M C T 3

Self-Pased Training Kit

Exam **70-643**

Configuring Windows Server* 2008 Applications Infrastructure

J. C. Mackin
Anil Desai

Mkxvsoft Press

Официальное пособие для самоподготовки

Учебный курс Microsoft"

Развертывание и настройка Windows Server 2008

Дж. К. Макин
Анил Десаи

экзамен 70-643

MCTS

Москва 2008

М. РУССКАЯ РЕДАКЦИЯ

УДК 004.45
ББК 32.973.81-018.2
М15

Макии Дж. К., Десаи Анил

М15 Развертывание и настройка Windows Server® 2008. Учебный курс Microsoft / Пер. с англ. — М. : Издательство «Русская Редакция», 2008. — 640 стр. : ил.

ISBN 978-5-7502-0368-0

Эта книга — подробное руководство по развертыванию и поддержке операционной системы Windows Server 2008. В книге даны пошаговые инструкции, описан механизм развертывания и процессы настройки новой ОС, ее основных компонентов: серверной системы хранения данных и кластеров, служб терминалов, веб-приложений, веб-сервера, служб FTP, SMTP, Windows Share Points Services и Windows Media 2008. Кроме того, приводятся советы по устранению различного рода неполадок.

Книга адресована специалистам в области информационных технологий, системным администраторам, а также всем, кто хочет научиться работать с Windows Server 2008. Настоящий учебный курс поможет вам самостоятельно подготовиться к сдаче экзамена № 70-643 по программе сертификации Майкрософт (сертификат Microsoft Certified Technology Specialist).

Книга состоит из 9 глав, содержит множество иллюстраций и примеров из практики. На прилагаемом компакт-диске находятся электронная версия книги (на англ. языке), вопросы пробного экзамена и другие справочные материалы.

УДК 004.45
ББК 32.973.81-018.2

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

ISBN 978-0-7356-2511-2 (англ.)
ISBN 978-5-7502-0368-0

Оригинальное издание на английском языке.
Anil Desai, J. C. Mackin. 2008
Перевод на русский язык, Microsoft Corporation, 2008
Оформление и подготовка к изданию, издательство «Русская Редакция». 2008

Краткое содержание

Введение XX

Глава 1. Развертывание Windows 1

Глава 2. Настройка серверной системы хранения данных и кластеров 74

Глава 3. Установка и настройка служб терминалов 122

Глава 4. Настройка инфраструктуры служб терминалов и управление ею 169

Глава 5. Установка и настройка веб-приложений 229

Глава 6. Управление безопасностью веб-сервера 296

Глава 7. Настройка служб FTP и SMTP 361

Глава 8. Настройка служб Windows Media 2008 418

Глава 9. Настройка служб Windows SharePoint Services 462

Приложение 509

Ответы 573

Словарь терминов 593

Содержание

Введение ... XX

Глава 1. Развертывание Windows ... **1**

Требования ... 1
Занятие 1. Развертывание Windows в среде Windows Server 2008 ... 2
Основы развертывания системы Windows ... 3
Что такое файл WIM ... 3
Утилиты автоматической установки Windows ... 4
Sysprep ... 7
Методы развертывания Windows ... 8
Загрузка с DVD-диска ... 8
Использование утилит Windows AIK и Network Share Distribution ... 9
Windows Deployment Services ... 10
System Center Configuration Manager 2007 ... 11
Практикум. Создание диска Windows PE ... 12
Упражнение 1. Создание диска Windows PE ... 12
Резюме ... 14
Закрепление материала ... 14
Занятие 2. Настройка Windows Deployment Services ... 14
Первое знакомство с Windows Deployment Services ... 15
WDS и утилиты Windows AIK ... 15
Преимущества WDS ... 16
Компоненты инфраструктуры WDS ... 16
Установка WDS ... 18
Настройка WDS ... 19
Начальная настройка сервера ... 19
Начальная настройка сервера WDS с помощью утилиты Wdsutil.exe ... 21
Добавление загрузочного образа по умолчанию ... 22
Добавление загрузочного образа с помощью утилиты Wdsutil.exe ... 23
Добавление установочного образа по умолчанию ... 24
Добавление установочного образа с помощью утилиты Wdsutil.exe ... 26
Другие задачи настройки ... 26
Захват образов с помощью WDS ... 28
Создание захваченного образа ... 29
Создание обзорного образа ... 30

Развертывание образов с помощью WDS....31
Ручное развертывание образа....31
Что происходит во время развертывания....33
Практикум. Настройка служб развертывания Windows....34
Упражнение 1. Добавление роли сервера развертывания Windows....34
Упражнение 2. Начальная настройка сервера....35
Упражнение 3. Добавление загрузочного и установочного образов....36
Упражнение 4. Добавление компьютера клиента в домен Contoso....37
Упражнение 5. Развертывание системы Windows Server 2008 с помощью WDS....38
Резюме....40
Закрепление материала....40
Занятие 3. Развертывание виртуальных машин....41
Что такое виртуальные машины....41
Зачем используют виртуальные машины....43
Virtual PC 2007....44
Virtual Server 2005 R2 SP1....48
Hyper-V....49
Программные и аппаратные требования....51
Создание виртуальной машины в Hyper-V....54
Типы виртуальных дисков....54
Настройка виртуальных сетей....55
Создание новых виртуальных сетей....55
Назначение виртуальных машин для виртуальных сетей....57
Резюме....58
Закрепление материала....59
Занятие 4. Применение инфраструктуры активации Windows....59
Типы активации продукта....60
Применение MAK-активации....60
Преимущества и недостатки MAK-лицензии....63
Применение KMS-активации....63
Минимальное количество KMS-клиентов....64
Обнаружение KMS-хоста....65
Установка и настройка KMS-хоста....66
Преимущества и недостатки KMS-лицензий....66
Пример инфраструктуры активации....67
Практикум. Активация системы Windows Server 2008....68
Упражнение 1. Создание диска Windows PE....68
Резюме....69
Закрепление материала....69
Закрепление материала главы....70
Резюме главы....70
Основные термины....71
Лабораторная работа....71
Задание 1. Службы развертывания....71
Задание 2. Создание инфраструктуры активации....71
Рекомендуемые упражнения....72
Пробный экзамен....73

Глава 2. Настройка серверной системы хранения данных и кластеров 74
Требования 74
Занятие 1. Настройка серверной системы хранения данных 75
Понимание технологий серверной системы хранения данных 75
Система хранения данных с прямым подключением к серверу 75
Система хранения данных, подключенная к сети 76
Сети хранения данных 77
Управление дисками, томами и разделами в операционной системе Windows Server 2008 82
Базовые и динамические диски 83
Создание томов 84
Расширение тома 91
Сжатие тома 91
Настройка точки монтирования 92
Практикум. Работа с наборами дисков 94
Упражнение 1. Работа с дисками и простыми томами 94
Упражнение 2. Создание точек монтирования 96
Упражнение 3. Добавление зеркального тома и разделение зеркального тома 98
Упражнение 4. Создание составного тома 99
Упражнение 5. Создание чередующегося тома 100
Упражнение 6. Сжатие и расширение тома 101
Резюме 102
Закрепление материала 103
Занятие 2. Настройка кластеров серверов 104
Основные принципы работы кластера серверов 104
Циклическое распределение 105
Балансировка сетевой нагрузки 106
Отказоустойчивость кластера 107
Настройка NLB-кластера 109
Создание отказоустойчивого кластера 111
Подготовка аппаратного обеспечения для отказоустойчивого кластера 111
Установка Средства отказоустойчивости кластеров 114
Проверка конфигурации кластера 114
Запуск Мастера создания кластера 115
Запуск Мастера высокой надежности 115
Тестирование отказоустойчивого кластера 116
Практикум. Анализ отказоустойчивости кластера 116
Упражнение 1. Просмотр демонстрационного ролика об отказоустойчивости кластера 116
Резюме 116
Закрепление материала 117
Закрепление материала главы 118
Резюме главы 118
Основные термины 119
Лабораторная работа 119
Задание 1. Проектирование хранилища данных 119
Задание 2. Проектирование высокой надежности 120

Рекомендуемые упражнения 120
Пробный экзамен 121
Глава 3. Установка и настройка служб терминалов 122
Требования 122
Занятие 1. Развертывание сервера терминалов 123
Службы терминалов 123
Службы терминалов и подключение к удаленному рабочему столу 124
Преимущества удаленного рабочего стола 126
Включение удаленного рабочего стола 127
Включение удаленного рабочего стола на компьютере с установленным ядром сервера 129
Установка служб терминалов 129
Выбор служб ролей 130
Удаление приложений 132
Выбор параметров сетевой проверки подлинности 132
Определение режима лицензирования клиентского доступа 133
Авторизация пользователей 135
Подготовка сервера терминалов 136
Установка встроенных компонентов Windows Server 2008 136
Установка приложений служб терминалов 138
Практикум. Установка сервера терминалов 139
Упражнение 1. Добавление и настройка роли Службы терминалов 139
Упражнение 2. Тестирование подключения к службам терминалов 140
Упражнение 3. Включение удаленного рабочего стола на компьютере с установленным ядром сервера Windows Server 2008 141
Резюме 142
Закрепление материала 142
Занятие 2. Настройка служб терминалов 143
Конфигурация служб терминалов 144
Настройка свойств подключения RDP-Tcp 145
Вкладка Общие 146
Вкладка Параметры входа в систему 147
Вкладка Сеансы 148
Вкладка Среда 149
Вкладка Удаленное управление 149
Вкладка Параметры клиента 150
Вкладка Сетевой адаптер 152
Вкладка Безопасность 152
Настройка свойств сервера служб терминалов 153
Вкладка Общие 153
Вкладка Лицензирование 155
Вкладка Посредник сеансов служб терминалов 156
Настройка перенаправления принтеров служб терминалов 158
Практикум. Установка и настройка сервера лицензирования 160
Упражнение 1. Установка роли сервера лицензирования служб терминалов 160
Упражнение 2. Активация сервера лицензирования служб терминалов 161
Упражнение 3. Установка лицензий служб терминалов TS CAL 163

Резюме 164
Закрепление материала 164
Закрепление материала главы 165
Резюме главы 166
Основные термины 166
Лабораторная работа 166
Задание 1. Выбор стратегии лицензирования служб терминалов 167
Задание 2. Устранение неполадок служб терминалов 167
Рекомендуемое упражнение 167
Пробный экзамен * 168
Глава 4. Настройка инфраструктуры служб терминалов и управление ею 169
Требования 169
Занятие 1. Конфигурирование клиентов служб терминалов и управление ими 170
Настройка клиентских параметров служб терминалов 170
Опции конфигурирования подключения к удаленному рабочему столу 171
Сохранение RDP-файлов 175
Настройка клиентов служб терминалов с помощью групповой политики 175
Конфигурирование пользовательских профилей для служб терминалов 176
Настройка домашних папок 178
Управление пользовательскими подключениями к службам терминалов 178
Управление пользовательскими сеансами 180
Завершение процесса сеанса пользователя TS 183
Управление ресурсами в клиентских сеансах 184
Практикум. Управление клиентскими подключениями 185
Упражнение 1. Просмотр сеансов служб терминалов 185
Упражнение 2. Управление сеансами служб терминалов 187
Упражнение 3. Повторное подключение к отключенному сеансу 188
Резюме 190
Закрепление материала 190
Занятие 2. Развертывание шлюза служб терминалов 191
Шлюз служб терминалов 192
Установка и настройка сервера шлюза служб терминалов 194
Добавление роли службы шлюза TS 194
Настройка подключения к удаленному рабочему столу с целью использования шлюза служб терминалов 199
Практикум. Установка и настройка шлюза служб терминалов 201
Упражнение 1. Добавление служб ролей шлюза TS 201
Упражнение 2. Создание консоли Сертификаты для управления сертификатами 202
Упражнение 3. Экспорт сертификата сервера 203
Упражнение 4. Импорт сертификата сервера 204
Упражнение 5. Подключение к шлюзу служб терминалов с помощью RDC 205
Резюме 206
Закрепление материала 206
Занятие 3. Публикация приложений с помощью утилиты RemoteApp 207
Удаленные приложения RemoteApp служб терминалов 208
Настройка сервера для программ RemoteApp 209

Добавление программ для публикации в диспетчере RemoteApp 210
Развертывание приложения RemoteApp через веб-достуи к службам терминалов 211
Создание RDP-файла приложения RemoteApp 213
Создание пакета установщика Windows для распределения удаленного приложения RemoteApp 215
Практикум. Публикация приложений с помощью диспетчера RemoteApp 218
Упражнение 1. Установка службы роли Веб-доступ к службам терминалов 218
Упражнение 2. Публикация приложения для веб-доступа к службам терминалов 219
Упражнение 3. Запуск удаленного приложения через веб-доступ к службам терминалов 219
Упражнение 4. Создание общего дистрибутивного ресурса 220
Упражнение 5. Создание RDP-файла опубликованного приложения 220
Упражнение 6. Запуск удаленного приложения с помощью локального RDP-файла 221
Упражнение 7. Создание пакета установщика Windows удаленного приложения RemoteApp для распространения 221
Упражнение 8. Установка удаленного приложения 223
Резюме 223
Закрепление материала 224
Закрепление материала главы 224
Резюме главы 225
Основные термины 225
Лабораторная работа 226
Задание 1. Управление сеансами служб терминалов 226
Задание 2. Публикация приложений 226
Рекомендуемые упражнения 227
Пробный экзамен 228
Глава 5. Установка и настройка веб-приложений 229
Требования 229
Занятие 1. Установка роли веб-сервера (IIS) 230
Безопасность веб-сервера 231
Веб-стандарты и протоколы 231
Сценарии с использованием веб-сервера 232
Новые компоненты IIS 234
Компоненты и опции IIS 235
Сервер приложений 236
Службы ролей IIS 7.0 238
Службы ролей IIS по умолчанию 240
Основные возможности HTTP 240
Разработка приложений 241
Работоспособность и диагностика 242
Безопасность 244
Быстродействие 245
Средства управления 246

Установка роли Веб-сервер (IIS) 246
Проверка установки IIS с помощью диспетчера сервера 249
Проверка установки IIS с помощью Internet Explorer 250
Управление службами ролей 251
Использование командной строки и опций автоматизированной установки 252
Удаление роли Веб-сервер (IIS) 253
Диспетчер системных ресурсов Windows 254
Практикум. Установка и проверка роли Веб-сервер (IIS) 255
Упражнение 1. Установка роли Веб-сервер (IIS) 255
Упражнение 2. Тестирование IIS 256
Резюме 256
Закрепление материала 257
Занятие 2. Настройка Internet Information Services 257
Средства управления IIS 258
Просмотр возможностей 259
Просмотр содержимого 261
Панель действий 262
Создание и настройка веб-сайтов 262
Сайты и привязка сайтов 262
Управление веб-сайтом по умолчанию 264
Добавление веб-сайтов 264
Настройка ограничений для веб-сайта 266
Настройка ведения журнала 267
Веб-приложения 268
Создание веб-приложений 268
Управление параметрами веб-приложений 269
Пулы приложений 270
Создание пулов приложений 270
Управление пулами приложений 272
Настройка параметров перезапуска 272
Настройка дополнительных параметров пула приложений 274
Виртуальные каталоги 274
Создание виртуального каталога 275
Сравнение виртуальных каталогов и веб-приложений 275
Управление из командной строки 275
Командные опции 276
Объекты 277
Примеры команды 277
Windows PowerShell 278
Выполнение автоматизации с использованием .NET Framework 278
Управление файлами конфигурации веб-сервера 279
Файл ApplicationHost.config 279
Восстановление файла AppllicationHost.config 280
Файлы Web.config 280
Миграция веб-сайтов и веб-приложений 281

Архивация и восстановление данных конфигурации с помощью утилиты AppCmd.exe ... 281
Использование централизованной конфигурации для ферм серверов ... 283
Миграция с версии IIS 6.0 ... 285
Обновление Windows Server 2003 и IIS 6.0 ... 285
Совместимость средств управления IIS 6.0 ... 286
Режимы интеграции ASP.NET ... 287
Практикум. Настройка параметров IIS и управление ими ... 287
Упражнение 1. Создание веб-сайтов и веб-приложений ... 288
Упражнение 2. Архивация и восстановление параметров конфигурации IIS ... 290
Резюме ... 291
Закрепление материала ... 291
Закрепление материала главы ... 292
Резюме главы ... 292
Основные термины ... 293
Лабораторная работа ... 293
Задание 1. Администрирование веб-сервера IIS ... 293
Задание 2. Управление множеством веб-сайтов ... 294
Рекомендуемые упражнения ... 294
Пробный экзамен ... 295
Глава 6. Управление безопасностью веб-сервера ... 296
Требования ... 296
Занятие 1. Настройка безопасности IIS ... 298
Учетные записи безопасности IIS 7.0 ... 299
Управление разрешениями файловой системы ... 299
Настройка компонентов администрирования IIS ... 300
Включение удаленного управления ... 301
Пользователи диспетчера IIS ... 303
Создание пользователей диспетчера IIS ... 303
Определение разрешений управления IIS ... 304
Настройка делегирования компонента ... 305
Подключение к удаленному серверу с помощью диспетчера IIS ... 308
Управление обработчиками запросов ... 311
Сопоставления обработчиков запросов ... 312
Настройка сопоставлений обработчиков ... 313
Удаление сопоставлений обработчиков ... 315
Управление наследованием обработчиков ... 316
Добавление сопоставлений обработчиков ... 316
Настройка ограничений запроса ... 318
Настройка разрешений функции ... 319
Практикум. Управление параметрами безопасности IIS ... 320
Упражнение 1. Настройка удаленного администрирования и управление им ... 320
Упражнение 2. Управление сопоставлениями обработчиков ... 322
Резюме ... 323
Закрепление материала ... 323

Занятие 2. Контроль доступа к веб-службам 324
Управление проверкой подлинности IIS 325
Анонимная проверка подлинности 325
Проверка подлинности с помощью форм 327
Проверка подлинности с запросом 328
Олицетворение ASP.NET 329
Проверка подлинности с помощью клиентских сертификатов 329
Требования проверки подлинности 330
Настройка параметров проверки подлинности 331
Управление правилами авторизации URL 333
Создание правил авторизации URL 333
Управление наследованием правил 335
Настройка сертификатов сервера 335
Сертификаты сервера 335
Создание запроса сертификата Интернета 336
Запрос установки сертификата Интернета 338
Создание сертификатов других типов 339
Создание самозаверяющих сертификатов 340
Просмотр сведений о сертификате 342
Импорт и экспорт сертификатов 343
Включение Secure Sockets Layer 344
Настройка ограничений по IP-адресам и именам домена 345
Добавление запрещающих и разрешающих элементов 346
Добавление доменных ограничений 347
Настройка уровней доверия .NET 349
Уровни ограниченного доверия 350
Уровни доверия .NET 350
Настройка уровней доверия .NET 351
Практикум. Безопасность веб-серверов и веб-содержимого 353
Упражнение 1. Управление параметрами проверки подлинности и их тестирование 353
Упражнение 2. Настройка сертификатов сервера 354
Резюме 355
Закрепление материала 355
Закрепление материала главы 356
Резюме главы 357
Основные термины 357
Лабораторная работа 357
Задание 1. Настройка удаленного управления для IIS 357
Задание 2. Повышение уровня безопасности веб-сайта 358
Рекомендуемые упражнения 358
Пробный экзамен 360
Глава 7. Настройка служб FTP и SMTP 361
Требования 361
Занятие 1. Конфигурирование FTP 361
Установка службы FTP-публикации 363
Удаление службы FTP-публикации 364

Настройка FTP-сайтов с помощью диспетчера служб IIS 6.0 ... 364
Создание FTP-сайта ... 365
Настройка свойств FTP-сайта ... 366
Настройка безопасных учетных записей ... 368
Сообщения FTP-сервера ... 369
Настройка опций корневого каталога ... 369
Управление параметрами безопасности каталога ... 371
Установка FTP 7 и управление им ... 371
Управление FTP-сайтами ... 372
Создание FTP-сайта ... 372
Файлы конфигурации FTP 7 ... 375
Создание виртуальных каталогов ... 375
Настройка дополнительных свойств FTP-сайта ... 376
Управление привязками FTP-сайта ... 377
Управление безопасностью FTP-пользователя ... 378
Настройка опций проверки подлинности ... 378
Определение правил авторизации FTP ... 380
Настройка опций изоляции пользователей FTP ... 381
Настройка разрешений диспетчера служб IIS ... 383
Настройка сетевой безопасности FTP ... 384
Настройка параметров SSL для FTP-сайта ... 384
Управление опциями брандмауэра FTP ... 386
Реализация ограничений по IP-адресам и именам домена ... 387
Управление параметрами FTP-сайта ... 388
Мониторинг текущих сеансов FTP ... 388
Управление сообщениями FTP ... 389
Настройка ведения журнала FTP ... 390
Настройка просмотра каталога ... 391
Программное обеспечение FTP-клиента ... 392
Практикум. Настройка и тестирование FTP ... 394
Упражнение 1. Использование FTP 6 для создания нового веб-сайта ... 394
Упражнение 2. Использование FTP 7 для добавления привязки FTP-узла ... 396
Резюме ... 397
Закрепление материала ... 397
Занятие 2. Конфигурирование SMTP ... 398
Установка сервера SMTP ... 399
Настройка служб SMTP ... 399
Создание виртуального сервера SMTP ... 399
Настройка основных параметров сервера SMTP ... 401
Безопасность доступа к виртуальному серверу SMTP ... 402
Настройка сообщений ... 405
Свойства доставки ... 406
Включение маршрутизации LDAP ... 408
Управление разрешениями безопасности ... 408
Мониторинг виртуальных серверов SMTP ... 409

Использование виртуального сервера SMTP 409
Утилита Telnet 410
Использование клиентского приложения для обмена сообщениями 410
Настройка параметров SMTP для ASP.NET 410
Практикум. Конфигурирование и тестирование служб SMTP 412
Упражнение 1. Создание нового виртуального сервера SMTP 412
Резюме 413
Закреплен ие материала 413
Закрепление материала главы 414
Резюме главы 414
Основные термины 415
Лабораторная работа 415
Задание 1. Реализация сайта Secure FTP 415
Задание 2. Настройка виртуального сервера SMTP 415
Рекомендуемые упражнения 416
Пробный экзамен 417
Глава 8. Настройка служб Windows Media 2008 418
Требования 419
Занятие 1. Настройка служб Windows Media 419
Службы Windows Media 419
Доставка транслируемого и предварительно записанного содержимого 420
Одноадресный и многоадресный потоки мультимедиа 420
Протоколы передачи данных 421
Установка служб потокового мультимедиа 421
Средства управления службами Windows Media 424
Управление пунктами публикации 427
Создание нового пункта публикации 427
Администрирование пунктов публикации 431
Наблюдение за пунктами публикации 432
Настройка параметров источника 433
Создание объявлений 434
Мастер создания сопровождения 435
Мастер одноадресных объявлений 436
Мастер многоадресных объявлений 438
Настройка свойств пункта публикации 440
Управление параметрами рекламы 442
Настройка безопасности служб Windows Media 443
Настройка проверки подлинности 444
Настройка опций авторизации 445
Разрешения веб-сервера 447
Управление прокси-сервером с кэшем 447
Включение параметров кэш/прокси-серверов 448
Настройка параметров кэширования 449
Настройка параметров прокси 451
Настройка параметров кэш/прокси для пунктов публикации 451
Мониторинг кэш/прокси-серверов 451

Обеспечение защиты мультимедиа с помощью DRM ... 452
Сторонний партнер DRM ... 452
Службы управления правами Active Directory ... 453
Другие методы обеспечения защиты содержимого ... 453
Практикум. Настройка служб Windows Media ... 453
Упражнение 1. Установка служб потокового мультимедиа ... 453
Упражнение 2. Создание и проверка нового пункта публикации ... 455
Резюме ... 456
Закрепление материала ... 457
Закрепление материала главы ... 458
Резюме главы ... 459
Основные термины ... 459
Лабораторная работа ... 459
Задание 1. Защита содержимого потокового мультимедиа ... 459
Задание 2. Повышение производительности и расширяемости сервера Windows Media ... 460
Рекомендуемые упражнения ... 460
Настройка служб Windows Media ... 460
Пробный экзамен ... 461
Глава 9. Настройка служб Windows SharePoint Services ... 462
Требования ... 462
Занятие 1. Настройка служб Windows SharePoint Services и управление ими ... 462
Службы Windows SharePoint Services ... 464
Опции развертывания WSS ... 465
Развертывание WSS в автономной конфигурации ... 465
Развертывание WSS в конфигурации фермы серверов ... 466
Мастер настройки продуктов и технологии SharePoint ... 467
Проверка установки WSS ... 468
Проверка ролей и параметров сервера ... 468
Проверка веб-сайтов WSS ... 469
Центр администрирования SharePoint ... 471
Выполнение административных задач ... 471
Навигация на веб-сайте центра администрирования SharePoint ... 472
Управление операциями SharePoint ... 475
Управление параметрами безопасности ... 474
Настройка параметров электронной почты ... 476
Управление параметрами ведения журнала ... 479
Обработка сведений об использовании ... 480
Определения заданий ... 481
Управление WSS с помощью утилиты stsadm ... 482
Резервное копирование и восстановление в WSS ... 483
Создание резервных копий SharePoint ... 483
Восстановление Windows SharePoint Services ... 485
Журнал резервного копирования и восстановления ... 487
Развертывание и конфигурирование сайтов SharePoint ... 487
Подузлы и семейства узлов ... 488
Создание семейства узлов ... 489

Определение шаблонов квот ... 491
Настройка параметров сайта ... 493
Управление веб-приложениями ... 494
Настройка общих параметров веб-приложений ... 495
Определение управляемых путей ... 497
Настройка разрешений веб-приложений ... 497
Управление параметрами проверки подлинности ... 499
Управление средствами самостоятельного создания сайтов ... 500
Установка шаблонов приложений ... 500
Практикум. Настройка и управление службами Windows SharePoint Services ... 501
Упражнение 1. Настройка сайтов и семейств узлов WSS ... 501
Упражнение 2. Резервное копирование и восстановление сайта Windows SharePoint ... 503
Резюме ... 505
Закрепление материала ... 505
Закрепление материала главы ... 506
Резюме главы ... 506
Основные термины ... 506
Лабораторная работа ... 507
Задание 1. Развертывание Windows SharePoint Services ... 507
Задание 2. Управление Windows SharePoint Services ... 507
Рекомендуемые упражнения ... 508
Пробный экзамен ... 508
Приложение. Развертывание Windows Server 2008 ... 509
Ответы ... 573
Словарь терминов ... 593

Введение

Эта книга предназначена для профессионалов в области информационных технологий (IT), которые занимаются поддержкой сетей Windows Server 2008 и в связи с этим хотели бы сдать сертификационный экзамен 70-643 на звание сертифицированного технического специалиста Microsoft MCTS (Microsoft Certified Technology Specialist). Предполагается, что читатель знаком с основами технологий, используемых клиентом Windows, серверных операционных систем и распространенных технологий Интернета.

Рассматриваемые в книге темы по сути являются темами сертификационного экзамена 70-643. Речь в первую очередь идет о сетевых технологиях Windows Server 2008, поддерживающих распределенный доступ к веб-содержимому, мультимедиа, операционным системам и приложениям. Изучив излагаемый здесь материал, вы сможете выполнять следующие действия:

- развертывать серверы и клиенты Windows в сети с помощью Служб развертывания Windows (Windows Deployment Services) и программного пакета Windows Automated Installation Kit (WAIK);
- конфигурировать Hyper-V и другие технологии виртуализации;
- конфигурировать решения хранилищ для серверов;
- настраивать в Windows Server 2008 Службы терминалов (Terminal Services) и управлять ими;
- настраивать службы Internet Information Services 7.0 и управлять ими;
- конфигурировать службы Windows Media (Windows Media Services);
- настраивать Windows SharePoint Services.

ПРИМЕЧАНИЕ Поиск дополнительной информации в Интернете
Новый или обновленный материал для данной книги доступен на регулярно обновляемом веб-сайте Microsoft Press Online Windows Server and Client. Это могут быть обновления книги, статьи, списки опечаток и т. д. Указанный сайт вы найдете по адресу *www.microsoft.com/learning/books/online/serverclient.*

Требования к оборудованию (Virtual PC)

Чтобы сэкономить время и снизить стоимость конфигурирования физических компьютеров, при изучении материала данной книги рекомендуется использо-

вать программное обеспечение версии не ниже Virtual PC 2007, которое можно загрузить по адресу *http://w7ciw.microsoft.com/downloads.* Вы, конечно, можете воспользоваться другим программным обеспечением, например Virtual Server R2 или Hyper-V, однако в инструкциях по установке предполагается, что это будет именно Virtual PC. Если вы не используете программное обеспечение для виртуализации, переходите к разделу с описанием требований к физическому оборудованию.

В случае использования программного обеспечения для виртуализации вы сможете выполнять рекомендуемые в книге упражнения на одном физическом компьютере. Такой физический хост-компьютер должен соответствовать следующим минимальным требованиям:

- процессор с частотой 1 ГГц;
- оперативная память объемом не менее 2 Гбайт (рекомендуется в случае использования Windows Vista и Windows Server 2008 в качестве главной операционной системы в виртуальной среде);
- 80 Гбайт доступного дискового пространства на жестком диске;
- привод DVD-ROM;
- наличие подключения к Интернету.

Требования к оборудованию (физическая машина)

Если вы решили вместо программного обеспечения использовать для виртуализации физические компьютеры, они должны соответствовать минимальным требованиям к оборудованию, изложенным ниже.

- Три компьютера с процессором 1 ГГц, с 512 Мбайт оперативной памяти, сетевой картой, видеокартой и приводом DVD-ROM.
- Требования хранилища:
  - компьютер 1 (Serverl) должен располагать одним подключенным жестким диском объемом не менее 20 Гбайт;
  - компьютер 2 (Server2) должен располагать как минимум двумя, а лучше — тремя подключенными жесткими дисками, объем каждого из которых составлял бы не менее 15 Гбайт;
  - компьютер 3 (Corel) должен располагать одним подключенным жестким диском объемом не менее 5 Гбайт.
- Все три компьютера должны быть физически подключены друг к другу и к Интернету.
- Сетевой адаптер на компьютере 2 (Server2) должен быть совместим с предзагрузочной средой исполнения PXE (Preboot Execution Environment).
- Если сеть не имеет шлюза Интернета, на компьютере 1 (Serverl) потребуется установить еще один сетевой адаптер, который будет выполнять роль шлюза Интернета для двух других компьютеров.
- Тестовая сеть, включающая указанные компьютеры, должна быть изолирована от производственной сети. (В частности, тестовая сеть не должна сразу включать DHCP-сервер, который автоматически назначает адреса компьютерам.)

Требования к программному обеспечению

Для выполнения практических упражнений, предлагаемых в рамках данной книги, потребуется программное обеспечение, перечисленное далее.

Если вы используете Virtual PC 2007 для выполнения упражнений в виртуальной среде, на физическом хост-компьютере должна быть установлена операционная система Windows и сетевые драйверы.

На время написания этой книги программное обеспечение Virtual PC 2007 официально поддерживалось в системах Windows Vista Business, Windows Vista Enterprise, Windows Vista Ultimate, Windows XP Professional и Windows XP Tablet PC Edition. На веб-сайте Virtual PC, расположеному по адресу *http://www.microsoft.com/windows/products/winfamily/virtualpc/default.mspx,* представлена обновляемая информация об операционных системах, которые можно запускать в Virtual PC.

Вам также необходимо иметь в своем распоряжении систему Windows Server 2008. Ознакомительный выпуск (Evaluation Edition) Windows Server 2008 можно загрузить в центре загрузок Microsoft по адресу *http://www.microsoft.com/downloads.* Отметим, что в Virtual PC следует использовать 32-разрядную версию Windows Server 2008.

Обязательно установите программный пакет Windows Automated Installation Toolkit (WAIK) — его также можно скачать в центре загрузок Microsoft.
Если вы не используете виртуализацию, вам потребуется программное обеспечение для управления файлами .iso и .img. Это программное обеспечения должно выполнять следующие функции (либо какую-то одну из них):

- записывать файлы .iso и .img на CD и DVD (кроме того, потребуется пишущий привод CD/DVD);
- подключать файлы .iso и .img как виртуальные диски CD/DVD на компьютере.

Инструкции по установке

Для выполнения рекомендуемых упражнений нужно подготовить, как уже было сказано, три компьютера. В приведенных ниже инструкциях предполагается, что вы используете версию программного обеспечения не ниже Virtual PC 2007 на хост-компьютере, соответствующем минимальным требованиям к оборудованию, которые изложены в разделе «Требования к оборудованию (Virtual PC)». Если вы выбрали для виртуализации другое программное обеспечение или решили работать с физическими компьютерами, то на основе следующих инструкций сможете определить общие требования к установке, однако вам придется настроить эти инструкции в соответствии со своей средой.

ВНИМАНИЕ! Загрузка требуемого программного обеспечения

Прежде чем приступать к подготовке компьютеров, вам нужно обзавестись копией Windows Server 2008 (в виде файла .iso или на DVD-диске) и программным пакетом Windows Automated Installation Kit (в виде файла .img или на DVD-диске).

Установка среды для выполнения упражнений производится в четыре этапа. На первом этапе создаются три виртуальные машины. Конфигурация виртуального оборудования виртуальных машин на данном этапе продемонстрирована на рис. В-1.

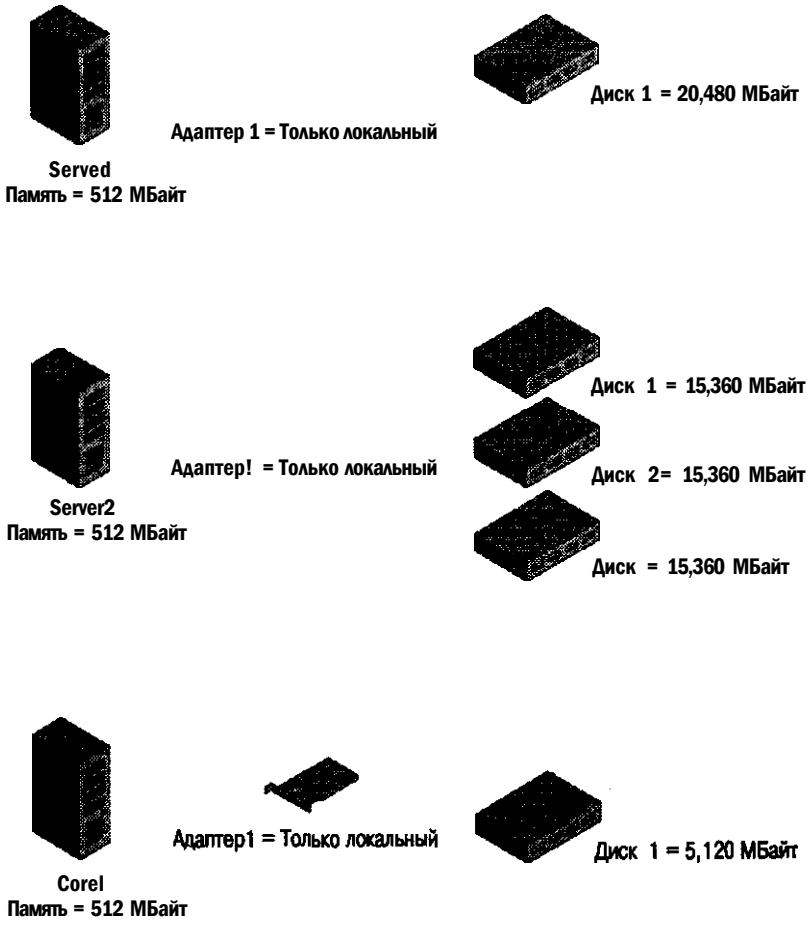


Рис. В-1. Конфигурация оборудования для трех компьютеров в Virtual PC

На втором этапе виртуализации выполняется конфигурирование программного обеспечения для машин Serverl и Corel. (Конфигурировать программное обеспечение для машины Server2 не нужно, поскольку этот компьютер будет оставлен в виде «голого» (Bare-Metal) виртуального оборудования.)

На третьем этапе настройки для всех трех компьютеров конфигурируется подключение к Интернету В результате выполнения этих действий на Serverl будет добавлен второй виртуальный сетевой адаптер и настроен процесс преобразования сетевых адресов NAT (Network Address Translation) для двух адаптеров (рис. В-2).

На последнем, четвертом, этапе установки среды выполняется активация серверов Serverl и Corel через Интернет.

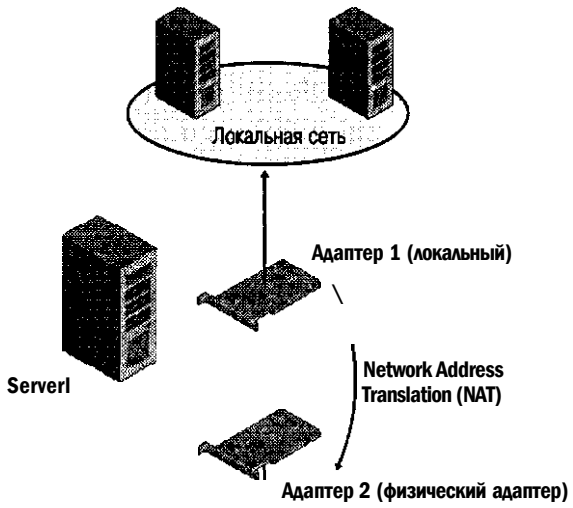


Рис. В-2. Обеспечение подключения к Интернету для всех трех компьютеров в Virtual PC

Этап 1. Создание виртуальных машин

Итак, вначале вам необходимо создать виртуальные машины, на которых будут выполняться рекомендуемые упражнения.

Создание виртуальной машины Server1

В консоли Virtual PC щелкните кнопку New, чтобы запустить мастер создания новой виртуальной машины New Virtual Machine Wizard, а затем щелкните Создать виртуальную машину (Create a Virtual Machine) и укажите следующие параметры:

- имя и местоположение новой виртуальной машины — Server1 (если вы укажете лишь имя машины, то будет использоваться местоположение по умолчанию);

- операционная система — Windows Server 2008 (если эта опция недоступна в вашей версии Virtual PC 2007, загрузите и установите Service Packl для Virtual PC в центре загрузки Microsoft);
- оперативная память — 512 Мбайт (при выборе операционной системы Windows Server 2003 программа Virtual PC предлагает использовать 256 Мбайт оперативной памяти, в таком случае измените рекомендуемый объем оперативной памяти — установите 512 Мбайт);
- размер виртуального жесткого диска — 20 480 Мбайт.

Конфигурирование сетевого адаптера в Virtual PC После создания новой (пустой) виртуальной машины Serverl в консоли Virtual PC откройте параметры машины Serverl. Затем для Adapter 1 выберите параметр подключения Local Only, как показано на рис. B-3. Второй адаптер пока не добавляйте.

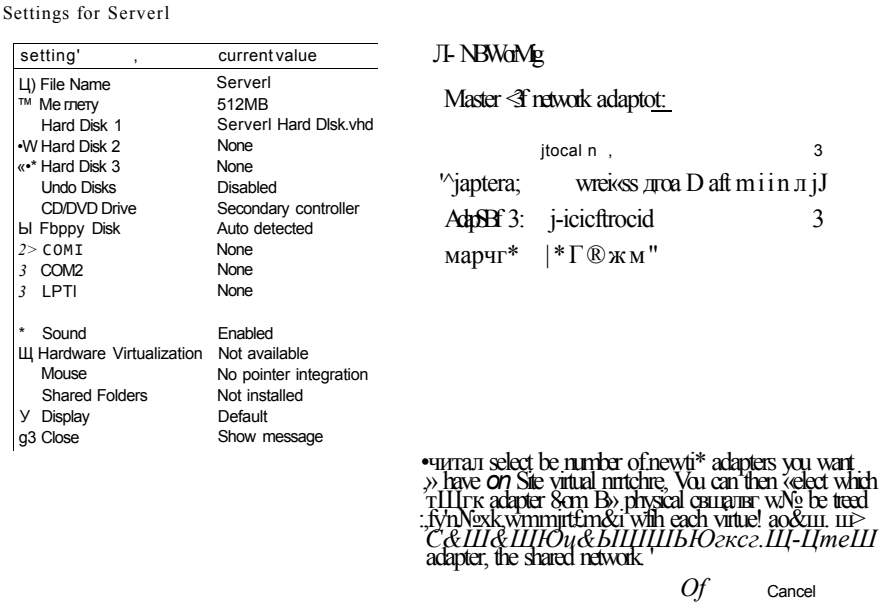


Рис. B-3. Настройка адаптера 1 для машины Serverl в Virtual PC

Создание виртуальной машины Corel

С помощью мастера New Virtual Machine Wizard создайте вторую виртуальную машину. Отконфигурируйте все параметры аналогично настройкам виртуальной машины Serverl (в частности, сетевой адаптер), за исключением следующих, для которых укажите такие значения:

- имя и местоположение новой виртуальной машины — Corel;
- размер виртуального жесткого диска — 5129 Мбайт.

Создание виртуальной машины Server2

С помощью мастера New Virtual Machine Wizard создайте последнюю виртуальную машину. Отконфигурируйте все параметры аналогично настройкам

виртуальной машины Serverl (в том числе сетевой адаптер), за исключением следующих — для них укажите такие значения:

- имя и местоположение новой виртуальной машины — Server2;
- размер виртуального жесткого диска — 15 360 Мбайт.

ВНИМАНИЕ! Использование унаследованных адаптеров для Server2 в Hyper-V
Если вы создаете свои серверы в среде Hyper-V, а не с помощью Virtual PC, отконфигурируйте сетевой адаптер на машине Server2 как унаследованный (или эмулированный) адаптер. В противном случае адаптер будет несовместим с PXE. Это необходимо для развертывания Windows Server 2008 на машине Server2 при выполнении упражнения в рамках занятия 1 в главе 2.

Настройка второго и третьего жесткого диска для Server2 В консоли Virtual PC откройте параметры виртуальной машины Server2. В диалоговом окне Settings For Server2 выберите в левой панели диск Hard Disk 2 и щелкните кнопку Virtual Hard Disk Wizard. С помощью мастера Virtual Hard Disk Wizard создайте виртуальный жесткий диск и задайте для него имя и местоположение. Выберите для диска опцию Динамическое расширение (Dynamically Expanding) и укажите размер диска — 15 360 Мбайт. После создания виртуального диска в диалоговом окне Settings For Server2 щелкните опцию Файл виртуального жесткого диска (Virtual Hard Disk File) и выберите созданный виртуальный диск.

И наконец, точно таким же образом создайте для машины Server2 виртуальный диск Hard Disk 3 объемом 15 360 Мбайт и подключите его.

После добавления еще двух виртуальных жестких дисков в окне параметров Server2 должны быть указаны VHD-файлы всех трех жестких дисков (рис. B-4).

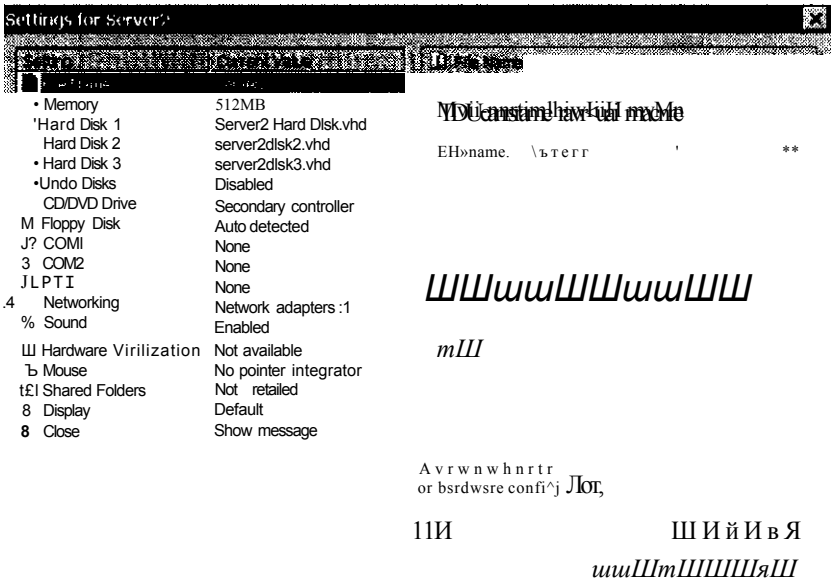


Рис. B-4. Виртуальная машина Server2 с тремя подключенными виртуальными жесткими дисками

Этап 2. Настройка операционных систем на машинах Server1 и Core1

Настраивая компьютеры Server1 и Core1, вы должны следовать приведенным ниже инструкциям.

Настройка машины Server1

Машина Server1 будет использоваться как DHCP-сервер, DNS-сервер и контроллер Active Directory домена contoso.com. На этой машине также нужно установить пакет WAIK. Для конфигурирования сервера выполните следующие действия.

1. В консоли Virtual PC запустите виртуальную машину Server1 и подключите к ней DVD-диск Windows Server 2008 или образ ISO, как показано на рис. B-5. (Напомним, что для захвата ISO- либо IMG-файла можно использовать команду Capture ISO Image.)

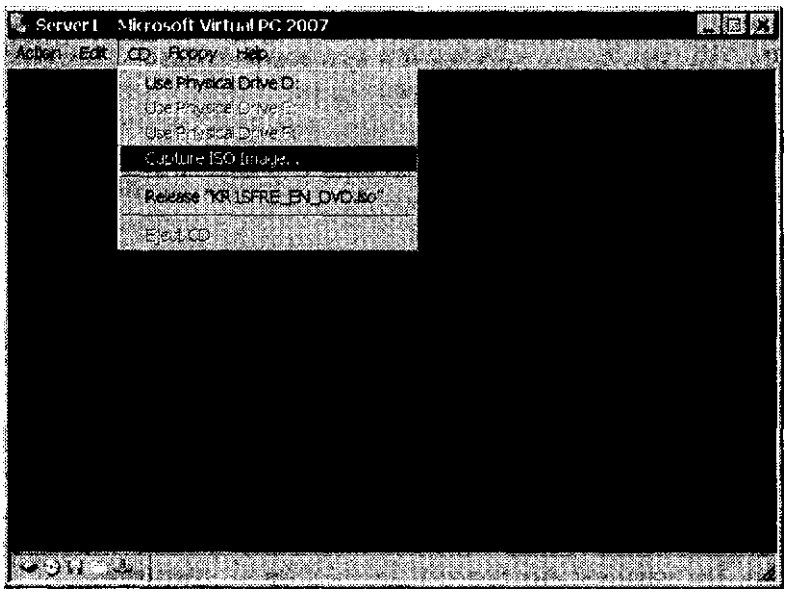


Рис. B-5. Подключение ISO-файла к виртуальной машине

2. Выполните установку Windows Server 2008 с опциями по умолчанию. Примите во внимание следующие директивы.
   - При желании выберите язык и клавиатуру, соответствующие вашему региону.
   - Ключ продукта пока не вводите.
   - Выберите выпуск Windows Server 2008 Standard (Полная установка) или Windows Server 2008 Enterprise (Полная установка).
   - Установите Windows в разделе по умолчанию Незанятое место на диске О (Disk 0 Unallocated Space).
   - При первом входе в систему в качестве администратора воспользуйтесь строгим паролем по своему усмотрению.

- После того как вы войдете в систему в качестве администратора, автоматически откроется окно Задачи начальной настройки (Initial Configuration Tasks).

3. На машине Serverl отконфигурируйте подключение по локальной сети (Local Area Connection). Это можно сделать в окне Задачи начальной настройки (Initial Configuration Tasks) или с помощью командной строки. В указанном окне щелкните ссылку Настроить сеть (Configure Networking), откройте окно свойств подключения по локальной сети (Local Area Connection) и отконфигурируйте свойства протокола TCP/IPv4, используя указанные опции и значения.
   - Щелкните опцию Использовать следующий IP-адрес (Use The Following IP Address) и задайте параметры конфигурации:
     - IP-адрес - 192.168.10.1;
     - маска подсети — 255.255.255.0;
     - основной шлюз — оставьте пустым.
   - Щелкните опцию Использовать следующие адреса DNS-серверов (Use The Following DNS Server Addresses) и назначьте параметры DNS:
     - предпочитаемый DNS-сервер — 192.168.101;
     - альтернативный DNS-сервер — оставьте пустым.
   - Чтобы отконфигурировать те же параметры с помощью командной строки, последовательно введите две команды:

     netsh interface ipv4 set address "local area connection" static 192.168.10.1

     255.255.255.0

     netsh interface ipv4 set dns "local area connection" static 192.168.10.1

   - Задайте имя компьютера. Это можно сделать в окне Задачи начальной настройки (Initial Configuration Tasks) или с помощью командной строки.
   - В том же окне щелкните ссылку Указать имя компьютера и домен (Provide Computer Name And Domain). Затем щелкните кнопку Изменить (Change) и укажите для машины имя Serverl; домен пока не указывайте.
   - Чтобы указать имя компьютера с помощью командной строки, введите команду:

     netdom renamecomputer %computername% /newname:Server1 /reboot

4. С помощью окна Выполнить (Run) меню Пуск (Start) запустите утилиту Dcpromo и отконфигурируйте Serverl как контроллер нового домена Active Directory с именем contoso.com. В окнах Мастера установки доменных служб Active Directory (Active Directory Domain Services Installation Wizard) произведите следующие установки:
   - щелкните опцию Создать новый домен в новом лесе (Create A New Domain In A New Forest);
   - задайте полное доменное имя корневого домена леса (FQDN Of The Forest Root) — *contoso.com;*

- оставьте флажок DNS-сервер (по умолчанию) в дополнительных параметрах контроллера домена (Additional Domain Controller Options);
- в окне предупреждения о динамическом назначении IP-адресов щелкните опцию Да (Yes);
- в окне предупреждения о невозможности делегирования для этого DNS-сервера щелкните опцию Да (Yes);
- оставьте размещение по умолчанию базы данных, файлов журнала, а также SYSVOL;
- пароль администратора для режима восстановления служб каталогов (Directory Services Restore Mode Administrator Password) введите no своему усмотрению.

5. После того как Мастер установки доменных служб Active Directory (Active Directory Domain Services Installation Wizard) завершит работу, сразу перезагрузите Serverl, а затем войдите в домен contoso.com с машины Serverl как CONTOSOX Администратор.

ВНИМАНИЕ! Вход на компьютер в Virtual PC

Отметим, что в Virtual PC при использовании комбинации клавиш Ctrl+Alt+Del нужно нажимать Alt справа+Del.

6. В окне Задачи начальной настройки (Initial Configuration Tasks) щелкните ссылку Добавить роли (Add Roles) и с помощью Мастера добавления ролей (Add Roles Wizard) добавьте роль DHCP-сервер (DHCP Server) с указанными опциями.
   - Привязки сетевых подключений (Network Connection Bindings) — по умолчанию (оставьте флажок 192.168.10.1).
   - Параметры IPv4 для DNS-сервера (IPv4 DNS Server Settings):
     - Родительский домен (Parent Domain) — contoso.com;
     - 1Py4-адрес основного DNS-сервера (Preferred DNS Server IPv4 Address) - 192.168.10.1;
     - 1Py4-адрес дополнительного DNS-сервера (Alternate DNS Server IPv4 Address) — оставьте поле пустым.
   - Параметры WINS-сервера — устанавливать не нужно, поскольку WINS-сервер не требуется.
   - Добавьте DHCP-область (DHCP Scope) со следующей спецификацией:
     - Имя области (Scope Name) — Contoso.com;
     - Начальный IP-адрес (Starting IP Address) — 192.168.10.2;
     - Конечный IP-адрес (Ending IP Address) - 192.168.10.10;
     - Маска подсети (Subnet Mask) — 255.255.255.0;
     - Основной шлюз (Default Gateway) — 192.168.10.1 (предполагается использовать конфигурацию доступа в Интернет, описанную на этапе 3);
     - Тип подсети (Subnet Type) — Проводной (Wired);
     - флажок Активировать эту область (Activate This Scope) — не устанавливайте;

- Режим DHCPv6 без отслеживания состояния (DHCPv6 Stateless Mode) — оставьте параметр по умолчанию;
- Параметры DNS-сервера IPv6 (IPv6 DNS Server Settings) — оставьте параметр по умолчанию;
- Авторизация DHCP-сервера (Authorize DHCP Server) — оставьте параметр по умолчанию.

7. Создайте три учетные записи администраторов домена, руководствуясь представленными ниже пошаговыми инструкциями.
   а) В дереве административной консоли Active Directory — пользователи и компьютеры (Active Directory Users And Computers) разверните узел contoso.com и найдите папку Users.
   б) Щелкните папку Users правой кнопкой мыши, в контекстном меню выберите Создать\Пользователь (New\User).
   в) В диалоговом окне Новый объект — Пользователь (New Object — User) в поля Полное имя (Full Name) и Имя входа пользователя (User Logon Name) введите *ContosoAdmin,* после чего щелкните кнопку Далее (Next).
   г) Введите пароль по своему усмотрению, щелкните сначала кнопку Далее (Next), а затем — кнопку Готово (Finish).
   д) В консоли Active Directory — пользователи и компьютеры (Active Directory Users And Computers) найдите на панели сведений созданную учетную запись. Щелкните эту запись правой кнопкой мыши и выберите Добавить в группу (Add To A Group).
   е) В диалоговом окне Выбор: «Группы» (Select Groups) введите *Администраторы домена (domain admins)* и нажмите Enter. В окне сообщения Доменные службы Active Directory (Active Directory Domain Services) щелкните OK.
   ж) Точно таким же образом создайте две дополнительные учетные записи, ContosoAdmin2 и ContosoAdmin3.
   з) При желании создайте дополнительную учетную запись администратора домена со своим именем.
8. На машине Serverl включите Общий доступ к файлам (File Sharing). В области уведомлений щелкните правой кнопкой мыши значок Сеть (Network) и откройте Центр управления сетями и общим доступом (Network And Sharing Center). В области Общий доступ и сетевое обнаружение (Sharing And Discovery) выберите опцию Общий доступ к файлам (File Sharing).
9. Установите пакет Windows Automated Installation Kit (WAIK) с DVD-диска WAIK или IMG-файла, загруженного в центре загрузок Windows. При этом последовательность ваших действий должна быть такой.
   а) В Virtual PC подключите DVD-диск с WAIK или IMG-файл как DVD-диск, выбрав в меню CD команду Capture ISO Image.
   б) В окне Welcome To Windows Automated Installation Kit с помощью ссылок .NET Framework Setup и MSXML 6.0 установите при необходимости одноименные компоненты. Если они уже установлены на локальной машине, опция Install будет недоступна.
   в) Щелкните ссылку Windows AIK Setup, и пакет WAIK будет установлен.

10. На машине Serverl установите дополнения Virtual Machine Additions. В меню Action выберите опцию Install Or Update Virtual Machine Additions и следуйте рекомендациям относительно установки Virtual Machine Additions на Serverl. Перезагрузите компьютер и вновь войдите в систему как CONTOSO\Администратор.

Настройка машины Corel

Компьютер Corel выполняет роль сервера в домене contoso.com. Вот как производится конфигурирование сервера Corel.

1. Подключите к виртуальной машине ISO-файл или DVD-диск с Windows Server 2008 и выполните установку ядра сервера (Server Core) Windows Server 2008.
   - При желании выберите язык и клавиатуру, соответствующие региону вашего пребывания.
   - Ключ продукта пока не вводите.
   - Выберите выпуск Windows Server 2008 Standard (Установка ядра сервера) или Windows Server 2008 Enterprise (Установка ядра сервера).
   - Установите Windows в разделе по умолчанию Незанятое место на диске О (Disk 0 Unallocated Space).
   - При первом входе щелкните значок Другой пользователь (Other User) и укажите имя администратора с пустым паролем. Вам будет немедленно предложено сменить пароль.
2. Проверьте конфигурацию IP. В командную строку введите команду ipconfig / all, чтобы убедиться в получении машиной. Corel данных конфигурации IP машины Serverl.
3. Откonфигурируйте имя компьютера Corel и членство в домене. В командную строку введите команду:

   ```
   netdom renamecomputer %computername% /newname:Corel
   ```

4. Чтобы присоединить Corel к домену Contoso.com, введите команду:

   ```
   netdom join %computername% /domain:Contoso.com /userd:ContosoAdmin1 /
   passwordd:*
   ```

5. Укажите пароль доменного пользователя ContosoAdminl.

ПРИМЕЧАНИЕ Об орфографии

Отметим, что две буквы d в переключателе пароля команды Netdom — не опечатка.

6. В завершение перезагрузите Corel с помощью команды:

   ```
   shutdown /r /t 0
   ```

Этап 3. Настройка доступа в Интернет для домена Contoso.com

На данном этапе на машине Serverl будет добавлен второй адаптер, который привязан к физическому сетевому адаптеру физического хост-компьютера.

Затем на машине Serverl будет отконфигурировано преобразование сетевых адресов NAT.

Добавление и настройка второго виртуального адаптера

Для того чтобы добавить и отконфигурировать второй виртуальный адаптер на машине Serverl, выполните такие действия.

1. Завершите работу Serverl. В консоли Virtual PC откройте параметры Serverl.
2. В диалоговом окне Settings For Serverl задайте количество сетевых адаптеров — 2. Для параметра Adapter2 выберите сетевой адаптер, соответствующий физическому адаптеру, подключенному к Интернету на хост-машине. Физическому адаптеру уже должен быть назначен собственный IP-адрес с доступом в Интернет. Пример такой конфигурации показан на рис. В-6.

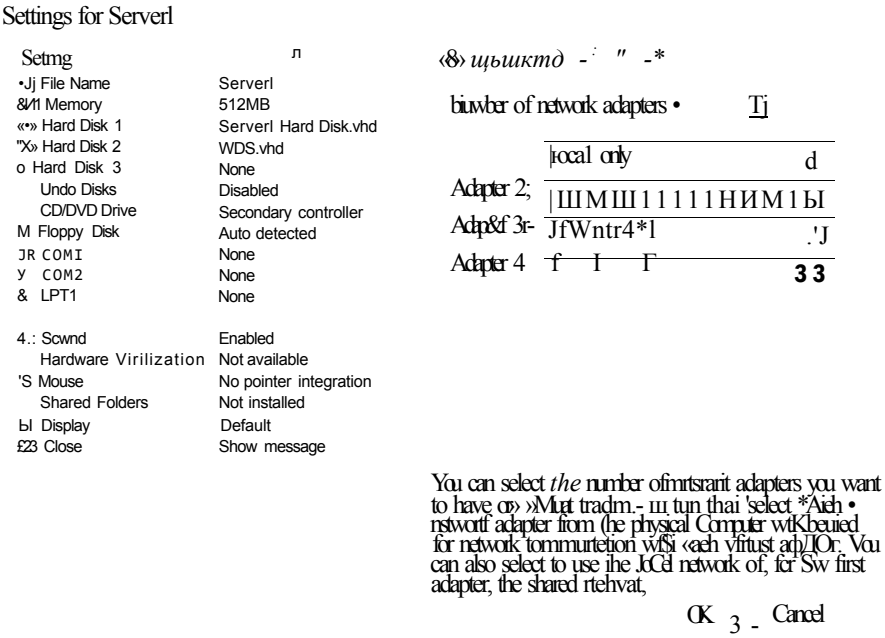


Рис. В-6. Настройка второго адаптера на машине Serverl

3. Запустите машину Serverl и войдите в систему.
4. В окне Диспетчера сервера (Server Manager) щелкните ссылку Добавить роли (Add Roles), после чего в окне Мастер добавления ролей (Add Roles Wizard) задайте необходимые параметры:
   - выберите роль сервера — Службы политики сети и доступа (Network Policy and Access Services);
   - выберите службу ролей — Службы маршрутизации и удаленного доступа (Routing and Remote Access Services). Другие службы ролей пока не выбирайте.

Настройка NAT на машине Serverl

Настраивая NAT на компьютере Serverl, вы можете руководствоваться следующими пошаговыми инструкциями.

1. Откройте средство для администрирования Маршрутизация и удаленный доступ (Routing And Remote Access).
2. В дереве консоли Маршрутизация и удаленный доступ (Routing And Remote Access) щелкните правой кнопкой мыши узел Serverl и выберите команду Настроить и включить маршрутизацию и удаленный доступ (Configure And Enable Routing And Remote Access).
3. В окне Мастер установки сервера маршрутизации и удаленного доступа (Routing And Remote Access Setup Wizard) выполните следующие установки:
   - на странице Конфигурация (Configuration) выберите Преобразование сетевых адресов (NAT) (Network Address Translation (NAT));
   - на странице Подключение к Интернету на основе NAT (NAT Internet Connection) выберите Подключение по локальной сети 2 (Local Area Connection 2).
4. В окне Диспетчер сервера (Server Manager) выберите узел Диспетчер сервера (Server Manager), а затем в области Сведения системы безопасности (Security Information) щелкните Настроить конфигурацию усиленной безопасности Internet Explorer (Configure IE ESC). Конфигурацию усиленной безопасности Internet Explorer (IE ESC) для администраторов отключите.
5. Откройте Internet Explorer и в меню Сервис (Tools) выберите Свойства обозревателя (Internet Options). В качестве домашней страницы укажите любую веб-страницу по своему усмотрению.
6. Проверьте подключение в Internet Explorer, щелкнув значок Домой (Home).

Этап 4. Активация серверов (рекомендуется)

Если вы располагаете ключами продукта для обеих машин, Serverl и Corel, активация производится следующим образом.

1. Сначала активируйте Serverl. Откройте на панели управления апплет Система (System) и щелкните опцию для изменения ключа продукта. Введите ключ продукта и щелкните кнопку Далее (Next). Операционная система автоматически выполнит активацию через Интернет.
2. Теперь выполните активацию Corel.
   а) Войдите в домен contoso.com с машины Corel как администратор домена и в командную строку введите следующую команду, указав ключ продукта (в том числе дефисы):

      slingr -ipk *ключ_продукта*

   б) Получив сообщение об успешной установке ключа продукта, введите команду:

      slmgr -ato

в) Когда получите сообщение об успешной активации продукта, завершите работу Corel, задав команду:
shutdown /s /t 0

Содержимое компакт-диска

На прилагаемом к книге компакт-диске вы найдете много полезных материалов и источников.

- **Пробные экзамены** Электронные пробные экзамены, составленные на основе вопросов, которые содержатся в разделах «Закрепление материала», помогут вам освежить в памяти свои знания по конфигурированию Windows Server 2008. Насколько хорошо усвоена тема, можно проверить, отвечая на вопросы определенных глав или всего сертификационного экзамена 70-643.
- **Веб-трансляции** На CD-диске вы найдете адреса каналов веб-вещания, спонсируемые корпорацией Microsoft. На этих каналах содержатся тексты лекций и демонстрационные ролики, которые послужат дополнительным источником информации по тематике данной книги.
- **Электронная версия книги (eBook)** Электронная версия этой книги (на английском языке) дается на тот случай, если вам не захочется носить с собой печатный вариант. Создана она в формате PDF (Portable Document Format), а следовательно, ее можно просматривать с помощью программ Adobe Acrobat и Adobe Reader.
- **Выборочные главы** На компакт-диске также представлены главы из других книг издательства Microsoft Press, посвященные Windows Server 2008. И эти главы даны в формате PDF.
- **Загрузка содержимого CD-диска через Интернет** Представленные на компакт-диске материалы можно загрузить, обратившись по адресу *http://download.microsoft.com/download/F/3/3/F335F2B1-2AA4-46D2-BA69-A495540B19FA/9780735625112_OCC.exe*. Информация здесь постоянно обновляется и доступна для всех читателей.

Установка заданий пробного экзамена

Для начала вам необходимо установить с компакт-диска на жесткий диск задания, которые рекомендуется выполнить для успешной сдачи пробного экзамена.

1. Вставьте компакт-диск в дисковод и примите условия лицензионного соглашения.

ПРИМЕЧАНИЕ Что делать, если меню диска не отображается
Если условия лицензионного соглашения на экране не отобразились или если не появилось меню компакт-диска, возможно, на компьютере отключена функция Автозапуск (AutoRun). Указания относительно альтернативного способа его установки вы найдете в файле Readme.txt на компакт-диске.

2. Щелкните опцию Practice Tests и следуйте выводимым на экран указаниям.

ПРИМЕЧАНИЕ Занятия и пробные экзамены
Если вы хотите попытаться ответить на вопросы из раздела «Закрепление материала», сопровождающего каждое занятие, выберите Lesson review\(70-643) Supporting and Troubleshooting Applications on a Windows Vista Client for Consumer Support Technicians. Чтобы ответить на любой из 200 вопросов сертификационного экзамена 70-643, выберите Practice test\(70-643) Supporting and Troubleshooting Applications on a Windows Vista Client for Consumer Support Technicians.

Закрепление материала

Чтобы закрепить пройденный материал, откройте диалоговое окно Custom Mode и настройте процедуру тестирования. Вы можете щелкнуть OK и принять параметры по умолчанию или же определить количество вопросов, режим работы программы, а также указать, какие экзаменационные темы должны затрагивать эти вопросы и нужно ли фиксировать время, затрачиваемое на подготовку ответов. Во время повторного тестирования вы можете ответить на все вопросы либо только на те, на которые не смогли дать правильный ответ в первый раз.

- Для того чтобы запустить тестирование, щелкните кнопку OK.
- Отвечая на вопросы теста, переходите от одного вопроса к другому с помощью кнопок Next, Previous и Go To.
- Если вы хотите выяснить, правильно ли ответили на вопрос, а также получить объяснения, щелкните Explanation.
- Чтобы узнать результаты тестирования, щелкните Score Test. Вы увидите краткий перечень выбранных экзаменационных тем и общее количество (в процентах) правильных ответов на тест, а также количество правильных ответов по конкретной теме. У вас имеется возможность распечатать копию выполненного теста, просмотреть свои ответы или пройти тест повторно.

Пробный экзамен

Вы можете выбрать один из трех режимов прохождения пробного экзамена.

- **Certification Mode** Данный режим в максимальной степени соответствует условиям проведения сертификационного экзамена. Тест содержит определенное количество вопросов, и время его выполнения фиксируется.
- **Study Mode** В этом режиме время не фиксируется, что позволяет вам просматривать правильные ответы и объяснения после каждого своего ответа.
- **Custom Mode** Режим, который предоставляет вам возможность настроить тест по своему усмотрению.

Во всех режимах используется фактически один и тот же пользовательский интерфейс, с той лишь разницей, что отменяются некоторые возможности.

Просматривая свой ответ на конкретный вопрос, вы увидите раздел References с указанием того, где можно найти информацию по затронутой теме. После того как вы щелкнете Test Results, чтобы узнать результаты тестирования, перейдите на вкладку Learning Plan и просмотрите список ссылок по каждому вопросу.

Удаление программного обеспечения, используемого для пробного экзамена

При необходимости удалить программное обеспечение, используемое для сдачи пробного экзамена, на панели управления щелкните значок Установка и удаление (для Windows XP) либо Программы и компоненты (для Windows Vista).

Программа сертификации специалистов Microsoft

Сертификация Microsoft обеспечивает наилучший метод проверки того, насколько хорошо специалист либо члены одной команды знают продукты и технологии Microsoft. Порядок сдачи экзаменов и механизм выдачи соответствующих сертификатов разработаны таким образом, чтобы экзаменующийся мог легко подтвердить свои профессиональные навыки в области конфигурирования. Профессионалы, имеющие сертификаты Microsoft, заслуженно считаются экспертами в области высоких технологий. Сертификаты обеспечивают многочисленные преимущества как для отдельных лиц, которым они принадлежат, так и для организаций, где такие специалисты трудятся.

К СВЕДЕНИЮ Все сертификаты Microsoft

Полный список сертификатов Microsoft можно найти по адресу *http://www.microsoft.com/leaming/mcp/default/asp.*

Техническая поддержка

Желающим получать дополнительную информацию по затрагиваемым в издании темам, а также ответы на часто задаваемые вопросы об установке и использовании различных продуктов, рекомендуем регулярно посещать сайт технической поддержки Microsoft Press, расположенный по адресу *http://www.microsoft.com/learning/support/books.* Мы постарались обеспечить максимальное соответствие содержимого этой книги и прилагаемого к ней компакт-диска. Если у вас по рассматриваемой теме имеются какие-либо вопросы, предложения или просто комментарии, присылайте их в издательство Microsoft Press.

Адрес электронной почты: tkinput@microsoft.com

Почтовый адрес: Microsoft Press,

Attn: MCTS Self-Paced Training Kit (Exam 70-643): Configuring Windows Server 2008 Applications Infrastructure, Editor

One Microsoft Way

Redmond, WA 98052-6399

Дополнительную информацию по этой книге и прилагаемому компакт-диску можно найти на веб-сайте Microsoft Press Technical Support. Если вы хотели бы подключиться к базе знаний Microsoft, с тем чтобы непосредственно вводить свои запросы, откройте страницу *http://support.microsoft.com/search.* Информацию о программном обеспечении Microsoft можно найти на сайте *http://support.microsoft.com.*

ГЛАВА 1

Развертывание Windows

Занятие 1. Развертывание Windows в среде Windows Server 2008 2
Занятие 2. Настройка Windows Deployment Services 14
Занятие 3. Развертывание виртуальных машин 41
Занятие 4. Применение инфраструктуры активации Windows 59

Появления операционных систем Windows Vista и Windows Server 2008 ждали много лет, но процесс развертывания Windows-систем в больших корпоративных сетях оставался долгое время без изменений. Последние версии операционных систем Windows предлагают несколько новых технологий развертывания, в частности ImageX и Windows Deployment Services, а также новые принципы развертывания операционной системы, такие как использование виртуальных машин и инфраструктуры активации Windows. Поэтому даже у опытных администраторов операционных систем Windows существует потребность в изучении процесса развертывания системы Windows. Прочитав эту главу, вы узнаете о многих новых технологиях установки системы, поймете концепцию экзамена 70-643.

Темы экзамена:

- Размещение образов с помощью Windows Deployment Services.
- Настройка активации Microsoft Windows.
- Настройка виртуальных машин и Windows Server Hyper-V.

Требования

Для изучения материала занятий в этой главе необходимо иметь:

- контроллер домена с именем Serverl.contoso.com с минимум 3 Гбайт свободного места на любом жестком диске или разделе;
- компьютер или виртуальную машину без операционной системы и как минимум 512 Мбайт оперативной памяти (этот виртуальный компьютер будет использоваться для машины Server2);
- загруженное из центра загрузки Microsoft (Microsoft Download Center, *http://www.microsoft.com/download* приложение Windows Automated Installation Kit

(Windows AIK); это приложение уже может быть установлено на компьютере Serverl.

Реальный мир

Дж. К. Макин

Стоит ли говорить о том, что на данный момент установка системы Windows уже производится с образов? Или же следует начать с ознакомления с новыми утилитами ImageX, Windows PE, Windows System Image Manager и Windows Deployment Services, о которых вы уже должны знать и которые используются при развертывании этих новых образов Windows?

А может быть, сначала нужно напомнить о том, что корпоративные версии Windows — это уже прошлое, и о том, что теперь вам нужно активизировать большое количество компьютеров после их установки? И, к слову, прежде чем размещать какие-либо серверы либо клиенты, вам нужно будет решить, где лучше их разместить — на физической или виртуальной платформе.

Разговор обо всем! Фактически новая система развертывания системы Windows Server 2008 является наиболее существенным изменением по сравнению с предыдущими версиями системы Windows Server.

Если вы новичок в администрировании, то можете за себя порадоваться — вы счастливчик! В этом деле — развертывании системы — вы, скорее всего, сможете обойти даже матерых администраторов. Если же вы считаете себя опытным администратором, то следите за своим сердцем. Как только вы ознакомитесь с новыми технологиями — установка системы Windows Server 2008 станет для вас очень легкой задачей, легче, чем вы могли бы себе представить.

Занятие 1. Развертывание Windows в среде Windows Server 2008

Развертывание операционной системы означает, что эта ОС становится доступной для использования. Обычно под понятием «развертывание» подразумевается установка операционной системы на большом количестве компьютеров корпорации.

В сетях, в которых клиенты используют операционные системы Windows Vista и которые управляются системами Windows Server 2008, вы можете размещать новые клиенты несколькими способами, и все эти методы, включая обычную установку, привязаны к технологии образов. Чтобы разместить образы Windows, следует воспользоваться установочным диском (DVD), работающими с образами утилитами, например ImageX и Microsoft System Center Configuration Manager 2007, либо же встроенным в систему Windows Server 2008 сервером Windows Deployment Services.

Изучив материал этого занятия, вы сможете:

- Использовать утилиты, которые помогут вам управлять, изменять и размещать образы Windows.
- Ознакомиться с разными методами развертывания систем Windows Vista и Windows Server 2008.
- Подключаться к дополнительному монитору.
- Создавать Windows PE CD.

Расчетная продолжительность занятия составляет 50 мин.

Основы развертывания системы Windows

Начав с системы Windows Vista и продолжив системой Windows Server 2008, корпорация Microsoft предложила новый принцип установки и развертывания системы Windows. Нововведение заключается в первую очередь в использовании новых технологий и утилит, которые поддерживают новый формат образов Windows, основанный на файлах WIM.

Что такое файл WIM

Файл WIM (Windows Imaging File) содержит один или более образов диска формата WIM. Эти образы файловые, а значит, состоят из коллекции файлов раздела (то есть это не посекторный снимок диска). Главное преимущество файловых образов над секторными образами заключается в том, что вы можете изменять их до, во время и после развертывания.

Кроме файла данных файлы WIM включают XML-метаданные — описания файлов и папок, из которых состоит каждый образ. Такие метаданные содержат контрольные списки доступа (Access Control Lists, ACL), короткие или длинные имена файлов, атрибуты и другую информацию, используемую для восстановления данных из образа. Метаданные файла WIM представлены на рис. 1-1.

ПРИМЕЧАНИЕ Install.wim

Наиболее важные данные системы Windows Server 2008 хранятся в файле Install.wim, который содержится на установочном DVD-диске.

Файлы WIM обеспечивают ряд преимуществ при развертывании системы Windows.

- Поскольку формат образов WIM не привязан к аппаратным устройствам, для поддержки многих аппаратных конфигураций или абстрактных аппаратных уровней (Hardware Abstraction Layers, HAL) необходим только один образ. Однако для разных архитектур процессора (86- и 64-разрядного) нужны разные образы.
- Файлы WIM позволяют изменять образы с помощью сценариев или автоматизировать их с помощью файлов вопросов во время установки.
- Содержимое образов формата WIM можно редактировать в автономном режиме. Предусмотрена возможность добавлять и удалять нужные компоненты операционной системы, обновления и драйверы устройств без необходимости создавать новый образ.

- WIM-образы состоят из одной копии всех файлов. Благодаря этому существенно уменьшается количество места, необходимого для хранения нескольких образов.
- Вы можете запустить компьютер с диска, на котором находится образ WIM, — для этого достаточно отметить нужный диск как загрузочный.
- Формат WIM позволяет осуществлять неразрушающее развертывание. Это означает, что вы можете оставить данные на разделе, к которому хотите применить образ, поскольку развертывание данных с образа не приводит к удалению существующих документов.
- Образы формата WIM занимают столько же места, сколько и содержащиеся в них занимают файлы. Поэтому вы можете использовать файлы WIM для захвата данных с диска, на котором нет свободного места, и затем перемещать их на другой раздел.
- Файл WIM можно разбить на несколько файлов, и использовать их, скажем, для записи на CD- или DVD-диски.
- Файлы WIM в дополнение к записи файлов без сжатия (самый быстрый способ) поддерживают два уровня сжатия: Xpress (быстрое) и LZX (высокое).

