного домена должны обязательно поддерживать смарт-карты или сертификаты X.509. Иначе все посланные удаленному домену сообщения будут возвращены с отчетом о невозможности доставки.

### Настройка направляющего узла для удаленного домена

Вы вправе отправлять исходящие сообщения домену-адресату не напрямую, а через направляющий узел. Таким образом, можно пересылать сообщения через конкретный сервер, что иногда выгоднее пересылки по обычному маршруту.

Настроить/удалить направляющий узел для удаленного домена можно так.

1. Запустите оснастку Internet Information Services и дважды щелкните значок виртуального сервера,
2. В левой части окна выберите узел Domains (Домены). Появится список имеющихся на сервере служебных доменов.
3. Щелкните правой кнопкой удаленный домен и выберите в контекстном меню команду Properties (Свойства).
4. Чтобы задать направляющий узел, щелкните Forward All Mail To Smart Host (Пересылать всю почту на направляющий узел) и затем введите IP-адрес или DNS-имя направляющего узла.



**Совет** IP-адрес направляющего узла следует заключить в квадратные скобки [], чтобы служба SMTP не пыталась выполнить по нему DNS-поиск. Заметьте также, что направляющий узел, указанный для удаленного домена, переопределит направляющий узел, заданный непосредственно для виртуального SMTP-сервера.

5. Для удаления направляющего узла щелкните Use DNS To Route To This Domain (Для маршрутизации на этот домен использовать DNS).
6. Щелкните ОК.

### Переименование и удаление служебных доменов

Переименовать служебный домен нельзя, но вы можете создать новый домен-псевдоним или удаленный домен и за-

тем удалить существующий. Например, если вы создали служебный домен `tcc.microsoft.com` вместо `tech.microsoft.com`, вам понадобится создать новый и лишь затем удалить старый служебный домен. Домен по умолчанию удалить нельзя. Домен по умолчанию переименовывается так.

1. Создайте домен-псевдоним с нужным именем.
2. Сделайте домен-псевдоним доменом по умолчанию.
3. Удалите старый домен по умолчанию.

Чтобы удалить служебный домен, сделайте так.

1. Запустите оснастку Internet Information Services и дважды щелкните значок виртуального сервера.
2. В левой части окна выберите узел Domains (Домены). Появится список имеющихся на сервере служебных доменов.
3. Щелкните домен правой кнопкой и выберите в контекстном меню команду Delete (Удалить). В ответ на запрос системы щелкните Yes (Да).

## Обработка входящих соединений

Управлять входящими соединениями виртуальных серверов можно несколькими способами. Вы можете предоставлять или блокировать доступ на основе IP-адресов или доменных имен Интернета, требовать безопасных входящих соединений, назначить проверку подлинности для входящих соединений, ограничивать число параллельных подключений и задавать интервал ожидания подключений.



**Примечание** Служба SMTP позволяет управлять как входящими, так и исходящими соединениями. Подробнее об управлении исходящими соединениями см. раздел «Обработка исходящих соединений» этой главы.

### Управление доступом на основе IP-адреса, подсети или домена

По умолчанию виртуальные серверы доступны с любого IP-адреса, что создает опасность некорректного использования нашего сервера злоумышленниками. Для управления использованием виртуального сервера можно предоставлять или блокировать доступ по IP-адресам, подсетям и доменам.

Предоставление доступа позволяет компьютеру обращаться к виртуальному серверу, но не гарантирует пользователям возможность отправлять или получать сообщения. Если включена проверка подлинности, пользователи должны ее пройти.

Отказ в доступе запрещает компьютеру обращаться к ресурсам. Значит, пользователи данного компьютера не отправят и не получат сообщения, даже если бы у них была возможность успешно пройти проверку подлинности.

Чтобы разрешить/запретить доступ к виртуальному серверу по IP-адресу, подсети или домену, сделайте так.

1. Запустите оснастку Internet Information Services, щелкните виртуальный SMTP-сервер правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке Access (Доступ) щелкните Connection (Подключение). В списке Computers (Список компьютеров) (рис. 8-9) перечислены компьютеры, для которых настроены разрешения доступа.

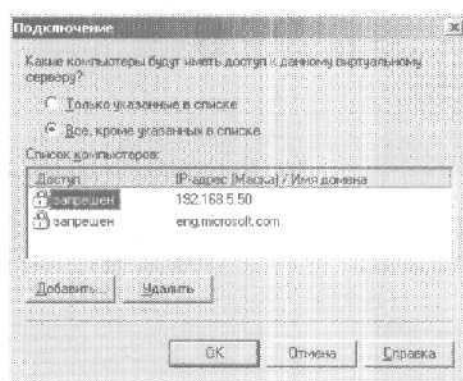



Рис. 8-9. Диалоговое окно Connection (Подключение)

3. Чтобы разрешить доступ определенным и запретить доступ остальным компьютерам, щелкните переключатель Only The List Below (Только указанные в списке).
4. Чтобы запретить доступ определенным и разрешить доступ остальным компьютерам, щелкните переключатель All Except The List Below (Все, кроме указанных в списке).

5. Создайте список доступа. Для этого щелкните Add (Добавить), затем в диалоговом окне Computer (Компьютер) - Single Computer (Отдельный компьютер), Group Of Computers (Группа компьютеров) или Domain (Домен) и введите:
  - для отдельного компьютера — его IP-адрес, например 192.168.5.50;
  - для группы компьютеров — адрес их подсети, например 192.168.5.0, и маску подсети, например 255.255.255.0.
  - для домена — его полное имя, например eng.domain.com.
-  **Внимание!** После предоставления или запрета доступа отдельному домену службы IIS должны выполнять по всем входящим соединениям обратный DNS-поиск, чтобы определить исходный домен. Это значительно замедляет отклик на первый запрос любого пользователя к Web-узлу.
6. Чтобы удалить запись из списка доступа, выделите ее в списке Computers (Список компьютеров) и щелкните Remove (Удалить).
7. Щелкните ОК.

### Защищенные входящие соединения

По умолчанию почтовые клиенты передают информацию по незащищенным подключениям. Настраиваются защищенные соединения так.

1. Создайте для виртуального SMTP-сервера, с которым хотите установить защищенную связь, запрос на сертификат. Сервер, обменивающийся сообщениями с защищенными серверами, также должен обладать сертификатом.
2. Перелайте запрос в сертификационный центр, и тот выдаст вам сертификат (обычно бесплатно).
3. Установите сертификат на виртуальном SMTP-сервере. Повторите пп. 1-3 для всех виртуальных SMTP-серверов, которым нужно обмениваться сообщениями по защищенным соединениям.
4. Настройте сервер так, чтобы он требовал защищенной связи ото всех виртуальных серверов.

Запросить и установить сертификат, а также разрешить его использование виртуальным сервером можно так.

1. В оснастке IIS щелкните правой кнопкой виртуальный сервер, на котором требуется настроить защищенную связь, и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке Access (Доступ) щелкните Certificate (Сертификат). Запустится Web Certificate Wizard (Мастер сертификатов Web-сервера), который поможет вам создать новый сертификат.
3. Перелайте запрос на сертификат в сертификационный центр. Получив сертификат, снова запустите мастер Web Certificate Wizard. Теперь вы можете обработать ожидающий запрос и установить сертификат.
4. Завершив установку сертификата, не закрывайте диалоговое окно Properties (Свойства), а щелкните Communicate (Связь) на вкладке Access (Доступ).
5. В диалоговом окне Security (Связь) щелкните Require Secure Channel (Требуется безопасный канал) и затем, если вы также настроили 128-разрядное шифрование, - Require 128-Bit Encryption (Требуется 128-и разрядное шифрование).
6. Дважды щелкните ОК.

#### Проверка подлинности входящих соединений

Служба SMTP поддерживает следующие режимы проверки подлинности.

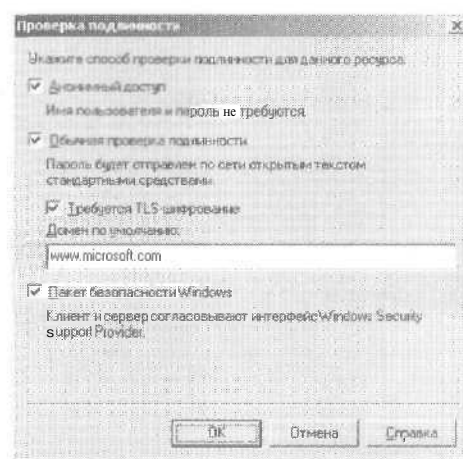
- Anonymous (Анонимный доступ) — пользователи могут анонимно подключаться к серверу и отправлять сообщения. Виртуальные SMTP-серверы большинства Web-серверов сконфигурированы для анонимного доступа, что позволяет приложениям и внешним пользователям передавать сообщения для отправки в домен, не проходя проверку подлинности. При таком подходе почтовый сервер не защищен от некорректного использования.
- Basic Authentication (Обычная проверка подлинности) — для установки связи с виртуальным SMTP-сервером пользователи должны указать регистрационные реквизиты, которые передаются по сети в незашифрованном виде.

Если на сервере настроена защищенная связь, можно требовать от клиентов использования протокола SSL - при этом регистрационные реквизиты перед передачей их серверу шифруются.

- **Windows Security Package** (Пакет безопасности Windows) — служба SMTP проверяет подлинность пользователя с применением обычной системы безопасности Windows. Вместо передачи регистрационных реквизитов по сети клиент указывает их при входе в Windows. Передаваемая информация полностью зашифрована, не требует использования SSL и включает имя пользователя и пароль для входа в сеть.

По умолчанию виртуальные SMTP-серверы используют все три режима проверки подлинности, которые **включаются/отключаются** так.

1. Запустив оснастку Internet Information Services, щелкните правой кнопкой значок виртуального сервера и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке Access (Доступ) щелкните Authentication (Проверка подлинности). Откроется одноименное диалоговое окно (рис. 8-10).



**Рис. 8-Ю.** Диалоговое окно Authentication (Проверка подлинности)

3. Выберите режим проверки подлинности. Помните, что, если анонимный доступ отключен, клиентам перед отправкой сообщений, возможно, придется проходить проверку подлинности. Тогда вам понадобится изменить конфигурационные параметры Web-приложений сервера.
4. Включив режим Basic authentication (Обычная проверка подлинности), задайте домен по умолчанию, который будет задействован, если при регистрации в системе не предоставлено сведений о домене. Это позволит гарантировать, что клиенты будут корректно проходить проверку подлинности. Кроме того, в режиме Basic authentication можно требовать TLS-шифрования. При этом для установки защищенной связи с сервером на клиентском компьютере должна быть установлена смарт-карта или сертификат.
5. Дважды щелкните ОК.

#### **Управление числом входящих соединений и временем ожидания подключения**

Для управления входящими соединениями виртуального SMTP-сервера можно ограничить число параллельных соединений и задать время ожидания подключения.

Обычно виртуальный SMTP сервер принимает неограниченное число соединений, и это оптимально для большинства сред. Однако в целях предотвращения перегрузки сервера можно ограничить число параллельных подключений. При достижении максимального числа подключений новым клиентам придется ждать, пока число подключений не сократится.

По истечении срока ожидания сервер разрывает клиентское подключение. Обычно срок ожидания подключения составляет 10 минут. Но иногда его требуется увеличить, например, если сервер отключает клиентов при передаче ими больших сообщений.

Для управления числом входящих соединений и временем ожидания подключения сделайте так.

1. Запустите оснастку Internet Information Services, щелкните правой кнопкой значок виртуального сервера и выберите в контекстном меню команду Properties (Свойства).



2. На вкладке General (Общие) щелкните Connection (Подключение). Откроется одноименное диалоговое окно (рис. 8-11).

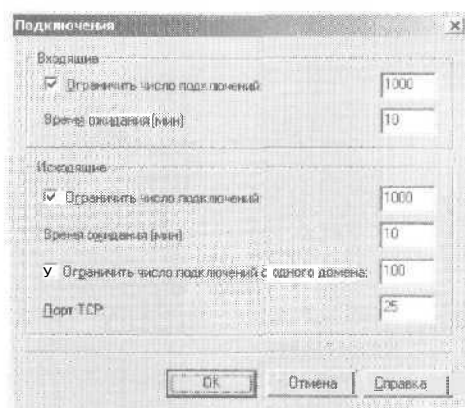


Рис. 8-11. Диалоговое окно Connections (Подключения)

3. Поле Limit Connections To (Ограничить число подключений) группы Incoming (Входящие) позволяет задать максимальное число подключений к SMTP-серверу. Чтобы снять ограничения на количество подключений, очистите данное поле.
4. В поле Time-Out (Время ожидания) можно задать интервал ожидания, рекомендуется 10-30 минут.
5. Дважды щелкните ОК, чтобы сохранить изменения.

### Обработка исходящих соединений

Существует несколько способов управления исходящими соединениями виртуальных серверов. Вы можете требовать проверки подлинности для исходящих соединений, ограничивать число параллельных подключений и задавать интервал ожидания подключений, задавать ограничения на сообщения, управлять сообщениями, доставка которых невозможна, задавать ограничения ретрансляции сообщений.

### Безопасность исходящих соединений

По умолчанию виртуальные SMTP-серверы доставляют сообщения другим серверам, не проходя проверки подлинно-

сти, т. е. анонимно. Кроме того, SMTP-сервер можно настроить для использования обычной проверки подлинности или проверки подлинности средствами Windows. И все же виртуальные SMTP-серверы крайне редко используют проверку подлинности.

Так, проверка подлинности средствами Windows для исходящих соединений применяется, только если виртуальному SMTP-серверу требуется доставлять все электронные сообщения на определенный сервер или адрес электронной почты в другом домене. Иначе говоря, если сервер доставляет почту только одному адресату и никому другому. Если вам нужно настроить проверку подлинности для почты, доставляемой на конкретный сервер, и одновременно доставлять почту на другие серверы, настройте для отсылки почты на первый сервер удаленный служебный домен, а для остальных сообщений используйте анонимную проверку подлинности.

Просмотреть/изменить параметры безопасности исходящих соединений можно так.

1. Запустите оснастку Internet Information Services, щелкните правой кнопкой значок виртуального сервера и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке Delivery (Доставка) щелкните Outbound Security (Безопасность подключений). Для обычной доставки исходящих сообщений щелкните Anonymous Access (Анонимный доступ).
3. Чтобы включить обычную проверку подлинности, пометьте флажок Basic Authentication (Обычная проверка подлинности) и введите в поля User Name (Имя пользователя) и Password (Пароль) имя учетной записи и пароль для подключения к удаленному серверу.
4. Чтобы включить проверку подлинности средствами Windows, пометьте флажок Windows Security Package (Пакет безопасности Windows) и введите в поля User Name (Учетная запись) и Password (Пароль) имя учетной записи Windows и пароль для подключения к удаленному серверу.
5. При использовании проверки подлинности можно также требовать шифрования данных. Для этого пометьте флажок TLS Encryption (TLS-шифрование).



**Примечание** Если помечен флажок TLS Encryption, конечные серверы удаленного домена должны обязательно поддерживать смарт-карты или сертификаты X.509. Иначе все посланные удаленному домену сообщения будут возвращены с отчетом о невозможности доставки.

6. Дважды щелкните ОК.

### Управление исходящими соединениями

Служба SMTP предоставляет гораздо больше возможностей управления исходящими соединениями, чем входящими. Вы можете ограничить число параллельных подключений и число подключений на один домен, задав максимальное число одновременных исходящих соединений. По умолчанию общее число подключений — 1 000, а число подключений на домен — 100. В целях повышения производительности измените эти значения в зависимости от емкости своего Web-сервера.

Можно также задать время ожидания, по истечении которого сервер разорвет клиентское подключение. Обычно он составляет 10 минут. При проблемах со связью или доставкой сообщений время ожидания следует увеличить.

Кроме того, для исходящих подключений вы вправе задействовать TCP-порт, отличный от номера 25. Если вы используете брандмауэр или прокси-сервер, привяжите исходящие соединения к другому порту и разрешите брандмауэру или прокси-серверу доставлять сообщения через SMTP-порт по умолчанию (25).

Для управления исходящими соединениями сделайте так.

1. Запустите оснастку Internet Information Services, щелкните правой кнопкой значок виртуального сервера и выберите в контекстном меню команду Properties (Свойства),
2. На вкладке General (Общие) щелкните Connection (Подключение). Откроется одноименное диалоговое окно (рис. 8-11).
3. Поле Limit Connections To (Ограничить число подключений) группы Outgoing (Исходящие) позволяет задать максимальное число подключений к SMTP-серверу. Чтобы снять ограничения на количество подключений, очистите это поле.

4. В поле Time-Out (Время ожидания) можно задать срок ожидания, рекомендуется 10-30 минут,
5. Поле Limit Connections Per Domain To (Ограничить число подключений с одного домена) позволяет задать максимальное число подключений на один домен. Чтобы снять ограничения на количество подключений, очистите это поле.
- fi. В поле TCP Port (Порт TCP) можно указать порт для исходящих соединений.
7. Дважды щелкните ОК, чтобы сохранить изменения.

#### **Настройка ограничений на исходящие сообщения для SMTP**

Ограничения на исходящие сообщения позволяют управлять использованием SMTP, а также ускорить доставку сообщений. Вы можете задать максимально допустимый размер входящих сообщений. Отправитель сообщения, превышающего заданный размер, получит соответствующий отчет о невозможности доставки. Максимальный размер сообщения по умолчанию — 2 048 Кб.

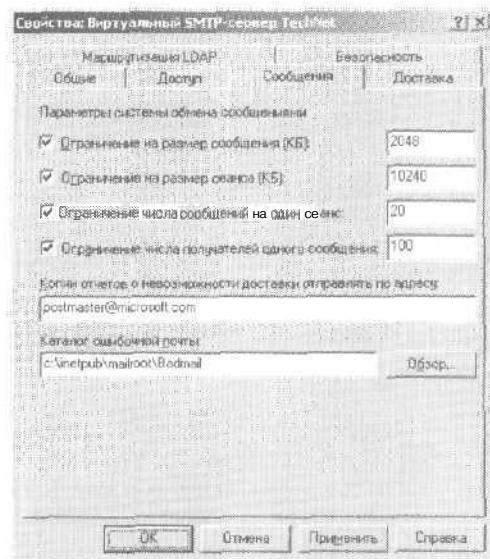
Можно задать максимальную длительность сеанса связи. Она всегда должна быть больше, чем максимальный размер отдельного сообщения, и по умолчанию равна 10 240 Кб. Клиент, пытающийся отправить несколько сообщений, общий размер которых превышает заданное значение, получит соответствующий отчет о невозможности доставки.

Кроме того, вы вправе ограничить число сообщений, отсылаемых по одному подключению. При превышении заданного значения служба SMTP установит новое соединение и продолжит передачу сообщений, пока не разошлет их все. Оптимизация этого значения для конкретной рабочей среды повысит производительность сервера, особенно если пользователи отправляют большое количество сообщений в одни и те же внешние домены. По умолчанию максимальное число сообщений, отправляемых по одному подключению, — 20. Таким образом, если в очереди на отправку к одному и тому же конечному серверу стоит 50 сообщений, SMTP доставит их по трем подключениям. Если оптимизировать число подключений, доставка почты займет меньше времени.

Вы также можете ограничить допустимое число адресатов одного сообщения. При превышении заданного значения SMTP откроет новое соединение и доставит по нему сообщения оставшимся адресатам. По умолчанию допустимое число адресатов одного сообщения — 100. С использованием параметров по умолчанию сообщение для 300 адресатов будет доставлено по трем подключениям. Если оптимизировать число адресатов, доставка почты займет меньше времени,

Ограничения исходящих соединений настраиваются так.

1. Запустив оснастку Internet Information Services, щелкните правой кнопкой значок виртуального сервера и выберите в контекстном меню команду Properties (Свойства),
2. Перейдите на вкладку Messages (Сообщения) (рис. 8-12).



**Рис. 8-12.** Вкладка Messages (Сообщения) диалогового окна свойств SMTP-сервера

3. Чтобы задать максимально допустимый размер сообщения, пометьте флажок Limit Message Size To [Ограничение на размер сообщения (КБ)] и в поле напротив вве-

- дите нужное значение. Чтобы снять ограничения, сбросьте флажок.
4. Чтобы задать максимальный размер сеанса связи, пометьте флажок `Limit Session Size To` [Ограничение на размер сеанса (КБ)] и в поле напротив введите нужное значение. Чтобы снять ограничения, сбросьте флажок.
  5. Чтобы служба SMTP открывала новые подключения, когда в очереди на доставку к одному серверу находится множество сообщений, пометьте флажок `Limit Number Of Messages Per Connection To` (Ограничение числа сообщений на один сеанс) и в поле напротив введите число сообщений, которое будет пересылаться по одному подключению. Чтобы снять ограничения, сбросьте флажок.
  6. Чтобы служба SMTP открывала новые подключения, когда в очереди на доставку находится сообщение, предназначенное множеству получателей, пометьте флажок `Limit Number Of Recipients Per Message To` (Ограничение числа получателей одного сообщения) и в поле напротив введите число получателей, которым будет отправляться сообщение по одному подключению. Чтобы снять ограничения, сбросьте флажок.
  7. Щелкните ОК.

#### **Управление сообщениями, доставка которых невозможна**

Если доставить сообщение невозможно или в процессе доставки произошла неустраняемая ошибка, SMTP генерирует отчет о невозможности доставки и пытается доставить его отправителю. Виртуальные SMTP-серверы предоставляют несколько способов управления сообщениями, доставка которых невозможна.

В целях мониторинга лучше отправлять копии всех отчетов о невозможности доставки на определенный адрес электронной почты. Этот адрес также помещается в поле `Reply-To` отчета, что позволяет пользователям реагировать на сообщения об ошибках.

Если доставить отчет отправителю не удастся, исходное сообщение помещается в папку `Badmail`. Находящиеся в ней сообщения невозможно доставить адресату или вернуть от-

правителю. Периодически просматривайте содержимое этой папки, чтобы вовремя выявлять сбои в работе вашей почтовой системы. По умолчанию путь к папке Badmail — Inetpub\Mailroot\Badmail. При локальной работе с сервером его можно в любой момент изменить.

Параметры обработки сообщений, доставка которых невозможна, настраиваются так.

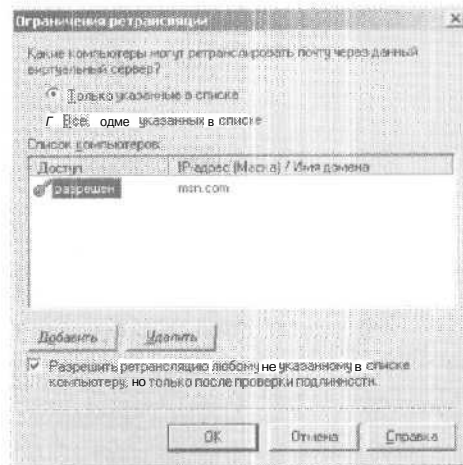
1. Запустив оснастку Internet Information Services, щелкните правой кнопкой значок виртуального сервера и выберите в контекстном меню команду Properties (Свойства).
2. Перейдите на вкладку Messages (Сообщения) (рис. 8-12).
3. В поле Send Copy Of Non-Delivery Report To (Копии отчетов о невозможности доставки отправлять по адресу) введите адрес электронной почты почтмейстера нашей организации или другого лица, которому следует отсылать копии отчетов о невозможности доставки.
4. В поле Badmail Directory (Каталог ошибочной почты) введите полный путь к папке Badmail или щелкните Browse (Обзор) и выберите папку в диалоговом окне Browse For Folder (Обзор папок).
5. Щелкните ОК.

#### Разрешение и запрет ретрансляции

Ретрансляцией называется пересылка через ваш почтовый сервер внешними пользователями сообщений для сторонних организаций. По умолчанию ретрансляция сообщений неавторизованными пользователями и компьютерами запрещена. Таким образом, ретранслировать почту через ваш сервер смогут только пользователи и компьютеры, прошедшие проверку подлинности.

Впрочем, можно разрешить или запретить ретрансляцию конкретным компьютерам, сетям или доменам, переопределив параметры по умолчанию.

1. Запустив оснастку Internet Information Services, щелкните правой кнопкой виртуальный SMTP-сервер и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке Access (Доступ) щелкните Relay (Ретрансляция). Откроется диалоговое окно Relay Restrictions (Ограничения ретрансляции) (рис. 8-13).



**Рис. 8-13.** Диалоговое окно Relay Restrictions (Ограничения ретрансляции)

3. Чтобы разрешить доступ определенным и запретить доступ остальным компьютерам, щелкните переключатель **Only The List Below** (Только указанные в списке).
4. Чтобы запретить доступ определенным и разрешить доступ остальным компьютерам, щелкните переключатель **All Except The List Below** (Все, кроме указанных в списке). Далее:
  - создайте список доступа, для этого щелкните **Add** (Добавить), затем в диалоговом окне **Computer** (Компьютер) — **Single Computer** (Отдельный компьютер), **Group Of Computers** (Группа компьютеров) или **Domain** (Домен);
  - для отдельного компьютера введите его IP-адрес, например 192.168.5.50;
  - для группы компьютеров введите адрес их подсети, например 192.168.5.0, и маску подсети, например 255.255.255.0;
  - для домена введите его полное имя, например - eng.domain.com.





**Внимание!** После предоставления или запрета доступа отдельному домену IIS должны выполнять по всем входящим соединениям обратный DNS-поиск, чтобы определить их исходный домен. Это заметно замедляет отклик на первый запрос любого пользователя к Web-узлу.

5. Чтобы удалить запись из списка доступа, выделите ее в списке Computers (Список компьютеров) и щелкните Remove (Удалить).
6. По умолчанию ретрансляция через данный виртуальный SMTP-сервер разрешена всем компьютерам, прошедшим процедуру проверки подлинности. Чтобы изменить это и управлять ретрансляцией по списку авторизации, снимите флажок Allow All Computers Which Successfully Authenticate To Relay (Разрешить ретрансляцию любому не указанному в списке компьютеру, но только после проверки подлинности).
7. Щелкните OK.

## Управление доставкой сообщений

Параметры доставки SMTP определяют, как будет осуществляться доставка сообщений после установки связи подтверждения конечным компьютером готовности к приему данных. Для управления доставкой сообщений можно настраивать интервалы повторной отправки внешних сообщений, уведомления о задержке локальных и внешних сообщений, срок окончания доставки локальных и внешних сообщений, число пересылок сообщения, доменные имена, обратный DNS-поиск, списки внешних DNS-серверов.

### Настройка параметров отправки сообщений

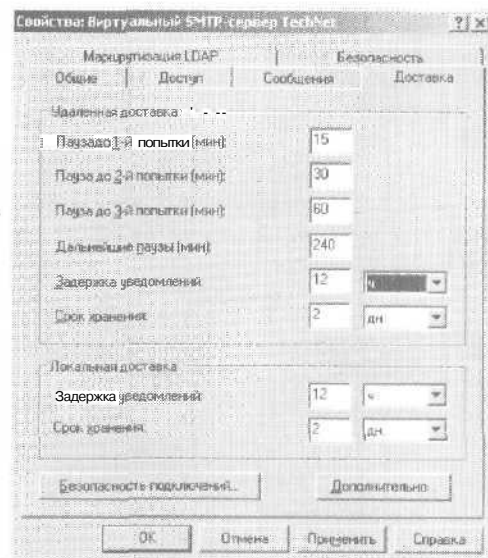
После того как будет установлена связь и конечный компьютер подтвердит готовность к приему данных, служба SMTP начинает доставку находящихся в очереди сообщений для этого компьютера. Если первая попытка оказалась неудачной, SMTP пытается доставить сообщение повторно через заданные промежутки времени, вплоть до наступления срока окончания доставки. Затем сообщение возвращается отправителю с отчетом о невозможности доставки. Срок окончания доставки по умолчанию — 2 дня.

После каждой неудачной попытки SMTP генерирует уведомление о задержке и помещает его в очередь для отсылки отправителю исходного сообщения. Уведомление отсылается не сразу, а лишь через определенный срок и только при условии, что сообщение все еще не отправлено. По умолчанию срок уведомления о задержке — 12 часов.

Для локальных и внешних сообщений служба SMTP использует различные сроки уведомления о задержке и окончании отправки сообщения. Сообщения, созданные внутри организации, обрабатываются в сроки уведомления о задержке и окончания отправки, заданные для локальных сообщений. Прочие сообщения обрабатываются в сроки, заданные для внешних сообщений.

Просмотреть/изменить параметры отправки сообщений можно так.

1. Запустив оснастку Internet Information Services, щелкните правой кнопкой значок виртуального сервера, и выберите в контекстном меню команду **Properties** (Свойства).
2. **Перейдите на вкладку Delivery (Доставка).** Поля этой вкладки (рис. 8-14) позволяют задать **время ожидания**:
  - **First Retry Interval** [(Пауза до первой попытки (мин))] — после первой попытки доставить сообщение, по умолчанию — 15 минут;
  - **Second Retry Interval** [(Пауза до второй попытки (мин))] — после второй попытки доставить сообщение, по умолчанию — 30 минут;
  - **Third Retry Interval** [(Пауза до третьей попытки (мин))] — после третьей попытки доставить сообщение, по умолчанию — 60 минут;
  - **Subsequent Retry Interval** [Дальнейшие паузы (мин)] — после четвертой и последующих попыток доставить сообщение, по умолчанию — 240 минут.
3. В полях **Delay Notification** (Задержка уведомлений) и **Expiration Timeout** (Срок хранения) группы **Outbound** (Удаленная доставка) задайте срок уведомления о задержке и окончании отправки исходящих сообщений. Сроки могут быть указаны в минутах, часах или днях и распространяются на сообщения для удаленных и прочих внешних доменов.



**Рис. 8-14.** Вкладка Delivery (Доставка) диалогового окна свойств SMTP-сервера

4. В полях Delay Notification (Задержка уведомлений) и Expiration Timeout (Срок хранения) группы Local (Локальная доставка) задайте срок уведомления о задержке и окончания отправки локальных сообщений. Сроки могут быть указаны в минутах, часах или днях и распространяются на сообщения для локальных и служебных доменов-псевдонимов.
5. Щелкните ОК.

#### Назначение числа пересылок сообщения

По пути к адресату сообщение зачастую проходит через множество серверов, количество которых называется числом пересылок. Администратор может задать максимально допустимое число пересылок сообщения, предотвращающее его многократную неверную маршрутизацию.

По умолчанию максимальное число пересылок — 15, что оптимально для большинства сетевых конфигураций. Но если пользователи часто получают отчеты о невозможности дос-

тавки сообщения из-за достижения максимального числа пересылок, можно увеличить это число. Число записей *Received* к заголовке сообщения показывает, сколько раз оно пересылалось.



**Внимание!** Прежде чем увеличить максимальное число пересылок сообщения, проверьте SMTP-маршрутизацию в своей сети. Отчеты о невозможности доставки из-за достижения максимального числа пересылок также указывают на сбой в SMTP-маршрутизации.

Число пересылок сообщения задается так.

1. Запустив оснастку *Internet Information Services*, щелкните правой кнопкой значок требуемого виртуального сервера, и выберите в контекстном меню команду *Properties* (Свойства).
2. На вкладке *Delivery* (Доставка) щелкните *Advanced* (Дополнительно). Откроется одноименное диалоговое окно.
3. Введите в поле *Maximum Hop Count* (Максимальное число пересылок) требуемое число пересылок. Возможные значения — от 10 до 256.
4. Дважды щелкните *OK*.

### Назначение параметров доменного имени

Доменные имена играют важную роль в определении порядка доставки почты. Вы можете задать подменяющий домен или ввести *полное доменное имя* (*fully qualified domain name*, *FQDN*) виртуального SMTP-сервера.

Подменяющий домен заменяет имя локального домена во всех строках *Mail From* заголовка сообщения. Сведения в поле *Mail From* определяют получателя отчета о невозможности доставки и не заменяют собой информацию поля *From* (От) исходного сообщения, выводимую конечным клиентам. Замена имени происходит только при первой пересылке сообщения.

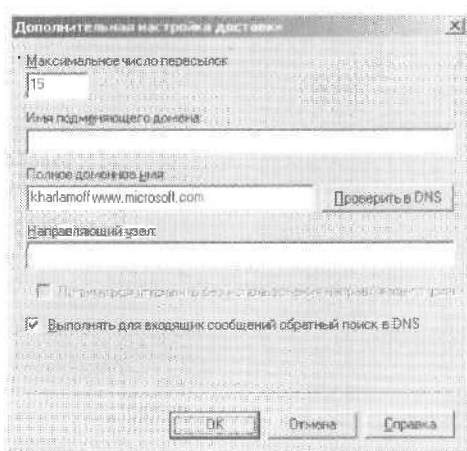
Полное доменное имя виртуального сервера используется при доставке почты, у сервера должно быть *FQDN*; посредством хранящейся в таблицах *DNS* записи о сервере сообщений этому *FQDN* сопоставляется домен электронной почты. *FQDN* можно задать двумя способами; задействовать имя, указанное на вкладке *Network Identification* (Сетевая

идентификация) утилиты System (Свойства системы), или указать уникальное FQDN для настраиваемого вами виртуального SMTP-сервера.

Имя с вкладки Network Identification (Сетевая идентификация) используется автоматически. Если его изменить, после перезагрузки компьютера будет использоваться новое имя. FQDN виртуального сервера при этом обновляется автоматически. Тем не менее, чтобы переопределить параметры вкладки Network Identification, задайте отдельное FQDN для этого виртуального сервера.

Чтобы задать имя подменяющего домена или переопределить FQDN по умолчанию, сделайте так.

1. Запустив оснастку Internet Information Services, щелкните правой кнопкой значок виртуального сервера, и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке Delivery (Доставка) щелкните Advanced (Дополнительно). Откроется одноименное диалоговое окно (рис. 8-15).



**Рис. 8-15.** Диалоговое окно Advanced Delivery (Дополнительная настройка доставки)

3. В поле Masquerade Domain (Имя подменяющего домена) введите доменное имя, на которое будут отсылаться отчеты о невозможности доставки сообщения. Это имя за-

менит имя домена по умолчанию в заголовках исходящих сообщений.

- Л. Чтобы переопределить FQDN по умолчанию, введите в поле Fully-Qualified Domain Name (Полное доменное имя) новое доменное имя. Щелкните Check DNS (Проверить в DNS) и убедитесь, что введено нужное имя и что разрешение DNS настроено правильно,
5. Дважды щелкните OK, чтобы сохранить изменения.

### Настройка обратного DNS-поиска

Обратный поиск позволяет службе SMTP убедиться, что IP-адрес почтового клиента соответствует компьютеру и домену, которые клиент указал в команде начала сеанса. Если IP-адрес и сведения DNS совпадают, SMTP пропускает сообщение без изменений. В противном случае в поле Received заголовка сообщения вставляется ключевое слово `unverified`.

Как уже говорилось, на производительность SMTP обратный поиск оказывает негативное влияние, которое лишь увеличивается с ростом числа параллельных пользователей и подключений. В связи с этим обратный DNS-поиск следует включать с осторожностью.

Обратный DNS-поиск включается так.