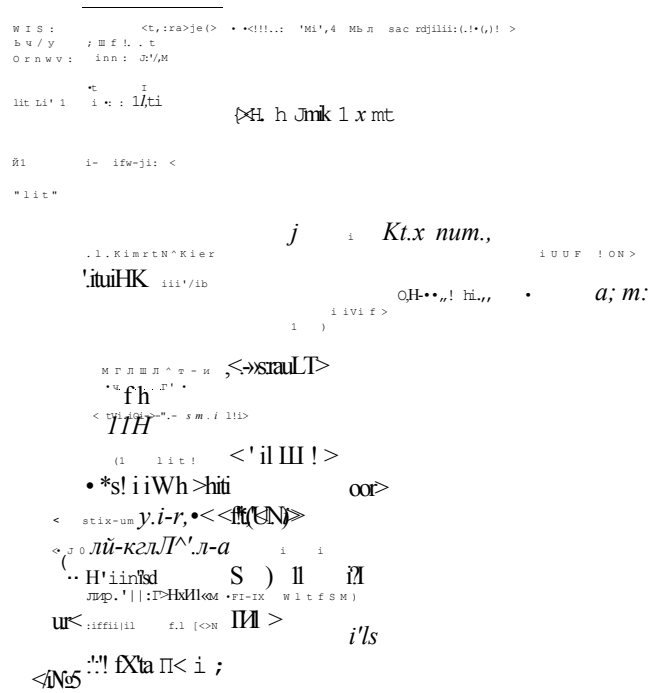


Рис. 1-1. Просмотр информации файла WIM

Утилиты автоматической установки Windows

Вы можете загружать утилиты автоматической установки Windows (Windows Automated Installation Kit, AIK) с веб-узла центра загрузки Microsoft (*http://*

www.microsoft.com/downloads). Windows AIK предлагает администраторам корпораций и производителям компьютеров набор утилит и документов для установки систем Windows Server 2008, Windows Vista, а также более ранних систем Windows XP и Windows Server 2003.

В набор Windows AIK включено несколько очень важных утилит, в том числе такие:

- **Windows Preinstallation Environment 2.0 (Windows PE 2.0)** Утилита Windows Preinstallation Environment, известная как WinPE, является загрузочной и облегченной версией Windows, которую вы можете использовать для запуска своего компьютера со съемного носителя, например с CD/DVD-диска, флэш-памяти или сетевого ресурса. Хотя главное назначение Windows PE — это предоставление пользователю среды, с которой он смог бы захватить или применить образ Windows, вы можете использовать эту облегченную версию операционной системы и для диагностики или восстановления уже инсталлированной операционной системы. Можно сказать, что Windows PE — это замена загрузочной дискеты MS-DOS, но в отличие от 16-разрядной версии MS-DOS, которой для корректной работы нужен был свой набор драйверов, 32- и 64-разрядные версии операционной системы Windows PE используют драйвер Windows Vista и Windows Server 2008.

ПРИМЕЧАНИЕ Облегченная версия Windows

Хотя при установке операционной системы Windows PE можно варьировать ее размер, для этого необходимо как минимум 100 Мбайт оперативной памяти. Из-за своего большого размера операционная система не может быть запущена с дискеты — она должна запускаться с CD/DVD-диска, флэш-памяти или сетевого ресурса.

В системе Windows PE можно запускать много разных программ (обычно это программы, которые запускаются из командной строки) и даже общаться в IP-сетях. Если вы загрузите компьютер с диска Windows PE, автоматически откроется окно командной строки (Command Prompt), откуда можно будет запускать встроенные утилиты и другие программы, которые вы сделаете доступными в процессе настройки данной системы.

ПРИМЕЧАНИЕ Установка Windows и Windows PE

Система Windows PE обеспечивает основу для установки систем Windows Vista и Windows Server 2008. Когда вы запускаете установку указанных систем с DVD-диска, то на самом деле Windows PE работает в фоновом режиме.

Хотя Windows PE загружается с CD-диска, система Windows PE 2.0 после загрузки работает не с CD — она создает виртуальный диск (часть оперативной памяти компьютера используется как этот виртуальный диск), загружается на него и с него же затем запускается. Указанный диск обозначается буквой X.

ПРИМЕЧАНИЕ Замена CD в системе Windows PE
Поскольку Windows PE загружается и работает с виртуального диска, вы можете убрать загрузочный диск Windows PE и установить другой, например с необходимыми драйверами или программами. В папке X:\Windows\System32 содержится много полезных программ и утилит, которые вы можете сразу использовать в этой операционной системе. Хотя большинство утилит идентичны тем, которые используются в системе Windows Vista, некоторые из них работают только под управлением операционной системы Windows PE.

- **ImageX** Утилита ImageX является командной, и вы можете ее использовать для захвата, изменения и развертывания образов WIM. Главными функциями утилиты ImageX являются захват раздела в образ WIM и развертывание образа WIM на указанный раздел жесткого диска. Например, для захвата образа вы можете загрузить систему Windows PE и выполнить команду *Imagex.exe /capture path\wimfilename.wim "Image_Name"*. Чтобы развернуть образ WIM на жесткий диск, выполните команду *Imagex.exe/apply path\wimfilename.wim 1*. (В данном случае цифра 1 означает порядковый номер образа в файле wimfilename.wim). Еще одной важной особенностью утилиты ImageX считается возможность подключения образа WIM к файловой системе Windows для его дальнейшего редактирования. Вы можете подключить образ операционной системы и добавить драйверы устройств, а затем отключить его; образ будет готов для развертывания на раздел.
- **Windows SIM** Утилита Windows System Image Manager (SIM) предназначена для создания файла ответов к программе установки системы Windows. В системах Windows Vista и Windows Server 2008 файлы ответов сохраняются в формате XML и содержат информацию, необходимую для программы установки операционной системы. Так, вы можете создать файл ответов, в котором будут указаны размеры разделов жесткого диска и их файловые системы, форматирование дисков перед установкой операционной системы или изменение веб-страницы по умолчанию. При изменении параметров в файле ответов вы также можете установить приложения от третьих разработчиков, драйверы устройств, языковые пакеты и другие обновления. Все это можно сделать с помощью утилиты Windows SIM.

ПРИМЕЧАНИЕ Windows SIM и Windows PE
Утилита Windows SIM заменила утилиту Setup Manager, которая использовалась в предыдущих версиях системы Windows.

Утилита Windows SIM работает не только с файлами образов WIM, но и с файлами-каталогами .clg. Она может отображать доступные компоненты и пакеты, добавляемые в файл ответов. После добавления новых пакетов или пакетов в файл ответа можно сразу отредактировать файлы-каталоги и файлы образов WIM.

ПРИМЕЧАНИЕ Файлы-каталоги (.els)
После обновления файла образа WIM нужно пересоздать файл-каталог, ассоциируемый с этим образом.

Окно утилиты Windows SIM изображено на рис. 1-2.

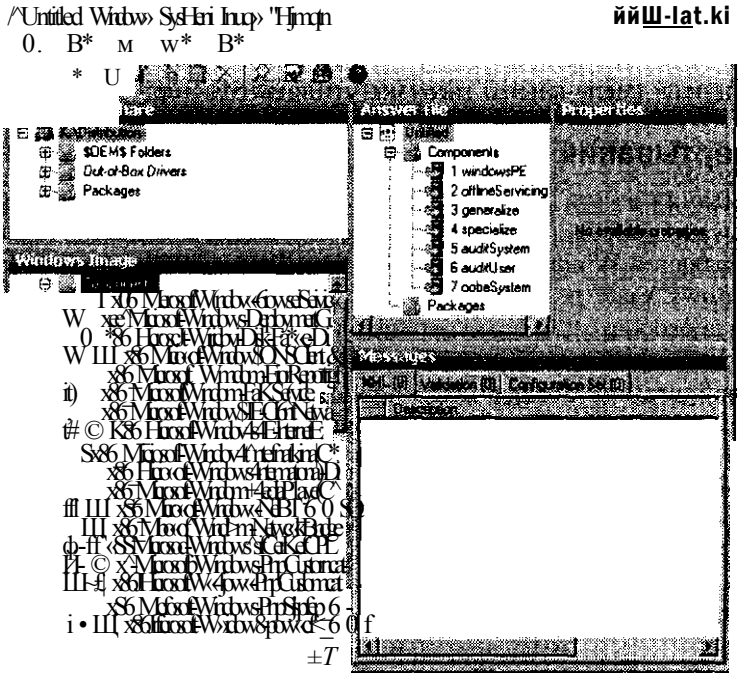


Рис. 1-2. Утилита Windows SIM

СОВЕТ Подготовка к экзамену

Для успешной сдачи экзамена 70-643 вы должны хорошо изучить функциональность системы Windows PE и утилит ImageX, Windows SIM.

Sysprep

В Widnows Vista, равно как и в Windows Server 2008, утилиту Sysprep можно найти в папке %SystemRoot%\System32\Sysprep. Основной задачей этой утилиты является обобщение установочного образа операционной системы для других компьютеров. Утилита Sysprep достигает своих целей за счет удаления только тех параметров, которые не должны повторяться на других компьютерах. В частности, ею удаляются такие параметры, как имя компьютера, принадлежность к домену, часовой пояс, ключ продукта, SID (security identified) и ряд других, связанных с пользователем и параметрами машины. Когда вы запускаете утилиту Sysprep для установочных файлов Windows, создается образ Sysprep, который также называют Sysprepped.

После запуска утилиты Sysprep компьютер выключается. Затем установочные файлы конфигурируются на жестком диске компьютера, измененные установочные файлы можно захватить утилитой ImageX или Windows Deployment Service в файл образа WIM и развернуть их на других компьютерах.

Кончено, удаленные утилитой Sysprep параметры впоследствии нужно будет заменить на всех компьютерах, операционная система которых была установлена с измененного образа. Некоторые из этих параметров, например Security Identifier

(SID), автоматически генерируются при первом запуске утилиты Sysprep. Другие параметры можно внести в файл ответов, и применить его при первой загрузке образа Sysprepped. Все прочие параметры, которые нужны системе для корректной работы, пользователю придется внести вручную в мастере — он будет автоматически запущен после первой загрузки утилиты Sysprep.

Методы развертывания Windows

Методы развертывания в сети Windows Server 2008 используются для размещения как Windows-клиентов, так и Windows-серверов. Далее будет рассказано о методах развертывания Windows Vista и Windows Server 2008.

Системы Windows Vista и Windows Server 2008 обычно развертываются одним из четырех способов: с помощью установочного DVD-диска, образа WIM, сохраненного на сетевом ресурсе, с помощью Windows Deployment Services или System Center Configuration Manager 2007. Каждый из перечисленных методов предлагает повышенный уровень автоматизации установки, но в то же время требует дополнительных ресурсов, проведения экспертиз и более длительной подготовки. Какой метод является наиболее подходящим для вас, зависит от доступных ресурсов, размеров вашей компании и от количества рабочих станций, которые вам нужно установить.

Загрузка с DVD-диска

Наиболее простой метод развертывания системы Windows на новом компьютере — это использование установочного DVD-диска. Если вы настроили файл с ответами, присвоили ему имя Autounattend.xml и сохранили его в корневую папку флэш-памяти или на дискету, то при запуске программы установки вы можете автоматизировать процесс инсталляции и уменьшить количество или вообще снять все вопросы, которые будут задаваться пользователю при установке. Этот метод установки чаще всего применяется в при отсутствии высокоскоростного подключения к другому компьютеру (например, при настройке компьютеров в филиале), когда нужно установить операционную систему на небольшое количество компьютеров и когда поблизости нет IT-специалистов. Правда, по сравнению с другими автоматизированными методами развертывания он требует дополнительных технических приготовлений, ресурсов и экспертиз.

Следует отметить, что развертывание операционной системы Windows при помощи DVD-диска имеет некоторые ограничения. Во-первых, этот метод подразумевает большую работу нетехнического персонала с системой установки операционной системы. Если на компьютере, на который устанавливается операционная система, нет дисковода или если файл Autounattend.xml распространяется по локальной сети, то конечному пользователю необходимо обладать достаточными навыками, чтобы поместить этот файл в корневую папку флэш-памяти или дискеты и загрузить компьютер с установленной дискеты или флэш-памяти. Во-вторых, этот метод не позволяет производить автоматическую установку дополнительных драйверов или обновлений (называемых настроечными пакетами) как процесс установки системы без вмешательства квалифицированных специалистов на стороне конечно пользователя. Последнее же ограничение заключается в том, что этот метод развертывания подразумевает необходимость покупки отдельного установочного диска на каждый компьютер.

Вы можете установить операционную систему лишь на столько компьютеров, сколько у вас есть установочных дисков.

Использование утилит Windows AIK и Network Share Distribution

Вы можете развернуть системы Windows Vista и Windows Server 2008 на компьютерах по сети двумя способами: воспользовавшись программой установки или применив файл образа WIM. Первый метод подразумевает, что содержимое установочных файлов системы Windows находится в общей папке. Вы можете сохранить начальную версию файла Insyall.wim или заменить его (также не забудьте заменить файлы каталогов) образом, который создали сами. После этого из командной строки запустится программа установки в системе Windows PE на локальном компьютере. Чтобы указать файл с ответами, воспользуйтесь идентификатором /unattend. Например, если вы подключили сетевую папку, в которой находятся установочные файлы, присвоили ей букву Y и сохранили файл с ответами deploy_unattend.xml в этой же папке, вы можете загрузить сначала локальный компьютер, затем систему Windows PE и в командной строке ввести: *Y:\setup.exe /unattend:deploy_unattend.xml.*

Второй способ развертывания системы Windows связан с общей сетевой папкой, в которой хранится захваченный образ WIM начальной версии установочных файлов, обработанных утилитой Sysprep. В этом случае вы можете оставить файл с ответами в сетевой папке %SystemRoot%\Panther/Unattend. (Файл с ответами должен иметь имя Unattend.xml или Autounattend.xml.) Затем на новом компьютере вы можете применить этот образ Windows с помощью системы Windows PE и утилиты ImageX. Например, если вы подключили сетевой диск Y, на котором сохранены образы WIM, то должны загрузить локальный компьютер под управлением Windows PE и в командной строке ввести команду *Imagex /apply Y:\myimage.wim 1 c:*

Развертывание системы Windows по локальной сети приемлемо только тогда, когда сеть может быстро передавать большие объемы информации, когда вам нужно разместить небольшое количество операционных систем (около 20) и когда сеть не использует домен Active Directory или приложение Center Configuration Manager 2007.

Главным недостатком описываемого метода является то, что он не может быть полностью автоматизирован. Этот метод подразумевает присутствие опытного IT-специалиста, который может загрузить систему Windows PE и выполнить нужные команды в командной строке. В отличие от Windows Deployment Services (WDS), это решение не может автоматически найти в сети исходные файлы и выполнить загрузку необходимых файлов операционной системы. В отличие от System Center Configuration Manager 2007, данное решение не позволяет администраторам автоматически развертывать операционные системы на удаленных компьютерах.

К проблемам автоматизации добавляется еще больший недостаток, связанный с невозможностью удаленного развертывания системы по сети; данное решение используется не очень часто. Нет централизованной утилиты, с помощью которой можно было бы изменять хранящиеся на сетевом ресурсе образы Windows и управлять ими. В результате развертывание по сети используется лишь в тех случаях, когда операционную систему нужно установить не более чем на 20 компьютеров.

Windows Deployment Services

В отличие от сценария развертывания операционной системы по сети, Windows Deployment Services (WDS) позволяет конечным пользователям, не имеющим достаточного компьютерного образования, использовать компьютеры без операционной системы и из предлагаемого меню выбирать образ Windows, который нужно установить. Целевой компьютер сможет самостоятельно найти WDS-сервер и загрузить это меню со списком операционных систем с помощью Preboot Execution Environment (PXE). PXE — это технология, работающая с протоколом DHCP (Dynamic Host Configuration Protocol), посредством которого она способна найти WDS-сервер во время загрузки.

ПРИМЕЧАНИЕ PXE-совместимые компьютеры
Чтобы компьютер клиента мог найти WDS-сервер, сетевая карта, установленная в нем, должна поддерживать PXE-загрузку.

WDS является более масштабируемым и управляемым решением, чем простое хранение образов WIM в сети. Однако практически при каждой установке (когда используется WDS) необходимо помнить о следующих требованиях к инфраструктуре:

- **Active Directory** WDS-сервер должен быть членом домена с Active Directory или контроллером домена для домена Active Directory. Домен с Active Directory и леса недопустимы; все домены и настройки лесов поддерживают WDS.
- **Dynamic Host Configuration Protocol (DHCP)** У вас должен работать DHCP-сервер с активным адресным пространством в сети, так как WDS использует PXE, который сам использует DHCP. DHCP-сервер не должен располагаться на сервере Windows Deployment Services, но DHCP-агенту не обязательно находиться в той же подсети, в которой находится компьютер клиента.
- **Domain Name System (DNS)** В сети должен быть рабочий DNS-сервер, чтобы работали Windows Deployment Services. DNS-сервер не должен быть запущен на сервере Windows Deployment Services.
- **Раздел NTFS** Для хранения образов на сервере, где запущены Windows Deployment Services, требуется файловая система NTFS.
- **Высокоскоростное постоянное соединение между серверами WDS и конечными компьютерами** Потребность в высокоскоростном соединении обусловлена большими объемами образов, которые нужно передать на конечные компьютеры. В дополнение эти серверы для удостоверения высокоскоростного подключения должны находиться в одной подсети с конечными компьютерами.

Кроме повышенных требований к инфраструктуре, у WDS имеется одно ограничение, которое связано с этим методом развертывания, — требуется участие конечного пользователя. Администратор не может удаленно запустить установку операционной системы.

По причине указанных ограничений WDS не применяется в больших корпоративных сетях с несколькими доменами Active Directry, IP-сетями и техническими площадками.

ПРИМЕЧАНИЕ WDS без Active Directory
Служба Deployment Server включает Windows Deployment Services и службу транспортного сервера (Transport Server). Роль службы транспортного сервера состоит в том, что она разрешает передачу любых файлов и папок (образов операционных систем, данных или даже MP3-библиотек) удаленным компьютерам, используя широковещательную IP-адресацию. В случае использования без службы Deployment Server транспортный сервер не требует инфраструктуры Active Directory или DHCP — это гораздо более усложненный метод развертывания операционной системы. В отличие от Deployment Server указанная служба не отвечает на запросы PXE. Ее можно использовать и управлять ею только с помощью запускаемой из командной строки утилиты Wdsutil.exe. Вне доменов Active Directory вы будете развертывать системы Windows Vista и Windows Server 2008 скорее всего с помощью общей папки в сети и утилиты Windows AIK.

Проверьте себя

- Каковы требования к серверу и инфраструктуре WDS?

Ответ

- Система Windows Server 2008 с установленным WDS, Active Directory, DNS, DHCP, раздел NTFS и постоянное высокоскоростное сетевое подключение.

System Center Configuration Manager 2007

При использовании совместно с различными методами развертывания System Center Configuration Manager 2007 позволяет создавать полностью управляемые решения по развертыванию операционных систем для больших организаций. В отличие от различных методов развертывания, System Center Configuration Manager 2007 позволяет производить развертывание совсем не подготовленной операционной системы на удаленные компьютеры.

System Center Configuration Manager 2007 помогает в решении многих задач, связанных с применением автоматических процедур для нескольких серверов и компьютеров клиентов, в том числе таких:

- выбор тех компьютеров, которые отвечают аппаратным требованиям операционной системы и которые вы готовы поддерживать;
- распространение исходных файлов операционной системы на все площадки, включая удаленные площадки и площадки, на которых нет персонала технической поддержки;
- мониторинг распространения данных по всем площадкам;
- распределение прав пользователей;
- автоматическое инициирование установки программных пакетов с возможностью контролировать рабочее время пользователей;
- решение проблем, связанных с распространением или установками систем;
- отчет о развертываниях;

- возможность удостовериться в том, что все компьютеры в вашей организации получили стандартные конфигурационные параметры операционной системы.

Развертывание систем Windows Vista и Windows Server 2008 с помощью System Center Configuration Manager 2007 требует постоянного высокоскоростного подключения между серверами и удаленными компьютерами, которые используются в процессе развертывания. Высокоскоростное подключение предназначено для передачи больших объемов информации (образов операционной системы) на удаленные компьютеры.

У этого метода развертывания имеются и недостатки. Во-первых, в отличие от других методов, рассмотренных ранее, System Center Configuration Manager 2007 требует для своей работы наличия системы Windows Server 2008. Во-вторых, установка и настройка инфраструктуры System Center Configuration Manager 2007 требует тщательной технической экспертизы. В-третьих, с помощью System Center Configuration Manager 2007, в отличие от WDS, вы не сможете развернуть операционную систему на чистом компьютере; на удаленном же компьютере должно быть установлено клиентское программное обеспечение System Center Configuration Manager 2007. (Из-за последнего ограничения System Center Configuration Manager 2007 фактически используется совместно с WDS, а не как его замена.)

Практикум. Создание диска Windows PE

В данном упражнении вы создадите загрузочный диск Windows PE, с помощью которого сможете захватывать и применять образы Windows. Для выполнения этого практического задания у вас на компьютере Serverl, на диске C, должна быть установлена утилита Windows AIK.

Упражнение 1. Создание диска Windows PE

В рамках этого упражнения вы создадите диск Windows PE, с которого сможете загрузить компьютер, а затем запустить утилиту ImageX.

1. На компьютере Serverl запустите утилиту Windows PE Tools Command Prompt, которая относится к группе Windows AIK.
2. В окне Windows PE Tools Command Prompt, в зависимости от архитектуры процессоров, установленных в удаленных компьютерах, для которых вы будете создавать диск Windows PE, введите следующее:

   Copype.cmd x86 C:\WinPE_x86

   Copype.cmd amd64 C:\WinPE_amd64

   Copype.cmd ia64 C:\WinPE_ia64

   Сценарий Copype.cmd создаст новую папку и присвоит ей имя, указанное в команде. После выполнения данной команды в созданной папке наряду с другими файлами и папками можно будет найти папку ISO. Эта папка имеет важное значение — в ней содержатся данные диска WinPE. Если вы хотите, чтобы в системе Windows PE были какие-либо утилиты (например, ImageX), вам нужно их скопировать в папку ISO.

3. В окне Windows PE Tools Command Prompt, в зависимости от архитектуры процессора компьютера или компьютеров, на которых вы будете использовать диск Windows PE, введите следующее:

```
Copy "C:\Program files\Windows AIK\Tools\x86\imagex.exe"
C:\WinPE_x86\ISO
Copy "C:\Program files\Windows AIK\Tools\amd64\imagex.exe"
C:\WinPE_amd64\ISO
Copy "C:\Program files\Windows AIK\Tools\ia64\imagex.exe"
C:\WinPE_ia64\ISO
```

4. В программе Блокнот (Notepad) создайте пустой файл Wimscript.ini и сохраните его в новую папку WinPE_x86\ISO, WinPE_amd64\ISO или WinPE_ia64\ISO.
5. Введите следующий код в файл Wimscript.ini и сохраните его еще раз.

```
[ExclusionList]
Ntfs.log
Hiberfil.sys
Pagefile.sys
"System Volume Information"
RECYCLER
Windows\CSC

[CompressionExclusionList]
*.mp3
*.zip
*.cab\WINDOWS\inf\
*.pnf
```

   В секции [ExclusionList] файла Wimscript.ini указаны те файлы, которые не надо захватывать при создании образа с помощью утилиты ImageX. В секции [CompressExclusionList] перечислены файлы или типы файлов, которые не нужно сжимать при сжатии образа с помощью утилиты ImageX.

6. В окне Windows PE Tools Command Prompt, учитывая архитектуру процессора компьютера или компьютеров, на которых вы будете использовать диск Windows PE, введите следующее:

```
Oscdimg -n -bc:\WinPE_x86\etfsboot.com c:\WinPE_x86\ISO
C:\WinPE_x86\WinPE_x86.iso
Oscdimg -n -be:\WinPE_amd64\etfsboot.com c:\WinPE_amd64\ISO
C:\WinPE_amd64\WinPE_amd64.iso
Oscdimg -n -bc:\WinPE_ia64\etfsboot.com c:\WinPE_ia64\ISO
C:\WinPE_ia64\WinPE_ia64.iso
```

   Команда Oscding создает файл .iso в указанной папке ISO. Параметр -b делает диск Windows PE загрузочным, при этом указывается путь к загрузочному файлу, а именно к etfsboot.com. Заметьте, что после параметра -Ь нет пробела. (Буква с, которая следует за этим параметром, отвечает за букву диска адреса файла etfsboot.com). Параметр -п разрешает длинные имена файлов в файле .iso.

7. (Опционально) Воспользовавшись любым программным обеспечением, запишите новый файл .iso на диск (или подключите его как виртуальный диск).

Резюме

- В сети, которая состоит из компьютеров с системой Windows Vista и сервера, управляемого системой Windows Server 2008, вы можете развертывать операционные системы для пользователей и сервера несколькими методами, и все эти методы, включая обычную установку, основаны на файлах WIM.
- WIM-файл — это файл, в котором содержится один или несколько образов дисков. WIM-файлы хранят информацию в обычном виде, а не по-секторно, поэтому образы WIM можно изменять до, во время и после развертывания.
- Утилита Windows AIK представляет собой ISO-файл, который вы можете загрузить с официального сайта корпорации Microsoft; она включает несколько важных средств, которые можно применить при развертывании, в том числе систему Windows PE, и утилиты ImageX и Windows SIM.
- Утилиту Sysprep можно найти в папке %SystemRoot%\System32\Sysprep, содержащейся в установочной папке систем Windows Vista или Windows Server 2008. Эта утилита применяется при подготовке установочных образов, следовательно, такие образы можно использовать на многих компьютерах.
- Вы можете развернуть операционную систему Windows с DVD-диска или с сетевой папки с помощью утилиты Windows AIK либо службы Windows Deployment Services.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных в ходе занятия 1. Эти вопросы представлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы
Ответы и пояснения к каждому их варианту размещены в разделе «Ответы» в конце книги.

1. Какие из перечисленных утилит можно использовать для изменения основной установки и для приготовления последней для захвата и последующего развертывания?
   А. Windows PE.
   Б. ImageX.
   В. Sysprep.
   Г. Windows SIM.

Занятие 2. Настройка Windows Deployment Services

Windows Deployment Services (WDS) — это набор компонентов, составляющих наиболее полную версию службы Remote Installation Services (RIS), технологию развертывания, которая впервые была представлена как часть операционной системы Windows Server 2000. В системе Windows Server 2008 вы можете легко

добавить WDS в любые службы в окне Управление сервером (Server Manager). WDS предлагает технологию развертывания, основанную на установке с сервера или образа и используемую в основном в средних по размеру компаниях, которым нужно автоматизировать процесс развертывания рабочих станций и серверов.

Версия WDS, входящая в состав Windows Server 2008, включает ряд усовершенствований, таких как улучшенный интерфейс управления, командная строка Wdsutil.exe, работающая со сценариями, поддержка нового формата образов WIM (.wim) и улучшения, которые делают развертывание большого числа компьютеров по сети более эффективным.

Изучив материал этого занятия, вы сможете:

S Размещать образы Windows с помощью Windows Deployment Services.

Расчетная продолжительность занятия составляет 120 мин.

Первое знакомство с Windows Deployment Services

WDS представляет собой серверную технологию, которая разработана для развертывания образов Windows на новые компьютеры. WDS-сервер используется для хранения образов Windows.

При установке на новые компьютеры клиенты находят WDS-сервер во время фазы загрузки с помощью загрузочного диска или PXE. Основанную на DHCP технологию PXE поддерживают большинство современных сетевых карт. Вы также можете использовать WDS-сервер для управления и изменения образов, что делает его незаменимым для организаций, у которых большие потребности в развертывании систем, нуждающихся в существенных изменениях.

WDS и утилиты Windows AIK

WDS предлагает пользователям графический интерфейс, что исключает возможность непосредственного использования некоторых утилит. Например, вы можете использовать WDS (а не ImageX) для захвата образов и их размещения на компьютере. Поддержка утилит Windows AIK увеличивает мощность WDS. Так, для создания файлов ответов, которые в дальнейшем можно будет использовать для автоматизации развертывания с помощью WDS, можно запустить Windows SIM.

Автоматическое развертывание системы Windows с помощью утилит Windows AIK требует выполнения большого объема работ по настройке и наладке вручную. Альтернативой в этом случае может служить WDS, предлагающая простую в использовании консоль, которая очень облегчает задачи по настройке и наладке.

Автоматизировать многие задачи в WDS позволяет утилита Wdsutil.exe, но при этом применяются сценарии. Таким образом, WDS — это серверное решение, которое упрощает управление большим количеством измененных загрузочных и установочных образов. Windows AIK не в состоянии предложить столь простое управление образами, вам нужно создавать и поддерживать их вручную.

Преимущества WDS

Утилита WDS обладает несколькими преимуществами, которые делают ее идеальным выбором при развертывании систем для многих организаций. Во-первых, это серверное решение; WDS может легко управлять всеми аспектами процесса развертывания, включая захват, изменение, поддержку, обновление и установку образов. Такая централизация помогает уменьшить комплексность процесса развертывания, и в то же время с помощью WDS можно уменьшить стоимость развертываний и сократить временные затраты. Во-вторых, утилита WDS, которая поставляется вместе с Windows Server 2008, поддерживает и такие операционные системы, как Windows Vista, Windows Server 2003 и Windows XP. Это означает, что если в вашей сети работают компьютеры с разными операционными системами (из числа перечисленных), то вам для их поддержки нужна всего лишь одна инфраструктура развертывания. В-третьих, утилита WDS включает в себя улучшения протокола TFTP (Trivial File Transfer Protocol) и широковещательную поддержку, что позволяет развертывать системы Windows в очень больших сетевых окружениях, не перегружая при этом сеть.

Компоненты инфраструктуры WDS

Прежде чем разворачивать сервер Windows Deployment Services, нужно подготовить сетевое окружение. Выполняемые при этом действия зависят от того, какие цели вы преследуете при установке WDS.

Устанавливая сервер Windows Deployment Services, вы можете выбирать между двумя вариантами служб.

- **Сервер развертывания (Deployment Server)** Этот вариант предлагает полную функциональность WDS и разрешает вам создавать и изменять образы, размещать их удаленно на новых компьютерах. Если вы выбрали данный вариант службы, то сначала в вашей сети нужно развернуть службы Active Directory Domain Services (AD DS), DNS-сервер и сервер DHCP.
- **Транспортный сервер (Transport Server)** Этот вариант предлагает функциональность WDS только в подсети, при этом WDS можно использовать для создания разных решений, используя отдельно стоящие серверы развертывания и широковещательную адресацию. Для поддержки служб сервера вам не понадобятся служба AD DS, DNS- или DHCP-серверы.

  Хотя транспортный сервер выдвигает не столь высокие требования к инфраструктуре сети, как сервер развертывания, первый используется для особых сценариев и требует специальной настройки для решения развертывания. В этой главе речь пойдет лишь об использовании сервера развертывания WDS для размещения систем Windows.

К СВЕДЕНИЮ Определение вашего DHCP-сервера

Вы можете установить Active Directory вместе с DNS-, DHCP- и WDS-серверами на один компьютер, вместо того чтобы размещать WDS на отдельном компьютере. Если вы решили так сделать, вам во время установки WDS придется выбрать специальную опцию. Для получения информации о настройке этой опции с помощью утилиты Wdsutil.exe просмотрите ниже раздел «Начальная настройка сервера с помощью утилиты Wdsutil.exe».

Компоненты сервера Размещены в WDS-сервере и включают: хранилище образов, где содержатся загрузочные образы, установочные образы и другие файлы, необходимые для удаленной установки по сети; PXE-сервер, разрешающий удаленному компьютеру удаленно загружаться без операционной системы; TFTP-сервер, который позволяет удаленному компьютеру загружать и устанавливать образы операционной системы из хранилища образов; сетевой слой, обеспечивающий поддержку широковещательной передачи файлов по сети; компонент диагностики, являющийся частью инфраструктуры Windows Eventing системы Windows Server 2008.

Компоненты клиентов Включают в себя графический интерфейс пользователей, который запускается в системе Windows PE и разрешает пользователям выбирать образ операционной системы для установки на удаленном компьютере. После выбора нужного образа компоненты клиента запрашивают и загружают нужный образ из хранилища образов, которое находится на WDS-сервере.

Компоненты управления Содержат консоль Windows Deployment Services, которую можно найти в группе программ Утилиты администрирования (Administrative Tools), утилиту Wdsutil.exe и ряд других утилит.

Упрощенная схема архитектуры WDS показана на рис. 1-3.

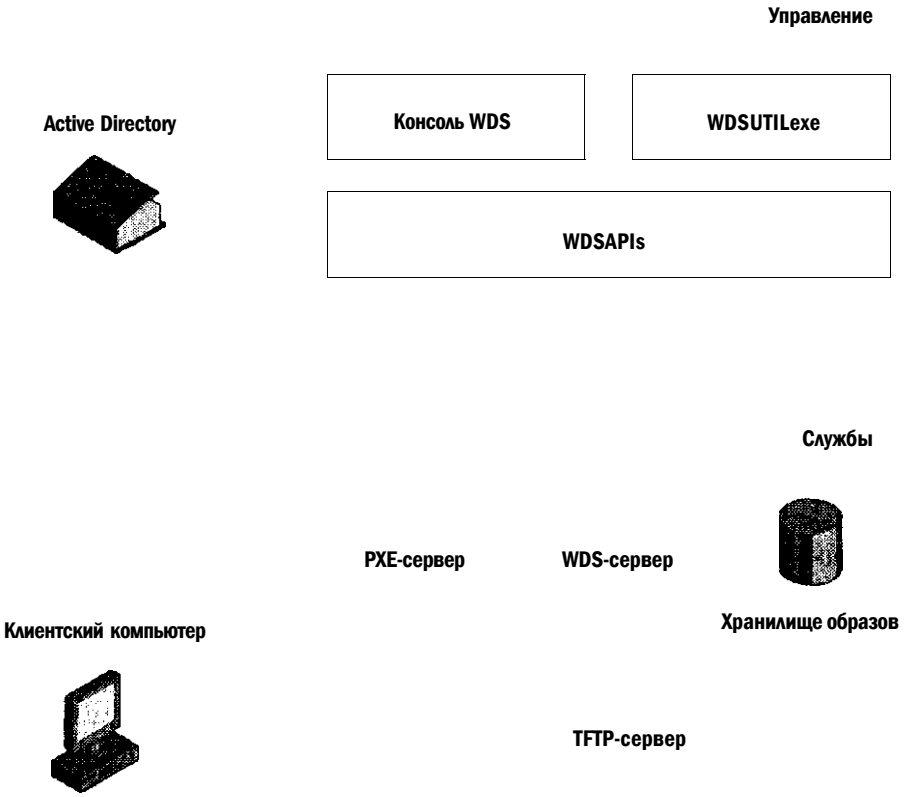


Рис. 1-3. Архитектура WDS

Установка WDS

Самый простой способ установки WDS состоит в использовании мастера Add Roles Wizard. Чтобы запустить его из Server Manager, щелкните правой кнопкой мыши Роли (Roles) и в появившемся меню выберите Добавить роли (Add Roles). Когда откроется страница Прежде, чем вы начнете работать (Before You Begin), щелкните кнопку Далее (Next). В окне Выберите роли сервера (Select Server Role) установите флажок Windows Deployment Services и щелкните кнопку Далее (Next), как показано на рис. 1-4.

ЦЦДМШМ

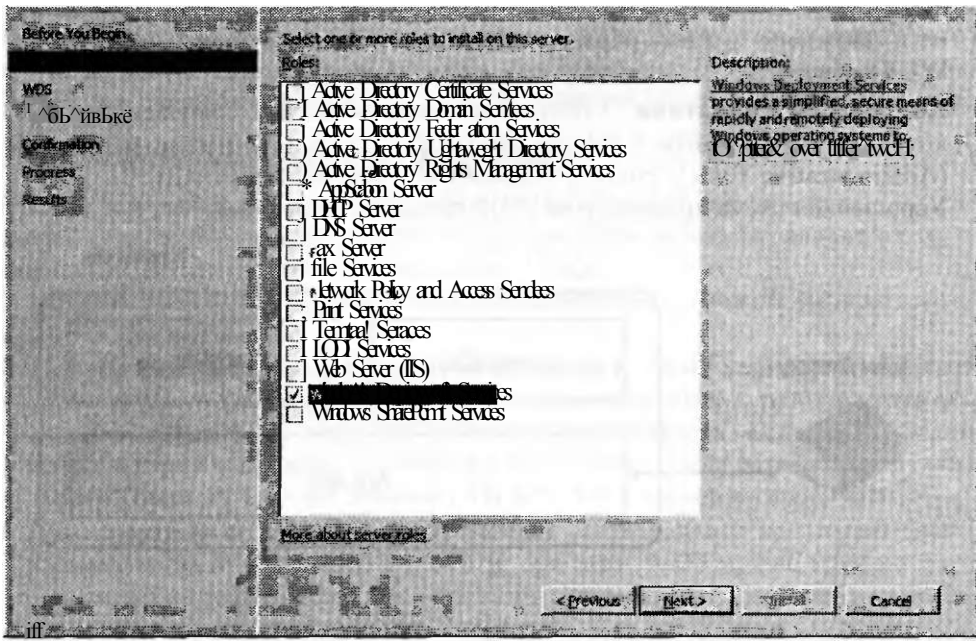


Рис. 1-4. Добавление роли Windows Deployment Services

Вы перейдете на страницу Обзор Windows Deployment Services (Overview Of Windows Deployment Services), содержащую краткий обзор WDS, а также гиперссылки, которые помогут вам при установке и настройке этой роли, а также при управлении ею.

Щелкнув кнопку Далее (Next), вы перейдете на страницу Выберите роли сервисов (Select Role Services), представленную на рис. 1-5.

Здесь следует указать, как будет работать ваш WDS-сервер: как Сервер развертывания (Deployment Server) или как Транспортный сервер (Transport Server). Если вы установите флажок Сервер развертывания (Deployment Server), вам также необходимо будет установить флажок Транспортный сервер (Transport Server), поскольку работа сервера развертывания зависит от транспортного сервера.

Чтобы завершить работу мастера, щелкните кнопку Далее (Next), просмотрите изменения, которые будут внесены на ваш сервер, щелкните кнопку Установить (Install), и установка роли службы будет запущена.

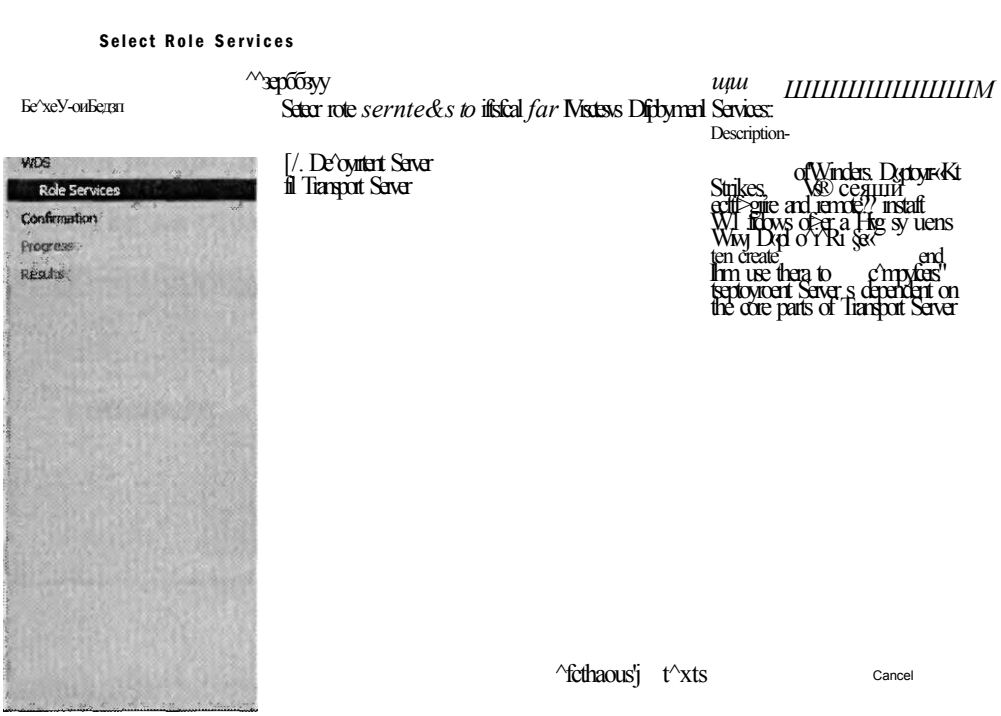


Рис. 1-5. Установка роли службы Сервер развертывания (Deployment Server)

Настройка WDS

Прежде чем использовать WDS, вам необходимо ее настроить. Ниже описаны самые распространенные задачи по настройке WDS, включая начальную настройку сервера, добавление загрузочного и установочного образов по умолчанию и настройку загрузочного меню.

Начальная настройка сервера

Начальную настройку WDS-сервера можно выполнить с помощью мастера или командной строки. Настройка сервера подразумевает выполнение нескольких операций.

Во-первых, создается хранилище образов, где будут содержаться загрузочные и установочные образы. По умолчанию мастер предлагает использовать для этой цели папку %SystemDrive%\RemoteInstall (рис. 1-6), по исходя из соображений производительности, вы можете использовать другую папку на выделенном жестком диске. Критерием выбора диска, который будет использоваться как хранилище образов, является файловая система NTFS, ну и, конечно же, наличие свободного места.

Во-вторых, при начальной настройке сервера вам необходимо сконфигурировать политику ответов для него. Это означает, что вы должны указать тип компьютеров клиентов, которым будет отвечать WDS-сервер (рис. 1-7).

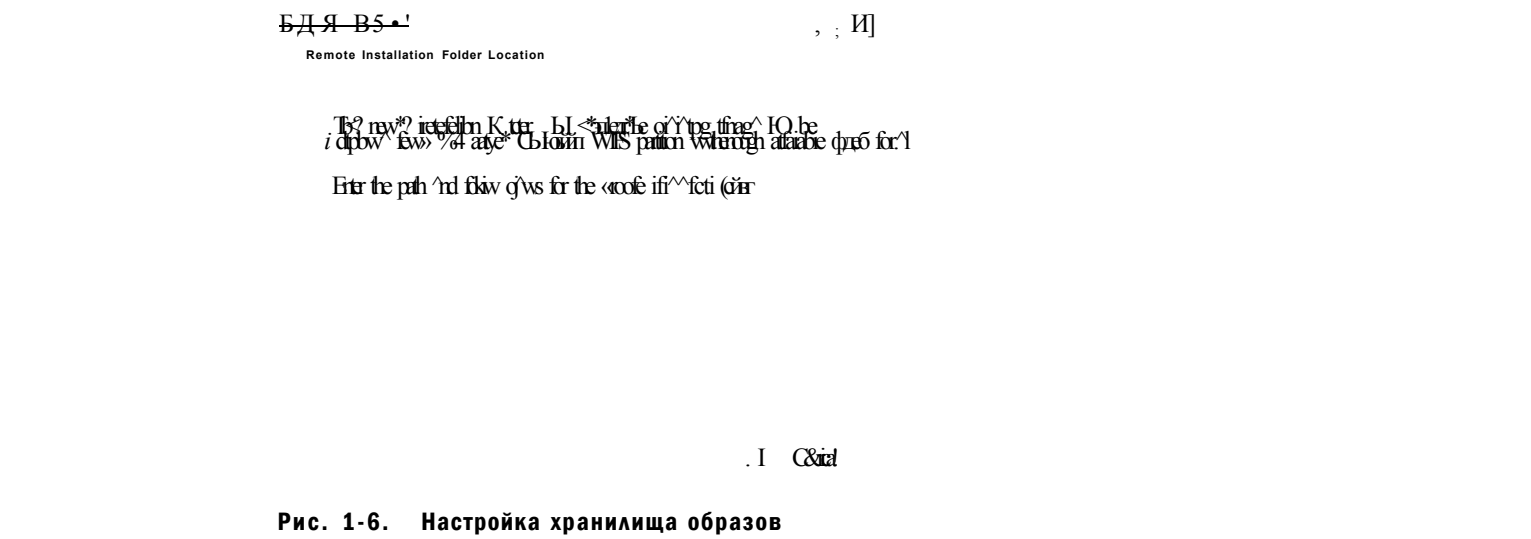


Рис. 1-6. Настройка хранилища образов

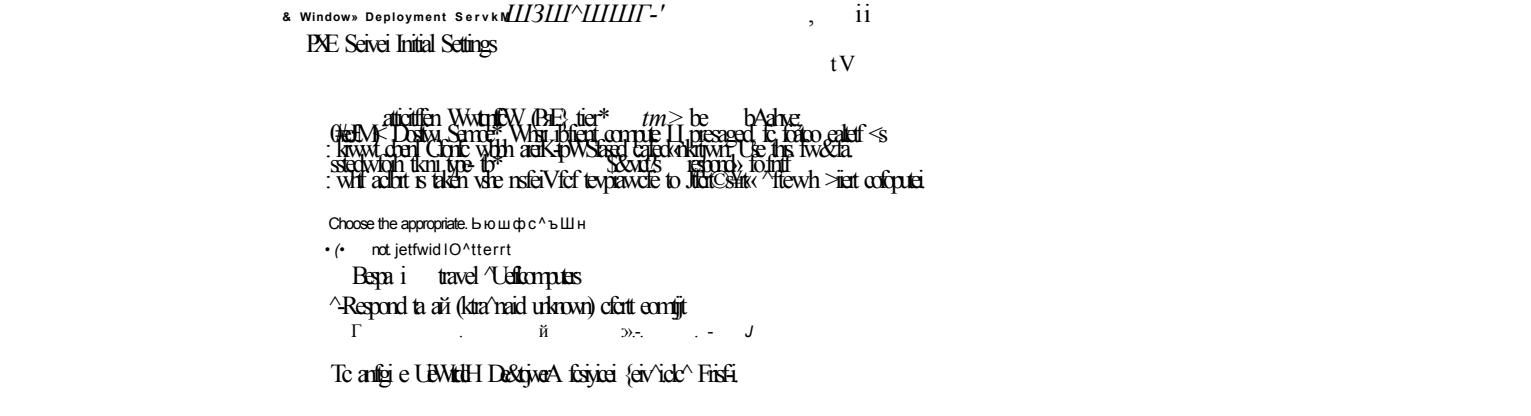


Рис. 1-7. Настройка начальных параметров сервера PXE

В зависимости от того, как вы настроите сервер, он будет вести себя совершенно по-разному.

- Не отвечать любым компьютерам клиентов (Do Not Respond To Any Client Computers) При выборе этого параметра WDS-сервер не будет работать с системами.
- Отвечать только на известные компьютеры клиентов (Respond Only To Known Client Computers) Известными компьютерами клиентов считаются компьютеры, чьи учетные записи указаны в Active Directory WDS-сервер не будет отвечать на запросы по установке от других систем.

- Отвечать всем компьютерам клиентов (Respond To All Client Computers) Выбор этой опции означает, что ваш WDS-сервер будет отвечать всем компьютерам клиентов, которые отправили запрос па установку.

И последнее, что происходит во время начальной настройки сервера, — это создание самого хранилища образов WDS-сервера. Хранилище образов состоит из нескольких подпапок, которые используются для размещения разных типов образов на вашем сервере.

Чтобы выполнить начальную настройку сервера WDS, откроите консоль Службы развертывания Windows (Windows Deployment Services) из группы Утилиты администрирования (Administrative Tools), щелкните правой кнопкой мыши узел, представляющий ваш сервер, и в появившемся меню щелкните Настроить сервер (Configure Server) (рис. 1-8).

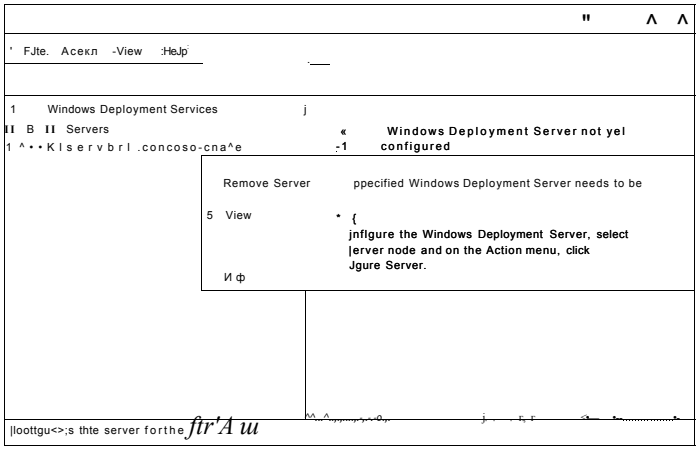


Рис. 1-8. Службы развертывания Windows (Windows Deployment Services), требующие настройки

Откроется окно мастера настройки служб развертывания Windows (Windows Deployment Services Configuration Wizard), после чего вам, чтобы завершить настройку своего сервера, достаточно будет следовать подсказкам мастера.

Начальная настройка сервера WDS с помощью утилиты Wdsutil.exe

Вы можете настроить свой WDS-сервер и с помощью утилиты Wdsutil.exe из командной строки. Сделать это очень просто. Сначала необходимо создать хранилище образов, выполнив команду:

```
Wdsutil.exe /Initialize-Server /reminst:path\foldername
```

Затем нужно настроить политику ответов для сервера с помощью указанной ниже команды. (В этом примере настраивается сервер, который будет отвечать на запросы всех компьютеров — как известных, так и неизвестных.)

```
Wdsutil.exe /Set-Server /AnswerClients:all
```

Наконец, если ваш компьютер также является и DIICP-сервером, вам нужно выполнить еще одну команду:

```
Wdsutil.exe /Set-Server /UseDHCPPorts:no /DHCPoption60:yes
```

Последняя команда делает следующее. Во-первых, отключает возможность использования DHCP-портов сервером WDS (/*UseDHCPPortsmo*). По умолчанию DHCP- и WDS-серверы будут прослушивать порт 67. Однако когда указанные серверы установлены на одном компьютере, WDS серверу не нужно использовать данный DHCP-порт, следовательно, эта команда не приведет к конфликту. WDS-сервер должен быть настроен таким образом, чтобы не использовать порт. Во-вторых, команда */DHCPoption60:yes* добавляет тег 60 к локальному DHCP-серверу. Этот тег использует пакет DHCPOffer для информирования DHCP-клиентов о наличии PXE-сервера, прослушивающего сеть.

Заметьте: вам нужно применять последнюю команду только при условии, что для начальной настройки сервера используется утилита Wdsutil.exe. Если вы для настройки своего сервера задействуете консоль Служб развертывания Windows (Windows Deployment Services), этот шаг автоматически выполняется мастером.

Проверьте себя

1. Какие параметры необходимо настроить на WDS-сервере, если вы не хотите, чтобы PXE-совместимые компьютеры автоматически подключались к вашему серверу и автоматически загружали образы?
2. Какой параметр нужно настроить на WDS-сервере, если вы планируете проверять учетные записи пользователей в Active Directory?

Ответы

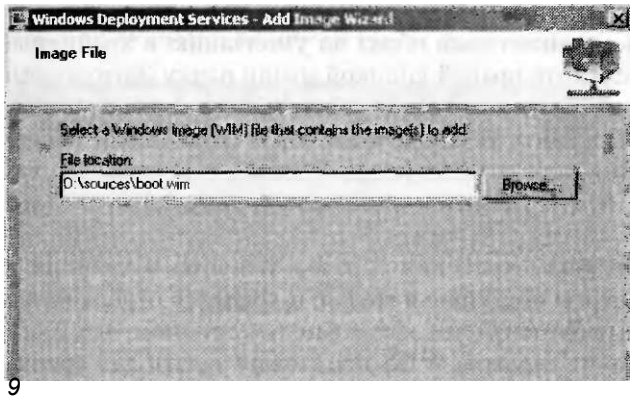
1. Установить флажок Не отвечать любым компьютерам клиентов (Do Not Respond To Any Client Computers) на вкладке Настройка ответа PXE (PXE Response Setting) страницы Свойства (Properties) WDS-сервера.
2. Установить флажок Отвечать только на известные компьютеры клиентов (Respond Only To Known Client Computers) на вкладке Настройка ответа PXE (PXE Response Setting) страницы Свойства (Properties) WDS сервера.

Добавление загрузочного образа по умолчанию

Самый простой способ использования WDS для размещения системы Windows состоит в использовании загрузочного образа по умолчанию, который хранится в папке \Sources на установочном DVD-диске с системой Windows Server 2008. Загрузочный образ — это небольшой по объему файл .wim, который можно использовать для загрузки нового компьютера и дальнейшей его подготовки к размещению операционной системы Windows Vista или Windows Server 2008. В папке \Source на установочных DVD-дисках систем Windows Vista и Windows Server 2008 содержатся два образа: загрузочный образ по умолчанию (Boot.wim) и установочный образ по умолчанию (Install.wim). Вы можете использовать загрузочный образ по умолчанию для загрузки компьютеров клиентов и начала процесса развертывания, а затем воспользоваться установочным образом по

умолчанию для установки системы Windows на компьютеры клиентов. Альтернативой этому может служить изменение одного или обоих образов.

Чтобы добавить загрузочный образ в хранилище образов на своем WDS-сервере, щелкните правой кнопкой мыши папку Загрузочные образы (Boot Images), которая находится под узлом вашего сервера, и в появившемся меню щелкните Добавить загрузочный образ (Add Boot Image). Когда откроется показанное на рис. 1-9 окно мастера добавления образа (Add Image Wizard), следуя выводимым на экран подсказкам, добавьте файл Boot.wim (с установочного диска системы Windows) в хранилище образов.



9

№

~ I - - -~

pщ .-|rigQ -.JSgiJ

1

Рис. 1-9. Добавление загрузочного образа

ВНИМАНИЕ! Используйте правильный загрузочный образ!

Если вы хотите воспользоваться преимуществами нововведений WDS, например такого, как широковещательная передача данных (в начальных версиях WDS не поддерживается), то должны использовать загрузочный образ с DVD-диска Windows Server 2008 или Windows Vista с интегрированным сервисным пакетом 1 (Service Pack 1). Если вы используете загрузочный образ системы Windows Vista версии RTM, то инфраструктура развертывания WDS не будет поддерживать усовершенствования, которые включены в WDS-сервер версии Windows Server 2008.

Добавление загрузочного образа с помощью утилиты Wdsutil.exe

Вы также можете, воспользовавшись утилитой Wdsutil.exe, добавить загрузочный образ по умолчанию с DVD-диска Windows Server 2008 в свое хранилище образов. Это можно сделать с помощью команды:

```
Wdsutil.exe /Add-Image /ImageFile:DVD_drive_letter\
Sources\Boot.wim /ImageType:boot
```

Добавление установочного образа по умолчанию

Еще раз повторим, что самый простой способ использования WDS — это использование установочного образа по умолчанию, который хранится в папке \Sources на вашем DVD-диске с системой Windows Server 2008.

После того как вы добавите этот образ (Install.wim) и загрузочный образ по умолчанию (Boot.wim), можно будет запустить WDS для загрузки удаленных компьютеров и установки на них операционной системы Windows. На практике вы, скорее всего, захотите изменить эти образы, а затем создать файл ответов, дабы быть уверенным в том, что развертывания этих систем отвечают требованиям организации.

Для того чтобы добавить установочный образ по умолчанию в хранилище образов на своем сервере, щелкните правой кнопкой мыши папку Загрузочные образы (Boot Images), которая расположена под узлом вашего сервера, и в появившемся меню щелкните Добавить установочный образ (Add Install Image). Запустится мастер добавления образа (Add Image Wizard), и первое, что вам нужно будет в нем сделать, — это указать или создать группу, которая будет содержать новый образ.

Группа образов — это механизм хранения образов Windows в хранилище образов WDS. Файловые ресурсы доступны в группе и хранятся отдельно, что делает использование группы образов более эффективным приемом, чем индивидуальное хранение образов на сервере. WDS предложит задать для группы образов имя по умолчанию ImageGroup I, но его можно изменить по своему усмотрению. Вы можете создать столько групп образов, сколько понадобится для управления образами (рис. 1-10).

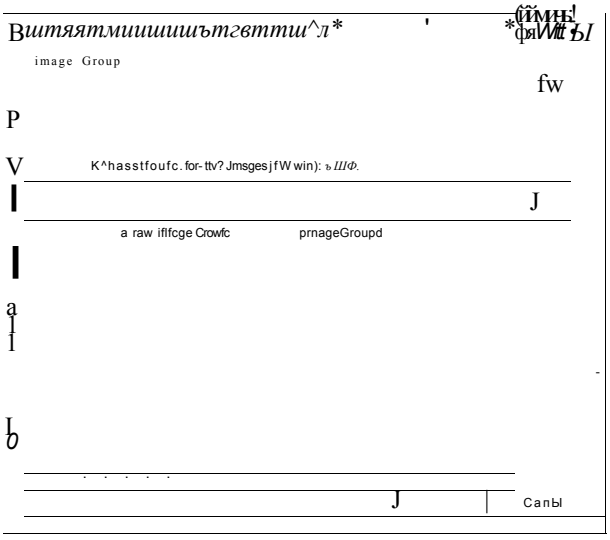


Рис. 1-10. Создание группы образов

После того как вы укажете группу образов, мастер попросит вас выбрать установочные образы, которые вы хотите добавить в хранилище образов. В зависимости от версии купленной вами операционной системы, будет отображено разное количество доступных образов. Например, на рис. 1-11 изображен

файл Install.wim, содержащий шесть образов системы Windows Server 2008 (три версии с двумя опциями — полная установка (Full) или Ядро сервера (Server Core) — для каждой версии).

Например, если вы приобрели ключ продукта для установки системы Windows Server 2008 версии Enterprise, вам нужно будет установить флажки напротив второй и пятой версий (см. рис. 1-11) и сбросить все остальные. В результате в ваше хранилище образов будет добавлено два образа: один для полной установки системы Windows Server 2008 Enterprise Edition, а другой для установки ядра сервера. Если же вы установите флажки напротив всех предложенных образов, ваше хранилище образов будет выглядеть примерно так, как показано на рис. 1-12.

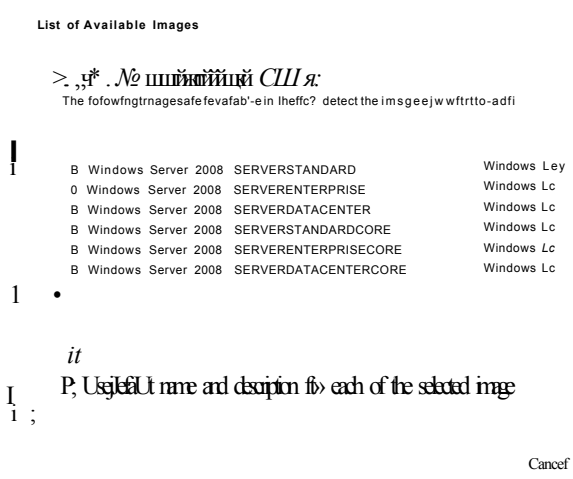


Рис. 1-11. Выбор установочных образов, которые следует добавить в хранилище образов

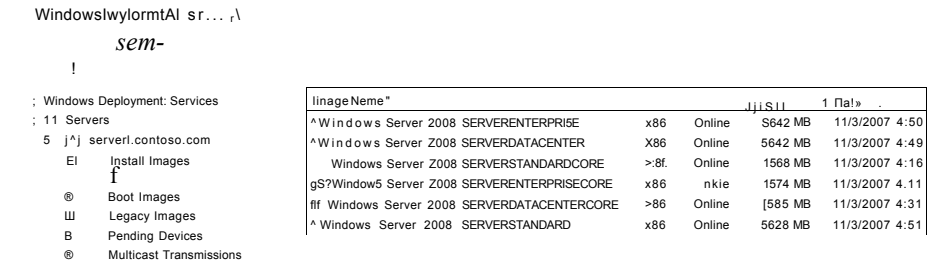


Рис. 1-12. Хранилище образов с шестью установочными образами

Вы также можете настроить доступ к образам в группе образов. Щелкните правой кнопкой мыши группу образов в консоли Служб развертывания Windows (Windows Deployment Services) и в отобразившемся меню щелкните Безопасность (Security). Когда откроется окно свойств группы образов (Image Group: Properties), перейдите на вкладку Безопасность (Security) и настройте ACL для своей группы образов и образов, которые к ней относятся.

Добавление установочного образа с помощью утилиты Wdsutil.exe

Вы также можете воспользоваться утилитой Wdsutil.exe и добавить установочный образ по умолчанию со своего DVD-диска Windows Server 2008 в нужную группу образов хранилища образов. Чтобы это сделать, необходимо выполнить такую команду:

```
Wdsutil.exe /Add-Image /ImageFile:DVD_drive_letter
\Sources\Boot.wim /ImageType:Install /ImageGroup:name
```

Другие задачи настройки

Еще одна задача, которую вам нужно решить, — это настроить загрузочное меню. Когда загружается PXE-совместимый компьютер, на котором нет операционной системы, он соединяется с PXE-сервером, находящимся на вашем WDS-сервере, получает IP-адреса и загружает WDS-клиент. Затем WDS-клиент отображает загрузочное меню, в котором содержится список предлагаемых для установки операционных систем. В этом загрузочном списке может быть указано несколько версий системы Windows, ряд возможных вариантов установки одной версии системы Windows, разные параметры установки (Полная (Full) или Ядро системы (System Core)) одной версии или разные типы архитектуры процессора (x86 или x64). В загрузочном меню WDS используется та же структура загрузочного меню, что и в меню BCD (Boot Configuration Data), используемого в системах Windows Vista и Windows Server 2008.

Загрузочное меню отображается только в том случае, если на WDS-сервере доступно более одного загрузочного образа. Другими словами, если вы добавите на сервер только загрузочный образ по умолчанию, то никакое загрузочное меню на компьютере клиента отображаться не будет. Загрузочные меню не могут поддерживать более тринадцати загрузочных образов, что связано с ограниченным количеством символов, которые могу быть отображены. Цель, которую вы будете преследовать, добавляя на сервер загрузочные образы, — это предоставление пользователям различных функций каждой операционной системы. Например, вы можете использовать один загрузочный образ для запуска программы установки системы Windows и инсталлировать ее в обычном режиме, второй загрузочный образ — для запуска мастера Захват образов WDS (WDS Image Capture Wizard), с помощью которого можно захватить образ основного компьютера и использовать его как установочный образ для последующих инсталляций, а третий загрузочный образ — для переразбивки и переформатирования жестких дисков, поддерживающих программу шифрования данных BitLocker Drive Encryption (предшествует установке системы Windows).

Добавив в свой WDS-сервер несколько загрузочных образов, вы сможете пользоваться утилитой Bcdedit.exe для изменения загрузочного меню — файла Default.bcd. Этот файл находится в папке Path\RemoteInstall\Boot\architecture

на вашем сервере. Папку RemoteInstall вы можете найти в NTFS-разделе, который вы выбрали во время настройки WDS. Для получения дополнительной информации об этой утилите введите в командной строке команду *bcdedit.exe /?*.

Параметров у самого WDS-сервера очень много. Для настройки этих многоуровневых параметров с помощью консоли Служб развертывания Windows (Windows Deployment Services) щелкните правой кнопкой мыши узел вашего сервера и в открывшемся меню выберите Свойства (Properties), а затем в появившемся окне перейдите на вкладку, которую хотите настроить (рис. 1-13).

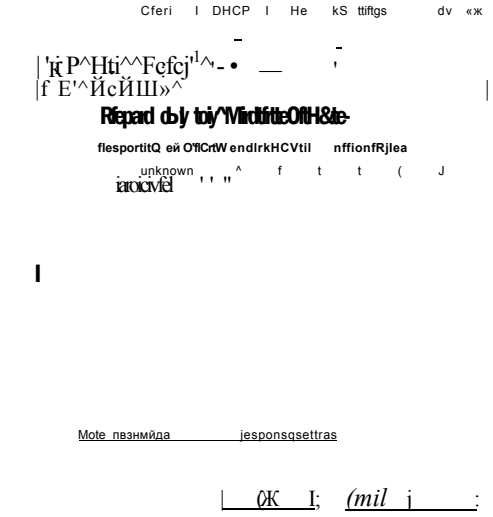


Рис. 1-13. Настройка параметров сервера

Ниже описаны доступные параметры для каждой из восьми вкладок окна свойств.

- Общие (General) Отображается имя сервера, режим работы, расположение удаленной папки, в которой хранятся образы.
- Параметры ответа PXE (PXE Response Settings) Определяются политика ответа сервера и типы компьютеров (известные или неизвестные), которые могут загружать и устанавливать образы с сервера. Также определяется время задержки загрузки PXE в секундах (по умолчанию — 0).
- Службы каталогов (Directory Services) Указываются имя учетной записи компьютера и место, где в Active Directory хранится информация об этой учетной записи для каждого компьютера, который использует WDS. При необходимости предотвратить создание учетной записи перейдите на вкладку Клиент (Client).
- Загрузка (Boot) Указываются сетевая программа загрузки по умолчанию и образ для каждого типа архитектуры (x86, x64 или IA64). Для компьютеров с архитектурой процессора x86 и x64 программа Pxeboot.com установлена по умолчанию. Эта программа при загрузке предлагает пользователям нажать кнопку F12, после чего продолжает WDS-установку. Альтернативой программе

Pxeboot.com является сетевая программа Pxeboot.nl2. Она немедленно переводит PXE-клиент в WDS-установку без необходимости нажимать кнопку F12. Другая альтернатива — программа Abortpxe.com. Эта сетевая загрузочная программа удостоверяется в том, что компьютер клиента может быть загружен со второго загрузочного устройства, указанного в BIOS. Кроме того, данная программа препятствует случайному запуску процесса загрузки PXE.

- **Клиент (Client)** Эта вкладка используется для активизации и настройки установки клиентского программного обеспечения WDS.
- **DHCP** Вам нужно настраивать данную вкладку только в том случае, если DHCP-сервер функционирует на вашем WDS-сервере. Когда DHCP-сервер работает локально, вам нужно настроить DHCP таким образом, чтоб он не прослушивал порт 67, и вам следует настроить для этого DHCP-сервера опциональный тег 60. Настройка этих параметров «делит» ответственность DHCP- и WDS-серверов, что предотвращает конфликты.
- **Параметры сети (Network Settings)** Указываются IP-адреса и диапазон портов, а также пропускная способность сети — от 10 Мбит/с до 1 Гбит/с (пропускную способность сети можно установить по своему усмотрению). Также эта вкладка используется для настройки широковещательного диапазона адресов при выполнении широковещательного развертывания.
- **Дополнительно (Advanced)** Используется для авторизации вашего WDS-сервера в DHCP, а также для указания доменного контролера и глобального каталога или разрешает WDS-серверу находить их самостоятельно.

Заметьте, вы можете воспользоваться утилитой Wdsutil.exe для настройки большинства из перечисленных выше параметров. Для получения дополнительной информации о Wdsutil.exe воспользуйтесь командой *wdsutil.exe /?*.

К СВЕДЕНИЮ Настройка параметров сервера

Для получения детальной информации о каждом параметре WDS в консоли Службы развертывания Windows (Windows Deployment Services) вызовите команду Справка\Помощь (Help\Help Topics).

Захват образов с помощью WDS

После установки и настройки WDS-сервера, следующим шагом должен стать захват и изменение загрузочного и установочного образов, которые вы будете использовать далее для инсталляции системы Windows на удаленные компьютеры (также известные, как компьютеры клиентов). Запомните, что WDS-сервер можно использовать для развертывания Windows Vista и Windows Server 2008 (и даже более ранних операционных систем Windows, в случае если вы обновили свой сервер с Windows Server 2003, поддерживающий WDS). Другими словами, эти процедуры могут быть использованы для развертывания операционных систем как на компьютеры клиентов, так и на серверы. Мы же рассмотрим развертывание операционной системы Windows Server 2008 с помощью WDS.

Загрузочный образ загружает компьютер и начинает процесс установки системы Windows. Загрузочные образы содержат в себе систему Windows PE

и клиент WDS, которые отображают загрузочное меню на компьютере клиента, что, в свою очередь, позволяет вам указать, с какого образа операционной системы необходимо делать установку. Загрузочные образы можно добавлять в хранилище образов WDS-сервера, можно изменять. Кроме того, вы можете использовать их как базис для создания двух специальных типов загрузочных образов: захваченных и обзорных.

Захваченный образ — это такой образ, который вы используете для загрузки основного компьютера. Основным называется компьютер, где установлена основная система — изменяемая система Windows, которую вы планируете дублировать на один или несколько удаленных компьютеров. Для использования захваченного образа вам сначала нужно приготовить основную установку путем настройки системы Windows, установки приложений и настройки других необходимых параметров. Затем вы должны на основном компьютере запустить утилиту Sysprep для удаления любой специфической информации с вашей основной установки. После того как утилита Sysprep выключает компьютер, вы перезагружаете систему, захватываете образ системы с помощью загрузившегося мастера захвата образов и сохраняете его как .wim-файл в указанную ранее папку. Захватив основной образ, вы должны поместить его в хранилище образов как новый установочный образ, который в последующем можно будет развертывать на удаленных компьютерах с помощью WDS-сервера.

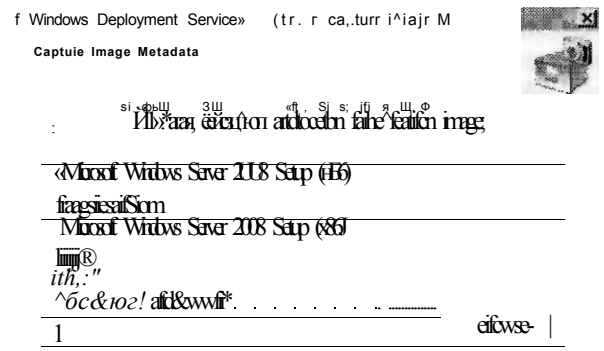
Обзорный образ — это загрузочный образ, который вы можете использовать для развертывания установочного образа на несовместимый с PXE компьютер. Обзорные образы применяются в разных ситуациях. Например, вы можете использовать такие образы для развертывания системы Windows на старые компьютеры, которые не поддерживают PXE-загрузку. Для этого нужно создать обзорный образ, сохранить его на загрузочный диск (CD/DVD) или на флэш-память, загрузить компьютер с этого носителя информации и начать процесс установки. Обзорные образы можно использовать и в средах, где PXE запрещено политикой безопасности. Также вы можете использовать обзорные образы в средах, где установлено несколько WDS-серверов, и настроить каждый обзорный образ на подключение к разным WDS-серверам для начала процесса развертывания.

Создание захваченного образа

Создавая новый захваченный образ, начните с загрузочного образа по умолчанию, который хранится в папке Загрузочные образы (Boot Images) консоли Службы развертывания Windows (Windows Deployment Services). Щелкните правой кнопкой мыши загрузочный образ по умолчанию и в появившемся меню выберите Создать захваченный загрузочный образ (Create Capture Boot Image), чтобы запустить мастер создания захваченного образа (Create Capture Image Wizard). На первой странице этого мастера вам нужно указать имя и привести описание захваченного образа, выбрать имя и папку для его хранения (рис. 1-14). Папка должна находиться на локальном жестком диске WDS-сервера.

Щелчок кнопки Далее (Next) приведет к тому, что мастер создания захваченного образа (Create Capture Image Wizard) начнет извлечение образа из исходного файла (загрузочный образ по умолчанию) и захватит его в конечный файл .wim, который вы указали ранее. После того как этот процесс завершится,

нужно щелкнуть правой кнопкой мыши папку Загрузочные образы (Boot Images), в открывшемся меню выбрать Добавить загрузочный образ (Add Boot Image) и добавить новый захваченный образ в хранилище образов (рис. 1-15).



4 j Щ. **J 0**

Рис. 1-14. Создание захваченного загрузочного образа

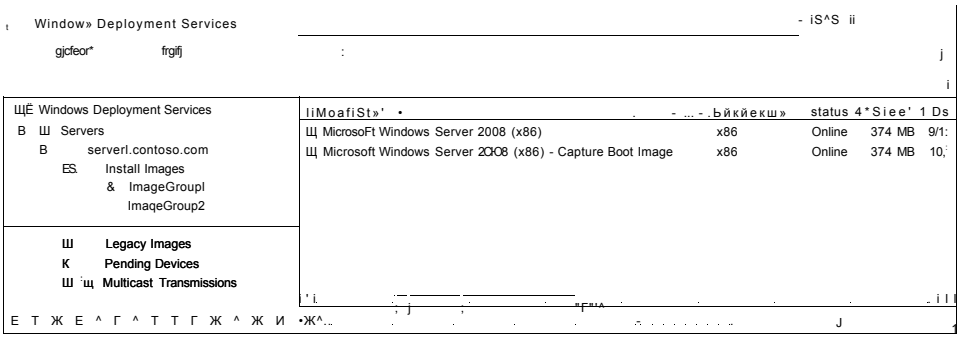


Рис. 1-15. Захваченный загрузочный образ и загрузочный образ по умолчанию

Создание обзорного образа

Создание обзорного образа требует несколько большего количества настроек, чем создание захваченного образа. Чтобы создать новый обзорный образ, щелкните правой кнопкой мыши загрузочный образ по умолчанию и в открывшемся меню выберите Создать обзорный загрузочный образ (Create Discover Boot Image). На первой странице мастера вам нужно указать имя и дать описание образа, определить имя и папку для его хранения, указать полное доменное имя (FQDN Fully Qualified Domain Name) WDS-сервера, к которому будет подключаться клиент (рис. 1-16). Щелчок кнопки Далее (Next) приведет к тому, что мастер начнет извлечение образа из исходного файла и захватит его в конечный файл .wim, который вы указали ранее. После этого вы сможете добавить новый обзорный образ в хранилище образов. Если вам нужно создать загрузочный

диск (CD/DVD) или флэш-память с этим образом, воспользуйтесь утилитой Oscdimg, которая находится в пакет Windows AIK. Принцип использования утилиты Oscdimg продемонстрирован в упражнении 1 предыдущего занятия.

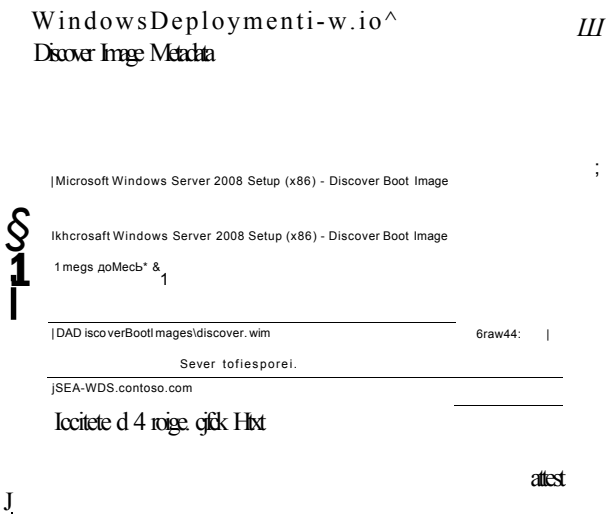


Рис. 1-16. Создание обзорного загрузочного образа

Развертывание образов с помощью WDS

После того как вы настроили WDS-сервер, добавили загрузочные образы, захватили установочный образ с измененного основного компьютера и добавили его в хранилище образов, вы можете начинать развертывать систему Windows на компьютерах клиентов. Чтобы это можно было сделать, компьютеры клиентов должны обладать как минимум 512 Мбайт оперативной памяти (в противном случае они не смогут загрузить и запустить систему Windows PE), а их система BIOS должна быть настроена таким образом, чтобы загрузка начиналась с установки PXE-совместимой сетевой карты (конечно, если вы не будете загружать компьютер с CD/DVD-диска или флэш-памяти).

Вы можете использовать WDS для развертывания образов как в ручном, так и в автоматическом режиме — для этого нужно использовать файлы ответов. Ручное развертывание требует меньших приготовлений с вашей стороны и много внимания со стороны клиента. При автоматическом развертывании для создания файла ответов понадобится утилита Windows SIM.

Ручное развертывание образа

Чтобы развернуть установочный образ в ручном режиме на компьютере клиента, загрузите компьютер клиента и сразу же после соответствующего запроса нажмите кнопку F12. На экран будет выведено окно загрузки Windows (Windows Boot), в нем нужно выбрать загрузочный образ, который вы хотите использовать для загрузки системы и начала процесса установки (рис. 1-17).

После того как загрузочный образ загрузится с TFTP-сервера, компьютер клиента запустит Windows PE, и система попросит вас указать язык, на котором необходимо будет запустить программу установки Windows (Windows Setup), как показано на рис. 1-18.

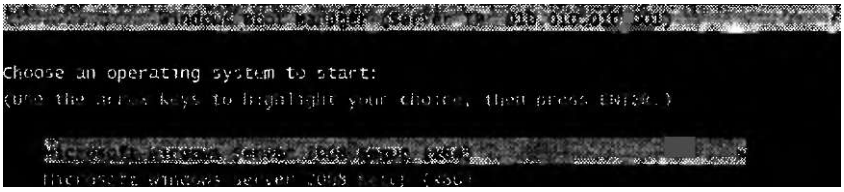


Рис. 1-17. Выбор загрузочного образа при развертывании в ручном режиме

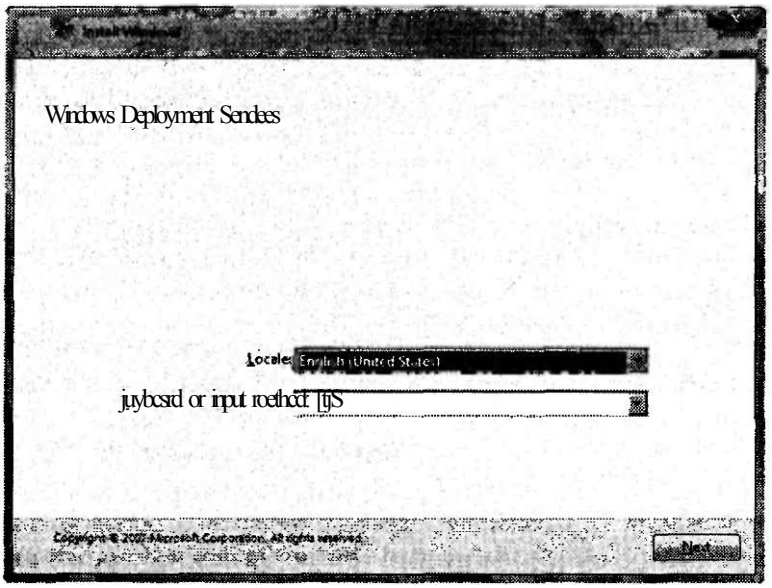


Рис. 1-18. Выбор языка установки

Вам нужно ввести реквизиты системного администратора домена, чтобы подключить компьютер клиента к хранилищу образов, которое находится на вашем WDS-сервере. После того как подключение будет установлено, на экране отобразится список доступных установочных образов. Выберите измененный образ вашей основной установки (рис. 1-19).

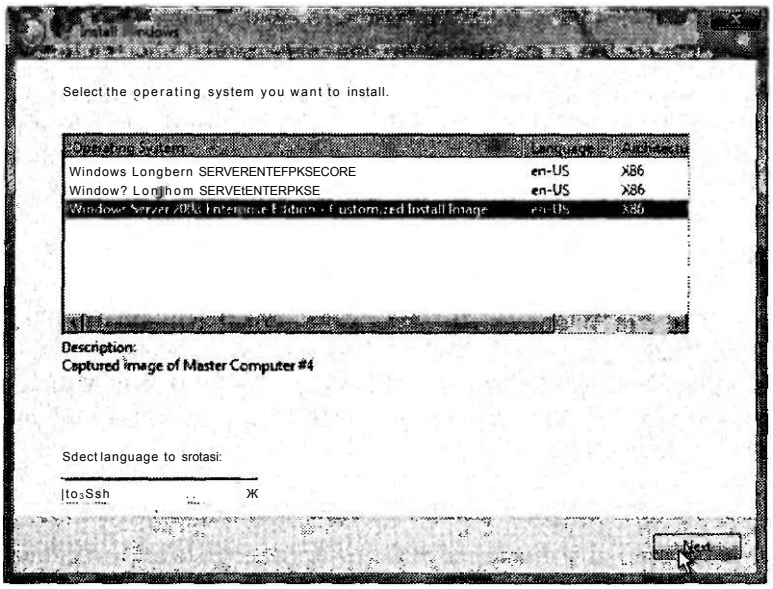


Рис. 1-19. Выбор установочного образа

После щелчка кнопки Далее (Next) система попросит указать диск, на который необходимо установить Windows, затем сервер инициирует сессию с компьютером клиента, начнет загрузку установочного образа и последующую его установку на компьютер клиента. По завершении этого процесса удаленный компьютер перезагрузится, и программа установки завершит свою работу.

Что происходит во время развертывания

Очень важно понимать, что же на самом деле происходит во время развертывания. Такого рода знания необходимы для диагностики проблем, которые могут возникнуть во время этого процесса. Ниже приведен краткий обзор того, что происходит на сетевом уровне, когда PXE-совместимый компьютер подключается к WDS-серверу для загрузки и установки образа.

1. Компьютер клиента передает сообщение DHCP для установки связи с DHCP-сервером.
2. DHCP-сервер отвечает, отправляя ответное сообщение DHCP, в котором он предлагает клиенту IP-адреса.
3. Клиент отправляет сообщение-запрос DHCP, в котором сообщает, что он арендует IP-адреса, которые были ему предложены в предыдущем сообщении.
4. DHCP отправляет клиенту сообщение-подтверждение, в котором сообщает, что указанные IP-адреса присвоены клиенту.
5. Клиент передает второе сообщение-запрос DHCP для того, чтобы найти PXE-сервер (WDS-сервер).
6. PXE отправляет сообщение-ответ DHCP, в котором содержатся информация о ServerHostName (имя WDS-сервера) и файл BooFileName (pxeboot.com) для инициирования ручной установки посредством нажатия кнопки F12 на компьютере клиента.)

7. Теперь клиент использует TFTP для загрузки загрузочного файла с TFTP-сервера (WDS-сервера). По сети начинает передаваться информация по протоколу UDP.
8. Завершив загрузку этого файла, клиент начинает загрузку файла Bootmgr.exe (Windows Boot Manager), используя TFTP.
9. После загрузки данного файла на компьютере клиента отображается меню загрузки, в котором вам нужно выбрать загрузочный образ.
10. Начинается загрузка загрузочного образа с сервера (с помощью TFTP) и последующая его загрузка в память компьютера клиента.
11. На данном этапе система Windows PE загружена в оперативную память, и после того как вы выберете установочный образ и укажете другую необходимую информацию, сервер начнет использовать SMB (Server Message Block) для загрузки и установки указанного вами образа, который можно будет применить к компьютеру.

Практикум. Настройка служб развертывания Windows

В этом практикуме вы установите и настроите Службы развертывания Windows (Windows Deployment Services) на компьютере Serverl. Затем вы, используя WDS, развернете систему Windows Server 2008 на компьютере Server2. Для выполнения этого практикума нужно иметь как минимум 3 Гбайт свободного пространства на жестком диске NTFS компьютера Serverl. Компьютер Server2 должен поддерживать PXE-загрузку и находиться в той же физической или виртуальной сети, что и компьютер Serverl, и на нем не должно быть операционной системы. Заметьте, что виртуальные машины в программе Virtual PC 2007 соответствуют требованиям PXE, о которых говорилось выше. Также следует иметь в виду, что в программе Virtual PC вам нужно удостовериться, что обе виртуальные машины подключены только к локальной сети.

Упражнение 1. Добавление роли сервера развертывания Windows

Выполняя данное упражнение, вы установите роль службы развертывания Windows (Windows Deployment Services) на компьютер Serverl.

1. Аутентифицируйтесь на компьютере Serverl как администратор домена и откройте Диспетчер сервера (Server Manager).
2. В дереве консоли Диспетчера сервера (Server Manager) разверните группу Роли (Roles) и на панели деталей щелкните Добавить роль (Add Roles).
   На экран компьютера будет выведено окно мастера добавления ролей (Add Roles Wizard).
3. Перейдите на страницу Прежде, чем вы начнете (Before You Begin) и щелкните кнопку Далее (Next).
4. Установите флажок Службы развертывания Windows (Windows Deployment Services) на странице Выберите роли сервера (Select Server Roles) и щелкните кнопку Далее (Next).
5. Ознакомьтесь с текстом, содержащимся на странице Обзор служб развертывания Windows (Overview Of Windows Deployment Services) и щелкните кнопку Далее (Next).

6. На странице Выберите роли сервера (Select Server Roles) удостоверьтесь, что выбраны обе роли сервера и щелкните кнопку Далее (Next).
7. Затем на странице Подтвердите установку (Confirm Installation Selection) щелкните кнопку Установить (Install).
8. На странице Результаты установки (Installation Results) щелкните кнопку Закрыть (Close).
9. Закройте окно Диспетчер сервера (Server Manager) и переходите к выполнению упражнения 2.

Упражнение 2. Начальная настройка сервера

В данном упражнении вы настроите WDS-сервер, создадите папку для хранения образов RemoteInstall и настроите параметры загрузки PXE для своего сервера.

1. Пока вы авторизированы на компьютере Serverl как администратор домена, запустите службы развертывания Windows (Windows Deployment Services) из группы программ Утилиты администрирования (Administrative Tools).
2. Расширьте дерево консоли до появления под группой Серверы (Servers) узла Локальный сервер (Local Server).
3. Щелкните правой кнопкой мыши указанный узел и в появившемся меню выберите Настроить сервер (Configure Server). В результате будет запущен мастер настройки служб развертывания Windows (Windows Deployment Services Configuration Wizard) и отобразится страница приветствия (Welcome).
4. Прочтите текст, представленный на странице Приветствие (Welcome) окна мастера настройки служб развертывания Windows (Windows Deployment Services Configuration Wizard), и щелкните кнопку Далее (Next).
5. Ознакомьтесь с текстом, который увидите на странице Папка удаленной установки (Remote Installation Folder Location).
6. В текстовом поле Путь (Path) измените путь по умолчанию (если это необходимо) на раздел NTFS, на котором свободно не менее 3 Гбайт дискового пространства. Рекомендуется (но не обязательно) указывать раздел, который не является системным разделом Windows. Именем папки по умолчанию оставьте RemoteInstall.
7. На странице Папка удаленной установки (Remote Installation Folder Location) щелкните кнопку Далее (Next).
8. Если на экране появится сообщение, в котором система предупредит вас, что выбранный раздел также является системным, щелкните кнопку Да (Yes), чтобы продолжить.
9. Прочтите текст, содержащийся на странице DHCP Option 60.
10. Пребывая на той же странице DHCP Option 60, установите оба имеющихся там флажка и щелкните кнопку Далее (Next).
11. На странице Начальные параметры PXE-сервера (PXE Server Initial Settings) прочтите весь текст.
12. На странице Начальные параметры PXE-сервера (PXE Server Initial Settings) установите флажок Отвечать только на известные компьютеры клиентов (Respond Only To Known Client Computers) и щелкните кнопку Готово (Finish).

Упражнение 3. Добавление загрузочного и установочного образов

В процессе выполнения этого упражнения вы добавите используемые по умолчанию загрузочный образ и установочный образ со своего установочного диска Windows Server 2008 в хранилище образов.

1. Пока вы авторизированы на компьютере Serverl как администратор домена, запустите службы развертывания Windows (Windows Deployment Services) из группы программ Утилиты администрирования (Administrative Tools).
2. В дереве консоли служб развертывания Windows (Windows Deployment Services) расширьте узел Локальный сервер (Local Server) под группой Серверы (Servers), пока не отобразятся папки, содержащиеся в хранилище образов.
3. Вставьте DVD-диск с системой Windows Server 2008 в привод DVD компьютера, на котором установлен WDS-сервер. Если откроется окно Автозапуск (AutoPlay), закройте его. Альтернативным решением может служить подключение .iso-файла с системой Windows Server 2008.
4. Щелкните правой кнопкой мыши кнопку Загрузочные образы (Boot Images) и в открывшемся меню щелкните Добавить загрузочный образ (Add Boot Image), чтобы запустить мастер добавления образа (Add Image Wizard).
5. На странице Файл образа (Image File) щелкните Обзор (Browse) и укажите путь к файлу Boot.wim, который находится в папке \Sources на системном DVD-диске. Затем щелкните Открыть (Open), чтобы начать добавление загрузочного образа Boot.wim с системного DVD-диска в хранилище образов вашего WDS-сервера.
6. На странице Файл образа (Image File) щелкните кнопку Далее (Next).
7. На странице Метаданные образа (Image Metadata) введите или примите предлагаемые по умолчанию имя образа и описание загрузочного образа, после чего щелкните кнопку Далее (Next).
8. Прочтите текст на странице Итог (Summary) и щелкните кнопку Далее (Next). Откроется окно Прогресс (Take Progress), и загрузочный образ с DVD-диска будет помещен в хранилище образов. Это может занять несколько минут.
9. После того как образ будет успешно добавлен в хранилище на вашем сервере, щелкните кнопку Готово (Finish).

   Теперь, когда вы добавили в WDS-сервер загрузочный образ по умолчанию, вам нужно добавить установочный образ по умолчанию со своего установочного DVD-диска с системой Windows Server 2008.
10. В консоли WDS щелкните правой кнопкой мыши узел Установочные образы (Install Images) и в открывшемся меню щелкните Добавить установочный образ (Add Install Image).

    Запустится мастер Добавление образа (Add Image Wizard). На первой станице мастера, имеющей название Группы образов (Image Group), вам нужно будет создать новую группу образов для сервера.
11. Примите предлагаемое имя группы образов и щелкните кнопку Далее (Next).
12. На странице Файл образа (Image File) укажите путь к файлу install.wim, который находится на вашем установочном DVD-диске. Откройте образ, чтобы начать процедуру его добавления в хранилище образов.

13. Пребывая на той же странице Файл образа (Image File), щелкните кнопку Далее (Next).
14. На странице Список доступных образов (List Of Available Images) просмотрите доступные образы. Установите флажки SERVERSTANDARD и SERVERENTERPRISE и щелкните кнопку Далее (Next).
15. Прочтите информацию, представленную на странице Итог (Summary), и щелкните кнопку Далее (Next). Когда откроется окно Прогресс (Task Progress), установочные образы с DVD-диска следует поместить в ваше хранилище образов. Это должно занять примерно 15 мин.
16. После того как образы будут успешно добавлены в хранилище на вашем сервере, щелкните кнопку Готово (Finish).

Упражнение 4. Добавление компьютера клиента в домен Contoso

В этом упражнении мы продолжим подготовку компьютера Server2 к установке системы. Вы добавите учетную запись компьютера Server2 в Active Directory и введете 32-битовое значение его MAC-адреса. Эта процедура необходима, так как вы настроили Службы развертывания Windows (Windows Deployment Services) отвечать только известным компьютерам.

Для выполнения этого упражнения компьютер Server2 должен работать на новой виртуальной машине или быть отдельно стоящим компьютером, поддерживающим загрузку PXE. На этом компьютере не должны быть установлены ни операционная система, ни какое-либо другое программное обеспечение. Также вам следует убрать с локальных дисков любые дисководы и CD/DVD-приводы.

1. Узнайте MAC-адрес компьютера Server2. Чтобы это сделать, запустите компьютер Server2. Если вы увидите 12-значный MAC-адрес через несколько секунд после начала загрузки, запишите его, выключите компьютер и переходите к выполнению шага 3. (В программе Virtual PC вы можете для записи MAC-адреса воспользоваться командой Пауза (Pause) меню Действие (Action).) Если вы не увидели MAC-адрес, то переходите к выполнению шага 2, чтобы активизировать PXE-загрузку в BIOS.
2. Перезагрузите компьютер Server2 и немедленно выберите опцию, которая отвечает за вход в BIOS. (В программе Virtual PC нужно нажать кнопку Del.) В программе BIOS удостоверьтесь, что PXE-загрузка задана с первого загрузочного устройства для компьютера Server2, и выйдите из этой программы, сохранив изменения. Перезагрузите компьютер Server2 и опять возвращайтесь к шагу 1.
3. Аутентифицируйтесь на компьютере Serverl как администратор домена. Откройте программу Пользователи и компьютеры Active Directory (Active Directory Users And Computers) из группы программ Утилиты администрирования (Administrative Tools).
4. В консоли Пользователи и компьютеры Active Directory (Active Directory Users And Computers) расширьте узел Contoso.com.
5. В дереве консоли щелкните правой кнопкой мыши Компьютеры (Computers) и в открывшемся контекстном меню щелкните сначала Новый (New), а затем Компьютер (Computer).

На экран будет выведено окно Новый объект - Компьютер (New Object - Computer).

6. Введите в текстовое поле Имя компьютера (Computer Name) имя *Server2* и щелкните кнопку Далее (Next). На экран будет выведено окно Управление (Managed).
7. Прочтите информацию в окне Управление (Managed) и установите флажок Этот компьютер управляется (This Is A Managed Computer).
8. Введите в текстовое поле Уникальный ID компьютера (GUID/UUID) (Computer's Unique ID (GUID/UUID)) 20 нулей и 12 символов MAC-адреса компьютера Server2. Например, если MAC-адресом компьютера Server2 является 00 03 FF 9F B5 36, вам нужно будет ввести *00000000000000000000 003FF9FB536*.
9. На странице Управление (Managed) щелкните кнопку Далее (Next).
10. Ознакомьтесь с информацией, представленной на странице Хост сервера (Host Server) и, оставив все предложенные настройки, щелкните кнопку Далее (Next).
11. На странице Новый объект - Компьютер (New Object - Computer) щелкните кнопку Готово (Finish).

Упражнение 5. Развертывание системы Windows Server 2008 с помощью WDS

В этом упражнении вы развернете систему Windows Server 2008 на компьютере Server2. Приступая к выполнению упражнения, удостоверьтесь, что компьютер Server2 находится в том же широковещательном домене (физическая подсеть или виртуальная сеть), что и компьютер Serverl. Если вы используете программу Virtual PC, этого можно добиться, настроив параметры сети (Networking Settings) для компьютера Server2, — нужно установить Адаптер №1 (Adapter #1) в режим Только локальная сеть (Local Only).

1. Запустите компьютер Server2. Через несколько секунд начнется процесс загрузки PXE, и локальный DHCP-клиент немедленно отправит запрос на получение IP-адресов для компьютера Server2. Когда IP-адреса будут выделены, система попросит вас нажать кнопку F12, чтобы начать процесс загрузки сетевой службы.
2. На компьютере Server2 нажмите кнопку F12. Для этого у вас будет всего несколько секунд. Если вы не успеете — перезагрузите компьютер Server2 и начните все с начала.

   На экране компьютера отобразится сообщение, в котором система оповестит вас о загрузке файлов загрузочного образа с компьютера Serverl. Эта процедура может занять примерно 5 мин.

   После того как загрузочный образ будет загружен, появится графический интерфейс. На экране компьютера отобразится страница WDS-мастера установки Windows (Install Windows Wizard).
3. На странице Службы развертывания Windows (Windows Deployment Services) выберите язык установки и язык клавиатуры, после чего щелкните кнопку Далее (Next). Система попросит вас ввести реквизиты доступа к домену.

4. Введите имя учетной записи и пароль администратора домена Contoso.com и щелкните кнопку ОК. Убедитесь, что имя учетной записи введено в формате соЩо5о\имя_учетной_записи.
5. На странице Выберите операционную систему, которую вы хотите установить (Select The Operating System, You Want To Install) установите флажок Windows Server 2008 SERVERSTANDARD или Windows Server 2008 SERVERENTERPRISE и щелкните кнопку Далее (Next).
6. На странице Куда вы хотите установить Windows (Where Do You Want To Install Windows) удостоверьтесь, что выбран Диск 0 (Disk 0), и щелкните кнопку Далее (Next).

   Начнется установка системы Windows. Процесс установки может продлиться около 30 мин, в течение которых сервер успеет перезагрузиться.
7. Когда появится страница Установка Windows (Set Up Windows), выберите параметры, соответствующие вашей стране или региону, время и валюту, раскладку клавиатуры и щелкните кнопку Далее (Next).
8. Если появится страница Введите ваш ключ продукта для активации (Type Your Product Key For Activation), введите соответствующий код (если он вам доступен) и щелкните кнопку Далее (Next).
9. На странице Пожалуйста, прочтите условия лицензии (Please Read The License Terms) просмотрите условия лицензии, установите флажок Я принимаю условия (I Accept The License Terms) и шелкните кнопку Далее (Next).
10. Когда будет выведено сообщение Спасибо (Thank You), щелкните кнопку Пуск (Start).
11. По запросу нажмите клавиши Ctrl + Alt + Del, чтобы аутентифицироваться в системе. В программе Virtual PC нужно нажать клавиши Alt справа + Del.
12. Щелкните Другой пользователь (Other User).
13. Введите реквизиты администратора домена Contoso.com и нажмите клавишу Enter. Появится рабочий стол и откроется окно Задачи начальной настройки (Initial Configuration Tasks).
14. Просмотрите информацию о компьютере в окне Задачи начальной настройки (Initial Configuration Tasks).

    Компьютер должен иметь полное имя Server2.contoso.com, а домен соответственно — contoso.com.
15. Щелкните Установить часовой пояс (Set Time Zone) для установки часового пояса, если это необходимо.
16. В окне Панель управления (Control Panel) откройте Центр управления сетями и общим доступом (Network And Sharing Center) и в выведенном на экран окне активизируйте Сетевое обнаружение (Network Discovery) и Общий доступ к файлам (File Sharing) на компьютере Server2.
17. Если вы задействовали программу Virtual PC, воспользуйтесь меню Действие (Action) и установите Дополнения к виртуальной машине (Virtual Machine Additions (VMA)) для компьютера Server2.

    Когда вы выберете опцию установки VMA, виртуальный CD-диск (файл .iso) прикрепится к виртуальной машине и функция автозапуска откроет новое

окно, в котором можно будет запустить файл Setup.exe с CD, а затем установить VMA.

18. Если вы используете программу Virtual PC, щелкните кнопку Готово (Finish), когда завершится установка VMA.
19. Выключите сначала компьютер Server2, а затем компьютер Serverl.

Резюме

- Службы развертывания Windows (Windows Deployment Services) — это серверная технология, которая используется для развертывания образов Windows на новые компьютеры.
- PXE-совместимый компьютер, на котором нет операционной системы, при загрузке подключается к PXE-серверу вашего WDS-сервера, получает IP-адреса и загружает WDS-клиент. Затем WDS-клиент отображает загрузочное меню, в котором имеется список доступных к установке операционных систем.
- Загрузочный образ (Boot Image) представляет смобой файл .wim, который можно использовать для загрузки нового компьютера клиента и начала развертывания на нем операционной системы. При развертывании образов с помощью WDS используются загрузочные образы по умолчанию, которые находятся в папке \Sources на установочном DVD-диске с системой Windows Server 2008.
- Установочный образ (Install Image) — это образ операционной системы Windows Vista или Windows Server 2008, который вы планируете развертывать на компьютерах клиентов. Самый простой метод использования WDS состоит в развертывании установочного образа по умолчанию, который хранится в папке \Sources на установочном DVD-диске с системой Windows Server 2008.
- Захваченным образом (Capture Image) принято называть специальный загрузочный образ, предназначенный для загрузки основного компьютера и записи образа на WDS-сервер.
- Загрузочный образ, который используется для развертывания установочного образа на PXE-совестимый компьютер, называется обзорным образом (Discover Image).

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных в ходе занятия 2. Эти вопросы представлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы

Ответы и пояснения к каждому их варианту размещены в разделе «Ответы» в конце книги.

1. Что из указанного ниже не является компонентом Служб развертывания Windows (Windows Deployment Services)?
   А. Хранилище образов.
   Б. Сервер TFTP (Trivial File Transfer Protocol).

В. Утилита Windows System Image Manager (SIM).
Г. Сервер PXE (Pre-boot execution Environment).

2. Вы хотите использовать WDS для развертывания системы Windows Vista RTM на пятидесяти PXE-совместимых компьютерах. Для этого вы установили WDS-сервер. Какие настройки следует выполнить?
   А. Создать папку Path\RemoteInstall на диске с файловой системой FAT32.
   Б. Настроить начальные параметры PXE-сервера (PXE Server Initial Settings), разрешив подключение известным и неизвестным компьютерам.
   В. Добавить файл Boot.wim иэ папки Path\Sources со своего установочного диска Windows Vista RTM в хранилище образов.
   Г. Добавить файл Install.wim из папки Path\Sources со своего установочного диска Windows Vista RTM в хранилище образов.
3. Попытавшись воспользоваться WDS-сервером, вы обнаружили, что он работает не так, как ожидалось. Хранилище образов вообще не функционирует, поэтому вы не можете воспользоваться улучшениями WDS-версии, предлагаемой в системе Windows Server 2008. Почему? (Выберите все подходящие варианты ответов.)
   А. Папка Path\RemoteInstall должна находиться на диске с файловой системой NTFS.
   Б. Начальные параметры PXE-сервера (PXE Server Initial Settings) должны быть настроены на работу только с известными компьютерами.
   В. Вы должны использовать файл Boot.wim с установочного диска Windows Server 2008 или Windows Vista с пакетом обновлений 1 (Service Pack 1).
   Г. Необходимо использовать файл Install.wim с установочного диска Windows Server 2008 или Windows Vista с пакетом обновлений 1 (Service Pack 1).

Занятие 3. Развертывание виртуальных машин

Виртуальный компьютер позволяет эмулировать физический компьютер в программной среде. С помощью таких программ, как Microsoft Virtual PC, Virtual Server и Hyper-V, вы можете запустить несколько операционных систем на одном физическом сервере. Эта технология получила широкое распространение, поскольку позволяет воспользоваться преимуществом консолидации физических компьютеров для поддержки старых операционных систем на новом аппаратном обеспечении, облегчает тестирование серверов и управление ими.

Изучив материал этого занятия, вы сможете:

- Разбираться в преимуществах виртуальных компьютеров.
- Понимать различия между тремя технологиями виртуальных компьютеров, предлагаемыми корпорацией Microsoft.

Расчетная продолжительность занятия составляет 50 мин.

Что такое виртуальные машины

Виртуальная машина (ВМ) — это программная эмуляция физического компьютера. С помощью ВМ на одном физическом компьютере можно запустить несколько операционных систем (рис. 1-20).

Рис. 1-20. На рабочем столе Windows представлено несколько ВМ

Такое программное обеспечение предлагает программную среду для операционной системы, которая идентична физическому компьютеру. Операционная система, работающая в виртуальной среде, называется *гостем* (Guest), а операционная система, под которой работает эта виртуальная среда, — *хостом* (Host). В разрезе операционной системы хоста или уровня аппаратной виртуализации каждая ВМ работает с собственной операционной системой со своими установленными приложениями (рис. 1-21).

Рис. 1-21. Аппаратная виртуализация

Зачем используют виртуальные машины

Вы можете развертывать виртуальные машины или перемещать в них данные с физических серверов для обеспечения возможности воспользоваться следующими функциями и преимуществами.

- Объединение серверов Виртуализация — наиболее распространенный способ объединения большого количества отдельно стоящих небольших физических серверов в меньшие группы физических серверов. В корпоративных сетях физические серверы обычно используют от 5 до 10 % своей мощности. Если переместить физические серверы в виртуальное окружение, эффективность их использования увеличится, а затраты на электроэнергию, охлаждение и содержание, наоборот, уменьшатся. Кроме того, таким образом сохраняется физическое место, а этот фактор часто является критичным во многих датацентрах.
- Поддержка старых операционных систем и приложений Виртуальные машины часто используются для работы приложений, функционирующих под управлением ранних операционных систем, таких как Windows NT. Если вы развернули операционную систему в виртуальной среде, то вам не придется для ее работы выделять отдельный физический сервер.
- Тестирование приложений и улучшений Виртуальную машину легко изолировать от корпоративной сети (или интегрировать в таковую); без труда поменять ее назначение. Некоторые приложения, разработанные для виртуальных машин, даже поддерживают тегирование VLAN, а также работу ВМ с несколькими подсетями. Так как виртуальные машину очень гибки в настройке, вы можете использовать их для тестирования и моделирования операционных систем, приложений или системы безопасности.
- Максимизация серверной работы Посредством виртуализации вы можете изолировать приложения в отдельной виртуальной машине и предотвратить эффект домино, когда сбой в одном приложении может повлечь за собой сбой в работе всех остальных приложений. Например, если и виртуальной машине происходит сбой какого-либо приложения, то это никак не влияет на работу сервера и других виртуальных машин. Еще одна причина, по которой говорят, что виртуализация улучшает общую работу сервера, — это уменьшение конфликтов на аппаратном уровне. Виртуальные машины с их программными аппаратными драйверами предлагают пользователям стабильное рабочее окружение для приложений, благодаря чему последние работают в виртуальных средах практически без сбоев.
- Эффективное управление сервером и его поддержка С помощью такой утилиты, как Microsoft System Center Virtual Machine Manager, вы можете удаленно управлять виртуальными машинами и даже перемещать виртуальную машину с одного физического сервера на другой с минимальными временными затратами. Это упрощает управление, обеспечивает гибкость при настройке сервера с учетом текущих нужд.

Корпорация Microsoft предлагает три решения для виртуализации компьютера: Virtual PC, Virtual Server и Hyper-V. Каждое решение отличается набором уникальных особенностей и используется для реализации определенных сценариев — каких именно, мы рассмотрим далее.

Virtual PC 2007

Подобно всем решениям по виртуализации, программа Virtual PC 2007 разрешает запускать несколько операционных систем на одном компьютере. Однако не следует забывать, что это приложение разработано для упрощения управления. В приложении Virtual PC каждая виртуальная машина отображается на рабочем столе в отдельном окне, причем размер окна можно изменить (рис. 1-22).

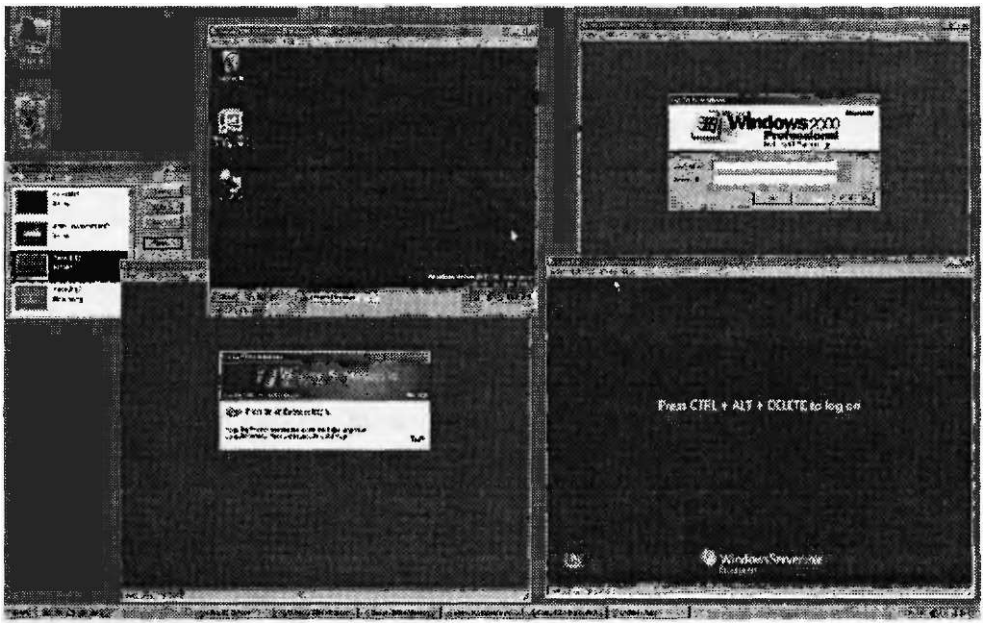


Рис. 1-22. В приложении Virtual PC каждая ВМ отображается на рабочем столе в отдельном окне

Вы легко можете изменить настройки для каждой ВМ — нужно лишь щелкнуть сначала ВМ в окне Консоль Virtual PC (Virtual PC Console), а затем кнопку Параметры (Settings), как показано на рис. 1-23.

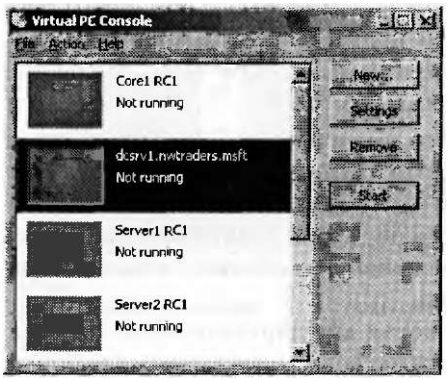


Рис. 1-23. Окно Консоль Virtual PC (Virtual PC Console) предлагает пользователям упрощенное администрирование

Ниже описаны особенности программы Virtual PC 2007 и существующие ограничения по ее использованию.

- Поддержка файлов виртуальных дисков Программа Virtual PC 2007 использует файлы виртуальных дисков (Virtual Hard Disk VHD) как локальные диски виртуальных машин. Такие виртуальные диски используются в программах Virtual Server и Hyper-V, поэтому виртуальные диски легко перемещать из одного решения в другое.
- Поддержка 64-разрядных приложений Корпорация Microsoft предлагает 64-разрядную версию программы Virtual PC 2007, в которой можно запускать программы, разработанные специально для 64-разрядных операционных систем. Однако вы не сможете запустить 64-разрядную виртуальную машину в программе Virtual PC 2007. Поддерживаются только 32-разрядные версии, даже на 64-разрядных компьютерах.
- Поддерживаемые операционные системы Вы можете установить и запустить программу Virtual PC 2007 под управлением следующих операционных систем:
  - Windows Server 2008;
  - Windows Vista;
  - Windows Server 2003;
  - Windows XP Professional;
  - Windows XP Tablet.
- Поддерживаемые гостевые операционные системы Только перечисленные ниже операционные системы могут быть запущены в виртуальных машинах программы Virtual PC 2007:
  - Windows Server 2008;
  - Windows Vista;
  - Windows Server 2003;
  - Windows XP Professional;
  - Windows 2000;
  - Windows 98 Second Edition;
  - OS/2.

  Следующие операционные системы также можно запустить в Virtual PC 2007, но официально они корпорацией Microsoft больше не поддерживаются:
  - MS-DOS 6.22;
  - Windows 95;
  - Windows 98
  - Windows Millennium Edition (Windows ME);
  - Windows NT 4.0 Workstation.
- Для гостевых систем поддерживается одноядерный процессор В программе Virtual PC 2007 каждой гостевой операционной системе соответствует отдельный виртуальный одноядерный процессор, вне зависимости от того, является ли хост-система многопроцессорной и/или многоядерной.
- Виртуальные сети Программа Virtual PC 2007 позволяет назначить для каждой гостевой операционной системы до четырех сетевых адаптеров. При

этом для каждого сетевого адаптера можно настроить один из следующих режимов работы.

- Не подключен (Not Connected) Когда выбрана данная опция, сеть в виртуальной машине недоступна. Эту опцию рекомендуется использовать при условии, что физический компьютер не подключен к сети или вы не планируете подключать виртуальную машину к сети Интернет.
- Только локальная сеть (Local Only) Опция выбирается при необходимости обеспечить сетевую поддержку только между локальными машинами. Это означает, что виртуальная машина не будет иметь доступ к каким-либо сетевым ресурсам компьютера хоста, но другие ВМ, подключенные к локальной сети, могут общаться между собой.
- Общая сеть (Shared Network (NAT)) Эта опция доступна только первому виртуальному сетевому адаптеру виртуальной машины. Когда она выбрана, ВМ подключается к частной сети, созданной программой Virtual PC. В этой сети есть виртуальный DHCP-сервер и виртуальный сервер трансляции сетевых адресов (NAT). Виртуальная машина может получить доступ к большинству TCP/IP-ресурсов, к которым имеет доступ операционная система хоста.
- Специфический физический адаптер хоста (Specific Host Physical Adapter) Если выбрана данная опция, то виртуальная машина напрямую подключается к указанному сетевому подключению операционной системы хоста. Виртуальная машина появится и будет вести себя в этой сети как отдельный физический компьютер. Если в сети используется DHCP-сервер, то виртуальная машина получит IP-адреса автоматически. Аналогично, если в сети используются статические IP-адреса, то вам придется вручную настроить виртуальную машину и присвоить ей подходящие статические IP-адреса.

ВАЖНО! Ограниченное число виртуальных сетей в программе Virtual PC
Главное ограничение программы Virtual PC заключается в том, что гостевые ВМ должны находиться в одной виртуальной сети домена. Другими словами, вы не можете создавать виртуальные сети для тестирования подключений между изолированными группами виртуальных машин.

- Подключение к хосту В программе Virtual PC вы можете подключиться к операционной системе хоста, только настроив сетевой диск, прикрепленный к какой-либо папке хоста (рис. 1-24). Это можно сделать с помощью кнопки Общая папка (Shared Folder).
- Аппаратная поддержка виртуализации Если процессор физического хоста поддерживает технологию улучшенной виртуализации, например Intel-VT или AMD-V, программа Virtual PC поддерживает эту технологию, вследствие чего производительность ВМ увеличивается. Эта опция (рис. 1-25) задана по умолчанию.
- PXE-загрузка Виртуальные сетевые адаптеры в программе Virtual PC 2007 поддерживают загрузку PXE по умолчанию. Данная технология позволяет

новым компьютерам получать DHCP-адреса и загружать операционную систему из сети. (PXE-загрузка описана в занятии 2.)

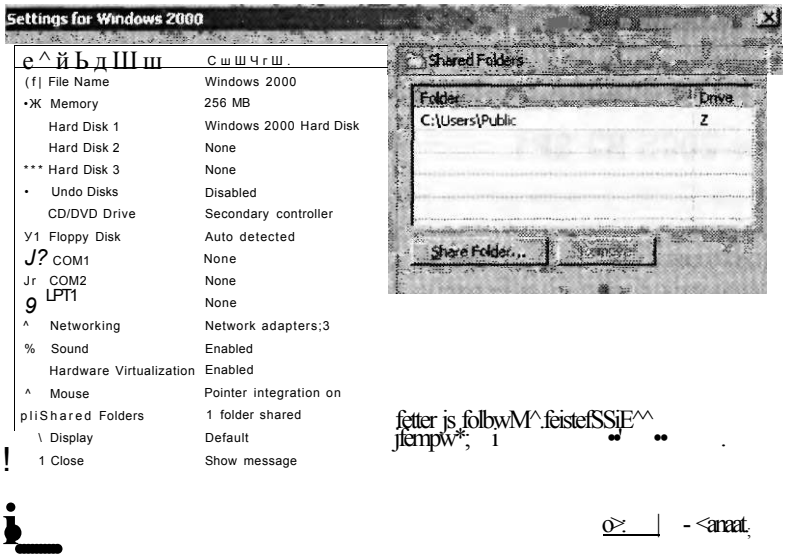


Рис. 1-24. В программе Virtual PC вы подключаете ВМ к операционной системе хоста через сетевые диски

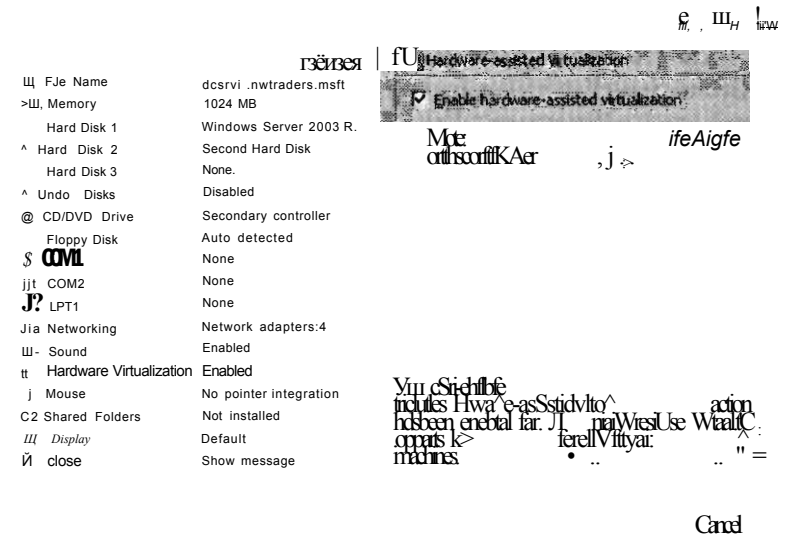


Рис. 1-25. Программа Virtual PC поддерживает аппаратную виртуализацию

Дополнения виртуальной машины Чтобы улучшить производительность любой виртуальной машины, вы должны в программе Virtual PC установить

Дополнения ВМ (VM Additions). Установка дополнений ВМ увеличивает общую производительность, повышает скорость перемещения курсора мыши, облегчает управление ею.

Поскольку в программе Virtual PC не так много нововведений и существуют определенные ограничения по применению, ее рекомендуют использовать для поддержки старых приложений, для тестирования приложений.

Virtual Server 2005 R2 SP1

Программа Virtual Server отличается от Virtual PC тем, что содержит большее количество улучшенных возможностей для корпоративных серверов и приложений, а также позволяет производить более совершенное администрирование.

Ниже описываются функции и усовершенствования программы Virtual Server, отсутствующие в Virtual PC.

- Расширенная поддержка гостевых операционных систем Наряду с операционными системами, поддерживаемыми Virtual PC, программа Virtual Server позволит вам работать и с некоторыми другими системами, называемыми гостевыми:
  - Red Hat Linux;
  - SuSE Linux;
  - Solaris;
  - Windows NT Server SP6a.
- Поддержка failover Программа Virtual Server предлагает двухузловую failover с одной виртуальной машины на другую. Эту ее особенность можно использовать только для тестирования и разработки.
- Поддержка NLB (Network Load Balancing) Для тестовых окружений программа Virtual Server поддерживает виртуальные NLB.
- Многопроцессорная поддержка Если на компьютере хоста установлены многоядерные процессоры или несколько процессоров, то одно ядро либо процессор можно назначить отдельной виртуальной машине. Вы не можете назначить более одного процессора или ядра одной гостевой виртуальной машине. Например, на компьютере с 32 процессорами вы можете распределить процессорную емкость между 31 виртуальной машиной так, чтобы каждый процессор отвечал за свою ВМ, при этом один процессор будет обрабатывать запросы хоста.
- Расширенная поддержка виртуальной сети С помощью программы Virtual Server вы можете создать бесконечное множество виртуальных сетей (широковещательных доменов), и у каждого такого домена будет свой DHCP-сервер. К тому же можно настроить DNS- и WINS-серверы, IP-адреса и время жизни таких IP-адресов.
- Поддержка SCSI Программа Virtual Server поддерживает виртуальные диски SCSI емкостью до 2 Тбайт.
- Поддержка удаленного управления Вы можете администрировать программу Virtual Server удаленно, с помощью специального веб-узла администрирования. Также вы можете получить удаленным 'доступ и администрировать виртуальные машины посредством утилиты Virtual Machine Remote Control (VMRC).

- Облегченная конверсия физических систем в виртуальные (Physical-to-virtual Conversion P2V) С помощью бесплатной утилиты Virtual Server 2005 Migration Toolkit (VSMT), которую вы можете загрузить и использовать вместе с программой Virtual Server 2005, утилита VSMT упрощает миграцию целой операционной системы вместе с установленными приложениями с физического сервера в виртуальную среду программы Virtual Server 2005.

К **СВЕДЕНИЮ Просмотрите демо P2V**
Для выполнения P2V-MnrpaijHii также можно воспользоваться утилитой Virtual Machine Manager 2007. Чтобы просмотреть пример миграции P2V с помощью утилиты Virtual Machine Manager, перейдите на веб-сайт *mms://mm.microsoft.com/ms/systemcenter/scvmm/demo/vmm_intro_03.wmv.*

Усовершенствованные возможности программы Virtual Server делают ее хорошим решением для объединения серверов, размещения сетевых приложений, тестирования комплексных сетевых сценариев, а также для поддержи в виртуальной среде операционных систем Linux и Solaris.

Hyper-V

Далее речь пойдет о Hyper-V — виртуальной технологии, которая в течение 180 дней с момента установки доступна в операционной системе Windows Server 2008. В отличие от программ Virtual PC и Virtual Server, технология Hyper-V является *hype/visor.*

Hypervisor — это тонкий слой программы, который работает на высшем аппаратном уровне и ниже операционной системы родителя. Когда установлен hypervisor, операционные системы родителя и гостя инсталлируются на разные разделы и имеют равный доступ к аппаратным ресурсам. Такая архитектура изображена на рис. 1-26.

Рис. 1-26. Hyper-V работает под управлением установленной операционной системы

В системе Windows Server 2008 технология Hyper-V управляется с помощью утилиты Hyper-V Manager, окно которой вы видите на рис. 1-27.

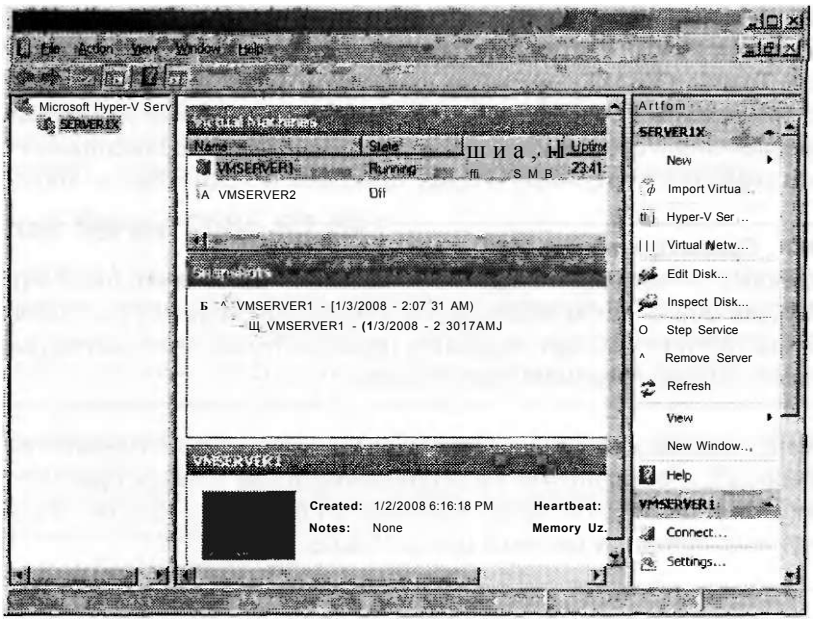


Рис. 1-27. Утилита Hyper-V Manager

По сравнению с программами Virtual PC и Virtual Server, технология Hyper-V предлагает существенные улучшения, касающиеся производительности, масштабирования и управления. Ниже перечислены некоторые специфические особенности и преимущества Hyper-V, нехарактерные для Virtual PC и Virtual Server.

- Поддержка 64-разрядных гостевых операционных систем Технология Hyper-V поддерживает в гостевых виртуальных машинах 64-разрядные операционные системы.
- Многоядерная и многопроцессорная гостевая поддержка На сервере, который поддерживает технологию Hyper-V, каждой гостевой виртуальной машине можно назначить до четырех процессоров.
- Дополнительная поддержка памяти для гостей В программах Virtual PC и Virtual Server вы могли назначать виртуальным машинам максимум 3,6 Гбайт оперативной памяти. На серверах, которые поддерживают Hyper-V, каждой виртуальной машине можно назначить до 32 Гбайт оперативной памяти.
- Повышенная производительность Технология hypervisor в сумме с поддержкой нескольких процессоров и больших объемов памяти обеспечивает более высокую производительность виртуальных машин в среде Hyper-V.
- Снимки экрана виртуальных машин Технология Hyper-V предоставляет пользователям возможность создавать образы работающих виртуальных машин, поэтому вы можете легко откатить операционную систему к предыдущим версии и состоянию.
- Улучшенная поддержка NLB Технология Hyper-V включает новую возможность виртуального переключения. Это означает, что виртуальные ма-

шины можно легко настроить на работу с NLB для балансировки загрузки виртуальных машин на разных серверах.

- Интеграционные компоненты Интеграционные компоненты (Integration Components, 1C) в технологии Иурег-V играют ту же роль, что и дополнения ВМ в программах Virtual PC и Virtual Server: они существенно увеличивают производительность и способствуют интегрированию виртуальной машины с физическим аппаратным обеспечением и родительской операционной системой. Когда вы создаете виртуальную машину в Hyper-V, то 1C, в отличие от дополнений ВМ, автоматически устанавливаются в гостевых операционных системах Windows. Однако в некоторых случаях вам все же придется устанавливать 1C вручную. Например, если вы решили переместить виртуальную машину с Virtual PC или Virtual Server в Hyper-V, сначала вам придется удалить ВМ-дополнения и только после этого начинать процесс миграции, а затем вручную устанавливать 1C. Устанавливать 1C вручную придется и в том случае, если гостевоц операционной системой является не Windows.

СОВЕТ Подготовка к экзамену

Для того, чтобы успешно сдать экзамен 70-643, вам нужно разбираться в особенностях Hyper-V.

Проверьте себя

- Что такое hypervisor?

Ответ

- Hypervisor — это тонкая прослойка программного обеспечения, которая работает под управлением родительской операционной системы и гарантирует родительской и гостевым операционным системам равный доступ к аппаратной части сервера. Можно сказать, что hypervisor превращает все локально установленные операционные системы в виртуальные машины.

Программные и аппаратные требования Hyper-V

Программа Hyper-V выдвигает жесткие требования к аппаратному обеспечению, которые привязаны к процессору. Для работы этой" программы нужен 64-разрядный процессор, который поддерживает аппаратную виртуализацию (AMD-v или Intel VT) и защиту выполнения данных. В системах с процессорами AMD эта функция защиты исполняемых данных получила название No Execute или NX Bit, а в системах с процессорами Intel она называется Execute Disable, а также XD Bit. В дополнение к этому все указанные функции должны быть активизированы в BIOS. По умолчанию они обычно отключены.

Программные требования Hyper-V: 64-разрядная версия системы Windows Server 2008 Standard Edition, Enterprise Edition или Datacenter Edition. Программа Hyper-V работает как на полной установленной версии Windows Server 2008, так и на установочном ядре сервера.

СОВЕТ Подготовка к экзамену
Запомните аппаратные и программные требования программы Hyper-V.

Установка Hyper-V

Чтобы установить Hyper-V на полной версии системы Windows Server 2008, выполните следующие действия.

1. Удостоверьтесь, что ваша система отвечает аппаратным и программным требованиям программы Hyper-V и что аппаратная виртуализация и защита выполнения данных включены в BIOS до начала установки. Если вы внесли изменения в BIOS чтобы удовлетворить последнее требование, нужно полностью выключить сервер и начать процесс установки.
2. В окне Управление сервером (Server Manager) добавьте роль Hyper-V. Чтобы это сделать, щелкните на Добавить роли (Add Roles) под Все роли (Roles Summary) и затем установите флажок Hyper-V в мастере добавления ролей (Add Roles Wizard), как изображено на рисунке 1-28.
3. Придерживайтесь инструкций, которые появляются на экране, чтобы завершить мастер добавления ролей (Add Roles Wizard).
4. По завершении работы мастера добавления ролей (Add Roles Wizard) вы должны перезагрузить компьютер, чтобы активизировать роль Hyper-V.
5. После перезагрузки аутентифицируйтесь в системе под той же учетной записью, под которой вы устанавливали роль Hyper-V.

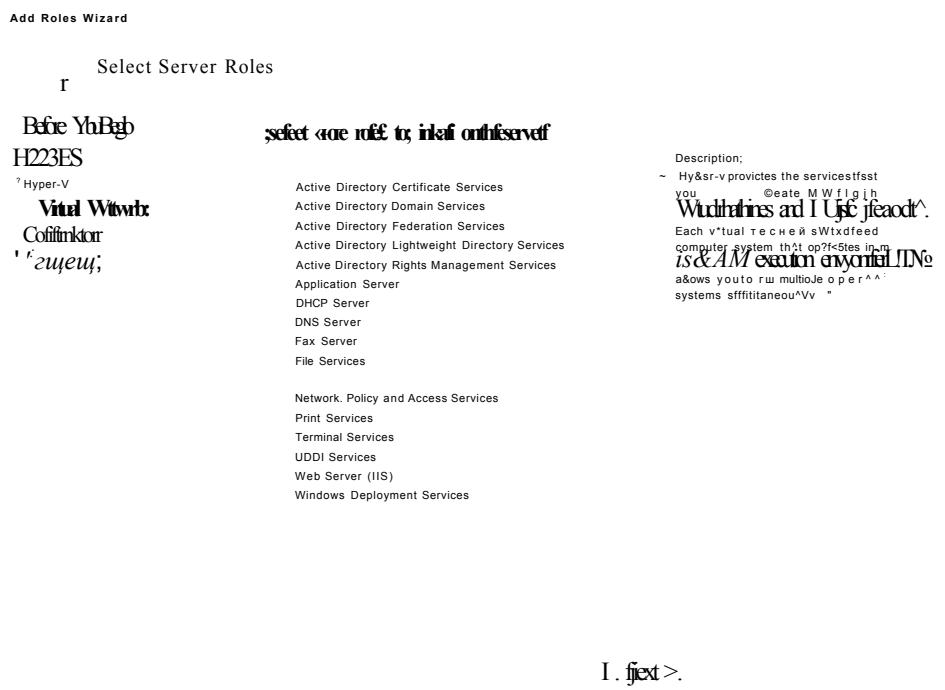


Рис. 1-28. Добавление роли Hyper-V

6. Подтвердите установку роли Hyper-V, расширив узел Роли (Roles) в окне Управление сервером (Server Manager), щелкните узел Hyper-V и удостоверьтесь, что одноименные службы запущены (рис. 1-29).

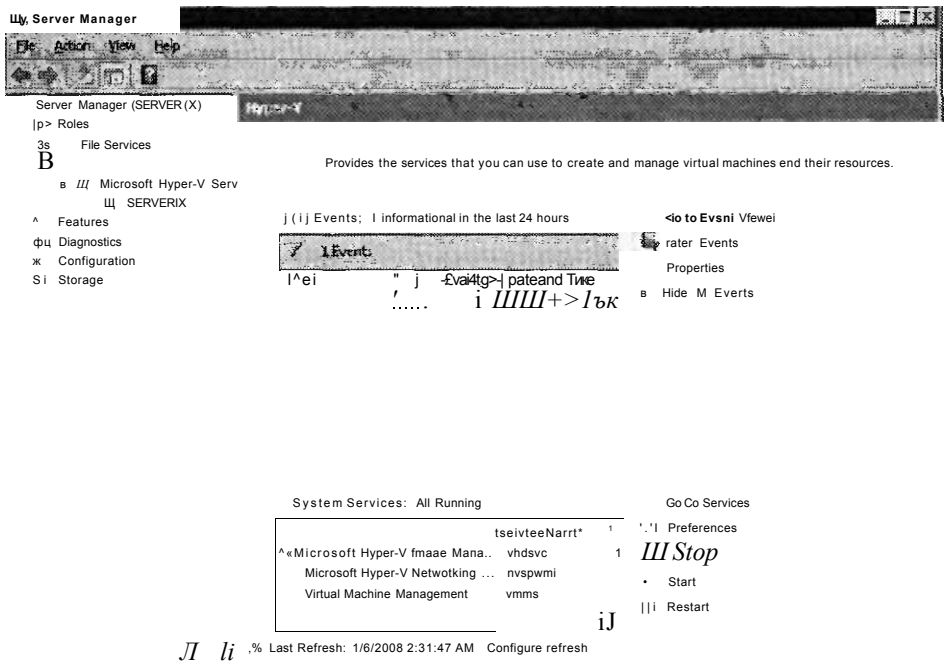


Рис. 1-29. Службы Hyper-V

ПРИМЕЧАНИЕ Сервер Hyper-V должен быть выделенным для этой роли
Для систем, у которых будет роль Hyper-V, рекомендуется выделять отдельные серверы и не устанавливать для них никакие другие роли.

Далее речь пойдет об инсталляции Hyper-V на установочном ядре сервера Windows Server 2008.

Активизация Hyper-V на установочном ядре сервера

1. Чтобы активизировать роль Hyper-V, выполните команду *start /me ocsetup Microsoft-Hyper- V.*
2. По запросу перезагрузите систему.

ПРИМЕЧАНИЕ
Для того чтобы получить возможность управлять программой Hyper-V, инсталлированной на установочном ядре сервера Windows Server 2008, необходимо удаленно подключиться к серверу с помощью программы Диспетчер Hyper-V (Hyper-v Manager).

После того как вы установите роль Hyper-V, можете начинать создавать виртуальные машины. При этом рекомендуем придерживаться описанной далее процедуры.

Создание виртуальной машины в Hyper-V

Для того, чтобы создать виртуальную машину, выполните действия, указанные ниже.

1. Откройте Диспетчер Hyper-V (Hyper-V Manager) из группы программ утилиты администрирования (Administrative Tools).
2. На панели Действия (Action) щелкните Новая (New), а затем щелкните Виртуальная машина (Virtual Machine).
3. Задавая собственные специфические параметры, следуйте подсказкам мастера. Щелкая кнопку Далее (Next), вы будете двигаться вперед, а щелкнув название страницы в левой панели, перейдете на нее.
4. Указав все необходимые параметры виртуальной машины, щелкните кнопку Готово (Finish).

Типы виртуальных дисков

Программа Hyper-V, подобно Virtual PC и Virtual Server, использует для записи содержимого виртуальных дисков файлы .vhd. Эти виртуальные жесткие диски могут быть динамически увеличивающимися, фиксированными и дифференцируемыми.

- Динамически увеличивающиеся (Dynamically Expanding) диски Диски имеют такой объем, который необходим для хранения данных. Создаваемый файл .vhd имеет небольшой размер, который при добавлении данных, естественно, увеличивается. При удалении данных с такого виртуального диска размер .vhd-файла автоматически не уменьшается. Вы можете уменьшить его объем и с помощью мастера Изменение виртуального жесткого диска (Edit Virtual Hard Disk Wizard).
- Фиксированные (Fixed) диски Фиксированные виртуальные жесткие диски используют .vhd-файл с фиксированным размером, указываемым при создании виртуального жесткого диска. Размер .vhd-файла остается неизменным вне зависимости от того, сколько на самом деле используется информации. Однако вы всегда можете, воспользовавшись мастером Изменение виртуального жесткого диска (Edit Virtual Hard Disk Wizard), увеличить размер виртуального жесткого диска, при этом размер .vhd-файла также увеличится.
- Дифференцированные (Differencing) диски Дифференцированный виртуальный жесткий диск — это виртуальный жесткий диск, который всегда ассоциирован с другим виртуальным жестким диском (связь «родитель-ребенок»). Дифференцированный диск является ребенком, а ассоциируемый виртуальный диск — родителем. Виртуальный диск родителя может быть любого типа. На дифференцированном диске (ребенке) сохраняются записи обо всех изменениях, которые были выполнены на диске родителя, и его применение является методом сохранения изменений без использования

диска родителя. Другими словами, при использовании разных дисков вы удостоверяетесь в том, что изменения, которые вы делаете по умолчанию, происходят на другом диске, а не на оригинальном виртуальном диске. По необходимости вы также можете применить изменения с другого диска для оригинального виртуального диска.

Вы можете использовать несколько дифференцированных дисков, ассоциированных с одним диском родителя. Этот метод позволяет сохранить место в том случае, если вам нужно использовать несколько виртуальных дисков, являющихся образами одного диска.

СОВЕТ Подготовка к экзамену

Для успешной сдачи экзамена 70-643 удостоверьтесь в том, что вы хорошо понимаете разницу между описанными типами виртуальных жестких дисков.

Настройка виртуальных сетей

Программа Hyper-V позволяет создавать комплексные виртуальные сети с несколькими подсетями или широковещательными доменами. Вы можете создать сеть любого из перечисленных далее типов.

- Внешняя (External) Внешняя виртуальная сеть привязана к физическому сетевому адаптеру, при этом виртуальные машины могут использовать ресурсы физических сетей. Например, если в физической сети работает DHCP-сервер, виртуальные машины, подключенные к внешней сети, будут получать DHCP-адреса с этого сетевого сервера.

  Добавляя роль сервера Hyper-V, вы получаете возможность создать внешнюю сеть для каждого аппаратного сетевого адаптера, подключенного к компьютеру.
- Внутренняя (Internal) Внутренняя виртуальная сеть позволяет подключить все виртуальные машины к локальным физическим компьютерам. Виртуальная сеть данного типа не может использовать ресурсы физических сетей.
- Частная (Private) Частная виртуальная сеть может быть использована только для подключения виртуальных машин, работающих на локальном физическом компьютере. Такую сеть нельзя подключить к локальному физическому компьютеру.

Создание новых виртуальных сетей

После установки роли сервера Hyper-V вы, возможно, захотите создать дополнительные виртуальные сети. Чтобы это сделать, в программе Hyper-V Manager в области Действия (Actions) щелкните Диспетчер виртуальной сети (Virtual Network Manager), а затем в открывшемся окне (рис. 1-30) с таким же названием установите флажок напротив нужного типа виртуальной сети и щелкните кнопку Добавить (Add).

Новую виртуальную машину, созданную с помощью мастера Новая виртуальная машина (New Virtual Machine Wizard), вы сразу же сможете подключить к любой из существующих виртуальных сетей (рис. 1-31).

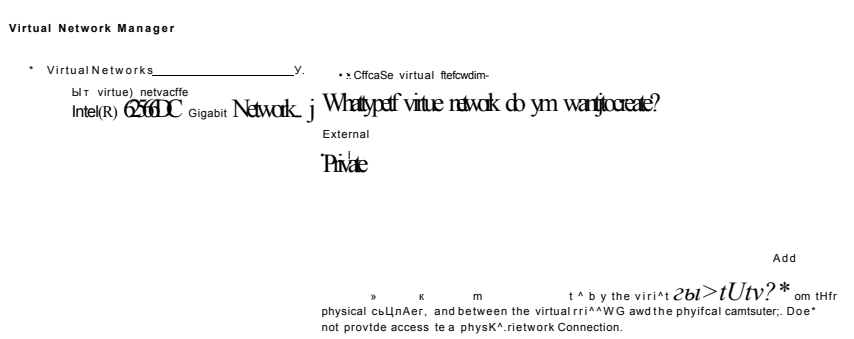


Рис. 1-30. Создание новой виртуальной сети

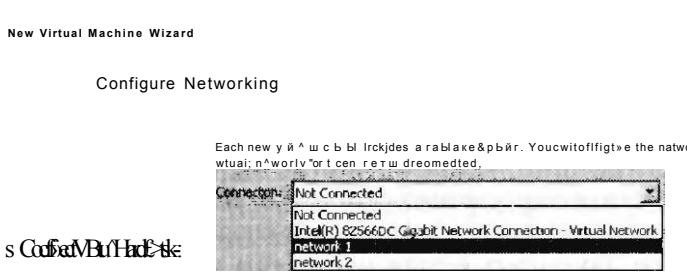


РИС. 1-31. **Добавление виртуальной машины к сети**

Назначение виртуальных машин для виртуальных сетей

Если вы хотите изолировать группу виртуальных машин от других виртуальных машин, находящихся на физическом компьютере, вам нужно объединить их в одну отдельную виртуальную сеть. Группу виртуальных машин также можно изолировать — для этого им следует назначить одну виртуальную подсеть в выделенной виртуальной сети.

Например, вы можете разделить внутреннюю виртуальную сеть InternalA на две подсети и назначить для каждой из них DHCP-сервер. Назначив отдельные виртуальные сети каждой части сети, вы можете назначить каждой виртуальной сети DHCP-сервер и разделить между этими виртуальными сетями всех клиентов. Клиенты в виртуальных сетях будут отвечать DHCP-серверам, назначенным этим сетям. Идентификаторы виртуальных сетей позволяют симулировать отдельные физические сети, которые будут находиться в одной виртуальной сети.

Чтобы назначить виртуальную машину для сети, в окне Hyper-V Manager щелкните правой кнопкой мыши виртуальную машину и в открывшемся меню выберите Свойства (Settings), как показано на рис. 1-32.

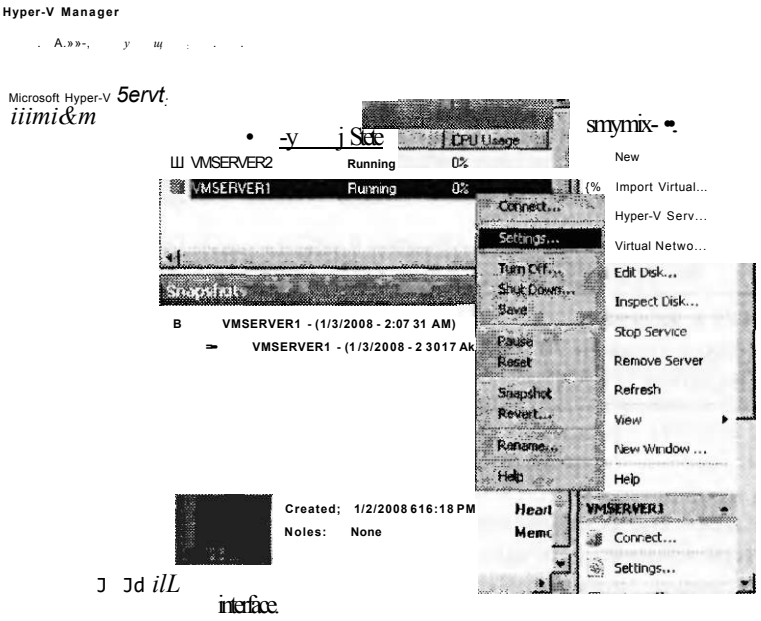


Рис. 1-32. Переход к свойствам виртуальной машины из окна Hyper-V Manager

Затем в окне свойств виртуальной машины выберите виртуальный сетевой адаптер и установите флажок напротив опции, которая отвечает за идентификацию сети (рис. 1-33). Выберите идентификатор виртуальной сети. Каждый идентификатор представляет собой подсеть с определенным сетевым адаптером. Когда идентификатор виртуальной сети активизирован на отдельной виртуальной машине, другие виртуальные машины могут подключаться к данной машине только при условии, что они прикреплены к этой же сети и к виртуальному идентификатору.

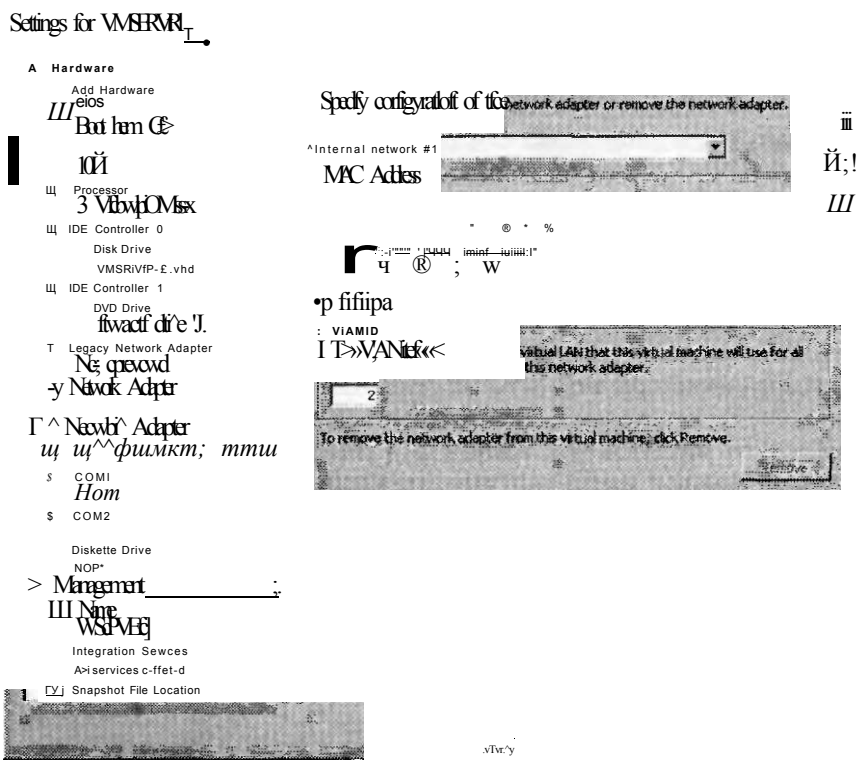


Рис. 1-33. Определение виртуальной машины в виртуальной сети

СОВЕТ Подготовка к экзамену

Чтобы успешно сдать экзамен 70-643, вам нужно изучить основы виртуальных сетей Hyper-V (включая VLAN).

Резюме

- Виртуальная машина представляет собой программную эмуляцию физического компьютера. Обычно виртуальные машины используют для объединения физических серверов, поддержки старых приложений и операционных сетей, а также для облегчения процессов разработки и тестирования приложений.
- Корпорация Microsoft предлагает три отдельных решения по виртуализации: Virtual PC, Virtual Server и Hyper-V. Каждая программа обладает уникальными возможностями.
- Установка дополнений к виртуальной машине существенно увеличивает ее производительность.
- Hyper-V — это технология hypervisor, являющаяся тонкой программной прослойкой, которая работает на верхнем аппаратном уровне и ниже родительской операционной системы. В отличие от Virtual PC и Virtual Server, программа Hyper-V поддерживает 64-разрядные операционные системы гостей, а также многоядерные и мультипроцессорные системы.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных в ходе занятия 3. Эти вопросы представлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы
Ответы и пояснения к каждому их варианту размещены в разделе «Ответы» в конце книги.

1. Какая из перечисленных ниже особенностей характерна только для программы Hyper-V, но не для Virtual PC и Virtual Server?
   А. Поддержка распределения загрузки сети.
   Б. На многопроцессорных серверах возможность назначать процессор хоста виртуальной машине.
   В. Поддержка 64-разрядных хостов.
   Г. Поддержка 64-разрядных гостевых компьютеров.
2. Какие из указанных утилит можно использовать для преобразования серверов из физического состояния в виртуальное?
   А. Virtual PC.
   Б. Virtual Server.
   В. Hyper-V.
   Г. Virtual Server Migration Toolkit.

Занятие 4. Применение инфраструктуры активации Windows

Лицензионный ключ — это ключ продукта, используемый для регистрации нескольких копий программного обеспечения. Обычно подобные ключи применяются в больших корпоративных сетях. С системами Windows XP и Windows Server 2003 эти ключи нужно было вводить во время установки, но такие системы не требовалось активировать. Со временем политика активации в системах Windows Vista и Windows Server 2008 была изменена, и теперь установленные системы нужно активировать в течение 30 дней после установки. Как результат, процесс активации является неотъемлемой частью корпоративного развертывания.

Новые параметры, процедуры и технологии, используемые для версий системы Windows Vista или Windows Server 2008, известны как Volume Activation 2.0. На данном занятии речь пойдет о параметрах и процедурах Volume Activation 2.0.

Изучив материал этого занятия, вы сможете:

- Описать различия между лицензированием MAK и KMS.
- Описать сценарии, в которых лучше использовать лицензирование MAK, а не KMS, и наоборот.
- Установить и настроить хост KMS.

Расчетная продолжительность занятия составляет 50 мин.

Типы активации продукта

Существует три типа активации продуктов для систем Windows Vista и Windows Server 2008: OEM, Retail и Volume. OEM-активация основана на BIOS. Это активация, которая происходит автоматически после установки операционной системы. Retail-активацией-называется активация операционной системы, купленной у розничного продавца. ГТри такой активации используется код активации, который можно применить только к одному компьютеру. После ввода этого лицензионного кода вы можете активировать программное обеспечение по Интернету или по телефону.

Volume-активация — более комплексный процесс. Выполняется она тремя методами с применением двух видов ключей.

- Многоразовый активационный ключ (Multiple Activation Key, МАК):
  - независимая МАК-активация;
  - активация МАК-ргоху.
- Ключ службы управления (Key Management Service, KMS):
  - KMS-активация.

СОВЕТ Как приобрести volume-лицензионный ключ

Чтобы получить volume-лицензионный ключ для продуктов Microsoft, перейдите по ссылке *http://www.microsoft.com/licensing*. Здесь же вы получите информацию о некоторых программах volume-лицензирования и контактные данные продавцов. Чтобы приобрести volume-лицензию для систем Windows Vista и Windows Server 2008, необходимо приобрести минимум пять лицензий.

Все покупатели могут приобретать и использовать МАК, но KMS-ключ предназначен только для организаций, активирующих не менее 25 компьютеров (для системы Windows Vista) или 5 физических компьютеров (для системы Windows Server 2008). Указанные ключи и методы активации описаны в следующих разделах.

Применение МАК-активации

МАК-активация обычно используется в средах, где количество компьютеров составляет менее 25. Ключ продукта используется для активации указанного числа установок системы Windows. Его пе нужно вводить во время установки, так как во всех выпусках систем Windows Vista и Windows Server 2008 вам предоставляется 30 дней, для того чтобы ввести ключ продукта и активировать систему. Активация Windows будет действительной до тех пор, пока в аппаратное обеспечение компьютера не будут внесены существенные изменения.

Есть два способа активации компьютеров с помощью МАК.

- Независимая МАК-активация Независимая активация производится в два этапа. Первый этап — ввод МАК в каждый компьютер. Вы можете это сделать во время установки операционной системы или после таковой. После установки вы можете ввести ключ клиента локально с помощью мастера изменения ключа продукта (Change Product Key Wizard) или удаленно — для этого нужно подключиться к компьютеру с помощью утилиты Volume Activation Management Tool (VAMT).

К СВЕДЕНИЮ Как можно приобрести утилиту VAMT
Утилиту VAMT можно загрузить из центра загрузок Microsoft, обратившись по адресу *http://www.microsoft.com/download.*

После завершения ввода МАК вы можете активировать систему на каждом компьютере с помощью утилиты VAMT или же по телефону (рис. 1-34).

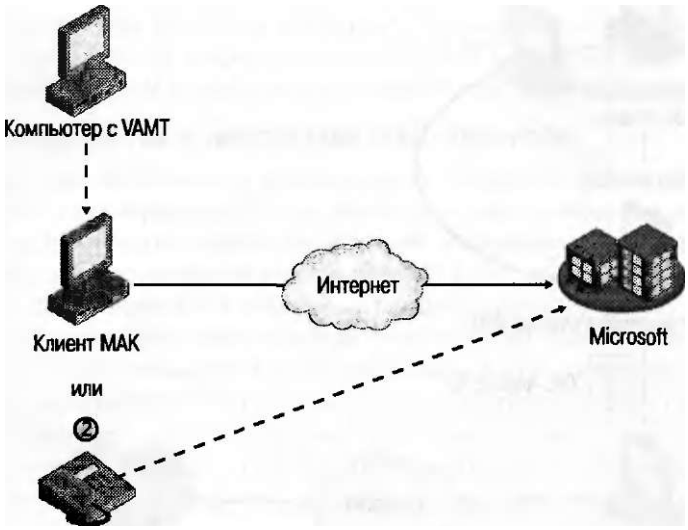


Рис. 1-34. Независимая МАК-активация производится с помощью утилиты VAMT, установленной на другом компьютере

Независимая активация — это метод, используемый для активации клиентов, которые подключены к сети Интернет. По телефону активируют не более трех компьютеров, которые к Интернету не подключены.