1. Запустив оснастку Internet Information Services, щелкните правой кнопкой значок виртуального сервера и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке Delivery (Доставка) щелкните Advanced (Дополнительно). Откроется одноименное диалоговое окно (рис. 8-15).
3. Чтобы включить обратный поиск, пометьте флажок Perform Reverse DNS Lookup On Incoming Messages (Выполнять для входящих сообщений обратный поиск в DNS). Чтобы отключить обратный DNS-поиск, снимите флажок.
- 4. Дважды щелкните OK.

### Пересылка исходящих сообщений на направляющий узел

Исходящие сообщения можно отправлять домену-адресату не напрямую, а через направляющий узел. Таким образом, можно пересылать сообщения через конкретный сервер, что иногда выгоднее пересылки по обычному маршруту.

Направляющий узел для удаленного домена настраивается/удаляется так.

1. Запустив оснастку Internet Information Services, щелкните правой кнопкой значок виртуального сервера и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке Delivery (Доставка) щелкните Advanced (Дополнительно). Откроется одноименное диалоговое окно (рис. 8-15).
3. Чтобы задать направляющий узел, введите в поле Smart Host (Направляющий узел) IP-адрес или DNS-имя направляющего узла. Если хотите, чтобы служба SMTP предварительно пыталась доставить сообщение непосредственно адресату, пометьте флажок Attempt Direct Delivery Before Sending To Smart Host (Попытаться отправить без использования направляющего узла).



**Совет** IP-адрес направляющего узла следует заключить в квадратные скобки [], чтобы служба SMTP не пыталась выполнить по нему DNS-поиск. Заметьте также, что направляющий узел, указанный для удаленного домена, переопределит направляющий узел, заданный непосредственно для виртуального SMTP-сервера.

4. Чтобы удалить направляющий узел, очистите поле Smart Host (Направляющий узел).
5. Дважды щелкните ОК.

## Глава 9

# Администрирование службы Indexing Service

Служба Indexing Service (Служба индексирования) позволяет создавать каталоги документов, где можно осуществлять поиск. Реализовав на Web-узле поддержку этой службы, вы предоставите пользователям возможность находить нужную информацию с помощью обычной HTML-формы. Как и Internet Information Services (IIS), Indexing Service интегрирована в ОС Microsoft Windows. Допустимо ее использование в интрасетях, внешних сетях и Интернете. Web-администратор должен уметь настроить необходимые Indexing Service каталоги и сконфигурировать их содержимое и ежедневно управлять их индексированием.

Управление Indexing Service значительно отличается от управления IIS. Перед использованием Indexing Service вы должны предпринять следующее.

1. Установите службу Indexing Service на узел или виртуальный сервер, которые нужно проиндексировать. По умолчанию Indexing Service сконфигурирована для запуска вручную. Измените параметры службы так, чтобы она запускалась автоматически.
2. Создайте каталог с документами, где будет осуществляться поиск. Каждый каталог нужно сопоставить отдельному Web-узлу и виртуальному NNTP-серверу.
3. Укажите индексируемые файлы и папки. Параметры индексирования можно задать в оснастке Internet Information Services.
4. Создайте на Web-узле страницу поиска, которая будет задействована для доступа к каталогу и извлечения информации, удовлетворяющей условиям поиска. В коде



страницы при помощи переменной `CiCatalog` должно быть определено физическое расположение каталога. Есть и дополнительные параметры для настройки поиска по индексам.

После установки и настройки Indexing Service автоматически создает и обновляет каталоги. Более того, служба пытается организовать каталоги так, чтобы данные в них были согласованными и актуальными. Данные каталогов иногда рассинхронизируются — в таких случаях придется перестроить каталог или с помощью службы Indexing Service провести принудительное сканирование папок на предмет требующих индексации документов. Далее мы рассмотрим эти и некоторые другие задачи администрирования.

## Основы работы со службой Indexing Service

Indexing Service извлекает информацию из указанных документов и преобразует результаты в каталог, в котором быстро и легко осуществлять поиск. К извлекаемой информации относятся как содержимое (текст) документов, так и их свойства, например сведения об авторе и названии. Чтобы понять принципы работы службы, мы рассмотрим, как установить и использовать Indexing Service, как она создает индексы и каталоги, как осуществлять поиск и управлять индексами.

### Использование службы Indexing Service

Служба Indexing Service индексирует:

- HTML-документы — .htm- или .html-файлы;
- текстовые файлы в формате ASCII — .txt-файлы;
- документы Microsoft Word — .doc-файлы;
- электронные таблицы Microsoft Excel — .xls-файлы;
- презентации Microsoft PowerPoint — .ppt-файлы;
- сообщения электронной почты и групп новостей (при индексировании виртуальных NNTP-серверов).

При установке специальных фильтров возможно индексирование и других документов.

Для установки Indexing Service на Web-сервере служит мастер Windows Components Wizard (Мастер компонентов Windows).

1. Зарегистрируйтесь в системе по учетной записи и паролю администратора.
2. Раскройте меню Start\Settings (Пуск\Настройка) и выберите Control Panel (Панель управления).
3. Дважды щелкните значок Add\Remove Programs (Установка и удаление программ). Откроется одноименное диалоговое окно.
4. Щелкните значок Add/Remove Windows Components (Добавление и удаление компонентов Windows). Запустится мастер Windows Components Wizard (Мастер компонентов Windows).
5. Выберите Indexing Service (Служба индексирования) и щелкните Next (Далее). Служба Indexing Service будет установлена на компьютер.

Управлять Indexing Service можно из оснастки Indexing Service (Служба индексирования) консоли MMC или узла Indexing Service (Служба индексирования) оснастки Computer Management (Управление компьютером). В любом случае вы сможете одинаково управлять как локальными, так и удаленными серверами. Единственное отличие; к удаленной системе нужно подключаться.

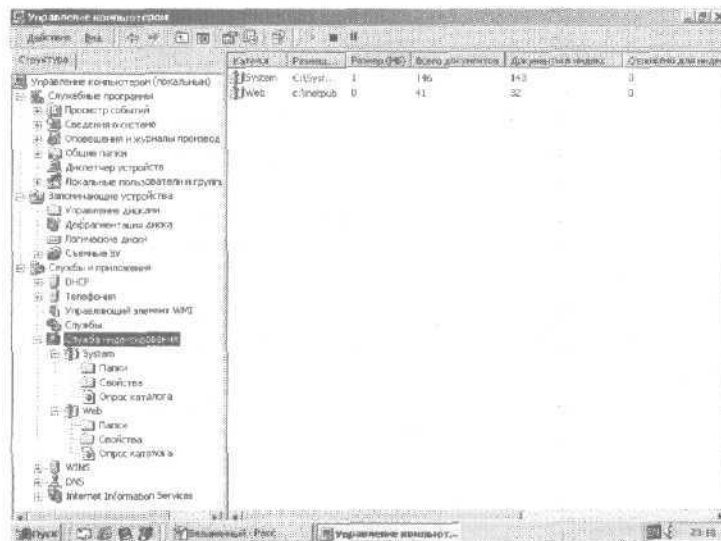
Для управления удаленным сервером из оснастки Indexing Service последнюю нужно добавить в консоль управления Microsoft.

Чтобы добавить оснастку Indexing Service в консоль MMC и выбрать требуемый сервер, сделайте следующее.

1. Раскройте меню Start (Пуск) и выберите команду Run (Выполнить). Откроется одноименное диалоговое окно.
2. В поле Run (Выполнить) введите *mmc* и щелкните ОК. Запустится консоль MMC.
3. В MMC щелкните Console (Консоль), а затем выберите Add/Remove Snap-In (Добавить/удалить оснастку). Откроется одноименное диалоговое окно.
4. На вкладке Standalone (Изолированная оснастка) щелкните Add (Добавить).
5. В диалоговом окне Add Standalone Snap-In (Добавить изолированную оснастку) выберите Indexing Service (Служба индексирования) и затем щелкните Add (Добавить).

6. Щелкните Local Computer (локальным компьютером), чтобы подключить к локальной системе. Кроме того, можно выбрать Another Computer (другим компьютером) и указать имя требуемого удаленного компьютера.
7. Щелкните Finish (Готово). Затем щелкните Close (Закреть) и OK.

При запуске оснастки Computer Management (Управление компьютером) автоматически подключается к локальной машине. Для подключения к другому компьютеру щелкните правой кнопкой узел Computer Management (Управление компьютером), выберите в контекстном меню команду Connect To Another Computer (Подключиться к другому компьютеру) и следуйте подсказкам на экране. Взгляните на узел Indexing Service (Служба индексирования) оснастки Computer Management (рис. 9-1).



**Рис. 9-1. Управление службой Indexing Service (Служба индексирования) с помощью оснастки Computer Management (Управление компьютером)**

Как видите, при выборе узла Indexing Service в правой части окна отображаются сведения об установленных катало-

гах, **включая** каталоги по умолчанию System и Web, в следующем формате:

- **Catalog** (Каталог) — описательное имя, заданное при создании каталога;
- **Location (Размещение)** — физическое **расположение** каталога, например D:\Catalogs\WWW\;
- **Size (Mb) (Размер, МБ)** — размер каталога в мегабайтах;



**Примечание** Обычно размер каталога — от 25 до 40% размера проиндексированных документов. Иначе говоря, при индексировании 1 Гб документов требуется 250–400 Мб дополнительного дискового пространства для создания соответствующего каталога.

- **Total Docs (Всего документов)** — общее число индексируемых в этом каталоге документов;
- **Docs to Index (Документы в индекс)** — число документов, которые осталось проиндексировать;
- **Deferred for Indexing (Отложено для индексирования)** — число документов, запланированное индексирование которых в данный момент **невозможно**, так как они заняты;



**Примечание** Indexing Service откладывает индексирование используемых документов и пытается проиндексировать их позже.

- **Word Lists (Списки слов)** — число связанных с данным каталогом и хранящихся в памяти системы списков слов;
- **Saved Indexes (Сохраненных индексов)** — число сохраненных в каталоге индексов;
- **Status (Состояние)** — состояние процесса индексирования.

Управляя Indexing Service из оснастки консоль Computer Management, вы обнаружите, что при установке службы было создано два каталога по умолчанию, содержащих:

- System — индекс всех документов на подключенных к серверу жестких дисках;
- Web — индекс Web-узла по умолчанию.



**Примечание** Рекомендую вам удалить каталог System. На IIS-серверах он обычно не используется, а на его поддержку требуются системные ресурсы.

Вы можете создать и дополнительные каталоги. При этом вы вправе сопоставить создаваемый каталог Web-узлу и виртуальному NNTP-серверу. Затем Indexing Service на основе параметров индексирования папок, связанных с Web-узлом, или виртуальным сервером, определяет подлежащие индексированию документы. Параметры индексирования задаются из оснастки Internet Information Services.

### Принципы работы службы Indexing Service

Indexing Service хранит сведения каталога в формате Unicode, благодаря чему может индексировать и запрашивать содержимое на разных языках. Для обработки содержимого документов служба Indexing Service выполняет три основные функции.

- **Индексирование** — извлечение информации из документов. Индекс включает содержимое тела документа, кроме слов из связанных с каталогом перечней исключений. Для экономии дискового пространства индексы хранятся в сжатом виде.
- **Создание каталога** — сохранение данных индекса в указанном месте. В каталогах хранится извлеченное содержимое документов в виде индексов и наборов свойств.
- **Слияние** — объединение временных индексов для создания сводных или основных индексов. Объединение индексов повышает производительность Indexing Service и снижает требования к объему ОЗУ для хранения временных индексов.

Индексирование и создание каталогов осуществляется автоматически в фоновом режиме в процессе работы Indexing Service. При первом запуске служба просматривает связанные с каждым каталогом папки и определяет подлежащие индексированию документы. Этот процесс называется сканированием. Indexing Service может осуществлять полное и выборочное сканирование.

При полном сканировании просматриваются все связанные с каталогом документы. Полное сканирование производится:

- при первом запуске службы Indexing Service после ее установки;
- после добавления папки в каталог;

- в процессе *восстановления* после серьезной ошибки;
- при запуске вручную.

В процессе выборочного сканирования просматриваются только *документы, измененные с момента последнего полного или выборочного сканирования*. Выборочное сканирование производится:

- при запуске или перезапуске службы Indexing Service;
- при изменении локального документа;
- утере службой Indexing Service *уведомлений* об изменениях;
- при запуске вручную.



**Примечание** Уведомления об изменениях в файловой системе — важная часть выборочного сканирования. Они генерируются ОС, и Indexing Service считывает их при любом изменении локальных документов. Зачастую уведомления об изменениях документов на удаленных *компьютерах* не достигают локальной Indexing Service. Зная об этом, Indexing Service периодически проводит выборочное сканирование всех связанных с каталогом удаленных папок.

Отсканировав подлежащие *индексированию* документы, Indexing Service приступает к созданию каталогов. Для этого она считывает все документы с помощью специальных фильтров — программных компонентов, интерпретирующих структуру документов определенного типа, например: текстовый файл ASCII, документ Microsoft Word, HTML-документ. Используя соответствующий фильтр, Indexing Service извлекает содержимое и значения свойств документа, помещая эти значения и путь к документу в индекс. Затем с помощью фильтра служба определяет язык документа и разбивает его содержимое на отдельные слова. Для всех *поддерживаемых* языков имеются списки слов-исключений, опускаемых Indexing Service.

Эти списки хранятся в папке `\%SystemRoot%\System32` и виде текстовых файлов формата ASCII с именем *Noise.lang*, где *lang* — трехсимвольное расширение, указывающее язык списка исключений. Добавлять слова в такой список или, наоборот, удалять их можно с помощью обычного текстового редактора.

Кроме того, Indexing Service заносит значения свойств документа в кэш свойств — место, где хранятся значения свойств, но которым будет осуществлен поиск, или которые требуется вывести в списке результатов поиска. В кэше свойств имеется два уровня хранения: первичный — для часто просматриваемых значений (поэтому значения здесь хранятся в формате, ускоряющем и упрощающем их получение) и вторичный — для дополнительных, редко просматриваемых значений.

Отбросив слова из перечня исключений и обновив кэш свойств, Indexing Service сохраняет остальное содержимое документа в виде списка слов. Каждому документу может быть сопоставлено несколько списков слов. Списки слов объединяются для создания промежуточных (временных) индексов. Последние хранятся на диске в сжатом виде. В любой момент времени в каталоге может находиться (и обычно находится) несколько таких индексов. Со временем при добавлении или изменении документов в проиндексированных папках, число временных индексов может существенно увеличиться.

При помощи фонового слияния Indexing Service объединяет списки слов и временные индексы, тем самым уменьшая количество используемых временных ресурсов и замедляя реакцию службы. Фоновое слияние — рутинная часть работы Indexing Service — производится при сканировании. Фоновое слияние запускается, если в памяти хранится слишком много списков слов (по умолчанию — 20), или если общий размер всех списков слов превышает заданное значение (по умолчанию — 256 Кб).

Конечный результат индексирования — основной индекс. У любого каталога он один, и только один. Основной индекс генерируется при создании каталога, и его актуальность поддерживается путем периодического слияния с временными индексами. В результате этого процесса, называемого полным слиянием, создается новый основной индекс. После полного слияния с каталогом будет связан только один сохраненный индекс — основной.

Полное слияние запускается автоматически на основе данных о размере временных индексов, объеме свободного пространства на диске каталога и числе изменений документов

в проиндексированной панке. Кроме того, полное слияние независимо от текущих условий происходит каждый день в полночь. При необходимости можно провести полное слияние принудительно — это заставит Indexing Service обновить каталог, и все изменения сразу отразятся на результатах поиска. Как вы понимаете, полное слияние — ресурсоемкий процесс, и поэтому выполнять его принудительно в часы пиковой нагрузки без веских причин не стоит.

Параметры, управляющие сканированием, слиянием и другими процессами службы Indexing Service, хранятся в разделе реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex`.

К параметрам реестра, управляющим сканированием и слиянием, относятся следующие.

- **MasterMergeCheckpointInterval** — интервал, по истечении которого определяется необходимость полного слияния. По умолчанию — 2 048 секунд.
- **MasterMergeTime** — время по умолчанию для ежедневного запуска полного слияния. По умолчанию — 0, т. е. полное слияние запускается с началом нового дня.
- **MaxFileSizeFiltered** — максимальный размер фильтруемого содержимого для отдельного документа. По умолчанию — 256 Кб.
- **MaxFreshCount** — максимальное число обновлений и изменений документов, при превышении которого запускается полное слияние. По умолчанию — 20 000 документов.
- **MaxIndexes** — максимальное число индексов, при превышении которого запускается фоновое слияние. По умолчанию — 25 индексов.
- **MaxShadowIndexSize** — максимальный размер временных индексов в приращениях по 128 Кб. Используется совместно с параметром **MinDiskFreeForceMerge** для запуска полного слияния, когда на диске не хватает свободного пространства, и размер временных индексов превышает заданное значение. По умолчанию — 15 (15×128 Кб = 1920 Кб).
- **MaxWordLists** — максимальное число списков слов в каталоге, при превышении которого запускается фоновое слияние. По умолчанию — 20 списков.



- **MaxWordlistSize** — максимальный размер связанных с каталогом списков слов в приращениях по 128 Кб. При превышении значения этого параметра запускается фоновое слияние. По умолчанию - 20 (20x128 Кб =2560 Кб).
- **MinDiskFreeForceMerge** — минимально приемлемый объем свободного пространства на диске. Если на диске каталогов меньше свободного пространства, чем задано этим параметром, и общий размер временных индексов превысит значение, заданное параметром **MaxShadowIndexSize**, служба Indexing Service выполнит полное слияние. По умолчанию — 15 Мб.
- **MinSizeMergeWordlists** — максимально приемлемый общий размер списков слов, при превышении которого запускается фоновое слияние. По умолчанию — 256 Кб.

### Поиск в каталогах

Поиск — это просмотр каталога для обнаружения необходимой информации. Поиск может осуществляться разными способами, но для Web-узлов чаще всего создают специальные формы запросов. Indexing Service включает формы поиска для каждого каталога, позволяющие протестировать установку службы. Кроме того, создать форму поиска можно, используя Active Server Pages и файлы Internet data query (IDQ).

При работе с ASP-страницами для создания формы запроса и обработки результатов применяется комбинация серверных сценариев, основанных на объектах ASP, HTML-коде и клиентских сценариях. Задействованные сценарии могут быть написаны на любом из установленных языков сценариев; по умолчанию установлены Microsoft VBScript и Microsoft Jscript. Обычно для реализации формы запроса и вывода результатов поиска по заданным пользователем параметрам применяют одну страницу. Например, можно создать ASP-страницу с именем QUERY.ASP, которая выводит форму запроса и содержит встроенный сценарий, отправляющий параметры поиска и затем форматирующий его результаты. С другой стороны, IDQ — специальный язык, предназначенный для передачи запросов службе Indexing Service. При

использовании IDQ создаются отдельные страницы для обработки каждого этапа процесса запроса, включая:

- **HTML-страницу с расширением .htm или .html** — выводит форму запроса;
- **IDQ-страницу с расширением .idq** — определяет фиксированные параметры запроса для осуществления поиска;
- **файл расширения HTML с расширением .htx** — форматирует результаты запроса.

IDQ-запросы быстрее и эффективнее используют ресурсы службы Indexing Service, чем ASP. Но независимо от того, что используется для поиска — IDQ или ASP, нужно указать основные параметры, задающие значения по умолчанию для службы Indexing Service (табл. 9-1).



**Примечание** В большинстве организаций есть Web-разработчики, в обязанности которых входит создание Web-страниц для поиска, обработки и вывода результатов. Задача Web-администратора — содействовать команде разработчиков в настройке параметров и публикации созданных Web-страниц.

**Табл. 9-1.** Основные конфигурационные параметры службы Indexing Service

Параметр	Задаёт	Пример значения для IDQ
CiCatalog	Расположение каталога, в котором будет осуществляться поиск. Если параметр опущен, Indexing Service ищет каталог по умолчанию в папке Inetpub.	CiCatalog = D:\Catalogs\WWW
CiFlags	Флаги поиска для запроса. Флаг DEEP указывает службе Indexing Service, просмотреть все вложенные папки в пределах текущей области.	CiFlags = DEEP
CiMaxRecords-InResultSet	Максимальное число записей, возвращаемых в наборе результатов	CiMaxRecords-InResultSet = 100
CiMaxRecords-PerPage	Максимальное число записей, возвращаемых на одной странице.	CiMaxRecords-PerPage = 20

Табл. 9-1. (продолжение)

Параметр	Задаёт	Пример значения для IDQ
CiRestriction	Хранит параметры поиска, заданные пользователем, в той же форме, в какой они были переданы из формы запроса.	CiRestriction = %CiRestriction%
CiScore	Область действия запроса в пределах каталога. Если параметру присвоено значение «/», поиск начинается с вершины (или корня) дерева документов.	CiScore = /Docs

## Основы администрирования службы Indexing Service

Рассмотрим основные методы управления Indexing Service.

### Назначение индексируемых Web-ресурсов

Сконфигурировать индексируемые Web-ресурсы можно из оснастки Internet Information Services. Параметры индексирования могут быть глобальными или локальными. Первые распространяются на все наследующие их Web-узлы IIS, т. е. применяются ко всем файлам на всех узлах и во всех вложенных папках. Чтобы задать глобальные параметры индексирования, сделайте следующее.

1. В оснастке IIS щелкните правой кнопкой узел Internet Information Services нужного компьютера и выберите в контекстном меню команду Properties (Свойства).
2. В группе Master Properties (Основные свойства) щелкните Edit (Изменить), а затем перейдите на вкладку Note Directory (Домашний каталог).
3. Чтобы включить индексирование всех Web-узлов на сервере, пометьте флажок Index This Resource и щелкните ОК. Параметры индексирования автоматически наследуются всеми Web-узлами. Кроме того, они автоматически распространяются на все внутренние ссылки Web-узлов.
4. Чтобы отключить индексирование всех Web-узлов на сервере, снимите флажок Index This Resource (Индексация каталога) и щелкните ОК. Прежде чем применить задан-

ные значения, IIS проверяет текущие параметры всех Web-узлов. Если на Web-узле используются другие значения, открывается диалоговое окно **Inheritance Overrides** (Изменение наследования). Отметьте в нем узлы, к которым следует применить новые значения, и щелкните ОК.

Локально заданные параметры распространяются на отдельные Web-узлы и папки. В случае с Web-узлом корневая и все связанные с узлом папки автоматически наследуют параметры индексирования узла, т. е. данные параметры используются всеми индексируемыми файлами в этих папках. Все вложенные папки наследуют параметры индексирования корневой для них папки, т. е. данные параметры используются всеми индексируемыми файлами в этих папках.

Параметры индексирования отдельного Web-узла или папки настраиваются так.

1. В оснастке IIS щелкните **правой** кнопкой нужный Web-узел или **нужную папку** и выберите в контекстном меню команду **Properties**.
2. Перейдите на соответствующую вкладку: Home Directory (Домашний каталог), Directory (Каталог) или Virtual Directory (Виртуальный каталог).
3. Чтобы включить индексирование текущего ресурса и всех его подкаталогов, пометьте флажок **Index This Resource** (Индексирование каталога) и щелкните ОК.
4. Чтобы отключить индексирование текущего ресурса и всех его подкаталогов, снимите флажок **Index This Resource** и щелкните ОК. Параметры индексирования наследуются автоматически.

### Создание и просмотр каталогов

Создание каталогов и управление ими осуществляется на уровне узла. У каждого узла, который требуется проиндексировать, должен быть собственный каталог. Узел также может обладать несколькими каталогами. Например, можно создать один каталог для индексов рабочих папок, а другой — для индексов папок служб.

Каталоги следует создавать в локальной файловой системе и помещать в отдельной от других каталогов папке. Чтобы упростить управление несколькими каталогами, создайте

корневую папку с именем Catalogs, а затем в ней — вложенные папки для всех необходимых каталогов. Папку каталога надо создать до создания каталога.

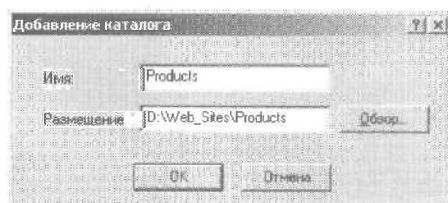
Чтобы создать каталог для узла сделайте следующее.

1. Запустите оснастку Computer Management (Управление компьютером) и раскройте узел Services and Applications (Службы и приложения).



**Примечание** При первом запуске оснастки Computer Management автоматически подключается к локальному компьютеру. Для подключения к другому компьютеру щелкните узел Computer Management (Управление компьютером) правой кнопкой, выберите в контекстном меню команду Connect To Another Computer (Подключиться к другому компьютеру) и следуйте инструкциям на экране. Помните: вы не сможете добавить каталог на удаленном компьютере, если на нем отключен установленный по умолчанию доступ администратора к ресурсам.

2. Щелкнув правой кнопкой узел Indexing Service (Служба индексирования), выберите в контекстном меню команду New\Catalog (Создать\Каталог). Откроется диалоговое окно Add Catalog (Добавление каталога) (рис. 9-2).



**Рис. 9-2.** Диалоговое окно Add Catalog (Добавление каталога)

3. В поле Name (Имя) введите название каталога.
4. В поле Location (Размещение) укажите полный путь к папке каталога. Кроме того, можете щелкнуть кнопку Browse (Обзор) и выбрать папку, и которой будет создан каталог.
5. Щелкните ОК. Закройте и перезапустите Indexing Service, чтобы она поместила в каталог соответствующие индексы.

### Просмотр состояния индексирования

Для поддержки каталогов администраторам следует периодически вести мониторинг индексирования, в том числе отслеживать состояние индексирования. Это значение отражает текущее состояние «ядра» индексирования. Возможны следующие варианты.

- **(Пусто)** — служба Indexing Service остановлена, и ее следует перезапустить для возобновления индексирования.
- **Indexing Paused (High I/O) (Индексирование приостановлено, высокая загрузка ввода-вывода)** — индексирование приостановлено из-за большого числа операций ввода-вывода. Чтобы снизить активность дискового ввода-вывода, закройте какие-нибудь приложения.
- **Indexing Paused (Low Memory) (Индексирование приостановлено, недостаточно памяти)** — индексирование приостановлено из-за нехватки виртуальной памяти. Чтобы увеличить объем доступной памяти, закройте какие-нибудь приложения.
- **Indexing Paused (Power Management) (Индексирование приостановлено, управление питанием)** — индексирование приостановлено в целях экономии заряда аккумуляторных батарей. Обычно данное состояние отображается только на ноутбуках.
- **Indexing Paused (User Active) (Индексирование приостановлено, действия пользователя)** — индексирование приостановлено, чтобы не мешать работе пользователя. Возможно, пользователь открыл большое число подлежащих индексированию файлов, или администратор изменяет конфигурацию службы Indexing Service из оснастки Computer Management.
- **Master Merge (Paused) (Основное слияние, приостановлено)** — полное слияние приостановлено из-за нехватки ресурсов. Возможно, мало доступной памяти, свободного места на диске или низка производительность системы.
- **Merge (Слияние)** — идет слияние — ресурсоемкий процесс, способный временно снизить производительность системы.
- **Query Only (Только запрос)** — служба Indexing Service запущена, но доступна только для запросов.

- **Recovering (Восстановление)** — служба Indexing Service восстанавливает каталог после аварийного завершения работы.
- **Scan Required (Требуется сканирование)** — в папках этого каталога изменены или добавлены один или несколько документов. Служба индексирования должна автоматически выполнить сканирование каталога. Если этого не произойдет, проверьте журнал событий Windows.
- **Scanning (Сканирование)** — одна или несколько папок сканируются на предмет наличия новых или измененных документов.
- **Scanning (NTFS) (Сканирование, NTFS)** - один или несколько томов NTFS сканируются на предмет обнаружения новых или измененных документов.
- **Started (Работает)** — служба Indexing Service для этого каталога запущена.
- **Starting (Запуск)** — служба Indexing Service запускается.
- **Stopped (Остановлено)** — служба Indexing Service для этого каталога остановлена.

Если пользователь не получает результатов поиска, возможно, что Indexing Service приостановлена, или остановлена полностью, или выполняется слияние, или каталоги сканируются повторно. Обычное состояние индексирования — **Started (Работает)**. Ключевое слово **Started** указывает на состояние самой службы Indexing Service. В данном случае служба запущена.

Состояние Indexing Service можно посмотреть.

1. Запустите оснастку Computer Management (Управление компьютером) и раскройте узел **Services and Applications (Службы и приложения)**.
2. В левой части окна выберите узел службы Indexing Service (Служба индексирования). В правой части отобразятся сведения о состоянии индексирования отдельных каталогов. Помните, что состояние индексирования каталогов может различаться.

### Запуск, остановка и приостановка службы Indexing Service

Как и любую другую службу, Indexing Service можно запускать, останавливать и приостанавливать. Выполнение запросов и получение их результатов возможно только при запущенной службе. Если служба остановлена или приостановлена, результаты запроса не будут получены.

Для управления Indexing Service сделайте следующее.

1. Запустите оснастку Computer Management и раскройте узел Services and Applications.
2. В левой части окна выберите узел службы Indexing Service. В правой части отобразятся сведения о состоянии индексирования отдельных каталогов. Помните, что состояние индексирования каталогов может различаться.
3. В левой части окна щелкните узел Indexing Service правой кнопкой и выберите из контекстного меню команду:
  - Start (Пуск) — чтобы запустить службу Indexing Service.
  - Stop (Стоп) — чтобы остановить службу Indexing Service.
  - Pause (Приостановить) — чтобы приостановить службу Indexing Service. Для возобновления работы службы Indexing Service щелкните Start.



**Примечание** При остановке и перезапуске индексирования Indexing Service проводит выборочное сканирование всех каталогов, связанных с узлами сервера.

### Настройка свойств службы Indexing Service

Indexing Service имеет несколько свойств, позволяющих управлять ее работой.

- **Index Files With Unknown Extensions (Индексировать файлы с неизвестными расширениями)** указывает, индексировать ли служба Indexing Service файлы с незарегистрированными расширениями. По умолчанию такие файлы индексируются, и это, если их много, может замедлить процесс.
- **Generate Abstracts (Генерировать аннотации)** указывает, генерирует и выводит ли Indexing Service в результатах поиска аннотации для найденных файлов. Аннотация



содержит ключевую информацию, извлеченную из документа, соответствующего параметрам поиска. По умолчанию генерация аннотаций включена.

- **Maximum Size (Максимальный размер)** задает максимальный размер (в символах) выводимой в результатах поиска аннотации. По умолчанию — 320. Диапазон допустимых значений — от 10 до 10 000. Свойство доступно лишь при помеченном флажке Generate Abstracts.
- **Add Network Share Alias Automatically (Добавлять псевдонимы папок общего доступа автоматически)** указывает Indexing Service автоматически задействовать имена совместно используемых сетевых ресурсов в качестве их псевдонимов. Если флажок снят, требуется вручную задать псевдоним для каждого индексируемого сетевого ресурса (см. раздел «Добавление папок в каталог» этой главы).

Первые три свойства вы найдете на вкладке Generation (Генерация), последнее — на вкладке Tracking (Слежение). Как и большинство других параметров службы Indexing Service, эти свойства можно задавать глобально или локально. Глобальные параметры наследуются всеми каталогами, для которых они не переопределены.

Настраиваются глобальные свойства так.

1. Запустите оснастку Computer Management (Управление компьютером) и раскройте узел Services and Applications (Службы и приложения).
2. Щелкните узел службы Indexing Service (Служба индексирования) правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
3. Свойства на вкладке Generation (Генерация) управляют обработкой результатов поиска и индексированием. Пометьте или сбросьте соответствующие флажки.
4. Свойства на вкладке Tracking (Слежение) позволяют следить за сетевыми ресурсами. Пометьте или сбросьте соответствующие флажки.
5. Щелкните ОК. Чтобы обеспечить наследование глобальных свойств каталогами, проверьте свойства каждого и убедитесь, что на вкладках Generation и Tracking помс-

чсн флажок **Inherit Above Settings From Service** (Наследовать вышеуказанные параметры из службы).

Для отдельных каталогов можно разрешить наследование глобальных свойств или переопределить их.

1. Запустите оснастку **Computer Management** и раскройте узел **Services and Applications**, а затем — узел службы **Indexing Service**. Появится список сконфигурированных на сервере каталогов.
2. Щелкните соответствующий каталог правой кнопкой и выберите в контекстном меню команду **Properties**.
3. Свойства на вкладке **Generation** управляют обработкой результатов поиска и индексированием. Чтобы обеспечить наследование этих свойств каталогами, пометьте флажок **Inherit Above Settings From Service**. Либо снимите флажок и измените свойства службы в соответствии со своими требованиями.
4. Свойства на вкладке **Tracking** позволяют следить за сетевыми ресурсами. Чтобы обеспечить наследование этих свойств каталогами, пометьте флажок **Inherit Above Settings From Service**. Либо снимите флажок и измените свойства службы в соответствии со своими требованиями.
5. Щелкните **OK**.

### Оптимизация производительности Indexing Service

Для оптимизации производительности службы **Indexing Service** следует настроить процессы индексирования и обработки запросов в соответствии с предполагаемой нагрузкой. Перечислю возможные режимы индексирования.

- **Lazy** (Отложенное) — для индексирования используется минимум системных ресурсов, **Indexing Service** с задержкой реагирует на генерируемые ОС уведомления об изменениях, в результате чего увеличивается периодичность сканирования. Режим лучше всего подходит для сред с нечастым изменением или обновлением документов.
- **Moderate** (Обычное) — служба **Indexing Service** использует для индексирования обычное количество системных ресурсов и пытается своевременно обрабатывать уведомления об изменениях. Режим используется по умолчанию.

и лучше всего подходит для стандартных сред с ежедневным изменением индексируемых документов.

- **Instant (Немедленное)** — Indexing Service резервирует для индексирования дополнительные системные ресурсы и активно реагирует на уведомления об изменениях, т. е. сканирование на предмет выявления новых и измененных документов проводится гораздо чаще. В результате изменения и дополнения документов быстро отражаются в каталогах. Режим лучше всего подходит для сред, в которых документы быстро меняются и эти изменения нужно отражать в результатах поиска.

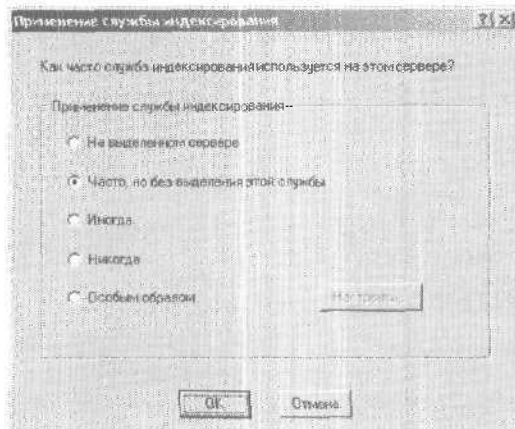
Indexing Service может обрабатывать запросы с разной скоростью.

- **Low Load (Низкая)** — количество системных ресурсов для обработки запросов минимизировано, в связи с чем параллельно может выполняться ограниченное число запросов. Режим лучше всего подходит для сред с нечастыми запросами. При резком увеличении числа запросов скорость реакции службы сильно снизится.
- **Moderate Load (Средняя)** — резервируется обычное количество системных ресурсов, пытается параллельно обрабатывается несколько запросов. Режим используется по умолчанию и лучше всего подходит для стандартных сред, где пользователи регулярно выполняют запросы, требующие должной обработки.
- **Heavy Load (Высокая)** — для обработки запросов используются дополнительные системные ресурсы, обрабатывается гораздо больше параллельных запросов. Режим лучше всего подходит для сред с мощным оборудованием, в которых требуется обрабатывать много запросов.