ВАЖНО! Активация ядра сервера
Чтобы активировать установку ядра сервера системы Windows Server 2008 с МАК- или Retail-ключом, воспользуйтесь командой *Slmgr* и выполните два описанных далее шага.

1. Если вы не ввели ключ во время установки Windows, выполните следующую команду из командной строки (*product key* — это ваш ключ продукта):

   Slmgr -ipk product key

   Если вы ввели ключ продукта во время установки Windows, то вы можете пропустить первый шаг.

2. Выполните следующую команду для активации:

   Slmgr -ato

Для удаленной активации вы можете воспользоваться командой *slmgr.* Чтобы получить дополнительную информацию по данной теме, выполните в командной строке команду *slmgr.*

Активация MAK-ргоху Активация клиентов по телефону — процедура очень кропотливая и отнимающая много времени. Если в вашей сети имеется от 4 до 24 компьютеров и все они изолированы от сети Интернет, то активировать их по телефону будет, мягко говоря, глупо. К счастью, существует простой метод активации групп компьютеров, не подключенных к сети Интернет. (Схема активации методом MAK-ргоху представлена на рис. 1-35.)

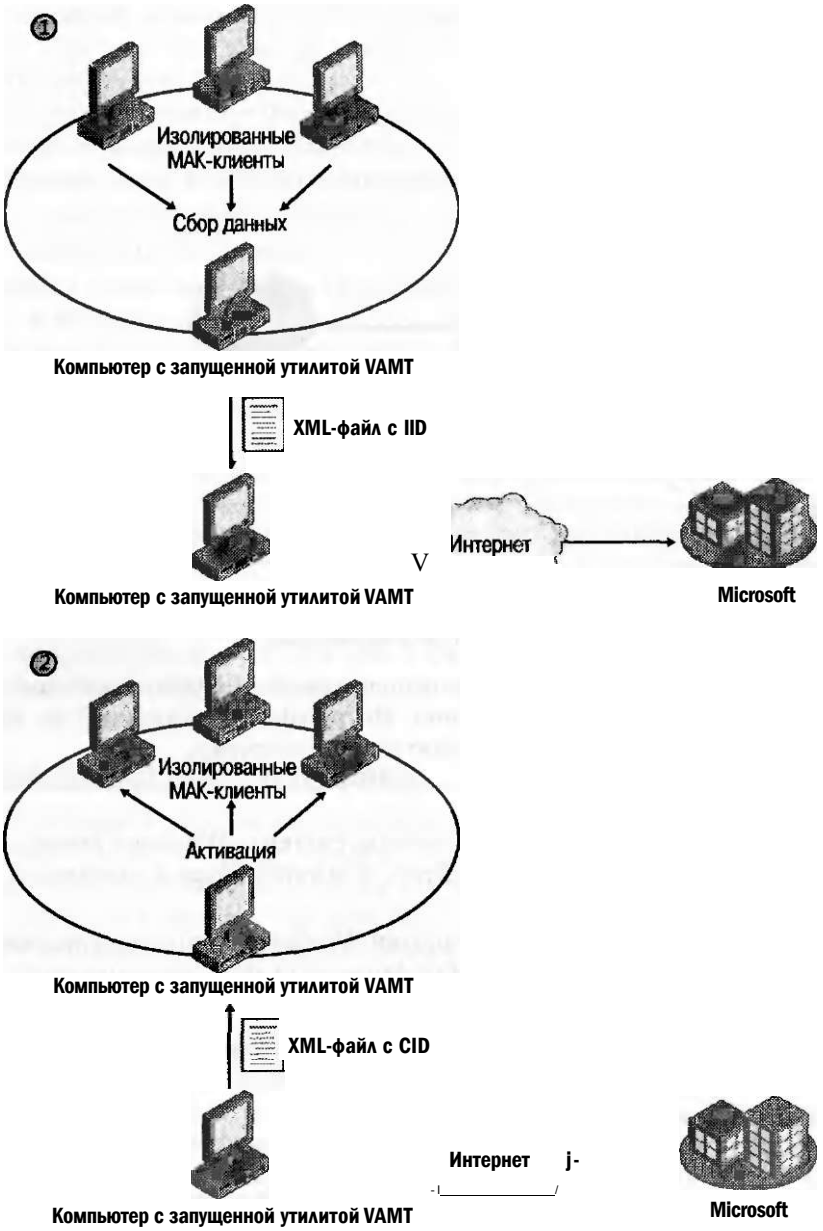


Рис. 1-35. При выполнении активации MAK-ргоху используется XML-файл

При выполнении активации MAK-proxy на компьютере, который может подключиться к изолированным компьютерам, вы для сбора установочных номеров (Installation ID IID этих компьютеров) и их последующего сохранения в XML-файл будете использовать утилиту VAMT.

Затем на компьютере, который подключен к Интернету, вы, опять воспользовавшись утилитой VAMT, подключитесь к веб-узлу Microsoft для получения подтвержденных номеров (Confirmation ID CID), которые ассоциированы с этими IID. При необходимости вы можете перемещать XML-файл от одного компьютера к другому вручную. CID сохраняются в тот же XML-файл, а после этого вы опять запускаете утилиту VAMT для подключения к изолированным компьютерам и используете обновленный XML-файл для их активации.

Преимущества и недостатки MAK-лицензии

Когда вам необходимо активировать небольшое количество компьютеров, то MAK-лицензирование — это именно то, что нужно. Такое лицензирование не требует никакой инфраструктурной установки. Для упрощения процедуры можно воспользоваться утилитой VAMT, но у вас также есть возможность ввести ключ продукта и активировать компьютеры локально — подобно тому, как это делается при использовании retail-ключей. Установленная версия Windows после MAK-активации будет действовать до тех пор, пока в аппаратное обеспечение компьютера не будут внесены существенные изменения.

Однако если нужно активировать большое число компьютеров клиентов, то администратор вряд ли согласится производить лицензирование этим методом. Вводить 250-2000 ключей продукта, запоминать, сколько раз тот или иной ключ был использован, и помнить, какие именно компьютеры уже активированы, — довольно-таки непростая задача.

Для столь больших сетей приемлемым решением будет такой способ активации, который не потребует ввода каких-либо ключей продукта на локальном компьютере и позволит активировать компьютеры клиентов без вмешательства пользователей. Такой способ существует, и называется он KMS-лицензированием.

Применение KMS-активации

KMS-активация разрешает пользователям в больших сетях активировать свои компьютеры автоматически, без подключения к серверу Microsoft. В KMS-инфраструктуре существует только один ключ на всю сеть — ключ KMS, и он устанавливается на один компьютер, который называется KMS-хостом. Из всех компьютеров сети в Microsoft активируется только KMS-хост, И эта процедура выполняется только один раз.

Компьютеры, на которых установлены volume-версии систем Windows Vista и Windows Server 2008 (KMS-клиенты), подключаясь к KMS-хосту, пытаются активироваться автоматически. Клиенты, которые не прошли процедуру активации, будут пробовать подключиться к KMS-хосту каждые два часа. По прошествии определенного времени KMS-клиенты должны проходить процедуру активации повторно, и это единственное отличие данного метода активации от других. KMS-клиенты проходят повторную активацию каждые 180 дней (или каждые 210 дней, если берется отсрочка). Активированные KMS-клиенты будут

пытаться подключиться к KMS-хосту каждые 7 дней и, если подключение пройдет успешно, обновлять 180-дневный термин активации. Если клиенты не могут подключиться к KMS-серверу по прошествии 180 дней, им предоставляется дополнительная 30-дневная отсрочка для завершения активации или выполнения переактивации. Компьютеры клиентов, которые не прошли активацию в указанный срок, перейдут в режим неполной функциональности (Reduced Functionality Mode, RFM).

Инфраструктура KMS изображена на рис. 1-36.

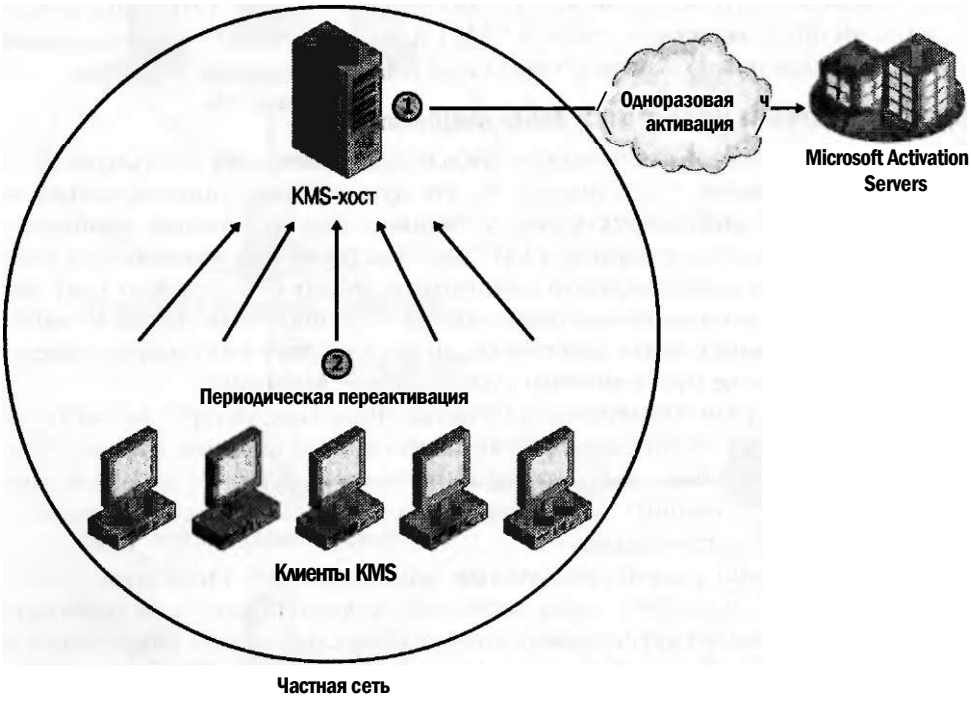


Рис. 1-36. KMS-клиенты периодически активируются, подключаясь к KMS-хосту в сети

Минимальное количество KMS-клиентов

Чтобы KMS-активация наверняка сработала, к KMS-хосту необходимо подключить минимальное количество физических (не виртуальных) компьютеров. Такое минимальное число называют порогом (Threshold). Этот ненастраиваемый параметр помогает удостовериться в том, что служба активации используется только в корпоративном окружении и работает в защищенной среде.

KMS-хост считает запросы на активацию, и отвечает на каждый верный запрос количеством систем, которые сделали запрос KMS-хосту за последние 30 дней. Если это значение равно или не превышает установленный порог KMS-активации, то KMS-клиенты будут активированы.

Пороги для систем Windows Server 2008 и Windows Vista различны и рассчитываются по определенной схеме.

- Для успешной активации системы Windows Server 2008 нужно как минимум 5 физических KMS-клиентов, которые запросят активацию у KMS-хоста. Запросы клиентов могут быть как от системы Windows Server 2008, так и от Windows Vista.
- Чтобы успешно активировать систему Windows Vista, нужно как минимум 25 запросов физических KMS-клиентов к KMS-хосту. Запросы клиентов могут быть как от системы Windows Server 2008, так и от Windows Vista.

Заметьте, что виртуальные машины не влияют на количество запросов, но после того как порог будет превышен, эти виртуальные машины также можно будет активировать.

Обнаружение KMS-хоста

Для выполнения KMS-активации клиенты должны иметь возможность обнаруживать KMS-хост в сети. Они могут найти KMS либо методом *автообнаружения* (Autodiscovery), при котором KMS-клиенты для автоматического определения KMS-хоста используют записи DNS, либо методом *прямого подключения* (Direct Connection), когда системный^администратор указывает адрес KMS-порта и порт подключения.

- Автообнаружение (Autodiscovery) По умолчанию KMS-клиенты обнаруживают KMS-хост с помощью запроса к DNS-серверу на наличие записи SRV с именем vlmcs.TCP. Если клиент ищет KMS-хост, то DNS-серверу, к которому он подключается, нужна запись SRV с именем vlmcs. TCP, в котором указан адрес KMS-хоста.

  KMS-хост будет автоматически пытаться создать запись SRV с помошыо динамического DNS. Чтобы функция автоматического обнаружения KMS работала корректно, DNS-сервер должен поддерживать регистрацию динамического DNS и записи ресурсов SRV.

  Если по каким-либо причинам динамическая регистрация DNS не работает, то администратор DNS-сервера должен создать запись SRV вручную. Полное имя записи должны быть следующим: vlmcs.TCP.DNSDomainName, где DNSDomainName — это имя локального DNS-домена. Время жизни (TTL) для таких записей составляет 60 мин. Адрес KMS-хоста и порт (1688/TCP) также должны быть включены в каждую запись.
- Прямое подключение (Direct Connection) Используя сценарий Windows Software Licensing Management Tool Slmgr.vbs, который находится в папке %SystemRoot%\System32, вы сможете указать KMS-хост на компьютере клиента и пропустить процесс автоопределения. Чтобы настроить такой тип прямого подключения, выполните следующую команду на компьютере KMS клиента (KMS-host — это DNS-имя или IP-адрес KMS-хоста):

  cscript %systemroot%\system32\slmgr.vbs -skms KMS-host

СОВЕТ Подготовка к экзамену

Чтобы успешно сдать экзамен 70-643, вам обязательно нужно знать метод ручной настройки SRV-записей на DNS-сервере и то, как можно указать прямое подключение к KMS-хосту.

Установка и настройка KMS-хоста

Все утилиты, необходимые для работы с KMS-хостом, уже включены в системы Windows Vista и Windows Server 2008. Вам нужно лишь использовать сценарий Slmgr.vbs для установки и последующей активации KMS-ключа. После выполнения этих процедур KMS-хост может начать обслуживание получаемых от KMS-клиентов запросов на активацию.

Вы должны настроить KMS-хост, выполнив указанные далее шаги на компьютере с системой Windows Vista или Windows Server 2008.

1. Установите корпоративный лицензионный ключ, выполнив в командной строке команду (Key — это корпоративный лицензионный ключ):

   Cscript %SystemRoot%\system32\slmgr.nbs -ipk Key

2. Активируйте KMS-хост по сети Интернет, выполнив следующую команду:

   Cscript %systemroot%\system32\slmgr.vbs -ato

3. Для того чтобы активировать KMS по телефону, запустите мастер активации Windows (Windows Activation Wizard) с помощью команды

   Slui.exe

   Щелкните сначала Активировать Windows по сети (Activate Windows Online Now), а затем — Использовать для активации телефон (Use The Automated Phone System To Activate).

4. Удостоверьтесь, что KMS-порт (по умолчанию это 1688/TCP) разрешен во всех брандмауэрах между KMS-хостом и компьютерами KMS-клиентов.

ПРИМЕЧАНИЕ

Не настраивайте незащищенный доступ к KMS-хосту по неконтролируемой сети, например через Интернет. Если вы это сделаете, то компьютеры других пользователей (не из вашей сети) могут быть активированы через вашу организацию.

5. Измените настройки с учетом потребностей окружения.

   Используя сценарий Slmgr.vbs и изменяя регистр KMS-хоста, нетрудно изменить настройки KMS. Например, вы можете настроить KMS на регистрацию SRV-записей ресурсов на нескольких DNS-доменах, на неполную регистрацию на DNS, использование нестандартных портов и даже на контроль временных интервалов обновления на компьютерах клиентов.

Преимущества и недостатки KMS-лицензий

KMS-лицензирование предпочтительнее MAK-лицензирования, поскольку не требует вмешательства со стороны пользователей. KMS-хост автоматически регистрирует свои адреса на DNS-сервере, после чего KMS-клиенты автоматически используют DNS для обнаружения KMS-хоста.

Недостатком KMS-лицензирования являются большие инфраструктурные требования. Во-первых, порог KMS-клиентов равен 25 KMS-клиентам системы Windows Vista и 5 клиентам системы Windows Server 2008. Во-вторых, все KMS-клиенты должны иметь возможность подключаться к KMS-хосту как

минимум один раз в 180 дней. MAK-лицензирования таких требований не выдвигает; MAK-клиент после активации остается активированным навсегда (по крайней мере до того, как в аппаратное обеспечение компьютера не будут внесены существенные изменения).

Эти технологии рассчитаны на применение в больших корпоративных сетях и обычно используются параллельно.

Пример инфраструктуры активации

Поскольку KMS-активация предпочтительнее MAK-активации, то основным правилом проектирования инфраструктуры активации для больших организаций будет простое использование KMS-лицензий, и только в некоторых случаях — использование MAK-лицензирования. Этот принцип проиллюстрирован на рис. 1-37 на примере сети с четырьмя площадками.

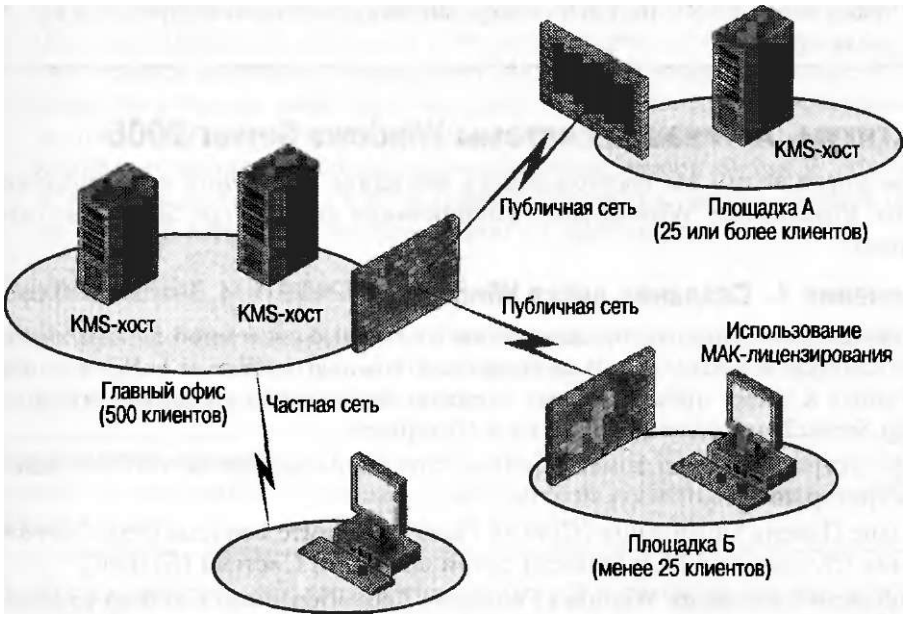


Рис. 1-37. Мультиуровневые сети обычно требуют одновременного применения KMS- и MAK-лицензирования

Как видите, на рисунке изображена частная сеть с четырьмя площадками. На площадке главного офиса 500 клиентов требуют использования KMS-лицензирования, поэтому выполняется KMS-активация. (Два сервера, показанных на рисунке, могут быть использованы для поддержки активации двух раздельных DNS-доменов и для распределения нагрузки запросов между ними). На площадке А имеется 25 или более клиентов, и этого вполне достаточно для использования локального KMS-хоста. На площадке Б для использования локального KMS-хоста клиентов не хватает, поэтому KMS-лицензирование на ней не применяется. К тому же клиенты с данной площадки не могут подключиться

к KMS-хосту, который находится в частной сети. В данном случае KMS-лицензирование применить невозможно, а вот MAK-лицензирование — вполне приемлемый вариант. На площадке B для использования локального KMS-хоста не хватает клиентов, но клиенты могут подключиться к KMS-хосту, который расположен на площадке главного офиса. Следовательно, KMS-лицензирование будет лучшим выбором.

Проверьте себя

- Для чего нужно создавать записи SRV?

Ответ

- KMS-клиенты проверяют находящуюся в DNS запись SRV, пытаясь обнаружить адрес KMS-хоста. Если локальный KMS-хост не создал такой записи SRV на DNS-сервере автоматически, то ее придется создать вручную.

Практикум. Активация системы Windows Server 2008

В этом упражнении вы воспользуетесь мастером изменения кода продукта (Change Product Key Wizard) для активирования компьютера Server2 по сети Интернет.

Упражнение 1. Создание диска Windows PE

При выполнении данного упражнения вы с помощью системной панели управления (System Control Panel) активируете компьютер Server2. Прежде чем приступить к этому практическому занятию, необходимо убедиться, что компьютер Server2 может подключиться к Интернету.

1. Зарегистрируйтесь на домене Contoso.com с компьютера Server2 как администратор домена.
2. В окне Панель управления (Control Panel) щелкните Система и ее обслуживание (System And Maintenance), затем щелкните Система (System).
3. В области Активация Windows (Windows Activation) окна Система (System) щелкните 30 дней для активации Windows (30 Day(s) To Activate Windows). Откроется страница Активируйте Windows сейчас (Activate Windows Now) мастера активации Windows (Windows Activation Wizard).
4. Щелкните Активировать Windows по сети (Activate Windows Online Now).
5. По запросу введите ключ продукта и щелкните кнопку Далее (Next). Мастер активации Windows (Windows Activation Wizard) сообщит, что активация прошла успешно, после чего будет открыто окно Активация Windows (Windows Activation), в котором система проинформирует, что вам нужно перезагрузить компьютер.
6. Щелкните кнопку Закрыть (Close) для закрытия окна Активация Windows (Windows Activation).
7. Щелкните кнопку Закрыть (Close), чтобы закрыть окно мастера активации Windows (Windows Activation Wizard).
8. Выключите компьютер Server2.

Резюме

- Политика volume-лицензирования Windows в системах Windows Vista и Windows Server 2008 была изменена, и теперь эти системы нужно активировать в течении 30 дней после их установки на компьютер.
- Для систем Windows Vista и Windows Server 2008 существует два типа volume-лицензий: с использованием многоразового активационного ключа (Multiple Activation Key, MAK) и ключа службы управления (Key Management Service, KMS). Каждая из таких лицензий ассоциирована с разными методами активации.
- MAK-лицензирование обычно применяется в средах, где менее 25 компьютеров. При MAK-активации вы используете ключ продукта для активации указанного числа копий системы Windows.
- KMS-лицензирование разрешает автоматическую активацию клиентов в больших корпоративных сетях, при этом компьютеры клиентов не подключаются к серверу активации корпорации Microsoft. В инфраструктуре KMS используется только один ключ продукта — KMS-ключ. Он устанавливается на отдельном компьютере, который называют KMS-хостом. Компьютеры, на которых установлены volume-лицензированные версии систем Windows Vista и Windows Server 2008 (KMS-клиенты), пытаются пройти процедуру автоматической активации, подключившись к KMS-хосту.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных в ходе занятия 4. Эти вопросы представлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы

Ответы и пояснения к каждому их варианту размещены в разделе «Ответы» в конце книги.

1. Вы администрируете корпоративную сеть. В главном офисе решено разместить 21 компьютер с системой Windows Vista и 4 сервера с системой Windows Server 2008. К каким операционным системам в главном офисе применимо KMS-лицензирование?
   А. Windows Vista.
   Б. Windows Server 2008.
   В. Windows Vista и Windows Server 2008.
   Г. Ни к одной из перечисленных систем.
2. Какой из указанных методов наиболее эффективен для активации 15 компьютеров с системой Windows Vista, которые находятся в тестовой сети и не имеют доступа к сети Интернет?
   А. Независимая MAK-активация.
   Б. Активация MAK-ргоху.
   В. KMS-хост активация.
   Г. Активация с использованием retail-ключа.

Закрепление материала главы

Для того чтобы попрактиковаться и закрепить знания, приобретенные в ходе изучения представленного в данной главе материала, вам необходимо:

- ознакомиться с резюме главы;
- повторить используемые в главе основные термины;
- выполнить задания лабораторной работы, которые моделируют реальные ситуации, требующие применения полученных знаний;
- выполнить рекомендуемые упражнения;
- сдать пробный экзамен с помощью тестов.

Резюме главы

- Вы можете развернуть системы Windows Vista и Windows Server 2008 с помощью установочного DVD-диска, утилит, которые включены в автоматический установочный набор Windows (Windows Automated Installation Kit, AIK) или с помощью Служб развертывания Windows (Windows Deployment Services, WDS).

  Все методы развертывания систем Windows Vista и Windows Server 2008 используют новый формат файлов образов Windows — WIM. Файлы образов .wim основаны на хранении файлов (в отличие от посекторного хранения), и поэтому их легко можно модифицировать до, во время или после развертывания.
- Вы можете использовать WDS для развертывания систем Windows Vista и Windows Server 2008 на новые компьютеры. PXE-совместимые компьютеры с помощью WDS подключаются к WDS-серверу и загружают меню доступных операционных систем. Затем конечный пользователь может выбрать из этого меню ту операционную систему, которую необходимо установить.
- Виртуальная машина — это эмуляция физического компьютера, которую в дальнейшем можно использовать для объединения серверов, тестирования и запуска старых приложений. Корпорация Microsoft предлагает три решения (Virtual PC, Virtual Server и Hyper-V), и все они применяются в разных средах.
- Hyper-V — это роль сервера системы Windows Server 2008, которая устанавливает hypervisor под операционной системой. Hyper-V дает родительской и гостевым операционным системам одинаковый доступ к аппаратным ресурсам компьютера.
- Даже volume-лицензированные версии систем Windows Server 2008 и Windows Vista нужно активировать. Существует два метода уоЫте-лицензирования: с использованием многоразового активационного ключа (Multiple Activation Key, MAK) и с помощью ключа службы управления (Key Management Service, KMS).

  MAK-лицензирование применяется в средах с 25 компьютерами. KMS-лицензирование рассчитано на большие корпоративные сети и предлагает более автоматизированное решение для активации.

Основные термины

Проверьте, знаете ли вы, что означают перечисленные ниже термины (свои ответы можно сверить с определениями, содержащимися в конце книги):

- загрузочный образ;
- захваченный образ;
- обзорный образ;
- гостевая (Guest) операционная система (ребенок);
- главная (Host) операционная система (родитель);
- hypervisor;
- установочный образ;
- служба управления ключом;
- многоразовый активационный ключ;
- файл .wim.

Лабораторная работа

Для выполнения следующих заданий используйте знания, полученные во время изучения этой главы. Правильные ответы вы сможете найти в разделе «Ответы» в конце книги.

Задание 1. Службы развертывания

Вас как администратора домена Contoso.com попросили разработать решения для развертывания 200 систем Windows Vista и 25 систем Windows Server 2008.

1. Руководство требует обеспечить возможность дистанционного управления операционными системами из центрального офиса. Какое решения для развертывания вы должны применить, чтобы выполнить это условие?
2. У вас только 20 серверов, на которых можно разместить систему Windows Server 2008; 10 других серверов компании используются для систем и приложений Windows NT и Linux и загружены на 15 %. Учитывая этот сценарий, как можно применить виртуализацию и уменьшить стоимость развертывания системы Windows Server 2008?

Задание 2. Создание инфраструктуры активации

Вы работаете в службе IT-поддержки компании Northwind Traders и входите в команду инженеров, которые занимаются развертыванием операционных систем. Компания планирует развернуть 500 компьютеров с системой Windows Vista и 50 серверов с системой Windows Server 2008. Вам поручили разработать инфраструктуру активации для этих новых операционных систем.

У сети компании Northwind Traders три площадки. На главной площадке в Нью-Йорке вы планируете развернуть 400 компьютеров с системой Windows Vista и 43 сервера с системой Windows Server 2008. В главном офисе находится изолированная исследовательская сеть на 20 компьютеров, где установлена система Windows Vista. Исследовательская сеть не имеет доступа в сеть Интернет и в остальную сеть Nwtraders.com.

Вторая площадка компании Northwind Traders находится в Бирмингеме, штат Нью-Йорк. В сети данного регионального офиса насчитывается 80 компьютеров с системой Windows Vista и 5 серверов с системой Windows Server 2008. Сеть бирмингемского офиса подключена к сети главного офиса по виртуальной частной сети (VPN).

Третья площадка размещена в городе Сиракузы, штат Нью-Йорк. В сети этого офиса насчитывается 20 компьютеров с системой Windows Vista и два сервера с системой Windows Server 2008. Сеть данного регионального офиса не соединена ни с сетью главного офиса, ни с сетью офиса в Бирмингеме.

1. Какую инфраструктуру активации вы предложите для главного офиса?
2. Какая инфраструктура активации подойдет для офиса в Бирмингеме?
3. Какую инфраструктуру активации следует разработать для офиса в Сиракузах?

Рекомендуемые упражнения

Чтобы успешно справиться с экзаменационными заданиями, выполните следующие упражнения.

Развертывание образов с помощью служб развертывания Windows

Это практическое задание поможет вам укрепить знания по развертыванию систем с помощью WDS.

- **Упражнение 1** Создайте и измените установочный образ системы Windows Vista, в котором будет пакет офисных программ Microsoft Office и ряд других программ, необходимых для повседневной работы. Затем, воспользовавшись утилитой Sysprep, завершите создание установки. С помощью захваченного образа преобразуйте установки Sysprepped в файл .wim, после чего загрузите новый образ в базу WDS и разверните образ на PXE-совместимом компьютере.
- **Упражнение 2** Ознакомьтесь с программой Криса Хенли (Chris Henley) «Overview of Windows Deployment Services», которая хранится на CD-диске в папке Webcasts. Вы также можете найти эту программу на веб-сайте *http://www.msevents.microsoft.com* по ключевым словам ID 1032322748.

Настройка активации Windows

Это упражнение поможет вам усвоить основы KMS- и MAK-лицензирования.

- **Упражнение 1** Просмотрите программу Томаса Линдемана (Thomas Lundeman) «Windows Vista Volume Activation 2.0», которая находится на CD-диске в папке Webcasts. Вы также можете найти эту программу на веб-сайте *http://www.msevents.microsoft.com* по ключевым словам ID 1032318045.

Настройка Hyper-V и виртуальных машин

Как и большинство других технологий, Hyper-V лучше всего работает при условии, что аппаратные параметры компьютера совпадают с ее требованиями (первое упражнение). В противном случае вы, вместо того чтобы получить

возможность работать в режиме реального времени, сможете лишь просмотреть слайд-шоу.

- **Упражнение 1** На компьютере с 64-разрядной архитектурой, аппаратные параметры которого удовлетворяют требованиям Hyper-V, установите систему Windows Server 2008 и добавьте роль Hyper-V. Затем установите любую гостевую операционную систему.
- **Упражнение 2** Просмотрите программу Кейта Комбса (Keith Combs) «Hyper-V Tour.wmv», которая содержится на CD-диске в папке Webcasts. Вы также можете найти эту программу на веб-сайте *http://blogs.technet.com/keithcombs.archive/2007/09/13/windows-server-2008-screencast-virtualization-10-minute-tour.aspx.*

Пробный экзамен

На прилагаемом к книге компакт-диске представлено несколько вариантов тренировочных тестов. Проверка знаний выполняется только по одной или же по всем экзаменационным темам сертификационного экзамена 70-643. Тестирование можно организовать таким образом, чтобы оно проводилось как экзамен, или же настроить его на изучение — в этом случае вы сможете после каждого своего ответа на вопрос просматривать правильные ответы и объяснения.

ПРИМЕЧАНИЕ Пробный экзамен

Подробнее о пробном экзамене рассказано во введении к данной книге.

ГЛАВА 2

Настройка серверной системы хранения данных и кластеров

Занятие 1. Настройка серверной системы хранения данных 75

Занятие 2. Настройка кластеров серверов 104

Сети хранения данных (SANs), адаптеры главной шины (HBAs) и номера логических устройств (LUNs) еще сравнительно недавно были областью деятельности исключительно специалистов по работе с устройствами хранения данных, уровень квалификации которых не дотягивал до уровня современного администратора операционной системы Microsoft Windows. Однако в связи с увеличением требований к корпоративным хранилищам, появлением таких новых технологий, как виртуальный диск Windows (Windows Virtual Disk) и технология iSCSI, эти некогда узкоспециализированные технологии включены в Windows Server 2008. Для того чтобы сегодня быть хорошим администратором сервера системы Windows, вам необходимо понимать отличия между различными уровнями RAID, а также дополнительно изучить технологии сетевого хранения данных.

В этой главе вы познакомитесь с основами управления дисками в операционной системе Windows Server 2008, а также с такими усовершенствованными технологиями хранения данных, как сети хранения данных (SANs). Кроме того, будут рассмотрены технологии создания кластеров, доступные в операционной системе Microsoft Windows Server 2008.

Темы экзамена:

- Настройка хранилища данных.
- Настройка высокой доступности.

Требования

Для изучения материала занятий в этой главе вам потребуется следующее.

- Компьютер с операционной системой Microsoft Windows Server 2008. Кроме диска с установленной операционной системой этот компьютер (присвоим ему имя Server2) должен быть оснащен одним или двумя дополнительными жесткими дисками. Оба дополнительных диска должны иметь емкость, рав-

ную емкости диска с операционной системой или большую. (Для выполнения этих требований рекомендуется использовать виртуальную машину Microsoft Virtual PC или сервер.)
- Базовое понимание администрирования Windows.

Занятие 1. Настройка серверной системы хранения данных

Операционная система Microsoft Windows Server 2008 предлагает новые способы решения проблемы хранения данных для корпоративных сетей. Из занятия вы узнаете об основных типах серверных хранилищ данных, а также о программах операционной системы Microsoft Windows Server 2008, которые могут быть использованы для управления такими хранилищами.

Изучив материал этого занятия, вы сможете:

- Разобраться в работе системы хранения данных с прямым подключением к серверу (Direct-Attached Storage), подключенной к сети системы хранения данных (Network-Attached Storage) и сетей хранения данных (Storage-Area Networks).
- Понять принцип работы службы виртуальных дисков (Virtual Disk Service).
- Понять назначение томов диска: простых, составных, чередующихся, зеркальных и RAID-5.
- Использовать оснастку Управление дисками (Disk Management) для создания различных томов диска.

Расчетная продолжительность занятия составляет 80 мин.

Понимание технологий серверной системы хранения данных

По мере возрастания спроса на системы хранения данных сервера разрабатывались новые технологии, используемые для хранения данных. За последние годы возможности серверных хранилищ данных расширились: наряду с простыми системами хранения данных с прямым подключением к серверу (Direct-Attached Storage, DAS) используются системы хранения данных, подключенные к сети (Network-Attached Storage, NAS), а также новейшие технологии, такие как волоконно-оптические каналы (Fibre Channel, FC) и сети хранения данных (iSCSI SANs).

Система хранения данных с прямым подключением к серверу

DAS — это система хранения данных, подключенная только к одному серверу. В качестве примера DAS можно привести группу внутренних жестких дисков сервера или смонтированную в стойке матрицу независимых дисковых накопителей с избыточностью (RAID), подключенную к серверу посредством SCSI- или FC-контроллера. Основная особенность DAS заключается в том, что система

предусматривает единственный сервер с быстрым доступом к данным на блочном уровне непосредственно через внутреннюю или внешнюю шину. (Доступ на блочном уровне, в противоположность доступу на файловом уровне, означает, что данные перемещены в неформатированные блоки, а не в отформатированные файлы.) DAS будет возможным решением проблемы хранения данных для серверов с высокой производительностью и не требующих значительных объемов памяти для хранения данных. Например, DAS часто применяется для серверов с инфраструктурой DNS, WINS и DNCP, а также для контроллеров доменов. Файл-серверы и веб-серверы могут хорошо работать и на серверах с системой DAS.

Основное ограничение системы DAS заключается в том, что прямой доступ к данным возможен только с единственного сервера, что приводит к неэффективному управлению системой хранения. Например, на рис. 2-1 изображена локальная сеть (Local Area Network, LAN), в которой вся система хранения данных непосредственно подключена к серверам. Несмотря на то что серверы Web и App2 имеют систему хранения с избыточностью, эти ресурсы не могут быть простым способом перенесены на серверы Mail или на Appl, для которых требуется большая емкость хранилища.

Рис. 2-1. Сеть с системой хранения DAS

Управление DAS **в операционной системе** Windows Server **2008** Основной инструмент, используемый для управления DAS в операционной системе Windows, — оснастка Управление дисками (Disk Management console). Это средство, доступное из консоли Диспетчер серверов (Server Manager), позволяет разбивать диски и форматировать наборы томов. Для выполнения таких же и других дополнительных функций вы можете использовать утилиту Diskpart.exe, работающую в режиме командной строки.

Система хранения данных, подключенная к сети

NAS является автономной системой хранения данных, легко доступной для подключения по сети для других серверов и клиентов. Устройство NAS — это сервер с заданной конфигурацией, работающий в операционной системе, специально разработанной для управления файловыми службами. Основным преимуществом NAS является простота введения в эксплуатацию и возможность обеспечить большой объем памяти для клиентов и серверов локальной сети (LAN). Недостаток NAS заключается в том, что из-за подключения серве-

ров и клиентов к устройству NAS по локальной сети, а не посредством локальной шины, доступ к данным осуществляется медленнее и происходит на файловом уровне, а не на блочном. Поэтому система NAS практически всегда работает медленнее системы DAS.

Из-за указанных особенностей и ограничений NAS часто является хорошим решением для файл-серверов, веб-серверов и других серверов, не требующих очень большой скорости доступа к данным. На рис. 2-2 изображена сеть, в которой клиенты использует устройство NAS в качестве файл-сервера.

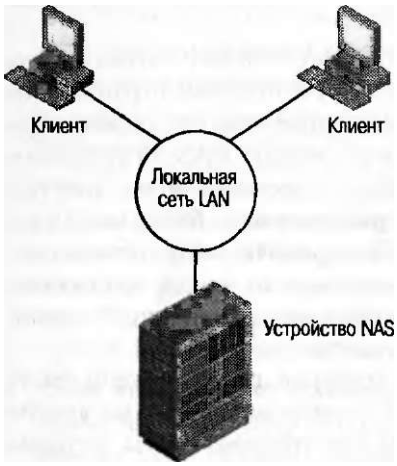


Рис. 2-2. Локальная сеть LAN с устройством NAS

Управление NAS Устройства NAS имеют собственные средства управления, которые в основном доступны через сеть.

Сети хранения данных

Сеть хранения данных (Storage Area Network, SAN) — это высокопроизводительная сеть, выделенная для передачи блочных данных между серверами и подсистемами хранения данных. С точки зрения операционных систем, SAN фигурирует как установленная локально сеть. Наиболее важное отличие SAN от DAS заключается в том, что подключенное в SAN устройство хранения является доступным не только одному, а любому из серверов. (В SAN устройство хранения может быть перемещено с одного сервера на другой, но за пределами конфигурации кластеризованной файловой системы не может быть одновременно доступно более чем для одного сервера.)

К СВЕДЕНИЮ SAN в сравнении с DAS

Хотя скорость передачи данных в системе DAS, как правило, выше, чем в системе SAN, ощутимое расхождение в эксплуатационных характеристиках систем постоянно уменьшается. Несмотря на большую скорость шины, обеспечиваемую DAS, сети SAN, тем не менее, считаются предпочтительными, так как их преимущество, которое заключается в обеспечении одновременного общего доступа серверов к хранилищу данных, компенсирует их недостаток — более низкую скорость доступа.

Сеть SAN состоит из специальных устройств, таких как адаптеры главной шины (Host Bus Adapters, HBA) на хост-серверах, коммутаторы, помогающие распределять трафик системы хранения, дисковые подсистемы хранения данных и библиотеки типов. Такие аппаратные устройства, соединяющие серверы и системы хранения данных в сети SAN, называются фабриками SAN. Все эти устройства связываются по волоконно-оптическому или медному кабелю. После первого подключения к фабрике общедоступный дисковый массив разбивается на виртуальные разделы, называемые логическими номерами устройств (Logical Unit Numbers, LUNs), которые впоследствии становятся локальными дисками для серверов.

Сети SAN спроектированы таким образом, что обеспечивают возможность централизации сетевых ресурсов хранения данных и уменьшения ограничений подключений, характерных для DAS. Например, параллельная архитектура шины SCSI накладывает следующие ограничения на систему DAS: 16 устройств (включая контроллер) на расстоянии не более 25 м. Технология волоконно-оптического канала для SAN позволяет увеличить расстояние до более чем 10 км и обеспечивает подключение к сети фактически неограниченного числа серверов. Указанные преимущества SAN дают возможность отделить хранилище данных от автономных серверов и консолидировать неограниченный массив данных в сети, где этот массив может быть использован совместно.

Сети SAN являются хорошим решением для серверов, где необходим быстрый доступ к очень большому массиву данных (особенно данных на уровне блоков). Такими серверами могут быть серверы электронной почты, серверы резервного копирования, потоковые мультимедийные серверы и серверы баз данных. Использование сетей SAN также предусматривает эффективное дублирование удаленных на большое расстояние данных, что является решением проблемы их аварийного восстановления после отказа системы. На рис. 2-3 показана простая сеть SAN.

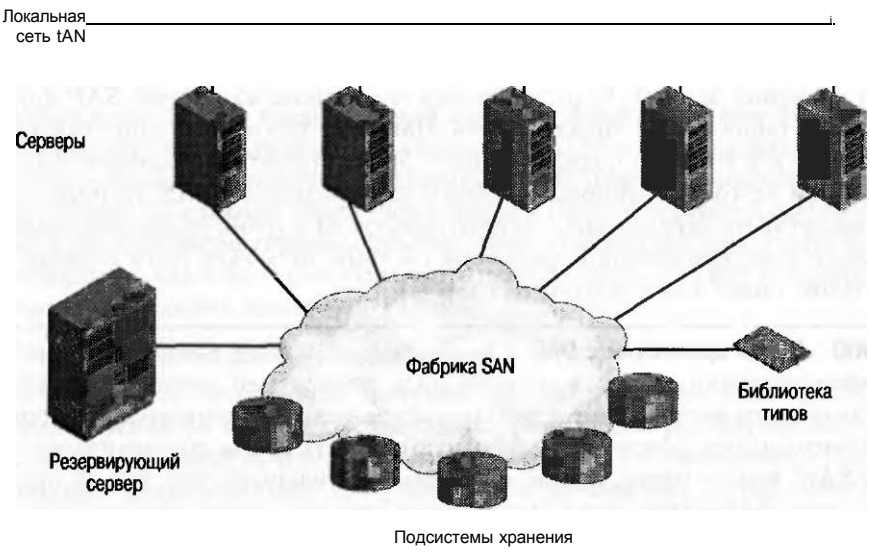


Рис. 2-3. Пример сети хранения данных SAN

Обычно сети SAN встречаются в двух модификациях: FC и iSCSI.

- **Сети SAN на базе технологии FC** Волоконно-оптический канал (Fibre Channel, FC) обеспечивает высокоскоростную передачу блочного ввода-вывода (Input/Output, I/O) на устройства хранения данных. Основанная на последовательной архитектуре SCSI, технология соединения FC является наиболее широко применяемой для сетей SAN. В отличие от устройств с параллельной архитектурой SCSI, FC-устройства не требуют вынесения на общую шину. Вместо этого в технологии FC используются специальные коммутаторы для одновременной передачи информации между множеством серверов и устройствами хранения данных.

  Основным преимуществом FC является то, что данная технология получила широкую реализацию в сетях SAN и, по крайней мере до недавнего времени, обеспечила наилучшую производительность. В числе недостатков технологии FC — высокие затраты на оборудование и сложная настройка. Компонентами сети на основе волоконно-оптического канала являются: адаптеры главной шины (HBAs), кабельная система и коммутаторы. Все эти составляющие, разработанные ведущими поставщиками специально для технологии FC, не всегда совместимы, относительно дороги, и для их установки требуются специальные знания.
- **Сети SAN на базе технологии iSCS** Internet SCSI (iSCSI) является промышленным стандартом, разработанным для обеспечения передачи блоков команд SCSI по сети Ethernet с использованием протокола TCP/IP. Сетевое соединение серверов с устройствами iSCSI осуществляется посредством локально установленной исполнительной программы, которая известна как *инициатор iSCSI* (iSCSI Initiator). Инициатор iSCSI выполняет запросы и получает ответы от *исполнителя iSCSI* (iSCSI Target), который сам по себе может быть конечным узловым устройством сети хранения или устройством-посредником, таким как коммутатор. Для фабрик iSCSI сеть также включает один или несколько серверов Службы имен устройств хранения (Internet Storage Name Service, iSNS), которые подобно серверам DNS в локальной сети обеспечивают открытость и разбивку на зоны ресурсов SAN.
  Основанные на протоколе TCP/IP, сети SAN на базе технологии iSCSI используют преимущества сетевых устройств, которые являются широко доступными и знакомыми пользователям, что в большинстве случаев делает сети SAN на базе технологии iSCSI более простыми и менее дорогими в реализации, чем сети SAN с использованием технологии FC.

Кроме сравнительно низкой стоимости и удобства исполнения существуют и другие преимущества технологии iSCSI.

- **Возможность соединения на больших расстояниях** Организациям, рассредоточенным на больших территориях, может понадобиться последовательное соединение удаленных «островов SAN», чего нельзя обеспечить из-за существующего ограничения связи в пределах 10-километровой зоны для технологии FC. (Существуют новые средства расширения зоны установления связи для сетей на базе технологии FC до нескольких сотен километров, однако эти методы являются сложными и дорогими.) В отличие от FC,

протокол iSCSI позволяет устанавливать соединение между удаленными офисами в SAN с использованием не только общегородских сетей (Metropolitan Area Networks, MANs), но и территориально распределенных сетей (Wide-Area Networks, WANs).

- **Встроенная функция безопасности** Протокол волоконно-оптического канала передачи данных не предусматривает никаких встроенных методов обеспечения безопасности. Вместо этого функция безопасности реализована в первую очередь посредством ограниченного физического доступа в сети SAN. В противоположность технологии FC, введение в эксплуатацию протокола iSCSI корпорацией Microsoft обеспечивает безопасность для устройств, подключенных к сети, с использованием Протокола аутентификации по квитированию вызова (Challenge Handshake Authentication Protocol, CHAP) для аутентификации и Межсетевого протокола Интернет (Internet Protocol Security, IPSec) для кодирования данных. Поскольку указанные выше методы обеспечения безопасности сетевых соединений уже существуют в сетях Windows, они могут быть полностью распространены с локальных сетей на сети SAN.

ПРИМЕЧАНИЕ Фабрика iSCSI SAN
Технология iSCSI SAN может использовать специализированные устройства для фабрики или работать на основе уже существующей в организациях инфраструктуры сетей LAN, MAN или WAN. Для обеспечения безопасности и производительности на базе протокола iSCSI рекомендуется отделить сетевой трафик от трафика хранилища.

Основным недостатком сетей SAN на базе технологии iSCSI, за исключением того, что они используют специализированные (а также дорогие) 10-гигабайтовые кабели и коммутаторы сети Ethernet, является меньшая скорость обмена I/O по сравнению с той, которую может обеспечить SAN на базе технологии FC. Но если вы действительно предпочли использование 10-гигабайтового оборудования для ваших сетей SAN на базе технологии iSCSI использованию расширенного стандарта гигабит Ethernet (Gigabit Ethernet), высокая стоимость такого решения нивелирует преимущество невысоких затрат на организацию сети, предлагаемых технологией iSCSI относительно технологии FC.

СОВЕТ Подготовка к экзамену
Для успешной сдачи экзамена вам необходимо знать значения следующих терминов: LUNs, HBA, iSCSI Initiator (инициатор iSCSI), iSCSI Target (исполнитель iSCSI), SAN fabric (фабрика SAN) и iSNS.

Управление сетями SAN Операционная система Windows Server 2008 содержит службу виртуальных дисков (Virtual Disk Service, VDS), представляющую собой интерфейс для программирования приложений (Application Programming Interface, API). Это дает возможность поставщикам аппаратных средств для сетей SAN на базе технологий FC и iSCSI предоставлять дисковые подсистемы и техническое оснащение для сетей SAN, доступное средствам администрирования в операционной системе Windows. Если аппаратные средства

поставщика включают аппаратные провайдеры VDS, вы можете управлять аппаратными средствами в операционной системе Windows Server 2008, используя такие инструменты, как оснастка Управление дисками (Disk Management), Диспетчер хранилища для сетей SAN (Storage Manager for SANs, SMfS), Обозреватель хранилищ (Storage Explorer), Инициатор iSCSI (iSCSI Initiator), приложение DiskRAID.exe, работающее в режиме командной строки.

- *SMfS* Операционная *система* Windows Server 2008 содержит средство SMfS, которое можно добавить с номощыо мастера добавления компонентов (Add Features Wizard). Вы можете использовать SMfS для управления сетями SAN, резервируя диски, создавая локальные сети LAN и назначая сети LAN различным серверам сети SAN. SMfS-консоль изображена на рис. *2-4.*

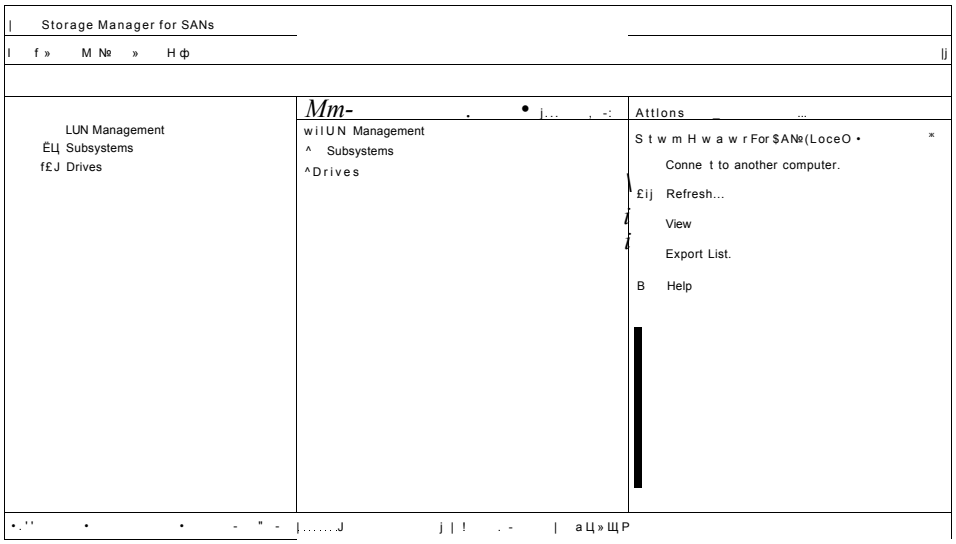


Рис. 2-4. Диспетчер хранилища для сетей SAN

- Обозреватель хранилищ (Storage Explorer) Новый инструмент Windows Server 2008 доступен по умолчанию в группе программ Администрирование (Administrative Tools). Вы можете использовать Обозреватель хранилищ (Storage Explorer) для отображения детализированной информации о серверах, подключенных к сети SAN, а также о компонентах фабрик, таких как HBA, FC-коммутаторы, инициаторы и исполнители iSCSI. Для выполнения административных задач на фабрике iSCSI вы также можете использовать Обозреватель хранилищ (Storage Explorer).
- Инициатор iSCSI Инициатор iSCSI (iSCSI Initiator) доступен по умолчанию в операционной системе Windows Server 2008 в группе программ Администрирование (Administrative Tools). Это средство дает вам возможность настроить безопасность, обнаружение и другие функциональные возможности локальных соединений серверов с исполнителями iSCSI.
- DiskRAID DiskRAID является приложением, работающим в режиме командной строки, которое позволяет вам управлять сетями LAN в аппаратных средствах RAID с поддержкой VDS.

СОВЕТ Подготовка к экзамену

Для успешной сдачи экзамена 70-643 вам необходимо понимать важность VDS и ее связь с описанными выше средствами.

Управление дисками, томами и разделами в операционной системе Windows Server 2008

Основной инструмент, который вы можете использовать для управления дисками, томами и разделами в операционной системе Windows Server 2008, — оснастка Управление дисками (Disk Management). С ее помощью вы можете инициализировать диски, переносить их в режиме онлайн и в автономном режиме, создавать тома на дисках, форматировать тома, изменять стили разделов дисков, расширять и уменьшать емкости томов, создавать наборы отказоустойчивых дисков.

Чтобы открыть окно оснастки Управление дисками (Disk Management), нужно ввести команду *Diskmgmt.exe* в строку Выполнить (Run), в консоли Диспетчер серверов (Server Manager) выбрать под узлом Запоминающие устройства (Storage) элемент Управление дисками (Disk Management) или выбрать узел Управление дисками (Disk Management) в консоли Управление компьютером (Computer Management) (данная консоль доступна из папки Администрирование (Administrative Tools)). Интерфейс оснастки Управление дисками (Disk Management) показан на рис. 2-5.

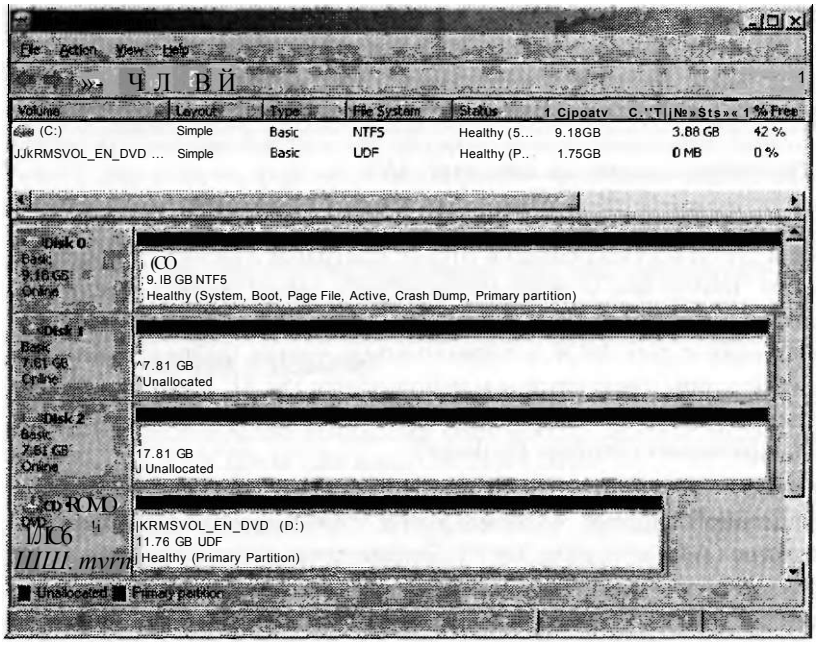


Рис. 2-5. Оснастка Управление дисками (Disk Management) в операционной системе Windows Server 2008

Базовые и динамические диски

Оснастка Управление дисками (Disk Management) служит для управления базовыми и динамическими дисками. По умолчанию все диски являются базовыми. Базовый диск — это физический диск, содержащий основные разделы, дополнительные разделы и логические диски. Количество разделов, которое вы можете создать на базовом диске, зависит от стиля разделов диска. На дисках, использующих стиль разделов главных загрузочных записей (Master Boot Record, MBR), можно создать до четырех основных разделов или до трех основных разделов и один дополнительный раздел на каждый базовый диск. В одном дополнительном разделе вы можете затем создать неограниченное количество логических дисков. На базовых дисках, использующих стиль таблиц разделов GUID (GUID Partition Table, GPT), можно создать до 128 основных разделов. Поскольку GPT-диски не ограничены четырьмя разделами, нет необходимости создавать дополнительные разделы или логические диски. GPT рекомендуется использовать для дисков, объем которых превышает 2 Тбайт, и дисков с 64-битовой системой.

ПРИМЕЧАНИЕ Стили разделов
Стили разделов относятся к наиболее простой структуре дисков, распознаваемой операционной системой. Стили разделов не имеют отношения к форматам файлов NTFS или FAT32 в разделах. Базовые и динамические диски могут иметь любой из перечисленных стилей разделов.

Динамические диски обеспечивают расширенные возможности, не поддерживаемые базовыми дисками; к ним относятся: возможность создания неограниченного числа томов, томов, охватывающих несколько дисков (составные тома и тома с чередованием) и отказоустойчивых томов (зеркальные тома и тома уровня RAID-5). Существует пять типов динамических томов: простые, составные, чередующиеся, зеркальные и тома уровня RAID-5.

В предыдущих версиях операционной системы Windows нужно было преобразовать базовые диски в динамические, и лишь после этого можно было создать на них любые из указанных типов томов. При использовании оснастки Управление дисками (Disk Management) в операционной системе Windows Server 2008 базовые диски автоматически преобразуются в динамические в процессе создания любого из упомянутых выше типов томов. В результате этого с административной точки зрения вопрос о том, является диск базовым или динамическим, стал менее важным. Несмотря на это усовершенствование, для конфигураций с загрузкой одной из двух операционных систем все еще важно знать, что многие ранние версии операционной системы Windows (в том числе Windows NT, Windows 98 и Windows ME) не поддерживают динамические диски. Еще один существенный факт относительно конфигураций с загрузкой одной из двух операционных систем: динамические диски совместимы только с операционными системами семейства Windows.

СОВЕТ Подготовка к экзамену
Даже несмотря на то, что' при необходимости базовые диски автоматически преобразуются в динамические, вам для успешной сдачи экзамена 70-643 следует знать, для каких типов томов требуются динамические диски.

Создание томов

Оснастку Управление дисками (Disk Management) и служебную программу в режиме командной строки Diskpart можно использовать для создания следующих типов томов в операционной системе Windows Server 2008.

- Простые, или базовые, тома Простые тома — это базовые диски, которые не являются отказоустойчивыми. Простой том может состоять из о/хной области на диске или нескольких объединенных вместе областей.
  Для создания простого тома с помощью оснастки Управление дисками (Disk Management) щелкните правой кнопкой мыши в области нераспределенного пространства диска, а затем щелкните Создать простой том (New Simple Volume), как показано на рис. 2-6. (Эта операция аналогична при создании тома и на базовом, и на динамическом диске, даже при создании тома на базовом диске новый том технически называется разделом или базовым томом.) Возможно, сначала вам нужно щелкнуть правой кнопкой мыши на диске и сделать раздел активным (Online).

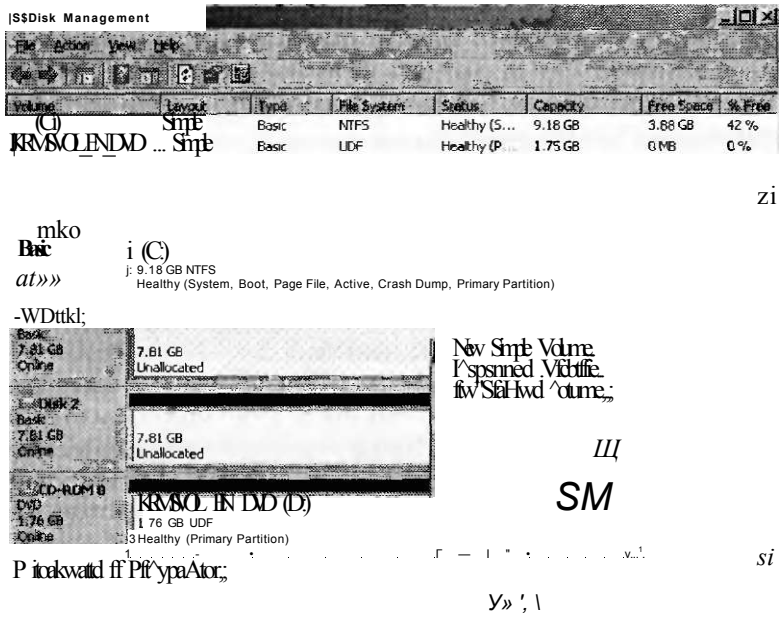


Рис. 2-6. Создание простого тома

Для создания простого тома с помощью утилиты Diskpart выберите диск, используя эту программу, а затем для динамического диска введите команду *create volume simple.* Для создания нового тома (раздела) на базовом диске введите команду *create partition.* Если вы хотели бы получить дополнительную информацию относительно синтаксиса данных команд, введите *create volume?* или *create partition?,*

u Составные тома Составной том — это динамический том, состоящий из дискового пространства более чем одного физического диска. Если простой

том не является системным или загрузочным, вы можете расширить его за счет присоединения дискового пространства других дисков, получив в результате составной том, или создать новый составной том, используя нераспределенное пространство более чем одного диска.

Для создания нового составного тома в оснастке Управление дисками (Disk Management) щелкните правой кнопкой мыши в области нераспределенного пространства одного из дисков — того, на котором вы хотите создать составной том, а затем щелкните Создать составной том (New Spanned Volume). В результате будет запущен Мастер создания составных томов (New Spanned Volume Wizard), с помощью которого к составному тому можно добавить свободное пространство из доступных дисков.

На рис. 2-7 изображен составной том, которому назначена буква диска E. Обратите внимание на то, как диск использует пространство дисков Disk 1 и Disk 2, являясь при этом единственным томом с емкостью 7,32 Гбайт.

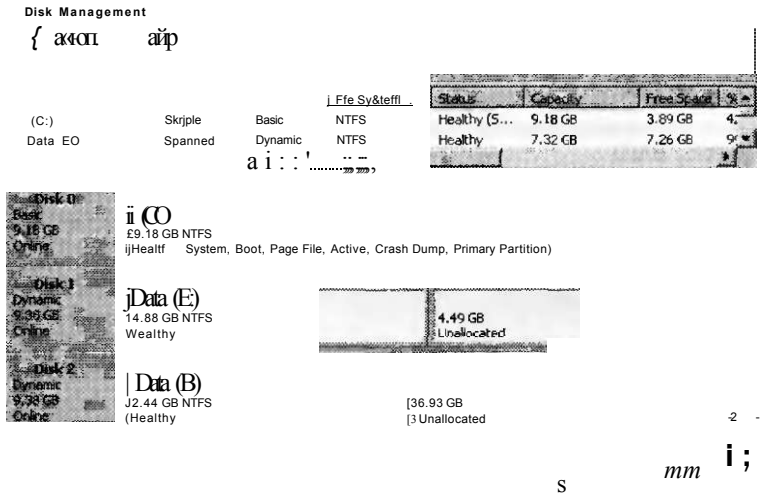


Рис. 2-7. Составной том в оснастке Управление дисками (Disk Management)

Чередующиеся тома Чередующийся том, известный также как RAID O, представляет собой динамический том, в котором данные разбиваются на полосы и хранятся на двух или большем количестве физических дисков. Чередующиеся тома обеспечивают наилучшую производительность среди всех доступных в операционной системе Windows томов, однако они не являются отказоустойчивыми. Если появился сбой на диске, содержащем чередующийся том, то данные всего тома будут утеряны. На рис. 2-8 показано, каким образом данные чередующегося тома записаны в набор дисков.

Когда следует использовать чередующиеся тома Чередующийся том является лучшим решением проблемы хранения временных данных, для которых не требуется отказоустойчивость, но необходима высокая производительность. Примерами таких временных данных являются файлы подкачки и папки каталога Temp. Для создания нового чередующегося тома щелкните

правой кнопкой мыши в области нераспределенного пространства на диске, а затем щелкните Создать чередующийся том (New Striped Volume).

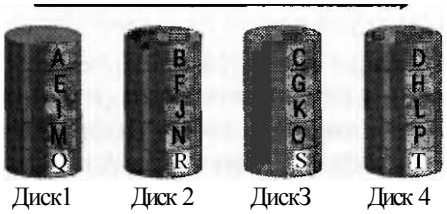


Рис. 2-8. Последовательная запись данных на диски чередующегося набора по технологии RAID 0

Чередующийся том в оснастке Управление дисками (Disk Management) показан на рис. 2-9. Обратите внимание на то, каким образом том использует 1,46 Гбайт свободного пространства обоих дисков, Disk 1 и Disk 2, являясь при этом единственным томом E емкостью 2,93 Гбайт, а также на то, как сам этот том используется для хранения временных данных (Файл подкачки (Page File)).

К СВЕДЕНИЮ Диски RAID

Для создания чередующегося тома, как и для всех решений RAID, используются диски одинакового объема.

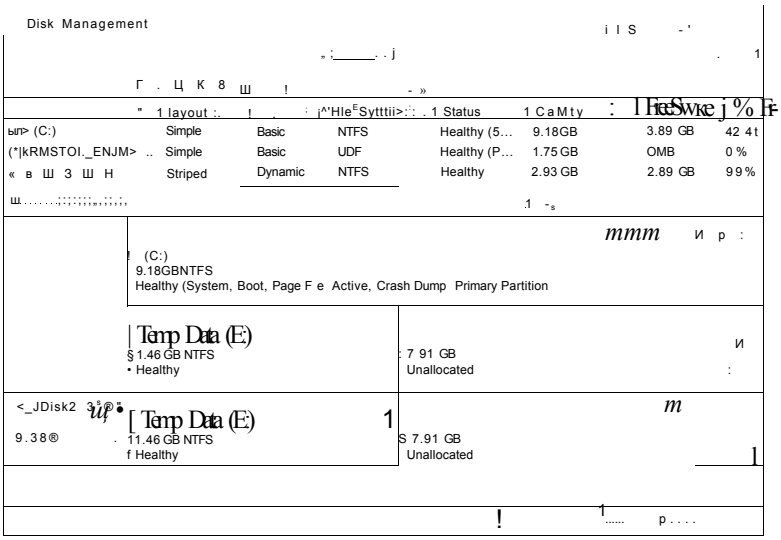


Рис. 2-9. RAID 0, или чередующийся том, в оснастке Управление дисками (Disk Management)

- Зеркальные тома Зеркальный том, известный также как RAID 1, является отказоустойчивым томом, который обеспечивает избыточность данных путем использования двух копий, или зеркал, одного и того же тома. Все данные,

отображенные в зеркальном томе, записаны в двух томах, расположенных на отдельных физических дисках. В случае отказа одного из физических дисков его данные становятся недоступными, но система продолжает функционировать, используя неповрежденный диск.

На рис. 2-10 показано, каким образом в зеркальном томе хранятся данные. Поскольку данные дублируются, они не будут утеряны в случае отказа любого из дисков.

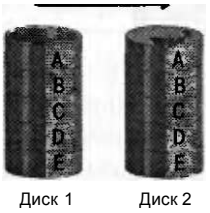


Рис. 2-10. **Создание копии всех данных на втором диске с помощью технологии RAID 1, или зеркального тома**

ПРИМЕЧАНИЕ Тройное и множественное зеркалирование
Хотя зеркальные тома, настроенные в операционной системе Windows Server 2008, предполагают использование двух дисков, существует возможность создать зеркала на трех и более дисках. В конфигурации с тремя зеркалами, например, содержимое одного диска дублируется на два дополнительных диска. Множественные зеркала снижают производительность при выполнении записи, однако повышают отказоустойчивость. Множественное зеркалирование является хорошим решением для критически важных данных.

Зеркальные тома, будучи отказоустойчивыми, имеют преимущества и недостатки. Одним из преимуществ зеркального тома является обеспечение очень высокой производительности при чтении данных, равно как и довольно высокой производительности при записи данных. Кроме того, для создания зеркальных томов достаточно наличия только двух дисков, и практически любой том, включая системные и загрузочные тома, может быть зеркалирован. Недостаток зеркальных томов заключается в том, что для обеспечения отказоустойчивости требуется зарезервировать 50 % общей емкости дискового пространства. Более того, когда необходимо обеспечить технологию хранения данных с отказоустойчивостью, зеркало будет полезным выбором, если: у вас имеется только два диска; вам нужна высокая производительность чтения и записи; требуется повышение отказоустойчивости для системного тома, загрузочного тома или других критически важных данных.

Для создания зеркального тома можно добавить зеркало к существующему тому или создать новый зеркальный том. Для добавления зеркала к существующему тому в оснастке Управление дисками (Disk Management) щелкните правой кнопкой мыши нужный том, а затем щелкните Добавить зеркало (Add Mirror), как показано на рис. 2-11.

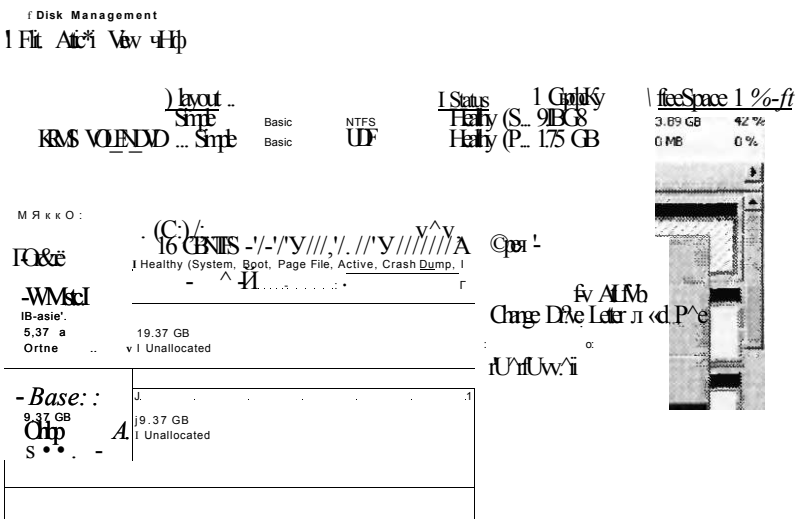


Рис. 2-11. Добавление зеркала к системному разделу

Для создания нового зеркального тома в оснастке Управление дисками (Disk Management) щелкните правой кнопкой мыши в области нераспределенного пространства диска, а затем щелкните Создать зеркальный том (New Mirrored Volume). Новый зеркальный том изображен на рис. 2-12. Обратите внимание на то, каким образом диск использует 5,86 Гбайт пространства обоих дисков, Disk 1 и Disk 2, являясь при этом единственным томом E с емкостью 5,86 Гбайт.

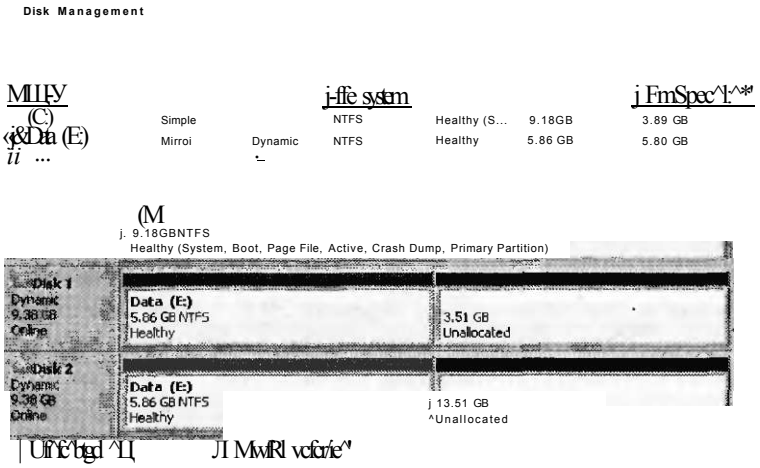


Рис. 2-12. RAID 1, или зеркальный том

Тома RAID-5 RAID-5 — это отказоустойчивый том, объединяющий области свободного пространства минимум трех физических жестких дисков в один логический том. Тома RAID-5 предполагают чередование данных с ин-

формацией о контрольной сумме (четности или нечетности) и равномерно распределены по всем дискам набора. При отказе одного из дисков операционная система Windows Server 2008 использует информацию о четности для восстановления данных вышедшего из строя диска. Тома RAID-5 допускают потерю данных только на одном диске из набора.

СОВЕТ Подготовка к экзамену
На экзамене 70-643 том RAID-5, возможно, будет называться чередующийся том с контролем четности.

На рис. 2-13 показан том RAID-5, состоящий из четырех дисков. Данные, записанные в этот том, равномерно распределены в виде полос на всех дисках слева направо. Для каждой полосы данных из дискового набора один диск используется для хранения контрольной информации о четности или нечетности для остальных данных полосы. В упрощенном примере, показанном на рис. 2-13, контрольной сумме присваивается значение 1, если сумма значений в полосе нечетная, и 0 — если сумма оставшихся значений четная. В случае отказа какого-либо одного (и только одного) диска операционная система Windows может восстановить все содержимое вышедшего из строя диска, используя информацию о четности вместе с оставшимися данными. Данные вышедшего из строя диска могут быть воссозданы в реальном времени по требованию пользователей. Информация о четности также может быть восстановлена на новом диске после замены отказавшего диска.

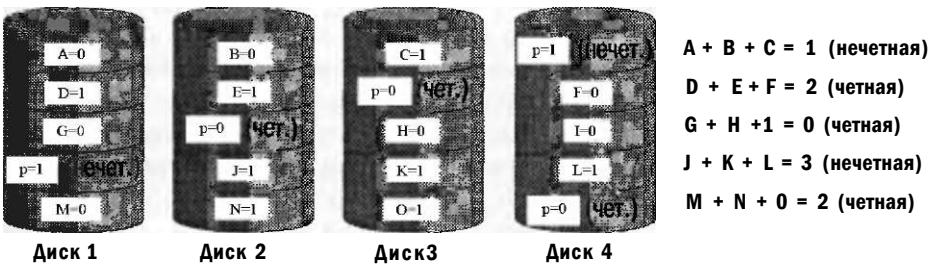


Рис. 2-13. Вычисление контрольной суммы (четности или нечетности) тома RAID-5 для обеспечения отказоустойчивости

Объем пространства, приблизительно эквивалентный размеру одного диска, всегда используется для обеспечения отказоустойчивости в томе RAID-5. Например, если вы создадите том RAID-5 из четырех дисков размером 120 Гбайт каждый, то общая емкость доступного хранилища в этом томе составит 360 Гбайт.

Когда следует применять технологию RAID-5? RAID-5 характеризуется очень высокой производительностью при выполнении операций чтения, относительно низкой производительностью при выполнении операций записи и оптимальным использованием пространства хранения для обеспечения отказоустойчивости данных. Следовательно, стоит подумать о применении конфигурации RAID-5, если высокая производительность записи не является приоритетной или вам необходима отказоустойчивая технология

хранения данных, обеспечивающая наилучшее использование доступного пространства хранения. Заметьте также, что системному или загрузочному разделу нельзя назначить том RAID-5, созданный в операционной системе Windows Server 2008.

ПРИМЕЧАНИЕ Программная и аппаратная реализация RAID

Том RAID-5, созданный с помощью оснастки Управление дисками (Disk Management), является примером программного RAID, так как он создан операционной системой. Несмотря на это, некоторые поставщики продают дисковые модули, включающие собственные встроенные программы установки RAID. Если вы настраиваете RAID-5 с собственным программным обеспечением, операционная система Windows Server 2008 видит запоминающее устройство как единичный локальный том. Подобная конфигурация RAID, которая является прозрачной для операционной системы, известна как аппаратная RAID. Хотя программная реализация RAID обеспечивает более низкую производительность, чем аппаратная, программная RAID является недорогой и легкой в настройке, так как, кроме необходимости наличия нескольких дисков, отсутствуют специальные требования к аппаратным средствам. Если фактор стоимости является более важным, чем производительность, программная RAID будет подходящим решением.

Реальный мир

Дж. К. Макин

Хотя операционная система Windows не позволяет вам создать уровни RAID, известные как RAID 0+1 и RAID 1+0, они становятся все более распространенными в реальном мире. RAID 0+1 (или 01) является *зеркалом сегментов чередования,* преимущественно двойной копией чередующегося тома. Этот тип RAID построен путем создания массивов RAID 0 с последующим их зеркалированием. RAID 1+0 (или 10), наоборот, представляет собой *чередование зеркал,* в котором данные чередуются в нескольких зеркальных наборах. Для конструирования данного типа RAID сначала необходимо создать набор зеркальных массивов, а затем построить массив RAID 0 из этого набора.

В вышеописанных технологиях 50 % дискового пространства отводится для обеспечения отказоустойчивости, и в обоих случаях достигается отличная производительность операций чтения и записи. RAID 1+0, однако, обеспечивает наибольшую вероятность восстановления данных в случае отказа более чем одного диска.

Заметьте также, что условные обозначения двух указанных уровней RAID не являются утвердившимися. Некоторые компании (включая корпорацию Microsoft) Moiyr обобщенно называть обе технологии RAID 01 и 10 одним термином 0+1. Если вам нужно разъяснить ваши требования к поставщикам, лучше употребить термины зеркало сегментов чередования или чередование зеркал.

Для создания тома RAID-5 в оснастке Управление дисками (Disk Management) щелкните правой кнопкой мыши в области нераспределенного пространства одного из динамических дисков — того, на котором вы хотите

создать том RAID-5, а затем щелкните Создать том RAID-5 (New RAID-5 Volume). После этого следуйте инструкциям мастера создания томов RAID-5 (New RAID-5 Volume Wizard). Для создания тома RAID-5 с помощью программы Diskpart воспользуйтесь командой create volume raid. Чтобы получить дополнительную информацию относительно синтаксиса данной команды, введите help create volume raid.

СОВЕТ Подготовка к экзамену
Для успешной сдачи экзамена 70-643 убедитесь в том, что вы разбираетесь в уровнях RAID и знаете различные типы томов.

Расширение тома

Емкость существующих простых и составных томов можно увеличить, расширяя их на нераспределенное пространство того же или другого диска. Том можно расширить лишь при условии, что он отформатирован под файловую систему NTFS либо вообще неформатированный. Для расширения тома в оснастке Управление дисками (Disk Management) щелкните правой кнопкой мыши том, который вы хотите расширить — простой или составной, а затем щелкните Расширить том (Extend Volume).

ПРИМЕЧАНИЕ Расширение загрузочных и системных томов
Вы не можете расширить загрузочный или системный том на другой диск.

Сжатие тома

Вы можете уменьшить пространство, используемое простыми или составными томами, посредством их сжатия на смежное свободное пространство в конце тома. Например, если вам необходимо увеличить размер нераспределенного пространства на диске для освобождения места под новый раздел или том, можно попытаться сжать существующие тома на диске. Когда вы сжимаете раздел, все обычные файлы автоматически перемещаются на диске для создания нового нераспределенного пространства. Нет необходимости переформатировать диск для сжатия раздела.

Размер пространства, получаемого сжатием тома, может значительно варьироваться. В общем случае, чем больше процент неиспользованного пространства тома и чем меньше неисправных кластеров, тем больше вы сможете сжать том. Тем не менее, если количество неисправных кластеров, выявленных динамическим переназначением плохих кластеров, слишком велико, то вы вообще не сможете сжать том. В подобном случае лучше переместить данные и заменить диск.

ВНИМАНИЕ! Не сжимайте неформатированные разделы, содержащие данные
Если раздел не отформатирован под файловую систему, но все еще содержит данные (например, файл базы данных), сжатие раздела может фактически привести к уничтожению данных.

Для сжатия тома в оснастке Управление дисками (Disk Management) щелкните правой кнопкой мыши том, который вы хотите сжать — простой или составной, а затем щелкните Сжать том (Shrink Volume), как показано на рис. 2-14.

СОВЕТ Подготовка к экзамену

Сжатие является новым средством в системе Windows Server 2008. Будьте готовы увидеть вопросы по этой теме на экзамене 70-643.

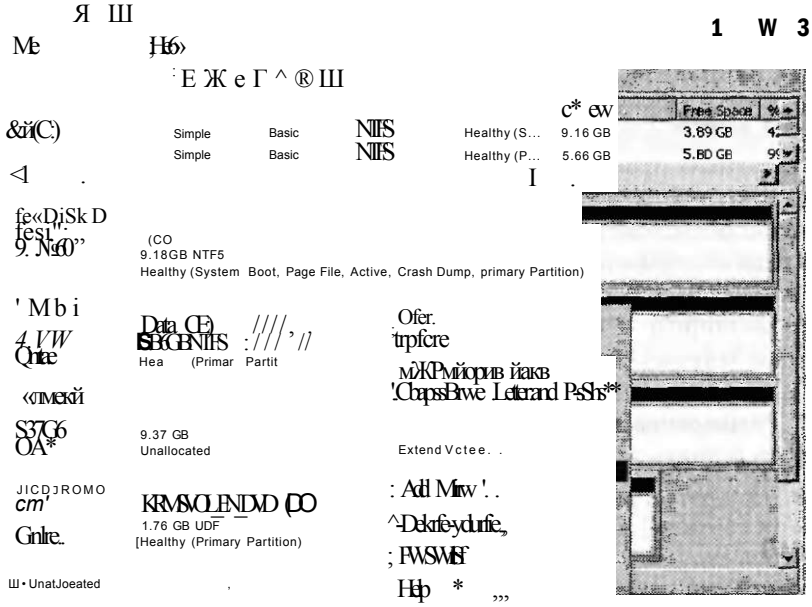


Рис. 2-14. Сжатие тома в оснастке Управление дисками (Disk Management)

Настройка точки монтирования

Точка монтирования — это папка тома, которая выполняет функцию указателя на корневой каталог другого тома. Например, если вам необходимо создать дополнительное свободное пространство для системного или загрузочного диска, можно создать новый том на другом диске и затем смонтировать этот том к папку на системном томе.

Такая конфигурация изображена на рис. 2-15. В данной постановке задачи емкость исходного диска С равняется 9,18 Гбайт. Монтируя том емкостью 3,51 Гбайт к папке MountedVolume на диске С, можно получить доступ к дополнительному дисковому пространству через диск С, даже если вы не изменили емкость диска.

Вы можете создать точку монтирования в оснастке Управление дисками (Disk Management),воздав новый том с последующим выбором параметра монтирования тома к пустой папке NTFS (рис. 2-16).

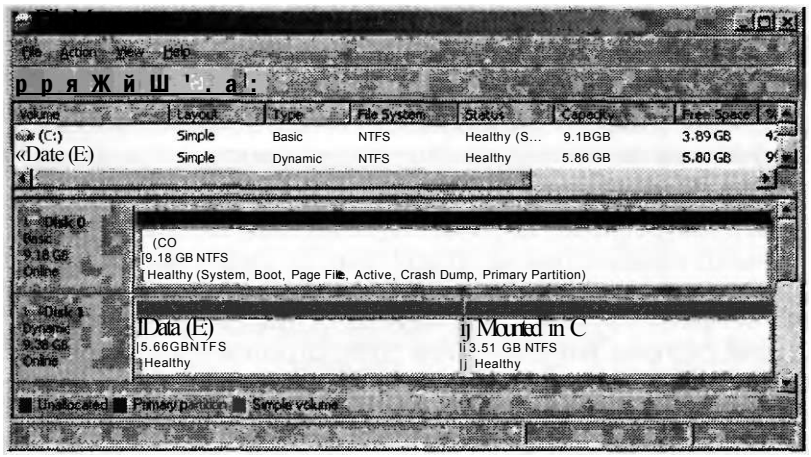


Рис. 2-15. Новый том, смонтированный к системному тому

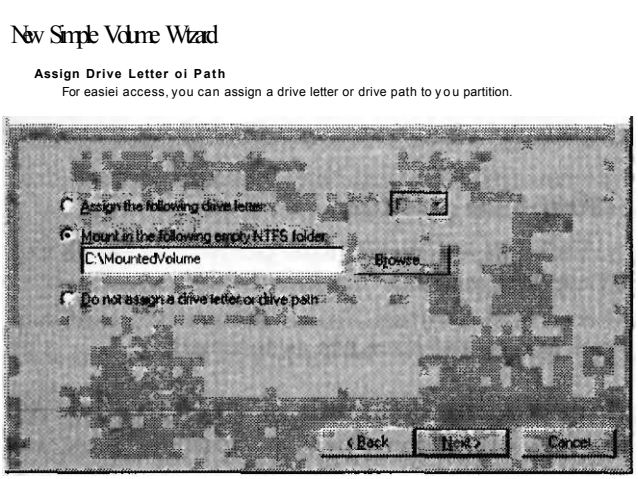


Рис. 2-16. Монтирование нового тома к пустой NTFS-папке

К СВЕДЕНИЮ Расширение системного или загрузочного раздела
Поскольку вы не можете расширить системный том на другой диск, создание точки монтирования — единственный способ получить дополнительное свободное пространство для системного тома без замены аппаратных средств.

Можно также создать точку монтирования для существующего тома, щелкнув правой кнопкой мыши том и выбрав Изменить букву диска и путь к диску (Change Drive Letter And Paths). В одноименном окне щелкните Изменить (Change), а затем выберите параметр монтирования тома к пустой NTFS-папке.

СОВЕТ Подготовка к экзамену
Для успешной сдачи экзамена 70-643 вам необходимо понимать, что такое точки монтирования.

Проверьте себя

1. Можно ли расширить зеркальный том?
2. Верно ли утверждение, что вы не можете использовать аппаратный том RAID-5 в качестве системного или загрузочного тома в операционной системе Windows Server 2008.

Ответы

1. Нет.
2. Не верно. Аппаратная реализация тома RAID-5 будет прозрачной для операционной системы Windows Server 2008. Ограничение для томов RAID-5 относится к тому, что вы можете настроить в операционной системе Windows. Вы не можете добавить системный или загрузочный раздел к программной реализации RAID-5 тома и не можете установить операционную систему на том RAID-5, который вы создаете в операционной системе Windows. (Обратите внимание: хотя операционную систему можно установить на аппаратный том RAID-5, делать это не рекомендуется из-за низкой производительности записи, характерной для RAID-5.)

Практикум. Работа с наборами дисков

Выполняя это практическое задание, вы создадите тома различных типов в оснастке Управление дисками (Disk Mangement).

ВАЖНО! Какое количество дисков вам потребуется для выполнения этих упражнений?

Для выполнения упражнений 1-3 необходимо, чтобы на компьютере Server2 был один неразделенный диск с емкостью не меньшей, чем емкость диска 0, на котором установлена операционная система. Для упражнений 4-6 кроме диска Disk 0 нужны еще два пустых диска (Disk 1 и Disk 2). Обратите внимание: вы без труда сможете создать новые диски на виртуальной машине Virtual PC или сервере.

Упражнение 1. Работа с дисками и простыми томами

В данном упражнении, которое выполняется на компьютере Server2, вы создадите простые тома на диске Disk 1: сначала — во время переключения между динамическим и базовым дисками, а затем — между дисками MBR и GPT.

1. Зарегистрируйтесь в домене Contoco.com с компьютера Server2 как администратор домена.
2. В окне Выполнить (Run) введите команду *diskmgmt.msc,* а затем нажмите клавишу Ввод (Enter).
3. В оснастке Управление дисками (Disk Mangement) удостоверьтесь, что в верхней области окна отображен только том C. Создайте резервную копию данных при необходимости, а затем удалите все другие тома.

В нижней области окна оснастки Управление дисками (Disk Mangement) должны быть отображены как минимум два диска: Disk 0, Disk 1 и (необязательно) Disk 2.

4. Щелкните правой кнопкой мыши в области нераспределенного пространства на диске 1, а затем щелкните Создать простой том (New Simple Volume). Откроется Мастер настройки простых томов (New Simple Volume Wizard).
5. На странице Добро пожаловать в мастер настройки простых томов (Welcome To The New Simple Volume Wizard) щелкните кнопу Далее (Next).
6. На странице Указание размера тома (Specify Volume Size) прочитайте весь текст, а затем щелкните кнопку Далее (Next).
7. Прочтите текст на странице Назначение буквы диска или пути к диску (Assign Drive Letter Or Path) и щелкните кнопку Далее (Next).
8. Ознакомьтесь с текстом, представленным на странице Форматирование раздела (Format Partition), выберите параметр Быстрое форматирование (Perform A Quick Format) и щелкните кнопку Далее (Next).
9. На странице мастера Завершение настройки простого тома (Completing The New Simple Volume Wizard) шелкните кнопку Готово (Finish).

   После завершения процесса создания и форматирования новый том появится в оснастке Управление дисками (Disk Mangement).
10. В нижней области окна оснастки Управление дисками (Disk Mangement) щелкните правой кнопкой мыши Disk 1, а затем щелкните Преобразовать в динамический диск (Convert To Dynamic Disk).
11. Перейдя в окно Преобразование в динамические диски (Convert To Dynamic Disk), удостоверьтесь, что выделен Disk 1, и щелкните кнопку ОК.
12. В окне Диски для преобразования (Disks To Convert) щелкните Преобразовать (Convert).
13. Ознакомьтесь с текстом, представленным в окне оснастки Управление дисками (Disk Mangement), после чего щелкните кнопку Да (Yes).

    Через некоторое время новый том поменяет цвет — синий на зеленый.
14. Щелкните правой кнопкой мыши Disk 1, а затем ответьте на следующие вопросы.

    Можете ли вы преобразовать Disk 1 снова в базовый диск?

    Ответ: Нет, поскольку этот параметр недоступен для выбора.

    Можете ли вы преобразовать Disk 1 в диск со стилем разделов GPT?

    Ответ: Нет, так как диск содержит разделы, и этот параметр недоступен.
15. Щелкните правой кнопкой мыши новый том, который вы создали на диске Disk 1, а затем щелкните Удалить том (Delete Volume). Щелкните кнопку Да (Yes) для подтверждения операции.
16. После того как том будет удален, ответьте на следующий вопрос:

    Disk 1 отображен в списке как Базовый (Basic) или как Динамический (Dinamic) диск?

    Ответ: Как базовый. Диски, не содержащие томов, по умолчанию являются базовыми.

17. Щелкните правой кнопкой мыши Disk 1 и выберите параметр для преобразования Disk 1 в динамический диск. Затем, после завершения процедуры преобразования, щелкните правой кнопкой мыши Disk 1 и опять преобразуйте его в базовый диск.

    Обратите внимание: когда диск не содержит томов, вы свободно можете преобразовать базовый диск в динамический, и наоборот. Однако если диск содержит тома, можно преобразовать только базовый диск в динамический.
18. Щелкните правой кнопкой мыши Disk 1, а затем щелкните Преобразовать в диск GPT (Convert To GPT Disk).
19. Через некоторое время снова щелкните правой кнопкой мыши Disk 1, а затем щелкните Преобразовать в диск MBR (Convert To MBR Disk). Заметьте, что когда диск не содержит томов, вы свободно можете преобразовывать диск со стилем разделов MBR в диск со стилем разделов GPT, и наоборот.
20. Оставьте открытой оснастку Управление дисками (Disk Management) и переходите к выполнению упражнения 2.

Упражнение 2. Создание точек монтирования

В этом упражнении, которое выполняется на компьютере Server2, вы смонтируете два тома в качестве папок к тому C.

1. Пока вы еще зарегистрированы в домене Contoco.com с компьютера Server2 как администратор домена, создайте на диске C две новые папки с именами Mount Vol 1 и Mount Vol2 соответственно.
2. В оснастке Управление дисками (Disk Management) щелкните правой кнопкой мыши в области нераспределенного пространства диск Disk 1, а затем щелкните Создать простой том (New Simple Volume).
3. На странице Добро пожаловать в мастер настройки простых томов (Welcome To The New Simple Volume Wizard) щелкните кнопку Далее (Next).
4. Когда перейдете на страницу Указание размера тома (Specify Volume Size), в поле Размер простого тома (Мбайт) (Simple Volume Size In MB) введите значение, соответствующее приблизительно половине объема свободного пространства. Например, если доступно 10 ООО Мбайт свободного пространства, введите 5 *ООО,* а затем щелкните кнопку Далее (Next).
5. На странице Назначение буквы диска или пути к диску (Assign Drive Letter Or Path) выберите Монтировать том как пустую NTFS-папку (Mount In The Following Empty NTFS Folder). Затем в соответствующее поле введите C:\ *MountVoll* (или найдите данную папку с помощью кнопки Обзор (Browse)) и щелкните кнопку Далее (Next).
6. На странице Форматирование раздела (Format Partition) в поле Метка тома (Volume Lable) вместо текста «Новый том» введите *Mounted in C.*
7. На странице Форматирование раздела (Format Partition) выберите Быстрое форматирование (Perform A Quick Format), а затем щелкните кнопку Далее (Next).

8. Перейдя на страницу мастера Завершение настройки простого тома (Completing The New Simple Volume Wizard), щелкните кнопку Готово (Finish).

   Через некоторое время новый том появится в оснастке Управление дисками (Disk Management). Обратите внимание на то, что тому назначена не буква диска, а метка Mounted in C.

9. В меню Пуск (Start) выберите Компьютер (Computer).

   В окне Компьютер (Computer) будет отображен только диск C. У вас нет прямого доступа к новому диску, который только что создан.

10. Откройте диск C.

    На диске C папка MountVol1 помечена специальной меткой. Это связано с большим размером, даже несмотря на то, что том является пустым.

11. Откройте окно свойств папки MountVoll.

    В окне Свойства MountVoll (MountVoll Properties) тип папки обозначен как Смонтированный том (Mounted Volume).

12. В окне Свойства MountVoll (MountVoll Properties) щелкните кнопку Свойства (Properties).

    Откроется окно Свойства Mounted In C (C:\ MountVoll) (Mounted In C (C:\ MountVoll) Properties). В этом окне будет отображена та же информация, которую можно найти в окне свойств тома.

13. Закройте окно Свойства Mounted In C (C:\ MountVoll) (Mounted In C(C:\ MountVoll) Properties), щелкнув кнопку OK, после чего щелкните кнопку OK в окне Свойства MountVoll (MountVoll Properties).

14. В оснастке Управление дисками (Disk Management) создайте новый простой том на диске Disk 1, используя процедуру, описанную в упражнении 1. Для нового тома используйте все оставшееся пространство на диске Disk 1 и не выбирайте параметр монтирования тома как NTFS-папки. Введите имя тома *Mounted in C (2) и* выберите параметр быстрого форматирования.

    После завершения процесса создания том появится в оснастке Управление дисками (Disk Management). Обратите внимание на то, что тому назначена буква диска E.

15. В оснастке Управление дисками (Disk Management) щелкните правой кнопкой мыши том Mounted in C (2), а затем щелкните Изменить букву диска и путь к диску (Change Drive Letter And Paths).

16. В окне Изменение буквы диска и пути к диску (Change Drive Letter And Paths) щелкните кнопку Удалить (Remove), а затем щелкните кнопку Да (Yes) для подтверждения операции.

    Вы можете монтировать существующий том, только предварительно удалив назначенную ему букву.

17. В оснастке Управление дисками (Disk Management) снова щелкните правой кнопкой мыши том Mounted in C (2) и еще раз щелкните Изменить букву диска и путь к диску (Change Drive Letter And Paths).

18. В открывшемся окне Изменение буквы диска и пути к диску (Change Drive Letter And Paths) щелкните кнопку Добавить (Add).
19. В окне Добавление буквы диска и пути к диску (Add Drive Letter And Paths) щелкните Монтировать том как пустую NTFS-папку (Mount In The Following Empty NTFS Folder), затем в соответствующее поле введите *C:\MountVol2,* или найдите данную папку с помощью кнопки Обзор (Browse).
20. В окне Добавление буквы диска и пути к диску (Add Drive Letter And Paths) щелкните кнопку ОК.
21. Щелкните Пуск (Start), затем щелкните Компьютер (Computer), дабы убедиться в том, что том Mounted in C (2) настроен в качестве точки монтирования к папке MountVol2 на диске C.
22. В оснастке Управление дисками (Disk Management) удалите оба тома, Mounted in C и Mounted in C (2). Удостоверьтесь в том, что на диске Disk 1 осталось только нераспределенное пространство.
23. Закройте все окна, за исключением окна оснастки Управление дисками (Disk Management), и переходите к выполнению упражнения 3.

Упражнение 3. Добавление зеркального тома и разделение зеркального тома

В этом упражнении, которое выполняется на компьютере Server2, вы будете использовать Disk 1 для добавления зеркала к тому C.

1. Пока вы еще зарегистрированы в домене Contoco.com с компьютера Server2 как администратор домена, в оснастке Управление дисками (Disk Management) щелкните правой кнопкой мыши том C (в верхней или нижней области окна) и затем щелкните Добавить зеркало (Add Mirror).
2. В окне Добавление зеркала (Add Mirror) выберите Disk 1 и щелкните Добавить зеркало (Add Mirror).
3. В окне оснастки Управление дисками (Disk Management) прочитайте весь текст, а затем щелкните кнопку Да (Yes).

   Новый том будет создан на диске Disk 1, и после того как Disk 0 и Disk 1 будут преобразованы в динамические диски, новому тому на диске Disk 1 также будет назначена буква диска C.

   В процессе создания зеркала состояние зеркальных томов отображается как Ресинхронизация (Resynching). Длительность ресинхронизации может быть различной в зависимости от объема томов.
4. Через некоторое время после завершения процесса ресинхронизации зеркального тома просмотрите оснастку Управление дисками (Disk Management), обратив внимание на единственный том, расположенный в верхней части окна, и его емкость.
5. На диске Disk 1 щелкните правой кнопкой мыши том C. Используя доступные параметры контекстного меню, ответьте на следующие вопросы:

   Какой параметр контекстного меню следует выбрать, если вы хотите разделить зеркальный том на два отдельных тома?

Ответ: Разделить зеркальный том (Break Mirrored Volume). Вам следует выбрать этот параметр, в случае если один из дисков отказал или поврежден. Какой параметр контекстного меню следует выбрать, если вы хотите сразу удалить зеркальный том на диске Disk 1?

Ответ: Удалить зеркальный том (Remove Mirror).

6. В контекстном меню щелкните Удалить зеркальный том (Remove Mirror).
7. В окне Удаление зеркального тома (Remove Mirror) выберите Disk 1 и щелкните Удалить зеркальный том (Remove Mirror).
8. В окне Управление данными (Data Management) щелкните кнопку Да (Yes) для подтверждения операции.

   В оснастке Управление дисками (Disk Management) Disk 1 снова появится в качестве базового диска с областью нераспределенного пространства.
9. Оставьте открытой оснастку Управление дисками (Disk Management) и перейдите к выполнению упражнения 4.

Упражнение 4. Создание составного тома

В этом упражнении вы создадите составной том на дисках Disk 1 и Disk 2. Обратите внимание: для этого вам потребуется два не разбитых на разделы динамических диска.

1. В оснастке Управление дисками (Disk Management) щелкните правой кнопкой мыши в области нераспределенного пространства на диске Disk 1, а затем щелкните Создать новый составной том (Create New Spanned Volume). Откроется Мастер создания составных томов (New Spanned Volume Wizard).
2. На странице Добро пожаловать в мастер создания составных томов (Welcome To The New Spanned Volume Wizard) щелкните кнопку Далее (Next).
3. На странице Выбор дисков (Select Disks) удостоверьтесь в том, что в области Выбраны (Selected) отображен только Disk 1.
4. В поле Выберите размер выделяемого пространства (Мбайт) (Select The Amount Of Space In MB) введите значение, равное приблизительно половине доступного пространства.

   Например, если в поле по умолчанию указано значение 10000, введите вместо него *5000*.
5. На странице Выбор дисков (Select Disks) выделите Disk 2, отображенный в области Доступны (Available), а затем щелкните кнопку Добавить (Add) для перемещения диска Disk 2 в область Выбраны (Selected).
6. В области Выбраны (Selected) выделите Disk 2, щелкнув его кнопкой мыши.
7. В поле Выберите размер выделяемого пространства (Мбайт) (Select The Amount Of Space In MB) введите значение, равное приблизительно 25 % доступного пространства.

   Например, если в поле по умолчанию указано значение 10000, введите вместо него *2500*.
8. На странице Выбор дисков (Select Disks) щелкните кнопку Далее (Next).

9. На странице Назначить букву диска или путь к диску (Assign Drive Letter Or Path) щелкните кнопку Далее (Next).
10. После того как вы перейдете на страницу Форматирование тома (Format Volume), в поле Метка тома (Volume Label) введите Составной том.
11. На странице Форматирование тома (Format Volume) установите флажок Быстрое форматирование (Perform A Quick Format) и щелкните кнопку Далее (Next).
12. Затем на странице мастера Завершение создания составного тома (Completing The New Spanned Volume Wizard) щелкните кнопку Готово (Finish).
13. После того как на экран будет выведено окно Управление дисками (Disk Management), прочитайте текст и щелкните кнопку Далее (Next).

    По завершении процесса создания и форматирования тома новый составной том будет отображен в оснастке Управление дисками (Disk Management). Disk 1 и Disk 2 будут соединены в новый том.
14. Потратьте некоторое время на просмотр информации, относящейся к новому тому и отображенной в оснастке Управление дисками (Disk Management). Обратите внимание на емкость тома и на то, что ему назначена единственная буква диска.
15. Оставьте оснастку Управление дисками (Disk management) открытой и переходите к выполнению упражнения 5.

Упражнение 5. Создание чередующегося тома

В этом упражнении вы создадите новый чередующийся том на оставшемся пространстве на дисках Disk 1 и Disk 2.

1. Пока вы еще зарегистрированы в домене Contoco.com с компьютера Server2 как администратор домена, в оснастке Управление дисками (Disk Manage^ ment) щелкните правой кнопкой мыши в области нераспределенного пространства диск Disk 1, а затем щелкните Создать чередующийся том (New Striped Volume).

   Откроется Мастер создания чередующихся томов (New Striped Volume Wizard).
2. На странице Добро пожаловать в мастер создания чередующихся томов (Welcome To The New Striped Volume Wizard) щелкните кнопку Далее (Next).
3. На странице Выбор дисков (Select Disks) обратите внимание на то, что в области Выбраны (Selected) отображен только Disk 1.
4. На странице Выбор дисков (Select Disks) выделите Disk 2, отображенный в области Доступны (Available), а затем щелкните кнопку Добавить (Add) для перемещения диска Disk 2 в область Выбраны (Selected).

   Обратите внимание на то, что размер пространства, относящегося к диску Disk 1, равен размеру пространства, относящегося к диску Disk 2. В чередующемся томе все диски должны иметь одинаковый размер.
5. На странице Выбор дисков (Select Disks) щелкните кнопку Далее (Next).

6. На странице Назначить букву диска или путь к диску (Assign Drive Letter Or Path) щелкните кнопку Далее (Next).
7. На странице Форматирование тома (Format Volume) в поле Метка тома (Volume Label) введите текст *Чередующийся том.*
8. На странице Форматирование тома (Format Volume) установите флажок Быстрое форматирование (Perform A Quick Format) и щелкните кнопку Далее (Next).
9. На странице мастера Завершение создания чередующегося тома (Completing The New Striped Volume Wizard) щелкните кнопку Готово (Finish).
10. Потратьте некоторое время на просмотр информации, относящейся к новому тому и отображенной в оснастке Управление дисками (Disk Management). Обратите внимание на емкость тома и на то, что ему назначена единственная буква диска.
11. Оставьте открытой оснастку Управление дисками (Disk Management) и перейдите к выполнению упражнения 6.

Упражнение 6. Сжатие и расширение тома

В этом упражнении вы будете сжимать составной том, созданный в упражнении 5. Затем, после удаления чередующегося тома, который был создан в аналогичном упражнении, вы расширите составной том на свободное пространство диска Disk 1.

1. Пока вы еще зарегистрированы в домене Contoco.com с компьютера Server2 как администратор домена, в оснастке Управление дисками (Disk Management) щелкните правой кнопкой мыши Составной том (Spanned Volume) диск Disk 2, а затем щелкните Сжать том (Shrink Volume).

   Откроется окно Определение пространства сжатия (Querying Shrink Space), а затем появится окно Сжатие [Буква диска] (Shrink [Drive Letter]).
2. В окне Сжатие (Srink) прочитайте весь текст.

   Обратите внимание на то, что в поле Введите размер пространства для сжатия (Мбайт) (Enter The Amount Of Space To Shrink In Mb) по умолчанию предлагается максимальный размер пространства для сжатия диска.
3. Щелкните кнопку Сжать (Shrink) для сжатия тома на максимально допустимое значение.

   Через некоторое время составной том будет отображен с новым, меньшим размером. Теперь том может быть ограничен пространством диска Disk 1 или может выходить за его пределы на Disk 2.
4. В оснастке Управление дисками (Disk Management) щелкните правой кнопкой мыши чередующийся том (не составной том) и щелкните Удалить том (Delete Volume).
5. В окне Удаление чередующегося тома (Delete Striped Volume) прочитайте текст и щелкните кнопку Да (Yes) для подтверждения операции.

   После того как том будет удален, на диске Disk 1 появится новое нераспределенное пространство.

6. Щелкните правой кнопкой мыши составной том на диске Disk 1, а затем щелкните Расширить том (Extend Volume).

   Откроется Мастер расширения томов (Extend Volume Wizard).
7. На странице Добро пожаловать в мастер расширения томов (Welcome To The Extend Volume Wizard) прочитайте текст и щелкните кнопку Далее (Next).
8. На странице Выбор дисков (Select Disk) удостоверьтесь в том, что в области Выбраны (Selected) отображен только Disk 1.
9. На странице Выбор дисков (Select Disk) оставьте указанный по умолчанию (полный) размер пространства для расширения на Disk 1 и щелкните кнопку Далее (Next).
10. На странице мастера Завершение расширения тома (Completing The Extend Volume Wizard) щелкните кнопку Готово (Finish).

    Через некоторое время том будет отображен в оснастке Управление дисками (Disk Management), занимая при этом все пространство на диске Disk 1. Если том занимает пространство только диска Disk 1, он определяется как простой том. Если некоторая часть тома остается на диске Disk 2, то он все еще определяется как составной том.
11. Щелкните правой кнопкой мыши том на диске Disk1, щелкните Удалить том (Delete Volume), а затем щелкните кнопку Да (Yes) для подтверждения операции удаления.

    Через некоторое время в оснастке Управление дисками (Disk Management) Disk 1 и Disk 2 будут отображены в исходном состоянии.
12. Завершите рабочий сеанс на компьютере Server2.

Резюме

- Дисковые запоминающие устройства бывают трех разновидностей: системы хранения данных с прямым подключением к серверу (Direct-Attached Storage, DAS), системы хранения данных, подключенные к сети (Network-Attached Storage, NAS), и сети хранения данных (Storage-Area Networks, SANs). Технологии DAS и SAN обеспечивают доступ к хранилищу данных на блочном уровне, технология NAS обеспечивает доступ на файловом уровне. Сети SAN предоставляют дополнительные преимущества совместно используемых запоминающих устройств, которые можно легко перемещать с сервера на сервер.
- Если дисковые подсистемы хранения данных поставщиков содержат аппаратные провайдеры для службы виртуальных дисков (Virtual Disk service, VDS), вы можете управлять аппаратными средствами в операционной системе Windows Server 2008, используя такие инструменты: оснастка Управление дисками (Disk Management), Диспетчер хранилища для сетей SAN (Storage Manager for SANs, SMfS), Обозреватель хранилищ (Storage Explorer), Инициатор iSCSI (iSCSI Initiator) и приложение DiskRAID.exe, работающее в режиме командной строки.
- Оснастка Управление дисками (Disk Management) является основным инструментом, который вы можете использовать для управления дисками

и томами в операционной системе Windows Server 2008. Оснастка Управление дисками (Disk Management) дает вам возможность создавать простые, составные, чередующиеся, зеркальные тома и тома RAID-5.

- Используя оснастку Управление дисками (Disk Management), вы можете расширить или сжать простой или составной том.
- С использованием оснастки Управление дисками (Disk Management) можно настроить том в качестве точки монтирования к другому тому.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных в ходе занятия 1. Эти вопросы представлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы

Ответы и пояснения к каждому их варианту размещены в разделе «Ответы» в конце книги.

1. В ваши обязанности как сетевого администратора входит управление системой хранения данных. Вам поручили приобрести новую дисковую подсистему хранения данных для принадлежащей компании сети хранения данных (SAN). Вы тестируете различные аппаратные средства и подключаете новую дисковую подсистему к сети. Затем вы принимаете решение зарезервировать новые диски и создать новые номера логических устройств (LUNs) для сервера Serverl. Открыв Диспетчер хранилища для сетей SAN (Storage Manager for SANs), нового оборудования вы там не видите, однако знаете, что его можно подключить, используя программное обеспечение, которое предоставляется поставщиком. Вы хотели бы управлять новой дисковой подсистемой, применяя Диспетчер хранилища для сетей SAN (Storage Manager for SANs). Что для этого нужно сделать?

   А. В оснастке Управление дисками (Disk Management) выбрать параметр Повторить сканирование дисков (Rescan Disks).

   Б. Выбрать дисковую подсистему хранения данных поставщика, которая содержит аппаратные провайдеры для службы виртуальных дисков (Virtfial Disk service, VDS).

   В. На сервере Serverl настроить инициатор iSCSI (iSCSI Initiator) для установки нового оборудования в качестве основной цели.

   Г. С помощью Обозревателя хранилищ (Storage Explorer) настроить сервер Serverl в качестве iSNS-сервера.

2. В ваши обязанности как специалиста службы поддержки информационных технологий входит управление системой хранения данных. Вы проектируете хранилище данных для нового сервера приложений. При использовании временного хранилища данных возникают определенные сложности, поэтому вы хотите зарезервировать для него три диска емкостью 20 Гбайт. В случае если приоритетной является высокая производительность чтения и записи данных и если вы хотите использовать максимально доступный объем

свободного пространства, какой из указанных ниже типов томов необходимо создать?

А. Простой том.

Б. Составной том.

В. Зеркальный том.

Г. Чередующийся том.

Д. Том RAID-5.

Занятие 2. Настройка кластеров серверов

В корпоративных сетях группы независимых серверов часто используются для создания общей системы серверных служб. Например, различные реальные компьютеры могут быть использованы для получения ответов на запросы к общему веб-сайту или серверу баз данных. Хотя данные группы серверов часто подпадают под такое общее понятие, как *кластеры,* кластеры различных типов могут использоваться с разными целями. На этом занятии вы познакомитесь с кластерами серверов с балансировкой нагрузки и высокой доступностью, которые можно настроить в операционной системе Windows Server 2008.

Изучив материал этого занятия, вы сможете:

- Понять особенности циклического распределения DNS.
- Уяснить назначение и особенности кластеров с технологией балансировки сетевой нагрузки.
- Ориентироваться в основных этапах настройки кластера с технологией балансировки сетевой нагрузки.
- Понять основную функцию и особенности отказоустойчивых кластеров.
- Усвоить требования для создания отказоустойчивого кластера.

Расчетная продолжительность занятия составляет 50 мин.

Основные принципы работы кластера серверов

В операционной системе Windows Server 2008 вы можете настроить группы серверов трех типов для обеспечения распределения нагрузки, масштабируемости и высокой доступности. Первая группа, называемая *группой циклического распределения,* представляет собой множество компьютеров, использующих технологию DNS для обеспечения основного распределения нагрузки с минимальными требованиями к конфигурации. Следующая группа, называемая *кластером с балансировкой сетевой нагрузки* (Network Load Balancing, NLB) (известная также как *ферма NLB),* — это группа серверов, используемых не только для распределения нагрузки, но и для увеличения масштабируемости. И последняя группа, называемая *отказоустойчивым кластером,* может быть использована для увеличения уровня доступности приложения или службы в случае отказа сервера.

К СВЕДЕНИЮ Что означает распределение нагрузки

Распределение нагрузки представляет собой механизм распределения входящих запросов на установление соединения с двумя или более серверами в такой форме, которая является прозрачной для пользователей. Распределение нагрузки может осуществляться с помощью аппаратного обеспечения, программного обеспечения или их комбинации.

Циклическое распределение

Циклическое распределение DNS — это простой метод распределения нагрузки в системе серверов. В технологии циклического распределения DNS-сервер настроен более чем с одной записью для преобразования имени другого сервера в IP-адрес. Когда клиенты осуществляют запросы к DNS-серверу на разрешение имени (поиск адреса) другого сервера, отклики DNS-сервера осуществляют циклическое переключение между записями за каждую единицу времени, и каждый успешный клиент направляется на разный адрес и разную машину.

Предположим, что DNS-сервер, аутентичный для DNS домена web.contoso.com, настроен с двумя отдельными записями ресурсов, при этом каждая из них разрешает имя web.contsco.com, направляя на разные серверы, как показано на рис. 2-17. Когда первый клиент (Client 1) запрашивает DNS-сервер разрешить имя web.contoso.com, отклик DNS-сервера направляет клиента к серверу с именем websrvl, который имеет адрес 192.168.3.11. Эта информация связана с первой записью DNS, соответствующей «web». Когда следующий клиент (Client 2) запрашивает сервер DNS разрешить то же самое имя (web.contoso.com), DNS-сервер отвечает на запрос, предоставляя информацию второй записи, соответствующей «web». Эта вторая запись указывает на имя сервера websrv2, который имеет адрес 192.168.3.12. Если третий клиент начнет запрашивать DNS-сервер разрешить то же самое имя, то сервер снова будет отвечать информацией первой записи.

Основной целью циклического распределения DNS является балансировка нагрузки запросов клиентов среди серверов. Основным преимуществом данной технологии считается легкость настройки. Циклическое распределение DNS по умолчанию доступно в большинстве DNS-серверов, поэтому для настройки этого простого вида балансировки нагрузки вам потребуется только создать соответствующие записи DNS на DNS-сервере.

Несмотря на это существуют серьезные ограничения циклического распределения как механизма балансировки нагрузки. Самый большой недостаток технологии заключается в том, что если выходит из строя один из целевых серверов, DNS-сервер не может откликнуться на это событие и препятствует клиентам, направляя их на недействующий сервер до тех пор, пока системный администратор не удалит с этого DNS-сервера запись DNS. Вторым недостатком технологии DNS является то, что каждой записи присваивается один и тот же весовой коэффициент, независимо от того, является ли целевой сервер более мощным, чем другой, и не занят ли уже данный сервер. Последний недостаток технологии заключается в том, что циклическое распределение не всегда функционирует так, как ожидается. Поскольку клиенты DNS кэшируют отклики серверов на запросы, клиент DNS по умолчанию будет подключаться к одному

и тому же целевому серверу до тех пор, пока отклики, помещенные в кэш, будут оставаться активными.

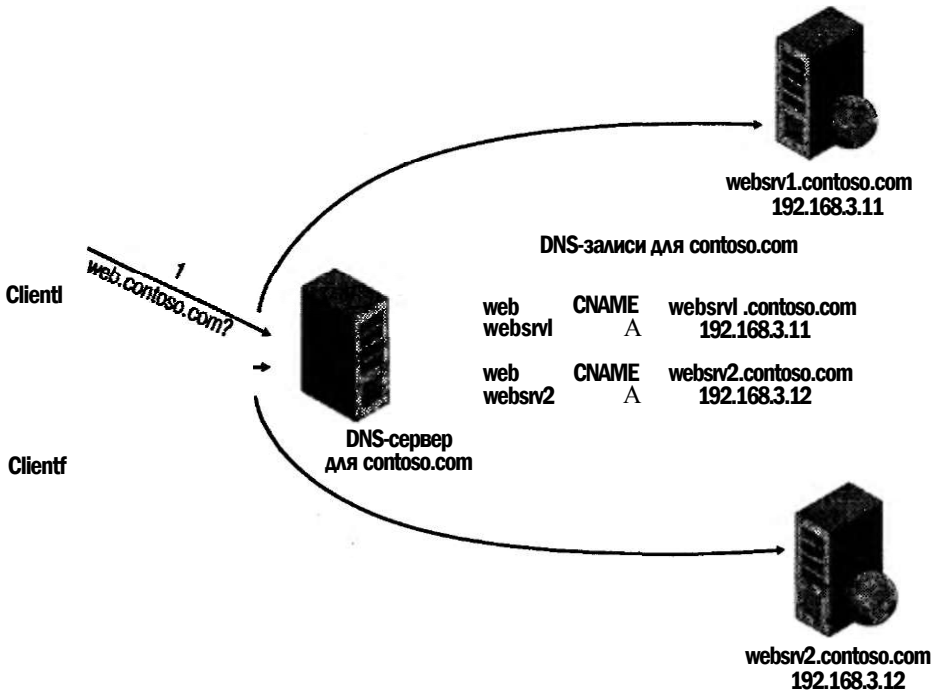


Рис. 2-17. В технологии циклического распределения DNS-сервер используется для распределения нагрузки клиентов между двумя и более серверами

Балансировка сетевой нагрузки

Технология NLB как устанавливаемый компонент в операционной системе Windows Sever 2008 прозрачно распределяет запросы клиентов среди серверов в NLB-кластере, применяя виртуальные IP-адреса и общее имя. С точки зрения клиента NLB-кластер представляет собой единственный сервер. В технологии распределения нагрузки NLB централизованный диспетчер не используется.

В общем сценарии NLB используется для создания *веб-фермы* — группы компьютеров, функционирующих с целью поддержки веб-сайта или группы веб-сайтов. Несмотря на это технология NLB также может быть применена для создания фермы серверов терминала, фермы серверов VPN или кластера брандмауэра ISA Server. На рис. 2-18 изображена базовая конфигурация веб-фермы NLB, расположенная за кластером брандмауэра NLB.

Как механизм балансировки нагрузки NLB обеспечивает значительные преимущества по сравнению с технологией циклического распределения DNS. Прежде всего, в противоположность циклическому распределению DNS, NLB автоматически определяет серверы, отключенные от NLB-кластера, и затем перераспределяет запросы клиентов на оставшиеся рабочие хосты. Эта особенность позволяет предотвратить отправку клиентами запросов на серверы, которые вышли из строя. Второе различие между NLB и циклическим распределе-

нием DNS заключается в том, что в механизме NLB вы можете установить процент нагрузки для каждого хоста. В результате клиенты будут статистически распределены между хостами таким образом, что каждый сервер будет получать заданный процент входящих запросов.

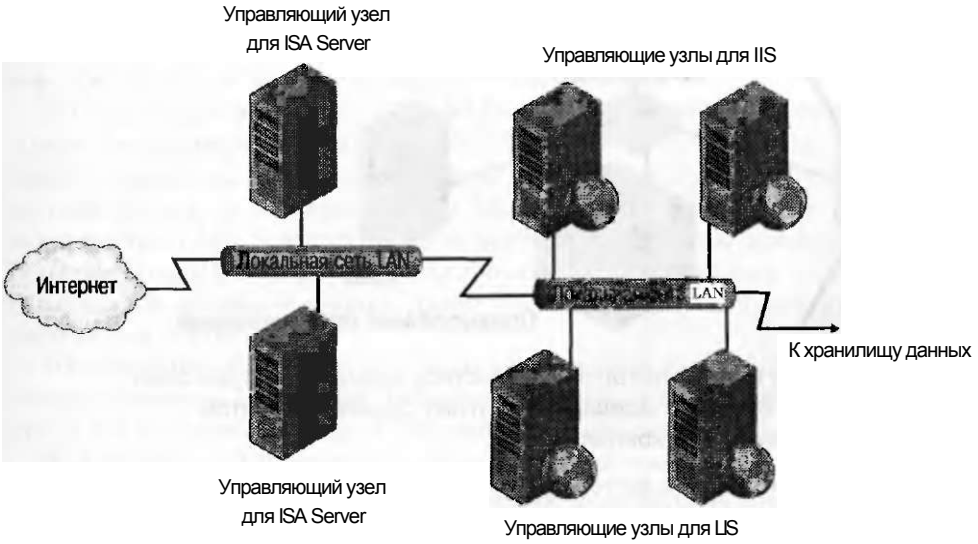


Рис. 2-18. Базовая конфигурация двух соединенных NLB-кластеров

Кроме балансировки нагрузки NLB также поддерживает масштабируемость. В связи с возрастанием требований к таким сетевым сервисам, как веб-сайты, к ферме могут быть подключены дополнительные серверы с минимальным увеличением административных расходов.

Отказоустойчивость кластера

Отказоустойчивый кластер представляет собой группу, состоящую из двух или более компьютеров, используемых для предотвращения длительных простоев приложений и служб. Серверы кластера (называемые узлами) соединены между собой посредством физических кабелей и подсоединены к общему дисковому хранилищу данных. В случае отказа одного из узлов кластера другой узел берет его работу на себя в процессе, известном как переход на другой ресурс при сбое. В результате пользователи, подключенные к серверу, практически не ощущают сбоя в обслуживании.

Серверы отказоустойчивого кластера могут выполнять различные функции, в том числе функцию файлового сервера, печатного сервера, сервера электронной почты или сервера баз данных, при этом серверы кластера позволяют обеспечить высокую доступность для множества других служб и приложений.

В большинстве случаев отказоустойчивый кластер содержит общее запоминающее устройство, которое физически подсоединено ко всем серверам кластера, хотя любой том запоминающего устройства за единицу времени может быть доступен только одному серверу.

На рис. 2-19 изображен процесс перехода на другой ресурс при сбое в базовом двухузловом отказоустойчивом кластере.

Рис. 2-19. Если в отказоустойчивом кластере выходит из строя один из серверов, его функции передаются другому серверу, при этом используется то же самое хранилище

В отказоустойчивом кластере тома запоминающего устройства или сети LUN, доступные узлам кластера, не должны быть доступны другим серверам, в том числе серверам другого кластера. Этот процесс проиллюстрирован на рис. 2-20: два двухузловых отказоустойчивых кластера разделяют хранилище данных сети SAN.

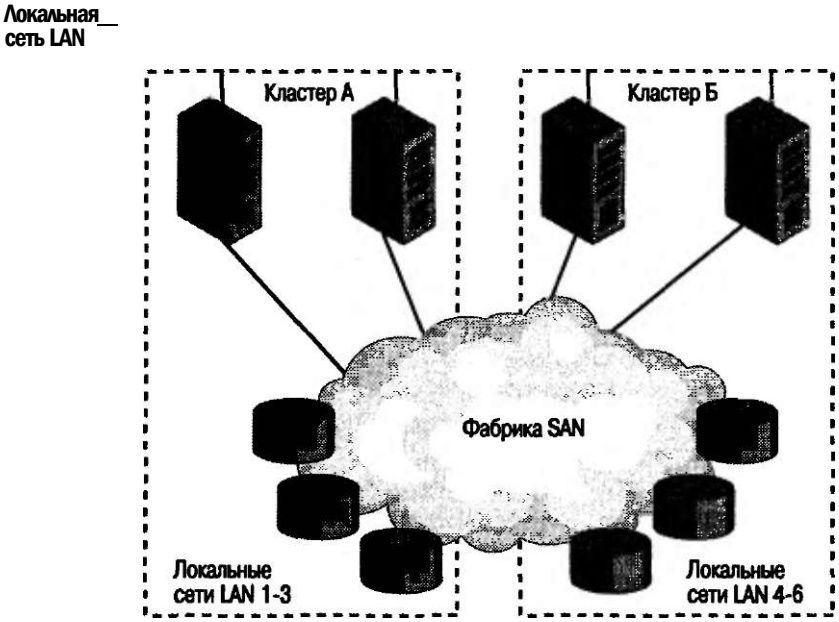


Рис. 2-20. Каждый отказоустойчивый кластер должен изолировать хранилище данных от других серверов

Настройка NLB-кластера

Создание NLB-кластера — относительно несложный процесс. Прежде всего установите операционную систему Windows Server 2008 на двух серверах, после этого настройте на обоих серверах службу или приложение, которое вы хотите предложить клиентам, например IIS. Обязательно создайте одинаковые конфигурации, чтобы время ожидания клиентов также было одинаковым, независимо от того, к какому серверу они подключены.

На следующем этапе настройки NLB-кластера необходимо установить компонент Балансировка сетевой нагрузки (Network Load Balancing) на всех серверах, которые вы хотите подключить к NLB-кластеру. Для этого откройте консоль Диспетчер серверов (Server Manager), а затем щелкните Добавление компонентов (Add Features). В окне мастера Добавление компонентов (Add Features Wizard) выделите Балансировка сетевой нагрузки (Network Load Balancing) и щелкните кнопку Далее (Next), а затем следуйте инструкциям мастера для установки.

На последнем этапе создания NLB-кластера для настройки кластера необходимо запустить компонент Диспетчер балансировки сетевой нагрузки (Network Load Balancing Manager). Эта процедура описана в следующем разделе.

Для создания NLB-кластера выполните предложенную инструкцию.

1. Запустите Диспетчер балансировки сетевой нагрузки (Network Load Balancing Manager) из папки Администрирование (Administrative tools). (Вы также можете открыть Диспетчер балансировки сетевой нагрузки (Network Load Balancing Manager) с помощью команды *Nlbmng.exe* командной строки.)
2. В дереве консоли Диспетчера балансировки сетевой нагрузки (Network Load Balancing Manager) щелкните правой кнопкой мыши Кластеры балансировки сетевой нагрузки (Network Load Balancing Clusters), а затем щелкните Создать кластер (New Cluster).
3. Подключитесь к узлу, который должен быть частью нового кластера. В поле Узел (Host) введите имя узла и щелкните Подключить (Connect).
4. Выберите интерфейс, который вы хотите использовать для кластера, а затем щелкните кнопку Далее (Next). (Интерфейс содержит виртуальный IP-адрес и принимает клиентский трафик для балансировки нагрузки.)
5. На странице Параметры узла (Host Parameters) выберите значение в раскрывающемся меню Приоритет (Уникальный идентификатор узла) (Priority (Unique host identifier)). Этот параметр определяет уникальный идентификатор для каждого узла. Узел с наименьшим числовым значением приоритета среди остальных членов кластера обрабатывает весь сетевой трафик кластеров, на которые не распространяются правила для портов. Вы можете переопределить данные приоритеты или установить балансировку нагрузки на конкретный диапазон портов, указывая правила портов на вкладке Правила портов (Port Rules) окна Свойства балансировки сетевой нагрузки (Network Load Balancing Properties).
6. На странице Параметры узла (Host Parameters) удостоверьтесь, что назначенный IP-адрес из выбранного вами интерфейса отображен в списке.

В противном случае щелкните кнопку Добавить (Add) для добавления адреса, а затем щелкните кнопку Далее (Next).

7. Для ввода IP-адреса кластера, который будет совместно использоваться каждым узлом в кластере, щелкните на странице IP-адреса кластера (Cluster IP Addresses) кнопку Добавить (Add). NLB добавит этот IP-адрес в стек TCP/IP выбранного интерфейса всех узлов, которые должны быть частью кластера. Щелкните кнопку Далее (Next).

ПРИМЕЧАНИЕ Используйте только статические адреса
Технология NLB не поддерживает Протокол динамического конфигурирования узла (Dynamic Host Configuration Protocol, DHCP). Протокол DHCP будет отключен на всех настраиваемых интерфейсах, поэтому IP-адреса должны быть статическими.

8. На странице Параметры кластера (Cluster Parameters) в области IP-конфигурация кластера (Cluster IP Configuration) задайте соответствующие значения для IP-адреса и маски подсети, затем введите Полное интернет-имя (Fully Qualified Domain Name) для кластера.

   Обратите внимание на то, что для 1Ру6-адресов не требуется указывать маску подсети. Заметьте также, что при использовании NLB со Службами терминалов (Terminal Services) не нужно вводить и Полное интернет-имя (Fully Qualified Domain Name).
9. На странице Параметры кластера (Cluster Parameters) в области Режим работы кластера (Cluster Operation Mode) щелкните параметр Одноадресный (Unicast) — тем самым вы укажете, что для операций кластера должен использоваться одноадресный MAC-адрес. В одноадресном режиме MAC-адрес кластера назначается сетевому адаптеру компьютера, и встроенный MAC-адрес сетевого адаптера не используется. Для данного режима рекомендуем принять параметры по умолчанию. Чтобы продолжить, щелкните кнопку Далее (Next).
10. На странице Правила для портов (Port Rules) щелкните кнопку Изменить (Edit), если требуется изменить правила для портов, установленные по умолчанию. Настроить правила можно следующим образом.
    - В области Диапазон портов (Port Range) выберите нужный диапазон в соответствии со службой, которую должен обеспечить NLB-кластер. Например, для веб-сервисов введите диапазон *с 80 по 80,* для того чтобы новое правило применялось только для http-трафика. Для Служб терминалов (Terminal Services) укажите диапазон *с 3389 по 3389,* для того чтобы новое правило применялось только для RDP-трафика.
    - В области Протоколы (Protocols) выберите TCP или UDP, чтобы применить правила для портов к протоколу TCP/IP Правила ограничивают сетевой трафик только для указанного протокола. Трафик, который не связан с правилом для порта, обрабатывается узлом по умолчанию.
    - В области Режим фильтрации (Filtering Mode) выберите Несколько узлов (Multiple Host), если вы хотите, чтобы для выбранного правила для пор-

та сетевой трафик обрабатывался несколькими узлами в кластере. Выберите Один узел (Single Host), если хотите, чтобы сетевой трафик обрабатывался одним узлом.

- Для параметра Сходство (Affinity) (применяется только для режима фильтрации Несколько узлов (Multiple Host)) установите значение Нет (None), если вы хотите, чтобы соединения с одного и того же IP-адреса клиента направлялись на различные узлы кластера. Оставьте параметр Один (Single), чтобы NLB направляла запросы с одного IP-адреса клиента на один и тот же узел кластера. Выберите параметр Сеть (Network), если необходимо, чтобы NLB направляла запросы с локальной подсети на один и тот же узел кластера.

11. После добавления правил портов щелкните кнопку Готово (Finish) для создания кластера.

    Для того чтобы добавить узлы к кластеру, щелкните правой кнопкой мыши новый кластер, а затем щелкните Добавить узел к кластеру (Add Host To Cluster). Настройте параметры узла (включая приоритет узла и назначенные IP-адреса) для всех добавляемых узлов, следуя тем же инструкциям, которые вы выполняли при настройке исходного узла. Поскольку вы добавляете узлы к уже настроенному кластеру, все общие для кластера параметры останутся неизменными.

Создание отказоустойчивого кластера

Создание отказоустойчивого кластера происходит в несколько этапов. На первом этапе необходимо настроить физическое аппаратное обеспечение для кластера. Затем нужно установить Средство отказоустойчивости кластера (Failover Clustering) и запустить средство Проверка конфигурации отказоустойчивого кластера (Failover Cluster Validation Tool), которое позволяет убедиться в том, что аппаратное и программное обеспечение соответствует требованиям отказоустойчивых кластеров. Сразу после того как программа завершит проверку конфигурации, создайте кластер, запустив Мастер создания кластера (Create Cluster Wizard). На заключительном этапе необходимо запустить Мастер высокой надежности (High Availability Wizard) для настройки режима работы кластера и определения доступности выбранных служб.

Подготовка аппаратного обеспечения для отказоустойчивого кластера

Существуют четкие требования к аппаратному обеспечению отказоустойчивых кластеров. Перед тем как приступить к настройке аппаратного обеспечения, проанализируйте следующий список требований к серверам, сетевым адаптерам, кабельным сетям, контроллерам и запоминающим устройствам:

- **Серверы** Используйте группу соединенных компьютеров, состоящую из одинаковых или похожих компонентов (рекомендуется).
- **Сетевые адаптеры и кабельные сети** В технологии создания отказоустойчивых кластеров аппаратное обеспечение для сетей, как и остальные компоненты, должно быть совместимо с операционной системой Windows Server 2008. Если вы используете технологию iSCSI, то каждый сетевой адаптер

должен быть предназначен только для сетевого соединения или только для iSCSI, но не для того и другого одновременно.

В сетевой инфраструктуре, соединяющей узлы кластеров, следует избегать появления единичных точек отказа. Существует несколько способов решения этой проблемы. Можно соединить узлы кластера посредством нескольких отдельных сетей. Альтернативный вариант — связать узлы кластера с одной сетью, построенной с помощью объединенных в группу сетевых адаптеров, резервных коммутаторов, резервных маршрутизаторов или аналогичного оборудования, позволяющего устранить единичные точки отказа.

Контроллеры устройств или соответствующие адаптеры для хранилища Если вы используете интерфейсы SCSI с последовательным подключением или FC, то контроллеры запоминающих устройств большой емкости, предназначенные для системы хранения данных кластера, должны быть идентичными во всех кластеризованных серверах. Кроме того, на них должна быть установлена одна и та же версия встроенного программного обеспечения. При использовании интерфейса iSCSI у каждого сервера в кластере должен быть хотя бы один сетевой адаптер или адаптер главной шины HBA, выделенный для системы хранения данных кластера. Сеть, которую вы применяете для технологии iSCSI, не может быть использована для сетевых взаимодействий. Во всех серверах кластера сетевые адаптеры, используемые для подключения к хранилищу iSCSI-цели, должны быть одинаковыми. Рекомендуется также применять адаптеры Gigabit Ethernet или адаптеры с большей скоростью. (Обратите внимание на то, что для технологии iSCSI нельзя использовать объединенные в группы сетевые адаптеры.)

Общее хранилище данных, совместимое с операционной системой Windows Server 2008 Для отказоустойчивого кластера, состоящего из двух узлов, хранилище данных должно содержать минимум два отдельных тома (LAN), настроенных на аппаратном уровне.

Первый том будет функционировать в качестве *диска-свидетеля,* который содержит копию базы данных кластерной конфигурации. Диски-свидетели, известные в операционной системе Windows Server 2008 как *диски кворума,* применяются во многих кластерных конфигурациях.

Второй том будет содержать общие файлы пользователей. Ниже перечислены требования, предъявляемые к хранилищу.

- Чтобы иметь возможность использовать встроенные средства поддержки дисков, включенные в отказоустойчивый кластер, задействуйте базовые, а не динамические диски.
- Рекомендуется отформатировать разделы дискового хранилища под файловую систему NTFS. (Для раздела диска-свидетеля файловая система NTFS является обязательной.)
- При развертывании сети хранения данных (SAN) с помощью отказоустойчивого кластера получите гарантии производителей и поставщиков относительно того, что хранилище, включая все драйверы, встроенное программное обеспечение и другие программы, используемые для хранилища, совместимы с отказоустойчивыми кластерами в операционной системе Windows Server 2008.

После выполнения требований к аппаратному обеспечению и подключения серверов кластера к хранилищу данных вы можете установить компонент Средство отказоустойчивости кластеров (Failover Cluster).

ПРИМЕЧАНИЕ Что означает термин «настройка кворума»

Настройка кворума в отказоустойчивом кластере определяет количество отказов, которые могут произойти в кластере, прежде чем он прекратит свою работу. В операционной системе Windows Server 2008 можно выбрать одну из четырех конфигураций кворума.

Первая конфигурация кворума, Большинство узлов (Node Majority), рекомендуется для кластеров с нечетным числом узлов. В указанной конфигурации продолжительность работы отказоустойчивого кластера такая же, как и у большинства узлов.

Вторая конфигурация кворума, Большинство узлов и дисков (Node And Disk Majority), рекомендуется для кластеров с четным числом узлов. При такой конфигурации кворума отказоустойчивый кластер использует диск-свидетель в качестве узла для разрешения конфликтов, в результате этого отказоустойчивый кластер работает столько же времени, сколько времени большинство узлов работают в сети и доступны.

Третья конфигурация кворума — Большинство узлов и общих файловых ресурсов (Node And File Share Majority). В данной конфигурации кворума, которая рекомендуется для кластеров с четным числом узлов и ограниченным доступом к диску-свидетелю, общий файловый ресурс-свидетель используется в качестве узла для разрешения конфликтов, и отказоустойчивый кластер работает столько же времени, сколько времени большинство узлов работают Ь сети и доступны.

Четвертая конфигурация кворума — Кворум без большинства: только диск (No Majority: Disk Only). В этой конфигурации, которую обычно использовать не рекомендуется, отказоустойчивый кластер работает в течение времени, когда единственный узел и его хранилище остаются подключенными к сети.

Проверьте себя

1. Что означает термин «диск-свидетель»?
2. Что такое настройка кворума для отказоустойчивого кластера?

Ответы

1. Диск-свидетель представляет собой общий том, используемый во многих кластерах, который содержит копию базы данных кластерной конфигурации.
2. Настройка кворума определяет количество отказов узлов, которые могут произойти в кластере, прежде чем он прекратит свою работу.

СОВЕТ Подготовка к экзамену

Для успешной сдачи экзамена 70-643 вам необходимо разбираться в вопросах настройки кворума, дисков-свидетелей или общих каталогов-свидетелей.

Установка Средства отказоустойчивости кластеров

Прежде чем создавать отказоустойчивый кластер, вам необходимо установить Средство отказоустойчивости кластеров (Failover Clustering) на всех узлах кластера. Для установки Средства отказоустойчивости кластеров (Failover Clustering) щелкните Добавление компонентов (Add Features) в консоли Диспетчер серверов (Server Manager). В открывшемся окне Мастера добавления компонентов (Add Features Wizard) установите флажок Средство отказоустойчивости кластеров (Failover Clustering). Щелкните кнопку Далее (Next) и начинайте выполнять установки компонента, следуя инструкциям мастера.

После того как компонент будет установлен на всех узлах, вы должны подтвердить правильность настройки аппаратного и программного обеспечения.

Проверка конфигурации кластера

Приступая к созданию нового кластера, запустите Мастер проверки конфигурации (Validate A Configuration Wizard), чтобы проверить, соответствуют ли ваши узлы необходимым требованиям аппаратного и программного обеспечения для отказоустойчивых кластеров.

Для запуска Мастера проверки конфигурации (Valdiate A Configuration Wizard) сначала откройте окно Управление отказоустойчивым кластером (Failover Cluster Management) из группы программ Администрирование (Administrative Tools). В окне Управление отказоустойчивым кластером (Failover Cluster Management) щелкните ссылку Проверить конфигурацию (Valdiate A Configuration) в разделе Управление (Management) или в разделе Действия (Actions), как показано на рис. 2-21.

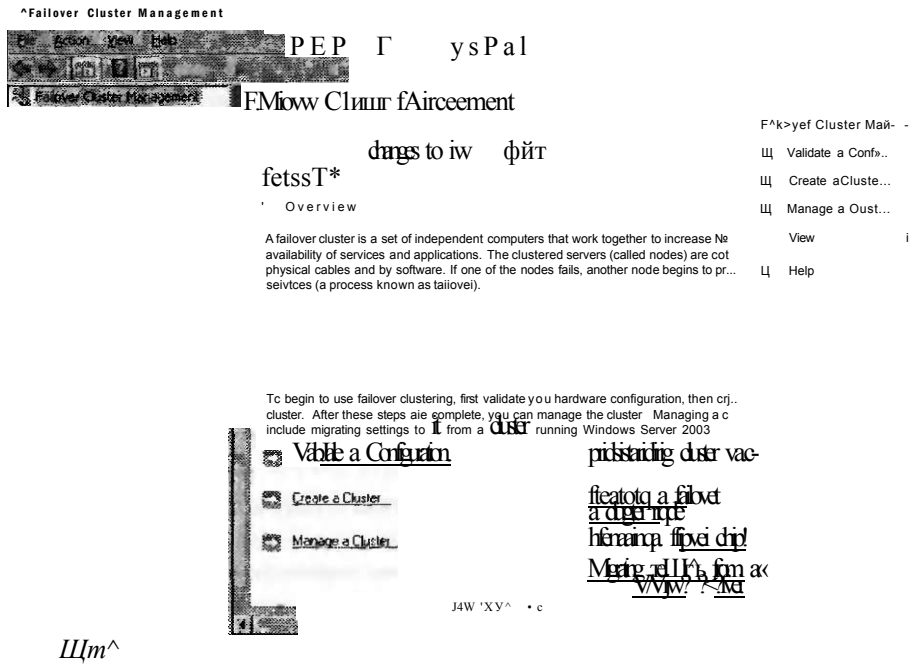


Рис. 2-21. Проверка требований отказоустойчивого кластера

После завершения работы мастера при необходимости внесите любые изменения в конфигурацию и возобновите проверку до ее успешного завершения. После того как необходимые условия для кластера будут проверены, вы сможете создать кластер, запустив Мастер создания кластера (Create Cluster Wizard).

Запуск Мастера создания кластера

На следующем этапе необходимо запустить Мастер создания кластера (Create Cluster Wizard). Этот мастер устанавливает основное программное обеспечение для кластера, преобразует подключенную систему хранения в диски кластера и создает для кластера учетную запись компьютера в Службе каталогов (Active Directory). Для запуска этого средства в оснастке Управление отказоустойчивым кластером (Failover Cluster Management) щелкните ссылку Создать кластер (Create A Cluster) в разделе Управление (Management) или в разделе Действия (Actions).

В окне Мастера создания кластера (Create Cluster Wizard) в ответ на приглашение программы введите имена узлов кластера. Затем мастер предложит вам ввести имя кластера и назначить ему IP-адрес, после чего этот кластер будет создан.

После завершения работы мастера потребуется настроить службы и приложения, для которых нужно обеспечить отказоустойчивость. Для выполнения данного вида настройки запустите Мастер высокой надежности (High Availability Wizard).

Запуск Мастера высокой надежности

Мастер высокой надежности (High Availability Wizard) настраивает параметры высокой надежности для отдельных служб и приложений. Для запуска этого мастера в оснастке Управление отказоустойчивым кластером (Failover Cluster Management) щелкните пункт Настройка службы или приложения (Configure A Service Or Application) в разделе Действия (Action) или в области Конфигурировать (Configure).

Для завершения работы Мастера высокой надежности (High Availability Wizard) выполните следующие действия.

1. Ознакомьтесь с текстом, представленным на странице Перед началом работы (Before You Begin), и щелкните кнопку Далее (Next).
2. На странице Выберите службу или приложение (Select Service Or Application) выберите службу или приложение, для которых требуется обеспечить высокую надежность, и щелкните кнопку Далее (Next).
3. Следуйте инструкциям мастера для уточнения необходимых деталей относительно выбранной службы. Например, для службы Файловый сервер (File Server) необходимо определить следующие параметры:
   - имя кластеризованного файлового сервера;
   - данные IP-адресации, не предоставляемые автоматически используемыми параметрами DHCP, например статический адрес IPv4 для этого кластеризованного файлового сервера;
   - один или несколько томов хранилища, которые должны использоваться этим кластеризованным файловым сервером.

4. Чтобы просмотреть отчет о выполненных мастером задачах, после завершения работы мастера и появления страницы Сводка (Summary) щелкните Просмотреть отчет (View Report).
5. Щелкните кнопку Готово (Finish), чтобы закрыть окно мастера.

Тестирование отказоустойчивого кластера

Когда работа мастера будет завершена, протестируйте отказоустойчивый кластер с помощью оснастки Управление отказоустойчивым кластером (Failover Cluster Management). Удостоверьтесь, что в дереве консоли развернута ветвь Службы и приложения (Services And Applications), и выберите службу, которую вы только что добавили с помощью Мастера высокой надежности (High Availability Wizard). Щелкните правой кнопкой мыши службу кластера, затем щелкните Переместить эту службу или приложение на другой узел (Move This Service Or Application To Another Node) и выберите один из доступных узлов. После перемещения экземпляра кластеризованного файлового сервера изменения состояния можно увидеть в центральной области оснастки. Успешное перемещение службы свидетельствует о правильной работе функции отказоустойчивости.

Практикум. Анализ отказоустойчивости кластера

Выполняя данное практическое занятие, вы увидите интернет-трансляцию, демонстрирующую процесс создания отказоустойчивого кластера в операционной системе Windows Server 2008.

Упражнение 1. Просмотр демонстрационного ролика об отказоустойчивости кластера

Для выполнения этого упражнения просмотрите созданный Жозе Баретто (Jose Baretto) 17-минутный демонстрационный ролик под названием «How to Create a Failover Cluster in Windows Server 2008». Вы также можете найти файл ролика в папке Webcast на компакт-диске. Кроме того, файл доступен для просмотра на веб-сайте: *https://www.livemeeting.com/cc/microsoft/view?id=FailoverClustering&pw=josebda.*

Резюме

- В операционной системе Windows Server 2008 можно настроить группы серверов для обеспечения балансировки нагрузки, масштабируемости или высокой доступности для определенных служб или приложений. Эти группы серверов называются кластерами и могут быть применены для различных целей. В большинстве случаев кластеры являются прозрачными, и клиенты видят их как единичные серверы.
- Циклическое распределение DNS представляет собой базовый метод балансировки запросов к единственному серверу между двумя и более серверами. Технология циклического распределения легко настраивается, однако существенным ее ограничением является недостаток информации о состоянии сервера.

- Балансировка сетевой нагрузки (Network Load Balancing, NLB) в операционной системе Windows Server 2008 представляет собой настраиваемый компонент. Подобно технологии циклического распределения NLB прозрачно распределяет запросы клиентов на единственный сервер между двумя и более серверами. Однако NLB не имеет таких ограничений, как циклическое распределение DNS, благодаря своим более совершенным возможностям, например возможности автоматического перенаправления запросов с отказавшего или загруженного сервера. Технология NLB часто используется для создания веб-ферм, которые представляют собой NLB-кластеры, применяемые для ответов на запросы к веб-сайту или группе веб-сайтов.
- Средство отказоустойчивости кластеров (Failover Clustering) в Windows Server 2008 также является настраиваемым компонентом. Отказоустойчивый кластер — это группа компьютеров, используемых для предотвращения длительных простоев выбранных приложений и служб. Серверы (или узлы) в отказоустойчивом кластере соединены между собой и подключены к общему хранилищу. Отказоустойчивые кластеры нуждаются в наличии довольно сложного аппаратного обеспечения, поэтому следует проанализировать зти требования перед принятием решения об их приобретении.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных в ходе занятия 2. Эти вопросы представлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы
Ответы и пояснения к каждому их варианту размещены в разделе «Ответы» в ,конце книги.

1. Вы работаете сетевым администратором в Tailspintoys.com. В ваши служебные обязанности входит поддержка служб компании. Ведущим узлом в сети Tailspintoys.com выступает веб-сервер, который функционирует на единственном сервере с именем Webservl. В последнее время посещаемость веб-сайта возросла, а производительность веб-сервера снизилась. В ближайшие пять-шесть лет ожидается дальнейшее увеличение сетевого трафика веб-сайта. Вам необходимо найти решение проблемы производительности веб-сервера и обеспечить работу веб-сайта с возросшей рабочей нагрузкой на ближайший период. Что для этого нужно сделать?

   А. Переместить веб-сайт на более мощный сервер.

   Б. Использовать технологию NLB, чтобы создать веб-ферму для обеспечения работы веб-сайта.

   В. Применить отказоустойчивые кластеры с несколькими серверами в кластере для обеспечения работы веб-сайта.

   Г. Добавить веб-сервер, а затем использовать циклическое распределение DNS для распределения запросов к веб-сайту между двумя серверами. При необходимости добавить дополнительные серверы.

2. Настраивая отказоустойчивый кластер для сервера базы данных, вы назначаете ему четыре узла. У вас есть соответствующее хранилище, а все узлы имеют доступ к сети SAN. Какой из указанных ниже параметров следует выбрать для настройки кворума?
   А. Большинство узлов (Node Majority).
   Б. Большинство узлов и дисков (Node And Disk Majority).
   В. Большинство узлов и общих файловых ресурсов (Node And File Share Majority).
   Г. Кворум без большинства: только диск (No Majority: Disk Only).

Закрепление материала главы

Для того чтобы попрактиковаться и закрепить знания, приобретенные в ходе изучения представленного в данной главе материала, вам необходимо:

- ознакомиться с резюме главы;
- повторить используемые в главе основные термины;
- выполнить задания лабораторной работы, которые моделируют реальные ситуации, требующие применения полученных знаний;
- выполнить рекомендуемые упражнения;
- сдать пробный экзамен с помощью тестов.

Резюме главы

- Для работы операционных систем и приложений на серверах необходим доступ к данным, основанный на блочной системе. Для этих целей обычно используется хранилище с прямым доступом. Указанный тип хранилища включает в себя все внутренне установленные жесткие диски, а также запоминающее устройство с внешним доступом.
- Операционная система Windows Server 2008 содержит Службу виртуальных дисков (Virtual Disk Service, VDS), которая позволяет управлять совместимыми дисковыми подсистемами с помощью средств администрирования операционной системы Windows Server 2008, например таких, как Диспетчер хранилища для сетей SAN (Storage Manager for SANs, SMfS).
- Для создания простых томов, составных томов, чередующихся томов, зеркальных томов и томов RAID-5 в операционной системе Windows Server 2008 используется оснастка Управление дисками (Disk Management). У вас имеется возможность расширить или сжать существующие тома.
- Балансировка сетевой нагрузки (Network Load Balancing, NLB) применяется с целью распределения рабочей нагрузки между несколькими серверами. Клиенты подключаются к NLB-кластеру, задавая виртуальное имя компьютера и виртуальный IP-адрес. Свободный сервер в составе NLB-кластера ответит на запрос.
- Отказоустойчивые кластеры позволяют минимизировать время простоя сервера. В отказоустойчивом кластере серверы или узлы используют общее

хранилище. При выходе из строя одного из серверов его работу берет на себя другой сервер.

Основные термины

Проверьте, знаете ли вы, что означают перечисленные ниже термины (свои ответы можно сверить с определениями, содержащимися в конце книги):

- на блочном уровне;
- кластер;
- инициатор iSCSI;
- цель iSCSI;
- контроль четности;
- стиль разделов;
- циклическое распределение DNS;
- фабрика SAN;
- веб-ферма;
- диск-свидетель.

Лабораторная работа

Выполняя следующие задания, вы будете применять знания, полученные во время изучения этой главы. Правильные ответы можно найти в разделе «Ответы» в конце книги.

Задание 1. Проектирование хранилища данных

Вы работаете специалистом в отделе информационных технологий в банке Woodgrove Bank.

Поскольку банк принял решение создать из некоторых серверов сеть SAN для совместного использования хранилища данных, вам поручили изучить технологию SAN. Выбранные серверы планируется переместить в сеть SAN в течение ближайшего года.

Основная цель создания будущей сети SAN — построение гибкого хранилища и обеспечение сравнительно непродолжительного времени ожидания для серверов баз данных.

Кроме того, важно с максимальной эффективностью использовать квалификацию персонала отдела в области сетевых технологий и по возможности способствовать управлению сетью SAN через интерфейс операционной системы Windows Server 2008. Ни один из специалистов отдела информационных технологий не имеет опыта работы с сетями SAN.

1. Какую технологию соединения вы выберете для сети SAN, исходя из требований организации?
2. Какое из предлагаемых поставщиками устройств вы выберете для выполнения административных задач сетью SAN?

Задание 2. Проектирование высокой надежности

Вы занимаете должность администратора сервера в компании Trey Research. Компания недавно приобрела важное коммерческое приложение Appl, которое ежедневно интенсивно используют 500 сотрудников. Appl — это базирующееся на интернет-технологиях приложение, которое устанавливает подключение к серверу базы данных.

Вместе с другими сотрудниками отдела информационных технологий вы проектируете серверы, которые будут выполнять роли ведущих узлов для Appl и базы данных.

Вообще предусматривается два отдельных сервера или кластера, один из которых станет ведущим узлом для IIS и Appl, а другой — для базы данных. Все серверы должны работать в операционной системе Windows Server 2008. Основная задача проектируемых серверов — минимизировать время простоя и обеспечить наилучшую производительность для приложения и базы данных. При этом должна использоваться единственная база данных, которая всегда внутренне совместима. Приложение Appl постоянно должно иметь доступ ко всем таблицам.

Вам как члену команды проектировщиков дали задание проанализировать варианты решений с кластерами для сервера веб-приложения и сервера базы данных. Какая встроенная в операционную систему Windows Server 2008 технология кластеризации будет наиболее подходящей для сервера веб-приложения и почему?

Рекомендуемые упражнения

Чтобы успешно справиться с экзаменационными заданиями, выполните следующие упражнения.

Настройка хранилища данных

Если вы имеете доступ к системе с тремя дополнительными дисками, виртуальными или физическими, вам следует выполнить все три упражнения. Если у вас нет доступа к такой системе, просмотрите интернет-трансляции, упоминаемые в упражнениях 2 и 3. Хотя упражнение 2 рассчитано на работу с операционной системой Windows Server 2003 R2, в нем вводятся многие понятия и средства, уместные и в операционной системе Windows Server 2008.