Для оптимизации производительности Indexing Service сделайте следующее.

1. Запустите оснастку Computer Management и раскройте узел Services and Applications.
2. В левой части окна щелкните узел службы Indexing Service. В правой части отобразится текущее состояние каждого каталога.

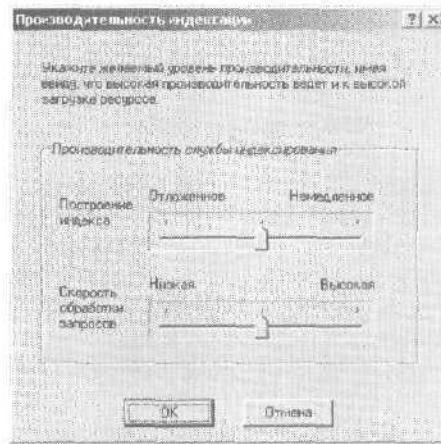
3. В левой части окна щелкните узел службы Indexing Service правой кнопкой и выберите в контекстном меню команду Stop.
4. Еще раз щелкните узел службы Indexing Service правой кнопкой и выберите в контекстном меню команду AI Tasks\Tune Performance (Все задачи\Настройка производительности). Откроется диалоговое окно Indexing Service Usage (Применение службы индексирования) (рис. 9-3).



**Рис. 9-3.** Диалоговое окно Indexing Service Usage (Применение службы индексирования)

5. Можно выбрать фиксированные или задать собственные параметры оптимизации. Для выбора фиксированных значений щелкните в диалоговом окне Indexing Service Usage один из следующих переключателей:
  - **Dedicated Server (На выделенном сервере)** задает режим индексирования Instant и режим обработки запросов Heavy load;
  - **Used Often, But Not Dedicated To This Service (Часто, но без выделения этой службы)** задает режим индексирования Instant и режим обработки запросов Moderate load;
  - **Used Occasionally (Иногда)** задает режим индексирования Lazy и режим обработки запросов Low load;

- **Never Used (Никогда)** — отключает Indexing Service (как если бы вы отключили ее в узле Applications and Services); служба будет остановлена до тех пор, пока вы не запустите ее вручную.
6. Чтобы задать собственные параметры оптимизации, щелкните переключатель Customize (Особым образом), а затем — кнопку Customize (Настроить) (рис. 9-4):
    - с помощью ползунка Indexing (Построение индекса) выберите режим индексирования Lazy (Отложенное), Moderate (Обычное) или Instant (Немедленное); среднему положению соответствует обозначенный на шкале режим Moderate;
    - с помощью ползунка Querying (Скорость обработки запросов) выберите режим обработки запросов Low Load (Низкая), Moderate Load (Средняя) или Heavy Load (Высокая); среднему положению соответствует обозначенный на шкале режим Moderate.



**Рис. 9-4.** Диалоговое окно Desired Performance (Производительность индексации)

7. Чтобы сохранить заданные параметры и вернуться к настройке Computer Management, дважды щелкните OK.

## Управление каталогами

Indexing Service хранит всю индексируемую информацию в каталогах. Там находятся извлеченное из основного текста документов содержимое, а также метаданные, описывающие документ и его свойства. При создании каталог сопоставляется одному из Web-узлов. После создания каталога для Web-узла пользователи могут осуществлять в нем поиск при помощи специальной формы на основе браузера.

Каталоги автоматически поддерживаются Indexing Service и обновляются посредством сканирования и слияния. Управляют каталогом вручную, а также путем запуска, остановки и приостановки монитора обновлений каталога. Кроме того, можно провести принудительное слияние отдельных индексов в основной индекс, тем самым повысив общую производительность и ускорив реакцию Indexing Service.

### Просмотр параметров каталога и индексируемых папок

Каждый сконфигурированный на сервере каталог обладает набором свойств, позволяющим управлять мониторингом сетевых ресурсов, созданием аннотаций документов, и настройкой индексирования. Каталог может использовать собственные параметры или наследовать глобальные параметры Indexing Service.

Вы вправе связать каталоги с Web-узлом, NNTP-узлом, а также с одной или несколькими внешними папками. К внешним папкам относятся как локальные, так и удаленные ресурсы. При сопоставлении каталога Web- или NNTP-узлу нужно из оснастки IIS указать индексируемые ресурсы. При связывании каталога с сетевым ресурсом можно указать, что после добавления в каталог папка должна быть проиндексирована.

Для просмотра текущих параметров каталога или индексируемой в данный момент папки сделайте следующее.

1. Запустите оснастку Computer Management (Управление компьютером) и раскройте узел Services and Applications (Службы и приложения), а затем — узел службы Indexing Service (Служба индексирования).
2. Появится список сконфигурированных на сервере каталогов. Раскройте узел какого-нибудь каталога. В левой

части окна щелкните узел Directories (Папки) — отобразится список внешних папок, связанных с выбранным в правой части каталогом.

3. Чтобы просмотреть свойства каталога, щелкните его значок правой кнопкой и выберите в контекстном меню команду Properties (Свойства). Откроется одноименное диалоговое окно, в котором можно задавать и просматривать параметры каталога,

### Добавление в каталог физических папок

В каталог можно добавлять внешние папки, которые будут индексироваться вместе с содержимым Web- или NNTP-узла. Эти внешние папки могут находиться как на локальном, так и на удаленном компьютере. Если флажок Add Network Share Alias Automatically (Добавлять псевдонимы папок общего доступа автоматически) снят, вам потребуется вручную задать псевдонимы для всех индексируемых сетевых ресурсов.

Внешняя папка в каталог добавляется так.

1. Запустите оснастку Computer Management (Управление компьютером) и раскройте узел Services and Applications (Службы и приложения), а затем — узел службы Indexing Service (Служба индексирования). Появится список имеющихся на сервере каталогов.
2. Щелкните нужный каталог правой кнопкой и выберите в контекстном меню команду New\Directory (Создать\Каталог). Откроется диалоговое окно Add Directory (Добавление папки) (рис. 9-5).

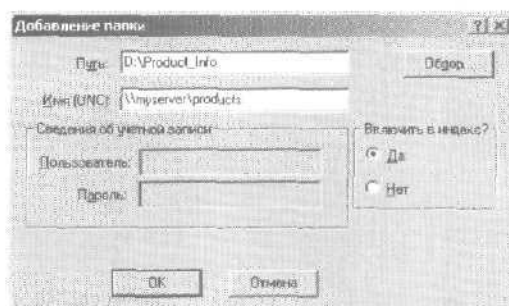



Рис. 9-5. Диалоговое окно Add Directory (Добавление папки)

3. В поле Path (Путь) введите полный путь к папке, которую хотите проиндексировать. Если путь неизвестен, щелкните Browse и выберите нужную папку.
  4. При настройке индексирования сетевой папки в поле Alias (UNC) [Имя (UNC)] диалогового окна Add Directory можно указать псевдоним, который будет использоваться для нее. Псевдоним должен соответствовать UNC-формату (Uniform Naming Convention, универсальные правила именования) и будет возвращаться в составе результатов поиска клиентам. Например, можно сопоставить псевдоним \\myserver\data существующему сетевому ресурсу \\Galileo\reports\fy2001.
-  **Совет** При работе с удаленными системами разрешите Indexing Service подключать административные ресурсы, иначе она не сможет индексировать содержимое.
5. Если вы настраиваете индексирование сетевого ресурса, можете задать имя пользователя и пароль, которые Indexing Service будет использовать для аутентификации в удаленной системе.
  6. Затем поставьте переключатель в положение Yes (Да), чтобы указать, что папку следует включить в индекс каталога. Положение No (Нет) исключает папку из индекса.
  7. Щелкните ОК.

#### **Принудительное полное и выборочное повторное сканирование папок**

Для контроля за модификацией файлов в индексируемых каталогах Indexing Service следит за уведомлениями об изменениях, генерируемыми ОС. Получив запрос, служба ставит соответствующую папку в очередь на выборочное сканирование. Иногда Indexing Service теряет уведомления об изменениях — причиной может стать большое число операций дискового ввода-вывода или загруженность центрального процессора. Это также случается, если Indexing Service не получает уведомления об изменениях для папок на удаленных системах.

Обычно для выявления проблем со сканированием достаточно попытаться найти в индексируемой папке недавно добавленные или обновленные документы. Если в результатах



поиска нет ссылок на эти документы, вам, вероятно, потребуется провести принудительное полное или выборочное повторное сканирование. Сделать это можно только на уровне внешних папок.

Для принудительного повторного сканирования внешней папки сделайте следующее.

1. Запустите оснастку Computer Management (Управление компьютером) и раскройте узел Services and Applications (Службы и приложения), а затем — узел службы Indexing Service (Служба индексирования). Появится список сконфигурированных на сервере каталогов.
2. Дважды щелкните нужный каталог и затем выберите связанный с ним узел Directories (Папки).
3. В правой части окна отобразится список включенных в каталог внешних папок. Щелкните нужную папку правой кнопкой и выберите в контекстном меню команду All Tasks\Rescan (Full) [Повторное сканирование (полное)] или All Tasks\Rescan (Incremental) [Повторное сканирование (добавочное)].
4. При запросах системы подтверждайте свои действия, щелкая Yes. Помните, что повторное сканирование папок с большим количеством документов может быть ресурсоемким, т. е. требовать дополнительных ресурсов процессора, памяти, и подсистемы файлового ввода-вывода.

### Запуск, остановка и приостановка отдельных каталогов

Для выполнения большого числа обновлений в индексируемых папках лучше временно остановить или приостановить каталог. Это укажет Indexing Service, что она не должна обрабатывать уведомления об изменениях для данного каталога. Важно понимать разницу между остановкой и приостановкой каталога. В первом случае служба прекращает обработку запросов и индексирование, т. е. соответствующие папки больше не индексируются и пользователи не могут осуществлять поиск по каталогу. Во втором — прекращает индексирование, но позволяет завершить обработку текущих запросов.

Для запуска, остановки или приостановки каталога требуется следующее.

1. Запустите оснастку Computer Management и раскройте узел Services and Applications, а затем — узел службы Indexing Service.
2. Щелкните нужный каталог правой кнопкой и выберите в контекстном меню команду All Tasks\Start (Все задачи\Пуск), All Tasks\Pause (Все задачи\Приостановить) или All Tasks\Stop (Все задачи\Стоп).



**Примечание** При остановке и последующем перезапуске каталога Indexing Service автоматически проводит выборочное сканирование. Это обеспечивает индексирование измененных и обновленных документов.

### Слияние каталогов

При обновлении каталога Indexing Service создает временные индексы, дополняющие основной. Эти индексы отражают изменения внутри папок каталога. В процессе работы число временных индексов может возрасти, это отражает число сохраненных индексов, связанных с каталогом. Так как временные индексы содержат дополнительные указатели и информацию, они занимают больше места, чем полностью построенный основной индекс. По мере возрастания количества временных индексов выполнение запросов к каталогу может замедлиться.

Вы можете ускорить реакцию Indexing Service и занимаемый временными индексами объем дискового пространства, объединив временные индексы с основным.

1. Запустите оснастку Computer Management (Управление компьютером) и раскройте узел Services and Applications (Службы и приложения), а затем — узел службы Indexing Service (Служба индексирования).
2. Щелкните правой кнопкой нужный каталог и выберите в контекстном меню All Tasks Merge (Все задачи | Слияние).
3. При необходимости подтвердите свои действия, щелкнув Yes (Да).

Как и в случае сканирования, процесс слияния может оказаться ресурсоемким, а скорость реакции Indexing Service временно снизится. И все же после завершения процесса слияния реакция Indexing Service на запросы пользователей ускорится.

**Включение в каталоги Web- или NNTP-узлов**

Каждый каталог можно сопоставить одному Web- и одному NNTP-узлу. Воспользуйтесь оснасткой IIS и укажите индексируемые ресурсы.

1. Запустите оснастку Computer Management и раскройте узел Services and Applications, а затем — узел службы Indexing Service.
2. Щелкните нужный каталог правой кнопкой и выберите в контекстном меню команду Properties (Свойства). Перейдите на вкладку Tracking (Слежение) (рис. 9-6) и затем:
  - из списка WWW Server (WWW-сервер) выберите Web-узел, который хотите сопоставить каталогу;
  - из списка NNTP Server (NNTP-сервер) выберите NNTP-узел, который хотите сопоставить каталогу.

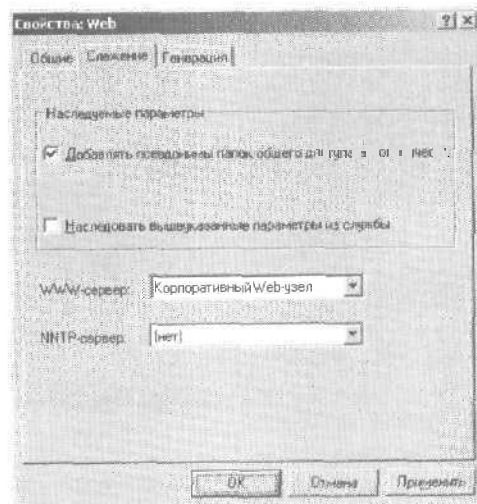


Рис. 9-6. Включение в каталог Web- и NNTP-узла

3. Щелкните OK.

**Тестирование каталогов с помощью запросов**

Настроив каталог для индексирования, выполните к нему несколько запросов, дабы убедиться в правильности полу-

## Производительность, оптимизация и поддержка

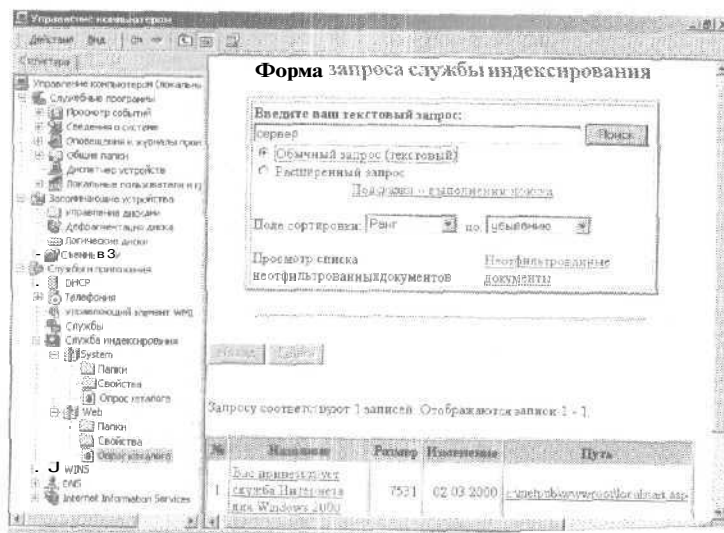
В четвертой части этой книги рассказывается об основных задачах оптимизации и поддержки Internet Information Services. Глава 10 посвящена мониторингу IIS и устранению проблем производительности, связанных с ОС и конфигурацией оборудования. В главе 11 обсуждаются журналы доступа и конфигурирование журналов сервера. В главе 12 рассматривается оптимизация IIS. Вы научитесь изменять параметры реестра, связанные с IIS, а также работать с метабазой IIS.

Обсуждаемые здесь вопросы очень важны для успешной работы. Зачастую администраторы забывают, что IIS — это набор служб, требующих постоянного мониторинга, обновления и обслуживания. Кроме того, серверы следует оптимизировать с учетом текущей нагрузки и распределения ресурсов. В против-

ченных результатов. В Indexing Service имеется предназначенная для этого встроенная форма запросов (рис. 9-7).

Чтобы открыть ее и выполнить запрос к каталогу, сделайте следующее.

1. Запустите оснастку Computer Management (Управление компьютером) и раскройте узел Services and Applications (Службы и приложения), а затем — узел Indexing Service (Служба индексирования).
2. Появится список сконфигурированных на сервере каталогов. Дважды щелкните нужный каталог и затем в правой части окна — значок Query The Catalog (Опрос каталога).
3. Введите текст запроса в поле Enter Your Free Text Query Below (Введите ваш текстовый запрос), а затем щелкните Search (Поиск). Если индексирование настроено правильно, Indexing Service отобразит результаты поиска. Щелкните название или путь к документу и убедитесь, что документ можно открыть со страницы результатов поиска. При возникновении каких-либо проблем проверьте параметры индексирования.



## Глава 10

# Мониторинг и настройка производительности

Мониторинг и настройка производительности — неотъемлемые части Web-администрирования. Мониторинг гарантирует безотказную работу серверов и позволяет устранять проблемы по мере их возникновения. Оптимизация производительности сервера связана с текущим объемом свободных ресурсов и объемом трафика. В Microsoft Windows 2000 имеется несколько утилит для мониторинга Internet Information Services, включая Performance Monitor, журналы событий Windows и журналы доступа IIS. Результаты мониторинга зачастую используются для оптимизации Internet Information Services.

Настройка производительности — это и искусство, и наука. Нередко при настройке применяется метод проб и ошибок: изменяются конфигурационные параметры сервера, замеряется достигнутый уровень производительности, а затем оцениваются изменения. Если уровень производительности не

### Зачем проводит мониторинг IIS?

Одна из основных причин мониторинга — устранение проблем производительности. Например, в случае проблем с подключением к серверу мониторинг позволяет выявить и устранить их источник.

Другая распространенная причина мониторинга IIS — повышение производительности сервера на основе полученных результатов. Это позволяет снизить потребность в дополнительных дорогостоящих серверах и комплектующих, например процессорах и памяти. Так что, когда вам понадобится приобрести новые серверы и комплектующие, вы сможете получить дополнительную отдачу от оборудования и бюджета.

Для достижения оптимальной производительности нужно выявить узкие места, максимизировать пропускную способность и минимизировать время обработки пользовательских запросов Web-приложениями. Вы должны заниматься следующим.

- Наблюдать за использованием памяти и процессора и предпринимать соответствующие меры для снижения загрузки сервера. Выполняющиеся на сервере процессы могут занимать ресурсы процессора и памяти, необходимые IIS. Для решения этой проблемы остановите второстепенные службы и перенесите вспомогательные приложения на другой сервер.
- Устранять проблемы с оборудованием. Если файлы с жесткого диска читаются медленно, попробуйте повысить пропускную способность дискового ввода-вывода. Если сетевые платы работают на полную мощность, установите дополнительные платы для выполнения ресурсоемких операций, например архивации.
- Оптимизировать Web-страницы и IIS-приложения. Протестируйте Web-страницы и IIS-приложения и убедитесь, что исходный код работает нормально. Удалите ненужные процедуры и оптимизируйте неэффективные процессы.

К сожалению, в случае с использованием ресурсов зачастую приходится идти на компромисс. Так, для повышения производительности сервера при увеличении числа обращающихся к нему пользователей следует искать не способы сни-

жения загруженности сети, а способы оптимизации Web-страниц и IIS-приложений.

### Подготовка к мониторингу IIS

Прежде всего, нужно определить базовый уровень производительности сервера. После этого замерьте производительность сервера в разное время и при разной нагрузке и сравните полученные результаты с базовым уровнем. Параметры производительности, значения которых сильно превышают базовый уровень, указывают на области, требующие оптимизации и настройки.

Определив базовый уровень производительности, составьте план мониторинга:

1. Решите, мониторинг каких ресурсов сервера позволит собрать сведения, необходимые для достижения поставленной цели.
2. Сконфигурируйте фильтры для уменьшения объема собираемой информации.
3. Сконфигурируйте счетчики производительности для мониторинга использования ресурсов.
4. Занесите данные мониторинга в журнал для последующего анализа.
5. Проанализируйте полученные данные и при необходимости воспроизведите их, чтобы найти решение проблемы.

Подробнее об этом см. раздел «Мониторинг производительности IIS» этой главы. План мониторинга следует составлять в большинстве случаев. И все же иногда он не обязательно будет включать все вышеперечисленные пункты.

### Средства мониторинга IIS

Основные средства мониторинга IIS таковы.

- **Системный монитор (Performance Monitor).** Здесь можно сконфигурировать счетчики для повременного наблюдения за использованием ресурсов. Полученная информация позволит оценить производительность IIS и выявить области, требующие оптимизации.
- **Журналы доступа (Access logs).** Информация из журналов доступа позволяет выявить проблемы со страницами, приложениями и IIS. На потенциальные проблемы

указывают записи, код состояния которых начинается с цифры 4 или 5.

- **Журналы событий (Event Logs).** Информация из журналов событий способствует устранению проблем уровня системы, включая проблемы с IIS и Indexing Service (Служба индексации).

Кроме того, в Microsoft Windows 2000 Resource Kit имеются дополнительные утилиты мониторинга.

- **HTTP Monitoring Tool** следит за HTTP-активностью сервера и записывает собранные сведения в файл или журнал событий Windows. Эта информация позволит вовремя выявить изменения HTTP-активности. Кроме того, файл вывода HTTP Monitoring Tool можно импортировать напрямую в Microsoft SQL Server.
- **Playback** состоит из двух компонентов: RECORDER.DLL и PLAYBACK.EXE. Первая утилита записывает текущую активность Web-узла, вторая позволяет позже воспроизвести ее для эмуляции реального трафика на производственных и тестовых серверах.
- **Web Application Stress Tool** имитирует Web-активность, позволяя оценить производительность сервера. Вы можете определять число пользователей, частоту и типы запросов. Web Application Stress Tool создает подробный отчет, включающий сведения о числе запросов, количестве ошибок, затраченном на обработку запросов времени и т. д.
- **Web Capacity Analysis Tool (WCAT)** тестирует различные конфигурации сервера и сети при помощи моделей рабочей нагрузки и содержимого, разработанных специально для нес. Изменив программную и аппаратную конфигурацию и повторно проведя тестирование, вы узнаете, как изменения повлияли на время реакции сервера.

## Выявление и устранение ошибок IIS

Службы IIS заносят сведения об ошибках в журналы доступа IIS и журналы событий Windows. Журналы доступа содержат данные об отсутствии ресурсов, ошибках проверки подлинности и внутренних ошибках сервера. В журналах событий содержится информация об ошибках IIS, ошибках IIS-

приложений и ошибках, связанных с другими выполняющимися на сервере приложениями.

### Просмотр журналов доступа

Если для Web-, FTP- и SMTP-узлов включено ведение журналов, создаются журналы доступа. При запросе клиентом файла с Web-узла в журнал заносится соответствующая запись. У всех записей имеется определенный код состояния, позволяющий определить успешность запроса. Код состояния неудачных запросов начинается с цифры 4 или 5.

Самая распространенная ошибка — 404 (ресурс не найден). Для ее устранения можно:

- поместить искомый файл по предполагаемому адресу;
- переименовать файл, если его имя не соответствует предполагаемому;
- изменить исходную ссылку и указать в ней правильные имя и расположение файла.

Журнал доступа определенного узла вы найдете так,

1. В оснастке Internet Information Services раскройте узел нужного компьютера. Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2 этой книги.
2. Щелкнув правой кнопкой нужный Web-, FTP- или SMTP-узел, выберите в контекстном меню команду Properties (Свойства).
3. В группе Enable Logging (Вести журнал) щелкните Properties (Свойства). Откроется диалоговое окно, подобное этому (рис. 10-1),
4. Поле Log File Directory (Каталог файла журнала) содержит имя корневой папки, в которой хранятся журналы данного узла. По умолчанию это %WinDir%\System32\LogFiles.
5. Поле Log File Name (Имя файла журнала) содержит имя вложенной папки и формат именования файлов журнала. Скажем, если имя файла журнала — \W3SVC1\EXYYMMDD.LOG (\W3SVC1\EXTГГММДД.LOG), журналы узла хранятся во вложенной папке W3SVC1. Теку-



ций журнал имеет самый последний временной штамп. Все остальные журналы являются архивными файлами, и их можно переместить в специальный каталог.

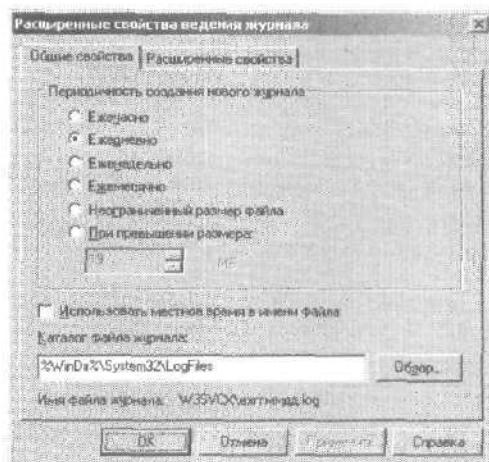


Рис. 10-1. Диалоговое окно Logging Properties (Свойства ведения журнала)

Зная, где находятся файлы журналов узла, можно искать в них записи о конкретных ошибках. Формат файлов журналов — ASCII, и поэтому их можно открыть в Microsoft Notepad (Блокнот) или другом текстовом редакторе и искать коды ошибок, например 404. Кроме того, можно искать коды ошибок с помощью команды FIND. Так, для поиска ошибок 404 во всех журналах текущей папки наберите в командной строке оператор:

```
find "404" *
```

Обнаружив отсутствующие файлы, устраните проблему одним из вышеперечисленных методов. Подробнее о журналах доступа и кодах состояния см. главу 11 этой книги.

### Просмотр журналов событий

Журналы событий содержат архивные сведения, позволяющие выявить проблемы со службами, процессами и приложениями. Отслеживаемые события определяются службой регистрации событий. После ее запуска события, связанные

с действиями пользователей и работой системных ресурсов, регистрируются в журналах:

- « **Application Log (Журнал приложений)** — события приложений, например IIS;
- **Directory Service** — события службы Active Directory и связанных с ней служб;
- **DNS Server** — события DNS-запросов, ответов и прочих DNS-операций;
- **File Replication Service (Служба репликации файлов)** — события, связанные с репликацией файлов в системе;
- **Security Log (Журнал безопасности)** — события, сконфигурированные для аудита в локальной или глобальной групповой политике; заметьте, что администраторам нужно предоставить доступ к журналам безопасности, назначив им соответствующие права;
- **System Log (Журнал системы)** — события ОС и ее компонентов, например, отказ при запуске службы.

Журналы событий можно просмотреть.

1. Раскрыв меню **Start\Programs\Administrative Tools (Пуск\Программы\Администрирование)**, выберите **Event Viewer (Просмотр событий)**. Запустится одноименное приложение.
2. По умолчанию Event Viewer отображает журналы локального компьютера. Чтобы просмотреть журналы удаленной машины, щелкните правой кнопкой в дереве консоли значок Event Viewer и выберите в контекстном меню команду **Connect To Another Computer (Подключиться к другому компьютеру)**. В диалоговом окне **Select Computer (Выбор компьютера)** введите имя нужного компьютера и щелкните **ОК**.
3. Выберите нужный журнал (рис. 10-2). Для определения источника события служит поле **Source (Источник)**.

В правой панели Event Viewer отображает краткие сведения о месте, времени и условиях возникновения события. Для просмотра подробной информации о событии дважды щелкните нужную запись. Перед датой и временем наступления события отображается его тип;

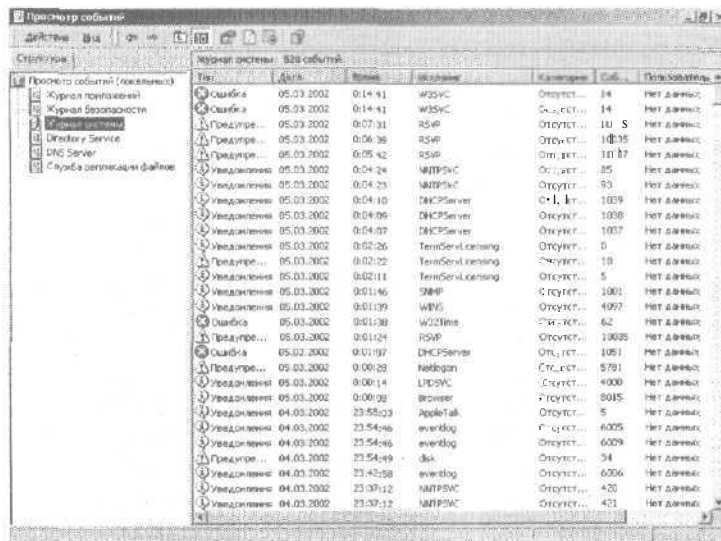


Рис. 10-2. Окно утилиты Event Viewer (Просмотр событий)

- **Information (Уведомление)** — событие, описывающее удачное завершение действия приложением;
- **Success Audit (Аудит успехов)** — событие, соответствующее успешно завершённому действию;
- **Failure Audit (Аудит отказов)** — событие, соответствующее неудачно завершённому действию;
- **Warning (Предупреждение)** — предупреждение; зачастую подробная информация предупреждения позволяет предотвратить системные проблемы;
- **Error (Ошибка)** — ошибка, например, сбой при запуске службы.



**Примечание** Всегда внимательно просматривайте предупреждения и ошибки. Если вы не уверены в причине их возникновения, дважды щелкните соответствующую запись и изучите подробное описание события.

Помимо типа, даты и времени, краткие и подробные описания содержат следующие сведения:

- **Source (Источник)** — приложение, служба или компонент, вызвавшие событие;
- **Category (Категория)** — категория события; обычно указывается как None, но иногда используется для подробного описания соответствующего события;
- **Event (Событие)** — идентификатор события;
- **User (Пользователь)** — учетная запись пользователя, зарегистрированного в системе при возникновении события (если осуществлялся вход в систему);
- **Computer (Компьютер)** — имя компьютера, на котором произошло событие;
- **Description (Описание)** — в подробном представлении: текстовое описание события;
- **Data (Данные)** — в подробном представлении: данные или код ошибки, выданные событием.

Источником событий могут быть:

- **Active Server Pages** — ASP-приложения и обработчики сценариев;
- **CERTSVC** — службы сертификации;
- **Si** — служба индексирования;
- **MSDTC** — координатор распределенных транзакций Microsoft;
- **MSFTPSVC** — служба FTP-публикаций;
- **NNTPSVC** - служба NNTP;
- **SMTPSVC** - служба SMTP;
- **W3SVC** — служба веб-публикаций.

Чтобы просматривать только предупреждения и ошибки, создайте фильтр.

1. В меню View (Вид) выберите команду Filter (Фильтр). Откроется диалоговое окно (рис. 10-3).
2. Снимите флажки Information (Уведомления), Success Audit (Аудит успехов) и Failure Audit (Аудит отказов).
3. Поставьте флажки Warnings (Предупреждения) и Errors (Ошибки).

4. Щелкните ОК. Будут отображаться только предупреждения и ошибки. Внимательно изучив их, примите меры по устранению имеющихся проблем.

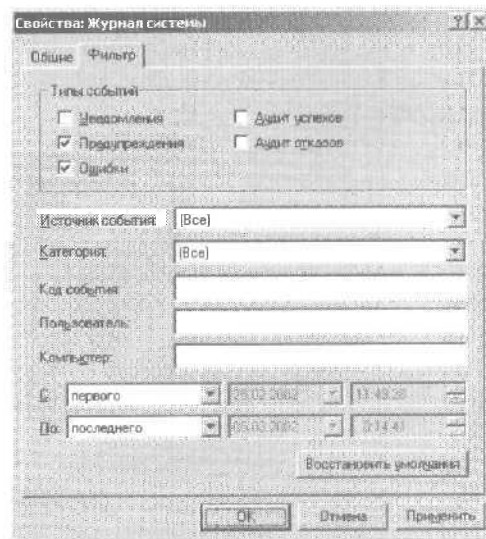


Рис. 10-3. Фильтрация событий для вывода предупреждений и ошибок

## Мониторинг производительности IIS

Осуществляется с помощью утилиты Performance Monitor (Системный монитор), графически представляющей статистику для выбранных вами параметров (счетчиков). При установке ITS в Performance Monitor добавляются счетчики для мониторинга производительности IIS. Кроме того, новые счетчики добавляются при установке дополнительных служб и компонентов IIS.

Performance Monitor (Системный монитор) строит график на основе информации наблюдаемых счетчиков. Интервал обновления графика может изменяться и по умолчанию равен 1 секунде. Самое полезное применение Performance Monitor — запись сведений о производительности в журнал и последующее их воспроизведение. Кроме того, утилита позволяет создать оповещения для отсылки сообщений при

наступлении определенного события, например, автоматического перезапуска IIS.

Ниже обсуждаются основные методы работы с Performance Monitor. Для запуска Performance Monitor выберите в меню Administrative Tools (Администрирование) команду Performance Monitor (Системный монитор).

#### Отбор наблюдаемых счетчиков

Performance Monitor выводит данные только наблюдаемых счетчиков. Если установлены все службы IIS, в системе будет доступно более сотни соответствующих счетчиков. Счетчики сгруппированы в объекты. Так, все счетчики, связанные с ASP, относятся к объекту Active Server Pages (Страницы Active Server). Кроме того, имеются объекты счетчиков и для других служб, включая:

- **Active Server Pages** (Страницы Active Server) — счетчики ASP-сценариев и приложений, выполняющихся на сервере;
- **FTP Service** (Служба FTP) — счетчики службы FTP;
- **HTTP Indexing Service** (Служба индексирования HTTP) — счетчики Службы индексирования, связанные с Web-узлами, активными запросами и результатами кэширования;
- **Indexing Service** (Служба индексирования) — счетчики Службы индексирования;
- **Indexing Service Filter** (Фильтр службы индексирования) — счетчики производительности и скорости индексирования содержимого фильтрами;
- **Internet Information Services Global** (Общий объект служб IIS) — счетчики всех служб Интернета (WWW, FTP, SMTP, NNTP и т. д.), выполняющихся на сервере.
- **NNTP Commands** (Команды протокола NNTP) — счетчики NNTP-команд, выполняемых пользователями на сервере;
- **NNTP Server** (NNTP-сервер) — счетчики для мониторинга общей производительности NNTP, например, числа отправленных/принятых/переданных статей в секунду;

- **SMTP NTFS Store Driver** (Драйвер SMTP NTFS Store) - счетчики для мониторинга общего числа сообщений и потоков сообщений;
- **SMTP Server** (SMTP-сервер) — счетчики для мониторинга общей производительности SMTP, например, числа отправленных/полученных сообщений в секунду;
- **Web Service** (Веб-служба) — счетчики службы WWW Publishing Service (Служба веб-публикаций).

Ниже дан список счетчиков для мониторинга производительности, сгруппированный по источникам и объектам (табл. 10-1). Самый простой способ ознакомиться с этими счетчиками — изучить их описания в диалоговом окне Add Counters (Добавить счетчики). Запустите Performance Monitor, щелкните на панели инструментов кнопку Add (Добавить) и выберите из списка Performance Object (Объект) нужный объект. Затем щелкните Explain (Объяснение) и просмотрите список доступных счетчиков.