- **Упражнение 1** **В** операционной системе Windows Server **2008** создайте том RAID-5. Сохраните данные в томе. Переведите один из дисков в автономный режим, а затем попытайтесь получить доступ к данным.
- **Упражнение 2** Просмотрите интернет-трансляцию Треса Хилла (Tres Hill) под названием «Build a Simple SAN with Windows Server 2003 R2 and Intelligent iSCSI Storage». Этот файл доступен и на компакт-диске, а кроме того, его можно найти по ключевому слову ID 1032289955 на сайте *http://msevents.mcrosoft.com.*

я **Упражнение 3** Просмотрите интернет-трансляцию Дэйва Лэлора (Dave Lalor) под названием «Reducing IT Overhead with Windows Server 2008 Sto-

rage Features». Этот файл также доступен и на компакт-диске, а кроме того, его можно найти по ключевому слову **ID 1032347804** на сайте *http://msevents.mcrosoft.com.*

Настройка высокой надежности

Выполните как минимум два первых упражнения. Если у вас имеется возможность использовать виртуальную машину или два физических сервера, не лишним будет выполнить и упражнение 3.

- **Упражнение 1** Просмотрите демонстрационный ролик Орина Томаса (Orin Thomas) под названием «Load Balancing», доступный на веб-сайте *mms://wm.microsoft.com/ms/windowsserversistem/compare/screencasts/Load_balancing_Windows.wmv.* Этот 5-минутный ролик демонстрирует процесс создания NLB-кластера в операционной системе Windows Server 2003.
- **Упражнение 2** Зайдите на веб-сайт *http://msevents.mcrosoft.com* и произведите поиск по ключевому слову **ID 1032345932.** Зарегистрируйтесь и выполните виртуальную лабораторную работу «TechNet Virtual Lab: Windows Server **2008** Enterprise Failover Clustering Lab».
- **Упражнение 3** Установите операционную систему Windows Server **2008** на два сервера, а затем добавьте на эти серверы компонент Балансировка сетевой нагрузки (Network Load Balancing). Создайте NLB-кластер и присоедините оба сервера к этому кластеру.

Пробный экзамен

На прилагаемом к книге компакт-диске представлено несколько вариантов тренировочных тестов. Проверка знаний выполняется по одной или же по всем экзаменационным темам сертификационного экзамена **70-643.** Тестирование можно организовать таким образом, чтобы оно проводилось как экзамен, или же настроить его на обучение — в этом случае вы сможете после каждого своего ответа на вопрос просматривать правильные ответы и объяснения.

ПРИМЕЧАНИЕ Пробный экзамен

Подробнее о пробном экзамене рассказано во введении к данной книге.

ГЛАВА 3

Установка и настройка служб терминалов

Занятие 1. Развертывание сервера терминалов 123

Занятие 2. Настройка служб терминалов 143

Если вы интерпретируете инфраструктуру приложений как набор технологий, обеспечивающих доставку приложений пользователям, то Службы терминалов (Terminal Services) можно назвать одним из главных компонентов. Службы терминалов представляют технологию, позволяющую удаленным пользователям устанавливать на компьютере Windows Server 2008 интерактивные сеансы — сеансы рабочего стола и сеансы приложений.

Роль Службы терминалов (Terminal Services) входит в темы сертификационного экзамена 70-643. Службы терминалов включают много компонентов, инструментов и функций. По этой причине данной роли посвящены две главы. В настоящей главе описано развертывание и конфигурирование ядра роли Службы терминалов, а в следующей рассказывается о многих дополнительных компонентах инфраструктуры служб терминалов.

Темы экзамена:

- Конфигурирование опций сервера служб терминалов.
- Настройка лицензирования служб терминалов.
- Настройка баланса нагрузки служб терминалов.

Требования

Для выполнения упражнений этой главы необходимо иметь:

- компьютер Windows Server 2008 с именем Server1, являющийся контроллером домена Contoso.com;
- компьютер Windows Server 2008 с именем Server2, который входит в домен Contoso.com;
- компьютер с инсталляцией ядра сервера системы Windows Server 2008 и именем Core1, входящий в домен Contoso.com.

Реальный мир

Дж. К. Макин

В Windows Server 2008 в Службы терминалов (Terminal Services) включен ряд радикально новых компонентов. Так, RemoteApp позволяет запускать удаленную программу на еще одном компьютере, другой компонент, Веб-доступ к службам терминалов (TS Web Access), создает веб-страницу, с которой можно запускать те же удаленные приложения. Сервер шлюза служб терминалов (Terminal Services Gateway, TS Gateway) обеспечивает альтернативу виртуальным частным сетям (VPN), позволяя авторизованным пользователям подключаться из Интернета к любому рабочему столу во внутренней сети.

Раньше такая функциональность была доступна лишь в приложениях сторонних производителей. Теперь же эти мощные функции встроены в Windows Server 2008.

Службы терминалов превратились в одну из основных технологий, принципы работы которой нужно знать.

Занятие 1. Развертывание сервера терминалов

В систему Windows Server 2008 уже включена технология Удаленный рабочий стол (Remote Desktop), с помощью которой можно выполнять те же функции, что и с использованием служб терминалов. По этой причине перед развертыванием роли Службы терминалов (Terminal Services) важно знать, какие преимущества обеспечивает эта роль в сравнении с удаленным рабочим столом.

Из данного занятия вы узнаете об уникальных компонентах служб терминалов, ознакомитесь с инструкциями по установке и развертыванию сервера терминалов.

Изучив материал этого занятия, вы сможете:

- Описать основные компоненты и функции служб терминалов.
- Сравнить службы терминалов со встроенным компонентом Удаленный рабочий стол (Remote Desktop).
- Инсталлировать Службы терминалов (Terminal Services) в конфигурации полной установки и установки ядра сервера Windows Server 2008.
- Описать опции лицензирования клиентов для сервера терминалов.
- Подготовить сервер терминалов к развертыванию.

Расчетная продолжительность занятия составляет 40 мин.

Службы терминалов

Службы терминалов (Terminal Services) позволяют удаленным пользователям устанавливать интерактивные сеансы рабочего стола или приложений на компьютере Windows Server 2008. Клиенты служб терминалов выполняют всю

обработку сеанса на сервере терминалов. Благодаря данной функциональности служб терминалов организация имеет возможность распределять ресурсы центрального сервера среди множества пользователей и клиентов. Например, службы терминалов часто используются для обеспечения единой инсталляции приложения для всех пользователей в организации. Особенно это удобно при развертывании приложений LOB (Line-Of-Business) и других программ для инвентаризации.

На рис. 3-1 продемонстрировано, как сервер терминалов может обеспечить доступ к центральному приложению для удаленных клиентов.

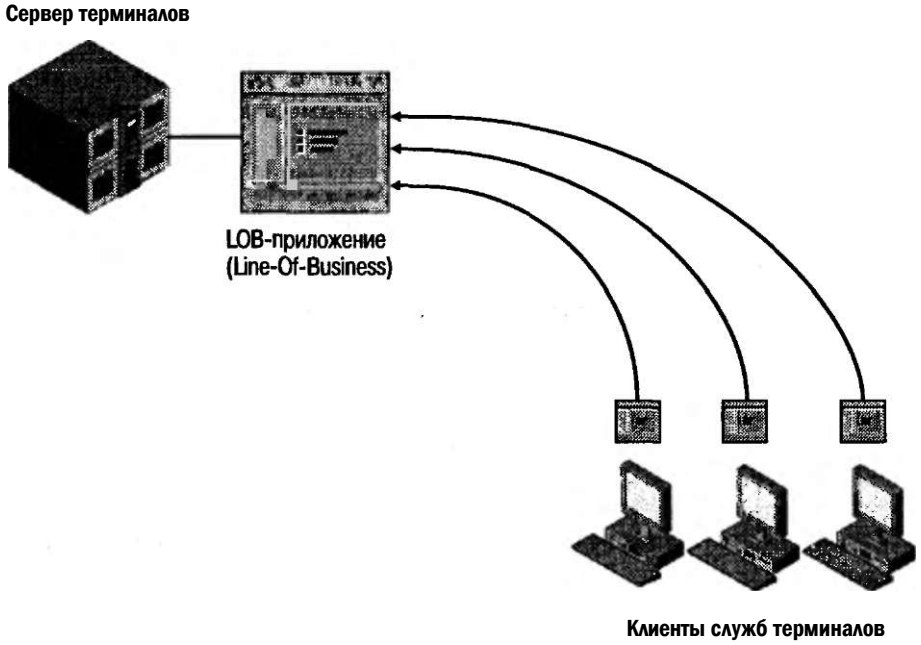


Рис. 3-1. Развертывание приложения с помощью сервера терминалов

Службы терминалов и подключение к удаленному рабочему столу

Системы Microsoft Windows XP, Windows Vista, Windows Server 2003 и Windows Server 2008 включают компонент Удаленный рабочий стол (Remote Desktop), который аналогично службам терминалов дает возможность пользователям устанавливать интерактивный сеанс рабочего стола на удаленном компьютере. Удаленный рабочий стол (Remote Desktop) и Службы терминалов (Terminal Services) близко связаны. Во-первых, обе технологии используют клиентское программное обеспечение Подключение к удаленному рабочему столу (Remote Desktop Connection), которое также называют Клиентом служб терминалов (Terminal Services Client) или Mstsc.exe. Это программное обеспечение встроено во все версии Windows, начиная с Windows XP, и может быть установлено практически на любом компьютере. Для удаленного пользователя процедура подклю-

чения к серверу терминалов аналогична подключению к удаленному рабочему столу. Во-вторых, практически идентична и серверная часть обоих компонентов. Оба компонента, Службы терминалов и Удаленный рабочий стол, используют одну службу Службы терминалов (Terminal Services). И наконец, оба компонента устанавливают сеансы с помощью одного протокола Remote Desktop Protocol (RDP) через один TCP-порт 3389.

Отличия между компонентами Удаленный рабочий стол (Remote Desktop) и Службы терминалов (Terminal Services) заключаются в том, что Службы терминалов предоставляют больше возможностей для расширяемости, а также содержат много дополнительных важных компонентов. Например, на компьютере Windows Server 2008 с включенным компонентом Удаленный рабочий стол (Remote Desktop) лишь два пользователя могут одновременно подключиться к активному сеансу рабочего стола (в том числе все локальные пользователи активных консольных сеансов). Таких ограничений не существует на сервере с установленными и отконфигурированными службами терминалов.

ПРИМЕЧАНИЕ Подключения и сеансы
Так в чем же состоит различие между подключением и сеансом служб терминалов? Подключение служб терминалов выполняется лишь для открытия окна Подключение к удаленному рабочему столу (Remote Desktop Connection), в котором отображается рабочий стол удаленного компьютера. Сеанс служб терминалов представляет продолжительный период времени, в течение которого пользователь подключен к удаленному компьютеру. Если закрыть окно Подключение к удаленному рабочему столу и не отключаться от удаленного компьютера, подключение будет завершено, однако сеанс продолжится (если это разрешено в конфигурации сервера). Если потом вновь подключиться к удаленному серверу, то откроется тот же сеанс со всеми открытыми программами и файлами, причем в том виде, в каком они находились до закрытия окна подключения. *Консольный сеанс,* как можно догадаться по названию, вообще не имеет отношения к сеансу служб терминалов, а представляет отдельный активный сеанс рабочего стола на физическом компьютере.

Помимо удаленного рабочего стола Службы терминалов (Terminal Services) в Windows Server 2008 включают следующие дополнительные компоненты.

- **Многопользовательская поддержка (Multiuser capacity)** Службы терминалов поддерживают два режима: режим выполнения Execute (для стандартного запуска приложений) и режим установки Install (для инсталляции приложений). При установке приложения на сервер терминалов в режиме TS Install параметры записываются в реестр или файлы .ini таким образом, чтобы обеспечить поддержку множества пользователей. В отличие от служб терминалов компонент Удаленный рабочий стол (Remote Desktop) в Windows не включает режим установки и не обеспечивает многопользовательскую поддержку приложений.
- **RemoteApp** В Windows Server 2008 компонент RemoteApp служб терминалов позволяет удаленно развертывать приложения для пользователей, как

если бы каждое такое приложение было запущено на локальном компьютере конечного пользователя. Вместо того чтобы предоставлять весь рабочий стол удаленного сервера терминалов в окне с изменяемыми размерами, компонент RemoteApp позволяет интегрировать удаленное приложение с рабочим столом пользователя. Приложение, развернутое через службы терминалов, запускается в собственном окне с изменяемыми размерами и собственным заголовком в панели задач.

- **Веб-доступ к службам терминалов (TS Web Access)** Этот компонент позволяет обеспечить для пользователей доступ к приложениям на удаленном сервере терминалов через веб-браузеры. После настройки веб-доступа к службам терминалов пользователи могут посещать веб-сайты (из Интернета или интрасети организации) и просматривать список всех приложений RemoteApp. Для запуска одного из перечисленных приложений пользователям достаточно щелкнуть значок программы на веб-странице.
- **Посредник сеансов служб терминалов (TS Session Broker)** Используя балансировку сетевой нагрузки NLB (Network Load Balancing) или циклическое распределение DNS, вы можете развернуть множество серверов терминалов в ферме, которая будет представлена для удаленных пользователей как единый сервер. Ферма серверов терминалов является наилучшим способом поддержки множества пользователей, а для расширения возможностей функциональности такой фермы используется служба ролей Посредник сеансов служб терминалов (TS Session Broker). Этот компонент позволяет клиентам фермы серверов терминалов подключаться к отключенным сеансам.
- **Шлюз служб терминалов (TS Gateway)** Этот компонент позволяет авторизованным пользователям в Интернете подключаться к удаленным рабочим столам и серверам терминалов, расположенным в частных корпоративных сетях. Шлюз служб терминалов обеспечивает безопасность таких подключений, выполняя туннелирование каждого RDP-сеанса в зашифрованном сеансе Hypertext Transfer Protocol Secure (HTTPS), обеспечивая авторизованным пользователям обширные возможности доступа к внутренним компьютерам через зашифрованное подключение. Во многих случаях шлюз служб терминалов исключает необходимость в VPN.

Преимущества удаленного рабочего стола

Основное преимущество компонента Удаленный рабочий стол (Remote Desktop) по сравнению со Службами терминалов (Terminal Services) заключается в том, что эта функциональность встроена в Windows Server 2008 и не требует приобретения клиентских лицензий доступа служб терминалов (TS CAL). Если вы не приобретете лицензии TC CAL для служб терминалов, то компонент TS перестанет работать через 120 дней.

Еще одно преимущество удаленного рабочего стола состоит в том, что данный компонент, в отличие от служб терминалов, легко реализуем. Для включения служб терминалов требуется установить и отконфигурировать новую роль сервера, а для включения удаленного рабочего стола нужно лишь выбрать одну опцию в диалоговом окне Свойства системы (System Properties).

ПРИМЕЧАНИЕ Удаленный рабочий стол и удаленный рабочий стол для администрирования

В Windows Server 2003 и Windows Server 2008 встроенный компонент Удаленный рабочий стол (Remote Desktop) часто именуется как Удаленный рабочий стол для администрирования RDA (Remote Desktop for Administration). Разница между RDA и компонентом Удаленный рабочий стол в Windows XP и Windows Vista состоит в том, что RDA в Windows Server 2008 включает два активных сеанса рабочего стола на сервере: либо два удаленных сеанса, либо один удаленный и один консольный сеанс. Системы Windows XP и Windows Vista не позволяют одновременно запускать два сеанса рабочего стола. Пользователь может подключиться лишь к одному рабочему столу, причем в момент подключения удаленного пользователя должен быть выполнен выход локального пользователя из системы.

СОВЕТ Подготовка к экзамену

В Windows Server 2008 компонент Удаленный рабочий стол (Remote Desktop) используется для удаленного администрирования, а управление приложениями осуществляется с помощью Служб терминалов (Terminal Services). Тем не менее основное отличие между этими двумя компонентами состоит в масштабах реализации, а цели их реализации частично совпадают. Удаленный рабочий стол можно использовать для подключения к редко применяемому приложению и удаленного администрирования сервера с установленными службами терминалов. Помните, что основные клиентские и серверные компоненты этой технологии используются совместно, следовательно, и некоторые термины часто применяются как взаимозаменяемые.

Включение удаленного рабочего стола

По умолчанию Windows Server 2008 не принимает подключения клиентов удаленного рабочего стола. Включить в Windows Server 2008 компонент Удаленный рабочий стол (Remote Desktop) можно на вкладке Удаленное использование (Remote) диалогового окна Свойства системы (System Properties). Чтобы получить доступ к этой вкладке, на панели управления нужно щелкнуть значок Система (System), а затем щелкнуть ссылку Настройка удаленного доступа (Remote Settings). Вы также можете ввести в окне Выполнить (Run) команду *control sysdm.cpl,* а затем в открывшемся диалоговом окне Свойства системы перейти на вкладку Удаленное использование (Remote).

Чтобы обеспечить высокий стандарт безопасности RDP-подключений, на вкладке Удаленное использование (Remote) выберите опцию сетевой проверки подлинности NLA (Network Level Authentication), как показано на рис. 3-2. При активизации данной опции лишь клиенты с версией удаленного рабочего стола не ниже Windows Vista смогут устанавливать подключения. Вы также можете разрешить подключения клиентов, работающих с любой версией рабочего стола.

Если в диалоговом окне Свойства системы (System Properties) системы Windows Server 2008 разрешить подключения к удаленному рабочему столу, автоматически будет создано исключение брандмауэра для RDP-трафика.

В таком случае вам не придется создавать исключение вручную, чтобы разрешить подключения клиентов удаленного рабочего стола.

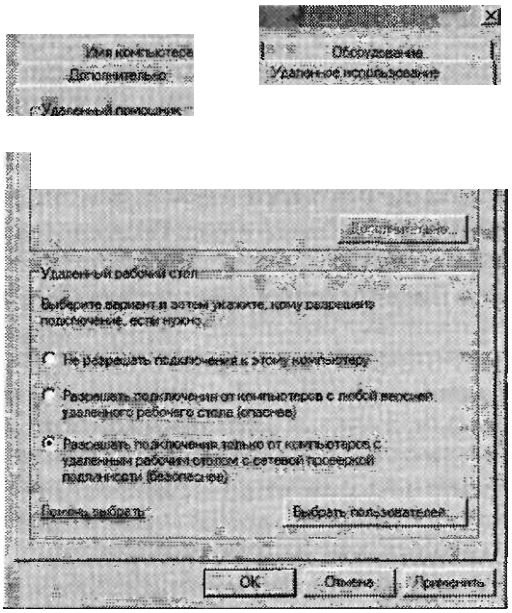


Рис. 3-2. Включение удаленного рабочего стола в Windows Server 2008

ПРИМЕЧАНИЕ Сетевая проверка подлинности

Компонент сетевой проверки подлинности NLA включен в протокол удаленного рабочего стола RDP 6.0 (Remote Desktop Protocol). При использовании этого протокола проверка подлинности пользователя выполняется перед полной установкой подключения Удаленный рабочий стол (Remote Desktop) между двумя компьютерами. В ранних версиях RDP пользователь мог ввести имя и пароль для проверки подлинности только после открытия окна входа в Windows удаленного компьютера в сеансе удаленного рабочего стола. Поскольку каждая попытка проверить подлинность сеанса требовала значительных ресурсов сервера, при использовании ранних версий RDP-подключений компьютеры с включенными компонентами Удаленный рабочий стол (Remote Desktop) и Службы терминалов (Terminal Services) были уязвимы для атак Denial-Of-Service (Отказ в обслуживании).

Важно знать, что по умолчанию клиентское программное обеспечение Подключение к удаленному рабочему столу (Remote Desktop Connection), которое также называют Клиентом служб терминалов (Terminal Services Client) или Mstsc.exe, не поддерживает сетевую проверку подлинности NLA на компьютерах Windows XP. Тем не менее для этой версии клиента удаленного рабочего стола на компьютере Windows XP SP2 можно обеспечить поддержку NLA, если загрузить и установить обновление клиента служб терминалов Terminal Services Client 6.0 для Windows XP (KB9255876), доступное па веб-сайте Microsoft.

Включение удаленного рабочего стола на компьютере с установленным ядром сервера

Конфигурация установки ядра сервера (Server Core) Windows Server 2008 не полностью поддерживает роль Службы терминалов (Terminal Services). Однако вы можете при таком типе установки включить компонент Удаленный рабочий стол (Remote Desktop) с помощью сценария Scregedit.wsf Редактора реестра ядра сервера (Server Core Registry Editor). Данный сценарий обеспечивает упрощенный способ настройки компонентов на компьютере с установленным ядром сервера Windows Server 2008.

ВНИМАНИЕ! Сценарий Scregedit.wsf

Сценарий Scregedit.wsf можно найти в папке %SystemRoot%\System32 установки ядра сервера.

Для того чтобы включить удаленный рабочий стол, запустите сценарий Scregedit.wsf с помощью сценария Cscript.exe, а затем задайте для переключателя /AR значение 0, чтобы разрешить подключения к удаленному рабочего столу. (По умолчанию переключателю /AR присвоено значение 1, запрещающее подключения к удаленному рабочего столу.) Включить удаленный рабочий стол позволяет команда:

```
Cscript.exe C:\Windows\System32\Scregedit.wsf /AR 0
```

ПРИМЕЧАНИЕ Подключение к ядру сервера с помощью удаленного рабочего стола

При подключении к компьютеру с установленным ядром, сервера с помощью компонента Удаленный рабочий стол (Remote Desktop) вы получите такой же интерфейс, который используется локально на сервере. Иными словами, подключение к удаленному рабочему столу компьютера с ядром сервера (Server Core) Windows Server 2008 не обеспечивает доступ к дополнительным графическим инструментам для управления сервером.

СОВЕТ Подготовка к экзамену

Для сдачи сертификационного экзамена 70-643 вы должны знать, как включить Удаленный рабочий стол (Remote Desktop) на компьютере с ядром сервера (Server Core) Windows Server 2008 и разрешить подключения RDP-клиентов с версией ниже RDP 6.0. Не удивляйтесь, если на экзамене этот процесс будет упомянут как «включение служб терминалов» или «включение служб терминалов для удаленного администрирования».

Установка служб терминалов

Для полной реализации служб терминалов, в отличие от реализации компонента Удаленный рабочий стол (Remote Desktop), нужно добавить роль сервера Служб терминалов (Terminal Services). Как и при любой роли сервера, самый простой способ установить службы терминалов на компьютере с полной версией

Windows Server 2008 — воспользоваться ссылкой Добавить Роли (Add Roles) в Диспетчере сервера (Server Manager).

Щелчком ссылки Добавить роли (Add Roles) запускается Мастер добавления ролей (Add Roles Wizard). На странице Выбор ролей сервера (Select Server Roles) необходимо установить флажок Службы терминалов (Terminal Services), как показано на рис. 3-3.

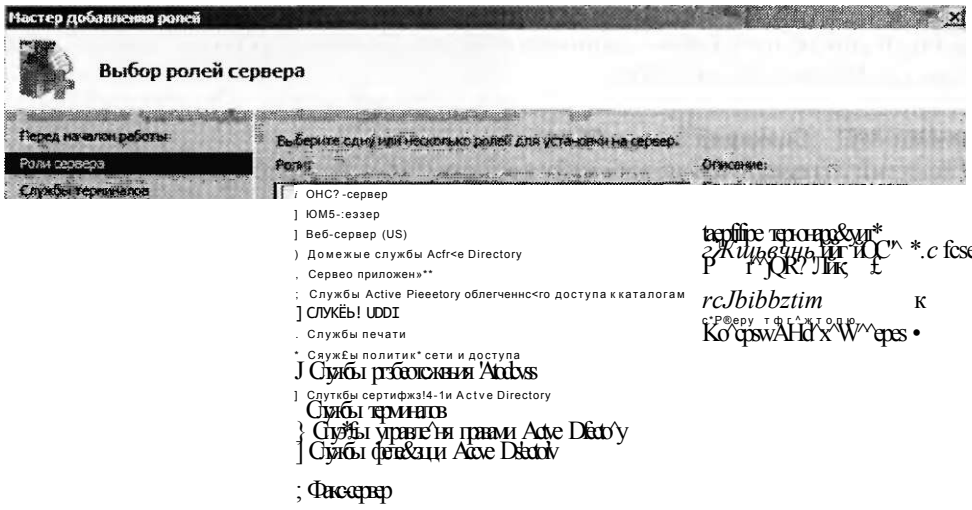


РИС. 3-3. **Добавление служб терминалов**

Щелкните кнопку Далее (Next), чтобы открыть страницу Службы терминалов (Terminal Services) мастера. На этой странице представлено короткое описание данной роли. Затем щелкните кнопку Далее (Next), и вы перейдете на страницу Выбор служб ролей (Select Role Services).

Выбор служб ролей

На странице Выбор служб ролей (Select Role Services) окна мастера добавления ролей можно выбрать следующие пять служб ролей, связанных с ролью Службы терминалов (Terminal Services).

- Сервер терминалов (Terminal Server) Эта служба ролей обеспечивает основную функциональность служб терминалов, включая RemoteApp.
- Лицензирование служб терминалов (TS Licensing) Данную службу ролей нужно установить лишь в том случае, если вы приобрели клиентские лицеи-

зии доступа служб терминалов (TS CAL) и должны активировать сервер лицензий. Для служб терминалов установлен период действия, равный 120 дням. Если вы не приобретете лицензии TS CAL и не установите их на сервере лицензий служб терминалов, то по истечении этого срока службы терминалов перестанут функционировать. (Сведения об установке и настройке лицензирования служб терминалов представлены в главе 2.)

- Посредник сеансов служб терминалов (TS Session Broker) Установите и отконфигурируйте эту службу ролей, если вы планируете реализовать службы терминалов в ферме серверов. Как уже было отмечено, эта служба ролей расширяет возможности функциональности фермы серверов, позволяя клиентам вновь подключаться к отключенным сеансам.
- Шлюз служб терминалов (TS Gateway) Установите эту службу ролей, если хотите обеспечить доступ к множеству серверов терминалов для авторизованных внешних клиентов, расположенных за пределами брандмауэра или устройства NAT (Network Address Translation).
- Веб-доступ к службам терминалов (TS Web Access) Установите эту службу ролей, если хотите обеспечить на веб-странице доступ клиентов к приложениям, развернутым через службы терминалов.

Страница Выбор служб ролей (Select Role Services) показана на рис. 3-4.

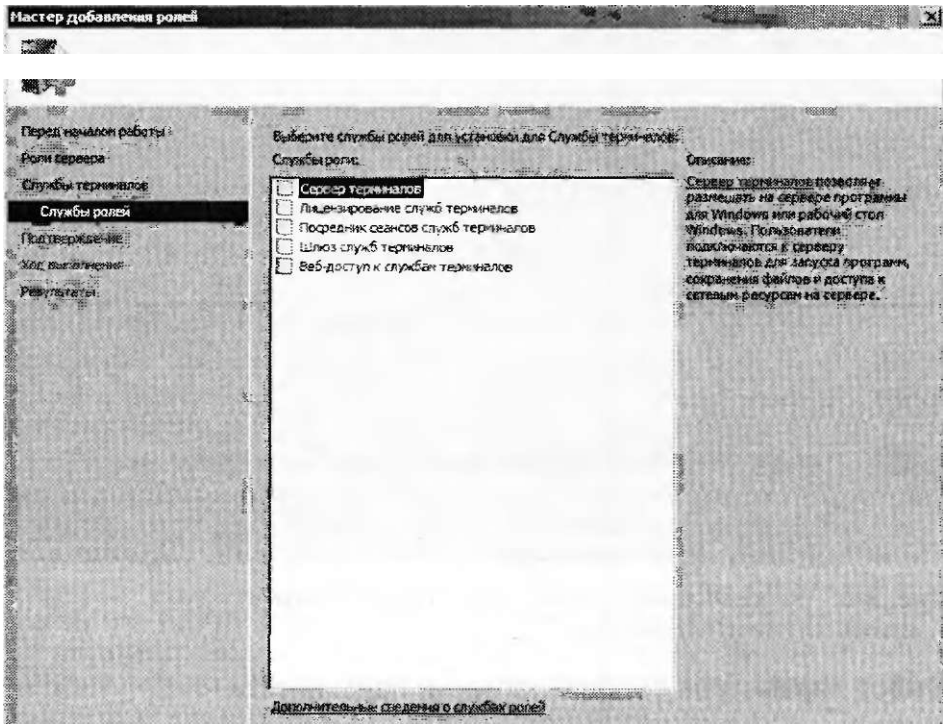


Рис. 3-4. Добавление службы ролей для роли Службы терминалов

В следующих разделах описан процесс установки служб ролей для роли Службы терминалов (Terminal Services).

Удаление приложений

После выбора роли Службы терминалов (Terminal Services) Мастер добавления ролей (Add Roles Wizard) напомнит о том, что все приложения, которые развертываются для пользователей через службы терминалов, должны быть установлены после добавления роли Службы терминалов. Если вы уже установили какие-либо приложения для развертывания, их следует удалить и установить позже (в режиме TS Install), чтобы обеспечить к ним доступ множества пользователей. Соответствующее напоминание вы видите на рис. 3-5.

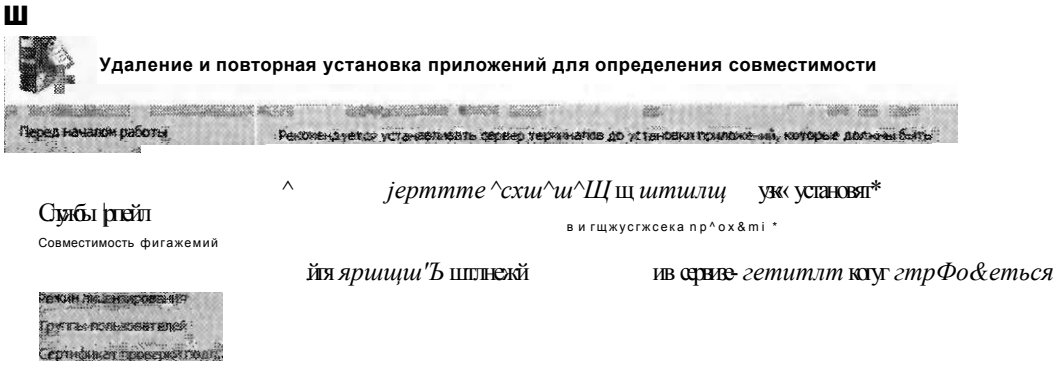


Рис. 3-5. Напоминание о необходимости переустановки приложений служб терминалов

Выбор параметров сетевой проверки подлинности

Далее нужно указать, должен ли сервер терминалов принимать подключения лишь от клиентов, которые могут выполнять поверку подлинности NLA. При выборе этого требования подключения к удаленному рабочему столу от компьютеров с операционными системами ниже Windows Vista будут блокироваться (рис. 3-6).

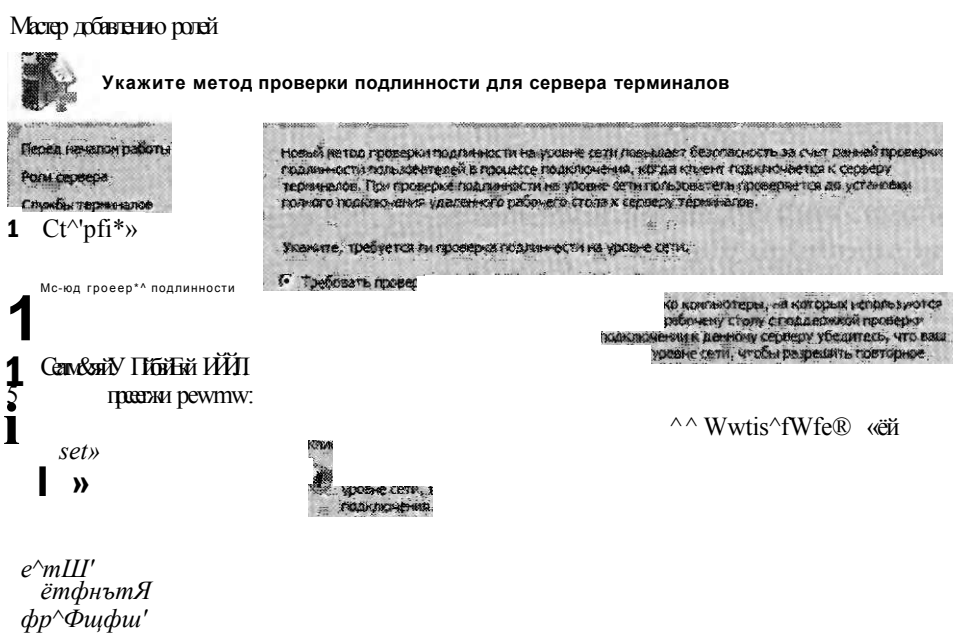


Рис. 3-6. Настройка требований к клиентской версии NLA

Определение режима лицензирования клиентского доступа

На следующей странице Мастера добавления ролей (Add Roles Wizard) нужно указать режим лицензирования TS CAL. Доступны два режима лицензирования CAL для служб терминалов.

- Режим лицензирования TS на устройство (TS Per Device CALs) Лицензирование TS на устройство являсгся перманентным и назначается для любого компьютера или устройства, которое неоднократно подключается к службам терминалов. При использовании режима лицензирования на устройство и при первом подключении к серверу терминалов клиентский компьютер или устройство по умолчанию получает временную лицензию. В случае повторного подключении при условии активации сервера лицензий и при наличии лицензий TS Per Device CAL сервер лицензий выдает клиентскому компьютеру или устройству постоянную лицензию TS Per Device CAL.
- Режим лицензирования TS на пользователя Лицензии TS Per User CAL предоставляют пользователям право доступа к службам терминалов с любого количества устройств. Лицензии TS Per User CAL не назначаются конкретным пользователям. Если вы решили воспользоваться режимом лицензирования

на пользователя, вам просто потребуется приобрести достаточное количество лицензий для всех пользователей в организации.

ПРИМЕЧАНИЕ Подготовка к экзамену
В Windows Server 2008 включено автоматическое отслеживание лицензий на устройство и на пользователя, чтобы вы могли определять количество текущих лицензий служб терминалов. В Windows Server 2003 включено лишь отслеживание лицензий на устройство.

Если вы выбрали для своей организации тип лицензий CAL, обязательно учтите ряд факторов. Во-первых, примите во внимание количество устройств и пользователей в организации. С финансовой точки зрения вполне приемлемо выбрать лицензии CAL на устройство, если в течение жизненного цикла сервера терминалов устройств будет меньше, чем пользователей. Если же пользователей в организации меньше, чем устройств, выберите лицензирование на пользователя. При этом следует учесть, как часто пользователи путешествуют и подключаются с различных компьютеров. Лицензирование на пользователя имеет смысл использовать, в частности, тогда, когда очень небольшое количество пользователей подключается к серверу терминалов с множества различных сайтов, предположим, в потребительских сетях.

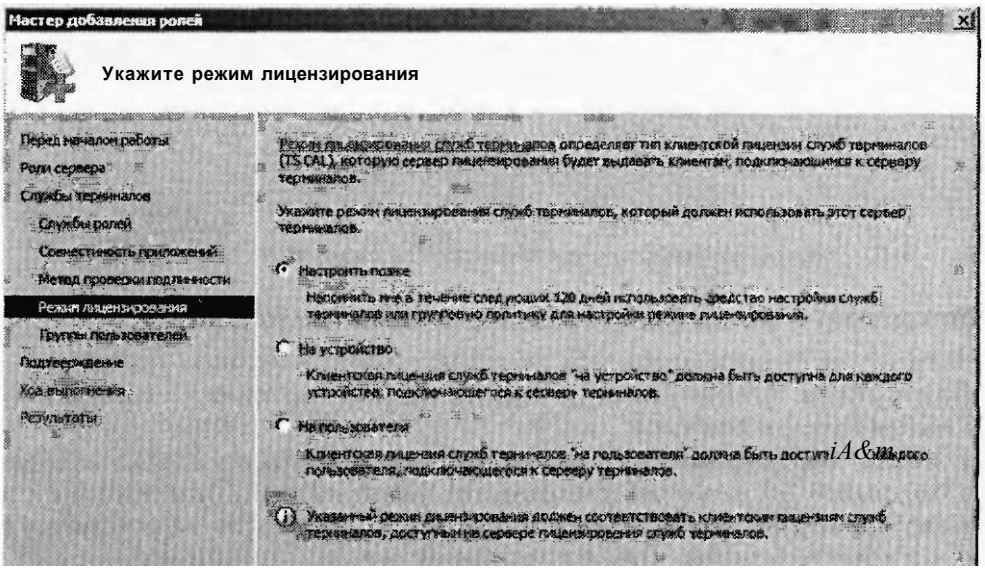


Рис. 3-7. Выбор режима лицензирования

Если вы еще не решили, какие лицензии TS CAL необходимо приобрести, имеет смысл выбрать опцию Настроить позже (Configure Later). В таком случае на приобретение лицензий TS CAL и нх установку на локально активированном сервере лицензий у вас будет 120 дней (рис. 3-7). По истечении этого срока службы терминалов перестанут функционировать.

ПРИМЕЧАНИЕ Подготовка к экзамену
Готовясь к сдаче сертификационного экзамена 70-643, вы должны понять, в чем разница между клиентскими режимами лицензирования доступа.

Авторизация пользователей

Последний этап конфигурирования состоит в выборе пользователей и групп, которым разрешен доступ через службы терминалов. Встроенной группе Пользователи удаленного рабочего стола (Remote Desktop Users) автоматически назначается право подключаться к локальному компьютеру через службы терминалов, и Мастер добавления ролей (Add Roles Wizard) просто обеспечивает возможность быстрого добавления учетных записей в эту группу. По умолчанию локальные администраторы уже являются членами этой группы (рис. 3-8).

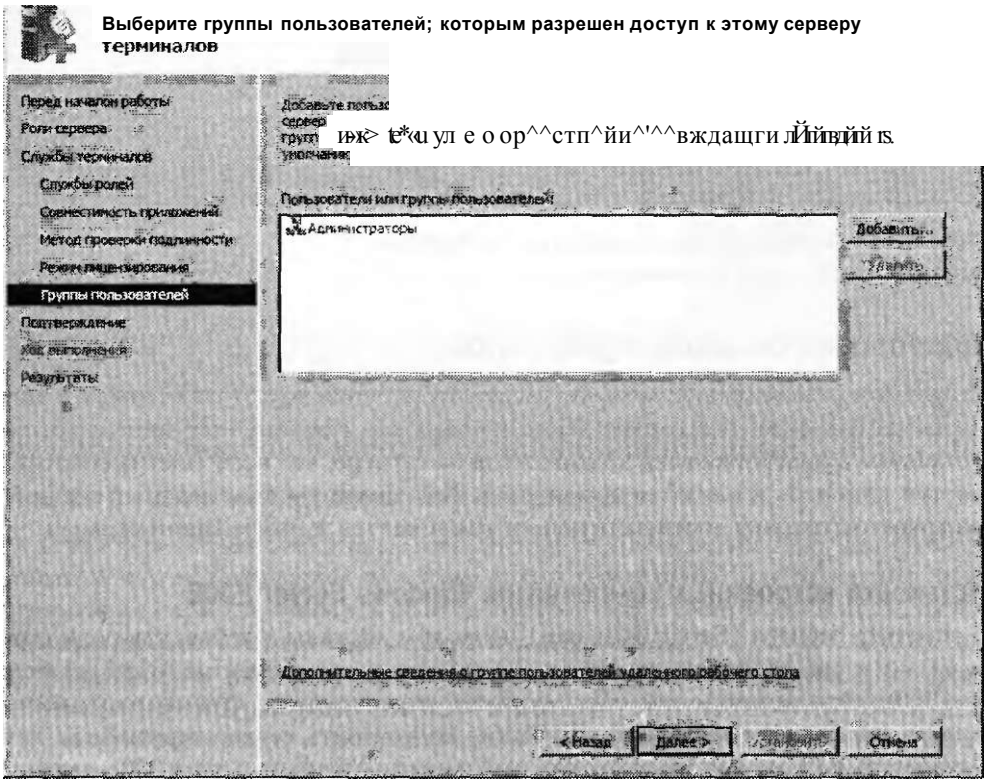


Рис. 3-8. Авторизация пользователей для служб терминалов

Выберите пользователей и подтвердите параметры, позволяющие начать установку служб терминалов (рис. 3-9).

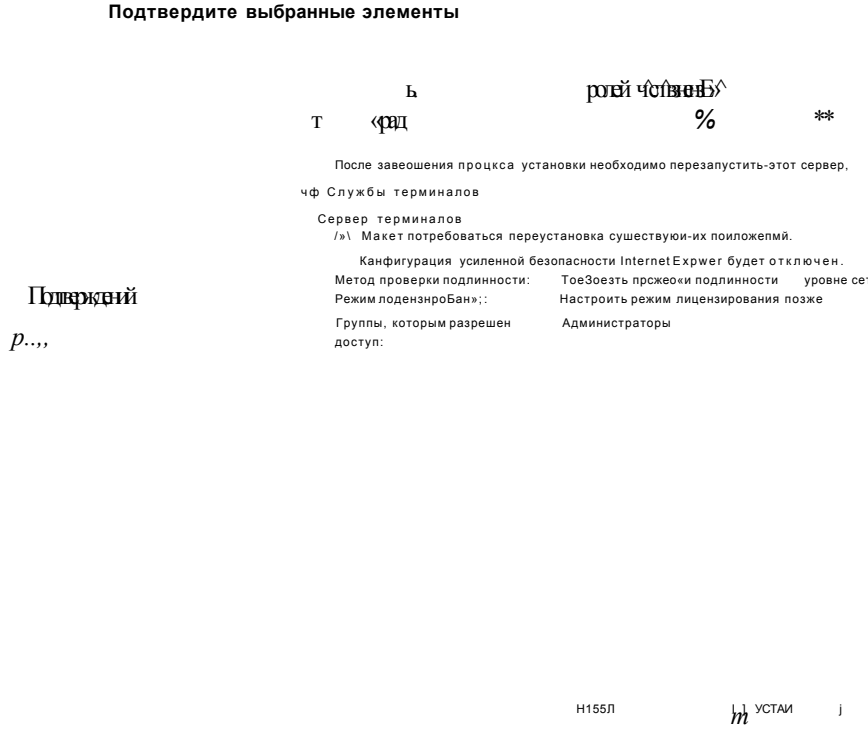


Рис. 3-9. Подтверждение элементов, выбранных для установки служб терминалов

Подготовка сервера терминалов

В процессе создания инфраструктуры осуществляется подготовка сервера к развертыванию. Если это сервер терминалов, в данном процессе производится установка и настройка всех компонентов на сервере, что позволяет обеспечить доступ клиентов к службам терминалов. Как минимум описываемый процесс включает установку соответствующих компонентов и приложений сервера.

Установка встроенных компонентов Windows Server 2008

Диспетчер сервера (Server Manager) позволяет не только добавлять роли сервера, но и устанавливать любой из 36 небольших компонентов Windows Server 2008. Эти компоненты обеспечивают определенную функциональность операционной системы Windows. Чтобы подготовить сервер терминалов для развертывания, нужно знать, какие компоненты Windows Server 2008 следует установить для обеспечения клиентских подключений к серверу терминалов.

Поскольку для удаленных пользователей доступны лишь те компоненты, которые вы установили на сервере терминалов, нужно определить потребности пользователей и функциональность, обеспечиваемую каждым компонентом. Например, если вы хотите для клиентов, подключающихся к службам терминалов, обеспечить доступ к Проигрывателю Windows Media (Windows Media Player) или интерфейсу Windows Aero, на компьютере с ролыо Службы терминалов (Terminal Services) нужно установить компонент Возможности рабочего стола (Desktop Experience).

Для того чтобы установить компонент в Диспетчере сервера (Server Manager), запустите Мастер добавления компонентов (Add Features Wizard), щелкнув ссылку Добавить компоненты (Add Features). На рис. 3-10 показан далеко не полный список компонентов, которые можно добавить с помощыо мастера.

ш

Выбор компонентов

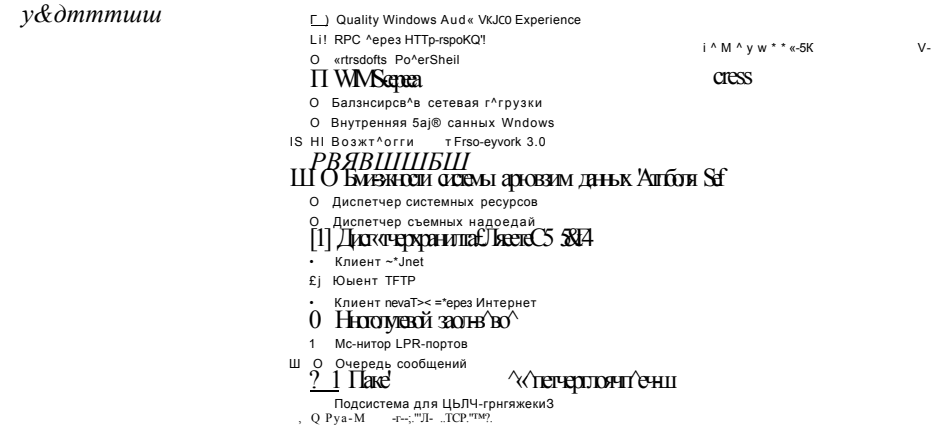


Рис. 3-10. Окно мастера добавления компонентов

Ниже перечислены некоторые компоненты Windows Server 2008, доступ к которым может потребоваться клиентам служб терминалов. Для успешного развертывания служб терминалов об этих компонентах нужно знать и пользоваться ими в процессе подготовки сервера к развертыванию.

- Возможности рабочего стола (Desktop Experience) Данный компонент устанавливает Проигрыватель Windows Media 11 (Windows Media Player 11), темы рабочего стола и фотоальбом. Он также обеспечивает доступ к графическим функциям Windows Aero, хотя последние каждый пользователь должен включать вручную.

- **Quality Windows Audio Video Experience** Платформа qWave (Quality Windows Audio Video Experience), обеспечивающая высокую производительность потокового мультимедиа.
- **Балансировка сетевой нагрузки (Network Load Balancing, NLB)** Компонент, который позволяет присоединить сервер к кластеру или ферме серверов NLB.
- **Возможности системы архивации данных Windows Server (Windows Server Backup Features)** Установка этого компонента дает администраторам возможность выполнять резервное копирование сервера терминалов во время удаленной поддержки компьютера.
- **Windows PowerShell** Оболочка командной строки PowerShell, которая представляет язык административных сценариев, встроенный в Windows Server 2008. Данный компонент можно установить для удаленного администрирования компьютера служб терминалов с помощью Windows PowerShell.
- **Управление групповой политикой (Group Policy Management)** Консоль, обеспечивающая единое средство администрирования для управления групповой политикой. Данный компонент можно установить для удаленного управления групповой политикой сервера.
- **Диспетчер системных ресурсов Windows (Windows System Resource Manager)** Административное средство WSRM, которое позволяет управлять ресурсами сервера с целью равномерного распределения рабочей нагрузки между ролями.

СОВЕТ Подготовка к экзамену

Готовясь к сертификационному экзамену 70-643, внимательно изучите все компоненты сервера. Особое внимание уделите компонентам, которые перечислены выше.

Установка приложений служб терминалов

Службы терминалов (Terminal Services) часто используются с целью развертывания единой установки приложения для множества пользователей. Развертывание приложения таким способом является идеальным решением для программ ввода данных, предназначенных для работы на одном сервере или использующих локально установленную базу данных. Тем не менее приложения можно развертывать и через службы терминалов, что позволяет снизить затраты на лицензирование, уменьшить нагрузки клиентских компьютеров, повысить эффективность работы пользователей в сеансе служб терминалов.

После выбора приложений, доступ к которым требуется обеспечить для клиентов через службы терминалов, эти приложения нужно установить таким образом, чтобы они были доступны для множества пользователей. Для этого их следует устанавливать в режиме Install служб терминалов. Программы можно установить в режиме TS Install с помощью установщика MSI, с помощью элемента Установка приложения на сервер терминалов (Install Application On Terminal Server) в панели управления либо с помощью команды *Change user/*

install или *Chgusr/install*. Более подробные сведения о режиме TS Install вы найдете в главе 4.

Проверьте себя

1. Какой компонент нужно установить на сервере терминалов, чтобы пользователи имели возможность воспроизводить аудио и видео в сеансах служб терминалов?
2. Каким количеством одновременно активных пользовательских сеансов (включая удаленные и консольные сеансы) может управлять компьютер Windows Server 2008 с компонентом Удаленный рабочий стол (Remote Desktop)?

Ответы

1. Возможности рабочего стола (Desktop Experience).
2. Двумя.

Практикум. Установка сервера терминалов

Выполняя предложенные упражнения, вы установите службы терминалов на компьютере с полной инсталляцией Windows Server 2008, а затем на компьютере с установленным ядром сервера включите удаленный рабочий стол.

Упражнение 1. Добавление и настройка роли Службы терминалов

В этом упражнении вы установите роль сервера Службы терминалов (Terminal Services) на сервере Server2.

1. Войдите на сервер Server2 в качестве администратора домена Contoso.com.
2. В окне Диспетчера сервера (Server Manager) выберите в дереве консоли узел Роли (Roles), а затем в панели справа щелкните ссылку Добавить роли (Add Roles). На странице Перед началом работы (Before You Begin) шелкните кнопку Далее (Next).
3. На странице Выбор ролей сервера (Select Server Roles) мастера добавления ролей установите флажок Службы терминалов (Terminal Services) и щелкните кнопку Далее (Next).
4. Затем на странице Службы терминалов (Terminal Services) прочитайте описание и щелкните кнопку Далее (Next).
5. Перейдя на страницу Выбор служб ролей (Select Role Services), установите флажок Сервер терминалов (Terminal Server) и опять-таки щелкните кнопку Далее (Next).
6. На странице Удаление и повторная настройка приложений для определения совместимости (Uninstall And Reinstall Applications For Compatibility) прочитайте весь текст и щелкните кнопку Далее (Next).
7. Прочитайте текст на странице Укажите метод проверки подлинности для сервера терминалов (Specify Authentication Method), выберите опцию Требовать

проверку подлинности на уровне сети (Require Network Level Authentication) и щелкните кнопку Далее (Next).

8. На странице Укажите режим лицензирования (Specify Licensing Mode) прочитайте весь текст, оставьте установленной опцию по умолчанию Настроить позже (Configure Later) и щелкните кнопку Далее (Next).
9. Прочитайте текст на странице Выберите группы пользователей, которым разрешен доступ к этому серверу (Select User Groups Allowed Access To This Terminal Server) и щелкните кнопку Далее (Next).
10. Ознакомьтесь с текстом, представленным на странице Подтвердите выбранные элементы (Confirm Installation Selections), после чего щелкните кнопку Установить (Install).
И. После завершения установки прочитайте текст на странице Результаты установки (Installation Results) и щелкните кнопку Закрыть (Close).
12. В диалоговом окне Мастер добавления ролей (Add Roles Wizard) щелкните кнопку Да (Yes), чтобы перезагрузить сервер.
13. После перезагрузки сервера вновь войдите с Server2 на Contoso.com с помощью той же учетной записи администратора. Через несколько секунд откроется страница Возобновить работу мастера настройки (Resume Configuration Wizard). На странице Результаты установки (Installation Results) щелкните кнопку Закрыть (Close).

ВНИМАНИЕ!

В Windows Server 2008 каждый раз после добавления или удаления роли сервера нужно перезагрузить компьютер. Для завершения процедуры после перезагрузки вы должны войти на сервер, используя ту же учетную запись.

14. В панели управления откройте Брандмауэр Windows (Windows Firewall).
15. Щелкните ссылку Разрешение запуска программы через брандмауэр Windows (Allow A Program Through Windows Firewall).
16. На вкладке Исключения (Exceptions) диалогового окна Параметры брандмауэра Windows (Windows Firewall Settings) проверьте, установлены ли флажки Дистанционное управление рабочим столом (Remote Desktop) и Службы терминалов (Terminal Services), и щелкните OK.
17. Закройте все открытые окна и переходите к выполнению упражнения 2.

Упражнение 2. Тестирование подключения к службам терминалов

В этом упражнении вы протестируете конфигурацию служб терминалов на Server2, подключившись к ним через подключение к удаленному рабочему столу на Serverl.

1. Войдите на сервер Serverl как администратор домена Contoso.com.
2. В меню Пуск (Start) щелкните команду Выполнить (Run).
3. В окне Выполнить (Run) введите команду mstsc и нажмите клавишу Enter. Откроется окно Подключение к удаленному рабочему столу (Remote Desktop Connection).

ПРИМЕЧАНИЕ Подготовка к экзамену
Для сдачи сертификационного экзамена 70-643 нужно знать команду Mstsc.

4. В текстовое поле Компьютер (Computer) окна Подключение к удаленному рабочему столу (Remote Desktop Connection) введите *server2.contoso.com* и нажмите клавишу Enter. Откроется окно Безопасность Windows (Windows Security).
5. В указанном окне введите учетные данные доменного администратора. Введите пользовательское имя в формате соп1ояо\имя_пользователя. Через несколько секунд будет установлено подключение к Server2. На рабочем столе Serverl рабочий стол Server2 будет обозначен желтым маркером server2.contoso.com.
6. На Server2 в меню Пуск (Start) сеанса подключения к удаленному рабочему столу завершите подключение.

Упражнение 3. Включение удаленного рабочего стола на компьютере с установленным ядром сервера Windows Server 2008

В данном упражнении вы включите удаленный рабочий, стол на компьютере Corel и протестируете подключение.

ПРИМЕЧАНИЕ Serverl и Server2
Для выполнения этого упражнения требуется Serverl. Если вы используете виртуальные машины и вам не хватает оперативной памяти, выключите машину Server2.

1. Войдите на сервер Corel как администратор домена Contoso.com.
2. В командную строку введите команду *cd C:\Windows\System32.*
3. Затем в командную строку введите команду *cscript csregedit.wsf/AR/v,* отображающую текущее состояние параметра реестра fDenyTSConnections. Если ему присвоено значение 1, значит, на локальном компьютере запрещены входящие подключения к удаленному рабочему столу.
4. Введите команду *cscript scregedit.wsf/AR 0.*
5. Для проверки измененного параметра введите команду *cscript scregedit.wsf/AR/v.* В результатах будет указано, что параметру реестра fDenyTSConnections присвоено значение 0.
6. Чтобы разрешить прием подключений клиентов с версией RDP ниже 6.0 или клиентов с версией Windows не выше XP, введите команду *cscript scregedit.wsf/CSO.*
7. Проверьте параметр путем ввода команды *cscript scregedit.wsf/CS/v.*
8. В результатах будет указано, что параметру RDP-Tcp UserAuthentication теперь присвоено значение 0. Этот параметр разрешает подключения ранних версий клиентов удаленного рабочего стола. Введите команду *netsh firewall show service,* и будут отображены исключения брандмауэра, созданные для различных служб на сервере Corel. В данном случае в результатах будет указано, что для службы Удаленный рабочий стол (Remote Desktop) в профиле домена создано (включено) исключение брандмауэра.

9. С сервера Serverl войдите на Contoso.com как администратор домена.
10. В окне Выполнить (Run) введите команду *mstsc* и нажмите клавишу Enter. Откроется окно Подключение к удаленному рабочему столу (Remote Desktop Connection).
11. После этого в текстовое поле Компьютер (Computer) введите *corel.contoso.* сот и щелкните кнопку Подключить (Connect).
12. Перейдя в окно Безопасность Windows (Windows Security), введите пользовательское имя и пароль администратора домена. Имя должно быть в формате соп1о8о\имя_пльзователя.
13. В окне Безопасность Windows (Windows Security) щелкните ОК. Через несколько секунд будет установлено подключение к удаленному рабочему столу Corel. В окне подключения отобразится тот же рабочий стол, который вы видите, подключаясь к серверу Corel локально.
14. На Serverl введите в командную строку сеанса подключения к удаленному рабочему столу команду *logoff.* Сеанс подключения к удаленному рабочему столу на Serverl будет закрыт.
15. Наконец, на Corel введите в командную строку команду *shutdown /p,* и компьютер будет выключен.

Резюме

- Службы терминалов (Terminal Services) дают возможность пользователям устанавливать сеанс удаленного рабочего стола на удаленном компьютере с установленными службами терминалов.
- Компоненты Службы терминалов (Terminal Services) и Удаленный рабочий стол (Remote Desktop) совместно используют основные службы и функции. Наиболее существенное различие между этими двумя компонентами состоит в том, что при включении удаленного рабочего стола Windows Server 2008 разрешает одновременно запускать только два сеанса удаленного рабочего стола (включая локальный консольный сеанс). Для служб терминалов таких ограничений не существует.
- В Windows Server 2008 службы терминалов включают множество новых и важных компонентов, в том числе Шлюз служб терминалов (TS Gateway), RemoteApp и Веб-доступ к службам терминалов (TS Web Access) — они детально описаны в главе 4.
- Для установки служб терминалов на компьютере Windows Server 2008 нужно добавить роль сервера Службы терминалов (Terminal Services).
- Службы терминалов требуют лицензирования клиентского доступа (CAL) для всех подключающихся пользователей или для всех подключающихся устройств. Если лицензии служб терминалов не будут приобретены и установлены, службы терминалов перестанут функционировать через 120 дней.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных в ходе занятия 1. Эти вопросы представлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы
Ответы и пояснения к каждому их варианту размещены в разделе «Ответы» в конце книги.

1. Вы хотите включить удаленный рабочий стол на компьютере с установленным ядром сервера Windows Server 2008 и разрешить серверу принимать подключения клиентов с версиями RDP ниже 6.0. Какие команды следует использовать? (Укажите две команды.)
   A. cscript scregedit.wsf/AR 0.
   Б. *cscript scregedit.wsf/AR 1.*
   B. cscript scregedit.wsf/CS 0.
   Г. *cscript scregedit.wsf/CS 1.*
2. Вы как один из 75 IT-консультантов компании Contoso.com вместе со своими коллегами должны обеспечить сетевую поддержку более чем для 150 бизнесменов города. Ваша компания реализует бизнес-процесс, в котором консультанты должны подключаться к серверу приложений в сети Contoso.com, выполняя роль потребителей. Для подключения к серверу приложений Contoso.com консультанты должны установить на компьютерах потребителей Windows XP или Windows Vista подключение к удаленному рабочему столу. Вас попросили выяснить, нужны ли компании новые клиентские лицензии доступа (CAL) для служб терминалов. Какие действия лучше всего предпринять для выполнения требований организации?
   А. Использовать на сервере приложений Удаленный рабочий стол для администрирования RDA (Remote Desktop for Administration) и приобрести лицензии CAL на пользователя.
   Б. Использовать на сервере приложений Удаленный рабочий стол для администрирования RDA и не приобретать лицензии CAL.
   В. Установить на сервере приложений Службы терминалов (Terminal Services) и приобрести лицензии CAL на устройство.
   Г. Установить на сервере приложений Службы терминалов (Terminal Services) и приобрести лицензии CAL на пользователя.

Занятие 2. **Настройка служб терминалов**

Консоль Конфигурация служб терминалов (Terminal Services Configuration) является основным средством, используемым для настройки роли Службы терминалов (Terminal Services). Опции сервера, доступные в этой консоли, изначально влияют на пользовательское окружение при подключении к локальному серверу терминалов. Другие доступные здесь опции связаны с лицензированием сервера и балансировкой нагрузки. После обсуждения всех опций и компонентов, настраиваемых в консоли Конфигурация служб терминалов (Terminal Services Configuration), мы на этом занятии рассмотрим дополнительные опции конфигурации, доступные в групповой политике, в частности опции перенаправления принтеров.

Изучив материал этого занятия, вы сможете:

- S (Сконфигурировать опции сервера терминалов.
  Настроить балансировку нагрузки служб терминалов.
  Установить и отконфигурировать сервер лицензий служб терминалов.

Расчетная продолжительность занятия составляет 50 мин.

Конфигурация служб терминалов

Консоль Конфигурация служб терминалов (Terminal Services Configuration, TSC) предназначена для управления параметрами, которые влияют на всех пользователей, подключающихся к серверу терминалов, или всех пользователей, применяющих определенные типы подключений. Например, вы можете использовать консоль TSC для назначения уровня шифрования всех сеансов служб терминалов, настройки графического разрешения сеансов, а также для запрета пользователям запускать более одного сеанса. Консоль TSC показана на рис. 3-11.

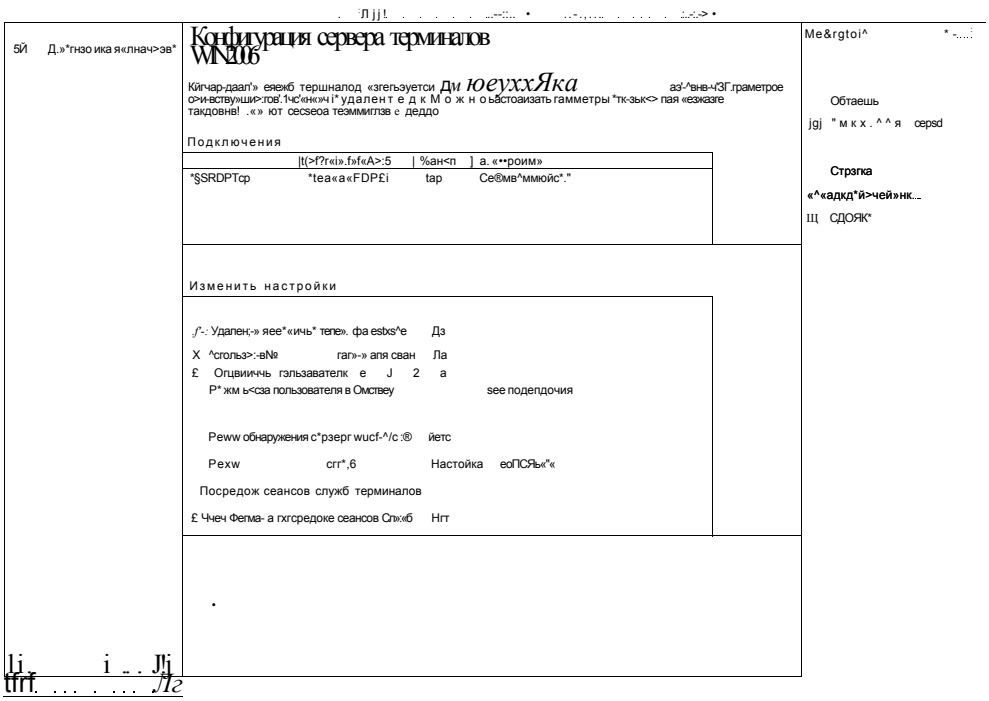


Рис. 3-11. Консоль Конфигурация служб терминалов (Terminal Services Configuration)

Консоль TSC содержит две основные области: раздел свойств подключений RDP-Tcp и область модификации параметров сервера терминалов. Доступные здесь опции описаны в последующих разделах.

Настройка свойств подключения RDP-Tcp

Свойства подключений позволяют настроить поведение всех сеансов служб терминалов, инициированных через определенные транспортные протоколы (например, RDP через TCP) пли через определенные сетевые адаптеры па сервере терминалов. По умолчанию можно конфигурировать лишь одно подключение (RDP-Tcp). Свойства, настроенные для этого подключения, применяются в сеансах RDP на всех локальных сетевых адаптерах компьютера. Помимо подключения по умолчанию можно создавать новые подключения для сторонних транспортных протоколов, а также для конкретных адаптеров.

Для сред, использующих лишь встроенную функциональность Windows Server 2008, подключение RDP-Tcp будет единственным; в диалоговом окне RDP-Tcp Свойства (RDP-Tcp Properties) представлены ключевые опции конфигурации для всего сервера.

Чтобы открыть свойства подключения RDP-Tcp, в области Подключения (Connections) консоли Конфигурация служб терминалов (Terminal Services Configuration) правой кнопкой мыши щелкните подключение RDP-Tcp и выполните команду Свойства (Properties). Откроется диалоговое окно RDP-Tcp Свойства (RDP-Tcp Properties), показанное на рис. 3-12.

Рис. 3-12. Свойства подключения RDP-Tcp

Ниже описаны опции, конфигурируемые на каждой из восьми вкладок диалогового окна свойств.

СОВЕТ Подготовка к экзамену

Изучите все параметры, представленные па восьми вкладках диалогового окна свойств подключения RDP-Tcp.

Вкладка Общие

На вкладке Общие (General) параметры можно модифицировать в трех областях безопасности: уровень безопасности, уровень шифрования, проверка подлинности на уровне сети. Далее эти три области описаны более подробно.

Уровень безопасности (Security Layer) Все RDP-подключения шифруются автоматически. Параметры уровня безопасности определяют тип шифрования, используемый для этих подключений служб терминалов. Доступны три опции уровня безопасности, а именно Уровень безопасности RDP (RDP Security Layer), SSL (TLS 1.0) и Согласование (Negotiate).

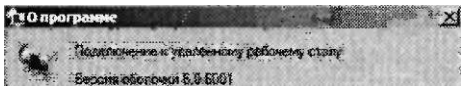
- Уровень безопасности RDP (RDP Security Layer) ограничивает шифрование методами, включенными в протокол удаленного рабочего стола. Преимущества использования этой опции заключаются в том, что она не требует дополнительной конфигурации и обеспечивает высокий стандарт производительности. Недостаток состоит в том, что ни для каких типов клиентов на сервере не обеспечивается проверка подлинности. Хотя RDP 6.0 может обеспечить проверку подлинности клиентов системы не ниже Windows Vista, клиенты служб терминалов версии не выше Windows XP не поддерживают проверку подлинности на сервере. Если вы хотите разрешить RDP-клиентам Windows XP перед установлением подключения проходить проверку подлинности на сервере терминалов, следует отконфигурировать шифрование SSL.
- Опция SSL (TSL 1.0) по сравнению с RDP-подключением обеспечивает как минимум два преимущества. Во-первых, она позволяет производить более строгое шифрование. Во-вторых, при использовании этой опции на сервере можно выполнять проверку подлинности клиентских версий RDP ниже 6.0. Таким образом, SSL поддерживает возможность проверки подлинности клиентов Windows XP. Однако установка этой опции может привести и к ряду отрицательных проявлений. Шифрование SSL требует наличия сертификата компьютера и для шифрования, и для проверки подлинности. Для повышения уровня безопасности следует получить действительный сертификат, изданный доверенным центром сертификации CA. Этот сертификат должен храниться в хранилище сертификатов на сервере терминалов. Еще один недостаток SSL состоит в том, что при проведении строгого шифрования производительность по сравнению с другими RDP-подключениями снижается.
- При выборе опции Согласование (Negotiate) сервер терминалов будет использовать безопасность SSL лишь при условии, что SSL поддерживается клиентом и сервером. В противном случае применяется традиционное шифрование RDP. Опция Согласование (Negotiate) назначается по умолчанию.

Уровень шифрования (Encryption Level) В этой области вкладки Общие (General) можно определить уровень алгоритма шифрования, используемого для RDP-подключений. По умолчанию задан уровень Совместимый с клиентским (Client Compatible), что предполагает максимально строгий ключ, поддерживаемый клиентским компьютером. Вы также можете использовать уровни FIPS-совместимый (FIPS Compliant) (самый строгий уровень), Высокий (High) и Низкий (Low).

Проверка подлинности на уровне сети (Network Level Authentication) Если установить флажок Разрешать подключения только от компьютеров с удаленным рабочим столом с проверкой подлинности на уровне сети (Allow Connections Only From Computers Running Remote Desktop With Network Level

Authentication), то к серверу терминалов смогут подключаться лишь клиенты с поддержкой NLA.

Чтобы определить, поддерживает ли версия клиента RDC (Remote Desktop Connection) проверку подлинности на уровне сети, запустите RDC-клпент, щелкните значок в левом верхнем углу диалогового окна Подключение к удаленному рабочему столу (Remote Desktop Connection), а затем щелкните опцию О программе (About). В диалоговом окне О программе (About Remote Desktop Connection), показанном на рис. 3-13, найдите фразу «Поддерживается проверка подлинности на уровне сети» (Network Level Authentication Supported).



•ЗЙ?-
яривфиг *тютювщ* из *у.*

Рис. 3-13. Проверка поддержки NLA

Вкладка Параметры входа в систему

Вкладка Параметры входа в систему (Logon Settings), показанная на рис. 3-14, позволяет конфигурировать всех клиентов служб терминалов, чтобы они использовали одно предварительно определенное пользовательское имя и пароль. Таким образом, общие учетные данные позволяют пользователям подключаться к серверу терминалов, не предоставляя никаких реквизитов. Эту опцию удобно использовать в тестовых средах и на общественных терминалах.

'йф^лкяяй* L temm itmmi .5 Ее
а всастж?

г

Л В

** 1 ffcmWHWTb

Рис. 3-14. Параметры входа в систему служб терминалов

Если выбрать опцию Всегда требовать пароль (Always Prompt For Password), то перед подключением пользователь должен будет ввести хотя бы пароль.

Вкладка Сеансы

Вкладка Сеансы (Sessions) предназначена для управления временем ожидания сеансов сервера терминалов. В частности, вы можете выбрать параметры времени ожидания отключенного сеанса, указать временные ограничения активного и бездействующего сеанса, а также указать, какие действия должны предприниматься в случае превышения ограничений или разрыва подключения.

По умолчанию указанные параметры определены не в этом диалоговом окне свойств RDP-Tcp, а в свойствах учетных записей домена. Чтобы заменить эти определяемые пользователем параметры, установите флажок Заменить параметры пользователя (Override User Settings), как показано на рис. 3-15, и задайте параметры для следующих политик.

- Завершение отключенного сеанса (End A Disconnected Session) Этот параметр устанавливает автоматическое завершение отключенного сеанса.
- Ограничение активного сеанса (Active Session Limit) Определяет продолжительность активного сеанса перед автоматическим отключением.
- Ограничение бездействующего сеанса (Idle Session Limit) Определяет продолжительность бездействующего сеанса перед автоматическим отключением.
- При превышении ограничений или разрыве подключения (When Session Limit Is Reached Or Connection Is Broken) Устанавливает автоматическое завершение или отключение сеанса пользователя в случае превышения ограничений или разрыва подключения.

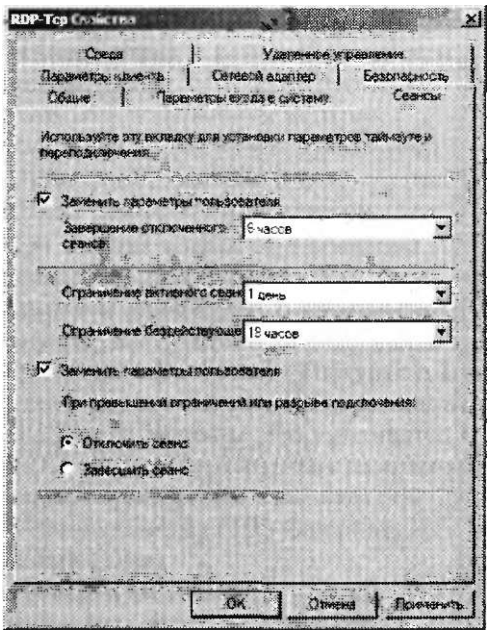


Рис. 3-15. Параметры времени ожидания и переподключения

Вкладка Среда

На вкладке Среда (Environment), представленной па рис. 3-16, можно указать, следует ли при запуске сеанса разрешать автоматический запуск начальных программ, определенных в профиле пользователя. Здесь также можно указать программу, которая будет запускаться для всех пользователей, подключающихся к локальному серверу терминалов с помощью сеансов удаленного рабочего стола.

Рис. 3-16. Параметры запуска начальных программ

Вкладка Удаленное управление

Удаленное управление в Службах терминалов (Terminal Services) позволяет администратору наблюдать за пользовательским сеансом служб терминалов и взаимодействовать с ним. По умолчанию свойства, определяющие поведение данной функции, назначаются для каждого пользователя в диалоговом окне свойств учетной записи. (Эти свойства определяют параметры наблюдения за пользовательскими сеансами служб терминалов или управления ими.) Вкладка Удаленное управление (Remote Control) позволяет управлять параметрами этой функции для каждого сервера (рис. 3-17).

По умолчанию параметры пользовательской учетной записи позволяют администратору взаимодействовать с сеансом служб терминалов еще одного пользователя, но только с его согласия. Однако на вкладке Удаленное управление (Remote Control) диалогового окна DRP-Tcp Свойства (RDP-Tcp Properties) можно разрешить администраторам вступать во взаимодействие с пользовательскими сеансами с согласия пользователей или без такового или же только

просматривать эти сеансы. Вы также можете установить для администраторов запрет на наблюдение за сеансами других пользователей и взаимодействие с ними.

ПРИМЕЧАНИЕ Удаленное управления из удаленного сеанса
Функции удаленного управления можно использовать только в сеансе RDP. Если администратор локально войдет на сервер терминалов, удаленное управление будет отключено.

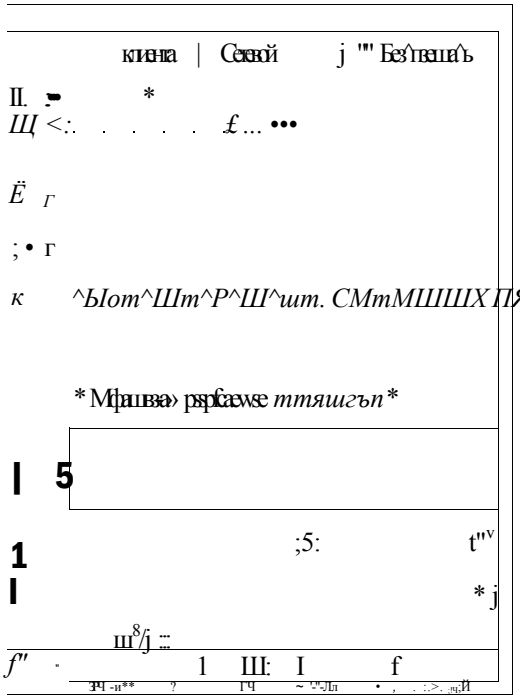


Рис. 3-17. Параметры удаленного управления

Вкладка Параметры клиента

На вкладке Параметры клиента (Client Settings), показанной на рис. 3-18, можно отконфигурировать перенаправление определенных компонентов пользовательского интерфейса.

В области Глубина цвета (Color Depth) можно определить глубину цвета, передаваемого клиенту с сервера терминалов. По умолчанию указана глубина, равная 16 бит, однако этот показатель можно изменить. При повышении качества цветопередачи RDP-подключений внешний вид окон улучшается за счет производительности.

В области Перенаправление - Отключить следующие возможности (Redirection - Disable The Following) можно определить компоненты, которые не будут перенаправлены клиенту. Преимущество отключения перенаправления состоит в повышении производительности, однако оно достигается за счет от-

ключения отдельных компонентов, обеспечивающих определенную функциональность.

- Диск (Drive) Если установить этот флажок, локальные диски клиента нельзя будет включить в подключение служб терминалов. (Для включения дисков нужно сбросить этот флажок и выбрать опцию Устройства (Drives), представленную на вкладке Локальные ресурсы (Local Resources) клиентского окна Подключение к удаленному рабочему столу (Remote Desktop Connection).

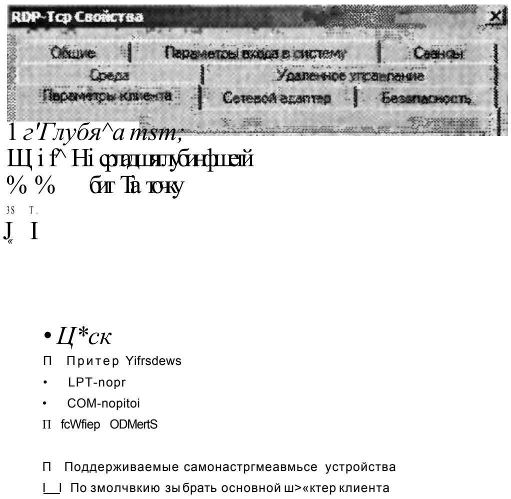


Рис. 3-18. Параметры клиента

Принтер Windows (Windows Printer) При выборе этой опции к локальным принтерам клиента нельзя будет получать доступ в подключении служб терминалов. Однако пользователь все же сможет подключиться к клиентскому принтеру из командной строки, сопоставив порты LPT или COM.