**Табл. 10-1.** Основные счетчики для мониторинга производительности сервера

Источник	Счетчик	Объект
ASP-сеансы	Session Duration (Длительность сеанса)	Active Server Pages (Страницы Active Server)
	Sessions Current (Текущих сеансов)	Active Server Pages (Страницы Active Server)
	Sessions Timed Out (Просроченных сеансов)	Active Server Pages (Страницы Active Server)
	Sessions Total (Всего сеансов)	Active Server Pages (Страницы Active Server)
ASP-транзакции	Transactions Aborted (Прекращено транзакций)	Active Server Pages (Страницы Active Server)
	Transactions Committed (Завершено транзакций)	Active Server Pages (Страницы Active Server)
	Transactions Pending (Транзакций в ожидании)	Active Server Pages (Страницы Active Server)
	Transactions Total (Всего транзакций)	Active Server Pages (Страницы Active Server)
	Transactions /Sec (Транзакций в секунду)	Active Server Pages (Страницы Active Server)

Табл. 10-1. (продолжение)

Источник	Счетчик	Объект
Использование полосы пропускания	Current Blocked Async I/O requests (Блокировано запросов асинхронного ввода/вывода)	Internet Information Services Global (Общий объект служб IIS), Web Service (Веб-служба), FTP Service (Служба FTP)
	Measured Async I/O Bandwidth usage (Использование полосы пропускания асинхронного ввода/вывода)	Internet Information Services Global (Общий объект служб IIS), Web Service (Веб-служба)
	Total Allowed Async I/O Requests (Всего разрешено запросов асинхронного ввода/вывода)	Internet Information Services Global (Общий объект служб IIS), Web Service (Веб-служба)
	Total Blocked Async I/O Requests (Всего блокировано запросов асинхронного ввода/вывода)	Internet Information Services Global (Общий объект служб IIS), Web Service (Веб-служба)
	Total Rejected Async I/O Requests (Всего отклонено запросов асинхронного ввода/вывода)	Internet Information Services Global (Общий объект служб IIS), Web Service (Веб-служба)
Кэширование и память	File Cache Flushes (Число удалений кэша файлов), URI Cache Flushes (Число удалений кэша URI)	Internet Information Services Global (Общий объект служб IIS)
	File Cache Hits (Попаданий в кэш файлов), URI Cache Hits (Попаданий в кэш URI)	Internet Information Services Global (Общий объект служб IIS)
	File Cache Hits % (Процент попаданий в кэш файлов), URI Cache Hits % (Процент попаданий в кэш URI)	Internet Information Services Global (Общий объект служб IIS)
	File Cache Misses (Промахов в кэше файлов), URI Cache Misses (Промахов в кэше URI)	Internet Information Services Global (Общий объект служб IIS)



Табл. 10-1. (продолжение)

Источник	Счетчик	Объект
Подключения	Maximum File Cache Memory Usage (Предельное использование памяти кэша файлов)	Internet Information Services Global (Общий объект служб IIS)
	Script Engines Cached (Кэшировано обработчиков сценариев)	Active Server Pages (Страницы Active Server)
	Template Cache Hit Rate (Попаданий в кэшированный шаблон)	Active Server Pages (Страницы Active Server)
	Template Notifications (Уведомлений шаблонов)	Active Server Pages (Страницы Active Server)
	Templates Cached (Кэшировано шаблонов)	Active Server Pages (Страницы Active Server)
	ConnectionAttempts/Sec (Попыток подключения в секунду)	Web Service (Веб-служба)
	CurrentAnonymousUsers (Подключено анонимных пользователей)	Web Service (Веб-служба), FTP Service (Служба FTP)
	Current Connections (Текущих подключений)	Web Service (Веб-служба), FTP Service (Служба FTP)
	Current File Cache Memory Usage (Текущее использование памяти кэша файлов)	Internet Information Services Global (Общий объект служб IIS)
	Maximum Connections (Максимальное число подключений)	Web Service (Веб-служба), FTP Service (Служба FTP)
	Current Files Cached (Файлы в кэше)	Internet Information Services Global (Общий объект служб IIS)
	Current NonAnonymousUsers (Подключено неанонимных пользователей)	Web Service (Веб-служба), FTP Service (Служба FTP)
	Maximum AnonymousUsers (Максимум анонимных пользователей)	Web Service (Веб-служба), FTP Service (Служба FTP)
	Maximum NonAnonymousUsers (Максимум неанонимных пользователей)	Web Service (Веб-служба), FTP Service (Служба FTP)

Табл. 10-1. (продолжение)

Источник	Счетчик	Объект
Ошибки	Total Anonymous Users (Всего анонимных пользователей)	Web Service (Веб-служба), FTP Service (Служба FTP)
	Total Connection Attempts (Всего попыток подключения (всех видов))	Web Service (Веб-служба), FTP Service (Служба FTP)
	Total Logon Attempts (Всего попыток входа)	Web Service (Веб-служба), FTP Service (Служба FTP)
	Total NonAnonymous Users (Всего неанонимных пользователей)	Web Service (Веб-служба), FTP Service (Служба FTP)
	Errors During Script Runtime (Ошибок во время выполнения сценария)	Active Server Pages (Страницы Active Server)
	Errors From ASP Preprocessor (Ошибок препроцессора ASP)	Active Server Pages (Страницы Active Server)
	Errors From Script Compiler (Ошибок компиляции сценария)	Active Server Pages (Страницы Active Server)
	Errors/Sec (Ошибок в секунду)	Active Server Pages (Страницы Active Server)
	Not Found Errors/Sec (Ошибок «Не найдено» в секунду)	Web Service (Веб-служба)
	Requests Not Authorized (Неразрешенных запросов)	Active Server Pages (Страницы Active Server)
	Requests Not Found (Ненайденных запросов)	Active Server Pages (Страницы Active Server)
	Requests Rejected (Отказанных запросов)	Active Server Pages (Страницы Active Server)
	Requests Timed Out (Просроченных запросов)	Active Server Pages (Страницы Active Server)
	Service Uptime (Доступное время службы)	Web Service (Веб-служба), FTP Service (Служба FTP)
	Total Not Found Errors (Всего ошибок «Не найдено»)	Web Service (Веб-служба)

Табл. 10-1. (продолжение)

Источник	Счетчик	Объект
Индекси- рование	Active Queries (Активных запросов)	HTTP Indexing Service (Служба индексирования HTTP)
	Queries Per Minute (Запросов/мин)	HTTP Indexing Service (Служба индексирования HTTP)
	Total Queries (Общее число запросов)	HTTP Indexing Service (Служба индексирования HTTP)
	Total Indexing Speed [Общая скорость индексирования (МБ/час)]	Indexing Service Filter (Фильтр службы индексирования)
Запросы	Get Requests/Sec (Запросов Get в секунду)	Web Service (Веб-служба)
	Head Requests/Sec (Запросов Head в секунду)	Web Service (Веб-служба)
	ISAPI Extension Requests/Sec (Запросов расширения ISAPI в секунду)	Web Service (Веб-служба)
	Post Requests/Sec (Запросов Post в секунду)	Web Service (Веб-служба)
	Put Requests/Sec (Запросов Put в секунду)	Web Service (Веб-служба)
	Request Bytes In Total (Всего входящих байт запросов)	Active Server Pages (Страницы Active Server)
	Request Bytes Out Total (Всего исходящих байт запросов)	Active Server Pages (Страницы Active Server)
	Requests Executing (Выполняется запросов)	Active Server Pages (Страницы Active Server)
	Requests Queued (Запросов в очереди)	Active Server Pages (Страницы Active Server)
	Requests Rejected (Отказанных запросов)	Active Server Pages (Страницы Active Server)
	Requests Succeeded (Успешных запросов)	Active Server Pages (Страницы Active Server)
	Requests Timed Out (Просроченных запросов)	Active Server Pages (Страницы Active Server)

Табл. 10-1. (продолжение)

Источник	Счетчик	Объект
Пропускная способность	Requests Total (Всего запросов)	Active Server Pages (Страницы Active Server)
	Requests/Sec (Запросов в секунду)	Active Server Pages (Страницы Active Server)
	Bytes Received/Sec (Получено байт в секунду)	Web Service (Веб-служба), FTP Service (Служба FTP)
	Bytes Sent/Sec. (Отправлено байт в секунду)	Web Service (Веб-служба), FTP Service (Служба FTP)
	Bytes Total/Sec (Всего байт в секунду)	Web Service (Веб-служба), FTP Service (Служба FTP)
	Files Received/Sec (Получено файлов в секунду)	Web Service (Веб-служба), FTP Service (Служба FTP)
	Files Sent/Sec (Отправлено файлов в секунду)	Web Service (Веб-служба), FTP Service (Служба FTP)
	Files/Sec (Файлов в секунду)	Web Service (Веб-служба), FTP Service (Служба FTP)
	Total Files Received (Всего получено файлов)	Web Service (Веб-служба), FTP Service (Служба FTP)
	Total Files Sent (Всего отправлено файлов)	Web Service (Веб-служба), FTP Service (Служба FTP)
	Total Files Transferred (Всего передано файлов)	Web Service (Веб-служба), FTP Service (Служба FTP)

Наблюдая за определенным объектом, Performance Monitor может отслеживать все экземпляры всех его счетчиков. Экземпляр — одно из «воплощений» конкретного счетчика. Скажем, счетчики объекта Web Service (Веб-служба) позволяют собирать данные обо всех или только определенных Web-узлах. Таким образом, если у вас есть узлы CorpWeb, CorpProducts и CorpServices, с помощью счетчиков объекта Web Service можно отслеживать сразу все или какой-то один из них.

Наблюдаемые счетчики выбираются так.

1. Раскрыв меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование), выберите Performance Monitor (Системный монитор).
2. Performance Monitor может отображать информацию в нескольких представлениях. Щелкните кнопку View Chart

(Просмотр диаграммы) для представления информации на диаграмме.

3. Чтобы добавить счетчики, щелкните на панели инструментов кнопку Add (Добавить). Откроется диалоговое окно Add Counters (Добавить счетчики) (рис. 10-4), поля которого позволяют:

- **Use Local Computer Counters (Использовать локальные счетчики)** — использовать счетчики локального компьютера;
- **Select Counters From Computer (Выбрать счетчики с компьютера)** — ввести UNC-имя удаленного ПС-компьютера (например \\ENGSRV01), счетчики которого требуется использовать;
- **Performance Object (Объект)** — выбрать нужный объект, например Active Server Pages;
- **All Counters (Все счетчики)** — выбрать все счетчики текущего объекта;
- **Select Counters From List (Выбрать счетчики из списка)** — выбрать один или несколько счетчиков текущего объекта, например, Requests Not Found (Не найденных запросов), Requests Queued (Запросов в очереди) и Requests Total (Всего запросов);
- **All Instances (Все вхождения)** — выбрать для мониторинга все экземпляры счетчика;

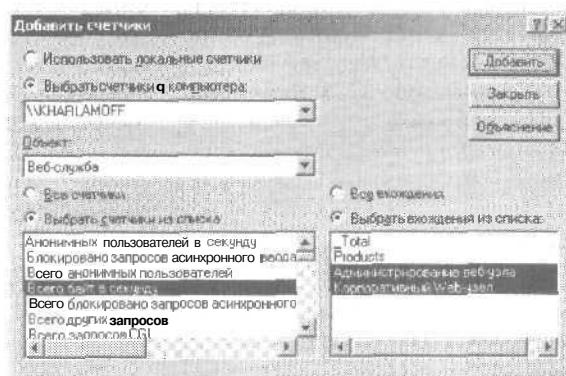


Рис. 10-4. Выбор наблюдаемых счетчиков

- **Select Instances From List (Выбрать вхождения из списка)** — выбрать для мониторинга один или несколько экземпляров счетчика; например, можно выбрать экземпляры счетчика Anonymous Users/Sec (Анонимных пользователей в секунду) для всех или только отдельных Web-узлов.



**Примечание** Не пытайтесь отобразить на диаграмме слишком много счетчиков. Это затруднит ее восприятие и потребует большого объема системных ресурсов, а именно памяти и времени процессора, влияющих на время реакции сервера.

4. Выбрав счетчики, щелкните Add (Добавить), чтобы добавить их на диаграмму. При необходимости повторите описанные действия, чтобы добавить дополнительные счетчики производительности.
5. Добавив все нужные счетчики, щелкните Close (Заккрыть),

## Создание и управление журналами Performance Monitor

Журналы Performance Monitor позволяют отслеживать производительность ИС и в дальнейшем воспроизводить собранные данные. Помните, что параметры в журналах и в окне Performance Monitor регистрируются отдельно. Файлы журналом можно сконфигурировать для автоматического или ручного обновления сведений счетчиков. При автоматическом ведении журнала через определенные интервалы времени, например 15 секунд, создается снимок ключевых параметров. Если журнал ведется вручную, создание снимков целиком зависит от вас. Существует два типа журналов производительности;

- **Counter logs (Журналы счетчиков)** — здесь с заданным интервалом регистрируются сведения о производительности, собираемые выбранными администратором счетчиками.
- **Trace Logs (Журналы трассировки)** — здесь регистрируются сведения о производительности при наступлении определенных событий.

## Управление журналами производительности

Журналы производительности создаются так.

1. Раскройте меню **Start\Programs\Administrative Tools** (Пуск\Программы\Администрирование) и выберите **Performance Monitor** (Системный монитор).
2. Раскройте узел **Performance Logs And Alerts** (Оповещения и журналы производительности). Для создания журнала счетчиков щелкните значок **Counter Logs** (Журналы счетчиков), а для создания журнала трассировки — значок **Trace Logs** (Журналы трассировки).
3. В правой панели отобразится список текущих журналов, если таковые имеются (рис. 10-5). Зеленый значок указывает, что журнал ведется, красный — что ведение журнала остановлено.

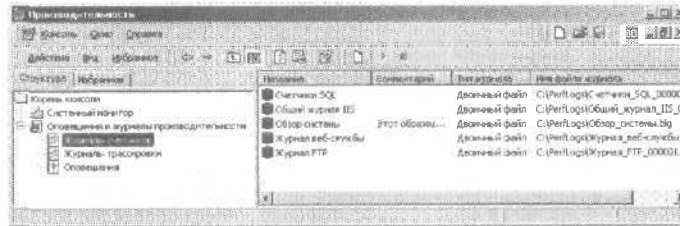


Рис. 10-5. Список текущих журналов производительности

4. Чтобы создать новый журнал, щелкните правой кнопкой в правой панели и выберите в контекстном меню команду **New Log Settings** (Новые параметры журнала). В открывшемся диалоговом окне введите имя нового журнала.
5. Чтобы добавить нужные счетчики, щелкните **Add** (Добавить), а затем — **ОК**.
6. Для управления существующим журналом щелкните правой кнопкой его значок и выберите одну из команд:
  - **Start** (Запуск) -- начать ведение журнала;
  - **Stop** (Остановка) — остановить ведение журнала;
  - **Delete** (Удалить) — удалить журнал;
  - **Properties** (Свойства) — открыть диалоговое окно **Log Properties** (Свойства журнала).


### Создание журналов счетчиков

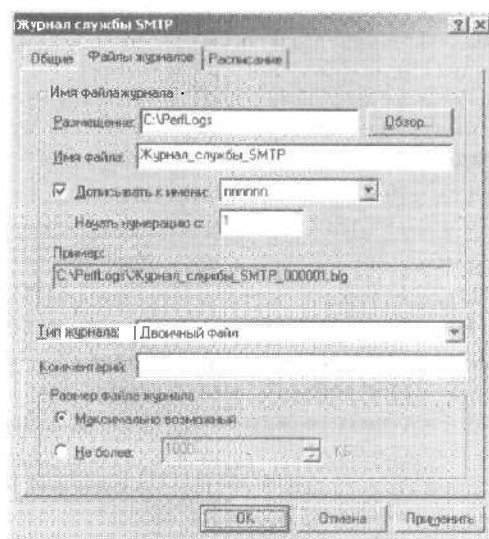
В журналы счетчиков через определенные интервалы времени записываются данные о производительности, регистрируемые выбранными администратором счетчиками. Скажем, можно каждые 5 минут записывать данные о производительности Web-службы. Журнал счетчиков создастся так.

1. В левой панели консоли Performance (Производительность) щелкните значок Counter Logs (Журналы счетчиков). Затем, щелкнув правой кнопкой в правой панели, выберите в контекстном меню команду New Log Settings (Новые параметры журнала).
2. Откроется одноименное диалоговое окно. Введите имя нового журнала, например, HTTP Performance Monitor или Total Request Monitor, и щелкните OK.
3. На вкладке General (Общие) щелкните Add (Добавить). Откроется диалоговое окно Select Counters (Выбор счетчиков), подобное этому (рис. 10-4).
4. Добавьте нужные счетчики и затем щелкните Close (Закрыть).
5. В поле Sample Data Every (Снимать показания каждые) введите интервал выборки показаний счетчика в секундах, минутах, часах или днях. Интервал выборки определяет время сбора новых данных. Так, если интервал выборки — 15 минут, данные журнала будут обновляться каждые 15 минут.
6. Поля вкладки Log Files (Файлы журналов) (рис. 10-6) позволяют задать параметры создаваемого файла журнала:
  - **Location** (Размещение) — папка, в которой будет храниться файл журнала;
  - **File Name** (Имя файла) — имя файла журнала;
  - **End File Names With** (Дописывать к имени) — суффикс, автоматически добавляемый к имени каждого нового файла ведущегося журнала; это может быть порядковый номер или дата;
  - **Start Numbering At** (Начать нумерацию с) — первый последовательный номер журнала, использующего автоматические цифровые суффиксы;



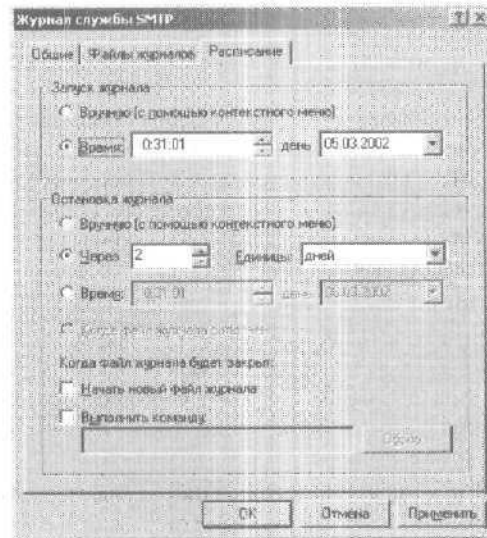
- **Log File Type (Тип журнала)** — тип создаваемого файла журнала. При выборе Text File — CSV (Текстовый файл — CSV) создается журнал с разделением записей запятыми; Text File — TSV (Текстовый файл — TSV) — с разделением символами табуляции; Binary File (Двоичный файл) — двоичный файл, который может быть считан Performance Monitor; Binary Circular File (Двоичный циклический файл) — двоичный файл, в котором при достижении максимального размера новые данные перезаписывают старые;
- **Comment (Комментарий)** — необязательное описание журнала, отображаемое в поле Comment (Комментарий);
- **Maximum Limit (Максимально возможный)** — отключение ограничений на размер файла;
- **Limit Of (Не более)** — задание конкретного размера файла журнала в Кб.

 **Примечание** Если вы собираетесь просматривать и анализировать журнал с помощью Performance Monitor, выберите один из двоичных форматов.



**Рис. 10-6.** Вкладка Log Files (Файлы журналов) диалогового окна свойств журнала счетчиков

7. Перейдите на вкладку Schedule (Расписание) и укажите время начала и прекращения ведения журнала (рис. 10-7).
8. Ведение журнала можно начать вручную или автоматически, с определенной даты. Щелкните нужный переключатель и, если надо, укажите дату начала ведения журнала.



**Рис. 10-7.** Вкладка Schedule (Расписание) диалогового окна свойств журнала счетчиков



**Примечание** Файлы журналов могут быстро увеличиваться в размере. Для регистрации данных в течение длительного периода создайте файл журнала на диске с большим объемом свободного пространства. Помните: чем чаще обновляется файл журнала, тем больше требуется дискового пространства и времени процессора.

9. Ведение журнала может быть прекращено:
  - вручную;
  - по прошествии определенного периода времени (например, 7 дней);
  - при наступлении конкретной даты и времени;

- при переполнении файла журнала (если задан его максимальный размер).
10. Настроив расписание ведения журнала, щелкните ОК. Подробнее об управлении созданным журналом см. раздел «Управление журналами производительности» этой главы.

### Создание журналов трассировки

В журналах трассировки данные регистрируются при наступлении событий соответствующих поставщиков. Поставщик — это приложение или служба ОС, обладающая доступными для трассировки событиями. На контроллерах доменов имеются системный поставщик, а также поставщики Local Security Authority (LSA) и Active Directory:NetLogon. На прочих серверах скорее всего будут доступны только системный поставщик и Local Security Authority (LSA).

Журнал трассировки создается так.

1. В левой панели консоли Performance (Производительность) щелкните значок Trace Logs (Журналы трассировки). Затем, щелкнув правой кнопкой в правой панели, выберите в контекстном меню команду New Log Settings (Новые параметры журнала).
2. Откроется одноименное диалоговое окно. Введите имя нового журнала, например Disk I/O Trace или Network TCP/IP Trace, и щелкните ОК. Откроется диалоговое окно (рис. 10-8).
3. Для трассировки событий ОС щелкните переключатель Events Logged By System Provider (События, регистрируемые системным поставщиком) и выберите нужные события (рис. 10-8).



**Внимание!** При сборе сведений о страничном обмене и файловых операциях сильно возрастает нагрузка на систему и быстро увеличивается размер файла журнала. В связи с этим подобную информацию рекомендуется собирать лишь в течение ограниченного периода.

4. Для сбора данных других поставщиков щелкните переключатель Nonsystem Providers (Несистемные поставщики), и затем — кнопку Add (Добавить). Откроется диа-

логовое окно Nonsystem Providers (Добавление несистемных поставщиков), в котором можно выбрать поставщиков.

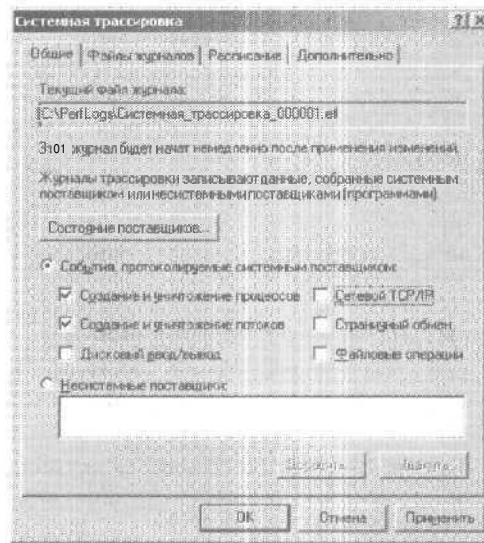


Рис. 10-8. Диалоговое окно свойств журнала трассировки

5. Выбрав поставщиков и события, перейдите на вкладку Log Files (Файлы журналов) и сконфигурируйте файл трассировки в соответствии с п. 6 раздела «Создание журналов счетчиков» этой главы. Единственное отличие — в типах журналов. Существует два типа журналов трассировки:
  - Sequential Trace File (Файл последовательной трассировки) — последовательно регистрирует события до достижения максимального размера файла журнала (если таковой определен);
  - Circular Trace File (Файл циклической трассировки) — при достижении максимального размера файла журнала старые данные перезаписываются новыми.
6. Перейдите на вкладку Schedule (Расписание) и укажите время начала и прекращения трассировки.

7. Ведение журнала можно начать вручную или автоматически, с определенной даты. Щелкните нужный переключатель и, если надо, укажите дату начала ведения журнала.
8. Ведение журнала может быть прекращено вручную, по прошествии определенного периода времени (например, 7 дней), при наступлении конкретной даты и времени или при переполнении файла журнала (если задан его максимальный размер).
9. Настроив расписание ведения журнала, щелкните ОК. Подробнее об управлении созданным журналом см. раздел «Управление журналами производительности» этой главы.

### Воспроизведение журналов производительности

При устранении проблем зачастую полезно собрать данные о производительности за длительный период времени и затем проанализировать их.

1. Сконфигурируйте автоматическое ведение журнала в соответствии с инструкциями раздела «Создание журналов счетчиков» этой главы.
2. После сбора данных для анализа файл журнала следует загрузить в Performance Monitor (Системный монитор). Для этого щелкните на панели инструментов Performance Monitor кнопку View Log File Data (Просмотр данных файла журнала). Откроется диалоговое окно Select Log File (Выбор файла журнала).
3. Выберите нужный файл и щелкните Open (Открыть).
4. Теперь можно строить графики на основе зарегистрированных счетчиками данных. Щелкните Add (Добавить) и выберите нужные счетчики.

### Создание оповещений для счетчиков производительности

Оповещения позволяют узнавать о наступлении определенных событий или достижении некоторых пороговых значений производительности. Оповещения могут отсылаться в форме сетевых сообщений или регистрироваться в журнале событий приложений. Кроме того, оповещение может запус-

кать приложения или начинать ведение журналов производительности.

В Performance Monitor оповещения добавляются так.

1. В левой панели консоли Performance (Производительность) щелкните значок Alerts (Оповещения). Затем, щелкнув правой кнопкой в правой панели, выберите в контекстном меню команду New Alerts Settings (Новые параметры оповещений).
2. В открывшемся диалоговом окне введите имя оповещения, например, ASP Error Alert или High User Connection Alert, и щелкните OK. Откроется диалоговое окно свойств оповещения (рис. 10-9).

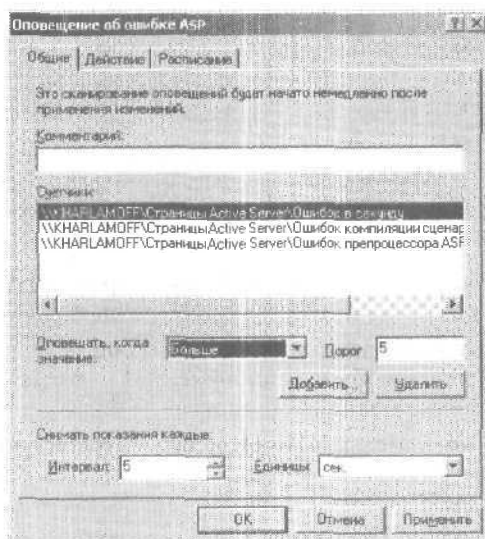


Рис. 10-9. Диалоговое окно свойств оповещения

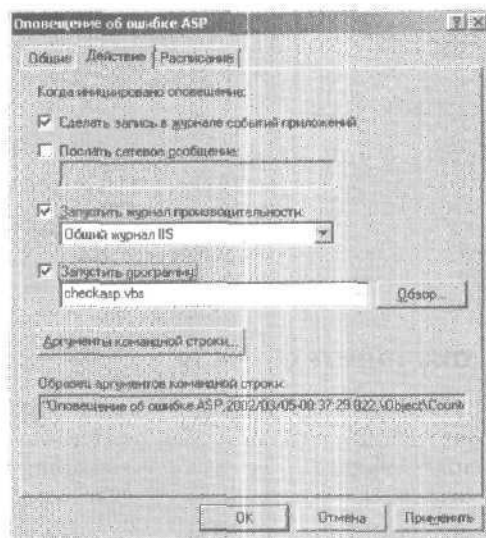
3. В поле Comment (Комментарий) вкладки General (Общие) введите необязательное описание оповещения. Затем щелкните Add (Добавить). Откроется диалоговое окно Select Counters To Log (Выбор счетчиков) (рис. 10-4).
4. Выберите счетчики для запуска оповещения и щелкните Close (Закреть).

5. Щелкните в группе Counters (Счетчики) первый счетчик и затем в поле Trigger Alert When Value Is (Оповещать, когда значение) укажите условие запуска соответствующего оповещения. Оповещение может срабатывать, если значение счетчика окажется больше или меньше заданного значения. Выберите Over (Больше) или Under (Меньше) и введите нужное значение. Единицы его измерения зависят от конкретного счетчика. Так, для запуска оповещения при загрузке процессора свыше 95% выберите Over (Больше) и введите 95. Повторите эту операцию для всех выбранных вами счетчиков.
6. В поле Sample Data Every (Снимать показания каждые) введите интервал выборки показаний счетчика в секундах, минутах, часах или днях. Интервал выборки определяет время сбора новых данных. Так, если интервал выборки — 5 минут, данные журнала будут обновляться каждые 5 минут.



**Внимание!** Не устанавливайте слишком короткий интервал времени — это потребует **большого объема** системных ресурсов и **может негативно** сказаться на **времени** реакции сервера.

7. Перейдите на вкладку Action (Действие) (рис. 10-10). Здесь можно указать действия при запуске оповещения:
  - **Log An Entry In The Application Event Log (Сделать запись в журнале событий приложений)** — в журнал событий заносится запись об оповещении;
  - **Send A Network Message To (Послать сетевое сообщение)** — на указанный компьютер отсылается сетевое сообщение;
  - **Start Performance Data Log (Запустить журнал производительности)** — когда срабатывает оповещение, начинается ведение указанного журнала производительности;
  - **Run This Program (Запустить программу)** — при запуске оповещения запускается указанная программа или сценарий.



**Рис. 10-10.** Вкладка Action (Действие) диалогового окна свойств оповещения



**Совет** Можно запускать любые исполняемые файлы, включая пакеты с расширением `.bat` или `.cmd`, а также сценарии Windows с расширениями `.vb`, `.js`, `.pl` и `.wsc`. Чтобы передать приложению или сценарию аргументы, щелкните Command Line Arguments (Аргументы командной строки) и пометьте нужные флажки. Обычно аргументы передаются в виде отдельных строк. Однако, если помечен флажок Single Arguments String (Строка одиночного аргумента), аргументы передаются в одной строке с разделением запятыми. В нижней части окна отображается пример передаваемого списка аргументов.

8. Перейдите на вкладку **Schedule (Расписание)**, и укажите **время начала и прекращения наблюдения за значением счетчика**. Так, можно начать наблюдение в пятницу вечером и прекратить в понедельник утром. Если в этот период **сработает уведомление**, будут выполнены соответствующие действия.



9. Наблюдение за значением счетчика может начинаться вручную или автоматически, с некоторой даты. Щелкните нужный переключатель и, если надо, укажите дату начала ведения журнала.
10. Прекратить наблюдение можно вручную, по истечении определенного периода времени (например, 7 дней) или при наступлении конкретной даты и времени.
11. Настроив расписание ведения журнала, щелкните ОК. Управление оповещениями осуществляется так же, как и управление журналами счетчиков и производительности.

## Настройка производительности Web-сервера

Изучив основы мониторинга Web-серверов, перейдем к оптимизации производительности ОС и оборудования. Мы рассмотрим оптимизацию:

- использования памяти и кэширования;
- загрузки процессора;
- дисковых операций ввода/вывода;
- сетевых подключений и пропускной способности сети.

## Мониторинг и настройка использования памяти

Зачастую память — это узкое место производительности, и поэтому перед исследованием других областей системы следует исключить проблемы с памятью. Одна из основных причин проблем с памятью в том, что файловый кэш *US* по умолчанию использует половину ОЗУ системы. Так, если в системе установлено 512 Мб ОЗУ, файловый кэш *IIS* может занимать до 256 Мб памяти (конечно, необходимый для кэширования объем ОЗУ зависит от количества файлов и периодичности запросов).

Кроме того, проблемы могут создавать параметры кэширования и виртуальной памяти. Увеличение ОЗУ сервера, испытывающего проблемы с кэшированием или виртуальной памятью, не поможет их устранить. В связи с этим вам следует одновременно проверять систему на наличие проблем с ОЗУ, кэшированием и виртуальной памятью.

Чтобы исключить упомянутые проблемы, можно:

- сконфигурировать параметры производительности приложений;
- оптимизировать сервер для максимальной пропускной способности сетевых приложений.

Выполнив необходимые действия и перезагрузив систему, проверьте наличие проблем с памятью сервера.

#### **Конфигурирование параметров производительности приложений**

Параметры производительности приложений определяют время реакции обычных и фоновых программ. Чаще всего необходимо одинаковое время реакции обычных и фоновых программ, а не низкое время реакции отдельных Web-приложений. Чтобы гарантировать своевременную реакцию сервера на запросы фоновых программ, сделайте так.

1. Раскрыв меню **Start\Settings** (Пуск\Настройка), выберите **Control Panel** (Панель управления). Дважды щелкните значок **System** (Система).
2. В открывшемся окне перейдите на вкладку **Advanced** (Дополнительно) и щелкните **Performance Options** (Параметры быстроедействия).
3. Щелкните **Background Services** (служб, работающих в фоновом режиме) и затем — **OK**.

#### **Оптимизация сервера для максимальной пропускной способности сетевых приложений**

Если сервер используется преимущественно как Web-сервер, сконфигурируйте его как сервер приложений. При этом он будет оптимизирован для максимальной производительности сетевых служб, Web-приложениям станет доступно больше памяти, улучшатся и мультипроцессорные характеристики сервера. Для этого сделайте так.

1. Раскрыв меню **Start\Settings** (Пуск\Настройка), выберите **Network And Dial-Up Connections** (Сеть и удаленный доступ к сети).
2. Щелкнув правой кнопкой значок **Local Area Connection** (Подключение по локальной сети), выберите в контекст-

ном меню команду Properties (Свойства). Откроется диалоговое окно (рис. 10-11).

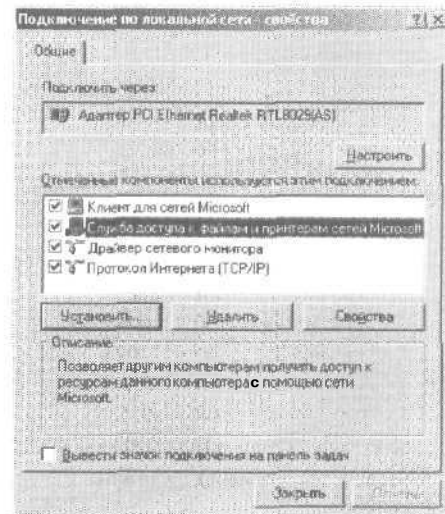



Рис. 10-11. Диалоговое окно Local Area Connection Properties (Подключение по локальной сети - свойства)

 **Примечание** На серверах с несколькими сетевыми платами в окне Network And Dial-Up Connections отображается несколько сетевых подключений. Оптимизируйте каждое из них соответствующим образом.

3. Выберите File And Printer Sharing For Microsoft Networks (Служба доступа к файлам и принтерам сетей Microsoft) и щелкните Properties (Свойства).
4. На вкладке Server Optimization (Оптимизация сервера) щелкните Maximize Data Throughput For Network Applications (макс. пропускная способность для сетевых приложений) и затем — ОК.
5. Перезагрузите сервер, чтобы изменения вступили в силу.

#### **Контроль использования ОЗУ, кэширования и виртуальной памяти**

Оптимизировав систему, можно посмотреть, как она использует память и проверить наличие проблем. Ниже перечис-

лены счетчики, позволяющие выявить узкие места ОЗУ, виртуальной памяти и кэширования (табл. 10-2).

### Мониторинг и настройка использования процессора

Реально обработку данных на сервере осуществляет процессор. В связи с этим при оптимизации производительности сервера сразу после устранения проблем с памятью нужно выявить и устранить проблемы с процессорами. Если процессоры сервера — узкое место производительности, установка дополнительных модулей ОЗУ, дисков и сетевых плат не решит проблемы. Вместо этого следует заменить процессоры на имеющие более высокую тактовую частоту или добавить дополнительные процессоры для повышения емкости сервера. Кроме того, можно перенести интенсивно использующие процессор приложения на другой сервер.

Прежде чем заменить имеющиеся или установить дополнительные процессоры, исключите проблемы с памятью и кэшированием. Если остальные признаки по-прежнему указывают на проблему с процессором, наблюдайте за следующими счетчиками производительности (табл. 10-3). Ведите мониторинг значений этих счетчиков для каждого процессора сервера.



**Совет** Зачастую одного сервера недостаточно для обработки сетевого трафика. При этом вам, возможно, потребуется распределить Web-узел между несколькими серверами. Например, можно реплицировать узел на дополнительные серверы и затем сбалансировать сетевой трафик при помощи распределителя нагрузки (*load balancer*). Если ваш узел уже находится на мультисерверной Web-ферме, можно добавить новые серверы.

### Мониторинг и настройка дискового ввода-вывода

Учитывая характеристики современных высокоскоростных накопителей, пропускная способность дисковой подсистемы редко является узким местом производительности. Тем не менее доступ к памяти осуществляется намного быстрее доступа к диску. И если серверу приходится выполнять много

операций чтения и записи на диск, его общая производительность может упасть. Для уменьшения объема дискового ввода-вывода следует эффективно управлять памятью сервера и выгружать страницы на диск только в случае крайней необходимости. Подробнее о мониторинге и настройке использования памяти см. одноименный раздел этой главы.

В дополнение к настройке памяти можно понаблюдать значения перечисленных ниже счетчиков, позволяющих оценить активность дискового ввода-вывода (табл. 10-4).



**Примечание** Иногда счетчики логических и физических дисков необходимо предварительно включить, введя в окне сеанса MS-DOS команду Diskperf -у для жесткого диска и Diskperf -yv — для программного массива RAID.

## Мониторинг и настройка сетевых подключений и пропускной способности сети

Работа сети, соединяющей сервер и клиентский компьютер — самый важный фактор, влияющий на восприятие производительности вашего узла пользователями. Задержка между созданием и получением запроса может стоить очень дорого. При больших задержках будет неважно, что ваш сервер — самый быстрый на планете. Пользователь, столкнувшийся с задержкой обработки запроса, станет думать, что наши серверы — медленные.

Вообще вы не можете управлять задержками, с которыми сталкиваются пользователи. Это зависит от типа пользовательского подключения и маршрута запроса через Интернет к вашему серверу. Тем не менее вам подвластны общая емкость сервера, используемая для обработки запросов, и полоса пропускания, доступная серверам. Доступная полоса пропускания зависит от способа подключения вашей организации к Интернету, а пропускная способность сети — от сетевых плат и интерфейсов, имеющихся на серверах.

Стандартная сетевая плата может эффективно обрабатывать сетевое подключение Fast Ethernet 100 Мбит/сек., что значительно превышает трафик обычного узла и обычный трафик, обрабатываемый сервером. Так что обычно ограничи-

Табл. 10-2. Выявление узких мест, связанных с памятью сервера

Проблема	Рекомендуемый объект	Счетчик	Описание
Использование физической и виртуальной памяти	Memory\Available Bytes (Память\Доступная КЗ) Memory\Committed Bytes (Память\Виртуальной памяти)	Memory\Available Bytes Memory\Committed Bytes (Память\Виртуальной памяти)	Счетчик Memory\Available Bytes показывает объем физической памяти, доступный для приложений на сервере. Счетчик Memory\Committed Bytes — размер выделенной виртуальной памяти. Если объем доступной памяти недостаточен, возможно, потребуется нарастить ОЗУ сервера. В целом рекомендуется, чтобы была доступна не менее 5% от общего объема физической памяти сервера. Если счетчик интенсивно использует виртуальную память, тем самым следует увеличить ОЗУ сервера. Обычно размер выделенной виртуальной памяти не должен превышать 75% от объема ОЗУ системы.
Кэширование памяти	Memory\Cache Bytes (Память\Кэш-памяти) Internet Information Services Global\Current File Cache Memory Usage (Общий объект служб IIS\Текущее использование памяти кэша файлов) Internet Information Services Global\File Cache Hits% (Общий объект служб IIS\Процент попаданий в кэш файлов) Internet Information Services Global\File Cache Flushes	Memory\Cache Bytes Internet Information Services Global\Current File Cache Memory Usage Internet Information Services Global\File Cache Hits% Cache Flushes	Счетчик Memory\Cache Bytes показывает общий объем файлового кэша системы. Счетчик Internet Information Services Global\Current File Cache Memory Usage — объем памяти, занимаемый файловым кэшем служб IIS. Счетчик Internet Information Services Global\File Cache Hits% представляет соотношение числа попаданий в кэш и общего числа обращений к нему и демонстрирует, насколько оптимальны параметры файлового кэша IIS. На узлах с преимущественно статичными файлами число попаданий в кэш должно быть велико (70% – 85%). Счетчик Internet Information Services Global\File Cache Flushes показывает, как часто IIS удаляет файлы из кэша. Если файлы удаляются слишком быстро, увеличьте срок хранения кэшированных объектов (параметр ObjectCacheTTL). Если файлы удаляются редко, вы, возможно, зря занимаете

Табл. 10-2. (продолжение)

Проблема	Рекомендуемый Объект\счетчик	Описание
	<i>(Общий объект служб IIS\Число удалений кэша файлов)</i>	нужную системе память, и вам следует уменьшить срок хранения кэшированных объектов.
Ошибки страниц памяти	Memory\Page Faults/sec <i>(Память\Ошибок страницы/сек)</i> Memory\Pages Input/sec <i>(Память \Ввод страниц/сек)</i> Memory Page Reads/sec <i>(Память\Чтений страниц/сек)</i>	Ошибка страницы возникает, если ОС не может найти запрошенную процессором страницу памяти по указанному адресу. Если страница находится в другой части памяти, ошибка называется безопасной. Если же нужную страницу требуется считать с диска, ошибка называется неисправимой. Многие процессоры могут быстро обрабатывать большое количество безопасных ошибок. И все же неисправимые ошибки могут вызвать значительную задержку. Счетчик Memory\Page Faults/sec показывает общую скорость обработки всех типов ошибок страниц процессором. Значение счетчика Memory\Pages Input/sec — это общее число страниц, считываемых с диска для обработки неисправимых ошибок. Счетчик Memory Page Reads/sec показывает общее число операций чтения с диска, необходимых для устранения неисправимых ошибок. Значение счетчика Memory\Pages Input/sec будет равно или больше значения счетчика Memory\Page Reads/sec и дает хорошее представление о скорости возникновения неисправимых ошибок страниц. При большом числе неисправимых ошибок страниц следует увеличить объем ОЗУ сервера или уменьшить размер кэша. Управлять памятью, используемой службами IIS, позволяют параметры MemCacheSize и MaxCachedFileSize.

Табл. 10-2. (продолжение)

Проблема	Рекомендуемый объект	Описание
Разделение страниц	Memory\Pool\GatherBytes (Память\Байты - пул) Memory\Pool\DoPragedBytes (Память\Байты неагрессив- ном пространстве пула)	Данные счетчики показывают объем выгружаемого и загружаемого страничного пула в байтах. Страничный пул — это область системной памяти, где хранятся объекты, которые, когда они не нужны, выгружаются на диск. Неагрессивный пул — это область системной памяти для объектов, которые нельзя выгрузить на диск. Если объем выгружаемого пула достаточно велик по отношению к общему объему физической памяти, нарастите объем ОЗУ системы. Если объем выгружаемого пула достаточно велик по отношению к общему объему страничной памяти сервера, увеличьте объем последней.

Табл. 10-3. Выявление узких мест, связанных с процессорами сервера

Описание	Рекомендуемый объект	Описание
Утилизация процессора	System\Process\Queue Length (Сист. ма. Длина очереди процессора)	Данный счетчик показывает число потоков в очереди, общую для всех процессоров сервера. Если значение данного счетчика в течение времени равно 2 и более потокам, значит установлен дополнительный процессор.
Среднее процессорное время	Processor\%Processor Time (Процессор\% время загрузки процессора)	Данный счетчик показывает, насколько выгружаемый поток загружает выбранный процессор. Если значение для процессора сервера. Если значения счетчиков processor\% processor time





Табл. 10-4. Выявление узких мест, связанных с дисковыми накопителями

Проблема	Рекомендуемый объект	Счетчик	Описание
Общая производительность дисков	PhysicalDisk\% Disk Time (Физический диск\% активности диска) совместно с Processor\% Processor Time (Процессор\% загрузки процессора) и Network Interface Connection\Bytes Total/sec (Сетевой интерфейс\Всего байт/сек)	% Disk Time	Если значение счетчика % Disk Time велико, а значения Processor\% Processor Time и Network Interface Connection\Bytes Total/sec малы, возможно, что жесткие диски являются узким местом системы. Значение счетчика % Disk Time следует наблюдать для всех жестких дисков сервера.
Дисковод ввода-вывода	PhysicalDisk\Disk Writes/sec (Физический диск\Обращения записи на диск/сек), PhysicalDisk\Disk Reads/sec (Физический диск\Обращения чтения с диска/сек), PhysicalDisk\Avg. Disk Write Queue Length (Физический диск\Средняя длина очереди записи на диск), PhysicalDisk\Avg. Disk Read Queue Length (Физический диск\Средняя длина очереди чтения диска), PhysicalDisk\Current Disk Queue Length (Физический диск\Текущая длина очереди диска)	Disk Writes/sec, Disk Reads/sec, Avg. Disk Write Queue Length, Avg. Disk Read Queue Length, Current Disk Queue Length	Число операций чтения и записи в секунду показывает о общую активность дисководов ввода-вывода. Длины очередей чтения и записи показывают, сколько запросов на чтение и записи ожидает обработки. В целом рекомендуется, чтобы длины очередей были небольшой. Помните: задержка запроса пропорциональна длине очереди за минусом числа накопителей в массиве RAID.

вающий фактор — это доступная вашей организации полоса пропускания. Если все Интернет-операции в организации осуществляются по общему каналу T1, ваши серверы разделяют полосу пропускания в 1,4 Мбит/сек. с остальным Интернет-трафиком. Если Web-узлы используют выделенный канал T1, им доступна полоса пропускания в 1,4 Мбит/сек. При наличии нескольких каналов T1 или одного канала T3 полоса пропускания, доступная вашим узлам, может колебаться от 3 до 45 Мбит/сек.

Приняв это за данность, помните: число параллельных подключений, которое сможет обработать ваша сеть, зависит от скорости подключения, объема передаваемых по отдельным подключениям данных и допустимого времени передачи. Например, если у вас есть канал T1 и стандартный объем передачи данных по подключению равен 50 Кб, а допустимое время передачи — 15 секунд, ваше сетевое подключение сможет обрабатывать:

- 21 операцию передачи данных в секунду

— или —

- 294 параллельных операции передачи данных.

С другой стороны, если у вас имеется канал T1 и стандартный объем передачи данных по подключению — 250 Кб, а допустимое время передачи — 15 секунд, ваше сетевое подключение сможет обрабатывать:

- 15 операций передачи данных в секунду

— или —

- 60 параллельных операций передачи данных.

Иногда ограничивающим фактором может быть пропускная способность сетевой платы. На большинстве серверов установлены сетевые платы 10/100, предоставляющие широкие возможности конфигурирования. Например, плату можно настроить для передачи данных со скоростью 10 Мбит/сек., а также для полнодуплексной или полудуплексной передачи данных. Предполагая, что проблемы пропускной способности сети связаны с сетевой платой, проверьте конфигурацию последней.



**Совет** Канал T1 — стандартный пример сетевого подключения коммерческих Web-узлов. Владельцы крупных коммерческих узлов обычно обращаются в службы размещения информации в сети (например ICOM), предоставляющие подключение к Интернету со скоростью от 100 Мбит/сек. Если вы владеец такого узла, помните, что конфигурация некоторых сетевых устройств может ограничивать доступную полосу пропускания. Например, брандмауэр может ограничивать полосу пропускания Web-служб 5 Мбит/сек., FTP-служб — 2 Мбит/сек., и SMTP-служб — 1 Мбит/сек.

Чтобы определить пропускную способность и текущую активность сетевых плат сервера, просмотрите значения таких счетчиков;

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

Если при средней нагрузке значение счетчика Network\Bytes Total/sec превышает 50% от общей пропускной, при пиковой нагрузке на сервере могут возникнуть проблемы. Измените конфигурацию, чтобы сильно загружающие сеть операции, например резервное копирование, использовали отдельную сетевую плату. Помните, что значения указанных счетчиков следует сравнивать со значениями PhysicalDisk\% Disk Time (Физический диск\% активности диска) и Processor\% Processor Time (Процессор\% загрузки процессора). Если их значения малы, а значения сетевых счетчиков велики, возможны проблемы с пропускной способностью сети.

Ограничить использование полосы пропускания и оптимизировать производительность сети в IIS можно несколькими способами, включая:

- ограничение пропускной способности;
- ограничение максимального числа подключений;
- HTTP-сжатие.

### Ограничение пропускной способности и числа подключений

Уменьшить использование полосы пропускания можно, ограничив пропускную способность и максимальное число подключений. Ограничивая пропускную способность, вы уменьшаете часть полосы пропускания, доступную службе или отдельным узлам, а ограничивая число подключений — общее число возможных соединений для определенной службы. При превышении этих значений пользователям может быть отказано в доступе, и поэтому ограничения стоит применять, только когда это действительно необходимо.

Прежде, чем ограничить пропускную способность, понаблюдайте за обсуждавшимися ранее счетчиками сетевых объектов. Если они указывают на возможную проблему, единственный способ устранить ее — ограничить пропускную способность. Ограничить пропускную способность всех Web- и FTP-узлов сервера можно так.

1. В оснастке IIS щелкните правой кнопкой значок нужного компьютера и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке Internet Information Services пометьте флажок Enable Bandwidth Throttling (Регулировка полосы пропускания).
3. В поле Maximum Network Use (Предельная нагрузка на сеть) укажите доступную службам IIS полосу пропускания в Кб/сек. Помните: вы задаете общую пропускную способность всех Web- и FTP-узлов сервера.
4. Щелкните ОК.

В отличие от FTP-узлов вполне допустимо ограничивать пропускную способность отдельных Web-узлов.

1. В оснастке IIS щелкните правой кнопкой нужный Web-узел и выберите в контекстном меню команду Properties (Свойства).
2. На вкладке Performance (Быстродействие) пометьте флажок Enable Bandwidth Throttling (Регулировка полосы пропускания).
3. В поле Maximum Network Use (Предельная нагрузка на сеть) введите укажите доступную узлу полосу пропускания в Кб/сек.

#### 4. Щелкните ОК.

Подробнее об ограничении числа подключений к Web- и FTP-узлам см. главы 3 и 7 этой книги соответственно.

#### Настройка HTTP-сжатия

Если включено HTTP-сжатие, перед передачей файлов клиентскому браузеру Web-сервер архивирует их. Это позволяет уменьшить объем пересылаемых между клиентом и сервером данных и, следовательно, снизить нагрузку на полосу пропускания и сеть, а также уменьшить *время* передачи. Для использования HTTP-сжатия клиентский браузер должен поддерживать протокол HTTP версии 1.1, и должна быть включена поддержка сжатия. В большинстве браузеров поддержка сжатия и HTTP 1.1 включены по умолчанию, однако старые браузеры могут не поддерживать указанный протокол. Они смогут загружать файлы с вашего узла, но без HTTP-сжатия.

Прежде чем включить сжатие, наблюдайте за использованием процессора сервера. HTTP-сжатие создает дополнительную нагрузку на сервер, что ведет к более интенсивному использованию процессора. Если на вашем узле широко используется динамическое содержимое и значение счетчика % Processor Time велико, вам, вероятно, не потребуется добавлять или заменять процессоры для включения HTTP-сжатия.

HTTP-сжатие включается так.

1. В оснастке IIS щелкните правой кнопкой значок нужного компьютера и выберите в контекстном меню команду Properties (Свойства).
2. В группе Master Properties (Основные свойства) выберите WWW Service (WWW-служба) и щелкните Edit (Изменить).
3. Перейдите на вкладку Service (Служба) (рис. 10-12).
4. Для сжатия динамического содержимого, например ASP-страниц, пометьте флажок Compress Application Files (Сжатие файлов приложений). Сжатые динамические файлы хранятся в памяти.

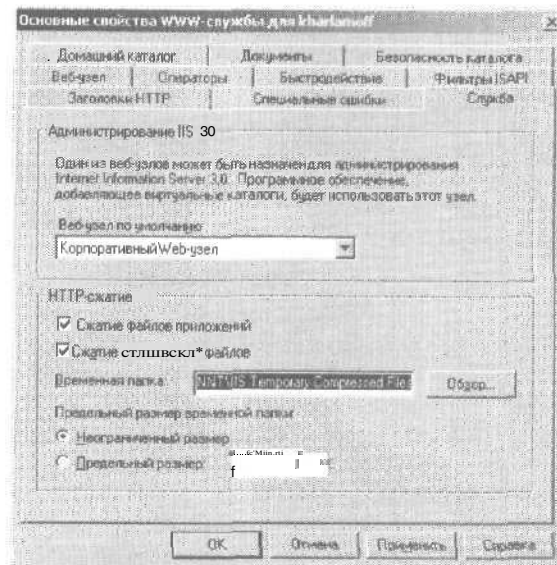


Рис. 10-12. Вкладка Service (Служба) диалогового окна WWW Service Master Properties (Основные свойства WWW-службы)

5. Для сжатия статичных файлов, например HTML-страниц, пометьте флажок Compress Static Files (Сжатие статических файлов). Сжатые статичные файлы хранятся в папке, указанной в поле Temporary Folder (Временная папка).
6. В поле Temporary Folder (Временная папка) указывается папка, где находятся сжатые статические файлы до истечения срока их хранения. Можно ввести путь к папке вручную или щелкнуть Browse (Обзор) и выбрать нужный каталог.



**Примечание** Папка должна располагаться на локальном диске с файловой системой NTFS. Кроме того, она не должна быть сетевым ресурсом и не может быть сжатой.

7. Чтобы ограничить кэш статических файлов, щелкните переключатель Limited To (Предельный размер) и введите максимальный размера папки в мегабайтах.
8. Дважды щелкните OK.

## Глава 11

# Ведение журналов и контроль пользовательского доступа

Одна из основных обязанностей Web-администратора — ведение журналов доступа к Интернет-серверам компании. Включить ведение журналов на HTTP-, FTP- и SMTP-серверах совсем несложно. Однако собрать и записать корректные сведения о доступе в формате, обеспечивающем их чтение и анализ, несколько труднее. ПО для анализа журналов доступа называется трассировочным. Существует множество разновидностей такого ПО. Большинство коммерческих трассировочных приложений создают подробные отчеты с таблицами и графиками, содержащими сведения об активности узла за определенный период. Так, трассировочные отчеты можно создавать ежедневно, еженедельно или ежемесячно.

Для HTTP-, FTP- и SMTP-серверов можно вести журналы доступа. Файлы журнала могут иметь разный формат — вы можете вести обычный, ODBC- или расширенный журнал. При ведении обычного журнала информация о пользовательском доступе заносится в ASCII-файл. При ведении ODBC-журнала сведения о пользовательском доступе заносятся непосредственно в ODBC-совместимую БД, например, Microsoft SQL Server 2000. При ведении расширенного журнала можно ограничить объем регистрируемой информации и записывать лишь нужные вам сведения о пользовательском доступе.

### Статистика трассировки: общая картина

Если для HTTP-, FTP- или SMTP-сервера включено ведение журналов, создаются журналы доступа. При запросе клиентом файлов с вашего Web-узла в журнал доступа за-



носится соответствующая запись; таким образом, журнал содержит сведения о всех удачных/неудачных попытках получения информации с узла. Каждой записи соответствует отдельная строка, и поэтому извлечь записи журнала для создания отчетов совсем нетрудно. Отчеты расскажут вам много интересного о посетителях вашего узла. Вы узнаете о:

- часах пик вашего узла;
- браузерах и платформах, используемых посетителями;
- популярных и непопулярных ресурсах;
- узлах, ссылающиеся на ваш узел;
- эффективности вашей рекламы;
- социальном потреблении посетителей вашего узла;
- используемых поисковых системах и ключевых словах;
- времени, проводимом посетителями на узле.

Вот возможные форматы журналов доступа.

- **Стандартный формат файла журнала NCSA (National Center for Supercomputing Applications, Национальный центр разработки приложений для вычислений на супер-ЭВМ)** [только для Web- и SMTP-узлов] — используйте данный формат, если вам нужны лишь общие сведения о доступе к узлу. Записи такого журнала имеют небольшой размер, и это снижает требования к свободному дисковому пространству для ведения журнала.
- **Формат файла журнала Microsoft IIS (Microsoft Internet Information Services)** — используйте формат журнала IIS, если вам не требуется подробная информация и нужно лишь чуть больше сведений о доступе. Записи такого журнала компактны, и это снижает требования к свободному дисковому пространству для ведения журнала.
- **Расширенный формат файла журнала W3C (World Wide Web Consortium)** — используйте данный формат, если вам нужны лишь определенные и подробные сведения о доступе. Записи такого журнала могут быть очень большими, и это сильно повышает требования к свободному дисковому пространству для ведения журнала. Кроме того, занесение длинных записей в журнал может негативно сказаться на производительности перегруженного сервера.

- Формат журнала **ODBC** — используйте данный формат, если вам требуется заносить информацию прямо в ODBC-совместимую базу данных. При ведении ODBC-журнала вам понадобится трассировочное ПО, способное считывать информацию из БД. Записи будут компактными и будут считываться гораздо быстрее, чем из обычного файла журнала. Помните: при записи в локальный экземпляр БД ведение ODBC-журнала требует больше ресурсов процессора.



**Совет** Microsoft разработала утилиту для преобразования файлов журналов в стандартный формат журнала NCSA — CONVLOG. Она находится в папке %WinDir%\System32. CONVLOG позволяет преобразовывать журналы из форматов 1IS и W3C в стандартный формат NCSA. Кроме того, в процессе преобразования CONVLOG выполняет обратный DNS-поиск, благодаря чему можно разрешать некоторые IP-адреса в доменные имена.

Ниже мы подробно рассмотрим возможные форматы файлов журнала.

### Стандартный формат файла журнала NCSA

Этот самый распространенный формат журнала является фиксированным ASCII-форматом, в котором каждая строка соответствует отдельному обращению к файлу. Его следует использовать, если вам нужны лишь общие сведения о доступе к узлу. В частности, он удобен для отслеживания такой информации, как:

- число попаданий на узел (количество уникальных запросов файлов);
- число просмотров страниц (количество уникальных запросов страниц);
- число обращений к узлу (количество пользовательских сеансов за указанный период);
- прочие базовые сведения о доступе.

В журнале такого формата записи имеют небольшой размер, и это снижает требования к свободному дисковому пространству для ведения журнала. Каждая запись включает семь полей:

- Host;
- Identification;
- User Authentication;
- Time Stamp;
- HTTP Request Type;
- Status Code;
- Transfer Volume.

Простой для понимания стандартный формат облегчает переход к расширенным форматам файлов журнала. Вот несколько записей в стандартном формате журнала NCSA. Поля записей разделены пробелами.

```
192.168.11.15 - ENGSVR01\wrstane [15/Jan/2001:18:44:57 -0800]
"GET / HTTP/1.1" 200 1970
192.168.11.15 - ENGSVR01\wrstane [15/Jan/2001:18:45:06 -0800]
"GET /home.gif HTTP/1.1" 200 5032
192.168.11.15 - ENGSVR01\wrstane [15/Jan/2001:18:45:28 -0800]
"GET /main.htm HTTP/1.1" 200 5432
192.168.11.15 - ENGSVR01\wrstane [15/Jan/2001:18:45:31 -0800]
"GET /details.gif HTTP/1.1" 200 1211
192.168.11.15 - ENGSVR01\wrstane [15/Jan/2001:18:45:31 -0800]
"GET /menu.gif HTTP/1.1" 200 6075
192.168.11.15 - ENGSVR01\wrstane [15/Jan/2001:18:45:31 -0800]
"GET /sidebar.gif HTTP/1.1" 200 9023
192.166.11.15 - ENGSVR01\wrstane [15/Jan/2001:18:45:31 -0800]
"GET /sun.gif HTTP/1.1" 200 4706
192.168.11.15 - ENGSVR01\wrstane [15/Jan/2001:18:45:38 -0800]
"GET /moon.gif HTTP/1.1" 200 1984
192.168.11.15 - ENGSVR01\wrstane [15/Jan/2001:18:45:41 -0800]
"GET /stars.gif HTTP/1.1" 200 2098
```

Большинство других форматов файлов журнала основано на формате NCSA, и поэтому мы подробно рассмотрим назначение описанных выше семи полей.

#### Поле Host

Первое поле записи в стандартном формате журнала. Идентифицирует компьютер, запросивший файл с вашего узла. Значением данного поля может быть как IP-адрес, например 192.168.11.15, так и полное доменное имя удаленного узла, например net48.microsoft.com. Вот запись HTTP-запроса,

инициированного узлом, IP-адрес которого был успешно разрешен в доменное имя:

```
net48.microsoft.com - ENGSR01\wrstane [15/Jan/2001:18:44:57
-0800] "GET / HTTP/1.1" 200 1970
```

IP-адреса — это численные эквиваленты полных доменных имен. Для определения доменного имени по IP-адресу обычно используют обратный DNS-поиск. Изучив имеющееся или полученное в результате преобразований доменное имя, можно больше узнать о посетителе узла. Подразделения домена разделены точками. Последнее подразделение — это класс домена, позволяющий узнать, где живет и работает пользователь.

Классы доменов организованы по географическому и демографическому принципу. Первые заканчиваются двух- или трехзначным кодом страны, к которой относится пользователь. Например, кол .ca охватывает фирмы Канады. Вторые указывают тип компании, предоставляющей пользователю доступ к Интернету.

**Табл. 11-1.** Основные классы доменов

Класс домена	Описание
.com	Коммерческий (commercial); пользователи из коммерческих организаций
.edu	Образовательный (educational); пользователи из колледжей и университетов
.gov	Правительственный (government); пользователи из правительственных учреждений за исключением военных организаций
.mil	Военный (military); пользователи из военных организаций
.net	Сетевой (network); пользователи из компаний-поставщиков услуг Интернета и прочих связанных с работой в сети фирм
.org	Некоммерческие организации (nonprofit organizations); пользователи из упомянутых организаций

**Поле Identification**

Второе поле записи в стандартном формате журнала, должно содержать имя пользователя, но на практике редко заполняется, и обычно вместо имени ставится тире (-).

```
net48.microsoft.com - ENGSVR01\wrstane [15/Jan/2001:18:44:57
-0800] "GET / HTTP/1.1" 200 1970
```

Если данное поле содержит какое-либо другое значение, помните, что указанное имя пользователя не прошло проверку. Возможно, что оно получено обманным путем и ему не следует доверять.

**Поле User Authentication**

Третье поле записи в стандартном формате. Если ваш Web-узел содержит защищенную паролем область, для доступа к ней пользователю следует указать соответствующие имя и пароль. После проверки подлинности имя пользователя заносится в поле User Authentication. Для незащищенных областей узла в данном поле обычно отображается тире (-), а для защищенных — имя учетной записи пользователя, прошедшего проверку подлинности. Имени учетной записи может предшествовать имя домена, в котором была пройдена проверка.

```
net48.microsoft.com - ENGSVR01\wrstane [15/Jan/2001:18:44:57
-0800] "GET / HTTP/1.1" 200 1970
```

**Поле Time Stamp**

Четвертое поле записи в стандартном формате журнала точно указывает время доступа к файлу на сервере:

ДД/МММ/ГГГГ:ЧЧ:ММ:СС Смещение

Например,

```
15/Jan/2001:18:44:57 -0800
```

Смещение — это разница между временем сервера и временем по Гринвичу (Greenwich Mean Time, GMT). В следующем примере разница составляет -8 часов, т. е. время сервера на 8 часов меньше времени по Гринвичу;

```
net48.microsoft.com - ENGSVR01\wrstane [15/Jan/2001:18:44:57
-0800] "GET / HTTP/1.1" 200 1970
```

**Поле HTTP Request**

Пятое поле записи в стандартном формате журнала. Указывает метод, которым удаленный клиент запросил ресурс, а также идентифицирует запрошенный ресурс и версию протокола HTTP, используя которую, клиент получил ресурс. В следующем примере поле HTTP Request выделено полужирным начертанием:

```
192.168.11.15 - ENGSVR01\wrstanek [15/Jan/2001:18:45:06 -0800]  
"GET /home.gif HTTP/1.1" 200 5032
```

Здесь метод передачи -- GET, запрошенный ресурс -- /HOME.GIF, протокол передачи — HTTP 1.1. Заметьте, что ресурсы указываются с использованием относительных URL, интерпретируемых сервером. Например, если вы запросите файл <http://www.microsoft.com/home/main.htm>, для доступа к нему сервер задействует относительный URL /home/MAIN.HTM. Запись, оканчивающаяся косой чертой, ссылается на документ каталога по умолчанию (обычно -- INDEX.HTM или DEFAULT.ASP).

**Поле Status Code**

Шестое поле записи в стандартном формате журнала. Код состояния показывает, успешно ли передан файл, был ли он загружен из кэша, не найден и т. д. Обычно код состояния включает три цифры, первая из которых указывает его класс или категорию.

**Табл. 11-2.** Классы кодов состояния

Код класса	Описание
1XX	Продолжение/смена протокола
2XX	Успешное выполнение
3XX	Перенаправление
4XX	Отказ/ошибка клиента
5XX	Ошибка сервера

Коды состояния, начинающиеся с единицы, очень редки, и поэтому вам следует запомнить лишь четыре других категории кодов. Коды состояния на 2 указывают, что соответствующий файл передан успешно, на 3 — что сервер отослал вас к другому ресурсу, на 4 — что произошла ошибка или

сбой на клиентском компьютере, на 5 — что произошла ошибка на сервере.

#### Поле Transfer Volume

Последнее поле записи в стандартном формате журнала указывает число байт, переданных клиенту в ответ на его запрос. В следующем примере клиенту передано 4 096 байт:

```
net48.microsoft.com - ENGSVR01\wrstane [15/Jan/2001:18:45:06
-0800] "GET / HTTP/1.1" 200 4096
```

Число переданных байт отображается, только если код состояния указывает на успешную передачу файла. В противном случае поле Transfer Volume будет содержать тире (-) или 0, показывая, что данные не передавались.

#### Формат файла журнала Microsoft IIS

Как и стандартный формат, формат файла журнала Microsoft IIS является фиксированным (ненастраиваемым) ASCII-форматом. В этом формате регистрируется больше данных. Кроме того, журнал форматируется как обычный ASCII-текст, и его можно открывать в любом стандартном текстовом редакторе или совместимом с ним приложении.

Формат журнала Microsoft IIS используется, если не требуется подробная информация и нужно лишь чуть больше сведений о доступе, чем содержит стандартный журнал. Записи такого журнала компактны, и это снижает требования к свободному дисковому пространству в сравнении с расширенным или ODBC-журналом.

Ниже приведено несколько записей из журнала формата Microsoft IIS. Записи журнала IIS включают как стандартные (IP-адрес клиента, имя пользователя, прошедшее проверку подлинности, время и дата запроса, HTTP-код состояния, число принятых сервером байт), так и дополнительные поля (например имя Web-службы, IP-адрес сервера и время работы). Заметьте: записи разделены запятыми и имеют значительно больший, чем в стандартном журнале, размер.

```
192.14.16.2, -, 12/28/2000, 20:55:25, W3SVC1, ENGSVR01,
192.15.14.81, 0, 594, 3847, 401, 5, GET, /localstart.asp, -,
192.14.16.2, ENGSVR01\wrstane, 12/28/2000, 20:55:25, W3SVC1,
ENGSVR01, 192.15.14.81, 10, 412, 3406, 404, 0, GET, /
localstart.asp, |-[0]404_Object_Not_Found,
```

```

192.14.16.2, -, 12/28/2000, 20:55:29, W3SVC1, ENGSVR01,
192.15.14.81, 0, 622, 3847, 401, 5, GET, /IISHelp/iis/misc/
default.asp, -,
192.14.16.2, ENGSVR01\wrstaneK, 12/28/2000, 20:55:29, W3SVC1,
ENGSVR01, 192.15.14.81, 10, 426, 0, 200, 0, GET, /IISHelp/iis/
misc/default.asp, -,
192.14.16.2, ENGSVR01\wrstaneK, 12/28/2000, 20:55:29, W3SVC1,
ENGSVR01, 192.15.14.81, 10, 368, 0, 200, 0, GET, /IISHelp/iis/
misc/contents.asp, -,
192.14.16.2, -, 12/28/2000, 20:55:29, W3SVC1, ENGSVR01,
192.15.14.81, 0, 732, 3847, 401, 5, GET, /IISHelp/iis/misc/
navbar.asp, -,
192.14.16.2, -, 12/28/2000, 20:55:29, W3SVC1, ENGSVR01,
192.15.14.81, 0, 742, 3847, 401, 5, GET, /IISHelp/iis/htm/
core/iowltop.htm, -,
192.14.16.2, ENGSVR01\wrstaneK, 12/28/2000, 20:55:29, W3SVC1,
ENGSVR01, 192.15.14.81, 20, 481, 0, 200, 0, GET, /IISHelp/iis/
misc/navbar.asp, -,
192.14.16.2, ENGSVR01\wrstaneK, 12/28/2000, 20:55:29, W3SVC1,
ENGSVR01, 192.15.14.81, 91, 486, 6520, 200, 0, GET, /IISHelp/
iis/htm/core/iowltop.htm, -,

```

Ниже перечислены поля, поддерживаемые службами IIS (табл. 11-3). Порядок перечисления соответствует обычно-му порядку записи полей в журнал.

**Табл. 11-3-** Поля записей журнала в формате Microsoft IIS

Название поля	Описание	Пример
Client IP	IP-адрес клиента	192.14.16.2
Username	Имя пользователя, прошедшее проверку подлинности	ENGSVR01\wrstaneK
Date	Дата завершения транзакции	12/28/2000
Time	Время завершения транзакции	20:55:29
Service	Имя Web-службы, регистрирующей транзакцию	W3SVC1
Computer Name	Имя компьютера, сделавшего запрос	ENGSVR01
Server IP	IP-адрес Web-сервера	192.15.14.81
Elapsed Time	Время (в миллисекундах) на завершение транзакции	40



Табл. 11-3. (продолжение)

Название поля	Описание	Пример
Bytes Received	Число байт, принятых сервером в запросе клиента	486
Bytes Sent	Число байт, переданных клиенту	6520
Status Code	HTTP-код состояния	200
Windows Status Code	Код состояния ошибки (Windows)	0
Method Used	Тип HTTP-запроса	GET
File URI	Запрошенный файл	/localstart.asp
Referer	Ссылающийся объект — ресурс, с которого пришел пользователь	http://www.microsoft.com/

### Расширенный формат файла журнала W3C

Значительно отличается от обсуждавшихся выше, представляет собой настраиваемый формат, включающий множество различных полей. Помните, что с каждым дополнительным полем увеличивается размер записей журнала и могут сильно возрасти требования к свободному дисковому пространству.

Вот несколько записей из расширенного журнала. Как и в стандартном журнале, поля записей расширенного журнала разделены пробелами.