LPT-порт (LPT Port) Если установить этот флажок, пользователям будет запрещено сопоставлять подключение LPT-принтеру.

COM-порт (COM Port) Блокировка подключений сеанса служб терминалов к COM-устройствам клиентского компьютера.

Буфер обмена (Clipboard) При выборе этой опции пользователям будет запрещено вырезать и копировать данные в сеансе RDP-подключения к службам терминалов и вставлять их в локальный сеанс на клиентском компьютере. Отключение перенаправления буфера обмена для медленных подключений может помочь устранить зависания экрана.

Аудио (Audio) Если данный флажок установлен, передача аудиоданных с удаленного рабочего стола на клиентский компьютер запрещена. Это единственная опция, используемая по умолчанию.

- Поддерживаемые самонастраиваемые устройства (Supported Plug And Play Devices) Если установить этот флажок, перенаправление локальных самонастраиваемых устройств клиента в сеанс служб терминалов будет запрещено.
- По умолчанию выбрать основной принтер клиента (Default To Main Client Printer) При активизации данной опции принтер, по умолчанию назначенный клиенту служб терминалов, будет запрещено использовать как принтер сеанса служб терминалов.

Вкладка Сетевой адаптер

На этой вкладке подключение RDP-Tcp можно ограничить прослушиванием лишь на одном конкретном сетевом адаптере. Здесь же можно ограничить количество подключений, разрешенных сервером терминалов. По умолчанию количество подключений пе ограничено (рис. 3-19).

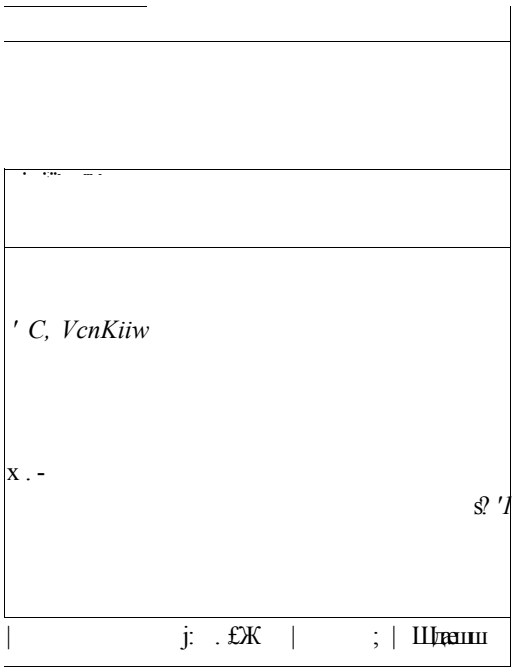


Рис. 3-19. Параметры сетевого адаптера

Вкладка Безопасность

На вкладке Безопасность (Security) можно указать пользовательские разрешения для всех RDP-подключений к серверу терминалов (рис. 3-20). Ее не рекомендуется использовать для настройки пользовательского доступа к службам терминалов; настройку следует выполнять в группе Пользователи удаленного рабочего стола (Remote Desktop Users). 11а этой вкладке для Служб терминалов (Terminal Services) необходимо определить пользователей с административной привилегией Полный доступ (Full Control).

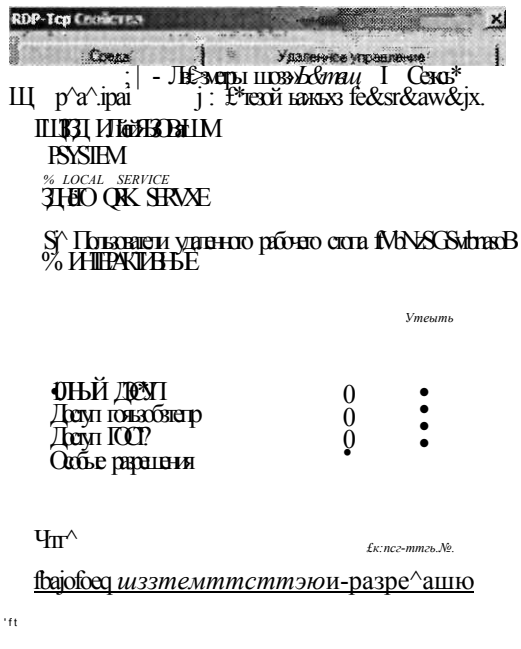


Рис. 3-20. Параметры безопасности подключений RDP-Tcp

Настройка свойств сервера служб терминалов

Помимо диалогового окна RDP-Tcp Свойства (RDP-Tcp Properties) консоль Конфигурация служб терминалов (Terminal Services Configuration) также позволяет конфигурировать службы терминалов в области Изменить настройки (Edit Settings). Эти параметры применяются на уровне всего сервера терминалов. В отличие от DRP-Tcp и других параметров подключении, данные параметры нельзя конфигурировать лишь для одного транспортного протокола или отдельного сетевого адаптера.

В области Изменить настройки (Edit Settings) представлены итоги по семи опциям сервера терминалов в трех категориях Общие (General), Лицензирование (Licensing) и Посредник сеансов служб терминалов (TS Session Broker). Чтобы изменить указанные параметры, дважды щелкните любой из них — откроется диалоговое окно Свойства (Properties) с тремя вкладками, названия которых соответствуют названиям категории. Эти вкладки описаны в последующих разделах.

Вкладка Общие

На вкладке Общие (General) можно отконфигурировать функции входа пользователей.

- Удаление временных папок при выходе (Delete Temporary Folders On Exit) Эта опция включена по умолчанию, прп выходе пользователя из сеанса служб терминалов временные файлы удаляются. Удаление временных

данных таким способом снижает производительность системы, зато повышает уровень конфиденциальности, поскольку пользователи не могут получать доступ к данным других пользователей.

Указанный параметр функционирует лишь при использовании временных папок для сеанса.

- **Использовать временные папки для сеанса (Use Temporary Folders Per Session)** Эта опция включена по умолчанию и предписывает создание новой папки временных данных в каждом пользовательском сеансе. Если этот флажок сбросить, временные данные будут совместно использоваться всеми активными сеансами. Совместное использование временных данных может содействовать повышению производительности за счет снижения конфиденциальности.
- **Ограничить пользователя единственным сеансом (Restrict Each User To A Single Session)** Данный флажок установлен по умолчанию, и каждому пользователю разрешен вход лишь в один сеанс сервера терминалов. Например, если локально войти на сервер с использованием встроенной учетной записи Администратор (Administrator), то на этот компьютер нельзя будет войти с помощью подключения к удаленному рабочему столу и той же учетной записи администратора, пока не будет выполнен локальный выход с сервера.

  Требование выйти из одного сеанса перед началом другого предотвращает возможные потери данных в пользовательском профиле. Кроме того, эта опция предотвращает простой сеансов, занимающих ресурсы сервера.
- **Режим входа пользователя в систему (User Logon Mode)** Параметры, задаваемые в этой области, запрещают вход новых пользователей на сервер терминалов, например перед запланированным отключением. По умолчанию установлена опция Разрешить все подключения (Allow All Connections). Чтобы запретить новым пользователям подключаться к серверу терминалов, нужно установить опцию Разрешить переподключения, но запретить новые попытки входа (Allow Reconnections, But Prevent New Logons). А для того чтобы запретить пользователям подключаться к серверу до перезагрузки сервера, можно воспользоваться опцией Разрешить переподключения, но запретить новые попытки входа до перезагрузки сервера (Allow Reconnections, But Prevent New Logons Until The Server Is Restarted). Отметим, что ни одна из указанных опций не предписывает завершение сеанса. Если вам нужно перезагрузить сервер, эти сеансы, возможно, придется завершать вручную, как описано в главе 4.

  Вкладка Общие (General) показана на рис. 3-21.

ПРИМЕЧАНИЕ Подготовка к экзамену

Три опции, представленные в области Режим входа пользователя в систему (User Logon Mode), являются новыми параметрами Windows Server 2008. По этой причине на сертификационном экзамене вам может попасться как минимум один вопрос по ним. Кроме того, отметим, что эти параметры предотвращают вход новых пользователей в так называемом режиме drain.

Рис. 3-21. Параметры входа пользователей в систему

Вкладка Лицензирование

Вкладка Лицензирование (Licensing), показанная на рис. 3-22, позволяет настроить две функции лицензирования сервера терминалов: режим лицензирования служб терминалов и режим обнаружения сервера лицензирования.

Рис. 3-22. Параметры лицензирования служб терминалов

- **Режим лицензирования служб терминалов** Данный режим можно задать во время установки роли Службы терминалов (Terminal Services) или же несколько позже. Чтобы задать или отменить режим лицензирования после установки, в области Режим лицензирования служб терминалов (Specify The Terminal Services Licensing Mode) выберите опцию На устройство (Per Device) либо На пользователя (Per User),
- м **Режим обнаружения сервера лицензирования** Режим обнаружения представляет метод, с помощью которого сервер терминалов связывается с сервером лицензирования для получения лицензий TS CAL. По умолчанию задан режим обнаружения Автоматически обнаруживать сервер лицензирования (Automatically Discover A License Server). В режиме автоматического обнаружения сервера лицензирования сервер терминалов пытается связаться с любым сервером лицензирования, опубликованным в службе каталогов Active Directory или установленным на контроллерах локального домена. Вы также можете задать сервер лицензирования вручную, выбрав опцию Использовать указанные серверы лицензирования (Use The Specified License Servers) и введя в текстовом поле имя или адрес сервера лицензирования.

ПРИМЕЧАНИЕ Подготовка к экзамену
В оснастке Active Directory — Пользователи и компьютеры (Active Directory — Users And Computers) содержится группа локальной безопасности домена Компьютеры сервера терминалов (Terminal Server Computers). Для ограничения коммуникаций серверов терминалов с серверами лицензирования в домене можно изменить членство в этой группе.

Вкладка Посредник сеансов служб терминалов

Вкладка Посредник сеансов служб терминалов (TS Session Broker Setting), показанная на рис. 3-23, используется для настройки параметров сервера посредника сеансов служб терминалов в ферме. Посредник сеансов служб терминалов позволяет балансировать нагрузку серверов в ферме, направляя новые пользовательские сеансы на сервер, где обрабатывается меньше сеансов. Посредник сеансов служб терминалов также обеспечивает автоматические переподключения к отключенным сеансам на соответствующем сервере в ферме.

ПРИМЕЧАНИЕ Посредник сеансов служб терминалов и Active Directory
Сервер, на котором устанавливается посредник сеансов служб терминалов, должен быть членом домена.

Для настройки фермы серверов терминалов нужно вначале службу ролей Посредник сеансов служб терминалов (TS Session Broker) установить на сервер, где планируется производить наблюдение за пользовательскими сеансами всей фермы. Таким образом, сервер станет посредником сеансов служб терминалов. Затем в локальную группу Компьютеры каталогов сеансов (Session Directory Computers) на сервере посредника сеансов служб терминалов фермы нужно добавить серверы терминалов. И наконец, серверы терминалов необходимо

присоединить к ферме, настроив соответствующие опции на описываемой вкладке.

- **Присоединиться к ферме в посреднике сеансов служб терминалов (Join A Farm In TS Session Broker)** Установите данный флажок при необходимости добавить локальный сервер в ферму и обеспечить доступ к остальным опциям конфигурации.

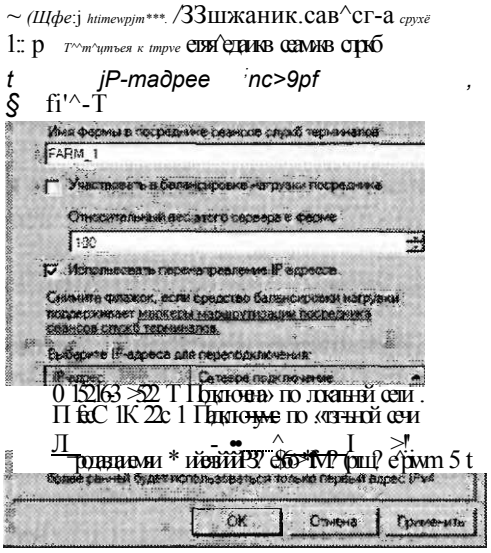


Рис. 3-23. Балансировка нагрузки служб терминалов

- **Имя или IP-адрес сервера посредника сеансов служб терминалов (TS Session Broker Server Name Or IP Address)** В это текстовое поле нужно ввести имя или IP-адрес сервера, на котором установлен посредник сеансов служб терминалов.
- **Имя фермы в посреднике сеансов служб терминалов (Farm Name In TS Session Broker)** В данное текстовое поле следует ввести имя фермы, которое будет совместно использоваться всеми ее серверами. Это DNS-имя будет использоваться клиентами для подключения к ферме серверов терминалов. (На соответствующем DNS-сервере нужно добавить множество записей DNS, отвечающих имени фермы, которые будут определять IP-адреса каждого члена фермы.)
- **Участвовать в балансировке нагрузки посредника (Participate In Session Broker Load-Balancing)** Установите этот флажок, чтобы откоифигурировать участие локального сервера в балансировке нагрузки, включенной посредником сеансов служб терминалов.
- **Относительный вес этого сервера в ферме (Relative Weight Of This Server In The Farm)** Данный параметр используется для назначения мощным серверам большего количества пользовательских сеансов и снижения таким образом нагрузки на менее мощные серверы. Например, если вы назначите

мощному серверу вес 200, а более слабому — вес 100, то первый сервер будет принимать в два раза больше сеансов, чем второй.

- **Использовать перенаправление IP-адресов (Use IP Address Redirection (Recommended))** Посредник сеансов может использовать два метода перенаправления клиента к отключенному сеансу: перенаправление IP-адреса и перенаправление маркера маршрутизации. Перенаправление IP-адреса включено по умолчанию и применяется в большинстве сценариев. Данный метод перенаправления работает в том случае, если клиенты могут непосредственно подключаться к каждому серверу терминалов в ферме. Этот флажок можно сбросить лишь в том случае, если клиенты служб терминалов не могут напрямую подключаться ко всем серверам терминалов в ферме, а в конфигурации балансировки сетевой нагрузки поддерживаются маркеры маршрутизации посредника сеансов служб терминалов.
- **Выберите IP-адреса для переподключения (Select IP Addresses To Be Used For Reconnection)** Здесь можно указать IP-адрес, который будет использоваться в ферме серверов терминалов.

ПРИМЕЧАНИЕ

Если в вашу сеть включен компонент для балансировки нагрузки (обычно аппаратный), поддерживающий маркеры маршрутизации, отключите перенаправление IP-адресов.

СОВЕТ Подготовка к экзамену

Во время сдачи сертификационного экзамена 70-643 и работы в реальных средах помните, что на сервере посредника сеансов служб терминалов каждого члена фермы нужно добавить в локальную группу Компьютеры каталогов сеансов (Session Directory Computers).

ВНИМАНИЕ! Исходные подключения посредника сеансов служб терминалов и балансировки нагрузки

При распределении исходных подключений в ферме серверов для балансировки нагрузки посредника сеанса служб терминалов должно использоваться такое решение балансировки, как Round-Robin DNS, Балансировка сетевой нагрузки (Network Load Balancing), или аппаратное средство балансировки нагрузки.

Настройка перенаправления принтеров служб терминалов

Благодаря перенаправлению принтеров клиентские принтеры можно использовать в сеансе служб терминалов. Основные опции перенаправления принтеров модифицируются на вкладке Параметры клиента (Client Settings) диалогового окна RDP-Tcp Свойства (RDP-Tcp Properties), важные дополнительные опции перенаправления содержатся в групповой политике.

Перенаправление принтеров можно отключить или настроить с помощью групповой политики в консоли Управление групповой политикой (Group Policy Management). Чтобы найти опции перенаправления принтеров в групповой

политике, откройте объект групповой политики GPO (Group Policy Object) и выполните команду Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Cjiy}K6bi терминалов\Сервер терминалов\Перенаправление принтеров (Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Printer Redirection). Вы перейдете в папку Перенаправление принтеров (Printer Redirection), где можно настроить пять параметров политики.

- **Не устанавливать используемый по умолчанию принтер клиента в качестве принтера для сеанса (Do Not Set Default Client Printer To Be Default Printer In A Session)** Сервер Службы терминалов (Terminal Services) автоматически назначает используемый по умолчанию принтер клиента в качестве принтера для сеанса служб терминалов. Этот параметр политики можно использовать для модификации перенаправления на принтер по умолчанию. Если данный параметр политики включен, то принтером по умолчанию является принтер, заданный на удаленном компьютере.
- **Не разрешать перенаправление клиентских принтеров (Do Not Allow Client Printer Redirection)** Параметр политики, запрещающий сопоставление клиентских принтеров в сеансах служб терминалов. Если этот параметр политики включен, пользователи не могут перенаправлять задания печати с удаленного компьютера на локальный клиентский принтер в сеансах служб терминалов.
- **Задать поведение сервера терминалов при выборе резервного драйвера принтера (Specify Terminal Server Fallback Printer Driver Behavior)** Этот параметр политики позволяет задать поведение сервера терминалов при выборе резервного драйвера принтера. По умолчанию подбор резервного драйвера принтера для сервера терминалов отключен. С помощью данного параметра можно назначить выбор драйвера принтера PCL (Printer Control Language), драйвера принтера PS (PostScript) или обоих драйверов.
- **Использовать в первую очередь драйвер принтера Easy Print служб терминалов (Use Terminal Services Easy Printer Driver First)** Драйвер принтера Easy Print служб терминалов обеспечивает стабильную печать из сеанса служб терминалов на корректном принтере клиентского компьютера. Кроме того, он обеспечивает пользователям комфортное выполнение операций печати между локальными и удаленными сеансами. По умолчанию сервер терминалов вначале пытается использовать драйвер принтера Easy Print служб терминалов для установки всех клиентских принтеров. Однако с помощью этого параметра политики можно отключить драйвер принтера Easy Print служб терминалов.
- **Перенаправлять только используемый по умолчанию принтер клиента (Redirect Only The Default Client Printer)** По умолчанию в сеансы служб терминалов перенаправляются все клиентские принтеры. Если же включить этот параметр политики, в сеансы служб терминалов будет перенаправляться только используемый по умолчанию принтер клиента.

СОВЕТ Подготовка к экзамену

Для сдачи сертификационного экзамена 70-643 вы обязательно должны изучить эти параметры групповой политики.

Проверьте себя

1. Вам нужно подготовить сервер в ферме к переходу в автономный режим, но вы не хотели бы заставлять пользователей выходить из своих сеансов. Что следует предпринять?
2. Вам нужно включить аудио в подключениях служб терминалов к серверу с именем TS1. Какие действия следует предпринять?

Ответы

1. В консоли Конфигурация служб терминалов (Terminal Services Configuration) нужно настроить свойства сервера терминалов, с тем чтобы разрешить переподключения и запретить вход новых пользователей.
2. На вкладке Параметры клиента (Client Settings) диалогового окна RDP-Tcp Свойства (RDP-Tcp Properties) сервера TS1 нужно сбросить флажок Аудио (Audio).

Практикум. Установка и настройка сервера лицензирования

После приобретения лицензий TS CAL от Microsoft или независимого поставщика вам нужно установить и активировать сервер лицензирования. В этом упражнении вы установите сервер лицензирования служб терминалов на Server1. Таким образом, сервер Server1 будет выполнять роль сервера лицензирования для Server2, где уже установлены службы терминалов.

После установки сервера лицензирования вы откроете консоль Диспетчер лицензирования служб терминалов (TS Licensing Manager) и просмотрите описание процедур активации сервера лицензирования, а также установки лицензий TS CAL.

Упражнение 1. Установка роли сервера лицензирования служб терминалов

В этом упражнении вы используете мастер добавления ролей для установки сервера лицензирования служб терминалов на контроллере домена Contoso.com.

1. Войдите на сервер Server1 как администратор домена Contoso.com.
2. Откройте Диспетчер сервера (Server Manager).
3. В дереве консоли диспетчера сервера выберите узел Роли (Roles) и в панели справа щелкните ссылку Добавить роли (Add Roles). Будет запущен Мастер добавления ролей (Add Roles Wizard).
4. На странице Перед началом работы (Before You Begin) щелкните кнопку Далее (Next).
5. Установите флажок Службы терминалов (Terminal Services) на странице Выбор ролей сервера (Select Server Roles) и щелкните кнопку Далее (Next).

6. Затем на странице Службы терминалов (Terminal Services) щелкните кнопку Далее (Next).
7. На странице Выбор служб ролей (Select Role Services) установите флажок Лицензирование служб терминалов (TS Licensing) и щелкните кнопку Далее (Next).
8. Ознакомьтесь с текстом, представленным на странице Настроить область обнаружения для лицензирования служб терминалов (Configure Discovery Scope For TS Licensing). Отметим, что вы можете настроить сервер лицензирования для локального домена Active Directory или целого леса в среде множества доменов. Текущая среда Active Directory состоит из леса одного домена.

СОВЕТ Подготовка к экзамену

Внимательно прочитайте описание областей лицензирования для сервера терминалов. Чтобы сдать сертификационный экзамен, нужно понимать концепции областей обнаружения для лицензирования служб терминалов.

9. Перейдя на страницу Настроить область обнаружения для лицензирования служб терминалов (Configure Discovery Scope For TS Licensing), оставьте заданным параметр по умолчанию Этот домен (This Domain) и щелкните кнопку Далее (Next).
10. Наконец, на странице Подтвердите выбранные элементы (Confirm Installation Selections) прочитайте весь текст и щелкните кнопку Установить (Install).

Упражнение 2. Активация сервера лицензирования служб терминалов

В этом упражнении вы активируете сервер лицензирования и проследите за ходом установки лицензий TS CAL. Для выполнения упражнения Serverl должен быть подключен к Интернету.

1. Войдите на Serverl как администратор домена, в меню Пуск (Start) откройте группу программ Администрирование (Administrative Tools), после этого откройте Службы терминалов (Terminal Services) и затем щелкните значок Диспетчер лицензирования служб терминалов (TS Licensing Manager). Так как диспетчер лицензирования служб терминалов автоматически устанавливается на любом сервере, где инсталлируется служба ролей Лицензирование служб терминалов (TS Licensing), сервером лицензирования не нужно управлять с самого сервера. Диспетчер лицензирования служб терминалов также можно установить на любом сервере и подключаться к серверу лицензирования удаленно.
2. В дереве консоли Диспетчер лицензирования служб терминалов (TS Licensing Manager) разверните узел Все серверы (All Servers) и выберите Serverl. (Последний узел должен быть помечен красным крестиком, поскольку сервер еще не активирован.)

3. Щелкните правой кнопкой узел Serverl и примените команду Активировать сервер (Activate Server). Запустится Мастер активации сервера (Activate Server Wizard).
4. На странице приветствия мастера прочитайте весь текст и щелкните кнопку Далее (Next).
5. На странице Метод подключения (Connection Method) прочитайте весь текст и ответьте на следующий вопрос:

   Какой метод подключения по умолчанию назначается серверу лицензирования?

   Ответ: Метод Автоподключение (рекомендуется) (Automatic Connection (Recommend).
6. На странице Метод подключения (Connection Method) выберите в раскрывающемся списке параметр В обозреватель веб-страниц (Web Browser).
7. Прочитайте обновленное содержимое разделов Описание (Description) и Требования (Requirements). Метод подключения В обозреватель веб-страниц (Web Browser) удобно использовать в случае, если сервер лицензирования не подключен к Интернету. При использовании этого метода потребуется лишь еще один сервер для подключения к серверу лицензирования и к Интернету.
8. На странице Метод подключения (Connection Method) выберите в раскрывающемся списке параметр Телефон (Telephone).
9. Прочитайте обновленное содержимое разделов Описание (Description) и Требования (Requirements). Метод подключения Телефон (Telephone) удобно использовать в том случае, если сеть не подключена к Интернету.
10. На странице Метод подключения (Connection Method) выберите в раскрывающемся списке параметр Автоподключение (Automatic Connection) и щелкните кнопку Далее (Next). Пока сервер подключается к сайту расчетной палаты Microsoft Clearinghouse, на короткое время отобразится окно Мастер активации сервера (Activate Server Wizard). Затем откроется страница Сведения об организации (Company Information).

И. Перейдя на страницу Сведения об организации (Company Information), введите в соответствующие текстовые поля имя, фамилию и название организации, после чего в раскрывающемся списке Выбор страны или региона (Country Or Region) выберите свой регион.

12. Щелкните кнопку Далее (Next).
13. Откроется еще одна страница Сведения об организации (Company Information). При желании вы можете ввести запрашиваемые сведения. Щелкните кнопку Далее (Next). На короткое время отобразится окно Мастер активации сервера (Activate Server Wizard), после чего откроется страница Завершение работы мастера активации сервера (Completing The Activate Server Wizard). Убедитесь, что на этой странице установлен флажок Запустить мастер установки лицензий (Start Install Licenses Wizard Now).
14. На странице Завершение работы мастера активации сервера (Completing The Activate Server Wizard) прочитайте весь текст и щелкните кнопку Далее (Next). Откроется страница приветствия мастера установки лицензий.
15. Оставьте все окна открытыми и переходите к выполнению упражнения 3.

Упражнение 3. Установка лицензий служб терминалов TS CAL

Установка клиентских лицензий является последним этапом развертывания сервера лицензирования. Даже если на этом этапе у вас нет лицензий TS CAL, имеет смысл просмотреть страницы мастера установки лицензий, чтобы лучше понять принцип развертывания.

1. На странице приветствия мастера установки лицензий прочитайте весь текст и щелкните кнопку Далее (Next). На короткое время отобразится окно Установка лицензий (Install Licenses), после чего откроется страница Программа лицензирования (License Program).
2. На странице Программа лицензирования (License Program) прочитайте весь представленный текст.
3. Просмотрите опции в раскрывающемся списке Программа лицензирования (License Program).
4. Ознакомьтесь с описанием различных опций программ лицензирования, выбрав каждую и прочитав соответствующий текст на странице.
5. Убедитесь, что в раскрывающемся списке Программа лицензирования (License Program) выбрана опция по умолчанию Получить ключевой пакет клиентской лицензии (License Pack (Retail Purchase)), и щелкните кнопку Далее (Next). Откроется страница Код лицензии (License Code).
6. Прочитайте весь текст на странице. Если вы получили действительный код лицензии, можете выполнить оставшиеся шаги упражнения. В противном случае щелкните кнопку Отмена (Cancel), чтобы закрыть мастер и просто прочитать об оставшихся шагах.
7. Введите действительный код лицензии и щелкните кнопку Добавить (Add).
8. На странице Код лицензии (License Code) щелкните кнопку Далее (Next). На короткое время появится окно Мастер установки лицензий (Install Licenses Wizard), а затем откроется страница Завершение работы мастера установки лицензий (Completing The Install Licenses Wizard).
9. На указанной странице щелкните кнопку Готово (Finish).
10. В дереве консоли Диспетчер лицензирования служб терминалов (TS Licensing Manager) узел Serverl теперь будет помечен зеленым маркером, указывающим на то, что сервер лицензирования отконфигурирован.
11. С сервера Server2 войдите на Contoso.com как администратор домена и откройте консоль Конфигурация служб терминалов (Terminal Services Configuration).
12. В разделе Лицензирование (Licensing) области Изменить настройки (Edit Settings) дважды щелкните опцию Режим лицензирования служб терминалов (Terminal Services Licensing Mode).
13. На вкладке Лицензирование (Licensing) диалогового окна Свойства (Properties) выберите опцию На устройство (Per Device) или На пользователя (Per User), руководствуясь типом лицензий TS CAL, установленных на Serverl.
14. В области Укажите режим обнаружения сервера лицензирования (Specify The License Server Discovery Mode) выберите опцию Использовать указанные

серверы лицензирования (Use The Specified License Servers) и в соответствующее текстовое поле введите *Server1.Contoso.com.*

15. Для того чтобы проверить подключение к серверу, щелкните кнопку Проверить (Check Names).
16. Когда будет выведено сообщение о том, что данный сервер назначен действительным сервером лицензирования служб терминалов, щелкните ОК.
17. В диалоговом окне Свойства (Properties) на сервере Server2 щелкните ОК. В консоли Конфигурация служб терминалов (Terminal Services Configuration) теперь будет назначена опция На устройство (Per Device) или На пользователя (Per User).
18. Закройте все открытые окна и выйдите с серверов Serverl и Server2.

Резюме

- Основным инструментом, используемым для настройки компонента Службы терминалов (Terminal Services), является консоль Конфигурация служб терминалов (Terminal Services Configuration).
- С помощью свойств подключения RDP-Tcp в консоли Конфигурация служб терминалов (Terminal Services Configuration) для сеанса можно отконфигурировать уровень строгости шифрования, параметры времени ожидания и доступность принтеров.
- Свойства сервера служб терминалов в консоли Конфигурация служб терминалов (Terminal Services Configuration) позволяют настроить балансировку сетевой нагрузки, режим обнаружения серверов лицензирования, параметры временных папок и ограничения на вход новых пользователей.
- Групповая политика обеспечивает дополнительный контроль над перенаправлением принтеров служб терминалов, в том числе над поведением сервера терминалов при выборе резервного драйвера принтера и перенаправлением на клиентский принтер по умолчанию.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных в ходе занятия 2. Эти вопросы представлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы

Ответы и пояснения к каждому их варианту размещены в разделе «Ответы» в конце книги.

1. В сети вашей организации реализована ферма серверов терминалов TSFARM1. Ферма состоит из пяти компьютеров Windows Server 2008, включая сервер с именем TSLB1, на котором установлена служба ролей Посредник сеансов служб терминалов (TS Session Broker). Вам нужно добавить в ферму шестой компьютер Windows Server 2008 с именем TSLB6. После конфигурирования сервера с использованием того же оборудования и программного обеспечения,

что и на других членах фермы, вы присоединили компьютер TSLB6 к ферме, указав его как сервер посредника сеансов служб терминалов. В свойствах посредника сеансов служб терминалов на TSLB6 вы указали имя фермы TSFARM1. Вы убедились, что некоторые пользователи, пытающиеся подключиться к виртуальному серверу TSFARM1, могут установить на TSLB6 сеансы служб терминалов, однако они не могут переподключаться к отключенным сеансам. Вам нужно, чтобы пользователи, подключающиеся к TSLB6 через TSFARM1, могли переподключаться к отключенным сеансам удаленного рабочего стола. Какие действия следует предпринять?

А. На компьютере TSLB6 добавить TSLB6 в локальную группу Компьютеры каталога сеансов (Session Directory Computers).

Б. На компьютере TSLB1 добавить TSLB6 в локальную группу Компьютеры каталога сеансов (Session Directory Computers).

В. В параметрах DNS-сервера добавить запись Host (A) с именем TSFARM1, сопоставленную с IP-адресом компьютера TSLB6.

Г. В параметрах DNS-сервера добавить запись Host (A) с именем TSLB6, сопоставленную с IP-адресом компьютера TSLB6.

2. Сеть вашей организации состоит из одного домена Active Directory с именем Contoso.com. В сети вы развернули службы терминалов на компьютере Windows Server 2008 с именем TS1. Некоторые пользователи, подключающиеся к TS1 через подключение к удаленному столу, жалуются, что не могут выполнять печать на своих локальных принтерах. Вам нужно, чтобы компьютер TS 1 использовал драйвер принтера PostScript, если сервер терминалов не найдет соответствующий драйвер клиентских принтеров служб терминалов. Какие действия следует предпринять в данном случае?

А. На вкладке Параметры клиента (Client Settings) окна свойств RDP-Tcp сервера TS1 установить флажок Принтер Windows (Windows Printer).

Б. На вкладке Параметры клиента (Client Settings) окна свойств RDP-Tcp сервера TS 1 установить флажок По умолчанию выбрать основной принтер клиента (Default To Main Client Printer).

В. В объекте групповой политики отконфигурировать параметр Использовать в первую очередь драйвер принтера Easy Print служб терминалов (Use Terminal Services Easy Printer Driver First) и применить объект политики для компьютера TS1.

Г. В объекте групповой политики отконфигурировать параметр Задать поведение сервера терминалов при выборе резервного драйвера принтера (Specify Terminal Server Fallback Printer Driver Behavior), указав драйвер PS, и применить объект политики для компьютера TS1.

Закрепление материала главы

Для того чтобы попрактиковаться и закрепить знания, приобретенные в ходе изучения представленного в данной главе материала, вам необходимо:

- ознакомиться с резюме главы;
- повторить используемые в главе основные термины;

- выполнить задания лабораторной работы, которые моделируют реальные ситуации, требующие применения полученных знаний;
- выполнить рекомендуемые упражнения;
- сдать пробный экзамен с помощью тестов.

Резюме главы

- Службы терминалов (Terminal Services) позволяют пользователям установить на удаленном компьютере сеанс рабочего стола или приложения. В Windows Server 2008 службы терминалов включают такие новые компоненты, как Сервер шлюза служб терминалов (Terminal Services Gateway, TS Gateway), RemoteApp и Веб-доступ к службам терминалов (TS Web Access).
- Для работы служб терминалов требуются клиентские лицензии доступа CAL для всех подключающихся пользователей или всех подключающихся устройств. Если не будут приобретены и установлены лицензии TS CAL, службы терминалов через 120 дней перестанут функционировать.
- Чтобы установить службы терминалов на компьютер Windows Server 2008, нужно добавить роль сервера Службы терминалов (Terminal Services).
- Основным инструментом, используемым для настройки компонента Службы терминалов (Terminal Services), является консоль Конфигурация служб терминалов (Terminal Services Configuration). Используя свойства подключения RDP-Tcp в консоли Конфигурация служб терминалов (Terminal Services Configuration), для сеанса можно отконфигурировать уровень строгости шифрования, параметры времени ожидания и доступность принтеров.

Основные термины

Проверьте, знаете ли вы, что означают перечисленные ниже термины (свои ответы можно сверить с определениями, содержащимися в конце книги):

- проверка подлинности на уровне сети;
- перенаправление принтеров;
- Удаленный рабочий стол для администрирования;
- протокол удаленного рабочего стола RDP;
- подключение служб терминалов;
- сеанс служб терминалов;
- Клиентская лицензия доступа служб терминалов.

Лабораторная работа

Для выполнения следующих заданий используйте знания, полученные во время изучения этой главы. Правильные ответы вы сможете найти в разделе «Ответы» в конце книги.

Задание 1. Выбор стратегии лицензирования служб терминалов

Вы работаете системным администратором в большой компании. Не так давно ваше подразделение реализовало два сервера терминалов, TS1 и TS2, и перед вами была поставлена задача разработать стратегию лицензирования для каждого сервера.

Компьютер TS1 является сервером приложений. Хотя приложение на нем не является особо важным, к нему желают одновременно подключаться пять пользователей. В целом, в разное время дня к TS1 должны подключаться 20 пользователей с 50 различных компьютеров.

Компьютер TS2 является DNS-сервером, на котором время от времени нужно производить техническое обслуживание и администрирование. К TS2 могут подключаться лишь администраторы.

1. Следует ли установить службы терминалов на сервере TS1? Какой тип клиентских лицензий доступа CAL имеет смысл приобрести?
2. Требуется ли установить службы терминалов на сервере TS2? Какой тип клиентских лицензий доступа CAL целесообразно приобрести в данном случае?

Задание 2. Устранение неполадок служб терминалов

Вы работаете в группе IT-поддержки большой организации, сеть которой включает лишь один домен Active Directory. Одной из ваших обязанностей является поддержка серверов терминалов отдела рекламы. В течение недели вы столкнулись с описанными ниже проблемами.

1. Вы развернули службы терминалов на новом компьютере Windows Server 2008 с именем App3, однако к ним не могут подключаться клиенты Windows XP. Какие действия следует предпринять?
2. Пользователи, подключающиеся к серверу терминалов App1, жалуются, что не всегда могут переподключаться к отключенному сеансу. Что вы им посоветуете?

Рекомендуемое упражнение

Чтобы успешно справиться с экзаменационными заданиями, выполните следующее упражнение.

- **Упражнение 1** Используя виртуальные или физические компьютеры, присоедините к домену два идентичных компьютера Windows Server 2008. Установите на обоих компьютерах службу ролей Сервер терминалов (Terminal Server) и лишь на одном компьютере установите службу ролей Посредник сеансов служб терминалов (TS Session Broker). Добавьте оба компьютера в локальную группу Компьютеры каталога сеансов (Session Directory Computers) на компьютере с посредником сеансов служб терминалов. На вкладке Посредник сеансов служб терминалов (TS Session Broker) консоли Конфигурация служб терминалов (Terminal Services Configuration) обоих компьютеров

отконфигурируйте ферму служб терминалов. В DNS создайте записи Host (A) для имени фермы (по одной записи для IP-адреса каждого сервера). Затем подключитесь к ферме серверов с помощью удаленного клиента Подключение к удаленному рабочему столу (Remote Desktop Connection).

Веб-вещание

Просмотрите в папке Webcasts на прилагаемом CD-диске веб-вещание «A Technical Overview of Windows Server 2008 Terminal Services» Блайна Бартона (Blain Barton). Оно также доступно в Интернете на сайте *http://msevents.microsoft.com',* код события — 1032345660.

Пробный экзамен

На прилагаемом к книге компакт-диске представлено несколько вариантов тренировочных тестов. Проверка знаний выполняется только по одной или же по всем экзаменационным темам сертификационного экзамена 70-643. Тестирование можно организовать таким образом, чтобы оно проводилось как экзамен, или же настроить его на изучение — в этом случае вы сможете после каждого своего ответа на вопрос просматривать правильные ответы и объяснения.

ПРИМЕЧАНИЕ Пробный экзамен

Подробнее о пробном экзамене рассказано во введении к данной книге.

ГЛАВА 4

Настройка инфраструктуры служб терминалов и управление ею

Занятие 1. Конфигурирование клиентов служб терминалов и управление ими 170

Занятие 2. Развертывание шлюза служб терминалов 191

Занятие 3. Публикация приложений с помощью утилиты TS RemoteApp 207

В этой главе мы отвлечемся от развертывания сервера терминалов и обсудим процесс настройки компонентов, составляющих инфраструктуру Службы терминалов (Terminal Services, TS) — клиентов, серверов, шлюзов и приложений.

Лучше всего можно понять принципы служб терминалов, работая с ними непосредственно. Обязательно выполняйте упражнения, предлагаемые в конце каждого занятия, чтобы закрепить навыки, требуемые как для сдачи экзамена, так и для работы в реальных средах.

Темы экзамена:

- Настройка клиентских подключений служб терминалов.
- Конфигурирование шлюза служб терминалов.
- Настройка утилиты Terminal Services RemoteApp (TS RemoteApp).
- Конфигурирование ресурсов Terminal Services и наблюдение за ними.

Требования

Для выполнения упражнений этой главы вам потребуются:

- компьютер Windows Server 2008 с именем Server1, являющийся доменным контроллером в домене Contoso.com;
- компьютер Windows Server 2008 с именем Server2 в домене Contoso.com. На Server2 устанавливается ролевая служба Сервер терминалов (Terminal Server), однако другие ролевые службы в роли Службы терминалов (Terminal Services) не устанавливаются;

- три доменные административные учетные записи: ContosoAdminl, Contoso-Admin2 и ContosoAdmin3.

Реальный мир

Дж. К. Макин

Виртуализация является в настоящее время общей тенденцией развития информационных технологий, и Службы терминалов (Terminal Services) отображают эту тенденцию, предлагая так называемую виртуализацию представления. Это выражение, согласитесь, звучит неплохо, однако следует выяснить реальное назначение данной технологии.

Помимо громкого названия реальное преимущество виртуализации представления состоит в ее возможности содействовать консолидации серверов. В последнее время многие IT-подразделения для повышения эффективности и снижения затрат занялись консолидацией своих серверов приложений с представлением. Консолидация серверов — это процесс централизации ресурсов множества серверов на нескольких физических серверах. Службы терминалов (Terminal Services) являются ключевым компонентом такой стратегии консолидации приложений, поскольку они предоставляют многим пользователям доступ к множеству приложений на одном сервере.

Занятие 1. Конфигурирование клиентов служб терминалов и управление ими

Инфраструктура Службы терминалов (Terminal Services) включает много областей для конфигурирования клиентов, таких как пользовательские профили, опции клиентских сеансов, распределение ресурсов и сама клиентская программа TS (Mstsc).

На этом занятии мы рассмотрим инструменты, которые можно использовать для административного управления этими и другими аспектами подключений TS-клиентов.

Изучив материал этого занятия, вы сможете:

- Использовать опции конфигурации, доступные при подключении к удаленному рабочему столу (Remote Desktop Connection).
- Управлять подключениями к Службам терминалов (Terminal Services).

Расчетная продолжительность занятия составляет 50 мин.

Настройка клиентских параметров служб терминалов

Клиентскую программу Подключение к удаленному рабочему столу (Remote Desktop Connection) инфраструктуры Службы терминалов (Terminal Services)

можно полностью отконфигурировать, например настроить клиент для отображения удаленного рабочего стола с определенным разрешением экрана или для обеспечения доступа к некоторым логическим дискам во время сеанса. Эти возможности конфигурируются в самом клиентском приложении или на уровне домена с помощью объекта групповой политики (Group Policy Object, GPO).

Опции конфигурирования подключения к удаленному рабочему столу

Клиентская программа Подключение к удаленному рабочему столу (Remote Desktop Connection, RDC) Mstsc.exe изначально используется для подключения к службам терминалов. Другая клиентская программа, Удаленные рабочие столы (Remote Desktops), представляет собой оснастку консоли управления компьютером Microsoft Management Console (MMC). Программа RDC позволяет настроить подключение служб терминалов согласно набору ограничений, назначенному на сервере или в групповой политике.

Для того чтобы просмотреть опции конфигурации программы RDC, откройте Подключение к удаленному рабочему столу (Remote Desktop Connection) и щелкните кнопку (Options), чтобы открыть окно, показанное на рис. 4-1.

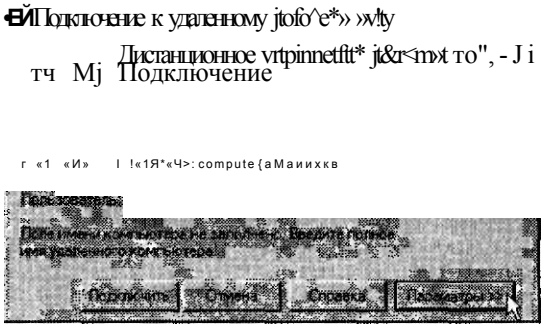


РИС. 4-1. Кнопка доступа к параметрам RDC

Откроется окно, содержащее шесть вкладок с параметрами RDC, описанными далее.

- Общие (General) Данная вкладка позволяет указать конечный компьютер и метод проверки подлинности для подключения (рис. 4-2). Здесь также можно сохранить в RDP-файле опции, которые предназначены для подключения.
- **Экран** (Display) На этой вкладке можно задать разрешение экрана и цветовую палитру для окна клиента TS (рис. 4-3).
- **Локальные ресурсы** (Local Resources) Здесь можно указать локальные ресурсы (например, буфер обмена, локально определенные принтеры и локальные диски), которые должны быть доступны в сеансе TS, а также определить работу звука и сочетания клавиш, которые используются в сеансе TS (рис. 4-4).
- **Программы (Programs)** На этой вкладке можно указать все программы для автоматического запуска в начале сеанса TS (рис. 4-5).

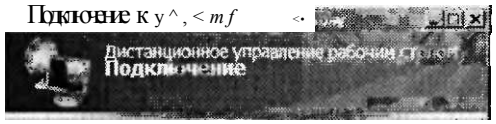


РИС. 4-2. Вкладка Общие (General) окна программы RDC

Рис. 4-3. Вкладка Экран (Display) программы RDC

Дополнительно (Experience) На вкладке, представленной на рис. **4-6,** можно выбрать опциональные эффекты графического пользовательского интерфейса для отображения с сервера терминалов. Например, фоновый рисунок рабочего стола и сглаживание шрифтов визуально улучшают вид сеанса TS, но интенсивно используют сетевые ресурсы и снижают быстродействие клиента TS. При выборе типа подключения параметры быстродействия автоматически будут указаны в качестве рекомендуемых.

4 Шаше) Зфт П&к^тг pvZ&te* | {^ододо \ •»*

§ Перемести на этот компьютер

Ер?

. ; v .J&mabsoBaib c^ та *ш «me/m* Л'rac-

ко в пс^ожанс^ реи^ 3 1

и»

г? £ оймай

. j Г-ждалетрь |J

Рис. 4-4. Вкладка Локальные ресурсы (Local Resources) программы RDC

| реи j *Vl^f* п. *ш* Пкгаммы *ы*[4] I >

•^ш Яквкдр ' j

Рис. 4-5. Вкладка Программы (Programs)

Подключение (Advanced) (Сконфигурировать функции Проверка подлинности сервера (Server Authentication) и Шлюз служб терминалов (Terminal Services Gateway, TS Gateway) можно на вкладке, которую вы видите на рис. 4-7. Проверка подлинности сервера — исконный компонент Windows Vista и Windows Server 2008, посредством которого сервер может подтвердить идентичность компьютера согласно указанной клиентом TS. Па вкладке Подключение (Advanced) можно указать предупреждение, блокирование

подключения к серверу, на котором возник сбой проверки подлинности, или разрешение TS-клиента.

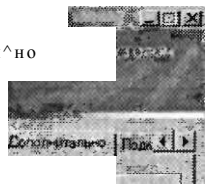


Рис. 4-6. Вкладка Дополнительно (Experience) программы RDC

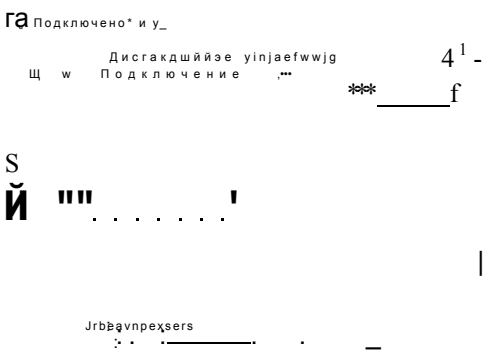


Рис. 4-7. Вкладка Подключение (Advanced) программы RDC

Шлюз служб терминалов (Terminal Services Gateway) позволяет TS-кл центу проходить проверку корпоративного брандмауэра и подключаться ко всем серверам терминалов в организации. Этот компонент и его конфигурация детально описаны в занятии 2 (данной главы).

Сохранение RDP-файлов

После определения требуемых опций для TS-клиента в программе RDC параметры сохраняются автоматически в скрытом файле Default.rdp в папке Документы (Documents). Этот файл содержит параметры, используемые для подключения к удаленному рабочему столу при открытии программы из меню Пуск (Start). Однако вы также можете сохранить параметры конфигурирования клиента служб терминалов в настраиваемых файлах custom.rdp, щелкнув кнопку Сохранить как (Save As). Эти файлы .rdp можно затем использовать для активизации сеансов служб терминалов с конкретными опциями клиента (например, имя сервера и данные аутентификации).

СОВЕТ Подготовка к экзамену

В сертификационный экзамен 70-643 включены вопросы о сохранении параметров подключения к удаленным рабочим столам в файлах .rdp. Поэтому вам следует внимательно просмотреть все параметры на вкладках программы Подключение к удаленному рабочему столу (Remote Desktop Connection) и выяснить, какие типы информации можно сохранить в таком файле.

Настройка клиентов служб терминалов с помощью групповой политики

Групповая политика (Group Policy) обеспечивает возможности централизованного управления пользователями и компьютерами в среде Active Directory. Объект групповой политики (Group Policy Object, GPO) можно использовать для управления множеством клиентов и настройки требуемых параметров подключения к удаленному рабочему столу.

Во многих случаях такой объект обеспечивает наиболее эффективный способ управления клиентами служб терминалов.

В разделе Конфигурация компьютера объекта GPO можно указать такие клиентские параметры, как сохранение паролей в RDC, требование от клиента подтверждения прав доступа, метод выполнения проверки подлинности сервера, а также ресурсы, перенаправляемые сеансу служб терминалов. Указанные параметры можно просмотреть в объекте GPO, открыв раздел Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Службы терминалов (Computer Configuration\Administrative Templates\Windows Components\Terminal Services).

В разделе Конфигурация пользователя (User Configuration) объекта GPO можно конфигурировать параметры, связанные с временными ограничениями сеанса, удаленным управлением и средой удаленного сеанса. Эти параметры можно просмотреть в разделе Конфигурация пользователя\Административные шаблоны\Компоненты Windows\Службы терминалов (User Configuration\Administrative Templates\Windows Components\Terminal Services).

Аутентификация Single Sign-On (SSO) Компонент клиента TS, который можно настроить в групповой политике. В доменной среде Active Directory технологию SSO можно применять для избавления пользователя от необходимости

вводить учетную запись и пароль при использовании программы RDC для подключения к серверу терминалов.

При использовании SSO программа Подключение к удаленному рабочему столу (Remote Desktop Connection) автоматически применяет привилегии текущего пользователя компьютера Microsoft Windows.

Для настройки SSO включите параметр политики Разрешить передачу сохраненных учетных данных (Allow Delegating Saved Credentials) в разделе Конфигурация компьютера\Административные шаблоны\Система\Передача учетных данных (Computer Configuration\Administrative Templates\System\Credentials Delegation). После включения этого параметра политики вам потребуется создать в той же политике список серверов терминалов, принимающих учетные данные SSO. Добавьте имя каждого сервера в форме TERMSRV/<Имя_сервера>.

Чтобы включить все серверы терминалов в области действия политики для принятия учетных данных SSO, можно добавить запись TERMSRV/*.

СОВЕТ Подготовка к экзамену

Для сдачи сертификационного экзамена 70-643 вы должны лишь знать, что групповая политика обеспечивает наилучший способ внедрения конфигурации TS или RDC для множества пользователей и компьютеров. Вам не нужно запоминать все конфигурируемые опции или место их расположения. Тем не менее имеет смысл просмотреть все опции и выяснить, которые из них можно использовать в среде Active Directory.

Конфигурирование пользовательских профилей для служб терминалов

В принципе пользовательский профиль представляет собой коллекцию данных, которые составляют индивидуальную среду пользователя, включая индивидуальные файлы пользователя, параметры приложений и конфигурацию рабочего стола. Пользовательский профиль содержится в автоматически создаваемой системой Windows личной папке, которой присваивается имя отдельного пользователя.

По умолчанию личная папка создается в папке C:\Пользователи (C:\Users) при первом входе пользователя в Windows Vista или Windows Server 2008. Она содержит такие подпапки, как Документы (Documents), Рабочий стол (Desktop) и Загрузка (Downloads), а также личный файл данных Ntuser.dat. Например, по умолчанию пользователь StefanR будет хранить данные, составляющие его личную среду, в папке C:\Пользователи\StefanR (C:\Users\StefanR).

В среде TS пользовательские профили по умолчанию хранятся на сервере терминалов. Этот момент играет важную роль, поскольку при получении множеством пользователей доступа к серверу терминалов для централизованного хранения профилей может потребоваться немало места на диске сервера. Если на сервере терминалов не хватает места для хранения, сохраняйте пользова-

тельские данные и профили па отдельном диске, где не установлена операционная система. Кроме того, с целью ограничения доступного для каждого пользователя пространства используйте дисковые квоты. (Их можно настроить в свойствах диска сервера терминалов, где хранятся профили.)

СОВЕТ Подготовка к экзамену
Чтобы сдать сертификационный экзамен 70-643, нужно знать принципы использования дисковых квот для ограничения размеров пользовательских профилей в среде служб терминалов.

Еще один способ управления пользовательскими профилями TS состоит в конфигурировании пользователей с помощью перемещаемого пользовательского профиля служб терминалов, который хранится в центральном общем сетевом ресурсе. Такой профиль загружается б каждый инициируемый TS-сеанс пользователя. Этот перемещаемый пользовательский профиль TS можно определить на вкладке Профиль служб терминалов (Terminal Services Profile) окна свойств учетной записи пользователя, как показано на рис. 4-8. В качестве альтернативы для определения перемещаемых пользовательских профилей TS можно использовать групповую политику. Параметры профилей служб терминалов содержатся в разделе Конфигурация компьютера\Лдминистративные шаблоны\Компоненты \¥т(1о\Уя\Службы терминалов\Сервер терминалов\РгоШея (Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Profiles). Для настройки перемещаемых пользовательских профилей служб терминалов используется параметр политики Задать путь для перемещаемого профиля пользователя служб терминалов (Set Path For TS Roaming User Profile).

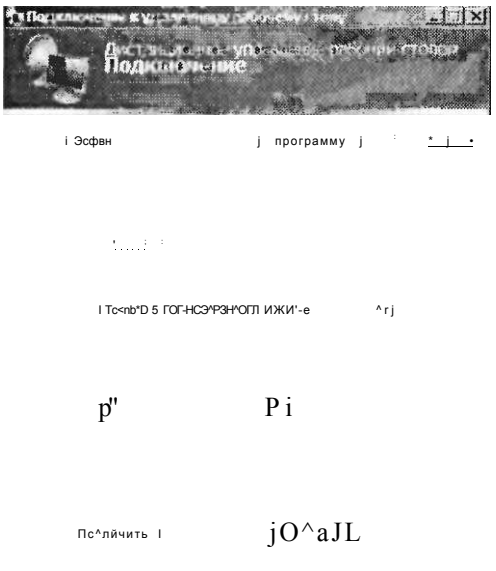


Рис. 4-8. Настройка перемещаемого профиля пользователя служб терминалов

ПРИМЕЧАНИЕ Перемещаемые пользовательские профили и службы терминалов

Стандартные перемещаемые пользовательские профили позволяют пользователю входить на различные компьютеры в домене Windows. Стандартные перемещаемые пользовательские профили нельзя применять для сеансов служб терминалов, поскольку это может привести к потере или повреждению данных. Если в вашей организации отконфигурированы перемещаемые пользовательские профили, обязательно реализуйте также пользовательские профили служб терминалов.

Настройка домашних папок

Когда пользователь сохраняет файл, путь сохранения по умолчанию указывает на так называемую домашнюю папку. Для служб терминалов домашняя папка по умолчанию расположена на сервере терминалов. Тем не менее ее можно конфигурировать на локальном диске или в сетевом ресурсе, чтобы пользователи могли без труда локализовать сохраненные файлы. Как и в случае с перемещаемыми профилями пользователей служб терминалов, вы можете определить размещение домашних папок для служб терминалов в свойствах учетной записи или в групповой политике. Параметры домашней папки для служб терминалов содержатся в разделе Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Службы терминалов\Сервер терминалов\ Profiles (Computer Configuration\Administrative Templates^Windows Components\ Terminal Services\Terminal Server\Profiles). Для настройки домашних папок используется параметр политики Установить домашний каталог пользователя TS (Set TS User Home Directory).

Проверьте себя

1. Где по умолчанию хранится профиль пользователя служб терминалов?
2. Как эффективней всего отконфигурировать опции программы RDC для множества пользователей в организации?

Ответы

1. На сервере терминалов.
2. Воспользовавшись групповой политикой.

Управление пользовательскими подключениями к службам терминалов

Диспетчер служб терминалов (Terminal Services Manager, TSM) является основным административным средством, используемым для управления подключениями к серверу терминалов. Диспетчер служб терминалов можно использовать для просмотра информации о пользователях, подключенных к серверу терминалов, для отслеживания пользовательских сеансов или выполнения та-

ких административных задач, как отключение пользователей и завершение пользовательских сеансов.

Чтобы открыть диспетчер TSM в меню Пуск (Start), подведите указатель мыши к элементу Администрирование (Administrative Tools), затем к элементу Службы терминалов (Terminal Services) и щелкните кнопку Диспетчер служб терминалов (Terminal Services Manager). Чтобы открыть диспетчер TSM, вы также можете ввести в поле поиска или окно Выполнить (Run) меню Пуск (Start) команду *tsadmin.msc.*

В следующем разделе описаны основные задачи управления, которые можно выполнять в диспетчере TSM, а также представлены альтернативные методы выполнения этих задач из командной строки. Чтобы усвоить принципы работы TSM, нужно выполнить упражнения, рекомендуемые в конце занятия.

СОВЕТ Подготовка к экзамену

Хотя диспетчер служб терминалов является основным средством управления пользовательскими подключениями к службам терминалов, для большинства функций управления также существуют эквивалентные функции командной строки. Поэтому вам следует изучить графический пользовательский интерфейс и версии командной строки всех функций, описанных в этом разделе.

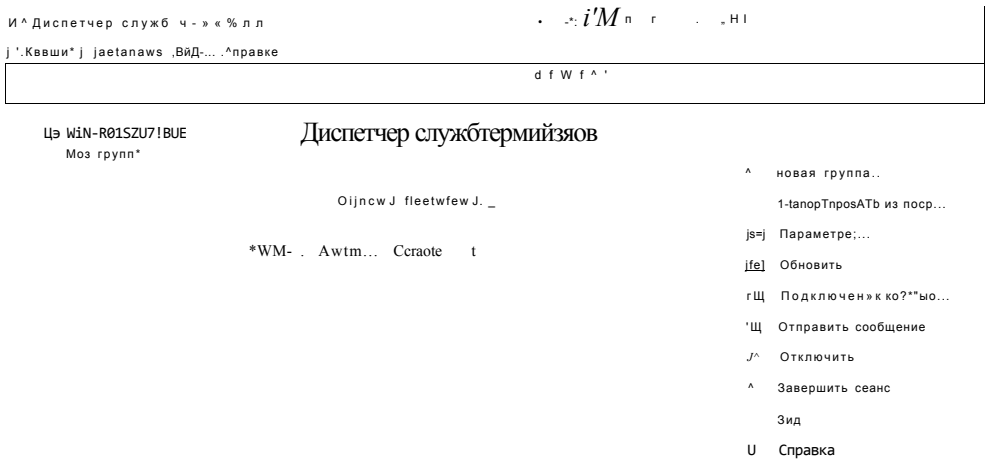


Рис. 4-9. Диспетчер служб терминалов (Terminal Services Manager)

Окно Диспетчер служб терминалов (Terminal Services Manager) содержит три вкладки: Пользователи (Users), Сеансы (Sessions) и Процессы (Processes), с помощью которых можно управлять подключениями к TS.

- Вкладка Пользователи (Users) отображает информацию о пользователях, подключенных к серверу терминалов, например текущие активные учетные записи, время входа пользователя на сервер и состояние сеанса.
  Чтобы отобразить информацию о пользовательских сеансах на сервере терминалов, можно также использовать команды *Query user* и *Quser* из командной строки.

К СВЕДЕНИЮ Использование переключателя /? для получения справки
Если вы хотите получить больше сведений об инструментах командной строки, описанных в данном разделе, просто введите интересующую вас команду в командную строку и добавьте переключатель /?. Например, для получения информации о синтаксисе Quser введите команду *quser/?*.

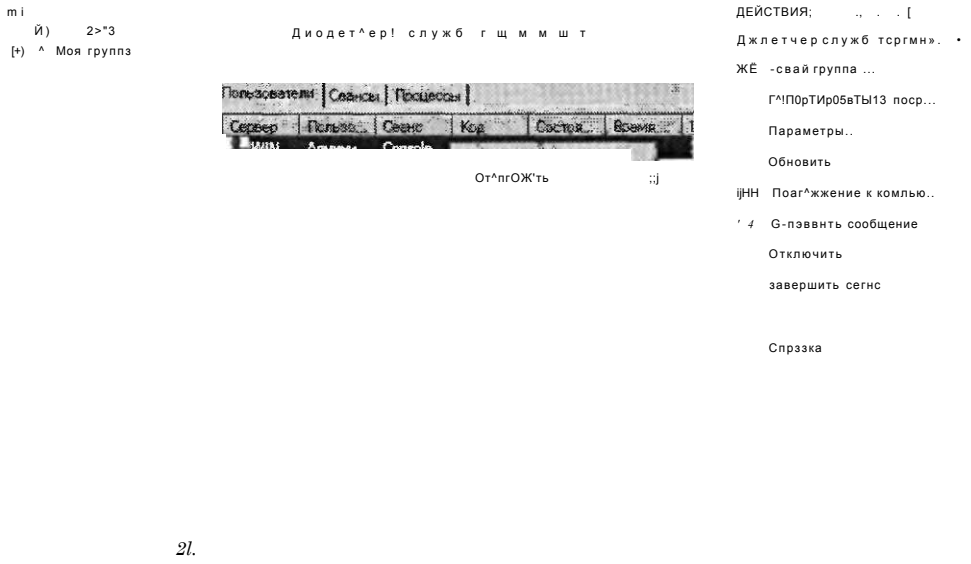
- Вкладка Сеансы (Sessions) содержит информацию о сеансах, подключенных к серверу терминалов. Поскольку некоторые сеансы инициируются службами или операционной системой, количество сеансов обычно превышает количество пользователей.
  Для отображения сведений о сеансах на сервере терминалов можно также использовать команду *Query session* из командной строки.
- Вкладка Процессы (Processes) отображает информацию о программах, запущенных каждым пользователем на сервере терминалов.
  Для отображения сведений о процессах, запущенных на сервере терминалов, можно также использовать команду *Query process* или *Qprocess* из командной строки.

Управление пользовательскими сеансами

Чтобы получить возможность управлять пользовательскими сеансами в Диспетчере служб терминалов (Terminal Services Manager), щелкните правой кнопкой мыши имя пользователя на вкладке Пользователи (Users) и выберите одну из семи командных опций в контекстном меню (рис. 4-10).

Далее описаны семь опций управления в контекстном меню для пользовательского сеанса, а также эквивалентные функции командной строки.

- **Подключиться (Connect)** Данную команду можно использовать для повторного подключения к собственному активному или отключенному пользовательскому сеансу. (Этот сценарий возможен только в случае настройки сервера терминалов на прием множества сеансов от одного пользователя.) Кроме того, если для подключения сервера RDP-Tcp указано право Полный доступ (Full Control) или особое разрешение Подключиться (Connect) (в консоли Конфигурация служб терминалов (Terminal Services Configuration)), вы также можете использовать эту команду для подключения к активному или отключенному сеансу другого пользователя.
  В качестве альтернативы Диспетчеру служб терминалов (TSM) для подключения к сеансу клиента TS вы также можете использовать команду *Tscon* из командной строки.



2l.

Рис. 4-10. Команды сеансов пользователей в Диспетчере служб терминалов (Terminal Services Manager)

ПРИМЕЧАНИЕ Использование команды Подключиться (Connect) в TSM
Использовать команду Подключиться (Connect) в TSM вы сможете лишь после подключения к серверу терминалов. При выполнении локального входа на сервер терминалов эта команда отключена в диспетчере служб терминалов. Локальный сеанс также называется сеансом консоли.

- **Отключить (Disconnect)** Эту команду можно использовать из панели Действия (Actions) или контекстного меню для отключения пользователя от сеанса. При отключении пользователя от сеанса все программы и процессы, запущенные в сеансе, продолжают выполняться. Поэтому в случае отключения множества сеансов могут быть заняты ресурсы сервера терминалов и быстродействие сервера снизится.

  В качестве альтернативы для отключения сеанса клиента TS с помощью диспетчера TSM вы также можете использовать средство командной строки Tsdiscon.

  Для отключения еще одного пользователя от сеанса в подключении сервера RDP-Tcp требуется разрешение Полный доступ (Full Control) или особое разрешение доступа Отключиться (Connect).
- **Отправить сообщение (Send Message)** Эта команда позволяет отправить простое консольное сообщение пользователю, подключенному к серверу

терминалов. Например, ее можно использовать для уведомления пользователя о предстоящем отключении или завершении сеанса.

Для отправки сообщения пользователю на сервере терминалов можно также применять инструмент командной строки *Msg*.

Для отправки сообщения еще одному пользователю в подключении сервера RDP-Tcp требуется разрешение Полный доступ (Full Control) или особое разрешение доступа Сообщение (Message).

- **Удаленное управление (Remote Control)** Эта команда позволяет управлять сеансом клиента TS еще одного пользователя. Поведение функции Удаленное управление (Remote Control) можно отконфигурировать в консоли Конфигурация служб терминалов (Terminal Services Configuration), на вкладке Удаленное управление (Remote Control) окна свойств учетной записи пользователя или в групповой политике.

  Для удаленного управления активным сеансом еще одного пользователя на сервере терминалов можно также использовать инструмент командной строки Shadow.

  Для удаленного управления сеансом еще одного пользователя в подключении сервера RDP-Tcp требуется разрешение Полный доступ (Full Control) или особое разрешение доступа Удаленное управление (Remote Control).

ПРИМЕЧАНИЕ Использование функции удаленного управления в диспетчере служб терминалов

Для использования компонента Удаленное управление (Remote Control) в TSM вы должны быть подключены к серверу терминалов в сеансе клиента. При выполнении локального входа на сервер терминалов этот компонент отключается в диспетчере служб терминалов.

- **Сброс (Reset)** При выполнении сброса сеанс служб терминалов немедленно удаляется без сохранения данных сеанса. Сброс сеанса следует выполнять только в том случае, если он перестает реагировать на запросы.

  Для сброса пользовательского сеанса на сервере терминалов вы также можете использовать команду *Rwinsta* или *Reset session* из командной строки. Для сброса сеанса TS еще одного пользователя в подключении сервера RDP-Tcp требуется разрешение Полный доступ (Full Control).
- **Состояние (Status)** Если щелкнуть правой кнопкой мыши сеанс пользователя на вкладке Пользователи (Users) и задать команду контекстного меню Состояние (Status), откроется диалоговое окно Состояние (Status), содержащее дополнительные сведения о состоянии сеанса. Представленная здесь информация включает IP-адрес TS-клиента, имя компьютера и общее количество байтов, которые были переданы во время сеанса. Такое диалоговое окно показано на рис. 4-11.

  Для просмотра состояния сеанса еще одного пользователя вы должны располагать разрешением Полный доступ (Full Control) или Особое разрешение (Query Information) в подключении DRP-Tcp сервера.
- **Завершить сеанс (Log Off)** При завершении сеанса прекращаются все пользовательские процессы, после чего сеанс удаляется с сервера терминалов.

Перед завершением сеанса пользователя отправьте ему сообщение. В противном случае пользователь может потерять несохраненные данные сеанса.
Помимо диспетчера служб терминалов для завершения сеанса пользователя можно также использовать команду *Logoff* из командной строки. Для завершения сеанса еще одного пользователя вы должны располагать разрешением Полный доступ (Full Control) в подключении DRP-Tcp сервера.

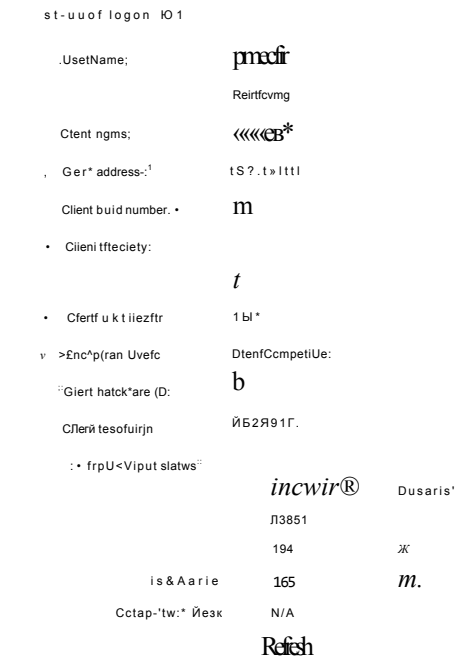


Рис. 4-11. Диалоговое окно Состояние (Status) диспетчера служб терминалов

Завершение процесса сеанса пользователя TS

Вкладку Процессы (Processes) диспетчера можно использовать для завершения отдельных процессов в сеансе пользователя. Такая потребность может возникнуть, например, в случае, если определенное приложение вызывает зависание пользовательского сеанса. Для завершения сбойного процесса достаточно щелкнуть его правой кнопкой мыши и выбрать команду Завершить процесс (End), как показано на рис. 4-12. Для завершения процесса в сеансе пользователя служб терминалов можно также применять команду *Tskill* из командной строки.

Проверьте себя

- Что представляет собой сеанс консоли на сервере терминалов?

Ответ

- Сеанс консоли является сеансом локально вошедшего пользователя.

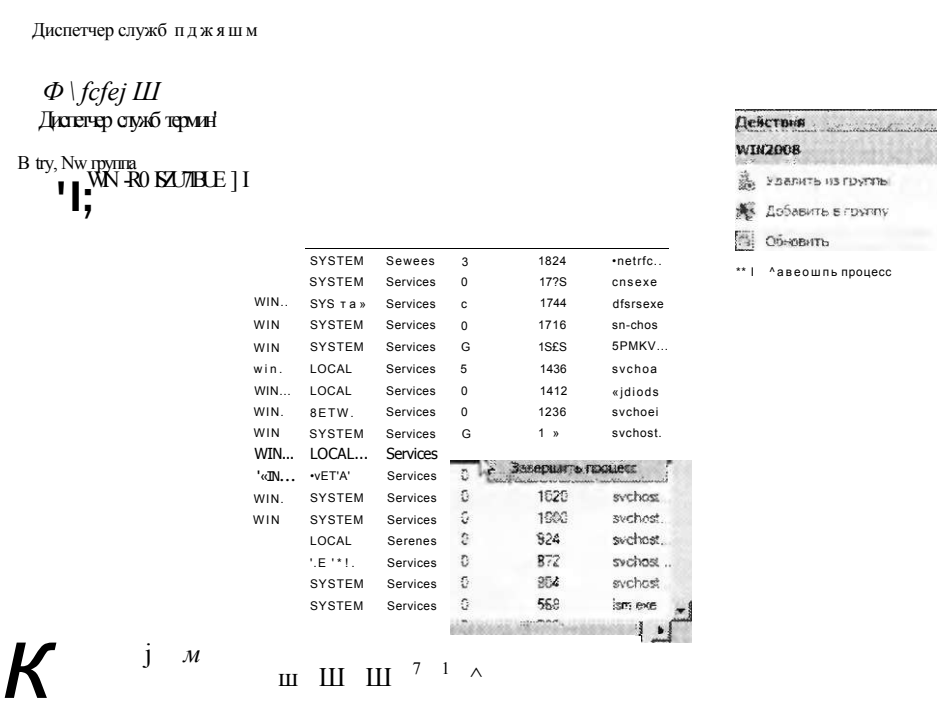


Рис. 4-12. Завершение процесса в сеансе пользователя TS

Управление ресурсами в клиентских сеансах

Диспетчер системных ресурсов Windows (Windows Server Resource Manager, WSRM) можно использовать в системе Windows Server 2008 для предоставления всем подключающимся к серверу терминалов клиентам равноценного доступа к ресурсам сервера. Чтобы установить WSRM, нужно открыть Диспетчер сервера (Server Manager), выбрать узел Компоненты (Features), а затем щелкнуть ссылку Добавить компоненты (Add Features). После этого для выбора компонента и выполнения его установки можно использовать Мастер добавления компонентов (Add Features Wizard). После установки компонента доступ к диспетчеру системных ресурсов можно получить через Администрирование (Administrative Tools).

Диспетчер системных ресурсов WSRM (Windows Server Resource Manager) использует Политики выделения ресурсов (Resource Allocation Policies) для распределения ресурсов компьютера между запущенными процессами. В любое время управляющей политикой является лишь одна политика выделения ресурсов.

В WSRM встроены четыре политики выделения ресурсов, две из которых предназначены для компьютеров со службами терминалов.

- **Equal_Per_User** Если эту политику назначить в качестве управляющей, доступные ресурсы CPU будут равноценно распределяться между пользователями. Например, если два пользователя запускают множество приложений, использующих 100 % выделенных ресурсов CPU, диспетчер WSRM снижая

приоритет запускаемых пользователем процессов, расходующих больше 50 % ресурсов CPU. В данной политике количество сеансов служб терминалов каждого пользователя не учитывается.

- **Equal_Per_Session** Если реализовать политику выделения ресурсов Equal_ Per Session, ресурсы CPU будут равномерно распределены между сеансами всех пользователей (и их процессов). Например, если два пользователя запускают два отдельных сеанса на сервере терминалов, каждый из которых занимает 100 % выделенных ресурсов CPU, диспетчер WSRM снижает приоритет процессов в сеансе служб терминалов, расходующих больше 25 % ресурсов CPU.

В целом эти встроенные Политики выделения ресурсов (Resource Allocation Policies) диспетчера WSRM гарантируют равномерное распределение доступных ресурсов сервера между пользователями или сеансами. Тем не менее диспетчер WSRM можно также использовать для создания настраиваемых политик выделения ресурсов. При создании настраиваемой политики выделения ресурсов определяется Условие соответствия процессов (Process Matching Criteria) с указанием служб, процессов или приложений на локальном сервере. В политике выделения ресурсов можно затем выделить для этих служб, процессов или приложений определенный объем ресурсов CPU или памяти.

СОВЕТ Подготовка к экзамену

Для сдачи сертификационного экзамена 70-643 нужно знать политики выделения ресурсов Equal Per User и Equal Per Session. Вам также следует понимать, какую роль играет условие соответствия процессов в настраиваемой политике выделения ресурсов.

Практикум. Управление клиентскими подключениями

В предложенных далее упражнениях вы будете использовать консоль TSM для просмотра сеансов, управления ими, а также для завершения сеансов пользователей служб терминалов.

Упражнение 1. Просмотр сеансов служб терминалов

Выполняя это упражнение, вы должны использовать консоль TSM для просмотра сеансов служб терминалов (TS) из сеанса консоли (локальный вход на сервер). Здесь потребуются три отдельные учетные записи администраторов домена, которые далее называются как ContosoAdminl, ContosoAdmin2 и ContosoAdmin3.

1. Войдите на компьютер Contoso.com с сервера Server2 с учетной записью ContosoAdminl.
2. Откройте Диспетчер служб терминалов (Terminal Services Manager). Для этого щелкните Пуск (Start), откройте Администрирование (Administrative Tools), откройте Службы терминалов (Terminal Services) и щелкните элемент Диспетчер служб терминалов (Terminal Services Manager).
3. Если откроется окно сообщения диспетчера служб терминалов, прочитайте содержащийся там текст и щелкните ОК.

4. В дереве консоли выберите узел Server2. На средней панели консоли будет указано Управление сервером терминалов: Server2 (Manage Terminal Server: Server2). Эта панель содержит три вкладки: Пользователи (Users), Сеансы (Sessions) и Процессы (Processes).
5. На средней панели выберите вкладку Пользователи (Users) и ответьте на следующие вопросы.
   Сколько пользователей подключено к серверу?
   Ответ: Один.
   Какой тип сеанса указан для перечисленных пользователей?
   Ответ: Консоль.
   С каким пользователем связан этот сеанс — локальным или удаленным?
   Ответ: локальным.
6. Щелкните правой кнопкой мыши пользователя, отображаемого на вкладке Пользователи (Users), и ответьте на следующие вопросы.
   Какие команды доступны в контекстном меню?
   Ответ: Отключить (Disconnect), Отправить сообщение (Send Message) и Завершить сеанс (Log Off).
   Какие из команд, перечисленных в контекстном меню, являются недоступными?
   Ответ: Подключиться (Connect), Удаленное управление (Remote Control), Сброс (Reset) и Состояние (Status).
   Почему эти команды недоступны?
   Ответ: Команды Подключиться (Connect) и Удаленное управление (Remote Control) нельзя выполнять из сеанса консоли. Команды Сброс (Reset) и Состояние (Status) можно выполнять лишь для сеанса еще одного пользователя.
7. Войдите на Contoso.com с сервера Serverl с учетной записью ContosoAdmin2.
8. На сервере Serverl запустите клиента Подключение к удаленному рабочему столу (Remote Desktop Connection).
9. В текстовое поле Компьютер (Computer) введите *setver2.contoso.com* и щелкните кнопку Подключить (Connect).
10. В диалоговом окне Безопасность Windows (Windows Security) введите учетные данные ContosoAdmin2 и щелкните ОК. Учетную запись пользователя нужно ввести в формате contoso\contosoadmin2.
11. На сервере Serverl сверните окно Удаленный рабочий стол (Remote Desktop).
12. На сервере Serverl откройте еще один экземпляр программы Подключение к удаленному рабочему столу (Remote Desktop Connection).
13. В текстовое поле Компьютер (Computer) введите *setver2.contoso.com* и щелкните кнопку Подключить (Connect).
14. В диалоговом окне Безопасность Windows (Windows Security) щелкните опцию Другая учетная запись (Use Another Account).
15. Используйте текстовые поля для ввода учетных данных ContosoAdmin3 и щелкните ОК. Имя пользователя нужно вводить в формате contoso\contosoadmin3.