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
«Date: 2000-12-29 05:27:58
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-
uri-stem cs-uri-query sc-status cs(User-Agent)
2000-12-29 05:27:58 192.14.16.2 ENGSRV01\wrstane 192.14.15.81
80 GET /iishelp/iis/htm/core/ierrcst.htm - 304 Mozilla/
4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2000-12-29 05:28:00 192.14.16.2 ENGSRV01\wrstane 192.14.15.81
80 GET /iishelp/iis/htm/core/ierrdtl.htm - 304 Mozilla/
4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2000-12-29 05:28:02 192.14.16.2 ENGSRV01\wrstane 192.14.15.81
80 GET /iishelp/iis/htm/core/ierrabt.htm - 200 Mozilla/
4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2000-12-29 05:28:02 192.14.16.2 ENGSRV01\wrstane 192.14.15.81
80 GET /iishelp/iis/htm/core/ierradd.htm - 200 Mozilla/
```

```

4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2000-12-29 05:28:05 192.14.16.2 ENGSRV01\wrstanek 192.14.15.81
80 GET /iishelp/iis/htm/core/iiprstop.htm - 200 Mozilla/
4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)

```

На первый взгляд записи расширенного журнала могут показаться сложными, так как включают директивы сервера и файловые запросы. Однако директивы сервера всегда начинаются со знака #, и их легко отличить от файловых запросов. Ключевые директивы, которые вы увидите, идентифицируют ПО сервера и записываемые поля (табл. 11-4).

**Табл. 11-4.** Директивы, используемые в расширенном формате файла журнала

Директива	Описание
Date	Дата и время занесения записей в журнал
End-Date	Дата и время закрытия и архивирования журнала
Fields	Используемые поля и их порядок в файле журнала
Remark	Комментарии
Software	Серверное ПО, создавшее записи журнала
Start-Date	Дата и время начала ведения журнала
Version	Версия используемого расширенного формата файла журнала

У большинства полей записей расширенного журнала есть префиксы, указывающие, как используется или было получено конкретное поле (табл. 11-5). Так, префикс *cs* указывает, что поле создано на основании запроса, переданного клиентом серверу.

**Табл. 11-5.** Префиксы полей расширенного журнала

Префикс	Описание
c	Поле, относящееся к клиенту
s	Поле, относящееся к серверу
г	Поле, относящееся к удаленному серверу
cs	Поле, созданное на основании запроса, переданного клиентом серверу
sc	Поле, созданное на основании запроса, переданного IIS-сервером клиенту
sg	Поле, созданное на основании запроса, переданного Web-сервером удаленному серверу (используется прокси-серверами)

Табл. 11-5. (продолжение)

Префикс	Описание
rs	Поле, созданное на основании запроса, переданного удаленным сервером IIS-серверу (используется прокси-серверами)
x	Префикс, специфичный для приложений

Все поля записей расширенного журнала имеют идентификатор, который расшифровывает тип информации, содержащейся в данном поле. Для создания поименованного поля IIS может объединить префикс и идентификатор поля или просто задействовать идентификатор. Ниже перечислены наиболее распространенные имена полей (табл. 11-6). Многие из приведенных полей напрямую связаны с уже обсуждавшимися полями записей стандартного и расширенного журналов. Основное же отличие в том, что расширенный формат предоставляет гораздо больше информации.

Табл. 11-6. Идентификаторы полей, применяемые в расширенном журнале

Тип поля	Имя поля	Описание
Bytes Received	cs-bytes	Число байт, принятых сервером
Bytes Sent	sc-bytes	Число байт, переданных сервером
Client IP Address	c-ip	IP-адрес клиента, обратившегося к серверу
Cookie	cs(Cookie)	Содержимое принятого/переданного файла cookie (если таковой был)
Date	date	Дата транзакции
Http Status	sc-status	HTTP-код состояния
Method Used	cs-method	Тип HTTP-запроса
Protocol Version	cs-protocol	Версия протокола, используемая клиентом
Referer	cs(Referer)	Предыдущий узел, посещенный пользователем (узел, ссылающийся на ваш Web-узел)
Server IP	s-ip	IP-адрес IIS-сервера
Server Name	s-computername	Имя IIS-сервера
Server Port	s-port	Номер порта, к которому подключился клиент

Табл. 11-6. (продолжение)

Тип поля	Имя поля	Описание
Server Name and Instance Number	s-sitename	Имя и номер экземпляра службы Интернета, выполнявшейся на сервере
Time	time	Время транзакции
Time Taken	time-taken	Время (в миллисекундах) на завершение транзакции
URI Query	cs-uri-query	Параметры, переданные в запросе (если таковые передавались)
URI Stem	cs-uri-stem	Запрошенный ресурс
User Agent	cs(User-Agent)	Тип и версия клиентского браузера
User Name	c-username	Имя пользователя, прошедшего проверку подлинности
Win32 Status	sc-win32-status	Код состояния ошибки (Windows)

Помимо регистрации запросов на доступ, IIS также может регистрировать связанную с HTTP-запросами информацию об использовании ресурсов процессами. Учетная информация процессов помогает определить объем ресурсов процессора, занимаемый отдельным Web-узлом. Но помните: регистрация учетной информации процессов возможна лишь для внепроцессных приложений. Для групповых и выполняющихся в процессе приложений это невозможно.

Ниже приведены поля для регистрации учетной информации процессов (табл. 11-7). Просмотрев файл журнала, для которого была включена и сконфигурирована регистрация учетной информации процессов, вы наряду с обычными записями увидите записи об использовании ресурсов.

Табл. 11-7. Поля с учетной информацией процессов, используемые в расширенных журналах

Тип поля	Имя поля	Описание
Active Processes	s-active-procs	Число CGI- (Common Gateway Interface) и внепроцессных приложений, запущенных на момент занесения записи в журнал

Табл. 11-7. (продолжение)

Тип поля	Имя поля	Описание
Process Event	s-event	Запущенное событие
Process Type	s-proc-type	Тип процесса, запустившего событие: CGI, внепроцессное приложение или оба
Total Kernel Time	s-kernel-time	Общее время процессора в режиме ядра (в секундах) на протяжении текущего интервала
Total Page Faults	s-page-faults	Число ссылок памяти, приведших к страничным ошибкам памяти
Total Processes	s-total-procs	Число CGI- и внепроцессных приложений, созданных на протяжении текущего интервала
Total Terminated Processes	s-stopped-procs	Число CGI- и внепроцессных приложений, остановленных в результате регулирования процессов
Total User Time	s-user-time	Общее время процессора в пользовательском режиме (в секундах) на протяжении текущего интервала

### Формат журнала ODBC

Применяется для записи информации о доступе прямо в ODBC-совместимую БД, например Microsoft Access или SQL Server 2000. Основное преимущество ODBC-журнала в том, что записи заносятся в БД в формате, который упрощает их чтение и анализ с помощью соответствующего ПО. Главный минус — необходимость наличия навыков конфигурирования и поддержки баз данных.

При ведении ODBC-журнала вам потребуется сконфигурировать имя источника данных (Data Source Name), позволяющее службам IIS подключаться к вашей БД. Нужно также создать БД, куда будут заноситься записи; она должна включать таблицу с соответствующими полями.

Обычно сведения от нескольких узлов помещаются в разные таблицы одной БД. Так, если надо регистрировать в БД сведения об HTTP-, FTP- и SMTP-доступе и соответствующие службы выполняются на разных узлах, можно создать в БД таблицы HTTPLog, FTPLog и SMTPLog. Они будут

включать поля с типами данных, перечисленные ниже (табл. 11-8). Определите поля именно так, как показано в таблице. Не волнуйтесь: в IIS есть LOGTEMP.SQL — сценарий, позволяющий создать нужные таблицы. Он находится в папке `\%WinDir%\System32\Inetsrv`.



**Примечание** При использовании сценария LOGTEMP.SQL не забудьте изменить имя таблицы в операторе CREATE TABLE. Имя таблицы по умолчанию — `inetlog`. Подробнее об использовании SQL-сценариев — в книге «Microsoft SQL Server 2000. Administrator's Pocket Consultant» издательства Microsoft Press, 2001 г.

**Табл. 11-8.** Поля ODBC-журнала

Имя поля	Тип данных	Описание
ClientHost	varchar(255)	IP-адрес клиента, обратившегося к серверу
Username	varchar(255)	Имя пользователя, прошедшего проверку подлинности
LogTime	datetime	Дата и время транзакции
Service	varchar(255)	Имя и номер экземпляра службы Интернета, выполнявшейся на сервере
Machine	varchar(255)	Имя компьютера, сделавшего запрос
ServerIP	varchar(50)	IP-адрес IIS-сервера
ProcessingTime	int	Время (в миллисекундах) на завершение транзакции
BytesRecvd	int	Число байт, принятых сервером
BytesSent	int	Число байт, переданных сервером
ServiceStatus	int	HTTP-код состояния
Win32Status	int	Код состояния ошибки (Windows)
Operation	varchar(255)	Тип HTTP-запроса
Target	varchar(255)	Запрошенный ресурс
Parameters	varchar(255)	Параметры, переданные в запросе (если таковые передавались)

## О ведении журналов узлов

Если включено ведение журнала IIS, при обращении пользователей к серверу генерируются новые записи. В результате размер и число файлов журнала стабильно увеличивают-

ся. На сервере с большим число посетителей журнал может быстро увеличиться до нескольких гигабайт, и, следовательно, вам требуется найти компромисс между потребностью в сведениях о доступе и уменьшением журнала до приемлемого размера.



**Совет** Помните: файлы журнала — это текстовые файлы формата ASCII, и поэтому их, как и любой ASCII-файл, можно произвольно разделять и объединять. Если при занесении записи в журнал на сервере кончается свободное дисковое пространство, службы IIS останавливаются, и в журнал приложений (Application log) помещается сообщение об ошибке. При появлении свободного пространства IIS возобновляют работу и заносят в журнал приложений сообщение о своем запуске.

Включая ведение журнала, вы указываете, где и как будут создаваться и храниться файлы журнала (табл. 11-9). Файлы могут создаваться по расписанию (например, каждый час, день, неделю, месяц) и иметь фиксированный (например, 100 Мб) или неограниченный размер. Имя файла журнала идентифицирует его формат, время создания или порядковый номер.

**Табл. 11-9.** Правила именования файлов журналов

Формат журнала	Период, охватываемый информацией в журнале	Имя файла
Microsoft IIS	По размеру файла	INETSVNN.LOG
	Неограниченный	INETSVNN.LOG
	Час	INFGMMDDCH.LOG
	День	INFGMMDD.LOG
	Неделя	INFGMMHH.LOG
Стандартный формат файла журнала NCSA	Месяц	INFGMM.LOG
	По размеру файла	NCSANN.LOG
	Неограниченный	NCSANN.LOG
	Час	NCFGMMDDCH.LOG
	День	NCFGMMDD.LOG
Расширенный формат файла журнала W3C	Неделя	NCFGMMHH.LOG
	Месяц	NCFGMM.LOG
	По размеру файла	EXTENDNN.LOG
	Неограниченный	EXTENDNN.LOG
	Час	EXFGMMDDCH.LOG
	День	EXFGMMDD.LOG
	Неделя	EXFGMMHH.LOG
	Месяц	EXFGMM.LOG

По умолчанию файлы журнала помещаются в папку `\%WinDir%\System32\LogFiles`. Однако это можно изменить и записывать файлы журнала, например, в папку `D:\LogFiles`. Независимо от того, в какой папке хранятся файлы журнала, в ней будут созданы вложенные папки для всех служб, регистрирующих сведения о доступе.

Синтаксис именования вложенных папок для узлов таков;

- `MSFTPSVCN`;
- `W3SVCN`;
- `SMTPSVCN`.

Здесь N — порядковый номер службы. Первый созданный сервер будет иметь порядковый номер 1, второй — 2 и т.д. Таким образом, вложенные папки с журналами узлов могут называться `W3SVC1`, `W3SVC2` и т. д.



**Примечание** Из-за частого удаления и добавления узлов на сервере может оказаться, что их порядковые номера не будут последовательными. Если вы удалили узел, IIS не может использовать его порядковый номер для нового узла.

## Включение ведения журналов для HTTP-, FTP- и SMTP-узлов

Теперь, когда вы знаете, как создаются и используются файлы журналов, мы подробно рассмотрим включение и конфигурирование ведения журналов.

### Конфигурирование стандартного формата файла журнала NCSA

Стандартный формат файла журнала NCSA применяется только для HTTP- и SMTP-узлов. Данный формат журнала следует использовать, если вам нужны лишь общие сведения о доступе к узлу. Журнал такого формата содержит записи небольшого размера, и это снижает требования к свободному дисковому пространству для ведения журнала.

Ведение стандартного журнала включается и конфигурируется так.

1. Запустите оснастку **Internet Information Services** и затем в левой панели раскройте узел нужного компьютера. Если компьютер не отображается, подключитесь к нему в



соответствии с инструкциями раздела «Подключение к другим серверам» главы 2.

2. Щелкнув значок требуемого HTTP- или SMTP-узла правой кнопкой, выберите в контекстном меню команду Properties (Свойства).
3. Пометьте флажок Enable Logging (Вести журнал) и затем в группе Active Log Format (Формат текущего журнала) выберите NCSA Common File Format (Общий формат файла журнала NCSA).
4. Щелкните Properties (Свойства). Откроется диалоговое окно NCSA Logging Properties (Свойства ведения журнала NCSA) (рис. 11-1).

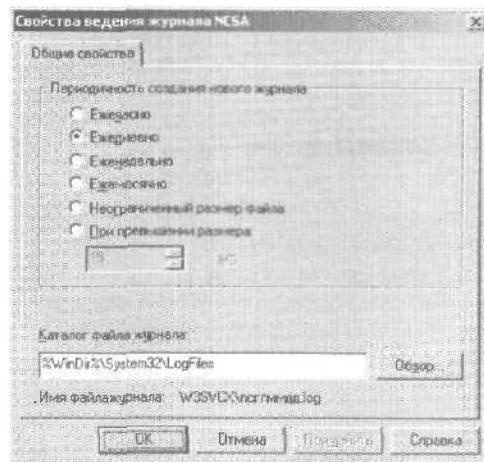


Рис. 11-1. Диалоговое окно NCSA Logging Properties (Свойства ведения журнала NCSA)

5. С помощью переключателей группы New Log Time Period (Периодичность создания нового журнала) задайте время создания нового файла журнала:
  - Hourly (Ежечасно) — каждый час;
  - Daily (Ежедневно) — в полночь;
  - Weekly (Еженедельно) — в полночь воскресенья;
  - Monthly (Ежемесячно) — в полночь последнего дня месяца;

- Unlimited File Size (Неограниченный размер файла) - файл журнала ведется постоянно, и им следует управлять вручную;
  - When File Size Reaches (При превышении размера) — по достижении заданного максимального размера файла (в Мб).
6. По умолчанию файлы журнала хранятся в папке `\\%WinDir%\System32\LogFiles`. Чтобы изменить это, введите в поле Log file directory (Каталог файла журнала) путь к нужной папке или щелкните Browse (Обзор) и выберите папку в открывшемся диалоговом окне.
  7. Дважды щелкните ОК. При необходимости будут автоматически созданы папка службы и файл журнала. Если у служб IIS нет разрешения Read/Write (Чтение/Запись) для папки с файлом журнала, появится сообщение об ошибке.

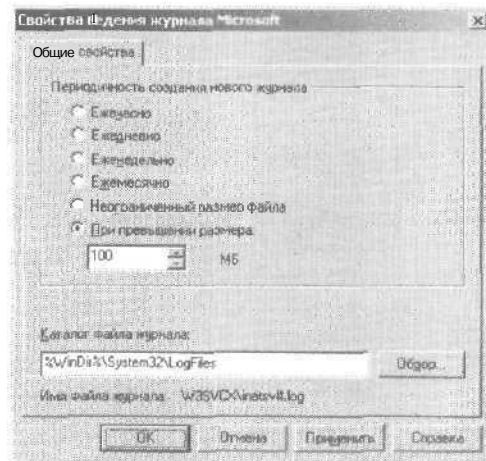
### Конфигурирование формата файла журнала Microsoft IIS

Формат журнала Microsoft IIS применяется для HTTP-, SMTP- и FTP-узлов. Данный формат используется, если не требуется подробной информации и нужно лишь чуть больше сведений о доступе, чем содержится в стандартном журнале. Записи такого журнала компактны, и это снижает требования к свободному дисковому пространству.

Ведение журнала формата Microsoft IIS включается и конфигурируется так.

1. Запустив оснастку Internet Information Services, в левой панели раскройте узел требуемого компьютера. Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2.
2. Щелкнув правой кнопкой значок требуемого HTTP-, FTP- или SMTP-узла, выберите в контекстном меню команду Properties (Свойства).
3. Поставьте флажок Enable Logging (Вести журнал) и затем в группе Active Log Format (Формат текущего журнала) поставьте переключатель в положение Microsoft IIS Log File Format.

4. Щелкните Properties (Свойства). Откроется диалоговое окно Microsoft Logging Properties (Свойства ведения журнала Microsoft) (рис. 11-2).



**Рис. 11-2.** Диалоговое окно Microsoft Logging Properties (Свойства ведения журнала Microsoft)

5. Переключателями группы New Log Time Period (Периодичность создания нового журнала) задайте время создания нового файла журнала:
- Hourly (Ежечасно) — каждый час;
  - **Daily** (Ежедневно) — в полночь;
  - Weekly (Еженедельно) — в полночь воскресенья;
  - Monthly (Ежемесячно) — в полночь последнего дня месяца;
  - **Unlimited** File Size (Неограниченный размер файла) — файл журнала ведется постоянно и им следует управлять вручную;
  - When File Size Reaches (При превышении размера) — по достижении заданного максимального размера файла (в Мб).
6. По умолчанию файлы журнала помещаются в папку %WinDir%\System32\LogFiles. Чтобы изменить это, введите в поле Log file directory (Каталог файла журнала)

путь к нужной папке или щелкните Browse (Обзор) и выберите папку в открывшемся диалоговом окне.

7. Дважды щелкните ОК. При необходимости будут автоматически созданы папка службы и файл журнала. Если у служб IIS нет разрешения Read/Write (Чтение/Запись) для папки с файлом журнала, появится сообщение об ошибке.

### Конфигурирование расширенного формата файла журнала W3C

Расширенный формат журнала W3C применяется для HTTP-, SMTP- и FTP-узлов. Он используется, если вам нужны лишь определенные и подробные сведения о доступе. Записи такого журнала могут быть очень большими, и это сильно повышает требования к свободному дисковому пространству для ведения журнала. Кроме того, занесение длинных записей в журнал может негативно сказаться на производительности перегруженного сервера.

Журнал расширенного формата W3C включается и конфигурируется так.

1. Запустив оснастку Internet Information Services, в левой панели раскройте узел требуемого компьютера. Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2.
2. Щелкнув правой кнопкой значок требуемого HTTP-, FTP- или SMTP-узла, выберите в контекстном меню команду Properties (Свойства).
3. Пометьте флажок Enable Logging (Вести журнал) и затем в группе Active Log Format (Формат текущего журнала) поставьте переключатель в положение W3C Extended Log File Format.
4. Щелкните Properties (Свойства). Откроется диалоговое окно Extended Logging Properties (Расширенные свойства ведения журнала) (рис. 11-3).
5. С помощью переключателей группы New Log Time Period (Периодичность создания нового журнала) задайте время создания нового файла журнала:
  - Hourly (Ежечасно) — каждый час;

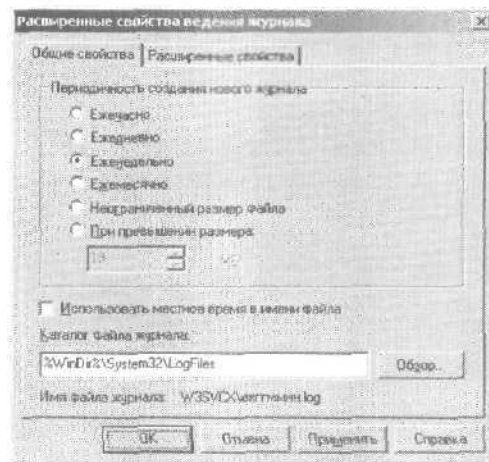


Рис. 11-3. Диалоговое окно Extended Logging Properties (Расширенные свойства ведения журнала)

- Daily (Ежедневно) — в полночь;
  - Weekly (Еженедельно) — в полночь воскресенья;
  - Monthly (Ежемесячно) — в полночь последнего дня месяца;
  - Unlimited File Size (Неограниченный размер файла) — файл журнала ведется постоянно и им следует управлять вручную;
  - **When File Size Reaches** (При превышении размера) — по достижении заданного максимального размера файла (в Мб).
6. По умолчанию новые файлы расширенного журнала создаются с использованием времени по Гринвичу, т. е. если не указано иное, ежедневный, еженедельный и ежемесячный журналы будут создаваться в 00:00 GMT. Чтобы новые файлы создавались по локальному времени, **поставьте флажок Use Local Time For File Naming And Rollover** (Использовать местное время в имени файла).
7. По умолчанию файлы журнала помещаются в папку `%WinDir%\System32\LogFiles`. Чтобы изменить это, введите в поле Log file directory (Каталог файла журнала)

путь к нужной папке или щелкните Browse (Обзор) и выберите папку в открывшемся диалоговом окне.

8. Перейдите на вкладку Extended Properties и укажите поля, которые следует заполнять. Обычно это:
  - Date\Time (Дата\Время);
  - Client IP Address/Server IP Address (IP-адрес клиента/Адрес IP сервера);
  - Method (Метод);
  - URI Stem/URI Query (Ресурс URI/Запрос URI);
  - Protocol Status (Состояние протокола);
  - Bytes Sent/Bytes Received (Передано байт/Получено байт);
  - User Agent (Агент пользователя);
  - Cookie (Объект Cookie);
  - Referer (Источник ссылки).
9. Дважды щелкните ОК. При необходимости будут автоматически созданы папка службы и файл журнала. Если у служб IIS нет разрешения Read/Write (Чтение/Запись) для папки с файлом журнала, появится сообщение об ошибке.

### Конфигурирование журнала формата ODBC

Журналы формата ODBC могут вестись для HTTP-, SMTP- и FTP-узлов. Используйте их, если требуется заносить информацию прямо в ODBC-совместимую БД. При ведении ODBC-журнала вам потребуется трассировочное ПО, способное считывать информацию из БД. Записи будут компактными и будут считываться гораздо быстрее, чем из обычного файла журнала.

Журнал формата ODBC включается и конфигурируется так.

1. Создайте БД с помощью ODBC-совместимого ПО. Если IIS смогут подключиться к ней по ODBC-подключению, БД не требуется находиться на IIS-сервере. Для узлов с небольшим и средним трафиком можно использовать Microsoft Access, а для узлов с большим трафиком — более устойчивое решение, например SQL Server 2000.

2. В БД создайте таблицу для записей, включающую поля с типами данных из табл. 11-8. Создать такую таблицу поможет сценарий LOGTEMP.SQL.
3. Затем создайте DSN, при помощи которого ИС сможет подключаться к БД. Возможно, для установления соединения с БД вы захотите задействовать системное DSN. При работе с SQL Server укажите способ проверки подлинности учетной записи. Если вы выберете проверку средствами Microsoft Windows NT, указанная вами в ИС учетная запись должна иметь разрешение на запись в БД. Выбрав проверку средствами SQL Server, укажите имя и пароль для доступа к БД.
4. Теперь включите ведение журнала узла и в группе Active Log Format (Формат текущего журнала) выберите ODBC Logging (Ведение журнала ODBC). При конфигурировании ведения журнала вам потребуется указать имя DSN, имя таблицы и реквизиты для подключения к БД.

Ниже рассказывается о конфигурировании ведения ODBC-журнала с помощью SQL Server 2000 и ИС. Предполагается, что вы обладаете достаточным опытом администрирования БД SQL Server 2000. Подробнее см. книгу «Microsoft Windows 2000. Справочник Администратора».

#### Создание БД и таблицы журнала в SQL Server 2000

В качестве сервера для ведения журнала можно использовать SQL Server. Вам потребуется создать БД и сконфигурировать таблицу журнала. БД создается так.

1. Запустите Enterprise Manager и затем в левой панели консоли раскройте узел группы требуемого сервера.
2. Раскройте узел требуемого сервера и, если надо, введите реквизиты для подключения и подсоединитесь.
3. Щелкнув правой кнопкой папку Databases, выберите в контекстном меню команду New Database. Откроется диалоговое окно Database Properties.
4. Перейдите на вкладку General и задайте имя БД как LoggingDB.
5. Щелкните ОК, чтобы создать базу данных.

Теперь найдите сценарий LOGTEMP.SQL. Обычно он находится в папке %WinDir%\System32\Inetsrv. Отредактируйте

сценарий и задайте в нем имя таблицы для журнала узла. Например, если вам нужно назвать таблицу HTTPLog, измените сценарий следующим образом:

```
use LoggingDB

create table HTTPLog (
  ClientHost varchar(255),
  username varchar(255),
  LogTime datetime,
  service varchar(255),
  machine varchar(255),
  serverip varchar(50),
  processingtime int,
  bytesrecvd int,
  bytessent int,
  servicestatus int,
  win32status int,
  operation varchar(255),
  target varchar(255),
  parameters varchar(255)
)
```

Обновив сценарий, запустите Query Analyzer. Щелкните кнопку Load SQL Script на панели инструментов и укажите расположение сценария. Затем запустите сценарий, щелкнув Run. По завершении выполнения сценария в БД LoggingDB будет создана новая таблица. Убедитесь, что для подключения к БД используется учетная запись с правами администратора.

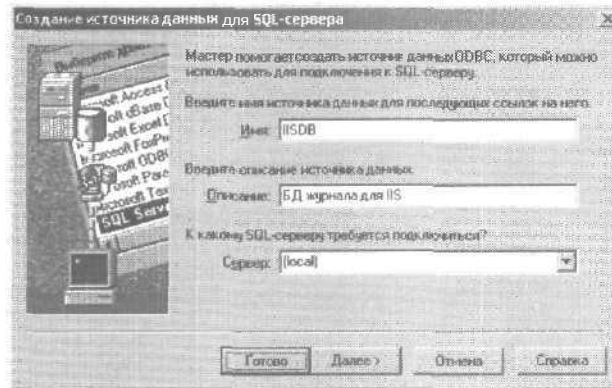
#### Создание DSN для SQL Server 2000

Создав БД и таблицу журнала, сконфигурируйте IIS для подключения к этой БД, создав DSN.

1. Раскройте меню Start\Settings (Пуск\Настройки) и выберите Control Panel (Панель управления). В открывшемся окне дважды щелкните Administrative Tools (Администрирование) и затем —Data Sources (ODBC) [Источники данных (ODBC)].
2. На вкладке System DSN (Системный DSN) щелкните Add (Добавить). Откроется диалоговое окно Create New Data Source (Создание нового источника данных).
3. В списке Driver Selection (Выберите драйвер) выберите SQL Server и щелкните Finish (Готово). Откроется диа-

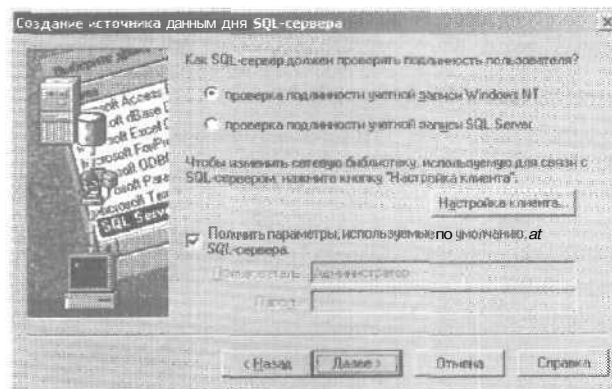


ловое окно Create A New Data Source To SQL Server (рис. 11-4).



**Рис. 11-4.** Диалоговое окно Create A New Data Source To SQL Server (Создание источника данных для SQL-сервера)

4. В поле **Name** (Имя) наберите имя **DSN**, например **IISDB**.
5. В поле **Server** (Сервер) наберите имя компьютера SQL Server, к которому нужно подключиться. Если SQL Server выполняется на одном компьютере с IIS, выберите (Local). Щелкните **Next** (Далее).



**Рис. 11-5.** Выбор метода проверки подлинности учетной записи для подключения к SQL Server

6. Теперь укажите метод проверки подлинности учетной записи для подключения к SQL Server (рис. 11-5). Если вы выберете проверку средствами Microsoft Windows NT, указанная вами в IIS учетная запись должна иметь разрешение на запись в БД. Выбрав проверку средствами SQL Server, укажите имя и пароль для доступа к БД.
7. Щелкните Next (Далее) и затем — Finish (Готово). Если Windows не сможет установить соединение с БД, проверьте введенные вами сведения. Возможно, вам также потребуется убедиться, что учетная запись имеет нужные разрешения доступа к БД.

#### **Включение и конфигурирование ведения ODBC-формата в IIS**

Журнал формата ODBC включается и конфигурируется так.

1. Запустив оснастку Internet Information Services, раскройте в левой панели узел нужного компьютера. Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2.
2. Щелкните правой кнопкой значок требуемого HTTP-, FTP- или SMTP-узла и выберите в контекстном меню команду Properties (Свойства).
3. Поставьте флажок Enable Logging (Вести журнал) и затем в группе Active Log Format (Формат текущего журнала) поставьте переключатель в положение ODBC Logging (Ведение журнала ODBC).
4. Щелкните Properties (Свойства). Откроется диалоговое окно ODBC Logging Properties (Свойства ведения журнала ODBC) (рис. 11-6).
5. В поле ODBC Data Source Name (DSN) [Источник данных ODBC (DSN)] наберите имя созданного вами источника данных.
6. В поле Table (Таблица) наберите имя таблицы журнала.
7. При проверке подлинности учетной записи средствами Windows введите в полях User Name (Имя пользователя) и Password (Пароль) имя и пароль для подключения к БД.

8. Дважды щелкните ОК, чтобы сохранить сделанные изменения.

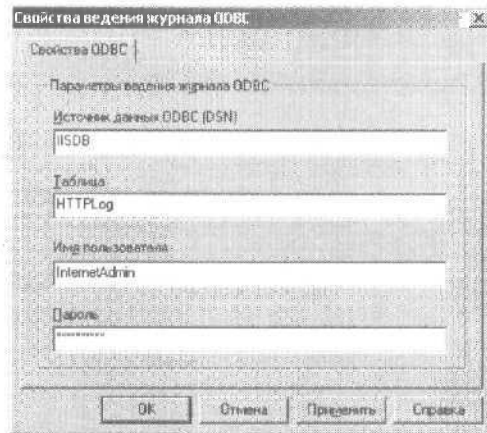


Рис. 11-6. Диалоговое окно ODBC Logging Properties (Свойства ведения журнала ODBC)

### Выключение ведения журнала

Если вам не нужны сведения о доступе пользователей к какому-либо узлу, отключите ведение журнала для этого узла.

1. Запустив оснастку Internet Information Services и затем в левой панели раскройте узел требуемого компьютера. Если компьютер не отображается, подключитесь к нему в соответствии с инструкциями раздела «Подключение к другим серверам» главы 2.
2. Щелкните правой кнопкой значок требуемого HTTP-, FTP- или SMTP-узла и выберите в контекстном меню команду Properties (Свойства).
3. Снимите флажок Enable Logging (Вести журнал) и щелкните ОК.

## Глава 12

# Оптимизация IIS и метабаза

В предыдущих главах мы обсуждали методы мониторинга IIS и оптимизации производительности оборудования сервера. Здесь мы рассмотрим оптимизацию IIS и связанных с ними служб. Я расскажу, как повышать производительность IIS, настраивать автоматический перезапуск служб IIS и получать максимальную отдачу от IIS-приложений. Кроме того, мы обсудим управление US с помощью системного реестра Windows и метабазы IIS.

В системном реестре Microsoft Windows хранятся конфигурационные параметры ОС, оборудования и всех установленных на сервере приложений, включая IIS. Метабаза содержит специфические конфигурационные параметры узлов, развернутых на конкретном WWW-сервере. Большинство параметров доступны в диалоговых окнах свойств IIS, но для изменения некоторых из них нужно редактировать системный реестр и метабазу. К таким параметрам относятся сложные переменные — изменять их значение следует лишь при необходимости.

### Методы повышения производительности IIS

Рассмотрим методы повышения производительности IIS. Основное внимание уделим снижению времени реакции служб IIS, оптимизацию оборудования сервера мы обсуждать не будем.

#### Удаление ненужных приложений и служб

Один из самых очевидных способов повысить производительность IIS — устранить утечки ресурсов на сервере. Начать можно с удаления приложений, влияющих на произво-

дительность IIS. Скажем, Microsoft SQL Server, Microsoft Exchange Server, службы доступа к файлам и принтерам, службы UNIX можно перенести на отдельный сервер. Если приложение перенести нельзя, попробуйте запускать его только в периоды относительно низкой активности системы. Например, ежедневное резервное копирование данных сервера можно выполнять поздно ночью, когда активность пользователей низка.

Кроме того, утечку ресурсов могут создавать системные службы. Ненужные службы следует остановить и настроить для запуска вручную. Перед остановкой службы проверьте зависимости и убедитесь, что ваши действия не окажут негативного влияния на работу сервера.

При работе с выделенным IIS-сервером обычно не нужны следующие службы:

- Alerter (Оповещатель);
- ClipBook (Сервер папки обмена);
- Computer Browser (Обозреватель компьютеров);
- DHCP Client (DHCP-клиент);
- DHCP Server (DHCP-сервер);
- Fax Service (Служба факсов);
- File Replication (Репликация файлов);
- Infrared Monitor (Монитор инфракрасной связи);
- Internet Connection Sharing (Общий доступ к подключению Интернета);
- Messenger (Служба сообщений);
- NetMeeting Remote Desktop Sharing;
- Network DDE (Служба сетевого DDE);
- Network DDE DSDM (Диспетчер сетевого DDE);
- NWLink NetBIOS;
- NWLink IPX/SPX (NWLink IPX/SPX/NetBIOS-совместимый транспортный протокол);
- Print Spooler (Диспетчер очереди печати);
- TCP/IP NetBIOS Helper Service (Служба поддержки TCP/IP NetBIOS);
- Telephony (Телефония);

- Telnet;
- Uninterruptible Power Supply (Источник бесперебойного питания).

### Оптимизация использования содержимого

Время реакции сервера тесно связано с содержимым развернутых на нем Web-узлов. Оптимизация использования содержимого часто дает заметный выигрыш в производительности. IIS поддерживает статичное (передаваемое прямо клиенту) и динамическое (предварительно обрабатываемое сервером) содержимое. Динамическое содержимое создает нагрузку на сервер, и для ее снижения лучше перейти на использование статичного содержимого.



**Примечание** Я не призываю заменить все динамическое содержимое статичным. Динамически генерируемое содержимое — мощное средство для разработки гибко настраиваемых и полнофункциональных узлов, но использовать его без особых на то причин не стоит.

Работая со статичным содержимым, при каждой возможности задавайте заголовки срока действия. Это позволит хранить связанные файлы в кэше клиентской системы и, если исходное содержимое не менялось, при повторных обращениях пользователя к узлу заметно повысить производительность. Подробнее о настройке заголовков срока действия см. раздел «Изменение содержимого Web-узла и HTTP-заголовков» главы 4.

При работе с динамическим содержимым рекомендуется ограничить использование CGI-приложений. Они требуют больше ОЗУ и времени процессора, чем их ISAPI- и ASP-аналоги, и поэтому CGI-приложения следует преобразовать для применения ISAPI или ASP. По возможности выбирайте приложения ISAPI, а не ASP: хотя часто разработка первых занимает больше времени, выполняются они быстрее. Кроме того, при использовании ISAPI- и ASP-приложений рекомендуется основную массу операций по обработке данных выполнять на клиентской системе. Это уменьшает потребность сервера в ресурсах и заметно ускоряет реакцию приложения. Пример такого перемещения — клиентский сценарий, проверяющий данные формы перед их отправкой

на сервер. Это решение снижает количество циклов обмена информацией между сервером и клиентом, тем самым серьезно повышая общую производительность приложения.

Есть и другие способы увеличить производительность обработки **содержимого**.

- **Проанализировать способ организации содержимого на жестких дисках.** Обычно связанные файлы содержимого следует хранить на одном логическом диске. Это повышает производительность кэширования файлов IIS.
- **Периодически дефрагментировать жесткие диски.** Со временем содержимое диска фрагментируется, что снижает производительность операций чтения-записи. Чтобы устранить эту проблему, периодически дефрагментируйте жесткие диски своего сервера. Многие утилиты дефрагментации дисков позволяют автоматизировать этот процесс и настроить его для запуска по расписанию, без вмешательства администратора.
- **Уменьшить размер файлов содержимого.** Чем больше размер файла, тем больше времени требуется на передачу его клиенту. Уменьшив размер HTML- и ASP-страниц путем оптимизации их кода, вы повысите производительность и ускорите реакцию Web-сервера. Значительную часть полосы пропускания занимают мультимедиа-файлы. При любой возможности сжимайте файлы изображений, аудио- и видеофайлы.
- **Разместить файлы журнала отдельно от файлов содержимого.** Ведение журнала на перегруженном сервере может сильно замедлить его реакцию. Лучше хранить журналы доступа и файлы содержимого на разных физических дисках. При этом операции записи на диск, связанные с ведением журнала, будут выполняться отдельно от операций чтения-записи файлов содержимого, что может заметно ускорить реакцию сервера.
- **Регистрировать только необходимые сведения.** Регистрация большого числа сведений на перегруженном сервере может серьезно снизить производительность системы. Расширенный формат журнала W3C позволяет уменьшить нагрузку по регистрации сведений и регистрировать лишь информацию, необходимую для создания

отчетов. Независимо от формата журнала нагрузку по его ведению можно уменьшить, поместив однотипное содержимое в одну папку и отключив ведение журнала для не требующих того папок. Например, поместите все файлы изображений в папку Images и затем отключите для нее ведение журнала.

### Оптимизация ISAPI- и ASP-приложений

Неверно сконфигурированные и плохо оптимизированные приложения могут стать причиной значительной утечки ресурсов IIS-сервера. Чтобы достичь максимальной производительности сервера, нужно оптимизировать настройки приложений.

- **Включите кэширование приложений ISAPI.** IIS может кэшировать приложения ISAPI в памяти, обеспечивая к ним быстрый доступ. Для управления кэшированием служит параметр CacheISAPI метабазы.
- **Правильно организуйте наполнение и очистку буфера приложениями.** Буферизация позволяет собрать в буфере весь вывод приложения перед передачей его клиенту, что уменьшает сетевой трафик и время реакции. Однако данные выводятся пользователю лишь по завершении обработки страницы. В итоге может создаться неверное впечатление о скорости реакции узла. Для управления буферизацией данных приложениями служит параметр AspBufferingOn метабазы.
- **Отключите отладку приложений.** Отладка приложений значительно снижает производительность IIS, и использовать ее следует лишь для устранения неполадок. В остальных ситуациях отладку рекомендуется отключить. Для управления отладкой служит параметр AppAllowDebugging метабазы.
- **Запускайте изолированные приложения только при необходимости.** Приложения, выполняющиеся в групповом процессе и вне процессов, используют дополнительные системные ресурсы и имеют чуть более низкую производительность, чем внутрипроцессные. Подробнее см. раздел «Использование и выполнение приложений» главы 4.
- **Правильно настройте управление сеансами.** Одновременно с изменением назначения сервера должен меняться



ся и подход к управлению сеансами. По умолчанию управление сеансами включено для всех приложений. Не используя в своих приложениях сеансы, вы зря тратите ресурсы системы. Рекомендуется по умолчанию сеансы отключить, а затем включить для конкретных приложений. Для управления сеансами служат параметры `AspAllowSessionState`, `AspSessionMax` и `AspSessionTimeout` метабазы.

- **Задайте разумное время ожидания ответа сеанса.** Значение срока ожидания чрезвычайно важно для определения объема ресурсов, используемого при управлении сеансами. Изменять значение этого параметра следует очень аккуратно. По истечении определенного срока сеанс должен закрываться. Для управления временем ожидания сеанса служит параметр `AspSessionTimeout` метабазы.
- **Задайте разумное время ожидания сценария и подключения.** Через определенное время ASP-сценарии и пользовательские подключения должны прекращать ожидать ответ на свои запросы и действия. По умолчанию срок ожидания ASP-сценариев — 90 секунд, а пользовательских подключений — 15 минут. «Мертвые» сценарии и активные пользовательские подключения занимают ресурсы сервера и могут увеличить время его реакции. Чтобы этого избежать, задайте подходящее время ожидания, основываясь на том, как используется Web-узел. Для управления временем ожидания сценариев и подключений служат параметры `AspScriptTimeout` и `ConnectionTimeout` метабазы.

#### Оптимизация кэширования и организации очередей IIS

IIS управляет ресурсами с помощью различных кэшей и очередей, постоянно находящихся в памяти. При широком использовании динамического содержимого и большом трафике к узлу рекомендуется оптимизировать конфигурацию этих кэшей и очередей для соответствия требованиям вашей среды. Вот варианты такой оптимизации.

- **Увеличить очередь соединений, использующих директиву Keep Alive протокола HTTP.** При использовании данной директивы службы IIS помещают все подключения пользовательского HTTP-сеанса в очередь соедине-

ний. По умолчанию размер очереди — 15 соединений. Если это не соответствует нашим нуждам, измените значение параметра `ServerListenBackLog` метабазы. Обычно рекомендуется задать максимальное число запросов на подключение, которое должен обрабатывать сервер.

- Включить регулирование потоков. Функция регулирования потоков динамически управляет числом параллельно выполняющихся потоков, обеспечивая своевременную обработку запросов. Если регулирование потоков включено, оно используется, когда процессор загружен менее чем на 50 или более чем на 80%. В первом случае, когда нагрузка низка или имеются заблокированные потоки, IIS увеличивает число активных потоков, обеспечивая обслуживание дополнительных запросов. Если загруженность процессора очень высока, IIS отключает потоки, снижая число операций на переключение контекста. Для управления регулированием потоков служат параметры `AspThreadGateEnabled`, `AspThreadGateLoadLow` и `AspThreadGateLoadHigh` метабазы.
- Изменить параметры файлового кэша IIS. По умолчанию IIS использует до 50% физической памяти сервера. Это гарантирует приемлемую производительность IIS, когда на сервере параллельно запущены другие приложения. Если IIS выполняется на выделенном сервере или на компьютере с большим объемом ОЗУ, можно увеличить значение данного параметра и предоставить IIS больше памяти. Для управления файловым кэшем IIS создайте в реестре Windows параметр `MemCacheSize` и задайте его значение.
- Изменить максимальный размер кэшируемых файлов. По умолчанию IIS кэширует файлы размером не более 256 Кб. При наличии часто просматриваемых файлов данных или мультимедийных большого размера можно увеличить значение этого параметра и разрешить IIS кэшировать такие файлы. Помните, кэширование файлов размером свыше 256 Кб не даст заметного прироста производительности. Дело в том, что нагрузка по чтению маленьких файлов с диска выше, чем из кэша, но в случае с большими файлами эта нагрузка может влиять на производительность незначительно. Для управления мак-

симальным размером кэшируемых файлов создайте в реестре Windows параметр `MaxCachedFileSize` и задайте его значение.

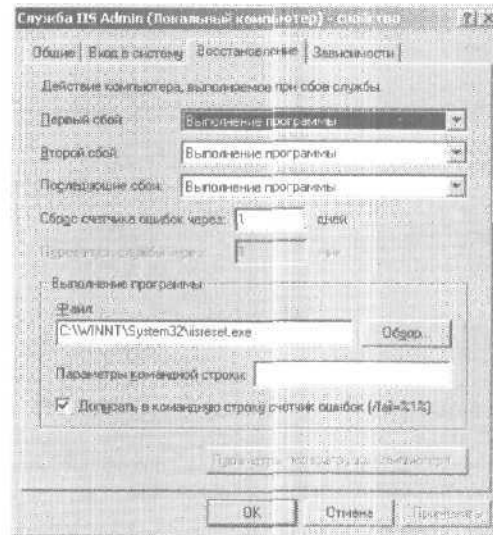
- **Изменить продолжительность нахождения ресурсов в кэше.** По умолчанию IIS удаляет из кэша все ресурсы, не просматривавшиеся последние 30 секунд. При наличии большого объема ОЗУ на сервере это значение можно увеличить, чтобы файлы не удалялись из кэша так быстро. Для управления TTL (время существования) кэшируемых ресурсов создайте в реестре Windows параметр `Windows ObjectCacheTTL` и задайте его значение.
- **Изменить параметры кэша шаблонов ASP.** Кэш шаблонов ASP определяет количество кэшируемых в памяти ASP-страниц. По умолчанию IIS кэширует не больше 250 файлов, что не всегда достаточно для узлов со множеством ASP-страниц. Записи кэша шаблонов могут ссылаться на одну или несколько записей кэша обработчика сценариев ASP. Для управления кэшированием служит параметр `AspScriptFileCacheSize` метабазы.
- **Изменить параметры кэша обработчика сценариев.** Кэш обработчика сценариев ASP — это область памяти, к которой напрямую могут обращаться используемые IIS обработчики сценариев, и поэтому IIS предпочтительнее извлекать информацию именно отсюда. По умолчанию кэш обработчика сценариев может содержать до 125 элементов. Для управления им служит параметр `AspScriptEngineCacheMax` метабазы.

### Настройка автоматического перезапуска IIS

Основным задачам администрирования IIS посвящена глава 2: в ней рассказывается об управлении службами и использовании утилиты IIS Reset. Для достижения максимальной производительности IIS рекомендуется настроить службу IIS Admin для автоматического запуска утилиты IIS Reset при возникновении проблем. Как правило, это позволяет IIS автоматически восстановить конфигурацию и продолжить работу.

Чтобы настроить автоматический перезапуск IIS, сделайте следующее.

1. В оснастке Computer Management (Управление компьютером) подключитесь к требуемому компьютеру.
2. Раскройте узел Services And Applications (Службы и приложения) и щелкните значок Services (Службы).
3. Щелкните значок службы IIS Admin Service (Служба IIS Admin) правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
4. Перейдите на вкладку Recovery (Восстановление), а затем в списках First Failure (Первый сбой), Second Failure (Второй сбой) и Subsequent Failure (Последующие сбои) выберите Run A File (Выполнение программы) (рис. 12-1).



**Рис. 12-1.** Настройка службы IIS Admin для запуска утилиты IIS Reset

5. В поле File (Файл) группы Run File (Выполнение программы) введите `\\%SystemRoot%\System32\IISRESET.EXE`.
6. Щелкните OK.

## Управление параметрами реестра MS

В системном реестре Microsoft Windows хранятся конфигурационные параметры ОС, оборудования и всех установлен-

ных на сервере приложений. Корректные значения параметров системного реестра важны для нормального функционирования ОС. Вносить изменения в реестр следует, только четко зная, как это повлияет на работу системы.

### Работа с системным реестром

Настроечные параметры в реестре хранятся в виде разделов и значений в одном из корневых разделов. Корневой раздел определяет порядок использования вложенных разделов и параметров. Существующие корневые разделы содержат:

- **HKEY\_CLASSES\_ROOT** — параметры конфигурационной настройки приложений и файлов; гарантирует, что при открытии файла с помощью OLE или из Windows Explorer (Проводник) будет запущено соответствующее приложение;
- **HKEY\_CURRENT\_CONFIG** - сведения об используемом профиле оборудования;
- **HKEY\_CURRENT\_USER** - конфигурационные параметры рабочей среды текущего пользователя;
- **HKEY\_LOCAL\_MACHINE** — конфигурационные параметры уровня системы;
- **HKEY\_USERS** — параметры учетных записей пользователя по умолчанию и других учетных записей в виде профилей.

На первом уровне вложенности в корневых разделах находятся основные разделы. Они организованы в древовидную структуру и управляют различными параметрами системы, пользователя и рабочей среды приложений. Параметры службы IIS Admin хранятся в разделе **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\InetInfo\Parameters**.

В нашем случае имя раздела — **Parameters**. Параметры в этом или любом другом разделе реестра имеют три составных части; имя, тип и значение. Для представления числовых параметров часто применяется шестнадцатеричный формат. Шестнадцатеричные значения включают префикс **0x** — например, **0x19** соответствует числу 25 в десятичном представлении. В следующем примере тип параметра **ListenBackLog** — **REG\_DWORD**, а значение - **0x19**:

**ListenBackLog : REG\_DWORD : 0x19**

**REG\_DWORD** — лишь один из возможных типов параметров. Полный список типов параметров таков:

- **REG\_BINARY** — двоичное значение в кодировке base-2 (0 или 1);
- **REG\_DWORD** — значение DWORD, состоящее из шестнадцатеричных данных; максимальный размер — не более 4 байт;
- **REG\_SZ** — строковое значение, содержащее последовательность символов;
- **REG\_EXPAND\_SZ** — дополняемое строковое значение, обычно используется для хранения пути к папке;
- **REG\_MULTI\_SZ** — многострочное значение.

Основная утилита для работы с системным реестром Windows — Registry Editor (Редактор реестра, REGEDT.EXE). Чтобы запустить ее, раскройте меню Start (Пуск) и выберите команду Run (Выполнить). Затем в поле Run (Выполнить) введите *REGEDT32* и щелкните ОК. Опытные администраторы управляют реестром с помощью сценариев Windows, позволяющих создавать, изменять и удалять параметры и разделы реестра. Следующий сценарий на VBScript изменяет значение параметра ListenBackLog:

```
'Инициализируем переменные и объекты
Dim Path
Path =
HKLM\SYSTEM\CurrentControlSet\Services\Inetinfo\Parameters\
Set ws = WScript.CreateObject("WScript.Shell")

'Считываем и выводим значение параметра
val = ws.RegRead(Path & "ListenBackLog")
WScript.Echo "Original ListenBackLog value: " & val

'Записываем и выводим новое значение параметра
retVal = ws.RegWrite(Path & "ListenBackLog", 50, "REG_DWORD")

val = ws.RegRead(Path & "ListenBackLog")
WScript.Echo "Updated ListenBackLog value: " & val
```



**Примечание** Подробное обсуждение сценариев выходит за рамки этой книги. Хороший источник информации по данной теме — книга «Windows 2000 Scripting Bible» Уиль-

яма Р. Станека (William R. Stanek), вышедшая в июле 2000 г. в издательстве IDG Books.

### Управление IIS с помощью реестра

Настроечные параметры IIS хранятся в разделе `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Inet-info\Parameters` реестра. В плане управления IIS особый интерес представляют следующие параметры этого раздела.

- **CacheSecurityDescriptor** определяет, кэшируются ли дескрипторы безопасности для файловых объектов. Значение 1 (по умолчанию) — кэширование включено, 0 — отключено. В первом случае при кэшировании файловых объектов сохраняются дескрипторы безопасности. Пока файл находится в кэше, службам IIS не требуется повторно обращаться к файлу для определения прав доступа новых пользователей. Параметр наиболее полезен для узлов, проверяющих подлинность пользователей, и бесполезен на узлах с анонимным доступом.
- **CheckCertRevocation** определяет, проверяет ли IIS клиентский сертификат по списку отозванных сертификатов. Если вы выдаете собственные сертификаты и осуществляете их локальную проверку, то, возможно, стоит включить эту функцию. Если нет, проверку лучше отключить, что и задано по умолчанию. Для включения функции задайте этому параметру значение 1.
- **DisableMemoryCache** определяет, включено ли кэширование памяти IIS. По умолчанию оно включено (т. е. его значение 0). Отключать кэширование памяти следует только для целей тестирования или разработки.
- **ListenBackLog** задает максимальное число активных подключений в очереди соединений. По умолчанию — 15 подключений; допустимый диапазон значений — от 1 до 250 подключений.
- **MaxCachedFileSize** задает максимальный размер файла, помещаемого в кэш. Файлы большего размера не кэшируются. По умолчанию — 262 144 байта (256 Кб).
- **MaxConcurrency** задает максимально допустимое число потоков, которые могут параллельно выполняться на одном процессоре при наличии ожидающих операций вво-

да-вывода. Значение по умолчанию — 0 — позволяет службам IIS управлять числом потоков для каждого процессора. Можно задать и конкретное значение.

- **MaxPoolThreads** задает число потоков пула, обрабатываемых одним процессором. Каждый поток пула ожидает сетевой запрос к CGI-приложению и обрабатывает его. Этот параметр не влияет на потоки приложений ISAPI. По умолчанию задано 4. Для однопроцессорных систем это означает, что одновременно могут выполняться только четыре CGI-приложения.
- **MemCacheSize** задает максимальный объем ОЗУ, используемый IIS для кэширования файлов. Если службам IIS не требуется вся выделенная им память, она будет передана другим приложениям. По умолчанию IIS использует 50% доступного объема ОЗУ. Допустимый диапазон значений — от 0 Мб до общего объема ОЗУ компьютера в мегабайтах.
- **ObjectCacheTTL** задает срок (в миллисекундах) хранения объектов в памяти. Объекты, не использовавшиеся в течение заданного срока, удаляются из памяти. Значение по умолчанию — 30 секунд (300 000 мсек).
- **PoolThreadLimit** задает максимальное число потоков пула, создаваемых на сервере, т. е. ограничивает общее количество всех потоков IIS. Значение по умолчанию равно двукратному размеру физической памяти в мегабайтах.

#### Управление службой Indexing Service с помощью реестра

Параметры службы Indexing Service хранятся в разделе HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex реестра. Подробнее об этом см. раздел «Основы работы со службой Indexing Service» главы 9.

Параметры служб World Wide Web Publishing, File Transfer Protocol и Simple Mail Transfer Protocol хранятся в разделе HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\ИмяСлужбы\Parameters реестра. Здесь *ИмяСлужбы* — это наименование требуемой службы, например:

- **MSFTPSVC** — служба File Transfer Protocol;



- **W3SVC** - служба World Wide Web Publishing;
- **SMTPSVC** — служба Simple Mail Transfer Protocol.

Большинство параметров этих разделов используются только службами IIS, однако вам может потребоваться изменить значение параметра **AllowGuestAccess**, определяющего, разрешен ли гостевой доступ к службам Интернета. По умолчанию он разрешен; чтобы отключить его, задайте **AllowGuestAccess** значение 0.

При работе со службой World Wide Web Publishing (Служба веб-публикаций) вам может потребоваться изменить значения следующих параметров.

- **SSIEnableCmdDirective** определяет, могут ли Web-страницы генерировать серверные операторы **include**, запускающие внешние программы. По умолчанию такая возможность отключена (т. е. задано значение 0), что обычно и требуется. Разрешив выполнение внешних программ из Web-страниц, вы можете сделать свой сервер уязвимым для атак злоумышленников.
- **TryExceptDisable** определяет, включено ли кэширование исключений для отладки. По умолчанию оно отключено (т. с. задано значение 0). Если кэширование исключений включено (т. с. задано 1), при возникновении любого исключения сервер останавливается и позволяет разработчику отладить приложение, вызвавшее исключение.
- **UploadReadAhead** при передаче клиентом информации на сервер определяет объем данных, считываемых сервером перед передачей управления обрабатывающему их приложению. По умолчанию — 48 Кб.
- **UsePoolThreadForCGI** определяет, могут ли CGI-запросы использовать общие потоки. По умолчанию это разрешено (т. с. задано 1). Если же это запрещено, CGI-запросы не используют пул соединений, и значение параметра **MaxPoolThreads** раздела **Inetinfo** на них не распространяется.

### Управление протоколом SSL с помощью реестра

Настроечные параметры протокола Secure Sockets Layer хранятся в разделе **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL** реестра.

Возможно, вам потребуется изменить значения следующих параметров.

- **EventLogging** определяет, будут ли в журнал Web-узла включаться записи о SSL-подключениях. По умолчанию такая возможность включена (т. е. задано 1). Чтобы отключить ее, задайте параметру значение 0.
- **ServerCacheTime** определяет продолжительность SSL-сеанса в миллисекундах. Создание SSL-сеанса требует много времени и ресурсов системы. Если вы предполагаете, что средняя продолжительность сеанса будет больше продолжительности, заданной по умолчанию, измените значение ServerCacheTime. По умолчанию длительность SSL-сеанса — 5 минут (300 000 миллисекунд). По окончании SSL-сеанса необходимо создать новый сеанс.

## Управление параметрами метабазы IIS

Метабаза — один из наиболее важных компонентов установки IIS. Здесь хранятся конфигурационные параметры узлов и виртуальных серверов, а также параметры по умолчанию узлов и виртуальных серверов: например, основные свойства WWW.

### Просмотр и редактирование метабазы

Метабаза IIS — это структурированный файл с именем METABASE.BIN, хранящийся в папке \Inetsrv. Редактировать его напрямую не следует, но есть масса иных способов просмотреть и изменить его содержимое. В разделе «Настройка резервного копирования и восстановления IIS» главы 2 рассказывалось о создании резервных копий и восстановлении метабазы в состояние на определенный момент времени. Кроме того, в предыдущих главах обсуждалось изменение конфигурационных параметров IIS стандартными средствами администрирования, например, из оснастки Internet Information Services. Любые изменения параметров, сделанные при помощи обычных административных утилит, отражаются в метабазе IIS.

Содержимое метабазы также можно просматривать и редактировать в специально сконфигурированном редакторе. В комплекте ресурсов Windows 2000 есть утилита Metabase Editor (METAEDIT.EXE). Чтобы установить ее, запустите

файл **SETUP.EXE** из папки **\Apps\Metaedit** компакт-диска комплекта ресурсов Windows 2000 и следуйте инструкциям на экране. Вы увидите, что эта утилита практически не отличается от Registry Editor (**REGEDT.EXE**).

Конфигурационные параметры организованы в иерархичную структуру со стандартными правилами именования, согласно которым каждый параметр находится в определенном разделе и по определенному пути (рис. 12-2).

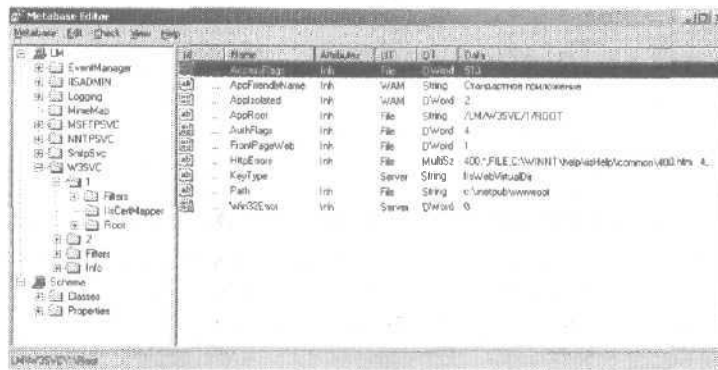


Рис. 12-2. Просмотр и редактирование параметров метабазы с помощью Metabase Editor

Раздел — это область метабазы, аналогичная папке файловой системы. Путь метабазы — это последовательность отделенных друг от друга косыми черточками (/) имен разделов, уникально идентифицирующая расположение раздела в метабазе. Структура иерархии такова:

/ L M/Служба/Веб\_узел/Корень

Здесь **LM** — это локальный компьютер, **Служба** — название службы Интернета, например **W3SVC** или **MSFTPSVC**, **Веб\_узел** — имя экземпляра виртуального сервера или узла, и **Корень** — корневой каталог виртуальной папки.

Чтобы понять, как используются пути метабазы, рассмотрим пример. Путь метабазы **/LM/W3SVC/1/Root** представляет корень первого экземпляра установленного на локальном компьютере Web-узла. Таким образом, если это значение свя-

зано с путем C:\Inetpub\Wwwroot, то URL `http://www.domain.com/index.htm` может быть связан с путем к физическому файлу C:\Inetpub\Wwwroot\INDEX.HTM.

На параметры метабазы распространяются правила наследования, обсуждавшиеся в предыдущих главах. Значения настроенных параметров, заданные на глобальном уровне, распространяются на узлы и на все их вложенные папки. Свойства, определенные на локальном уровне, могут наследовать значения параметров, заданные на глобальном уровне. Аналогично дочерние узлы наследуют значения параметров узла или папки. Наследование происходит автоматически, но его можно отключить. Например, для этого перед изменением параметра в Metabase Editor следует удалить атрибут `Inheritance`. Кроме того, можно задать значение отдельного параметра на уровне узла. Так, чтобы включить буферизацию для конкретного узла, задайте для него параметру `AspBufferingOn` значение `TRUE`.

### Редактирование параметров метабазы

Изменять параметры метабазы позволяют утилита Metabase Editor или сценарии VBScript для Windows. Утилита Metabase Editor во многом аналогична утилите Registry Editor. Вы можете:

- просматривать древовидную структуру метабазы для поиска требуемого свойства;
- дважды щелкнув свойство, изменить его значение с помощью диалогового окна (рис. 12-3);

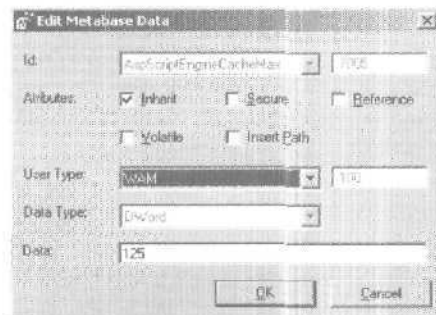


Рис. 12-3. Диалоговое окно **Edit Metabase Data**

- просматривать и редактировать значение свойства в поле Data, Завершив редактирование свойства, щелкните ОК.



**Примечание** Работая со свойствами метабазы помните, что новые значения параметров не вступят в силу до перезапуска соответствующей службы. Например, после перенастройки Web-узла вам, возможно, потребуется остановить и затем запустить его.

Кроме того, Metabase Editor позволяет найти свойство, значение которого требуется изменить.

1. Нажмите комбинацию клавиш **Ctrl+F** или выберите в меню View команду Find.
2. В поле Find диалогового окна Find введите название свойства и щелкните ОК.
3. Обнаружив требуемое свойство, Metabase Editor покажет и выделит его в дереве метабазы. Дважды щелкните свойство и в открывшемся диалоговом окне измените его значение. Затем щелкните ОК.
4. Если найти свойство невозможно, Metabase Editor выведет сообщение об ошибке. Проверьте, правильно ли введено название параметра, и попробуйте снова найти его.

Как вы понимаете, можно изменять значения сотен свойств метабазы. Свойства, с которыми вам придется работать, задают глобальные настроечные параметры Web-серверов и находятся в разделе \LM\W3SVC метабазы. Перечислим их.

- **AppAllowDebugging** определяет, включена ли на сервере ASP-отладка. Если значение свойства — TRUE, каждому сконфигурированному на сервере IIS-приложению предоставляется только один поток выполнения, что позволяет отлаживать приложения индивидуально. Значение свойства по умолчанию — FALSE. Изменять сто на TRUE следует только для отладки приложений.
- **AspAllowSessionState** определяет, включены ли сеансы для приложений. Если значение — TRUE (задано по умолчанию и означает, что сеансы включены), IIS будет регистрировать сведения о пользовательских сеансах. Если сеансы не используются, для повышения производительности свойству можно задать FALSE и затем по необходимости включать сеансы в отдельных приложе-

ниях с помощью оператора `<% @ENABLESESSIONSTATE=TRUE%>`.

- **AspBufferingOn** определяет, включена ли ASP-буферизация. Если значение — TRUE (задано по умолчанию и означает, что буферизация включена), перед отсылкой клиенту выходные данные накапливаются в буфере. Если задать FALSE, вывод ASP-сценариев будет передаваться клиентскому браузеру сразу после генерации.
- **AspQueueConnectionTestTime** задаст интервал, по истечении которого проверяется, по-прежнему ли подключен клиент к серверу. Если запрос находился в очереди дольше этого времени, перед его выполнением сервер проверяет, подключен ли клиент. По умолчанию — 3 секунды. Свойство позволяет «бороться» с нетерпеливыми пользователями, заполняющими очередь множеством запросов к одной и той же странице. Проверять, подключен ли клиент, ASP-страницы могут также с помощью метода `Response.IsClientConnected`.
- **AspRequestQueueMax** задает максимальное число ASP-запросов в очереди соединений. По умолчанию — 3 000 запросов. Значение этого свойства следует изменять в зависимости от характеристики приложения. Например, если время выполнения и время нахождения среднего запроса в очереди мало, максимальное число ASP-запросов в очереди соединений можно увеличить (особенно при перегруженном сервере).
- **AspScriptEngineCacheMax** задает максимальное число кэшируемых в памяти сценариев. Попадание в кэш обработчика сценариев позволяет избежать повторной компиляции шаблона в двоичный код. По умолчанию — 125 сценариев.
- **AspScriptFileCacheSize** задает число предварительно скомпилированных файлов сценариев, хранимых в кэше шаблонов ASP. По умолчанию — 250 сценариев. Если свойству задать -1, будут кэшироваться все запрошенные файлы сценариев, 0 — файлы сценариев не кэшируются.
- **AspSessionMax** задаст максимальное число параллельных пользовательских сеансов для ASP-приложений. По умолчанию сеансы ограничены по времени, а не по общему числу подключений.

- **AspSessionTimeout** задает тайм-аут, после которого необходимо обновлять ASP-сессии. По умолчанию — через 20 минут.
- **AspThreadGateEnabled** определяет, включено ли регулирование потоков, позволяющее динамически управлять потоками выполнения. По умолчанию задано FALSE. Чтобы включить регулирование потоков, задайте TRUE.
- **AspThreadGateLoadHigh** задает максимальный уровень использования процессора при регулировании потоков. Если загрузка процессора превышает это значение, IIS отключает некоторые потоки, снижая тем самым количество переключений контекста. Эта превентивная мера позволяет повысить производительность при большой загрузке сервера.
- **AspThreadGateLoadLow** задает минимальный уровень использования процессора при регулировании потоков. Если загрузка процессора меньше этого значения, IIS увеличивает число активных потоков — превентивная мера на случай блокирующих потоков.
- **CacheISAPI** определяет, кэшируются ли динамические библиотеки ISAPI в памяти после использования. По умолчанию равно TRUE, т. е. динамические библиотеки ISAPI хранятся в кэше до останова сервера. Если свойству задать FALSE, библиотеки будут выгружаться сразу после использования.
- **ConnectionTimeout** задает тайм-аут, после которого сервер отключает неактивное соединение. По умолчанию — 900 секунд (15 минут).
- **DisableMemoryCache** определяет, включено или отключено кэширование памяти IIS. По умолчанию кэширование памяти включено (т. е. задано 0). Отключать кэширование памяти рекомендуется только для целей тестирования или разработки.
- **ServerListenBackLog** задает размер очереди запросов. Значение по умолчанию основано на значении параметра AcceptEx ОС и значении свойства ServerSize базы данных. Если значение ServerSize — 1, значение ServerListenBackLog по умолчанию равно 40 запросам. Если значение ServerSize — 2, значение ServerListenBackLog по

умолчанию — 100 запросов. Диапазон допустимых значений `ServerListenBackLog` — от 5 до 1 000 запросов.

- **ServerSize** задает масштаб сервера — количество обрабатываемых за день клиентских запросов: 0 — запросов меньше 10 000, 1 — от 10 000 до 100 000, 2 — свыше 100 000 запросов в день.

#### Управление метабазой при помощи сценариев

Сценарии Windows — еще один способ управлять метабазой. Взаимодействие с параметрами метабазы в сценариях Windows осуществляется при помощи ADSI-поставщика для IIS, позволяющего управлять административными объектами IIS. Основные объекты администрирования — `IisComputer`, `IisWebServer` и `IisFtpServer`.

Объект `IisComputer` позволяет задавать глобальные свойства IIS и управлять резервными копиями метабазы. Помните: все дочерние узлы (Web-узлы, папки и т. д.) могут наследовать глобальные настроечные параметры. Объект `IisComputer` представляет собой объект-контейнер ADSI, для которого параметр `AdsPath` имеет значение `IIS://ИмяКомпьютера`, где *ИмяКомпьютера* — это имя любого компьютера или LocalHost, например `IIS://engsvr01`.

Чтобы получить объект `IisComputer` для сервера `ENGSVR01` с помощью сценария VBScript:

```
'Инициализируем переменные
Dim compObject, serverName
serverName = "engsvr01"
'Получаем объект IISWebServer
Set compObject = GetObject("IIS://" & serverName)
```



**Примечание** Подробное обсуждение способов управления метабазой с помощью сценариев выходит за рамки этого издания. Хороший источник информации по данной теме — уже упоминавшаяся книга «Windows 2000 Scripting Bible». Кроме того, просмотрите в интерактивной документации IIS список доступных объектов и порядок работы с ними.

Теперь можно работать с любыми методами и свойствами объекта `IisComputer`, например, так:

```
'Инициализируем переменные
Dim compObject, serverName
```



```
serverName = "engsvr01"
```

```
'Получаем объект IISWebServer
Set compObject = GetObject("IIS://" & serverName)
```

```
'Восстанавливаем конфигурацию метабазы на основе последней
рабочей копии
compObject.Restore
```

Для задания свойств метабазы, распространяющихся на конкретный Web-узел, а также для назначения наследуемых свойств папок и файлов служит объект `IISWebServer`. Кроме того, управлять работой сервера можно, используя методы. Например, метод `Stop` позволяет остановить, а метод `Start` — запустить Web-узел,

Web-узлы идентифицируются по индексу в метабазе. Индекс первого созданного на сервере экземпляра Web-узла — 1, второго — 2 и т. д. Объект `IISWebServer` представляет собой объект-контейнер ADSI, для которого параметр `AdsPath` имеет значение `IIS://ИмяКомпьютера/W3SVC/N` здесь *ИмяКомпьютера* — это имя любого компьютера или Local Host, `W3SVC` — идентификатор службы Web Service и `N` — индекс Web-узла. Параметр `AdsPath` указывает на первый экземпляр Web-узла на сервере ENGSR01:

```
IIS://engsvr01/W3SVC/1
```

Чтобы получить объект `IISWebServer` для первого экземпляра Web-узла в сценарии VBScript:

```
'Инициализируем переменные
Dim webObject, serverName, webN
serverName = "engsvr01"
webN = "1"
```

```
'Получаем объект IISWebServer
Set webObject = GetObject("IIS://" & serverName & "/W3SVC/" & webN)
```

Теперь можно работать с любыми методами и свойствами объекта `IISWebServer`, например так:

```
'Инициализируем переменные
Dim webObject, serverName, webN
serverName = "engsvr01"
webN = "1"
```

```

'Получаем объект IISWebServer
Set webObject = GetObject("IIS://" & serverName & "/W3SVC/" &
webN)

'Останавливаем Web-узел
webObject.Stop

'Включаем ASP-буферизацию
webObject.AspBufferingOn = True

'Сохраняем измененное значение в метабазе
webObject.SetInfo

'Запускаем Web-сервер
webObject.Start

```

Задать свойства метабазы, распространяющиеся на конкретный FTP-сервер, а также наследуемые свойства для каталогов, позволяет объект `IisFTPServer`. Как и в случае с объектом `IisWebServer`, управлять работой сервера можно, используя методы. Например, с помощью метода `Pause` приостановите FTP-сервер, а затем возобновите работу, вызвав метод `Continue`.

FTP-серверы идентифицируются по индексу в метабазе. Индекс первого сервера — 1, второго — 2 и т. д. Объект `IisFTPServer` представляет собой объект-контейнер `ADSI`, для которого параметр `AdsPath` имеет значение `IIS://ИмяКомпьютера/MSFTPSVC/N`. Здесь *ИмяКомпьютера* — это имя любого компьютера или `localhost`, `MSFTPSVC` — идентификатор службы FTP Service, и *N* — индекс сервера. Параметр `AdsPath` указывает на первый FTP-сервер на компьютере `ENGsvr01`:

```
IIS://engsvr01/MSFTPSVC/1
```

Чтобы получить объект `IisFtpServer` для первого экземпляра FTP-сервера с помощью сценария VBScript:

```

'Инициализируем переменные
Dim ftpObj, serverName, ftpN
serverName = "engsvr01"
ftpN = "1"

'Получаем объект IisFtpServer
Set ftpObj = GetObject("IIS://" & serverName & "/MSFTPSVC/" &
ftpN)

```

Теперь можно работать с любыми методами и свойствами объекта `IisFtpServer`, например, так:

```
' Инициализируем переменные
Dim ftpObj, serverName, ftpN
serverName = "engsvr01"
ftpN = "1"

' Получаем объект IisFtpServerSet
ftpObj = GetObject("IIS://" & serverName & "/MSFTPSVC/" & ftpN)

' Останавливаем FTP-сервер
ftpObj.Stop

' Включаем анонимный доступ
ftpObj.AllowAnonynous = True

' Сохраняем измененное значение в иетабазе
ftpObj.SetInfo

' Запускаем FTP-сервер
ftpObj.Start
```

# Предметный указатель

## A

Access log 336  
Active Directory 16  
Active Directory —  
    пользователи и компьютеры  
    см. Active Directory Users  
    and Computers  
Active Directory Services  
    Interface *CM*. ADSI  
Active Directory Users and  
    Computers 11  
Active Server Pages *CM*. ASP  
Ad Rotator (ADROT.DLL) 85  
Administration Application *CM*.  
    приложение, администриро-  
    вание  
Administration Web site (адми-  
    нистрирование веб-узла) 7  
ADSI (Active Directory  
    Services Interface) 15  
Alerter 407  
AppAllowDebugging 423  
Application Log см. журнал,  
    приложений  
ASCII 380, 385  
ASP (Active Server Pages) 2,  
    81, 84, 102, 344, 408  
AspAllowSessionState 423  
AspBufferingOn 424  
AspQueueConnectionTestTime  
    424  
AspRequestQueueMax 424  
AspScriptEngineCacheMax  
    424  
AspScriptFileCacheSize 424  
AspSessionMax 424  
AspSessionTimeout 424  
AspThreadGateEnabled 425  
AspThreadGateLoadHigh 425  
AspThreadGateLoadLow 425

## B

Browser Capabilities  
    (BROWSERCAPI.DLL) 85

## C

CA  
    — автономный дочерний 186  
    — автономный корневой 186  
    — архивирование информа-  
    ции 194  
    - восстановление информации  
    196  
    — дочерний предприятия 186  
    — корневой предприятия 186  
    — сертификат 200  
CA 183  
CacheISAPI 425  
CacheSecurityDescriptor 417  
Certificate Authority см. CA  
Certificate Export Wizard 223  
certificate revocation list *CM*.  
    CRL  
Certificate Services 180, 185  
    — доступ 191  
    - запуск 193  
    — остановка 193  
    — установка 187  
certificate revocation list  
    см. CRL  
Certification Authority Restore  
    Wizard 197  
CHACCESS *CM*. Change Access  
    Restrictions  
Change Access Restrictions 16  
CheckCertRevocation 417  
Circular Trace File см. файл  
    циклической трассировки  
ClipBook 407  
COM 85

Common Internet Scheme  
Syntax *см.* синтаксис схем  
Интернета  
Computer Browser 407  
Computer Management  
11, 35  
ConnectionTimeout 425  
Content Linking  
(NEXTLINK.DLL) 85  
Continue FTP Server  
(CONTFTP) 16  
Continue Server  
(CONTSRV) 16  
Continue Web Server  
(CONTWEB) 16  
Counter log *см.* журнал, счет-  
чиков  
Counters (COUNTERS.DLL)  
86  
Create Virtual Directory  
(MKWEBDIR) 17  
Create Web Site (MKW3SITE)  
17  
CRL 186

**D**

Data Sources 11  
Database Access  
(MSADO20.DLL) 86  
Default FTP site 7  
Default NNTP Virtual Server  
(виртуальный NNTP-сервер  
по умолчанию) 8  
Default SMTP Virtual Server  
(виртуальный SMTP-сервер  
по умолчанию) 7  
Default Web site (Web-узел по  
умолчанию) 7  
DHCP Client 407  
DHCP Server 407  
DHCP-клиент *см.* DHCP Client  
DHCP-сервер *см.* DHCP  
Server  
Directory Service 340  
DisableMemoryCache 417, 425

Display Administrative Node  
(DISPNODE) 17  
Display Administrative Tree  
(DISPTREE) 17  
DLL 82  
DLL-сервер 21  
DNS 11  
DNS (Domain Name System)  
47  
DNS Server 340  
DNS-поиск 382  
Domain Name System *см.* DNS  
DSN 402

**E**

ESMTP (Extension to SMTP)  
275  
Event Log 34 337  
Event Viewer 11, 149  
EventLogging 420  
Extension to SMTP  
*см.* ESMTP

**F**

Failure Audit *см.* аудит,  
отказов  
Fax Service 407  
File Access Component  
(FSCFG.DLL) 86  
File Replication 407  
File Replication Service *см.*  
служба, репликация файлов  
File Transfer Protocol *см.* FTP  
Find Web Site (FINDWEB)  
17  
FQDN 22, 300  
FTP 19, 40, 131, 228  
— перезапуск 2  
— сервер 6  
FTP Publishing Service 235  
FTP Service 344  
FTP-сеанс 231, 246  
FTP-сервер 229, 248  
FTP-служба 234  
FTP-узел 233, 235, 237

— по умолчанию *см.* Default FTP site  
 fully qualified domain name  
*см.* FQDN

## Н

NKEY\_CLASSES\_ROOT 415  
 NKEY\_CURRENT\_CONFIG 415  
 NKEY\_CURRENT\_USER 415  
 NKEY\_LOCAL\_MACHINE 415  
 NKEY\_USERS 415  
 HTTP 10, 52, 65, 83, 229  
 — сжатие 2  
 HTTP Indexing Service 344  
 HTTP Keep-Alives 65, 66  
 HTTP Monitoring Tool 11, 337  
 HTTP-заголовок 113  
 HTTP-сжатие 376  
 Hyper Text Transfer Protocol  
*см.* HTTP

## I

IDQ 313  
 IIS  
 - FTP Publishing Service 235  
 - NNTP 10  
 — автоматический переза-  
 пуск 413  
 — администрирование 3, 10,  
 19  
 — архитектура 19  
 — — основа 20  
 — безопасность 151  
 — восстановление 38, 41  
 — интерфейс администрирова-  
 ния 13  
 — каталог 66  
 — метабазы 16  
 — — путь 16  
 — — раздел 16  
 — мониторинг 335, 343  
 — оснастка 25

— поврежденная установка  
 40, 42  
 — подкомпоненты  
 — — Common Files (Общие  
 файлы) 6  
 — — Documentation (Докумен-  
 тация) 6  
 — — File Transfer Protocol  
 Server (FTP-сервер) 6  
 — - FrontPage 2000 Server  
 Extensions (Серверные рас-  
 ширения FrontPage) 6  
 — — Internet Information  
 Services Snap-In (Оснастка  
 IIS) 6  
 — — Internet Services Manager  
 (Диспетчер служб Интер-  
 нета) 6  
 — — Network News Transfer  
 Protocol Service (Служба  
 NNTP) 7  
 — — Simple Mail Transfer  
 Protocol Service (Служба  
 SMTP) 7  
 — - Visual InterDev RAD  
 Remote Deployment Support  
 (Поддержка удаленного раз-  
 вертывания Visual InterDev  
 RAD) 7  
 — - World Wide Web Server  
 (Веб-сервер) 7  
 — производительность 406  
 — разрешение доступа 139  
 — резервная копия configura-  
 ции 40 43  
 — резервное копирование 38  
 — служба 35  
 — — FTP-публикаций 10  
 — - IIS Admin 10  
 — — веб-публикаций 10  
 — — индексирования 10  
 — — перезапуск 21  
 — служба индексирования 2  
 — удаленная установка 14, 15  
 — управление 11  
 — управление службами 33

- уровень безопасности 134
  - установка 6
  - учетная запись 133
  - - IUSR 10
  - - IWAM 10
  - IIS 2, 7, 10, 12, 13, И, 19, 28, 31, 32, 334
  - IIS Admin Service *см.* служба, IIS Admin
  - IIS Administration Script Utility 11, 17
  - IIS Help Application *см.* приложение, справочное
  - IISRESET 28, 30, 32
  - Indexing Service 34, 304, 344
    - запуск 320
    - индексируемая папка 326
    - каталог 326
    - настройка 320
    - остановка 320
    - приостановка 320
    - производительность 322
    - слияние каталогов 330
    - тестирование каталога 331, 332
    - управление 11
    - установка 6
  - Indexing Service Filter 344
  - InetInfo 21, 28
  - Infrared Monitor 407
  - Internet Connection Sharing 407
  - Internet data query *см.* IDQ
  - Internet Information Manager 14
  - Internet Information Services *см.* IIS
  - Internet Information Services Global 344
  - Internet Service Provider *см.* ISP
  - Internet Services Manager 7, 12, 13, 19, 25
  - IP-адрес 19, 26, 46, 239, 256, 382
    - аренда 47
    - изменение 60
    - назначение 49
    - ограничение доступа 166
    - сервера 52
    - IP-фильтрация 14
    - ISAPI 3, 21, 39, 81, 106, 408
    - ISP 47
- J**
- Java Servlet Pages 81
  - JScript 84
- L**
- LDAP 16
  - Lightweight Directory Access Protocol *см.* LDAP
  - ListenBackLog 417
  - Logging Utility (LOGSCRIPT.DLL) 86
- M**
- Macintosh 86
  - MaxCachedFileSize 417
  - MaxConcurrency 417
  - MaxPoolThreads 418
  - MemCacheSize 418
  - Messenger 407
  - Metabase Editor 420, 422
  - Microsoft Exchange 2000 16
  - Microsoft Exchange 2000 Server 260
  - MIME 122
  - MMC 25
  - MyInfo (MYINFO.DLL) 86
- N**
- National Center for Supercomputing Applications *см.* NCSA
  - NCSA 379, 380, 394
  - NetBIOS 22, 47
  - NetMeeting Remote Desktop Sharing 407
  - Network DDE 407
  - Network DDE DSDM 407

Network News Transfer  
Protocol *см.* NNTP  
Network News Transport  
Protocol *см.* NNTP  
NNTP 2, 10, 19, 29, 35, 131  
NNTP Commands 344  
NNTP Server 344  
NWLink IPX/SPX 407  
NWLink IPX/SPX/NetBIOS-  
совместимый транспортный  
протокол *см.* NWLink  
IPX/SPX  
NWLink NetBIOS 407

## O

ObjectCacheTTL 418  
ODBC 380, 391, 400, 404

## P

Page Counter (PAGECNT.DLL)  
86  
Pause FTP Server (PAUSEFTP)  
17  
Pause Server (PAUSESrv) 17  
Pause Web Server  
(PAUSEWEB) 17  
Performance 12  
Performance Monitor 336, 343  
Permission Checker  
(PERMCHK.DLL) 86  
PICS (Platform for Internet  
Content Selection) 114  
Platform for internet Content  
Selection *см.* PICS  
Playback 337  
PoolThreadLimit 418  
Print Spooler 407

## R

RAID 5  
RAID-0 3  
RAID-1 5  
Recreational Software Advisory  
Council *см.* RSAC  
REG\_BINARY 416  
REG\_DWORD 416

REG\_EXPAND\_SZ 416  
REG\_MULTI\_SZ 416  
REG\_SZ 416  
Registry Editor 416  
Restart Internet Services *см.*  
служба, Интернета, переза-  
пуск  
RSAC 114

## S

Sample Application *см.* прило-  
жение учебное  
SCSI 5  
Secure Sockets Layer *см.* SSI-  
Security Log *см.* журнал безо-  
пасности  
Sequential Trace File *см.* файл  
последовательной трасси-  
ровки  
Server Extensions  
Administrator 12  
ServerCacheTime 420  
ServerListenBackLog 425  
ServerSize 426  
Services 12  
Simple Mail Transfer Protocol  
*см.* SMTP  
SMTP 19, 29, 35, 131, 260  
SMTP 2  
SMTP NTFS Store Driver 345  
SMTP Server 345  
SMTP-сервер 265  
— виртуальный 265  
— мониторинг 270  
— уникальный идентификатор  
267  
SSIEnableCmdDirective 419  
SSL 3, 180, 213, 226  
SSL 52  
Start FTP Server  
(STARTFTP) 17  
Start Internet Services *см.*  
служба, Интернета, запуск  
Start Server (STARTSRV) 17  
Start Web Server  
(STARTWEB) 17



- Status (STATUS.DLL) 86  
 Stop FTP Server (STOPFTP) 17  
 Stop Internet Services *см.* служба, Интернета, остановка  
 Stop Server (STOPSRV) 17  
 Stop Web Server (STOPWEB) 18  
 Success Audit *см.* аудит, успехов  
 System Log *см.* журнал, системы
- T**
- TCP 229  
 TCP/IP 26, 47  
 TCP/IP NetBIOS Helper Service 407  
 Telephony 407  
 Telnet 408  
 TLS 280  
 Tools (TOOLS.DLL) 86  
 Trace Log *см.* журнал, трассировки  
 Transmission Control Protocol *CM.* TCP  
 Transmission Control Protocol/Internet Protocol *CM.* TCP/IP  
 Transport Layer Security *CM.* TLS  
 TryExceptDisable 419  
 TSL 3
- U**
- UDP 26  
 UNC 234  
 UNC 48  
 Uniform Naming Convention *см.* UNC  
 uniform resource locator *CM.* URL  
 Uninterruptible Power Supply 408  
 UNIX 407  
 UploadReadAhead 419  
 URL 19, 22, 48, 234
- UsePoolThreadForCGI 419  
 User Datagram Protocol *CM.* UDP
- V**
- VBScript 84, 422  
 Visual Basic Scripting Edition *CM.* VBScript
- W**
- W3C 379, 387, 398  
 WCAT 337  
 Web Application Stress Tool 337  
 Web Capacity Analysis Tool *CM.* WCAT  
 Web Distributed Authoring and Versioning *CM.* WebDAV  
 Web Service 345  
 Web Site Creation Wizard 56  
 WebDAV 3, 152, 158  
 Web-администратор 378  
 Web-сервер 31, 376  
 — производительность 363  
 — разрешение 152  
 — — глобальное 152  
 — — локальное 153  
 — — настройка 153  
 — управление безопасностью 131  
 — уровень безопасности 172  
 Web-служба 54  
 Web-узел 46  
 - IISAdmin 55  
 - IISHelp 55  
 - IISSamples 55  
 — SSL-порт 213  
 - администрирование 15, 171  
 — домашний каталог 59  
 - защищенная область 152  
 — идентификатор 48, 62  
 — идентификация 46  
 — имя 46  
 - оператор 169  
 — отключение 173  
 — оценка содержимого 115

- ошибка 116, 130
- перенаправление запроса 74, 79, 80
- производительность 64
- создание 54
- узел обновления 127
- управление содержимым 72
- файл
  - изменение 72
  - переименование 73
  - просмотр 72
  - удаление 73
- Windows Components Wizard 8
- Windows Scripting Host *см.* WSH
- Windows Security Package *см.* пакет безопасности Windows
- World Wide Web *см.* WWW
- World Wide Web Consortium *см.* W3C
- World Wide Web Publishing Service *см.* служба, веб-публикаций
- WSH 15
- WWW 19

## А

администрирование 3, 12

- Web 13

активные серверные страницы *см.* ASP

анонимное

- подключение 243, 249
- соединение 23

анонимный доступ 163

аудит 3, 149

- Audit Account Logon Events 150
- Audit Account Management 150
- Audit Directory Service Access 150

- Audit Logon Events 150
- Audit Object Access 151
- Audit Policy Change 151
- Audit Privilege Use 151
- Audit Process Tracking 151
- Audit System Events 151
- отказов 341
- успехов 341

аутентификация 9

## Б

баннер 129

брандмауэр 3, 172

браузер 376

буферизация 93

## В

виртуальный сервер 19, 31

## Г

групповая политика 144

- параметры 145
- управление 147

## Д

диапазон адресов 47

динамически

- назначаемый порт 232
- подключаемые библиотека *см.* DLL

Диспетчер

- очереди печати *см.* Print Spooler
- сетевого DDE *см.* Network DDE DSDM
- служб Интернета *см.* Internet Services Manager

домен 256, 382

- локальный 261, 272
- настройка 271
- переименование 282
- по умолчанию 273
- подменяющий 300
- псевдоним 273
- система безопасности 9
- служебный 271

- тип 22
- удаленный 261 275 280
- электронная почта 261

**Ж**

- журнал
  - безопасности 340
  - ведение 392, 405
  - директива 388
  - доступа 338, 378
  - — формат 379
  - идентификатор поля 389
  - именование файлов 393
  - поле с учетной информации процессов 390
  - префикс 388
  - приложений 340
  - производительности 352, 359
  - — управление 353
  - системы 340
  - событий 339
  - счетчиков 352 354
  - таблица 401
  - трассировки 352 357
  - файл 356, 393

**З**

- заголовок узла 2, 51, 239
- защита приложения 3
- зеркалирование диска 5

**И**

- ИБП 5
- идентификатор 100, 239, 267
- идентификация ресурсов 22
- индекс 311
- индексирование 309, 318
- интернет-сервер
  - дисковое пространство 5
  - защита данных 5
  - память 4
  - процессор 4
  - симметричная многопроцессорная обработка 4
- интерфейс 16

- интрасеть 47
- информационное сообщение 245

**Информационные службы**

- Интернета см. IIS
- источник бесперебойного питания см. ИБП
- источники данных ODBC 11

**К**

- каталог
  - виртуальный 55, 67, 68, 177, 243
  - изменение 71
  - переименование 71
  - подключение 70
  - слияние 330
  - создание 316
  - способ отображения 244
  - тестирование 331
  - удаление 71
  - физический 67, 242
- код состояния 116
- колонтитул 110
- команда REST 2
- конфигурирование 398
- кэш 311
- кэширование 93, 95, 111, 366, 410

**М**

- мастер
  - восстановления центра сертификации см. Certification Authority Restore Wizard
  - компонентов Windows 6
  - создания Web-узлов см. Web Site Creation Wizard
  - экспорта сертификатов см. Certificate Export Wizard
- метабаза 19, 89, 420
- раздел 421
- редактирование 420, 422
- свойства 423
- управление 426
- метаданные 326

Монитор инфракрасной связи  
*см.* Infrared Monitor  
 мониторинг 294, 334, 343  
 — дисковый ввод-вывод 366  
 — пропускная способность  
 сети 367  
 — процессор 366  
 — сетевое подключение 367  
 — составление плана 336  
 — средства 336

## Н

Наблюдательный совет по  
 развлекательному ПО *см.*  
 RSAC  
 направляющий узел 282  
 настройка производитель-  
 ности 334  
 Национальный центр разра-  
 ботки приложений для вы-  
 числений на супер-ЭВМ  
*см.* NCSA  
 номер порта 19, 22, 48, 50,  
 234, 239, 267

## О

обозреватель компьютеров  
*см.* Computer Browser  
 общий доступ к подключению  
 Интернета *см.* Internet  
 Connection Sharing  
 ограничение доступа 167  
 оператор 258  
 операционная система  
 - Windows 2000 4, 16, 28  
 — Windows 2000 Professional  
 49  
 — Windows NT 177  
 оповещатель *см.* Alerter

## П

пакет безопасности Windows  
 280  
 параллельное подключение  
 64

параметры документа 109  
 поиск 313  
 полное доменное имя 11  
 пользовательский сеанс 65  
 пользовательское прило-  
 жение 86  
 поставщик услуг Интернета  
*см.* ISP  
 почтовый интернет-сервер  
 260  
 почтовый шлюз 278  
 приложение 87  
 — администрирование 55  
 — буферизация 101  
 — внепроцессное 89  
 — защита 89  
 — изолированное 105  
 — использование 88  
 — кэширование 91  
 — начальная точка 88  
 — отладка 103  
 — ошибка 104  
 — родительские пути 102  
 — создание 91  
 — сопоставление 178  
 — — добавление 96  
 — — редактирование 98  
 — — удаление 99  
 — — управление 95  
 — справочное 55  
 — удаление 105  
 — управление 93  
 — учебное 55  
 — учетная запись 136  
 — язык сценариев 102  
 приоритет 82  
 проверка подлинности 3, 19,  
 160  
 — Basic Authentication 161  
 — Digest Authentication 161  
 — Integrated Windows  
 Authentication 161  
 — включение 163  
 — краткая 3  
 — отключение 163

прокси-сервер 3  
 пропускная способность 375  
 пространство имен 88

## Р

раздел 421  
 разрешение 20  
 — глобальное 253  
 — локальное 254  
 разрешение имени 47  
 расширение 81 83  
 регулирование процессов 3  
 реестр  
 — системный 415  
 — управление  
 — - IIS 417  
 — — протоколом SSL 419  
 — — службой Indexing Service 418  
 режим проверки подлинности 286  
 ретрансляция 276 295  
 РосНИИРОС 47  
 Российский НИИ Развития  
 Общественных Сетей *см.*  
 РосНИИРОС

## С

сеанс 99  
 — состояние 93  
 сервер  
 — базовый уровень производи-  
 тельности 336  
 — виртуальный 31, 262, 278,  
 283  
 — оптимизация 364  
 — нанки обмена *см.* ClipBook  
 — сценариев Windows  
*см.* WSH  
 — полнофункциональный  
 260  
 — производительность 336  
 — сохранение конфигурации  
 38  
 сервисный пакет 174  
 сертификат 3, 182, 197, 213

— генерирование 198  
 — замена 221  
 — запрос 203 212  
 — обновление 200 221  
 — отзыв 199  
 — просмотр 200  
 — создание 202  
 — удаление 221  
 — управление 219  
 — установка 202, 211  
 — экспорт 222  
 Сетевой Информационный  
 Центр 18  
 сеть  
 — общедоступная 47  
 — частная 47  
 синтаксис схем Интернета 24  
 система  
 — проверки подлинности 9  
 — доменных имен *см.* DNS  
 Системный монитор  
*см.* Performance Monitor  
 сканирование 309, 328  
 служба  
 — FTP-публикаций 29, 34,  
*см. также* FTP Publishing  
 Service  
 - IIS Admin 29, 34  
 - SMTP 261  
 - World Wide Web Publishing  
 Service 31  
 — веб-публикаций 29, 35, 54,  
 345  
 — восстановление 37  
 — запуск 35, 36  
 — индексирования 344, *см.*  
*также* Indexing Service  
 — Интернета  
 — — запуск 28  
 — — остановка 28  
 — — перезапуск 29  
 — каталогов 16  
 — остановка 35  
 — поддержки TCP/IP  
 NetBIOS *см.* TCP/IP  
 NetBIOS Helper Service

- приостановка 35
- репликация файлов 340
- сетевого DDE *см.* Network DDE
- сообщений *см.* Messenger
- факсов *см.* Fax Service
- служебная программа администрирования IIS *см.* IIS Administration Script Utility
- список отозванных сертификатов *см.* CRL
- статистика трассировки 378
- стойкость шифра 185
- страница перехода 129
- строка запроса 177
- счетчик 343, 345
- создание оповещений 359

**Т**

трассировочное ПО 378

**У**

- уведомление 174
- удаленные ресурсы 39
- узел 19, 31
- универсальное правило именования *см.* UNC
- универсальный указатель ресурсов *см.* URL
- уникальный идентификатор 60
- управление доступом 3
- управляющий код 25
- уровень безопасности
  - IIS, 131, 134
  - Windows 131, 138
- утечка ресурсов 406
- учетная запись
  - Administrator 173

- IUSR 132
- IWAM 132
- LocalSystem 132
- Интернет 134
- пользователя 3, 132
- системная 133

**Ф**

файл

- последовательной трассировки 358
- циклической трассировки 358

фильтр 81, 106

- глобальный 82, 106
- локальный 82, 107

фоновое слияние 311

**Ц**

центр сертификации *см.* CA

**Ч**

Content Rotator  
(CONTROT.DLL) 86

**Ш**

шаблон 79

- безопасности 175

шифрование 181

- ключ
  - — закрытый 181
  - — открытый 181
  - — секретный общего пользования (ключ сессии) 181

**Э**

электронный адрес 261

## Об авторе

Уильям Р. Станек (William. R. Stanek, win2000-consulting@tvpress.com) имеет за плечами более 15 лет опыта программирования и разработки. Он один из ведущих экспертов по сетевым технологиям и автор множества известных книг. На протяжении многих лет его практические советы помогали программистам, разработчикам и сетевым инженерам по всему миру. Он также регулярно пишет для ведущих журналов типа «PC Magazine», где его статьи обычно можно найти в разделе «Solutions». Он участвовал в написании более 20 книг. Самые последние из них — «Microsoft Windows 2000. Справочник администратора», «Microsoft Exchange 2000 Server. Справочник администратора», «Microsoft SQL Server 2000. Справочник администратора» и «Windows 2000 Scripting Bible».

Станек активно участвует в разработке коммерческих Интернет-проектов с 1991 г. Первый опыт в области технологий он получил в армии, в которой прослужил 11 лет. Он обладает обширными знаниями в области разработки серверных решений, шифрования, Интернет-разработки, а также развертывания и технологий электронной коммерции. В 1998 и 1999 гг. Станек работал одним из начальников технической службы iCat (сейчас — часть подразделения Internet Online Services корпорации Intel) бизнес-подразделения IDS корпорации Intel. В 1999 и 2000 гг. в компании-поставщике прикладных служб GeoTrust (Портленд, Орегон) он разработал основополагающие бизнес-стратегии и долгосрочные технологические планы, превратившие компанию из бумажной концепции в многомиллионный бизнес.

Станек имеет степень магистра информационных систем с отличием и степень бакалавра информатики *magna cum laude*. Он гордится тем, что участвовал в военной операции в Персидском заливе и был членом экипажа самолета. Совершив множество боевых вылетов в Ирак, он получил девять медалей, включая высшую американскую летную награду — Крест за отличие ВВС США. Сейчас он вместе с женой и детьми проживает на Северо-западном побережье Тихого Океана.

Уильям Р. Станек

# Internet Information Services 5.0, Справочник администратора

Перевод с английского под общей редакцией *А. П. Харламова*

Компьютерная верстка *В. Б. Хильченко*

Технический редактор *Н. Г. Тимченко*

Дизайнер обложки *Е. В. Козлова*

Оригинал-макет выполнен с использованием  
издательской системы Adobe PageMaker 6.0

TypeMarketFontLibrary  
легальный пользователь

Пользователь  
Para(-)Type  
INTERNAL USE

Главный редактор *А. И. Козлов*

Подготовлено к печати  
Издательско-торговым домом «Русская Редакция»

 РУССКАЯ РЕДАКЦИЯ

Лицензия ЛР № 066422 от 19.03.99 г.  
Подписано в печать 17.04.2002 г. Тираж 4 000 экз.  
Формат 84x108/32. Физ. п. л. 14,5

Отпечатано в ОАО «Типография «Новости»»  
107005, Москва, ул. Фр. Энгельса, 46



msdn  
журнал для разработчиков  
**msdn**  
magazine  
Российская Редакция  
март 2002  
(3-3)  
СПЕЦВЫПУСК №1

**Новости**  
Инструменты  
разработчика

**Web-сервисы**  
Дан Вилс  
Порталы на .NET  
и Web-сервисы

**Интервью**  
Будди Бук и Бурзак  
разработчики ПО

**Web: вопросы  
и ответы**  
Маска Мейерс  
Почему у вас  
пару тысяч на сайте,  
а у конкурента — десятки?

**XML**  
Борис Соловьев  
XML-парсеры  
и трансформации DTD  
в XSD

**Безопасность**  
Борис Соловьев  
Как защитить свой сайт  
от взлома?

Март Руссовет и Давид Соломон  
**Windows XP**  
Усовершенствования  
в ядре

Мак Петров  
**Win32**  
Формат Portable Executable

**...теперь на русском языке**

Подписной индекс по каталогу Агентства «Роспечать» — **81240**  
Подписной индекс по каталогу Агентства «Книга-сервис» — **43449**  
Интернет-магазин [www.ITbook.ru](http://www.ITbook.ru)

тел.: (095) 142-0571, тел./факс: (095) 145-4519, e-mail: [emsdn@rusedit.ru](mailto:emsdn@rusedit.ru), <http://www.rusedit.ru>  
<http://www.microsoft.com/rus/msdn/magazine>



профессиональный журнал

# ПРОГРАММИСТ

Профессиональный журнал,  
посвященный исключительно  
вопросам разработки. Наши  
авторы - профессиональные  
программисты, которые  
делятся с читателями  
«секретами мастерства».

Мы публикуем материалы о  
самых современных  
технологиях и средствах  
разработки, статьи о  
принципах и методах, теории  
и практике  
программирования.

Мы предлагаем статьи на  
самые разные  
«программерские» темы,  
любого уровня сложности.

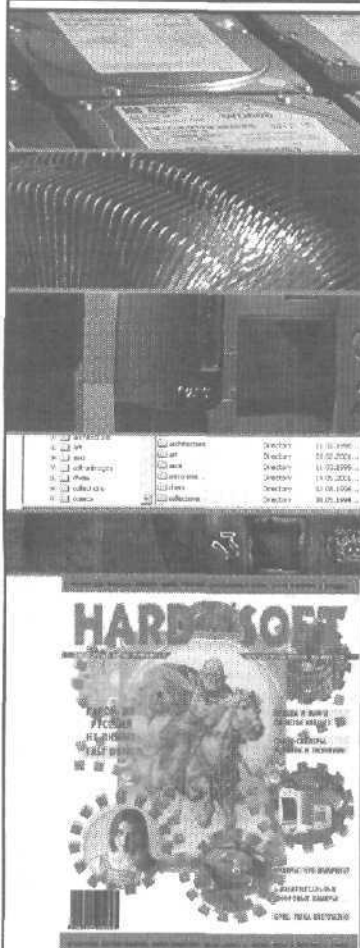
#### Подписка

Индекс в каталоге агентства  
"Роспечать" - 80467,  
в каталоге  
"Пресса России" - 45775.

[www.programme.ru](http://www.programme.ru)  
[info@programme.ru](mailto:info@programme.ru)



**ЕЖЕМЕСЯЧНЫЙ  
НАУЧНО-ПОПУЛЯРНЫЙ  
КОМПЬЮТЕРНЫЙ ЖУРНАЛ**



**e-mail:**  
**info@hardnsoft.ru**

# HARD'n'SOFT

**МАКСИМАЛЬНО ПОЛНАЯ  
И ОБЪЕКТИВНАЯ ИНФОРМАЦИЯ  
ДЛЯ ЧИТАТЕЛЕЙ, УВЛЕЧЕННЫХ  
КОМПЬЮТЕРНОЙ ТЕХНИКОЙ**

**В каждом из номеров нашего журнала:**

- новости компьютерной индустрии
- подробности о современных и перспективных технологиях
- тесты и обзоры аппаратных и программных продуктов
- интернет и мультимедиа, игры • прикладные программы
- консультации экспертов, встречи с интересными людьми
- CD-приложение с полезными утилитами



**НАШИ ИНДЕКСЫ:**

**Hard'n'Soft - 73140, Hard n Soft + CD - 26067**

# SoftLine<sup>direct</sup>

## КАТАЛОГ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ



119991 г. Москва,  
ул. Губкина, д. 8  
(095) 232-0023  
[www.softline.ru](http://www.softline.ru)  
E-mail: [info@softline.ru](mailto:info@softline.ru)

- Если Вы хотите быть в курсе всех последних событий на рынке программного обеспечения,
- Если Вы хотите получать наиболее полную информацию о программных продуктах из первых рук - от самих производителей,
- Если Вы ведете честный бизнес и покупаете лицензионное ПО,

## ЗНАЧИТ ВАША ЖИЗНЬ МОЖЕТ СТАТЬ ЕЩЕ ПРОЩЕ!

Подпишитесь на новый полноцветный каталог, издаваемый одним из крупнейших поставщиков программного обеспечения в России, и Вы будете регулярно получать его по почте БЕСПЛАТНО! Кроме того, по Вашему желанию на Ваш электронный адрес будут регулярно приходить еженедельные новости рынка программного обеспечения от компании «СофтЛайн»



**БЕСПЛАТНО!**  
ПОДПИСКА

Microsoft\*

# Internet Information Services 5.0

## Справочник администратора

### Компактный справочник по администрированию IIS 5.0

Независимо от того, сколько пользователей в вашей организации — 50 или 5 000, этот справочник поможет найти ответы на все, даже самые сложные вопросы администрирования Microsoft Internet Information Services и Microsoft Indexing Services. Подробные таблицы, списки и инструкции позволяют моментально найти нужную информацию и уменьшить время простоя.

#### Вы научитесь:

- администрировать Web-серверы: справочник содержит детальное описание средств, способов и концепций администрирования Web-серверов под управлением IIS;
- управлять основными службами: подробные инструкции помогут быстро освоиться с администрированием FTP-, SMTP- и NNTP-серверов, а также службы Indexing Service;
- оптимизировать и поддерживать IIS: в книге даны советы по наблюдению, оптимизации и устранению проблем производительности IIS, а также по работе с журналами доступа и сервера.

Издательство «Русская Редакция» представляет новую серию книг Microsoft Press

**Справочник администратора** (Administrator's Pocket Consultant)



Каждое издание серии объединяет руководство по эксплуатации и подробный справочник по основным функциям и параметрам системы.

ISBN 5-7502-0188-0



9 785750 201884

**ITProfessional**

Web-узел издательства: [www.rusedit.ru](http://www.rusedit.ru)  
Интернет-магазин: [www.ITbook.ru](http://www.ITbook.ru)