16. Вернитесь к диспетчеру служб терминалов TSM на сервере Server2. Обновите вкладку Пользователи (Users) с помощью команды Обновить (Refresh) из панели Действия (Actions).
17. Ответьте на следующие вопросы.

    Сколько сеансов пользователей теперь отображается на вкладке Пользователи (Users)?

    Ответ: Три.

    Какой тип сеанса указан для ContosoAdmin2 и ContosoAdmin3?

    Ответ: RDP-Tcp.

    Какие две команды, которые недоступны для сеанса консоли, теперь доступны для сеансов RDP-Tcp?

    Ответ: Сброс (Reset) и Состояние (Status).

    В чем разница между командами Сброс (Reset) и Завершить сеанс (Log Off)?

    Ответ: Обе команды отключают и завершают сеанс. Однако команда Сброс (Reset) сразу удаляет сеанс без завершения работы пользователя.
18. Оставьте все окна открытыми и переходите к выполнению упражнения 2.

Упражнение 2. Управление сеансами служб терминалов

В этом упражнении вы будете управлять одним сеансом служб терминалов из другого сеанса. Для выполнения упражнения у вас должны быть запущены два активных сеанса TS с сервера Serverl на сервере Server2.

1. Вернитесь к серверу Serverl.
2. В сеансе удаленного рабочего стола ContosoAdmin2 откройте Диспетчер служб терминалов (Terminal Services Manager). Чтобы отличать два сеанса удаленного рабочего стола, можно использовать меню Пуск (Start).
3. Ответьте на следующий вопрос.

   Какой сеанс на вкладке Пользователи (Users) помечен зеленой стрелкой, направленной вверх?

   Ответ: Сеанс пользователя ContosoAdmin2.
4. На сервере Serverl переключитесь к окну сеанса удаленного рабочего стола ContosoAdmin3. Если экран заблокирован, введите учетные данные, чтобы вновь открыть рабочий стол сервера Server2.
5. Пометьте рабочий стол ContosoAdmin3, чтобы его можно было распознать как рабочий стол пользователя ContosoAdmin3. Например, вы можете сохранить на рабочем столе файл блокнота ADMIN3.
6. Вернитесь к окну сеанса удаленного рабочего стола ContosoAdmin2. В диспетчере служб терминалов щелкните правой кнопкой мыши сеанс пользователя ContosoAdmin3 и примените команду Удаленное управление (Remote Control).
7. В диалоговом окне Удаленное управление (Remote Control) прочитайте весь текст и щелкните ОК.
8. Переключитесь к окну сеанса удаленного рабочего стола ContosoAdmin3. Откроется диалоговое окно Запрос удаленного управления (Remote Control Request). В этом окне указано, что пользователь ContosoAdmin2 запрашивает удаленное управление вашим сеансом.

9. В диалоговом окне Запрос удаленного управления (Remote Control Request) щелкните кнопку Да (Yes).
10. Вернитесь к сеансу удаленного рабочего стола ContosoAdmin2. Теперь рабочий стол ContosoAdmin3 будет отображаться в сеансе ContosoAdmin2.
11. В окне удаленного управления выполните любое действие, например откройте программу Блокнот (Notepad). Теперь пользователь ContosoAdmin2 может управлять рабочим столом ContosoAdmin3.
12. Переключитесь к серверу Server2.
13. На вкладке Пользователи (Users) диспетчера служб терминалов щелкните правой кнопкой мыши сеанс ContosoAdmin3 и примените команду Завершить сеанс (Log Off).
14. В диалоговом окне Диспетчер служб терминалов (Terminal Services Manager) щелкните OK для подтверждения своего действия. Сеанс ContosoAdmin3 будет завершен. Чтобы сеанс этого пользователя исчез из списка, может потребоваться выполнить действие Обновить (Refresh).
15. На вкладке Пользователи (Users) диспетчера служб терминалов щелкните правой кнопкой мыши сеанс ContosoAdmin2 и примените команду Отключить (Disconnect).
16. В диалоговом окне Диспетчер служб терминалов (Terminal Services Manager) щелкните OK для подтверждения команды. Состояние сеанса ContosoAdmin2 изменится с Active на Disconnected. Для отображения этого изменения, возможно, потребуется выполнить действие Обновить (Refresh).
17. Оставьте все окна открытыми и переходите к выполнению упражнения 3.

Упражнение 3. Повторное подключение к отключенному сеансу

В этом упражнении вы повторно подключитесь к отключенному сеансу. Затем вы попытаетесь вновь подключиться к серверу терминалов с помощью того же пользовательского имени и проверите результат.

1. В диспетчере служб терминалов на сервере Server2 откройте вкладку Сеансы (Sessions), на которой указано, что сеанс ContosoAdmin2 отключен.
2. Перейдите на вкладку Процессы (Processes). На этой вкладке указаны все еще запущенные процессы сеанса ContosoAdmin2.
3. Щелкните правой кнопкой мыши любой из перечисленных процессов. В контекстном меню есть команда завершения процесса. Процесс также можно завершить с помощью опции Завершить процесс (End Process) панели Действия (Actions) консоли TSM. Кроме того, процесс можно завершить с помощью команды *Tskill* из командной строки.
4. Не завершая выбранный процесс, переключитесь к серверу Server1. Должно открыться окно сообщения Удаленный рабочий стол отключен (Remote Desktop Disconnected), где указано, что сеанс удаленного рабочего стола ContosoAdmin2 отключен.
5. В диалоговом окне сообщения об отключении удаленного рабочего стола щелкните OK. На рабочем столе появится окно подключения к удаленному рабочему столу.

6. Используйте клиент Подключение к удаленному рабочему столу (Remote Desktop Connection) и учетные данные ContosoAdmin2 для установки нового подключения к серверу Server2 с сервера Serverl.
7. Переключитесь к серверу Serverl.
8. В консоли диспетчера служб терминалов на сервере Server2 щелкните вкладку Пользователи (Users). Обратите внимание на то, что сеанс ContosoAdmin2 вновь указан как активный (Active).
9. Переключитесь к серверу Serverl.
10. Сверните текущее окно сеанса удаленного рабочего стола на сервере Serverl.
11. С помощью меню Пуск (Start) откройте Подключение к удаленному рабочему столу (Remote Desktop Connection).
12. Чтобы попытаться создать второй сеанс служб терминалов на сервере Server2, используйте учетные данные ContosoAdmin2.
13. Проанализируйте данные во всех открытых окнах на серверах Serverl и Server2, а затем ответьте на следующий вопрос.

    Могли ли вы установить второй одновременный сеанс служб терминалов на сервере Server2?

    Ответ: Нет. Второе подключение попытается лишь взять под контроль активный пользовательский сеанс, так что первое подключение будет удалено.
14. Переключитесь к серверу Server2.
15. Откройте консоль Конфигурация служб терминалов (Terminal Services Configuration, TSC). Для этого щелкните Пуск (Start), откройте Администрирование (Administrative Tools), откройте Службы терминалов (Terminal Services) и щелкните элемент Конфигурация служб терминалов (Terminal Services Configuration).
16. В центральной панели консоли TSC в разделе Изменить настройки — Общие (Edit Settings — General) дважды щелкните опцию Ограничить пользователя единственным сеансом (Restrict Each User To A Single Session).
17. В диалоговом окне Свойства (Properties) сбросьте флажок Ограничить пользователя единственным сеансом (Restrict Each User To A Single Session) и щелкните ОК.
18. Если появится сообщение об ошибке конфигурации служб терминалов, прочитайте его и щелкните ОК.
19. Вернитесь к серверу Serverl и вновь попытайтесь установить второе подключение к удаленному рабочему столу сервера Server2 с использованием учетных данных ContosoAdmin2. Будет установлено второе подключение к удаленному рабочему столу. Если щелкнуть кнопку Обновить (Refresh) в консоли диспетчера служб терминалов на сервере Server2, отобразятся два сеанса ContosoAdmin2 в состоянии Active. Следует отметить, что при включении одновременных сеансов на компьютере с запущенными службами терминалов появляется возможность создания цепочки сеансов.
20. На сервере Server2 используйте диспетчер служб терминалов для завершения первого сеанса ContosoAdmin2 и сброса второго.

21. На сервере Server2 используйте диспетчер служб терминалов, чтобы вновь включить ограничение каждого пользователя одним сеансом.
22. Закройте все открытые окна на серверах Server1 и Server2 и завершите сеансы всех пользователей.

Резюме

- Параметры TS-клиента можно конфигурировать на стороне клиента с помощью опции Подключение к удаленному рабочему столу (Remote Desktop Connection) или на уровне домена с помощью объекта групповой политики GPO.
- При подключении пользователей к серверу терминалов их профили по умолчанию сохраняются на удаленному сервере. В результате получения множеством пользователей доступа к серверу терминалов профили могут занимать немало места на диске. Для экономии дискового пространства можно использовать дисковые квоты.
- Профилем пользователя TS можно управлять, отконфигурировав перемещаемый профиль пользователя служб терминалов, который хранится в центральном сетевом ресурсе. Этот перемещаемый профиль пользователя служб терминалов можно определить на вкладке Профиль служб терминалов (Terminal Services Profile) окна свойств учетной записи пользователя или в групповой политике.
- Диспетчер служб терминалов (Terminal Services Manager, TSM) — основной административный инструмент, используемый для управления подключениями на сервере терминалов. Его можно применять для просмотра информации о пользователях, подключенных к серверу терминалов, для отслеживания сеансов пользователей, выполнения таких административных задач, как завершение или отключение сеансов пользователей.
- Диспетчер системных ресурсов Windows (Windows System Resource Manager, WSRM) можно использовать для равномерного распределения ресурсов сервера терминалов между пользователями или сеансами.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных в ходе занятия 1. Эти вопросы представлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы
Ответы и пояснения к каждому их варианту размещены в разделе «Ответы» в конце книги.

1. На сервере TS1 запущена система Windows Server 2008 и Службы терминалов (Terminal Services). Пользователи в организации подключаются к серверу TS1 для запуска бизнес-приложения. В последнее время вы обратили внимание на то, что пользовательские профили угрожают занять все дисковое пространство сервера TS1. Вы хотите, чтобы пользователи могли сохра-

нять свои данные, но их профили не занимали все дисковое пространство на TS1. Какие действия следует предпринять?

А. Использовать групповую политику для назначения обязательных профилей пользователям, подключающимся к TS1.

Б. (Сконфигурировать дисковые квоты на диске TS1, где хранятся пользовательские профили.

В. Использовать групповую политику для назначения перемещаемых пользовательских профилей служб терминалов пользователям, которые подключаются к TS1.

Г. Отконфигурировать дисковые квоты локального диска каждого пользователя, который подключается к TS1.

2. На сервере TS3 запущена система Windows Server 2008 и Службы терминалов (Terminal Services). Вам нужно поддерживать пользователей, которые подключаются к TS3 для запуска различных приложений. Пользователи жалуются, что приложение медленно реагирует. С помощью команды *quser* на сервере TS3 вы определили, что многие пользователи располагают на сервере множеством отключенных сеансов, время простоя которых составляет несколько дней. Вы хотите снизить нагрузку TS3, удаляя отключенные сеансы с временем простоя более двух дней. Какие действия следует предпринять в этом случае?

А. Использовать команду *Rwinsta.*

Б. Использовать команду *Tsdicon.*

В. Использовать команду *Tskill.*

Г. Использовать команду *Tscon.*

Занятие 2. Развертывание шлюза служб терминалов

Шлюз служб терминалов (Terminal Services Gateway, TS Gateway) позволяет авторизованным пользователям устанавливать подключения к серверам терминалов, расположенным за брандмауэром. Шлюз TS играет очень важную роль. Ранее для подключения к ресурсам в частной сети из Интернета приходилось использовать частную виртуальную сеть (Virtual Private Network, VPN). Теперь вы можете подключаться к еще большему количеству ресурсов, включая рабочие столы сервера терминалов и опубликованные приложения, с помощью технологии, которую намного проще реализовать.

На этом занятии мы рассмотрим принципы установки, конфигурирования и использования шлюза служб терминалов.

Изучив материал этого занятия, вы сможете:

- Описать работу шлюза служб терминалов.
- Установить шлюз служб терминалов.
- Отконфигурировать шлюз служб терминалов.
- Настроить подключение к удаленному рабочему столу для использования шлюза служб терминалов.

Расчетная продолжительность занятия составляет 50 мин.

Шлюз служб терминалов

Шлюз служб терминалов (TS Gateway) представляет собой опциональный компонент, позволяющий авторизованным клиентам удаленного рабочего стола устанавливать сеанс RDP (Remote Desktop Protocol) между Интернетом и ресурсами служб терминалов, расположенными за брандмауэром в частной сети. (В данном случае выражение «ресурсы служб терминалов» означает серверы терминалов и компьютеры с включенным компонентом Удаленный рабочий стол (Remote Desktop).)

Поскольку передача данных осуществляется через Интернет, RDP-подключения к серверу шлюза служб терминалов защищены и зашифрованы протоколом Secure Sockets Layer (SSL).

Ключевая особенность шлюза служб терминалов состоит в том, что он пропускает поток RDP-трафика через TCP-порт 443 корпоративных брандмауэров, который обычно открыт для SSL-трафика. (По умолчанию RDP-трафик проходит через TCP-порт 3389.)

В базовом развертывании шлюза служб терминалов, схема которого показана на рис. 4-13, пользователь домашнего компьютера (под номером 1) подключается через Интернет к шлюзу служб терминалов (под номером 2), расположенному за внешним корпоративным брандмауэром.

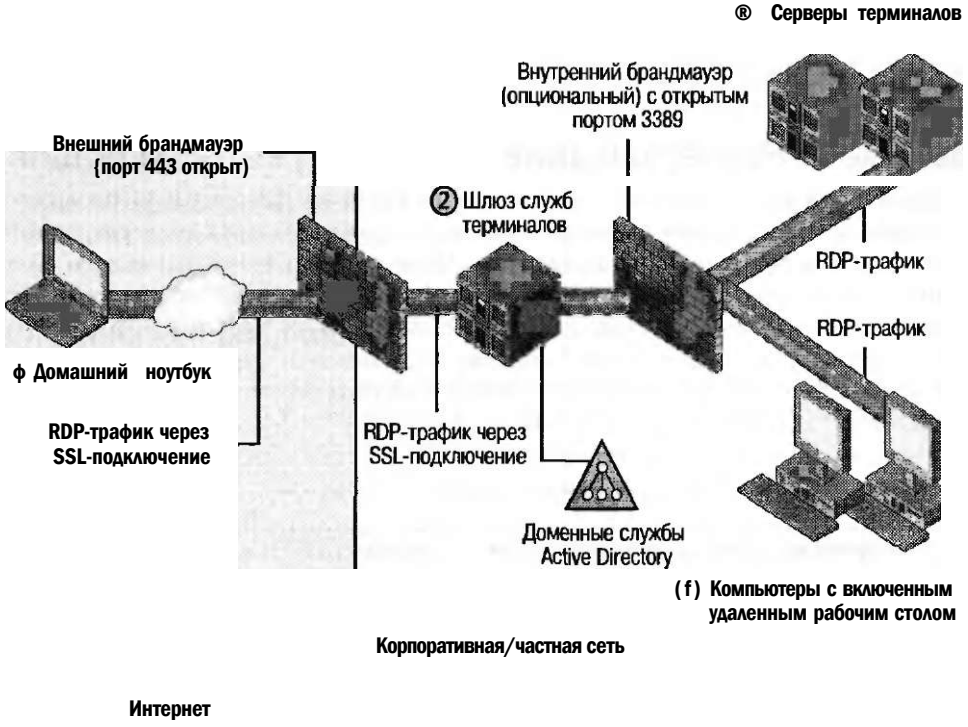


Рис. 4-13. Базовый сценарий работы шлюза служб терминалов

Подключение от точки 1 к точке 2 устанавливается протоколом RDP, инкапсулированным в туннель HTTPS (HTTP через SSL). Для получения этого HTTPS-подключения в периметре сети на сервере шлюза служб терминалов должен быть запущен веб-сервер Internet Information Services (IIS). После приема подключения сервер TS-шлюза извлекает данные HTTPS и направляет RDP-пакеты на конечные серверы терминалов (под номером 3), расположенные за вторым, внутренним брандмауэром. Если в данном сценарии требуется разрешить или запретить входящие подключения к учетным записям Active Directory, на шлюзе служб терминалов нужно установить Службу каталогов Active Directory (Active Directory Domain Services).

В качестве альтернативы базовому сценарию, схема которого показана на рис. 4-13, вы можете использовать вместо сервера шлюза служб терминалов (TS Gateway) сервер ISA (Internet Security and Acceleration) как конечную точку SSL/HTTPS для входящего подключения TS-клиепта.

В данном сценарии, схема которого показана на рис. 4-14, ISA-сервер (под номером 2) выступает в качестве моста HTTPS-to-HTTPS или IITTPS-to-IITTP к серверу шлюза TS (под номером 3), а сервер шлюза TS затем направляет RDP-подключение к соответствующему внутреннему ресурсу (под номером 4). Этот метод обеспечивает преимущество защиты информации Active Directory в корпоративной сети.

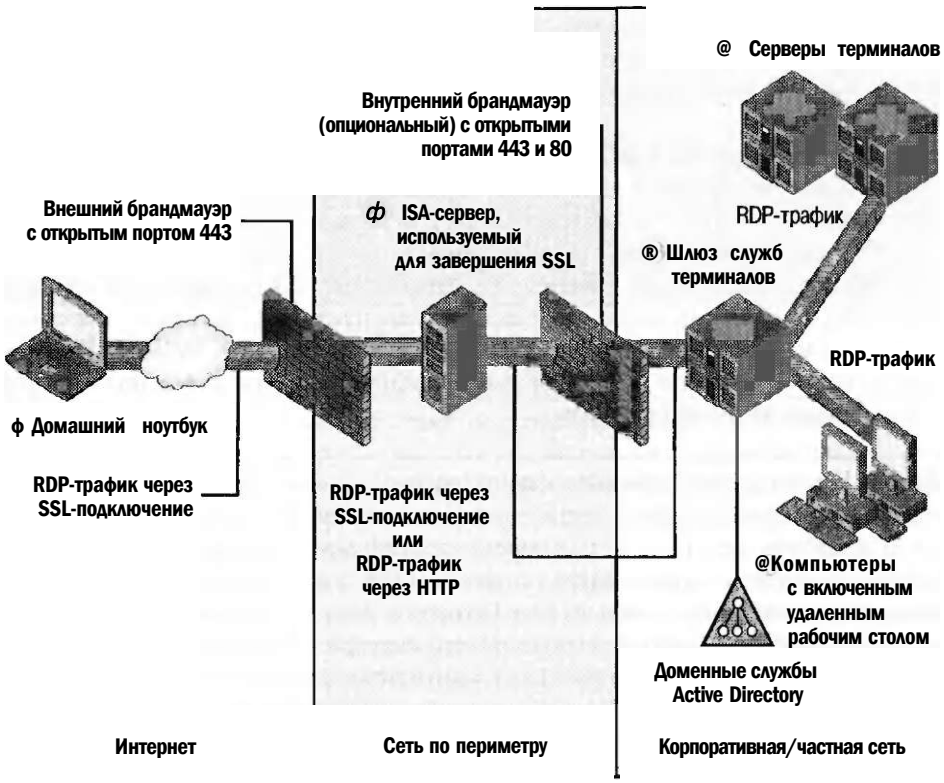


Рис. 4-14. TS-шлюз с ISA-сервером, используемым для завершения SSL

СОВЕТ Подготовка к экзамену
При использовании ISA-сервера в качестве моста HTTPS-to-HTTPS к шлюзу служб терминалов не забудьте экспортировать сертификат сервера, применяемый к SSL-подключению с сервера шлюза TS к компьютеру с ISA-сервером, и установить этот сертификат на последнем сервере.

Установка и настройка сервера шлюза служб терминалов

Сервер шлюза TS можно установить и отконфигурировать, добавив вначале роль службы шлюза TS, а затем отконфигурировав клиентов для указания сервера шлюза служб терминалов. Эти шаги детально описаны в следующем разделе.

Добавление роли службы шлюза TS

При добавлении роли шлюза служб терминалов с помощью Диспетчера сервера (Server Manager) запускается мастер Добавление служб ролей (Add Role Services Wizard), который выполняет две основные задачи. Во-первых, он автоматически устанавливает (при необходимости) предварительные роли для шлюза служб терминалов — веб-сервер IIS и сервер сетевых политик NPS (Network Policy Server). Во-вторых, он выполняет процесс настройки трех компонентов шлюза TS, которые требуются для функционирования роли, — сертификата сервера для шифрования SSL, сетевой политики авторизации подключений к службам терминалов (TS Connection Authorization Policy, TS CAP) и политик авторизации ресурсов служб терминалов (TS Resource Authorization Policy, TS RAP).

- **Сертификат сервера для SSL** Подключения TS-клиентов к шлюзу служб терминалов шифруются с помощью протокола SSL (также известного как протокол Transport Layer Security (TLS)), который требует сертификат сервера. Этот сертификат может быть получен от доверенного стороннего центра сертификации (CA) или доверенного локального CA (например, Certificate Services). В качестве менее защищенного варианта, подходящего для тестовых сред, мастер Добавление служб ролей (Add Role Services Wizard) может также самостоятельно генерировать сертификат сервера для использования со шлюзом служб терминалов.

ВАЖНО! Клиент должен доверять корневому сертификату сервера
Каждый TS-клиент, который подключается к серверу шлюза служб терминалов, должен доверять центру CA, издавшему сертификат сервера шлюза TS. Если сертификат издан не доверенным сторонним CA и не центром CA, интегрированным в собственный домен Active Directory клиента, вы должны экспортировать и установить корневой сертификат сервера шлюза служб терминалов (TS Gateway Server Root Certificate) в хранилище доверенных корневых центров сертификации (Trusted Root Certification Authorities) клиента служб терминалов. Это хранилище можно просмотреть с помощью оснастки Сертификаты (Certificates). Указанная процедура описана в практическом разделе в конце данного занятия.

На рис. 4-15 показана страница мастера, на которой можно указать или создать сертификат сервера для шифрования SSL.

TS CAP Политика TS **CAP** определяет внешних пользователей **и** компьютеры, которые могут подключаться к шлюзу служб терминалов. Мастер Добавление служб ролей (Add Role Services Wizard) позволяет создать лишь первую и исходную политику TS CAP, однако позже вы сможете с помощью административной консоли Диспетчер шлюза служб терминалов (TS Gateway Manager) создать другие политики.

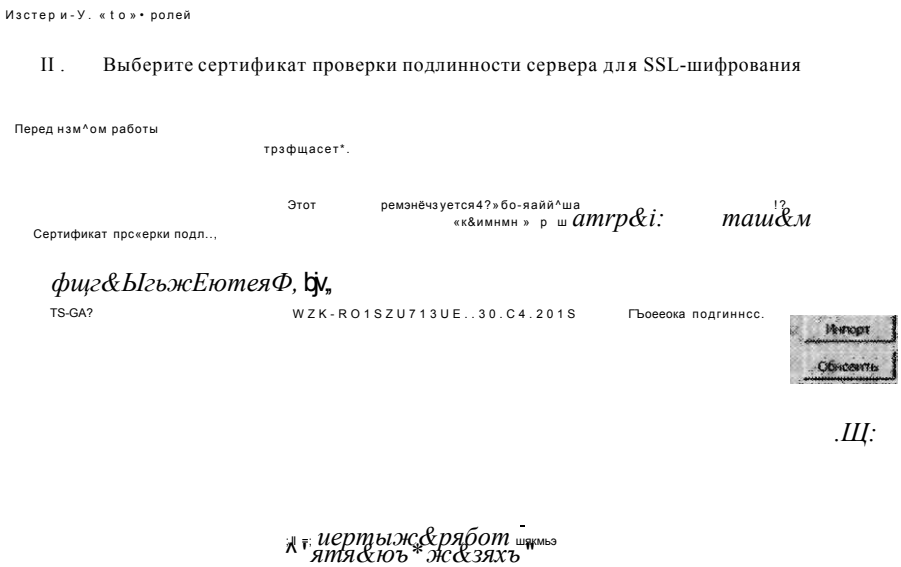


Рис. 4-15. **Выбор сертификата сервера для шифрования SSL**

ПРИМЕЧАНИЕ Диспетчер шлюза служб терминалов и политики TS CAP

Чтобы запустить Диспетчер шлюза служб терминалов, щелкните кнопку Пуск (Start), откройте Администрирование (Administrative Tools), откройте Службы терминалов (Terminal Services) и щелкните элемент Диспетчер шлюза служб терминалов (TS Gateway Manager).

Если вы хотите создать в диспетчере шлюза служб терминалов новую политику TS CAP, в дереве консоли щелкните правой кнопкой мыши папку Политики авторизации подключений (Connection Authorization Policies), примените команду Создать новую политику (Create New Policy) и укажите тип Мастер (Wizard) или Другое (Custom) но своему усмотрению. Для модификации свойств существующей политики TS CAP в панели Политики авторизации подключений (Connection Authorization Policies) щелкните правой кнопкой мыши политику TS CAP и примените команду Свойства (Properties).

На странице Выберите группы пользователей, подключающихся через шлюз TS (Select User Group That Can Connect Through TS Gateway) мастера Добавление служб ролей (Add Role Services Wizard), процесс создания первой политики TS CAP упрощен и позволяет указать пользователей (как правило, группы безопасности Active Directory), которым разрешено подключаться (рис. 4-16). Эти же группы пользователей затем становятся доступными для основной политики TS RAP, создаваемой далее мастером.

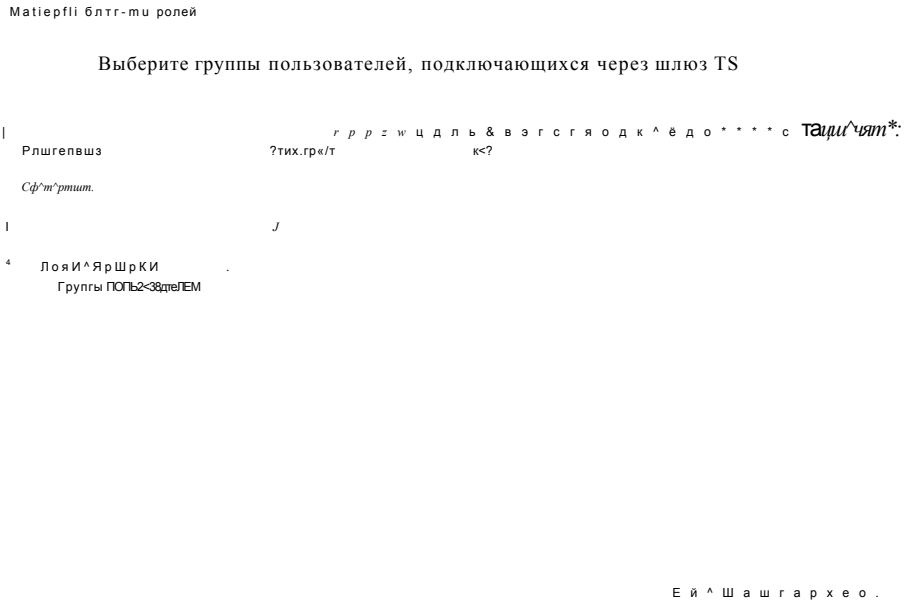


Рис. 4-16. Определение групп для политик TS CAP и TS RAP

Отметим, что политика TS CAP также позволяет выбрать метод аутентификации удаленных пользователей: Пароль (Password), Смарт-карта (Smart Card) или оба.

При использовании консоли Диспетчер шлюза служб терминалов (TS Gateway Manager) для создания или модификации политики TS CAP вы можете указать компьютеры, для которых разрешен доступ к шлюзу TS, и ограничить перенаправление устройств (опция, доступная только в диспетчере шлюза служб терминалов). Другими словами, вы можете использовать TS CAP для предотвращения перенаправления таких клиентских устройств, как USB-диски, в сеанс пользователя TS через шлюз служб терминалов.

Окно свойств TS CAP в диспетчере шлюза служб терминалов показано на рис. 4-17.

TS RAP Политика шлюза служб терминалов TS RAP определяет пользователей, которые могут подключаться к определенным ресурсам служб тер-

миналов в организации. Мастер Добавление служб ролей (Add Role Services Wizard) позволяет создать первую и исходную политику TS RAP, однако позже вы сможете создать другие политики с помощью диспетчера шлюза служб терминалов.

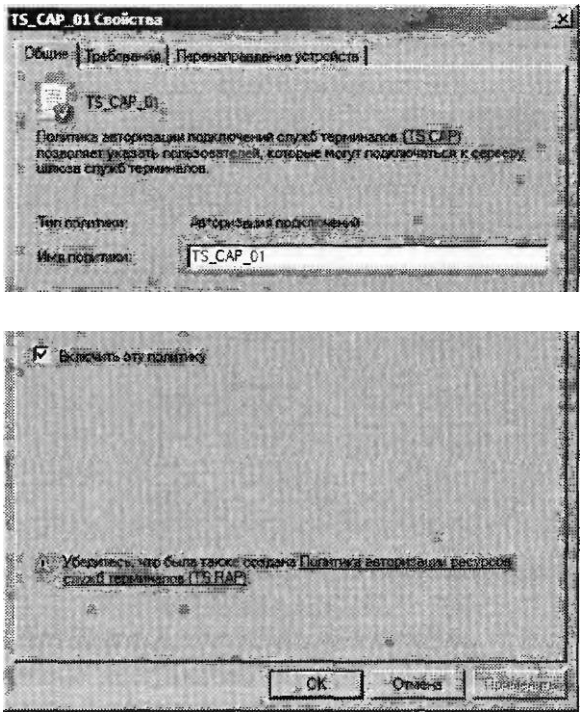


Рис. 4-17. Модификация политики TS CAP

ПРИМЕЧАНИЕ Диспетчер шлюза служб терминалов и политики TS RAP
Чтобы создать в диспетчере шлюза служб терминалов новую политику TS RAP, в дереве консоли щелкните правой кнопкой мыши папку Политики авторизации ресурсов (Resource Authorization Policies), примените команду Создать новую политику (Create New Policy) и укажите тип Мастер (Wizard) или Другое (Custom) по своему усмотрению.
Для модификации свойств существующей политики TS RAP в панели Политики авторизации ресурсов (Resource Authorization Policies) щелкните правой кнопкой мыши политику TS RAP, а затем примените команду Свойства (Properties).

В упрощенной политике, которая создается мастером Добавление служб ролей (Add Role Services Wizard), группе пользователей, выбранной на странице Выберите группы пользователей, подключающихся через шлюз TS (Select User Group That Can Connect Through TS Gateway), можно разрешить доступ ко всем серверам терминалов в сети или ограничить доступ лишь подсетью, определенной группой безопасности Active Directory.

На рис. 4-18 показана страница Создайте TS RAP для шлюза служб терминалов (Create A TS RAP For TS Gateway) мастера Добавление служб ролей (Add Role Services Wizard).

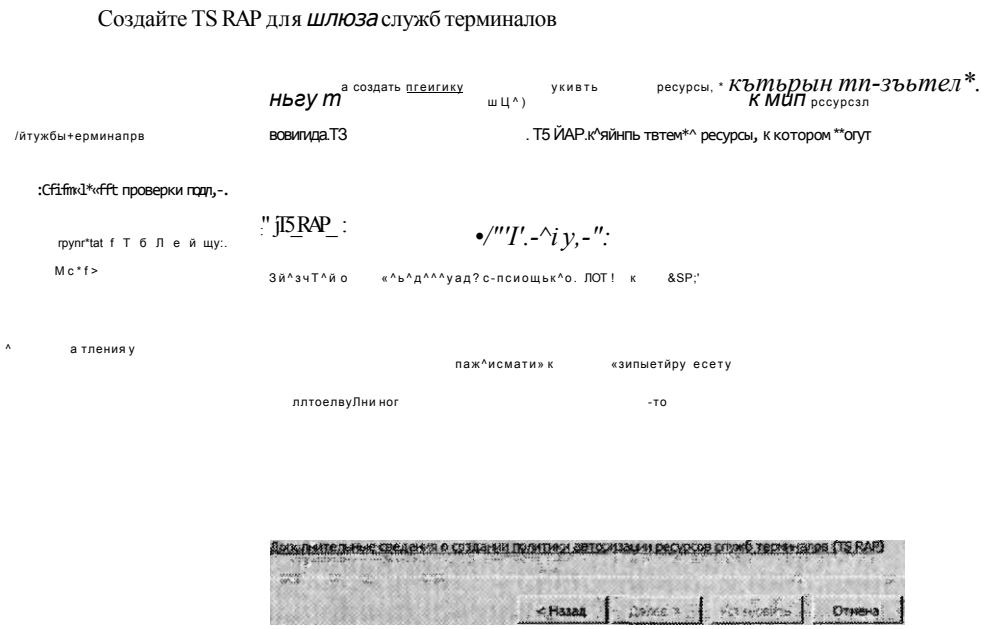
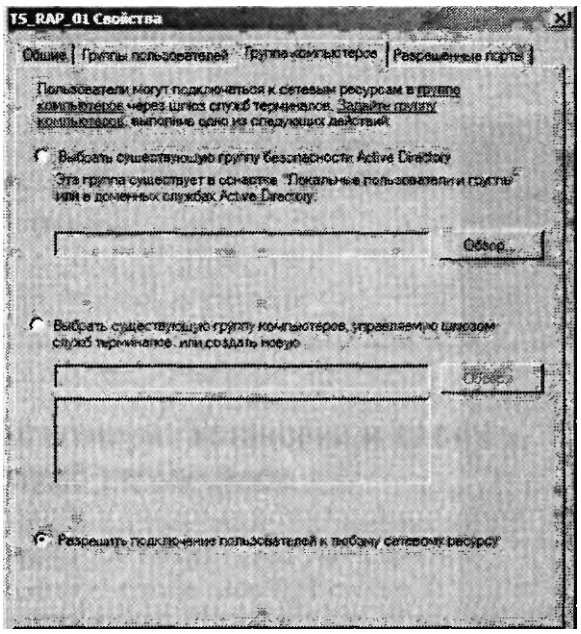


Рис. 4-18. Создание политики TS RAP мастером добавления служб ролей

Как и в случае с TS CAP, при использовании диспетчера шлюза служб терминалов для создания или модификации TS RAP можно применять дополнительные опции конфигурации. Например, при использовании диспетчера шлюза служб терминалов для создания TS RAP группой компьютеров, для которой разрешается доступ, может быть группа безопасности Active Directory или группа компьютеров, управляемая шлюзом TS (рис. 4-19). ГТослед-1ш#тип группы используется только для шлюза служб терминалов и создается в консоли Диспетчер служб терминалов (TS Gateway Manager). Второй опцией конфигурации TS RAP, доступной лишь в консоли диспетчера шлюза TS, является возможность управления TCP-портами, через которые клиент TS может подключаться к ресурсу, Например, вы можете ограничить все RDP-подключения TCP-портом 3389 (стандартный порт RDP-подключений) либо указать нестандартный порт или набор портов, на которых группа компьютеров будет прослушивать подключения.

СОВЕТ Подготовка к экзамену

Для просмотра сеансов текущих пользователей, подключенных через шлюз TS в диспетчере шлюза служб терминалов, используйте Узел Наблюдение (Monitoring).



<ж г Огфи*

Рис. 4-19. Указание группы компьютеров для политики TS RAP

Настройка подключения к удаленному рабочему столу с целью использования шлюза служб терминалов

Для того чтобы иметь возможность использовать Подключение к удаленному рабочему столу (Remote Desktop Connection, RDC) для инициирования подключений через шлюз служб терминалов, вы должны вначале отконфигурировать RDC для использования этого шлюза. Откройте RDC, щелкните кнопку Параметры (Options), потом перейдите на вкладку Подключение (Advanced), а затем в разделе Подключение из любого места (Connect From Anywhere) на вкладке Подключение (Advanced) щелкните кнопку Параметры (Settings), как показано на рис. 4-20. После этого на экран будет выведено диалоговое окно Параметры сервера шлюза служб терминалов (Gateway Server Settings), представленное на рис. 4-21.

В диалоговом окне Параметры сервера шлюза служб терминалов (Gateway Server Settings) выберите опцию Использовать следующие параметры шлюза служб терминалов (Use These TS Gateway Server Settings).

Затем укажите в поле Имя сервера (Server Name) сервер шлюза TS и соответствующий метод входа (пароль или смарт-карта) в поле Метод входа (Logon Method). Чтобы программа RDC использовала шлюз служб терминалов даже для компьютеров в локальной сети LAN, сбросьте флажок Не использовать шлюз служб терминалов для локальных адресов (Bypass TS Gateway Server Local Addresses).

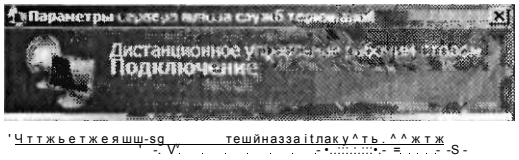
В разделе Параметры входа (Logon Settings) можно задать передачу сервером шлюза служб терминалов ваших учетных данных на конечный сервер термина-

лов. Эта опция выбрана по умолчанию. Тем не менее если вам нужно вводить на удаленном сервере другое пользовательское имя или пароль, сбросьте указанный флажок.

*..f-T^B^jS^
Ввет рг^ть гйрамвтры

I &

Рис. 4-20. Настройка RDC для использования шлюза служб терминалов, шаг 1



||

! r " ' *

•>^v^SSgrf-

СУХ

i

Рис. 4-21. Настройка RDC для использования шлюза служб терминалов, шаг 2

Проверьте себя

1. Какой тип политики авторизует подключения к шлюзу служб терминалов из Интернета?
2. Какой тип политики авторизует подключения шлюза служб терминалов к внутренним ресурсам?

Ответы

1. Политика TS CAP.
2. Политика TS RAP.

Практикум. Установка и настройка шлюза служб терминалов

В предлагаемых ниже упражнениях вы установите шлюз служб терминалов на сервере Server2, а затем настроите RDC на сервере Serverl для подключения к серверу терминалов через шлюз. Перед выполнением упражнений на сервере Serverl нужно установить сертификат сервера Server2.

Упражнение 1. Добавление служб ролей шлюза TS

Начнем же мы с установки службы роли шлюза TS на Server2.

1. Войдите на компьютер Contoso.com с сервера Server2 как доменный администратор.
2. Откройте Диспетчер сервера (Server Manager).
3. В дереве консоли Диспетчер сервера разверните Роли (Roles) и выберите узел Службы терминалов (Terminal Services).
4. В области Службы ролей (Role Services) панели сведений щелкните ссылку Добавить службы ролей (Add Role Services).
5. На странице Выбор служб ролей (Select Role Services) мастера Добавление служб ролей (Add Role Services Wizard) установите флажок Шлюз служб терминалов (TS Gateway). На этом этапе может открыться диалоговое окно Добавление служб ролей (Add Role Services), в котором будет предложено добавить службы ролей, требуемые для шлюза служб терминалов.
6. Если откроется диалоговое окно Добавление служб ролей (Add Role Services), щелкните кнопку Добавить требуемые службы роли (Add Required Role Services).
7. На странице Выбор служб ролей (Select Role Services) мастера Добавление служб ролей (Add Role Services) щелкните кнопку Далее (Next).
8. Ознакомьтесь с информацией, представленной на странице Выберите сертификат проверки подлинности сервера для SSL-шифрования (Choose A Server Authentication Certificate For SSL Encryption). На этом этапе в производственной среде назначается сертификат проверки подлинности сервера, полученный из доверенного центра CA. В тестовой среде мы используем самозаверяемый сертификат.

9. Выберите опцию Создать самозаверяемый сертификат для шифрования SSL (Create A Self-Signed Certificate For SSL Encryption) и щелкните кнопку Далее (Next).
10. На странице Создайте политики проверки подлинности для шлюза служб терминалов (Create Authorization Policies For TS Gateway) прочитайте всю информацию, оставьте опцию по умолчанию в разделе Создать политики авторизации (Create Authorization Policies) и щелкните кнопку Далее (Next).
11. Перейдя на страницу Выберите группы пользователей, подключающихся через шлюз TS (Select User Groups That Can Communicate Through TS Gateway), прочитайте излагаемую на ней информацию и щелкните кнопку Далее (Next).
12. На странице Создайте TS CAP для шлюза служб терминалов (Create A TS CAP For TS Gateway) также прочитайте всю информацию, оставьте флажок Пароль (Password) и щелкните кнопку Далее (Next).
13. Теперь прочитайте информацию на странице Создайте TS RAP для шлюза служб терминалов (Create A TS RAP For TS Gateway) и выберите опцию, позволяющую пользователям подключаться к любому компьютеру в сети. Щелкните кнопку Далее (Next).
14. Ознакомьтесь с информацией, представленной на странице Службы политики сети и доступа (Network Policy And Access Services), после чего щелкните кнопку Далее (Next).
15. На странице Выбор служб ролей (Select Role Services) прочитайте весь текст и щелкните кнопку Далее (Next).
16. Прочтите информацию, содержащуюся на странице Веб-сервер (IIS) (Web Server (IIS)), и щелкните кнопку Далее (Next).
17. На странице Выбор служб ролей (Select Role Services) щелкните кнопку Далее (Next).
18. На странице Подтвердите выбранные элементы (Confirm Installation Selections) просмотрите выбранные для установки элементы и щелкните кнопку Установить (Install).

    Во время установки выбранных служб ролей будет отображаться страница Ход выполнения установки (Installation Progress). После этого откроется страница Результаты установки (Installation Results).
19. На странице Результаты установки (Installation Results) щелкните кнопку Закрыть (Close).

Упражнение 2. Создание консоли Сертификаты для управления сертификатами

В этом упражнении вы создадите консоли на серверах Serverl и Server2 для управления сертификатами.

1. Войдите на Serverl как администратор.
2. В поле Начать поиск (Start Search) меню Пуск (Start) введите *mmc* и нажмите клавишу Enter.

3. Откройте меню Консоль (File) и щелкните кнопку Добавить или удалить оснастку (Add/Remove Snap-In).
4. В окне Добавление и удаление оснастки (Add Or Remove Snap-Ins) выберите в списке доступных оснасток элемент Сертификаты (Certificates) и щелкните кнопку Добавить (Add).
5. На странице Оснастка диспетчера сертификатов (Certificates Snap-In) выберите опцию учетной записи компьютера (Computer Account) и щелкните кнопку Далее (Next).
6. На странице Выбор компьютера (Select Computer) щелкните кнопку Готово (Finish).
7. В окне Добавление и удаление оснастки (Add Or Remove Snap-Ins) щелкните ОК.
8. В меню Консоль (File) сохраните оснастку под именем MMC Сертификаты. Сохраните консоль в папке по умолчанию Администрирование (Administrative Tools).
9. Повторите шаги с 1 по 8 на Server2.

Упражнение 3. Экспорт сертификата сервера

В этом упражнении вы экспортируете самозаверяемый сертификат на Server2 в папку Документы (Documents). Затем вы скопируете экспортированный сертификат на Serverl.

1. На сервере Server2 откройте консоль MMC Сертификаты. Если вы сохранили эту консоль в папке Администрирование (Administrative Tools), то можете найти ее, щелкнув кнопку Пуск (Start), открыв Все программы (All Programs), Администрирование (Administrative Tools) и щелкнув элемент MMC Сертификаты.
2. В дереве консоли MMC Сертификаты на сервере Server2 откройте папку Сертификаты (локальный компьютер)\Личное\Сертификаты (Certificates (Local Computer)\Personal\Certificates).

   При выборе папки Сертификаты (Certificates) в панели сведений отображается сертификат Server2.contoso.com. Этот сертификат издан на Server2. contoso.com и является самозаверяющим сертификатом, созданным в упражнении 1.
3. Щелкните правой кнопкой мыши сертификат Server2.contoso.com, в контекстном меню откройте Все задачи (All Tasks) и примените команду Экспорт (Export).

   Запустится Мастер экспорта сертификатов (Certificate Export Wizard).
4. Прочитайте информацию на странице приветствия мастера и щелкните кнопку Далее (Next).
5. На странице Экспортирование закрытого ключа (Export Private Key) оставьте опцию по умолчанию (не экспортировать закрытый ключ) и щелкните кнопку Далее (Next).

6. На странице Формат экспортируемого файла (Export File Format) оставьте опции по умолчанию и щелкните кнопку Далее (Next).
7. На странице Имя экспортируемого файла (File To Export) щелкните кнопку Обзор (Browse).
8. В диалоговом окне Сохранить как (Save As) присвойте файлу имя Server2cert и сохраните его в папке Документы (Documents).
9. На странице Имя экспортируемого файла (File To Export) щелкните кнопку Далее (Next).
10. На странице Завершение мастера экспорта сертификатов (Completing The Certificate Export Wizard) просмотрите имя и место размещения экспортируемого сертификата и щелкните кнопку Готово (Finish).
11. Откроется окно сообщения мастера экспорта сертификатов об успешном выполнении экспорта. Щелкните ОК.
12. С помощью любого метода скопируйте файл Server2cert.cer с сервера Server2 на Serverl и переходите к выполнению упражнения 4.

    Например, вы можете использовать флэш-память USB для копирования и переноса файла с Server2 на Serverl, либо создать на Serverl общую папку и скопировать в нее файл через сеть.

Упражнение 4. Импорт сертификата сервера

В этом упражнении вы импортируете сертификат, экспортированный с Server2, в хранилище Доверенные корневые центры сертификации (Trusted Root Certification Authorities) на сервере Serverl.

1. На Serverl откройте консоль MMC Сертификаты. Если вы сохранили эту консоль в папке Администрирование (Administrative Tools), то можете найти ее, щелкнув кнопку Пуск (Start), открыв Все программы (All Programs), открыв Администрирование (Administrative Tools) и щелкнув элемент MMC Сертификаты.
2. В дереве консоли MMC Сертификаты на сервере Serverl откройте папку Сертификаты (локальный компьютер)\Доверенные корневые центры сертификации\Сертификаты (Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates).
3. Щелкните правой кнопкой мыши папку Сертификаты (Certificates), в контекстном меню выберите Все задачи (All Tasks) и задайте команду Импорт (Import).

   Запустится мастер импорта сертификатов (Certificate Import Wizard).
4. Ознакомьтесь с информацией на странице приветствия мастера и щелкните кнопку Далее (Next).
5. На странице Импортируемый файл (File To Import) щелкните кнопку Обзор (Browse). На экран будет выведено окно Открыть (Open).
6. С помощью дерева навигации найдите в окне и выберите локальную копию файла Server2cert.cer, сохраненного при выполнении упражнения 3, а затем щелкните кнопку Открыть (Open).
7. На странице Импортируемый файл (File To Import) щелкните кнопку Далее (Next).

8. Перейдя на страницу Хранилище сертификатов (Certification Store), оставьте опции по умолчанию и щелкните кнопку Далее (Next).
9. На странице Завершение мастера импорта сертификатов (Completing The Certificate Import Wizard) щелкните-кнопку Готово (Finish).
10. Откроется окно мастера импорта сертификатов с сообщением об успешном импорте. Щелкните ОК.

Упражнение 5. Подключение к шлюзу служб терминалов с помощью RDC

В этом упражнении вы отконфигурируете Подключение к удаленному рабочему столу (Remote Desktop Connection) для подключения к компоненту Службы терминалов (Terminal Services) через компонент Шлюз TS (TS Gateway) на Server2. Затем вы протестируете это подключение.

1. Войдите на Serverl как администратор домена и откройте Подключение к удаленному рабочему столу (Remote Desktop Connection).
2. В окне Подключение к удаленному рабочему столу (Remote Desktop Connection) щелкните кнопку Параметры (Options).
3. Перейдите на вкладку Подключение (Advanced).
4. В области Подключение из любого места (Connect From Anywhere) щелкните кнопку Параметры (Settings).
5. В области Параметры подключения (Connection Settings) выберите опцию Использовать следующие параметры шлюза служб терминалов (Use These TS Gateway Server Settings). Параметры сервера шлюза TS автоматически запрашиваются в групповой политике.
6. В текстовое поле Имя сервера (Server Name) введите *server2.contoso.com.*
7. В раскрывающемся списке Метод входа (Logon Method) выберите опцию Запрашивать пароль (NTLM) (Ask For Password (NTLM)).
8. Сбросьте флажок Не использовать шлюз служб терминалов для локальных адресов (Bypass TS Gateway Server For Local Address).
9. Установите флажок Использовать мои учетные данные шлюза служб терминалов для удаленного компьютера (Use My TS Gateway Credentials For The Remote Computer) и щелкните ОК.
10. В окне Подключение к удаленному рабочему столу (Remote Desktop Connection) перейдите на вкладку Общие (General).
И. В текстовом поле Компьютер (Computer) введите или выберите *server2. contoso.com.*
12. В текстовом поле Пользователь (User Name) введите учетные данные администратора домена.
13. Щелкните кнопку Подключить (Connect). Откроется диалоговое окно Безопасность Windows (Windows Security).
14. Прочитайте информацию в диалоговом окне Безопасность Windows (Windows Security). Обратите внимание на то, что указанные учетные данные будут использоваться для шлюза служб терминалов и удаленного сервера терминалов.

15. Введите учетные данные администратора домена и щелкните ОК. Будет установлено подключение служб терминалов к Server2 через шлюз TS.
16. С Server2 войдите на Contoso.com, используя другую учетную запись доменного администратора вместо той, которая применялась для подключения через RDC на Serverl.
17. На Server2 откройте Диспетчер шлюза терминалов (TS Gateway Manager). Для этого щелкните кнопку Пуск (Start), откройте Администрирование (Administrative Tools), укажите Службы терминалов (Terminal Services) и щелкните Диспетчер шлюза служб терминалов.
18. В дереве консоли диспетчера шлюза служб терминалов выберите Server2 (Локальный) и откройте папку Наблюдение (Monitoring). В центральной панели будет перечислено подключение с Serverl. Это подключение успешно принято шлюзом служб терминалов.
19. На Serverl в окне Удаленный рабочий стол (Remote Desktop) завершите сеанс на Server2.
20. На обоих серверах, Serverl и Server2, закройте все открытые окна и завершите работу.

Резюме

- Шлюз служб терминалов (TS Gateway) представляет собой службу роли, позволяющую авторизованным удаленным пользователям устанавливать RDP-подключения к серверам терминалов, расположенным за корпоративным брандмауэром.
- Коммуникации TS-клиентов со шлюзом TS шифруются с помощью протокола SSL и используют SSL-порт 443.
- Как правило, сервер шлюза служб терминалов располагается в сети по периметру, а удаленные TS-клиенты сообщаются с ним напрямую. Тем не менее вы также можете использовать ISA-сервер для пересылки клиентских запросов на шлюз служб терминалов.
- Для работы шлюза служб терминалов требуются: сертификат сеовера для шифрования SSL, политика TS CAP (авторизация подключений к шлюзу) и политика TS RAP (авторизация подключений к внутренним ресурсам),
- Основным инструментом, используемым для управления шлюзом служб терминалов, является Диспетчер шлюза служб терминалов (TS Gateway Manager).

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных в ходе занятия 2. Эти вопросы представлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы

Ответы и пояснения к каждому их варианту размещены в разделе «Ответы» в конце книги.

1. Какой TCP-порт следует оставить открытым в брандмауэре, чтобы клиенты могли инициировать RDP-подключения к серверам терминалов через шлюз служб терминалов?
   А. 25.
   Б. 3389.
   В. 443.
   Г. 80.
2. В вашей сети расположен сервер шлюза служб терминалов TSG1. На сервере TSG1 установлен самозаверяющий сертификат сервера, используемый для SSL-коммуникаций. Вы хотите использовать компьютер с запущенным ISA-сервером в качестве конечной точки SSL для подключений шлюза служб терминалов. Какие действия нужно выполнить для обеспечения возможности коммуникаций ISA-сервера со шлюзом служб терминалов?
   А. Включить мост HTTPS-HTTP между ISA-сервером и шлюзом служб терминалов.
   Б. Открыть TCP-порт 443 на компьютере с установленным ISA-сервером.
   В. Экспортировать SSL-сертификат ISA-сервера на шлюз служб терминалов.
   Г. Экспортировать SSL-сертификат шлюза служб терминалов на ISA-сервер.

Занятие 3. Публикация приложений с помощью утилиты TS RemoteApp

Технология TS RemoteApp, встроенная в Службы терминалов (Terminal Services), позволяет публиковать приложения (то есть делать их доступными для удаленных пользователей). На этом занятии вы изучите принципы применения TS RemoteApp для публикации приложений тремя способами: через веб-доступ к службам терминалов (Terminal Services Web Access, TS Web Access), RDP-файлы и пакеты установщика Windows (Windows Installer).

Изучив материал этого занятия, вы сможете:

- Описать принципы работы удаленных приложений RemoteApp служб терминалов и сценарии их использования.
- Установить приложение на сервере терминалов, чтобы оно могло поддерживать множество пользователей.
- Сделать приложение, установленное на сервере терминалов Windows Server 2008, доступным для удаленных пользователей через веб-браузер.
- Создать RDP-файл, который запускает приложение, установленное на удаленном сервере терминалов Windows Server 2008.
- Создать пакет установщика Windows (Windows Installer), который создает ярлыки к приложениям RemoteApp в пользовательском меню Пуск (Start) и на рабочем столе.

Расчетная продолжительность занятия составляет 45 мин.

Удаленные приложения RemoteApp служб терминалов

Технология TS RemoteApp позволяет программам запускаться через службы терминалов и работать точно так же, как при запуске на локальном компьютере пользователя. До появления системы Windows Server 2008 пользователям служб терминалов, которым требовалось запустить приложение на удаленном сервере терминалов, вначале приходилось устанавливать на сервере сеанс рабочего стола, а затем запускать приложение в этом сеансе. При использовании TS RemoteApp приложение отображается в окне с изменяемыми размерами на локальном рабочем столе пользователя через RDP-подключение.

Программу RemoteApp можно развернуть для пользователей следующими способами.

Вы можете сделать программы RemoteApp доступными на веб-сайте, распространив эти программы через страницу Веб-доступ служб терминалов (TS Web Access). Эта страница локализована по адресу http://*имясервера*/ts или *\yXXщ\//имя_сервера/X&* (если веб-сервер может принимать SSL-подключения). В данном сценарии выполняется настройка страницы Веб-доступ служб терминалов (TS Web Access) для отображения значков доступных программ RemoteApp. Щелчком значка на этой странице на компьютере пользователя запускается соответствующая программа RemoteApp.

Вы можете распространить программы RemoteApp в виде RDP-файлов или пакетов установщика Windows (Windows Installer) через общий файловый ресурс или другие механизмы распространения, такие как Microsoft Systems Management Server 2003, Microsoft System Center Configuration Manager 2007 или механизм распространения программного обеспечения Active Directory. После получения RDP-файла или его установки с помощью пакета установщика Windows пользователь может запускать программу двойным щелчком этого RDP-файла, из меню Пуск (Start), или открыв файл, расширение которого сопоставлено с программой RemoteApp.

После запуска программы RemoteApp одним из указанных выше способов пользователь может запускать программу точно таким же образом, как локально установленное приложение. Как и в случае с сеансом служб терминалов, сервер терминалов виртуально обеспечивает все ресурсы, необходимые для запуска программы RemoteApp.

ПРИМЕЧАНИЕ Технология TS RemoteApp и пользовательские сеансы
Когда пользователь запускает две программы RemoteApp, размещенные на одном сервере терминалов, они запускаются в одном пользовательском сеансе служб терминалов.

Технология TS RemoteApp позволяет использовать ресурсы центрального сервера и упростить управление в следующих ситуациях.

- Пользователям требуется удаленно получать доступ к программам, размещенным в вашей сети. В таком случае вы можете развернуть TS RemoteApp вместе со шлюзом служб терминалов, чтобы удаленные пользователи могли получать доступ к вашим программам из Интернета.

- Ваша сеть содержит старые компьютеры, на которых нет оборудования или ресурсов, требуемых для запуска приложения.
- В филиале вашей компании отсутствует IT-персонал, необходимый для поддержки данного приложения на сайте.
- Ваша сеть содержит настольные компьютеры с операционными системами или программным обеспечением, конфликты которых не позволяют установить требуемое приложение.
- Вам требуется поддерживать пользователей, которым не выделены никакие компьютеры и которым необходимо постоянно использовать отдельное приложение.
- Вы хотите снизить затраты на приобретение приложения, установив его лишь на одном компьютере.

Настройка сервера для программ RemoteApp

Чтобы подготовить сервер для программ RemoteApp, нужно вначале установить на этом сервере службу роли Службы терминалов (Terminal Services). Другие службы ролей не нужны, поскольку TS RemoteApp интегрируется в главный компонент служб терминалов.

Следующий этап процесса настройки сервера для управления программами RemoteApp состоит в установке требуемых приложений таким образом, чтобы они были доступны для множества пользователей. Программу можно установить лишь в режиме установки TS-Install сервера. В этом режиме служб терминалов при установке приложений создаются лишь главные копии записей реестра или файлы .ini, которые используются для хранения пользовательских данных приложения. Эти главные записи копируются в профили пользователей для хранения личных параметров только при последующем запуске приложения пользователем.

Приложение можно установить в режиме TS-Install одним из способов описанных ниже.

- Для установки программы можно использовать MSI-файл пакета установщика Windows (Windows Installer). При установке с помощью пакета установщика Windows программа будет установлена в режиме TS-Install.
- Вы можете использовать опцию Установка приложения на сервер терминалов (Install Application On Terminal Server) в панели управления (Control Panel), как показано на рис. 4-22.
- Перед установкой программы в командной строке можно запустить команду *Change user /install* или *Chguser /install.* После установки программы для выхода из режима TS-Install нужно запустить в командной строке команду *Change user /execute* или *Chguser /execute.*

СОВЕТ Подготовка к экзамену

Для сдачи сертификационного экзамена 70-643 нужно знать назначение режима TS-Install и все способы установки приложения в этом режиме.

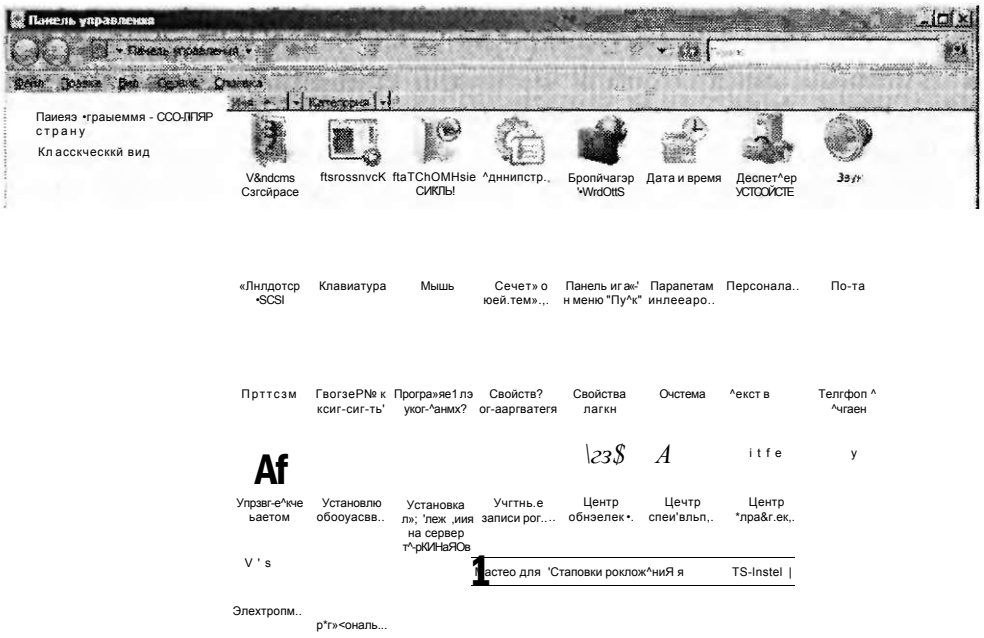


Рис. 4-22. Опция панели управления, позволяющая установить программу для множества пользователей TS

Добавление программ для публикации в диспетчере RemoteApp

После установки требуемых приложений в режиме TS-Install требуется добавить эти программы в список Удаленные приложения RemoteApp (RemoteApp Programs) Диспетчера удаленных приложений RemoteApp служб терминалов (TS RemoteApp Manager).

ПРИМЕЧАНИЕ Диспетчер удаленных приложений RemoteApp служб терминалов
Диспетчер удаленных приложений RemoteApp служб терминален (TS RemoteApp Manager) является основной административной консолыо. используемой для развертывания, настройки программ RemoteApp и управления ими. Чтобы открыть эту консоль, щелкните кнопку Пуск (Start), откройте Администрирование (Administrative Tools), откройте Службы терминалов (Terminal Services) и щелкните элемент Диспетчер удаленных приложений RemoteApp служб терминалов.

Для выполнения этой операции откройте Диспетчер удаленных приложений RemoteApp служб терминалов и в панели Действия (Actions) щелкните действие Добавление удаленных приложений RemoteApp (Add RemoteApp Program). После выбора программы в окне мастера это приложение появится в списке Удаленные приложения RemoteApp (RemoteApp Programs), как показано на рис. 4-23.

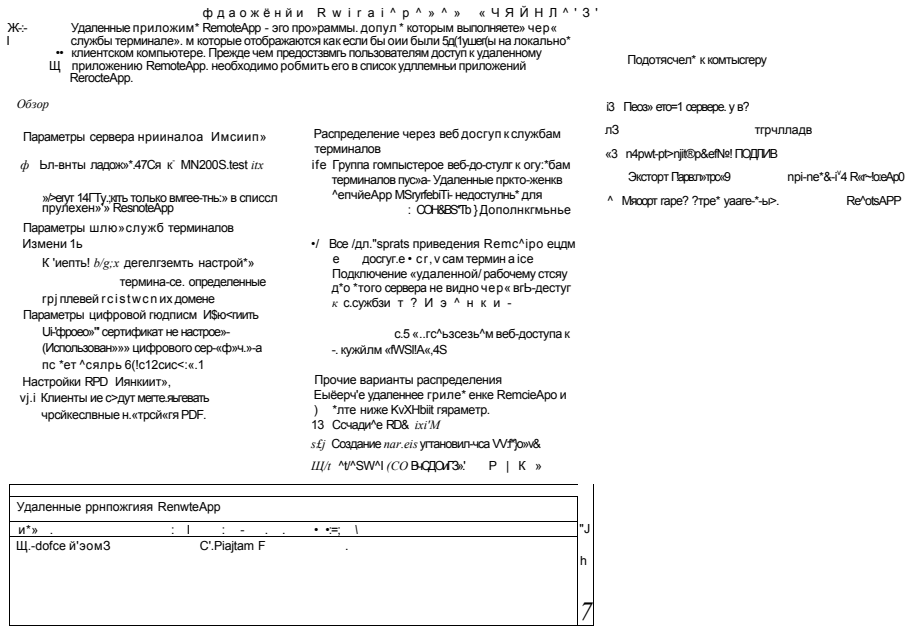


Рис. 4-23. Добавление приложения RemoteApp

После добавления в этот список программы автоматически отображаются на странице Веб-доступ к службам терминалов (TS Web Access) по умолчанию, если этот компонент уже установлен на том же сервере терминалов. Диспетчер удаленных приложений RemoteApp служб терминалов (TS RemoteApp Manager) можно также использовать для создания RDP-файлов или пакетов установщика Windows для программ, которые уже добавлены в список. Все три опции публикации подробно описаны в следующих разделах.

Развертывание приложения RemoteApp через веб-доступ к службам терминалов

Для начала вам нужно установить службу роли Веб-доступ к службам терминалов (TS Wei) Access). Если вы установите Веб-доступ к службам терминалов на том же сервере, где сервер терминалов содержит программы RemoteApp, все приложения, перечисленные в списке Удаленные приложения RemoteApp (RemoteApp Programs), по умолчанию будут отображаться на странице Веб-доступ к службам терминалов (TS Web Access).

Чтобы открыть страницу Веб-доступ к службам терминалов (TS Web Access), пользователям нужно открыть Internet Explorer и перейти к странице http:// *имя сервера/*ts. (В качестве альтернативы пользователи могут перейти к странице htt.ps\//*имя сервера*/Is, если сервер настроен с помощью сертификата сервера, изданного доверенным центром сертификации.) Страница Веб-доступ к службам терминалов (TS Web Access) показана на рис. 4-24.

Удаленны* приложений RemoteApp : Удаленный рабочий стел Конфигурация

ш
АсЮЬг
Reader8

Рис. 4-24. Веб-доступ к службам терминалов (TS Web Access)

На этой странице пользователи могут запускать приложения RemoteApp, щелкая соответствующие значки. В сценарии с двумя серверами компоненты Веб-доступ к службам терминалов (TS Web Access) и Службы терминалов (Terminal Services) запускаются на разных серверах. В этом случае вам потребуется выполнить два дополнительных шага, чтобы страница Веб-доступ к службам терминалов отображала приложения RemoteApp, размещенные на сервере терминалов.

1. В текстовое поле Имя сервера терминалов (Terminal Server Name) на вкладке Конфигурация (Configuration) страницы Веб-доступ к службам терминалов (TS Web Access) нужно ввести имя удаленного сервера терминалов, как показано на рис. 4-25. (Чтобы открыть вкладку Конфигурация, вы должны подключиться к серверу веб-доступа к службам терминалов, используя учетные данные пользователя, являющегося членом локальной группы Администраторы веб-доступа к службам терминалов (TS Web Access Administrators) сервера веб-доступа к TS.)
2. Вы должны добавить учетную запись компьютера с сервером веб-доступа к службам терминалов в расположенную на сервере терминалов группу безопасности Компьютеры веб-доступа к службам терминалов (TS Web Access Computers).

ПРИМЕЧАНИЕ Указание веб-доступа к службам терминалов на одном сервере
Независимо от количества серверов, участвующих в реализации компонента Веб-доступ к службам терминалов (TS Web Access), страница Веб-доступ к службам терминалов отображает ресурсы, размещенные лишь на одном сервере терминалов.

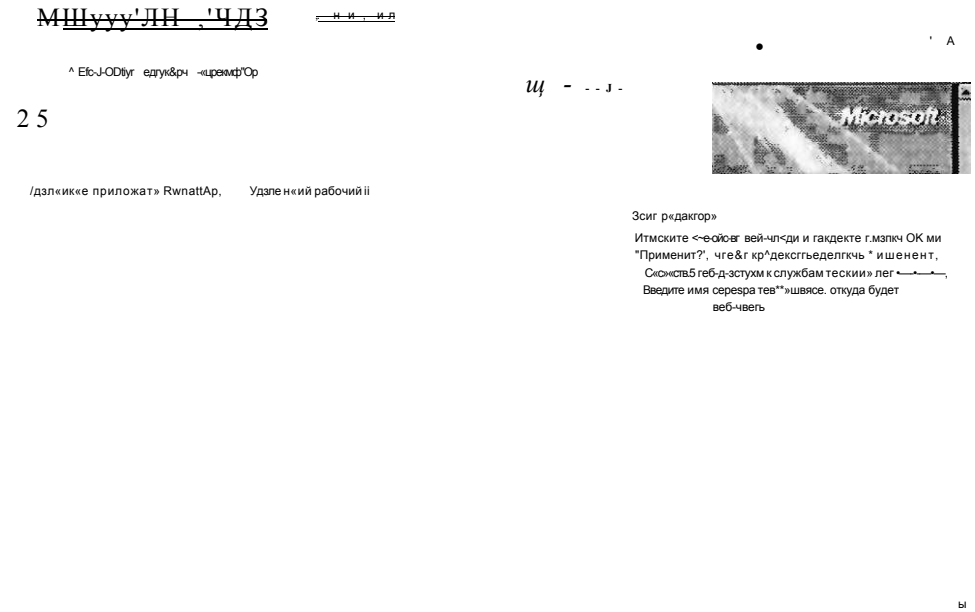


Рис. 4-25. Конфигурирование веб-доступа к службам терминалов для получения сведений о приложении RemoteApp еще с одного сервера

Создание RDP-файла приложения RemoteApp

Вы можете создать RDP-файл любого приложения, имеющегося в списке Удаленные приложения RemoteApp (RemoteApp Programs) Диспетчера удаленных приложений RemoteApp служб терминалов (TS RemoteApp Manager). Для этого просто выберите приложение в списке, а затем щелкните ссылку Создание RDP-файла (Create .RDP File) в разделе Прочие варианты распределения (Other Distribution Options), как показано на рис. 4-26.

Эта процедура запускает Мастер удаленных приложений RemoteApp (RemoteApp Wizard). Перед созданием RDP-файла, указывающего удаленную программу. Мастер удаленных приложений RemoteApp позволяет отконфигурировать определенные параметры этого RDP-файла на странице Назначение параметров пакета (Specify Package Settings).

Например, вы можете указать TCP-порт, на котором удаленный сервер терминалов будет прослушивать запросы подключений. (Обычно используется стандартный порт 3389).

Мастер также позволяет назначить параметры сервера шлюза служб терминалов для пользовательских подключений перед запуском приложения RemoteApp. И наконец, мастер позволяет подписать RDP-файл цифровой подписью сертификата. Эта подпись гарантирует, что RDP-файлы опубликованы доверенным издателем.

На рис. 4-27 показана страница Задание параметров пакета (Specify Package Settings).

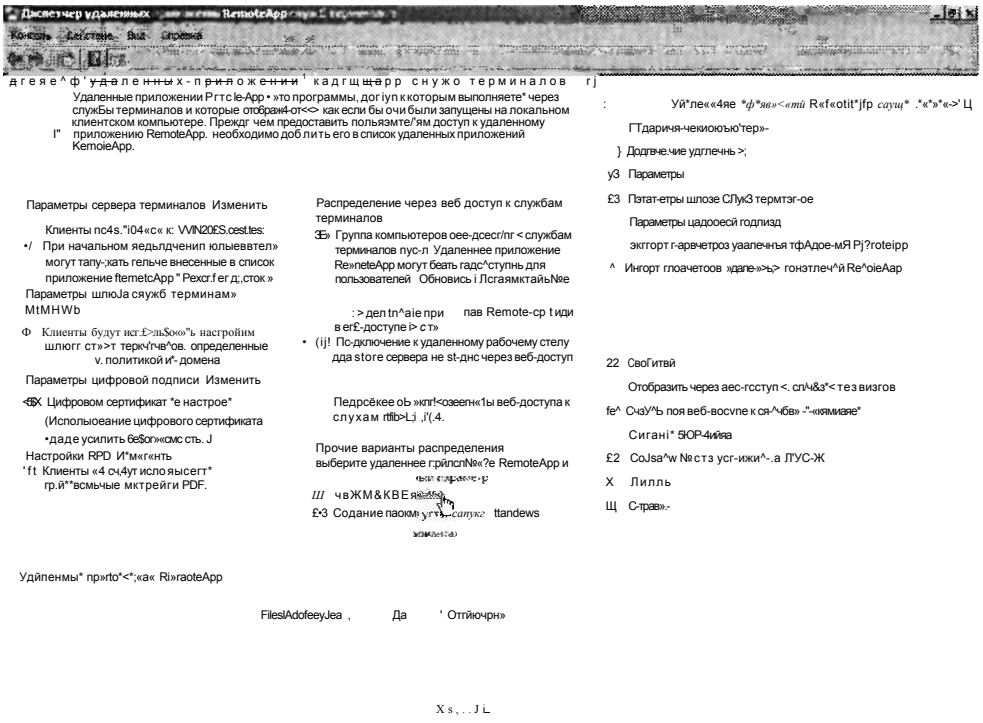


Рис. 4-26. Создание RDP-файла, указывающего приложение RemoteApp

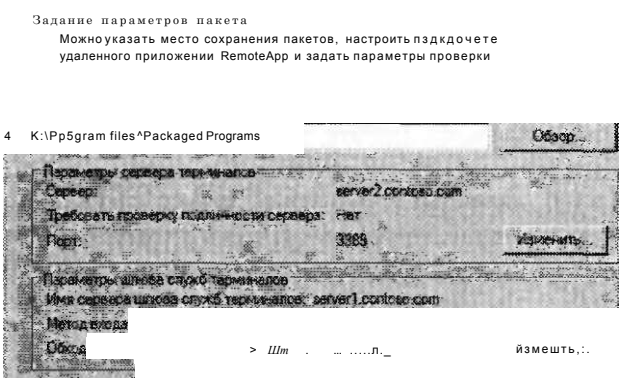


Рис. 4-27. Задание параметров RDP-файла

СОВЕТ Подготовка к экзамену

Вы можете отконфнгурировав групповую политику, ограничить использование подписанных RDP-файлов, доступных в дистрибутивном общем ресурсе. Например, вы можете разрешить использовать RDP-файлы лишь тем пользователям, которые входят на компьютеры в отдельной организационной единице, и явно запретить применение этих файлов другим пользователям домена. Один из способов выполнения этой задачи состоит в отключении RDP-файлов для действительных издателей на доменном уровне и последующем включении этого параметра политики для организационной единицы, содержащей клиентские компьютеры, пользователям которых нужно применять эти файлы. Откройте папку Конфигурация компьютера\Административные шаблоны\Компоненты Штс1о\¥5\Службы терминалов\Клиент подключения к удаленному рабочему столу (Computer Configuration\Administrative Templates\Windows Components\ Terminal Services\Remote Desktop Connection Client), а затем включите параметр политики Разрешать RDP-файлы от допустимых издателей и пользовательские параметры RDP, заданные по умолчанию (Allow .RDP Files From Valid Publishers And User's Default .RDP Settings).

После создания RDP-файла с помощью Мастера удаленных приложений RemoteApp (RemoteApp Wizard) вы можете распределить этот файл на клиентских компьютерах, используя существующий процесс распределения программного обеспечения: Microsoft Systems Management Server (SMS) 2003, Microsoft System Center Configuration Manager 2007 или групповую политику. В качестве альтернативы вы можете распределить файл по электронной почте или через общий сетевой ресурс.

Создание пакета установщика Windows для распределения удаленного приложения RemoteApp

Вместо RDP-файлов вы можете создавать и распределять MSI-файлы. Для выполнения этой задачи выберите в списке программ Диспетчера удаленных приложений RemoteApp служб терминалов (TS RemoteApp Manager) требуемое вам приложение и щелкните ссылку Создание пакета установщика Windows (Create Windows Installer Package) в разделе Прочие варианты распределения (Other Distribution Options), как показано на рис. 4-28.

Запустится Мастер удаленных приложений RemoteApp (RemoteApp Wizard). Как и в случае с RDP-файлами, мастер открывает страницу Назначение параметров пакета (Specify Package Settings), где можно указать сервер терминалов, параметры шлюза служб терминалов и цифровой сертификат для создаваемого пакета установщика Windows.

Однако при создании пакета установщика Windows (Windows Installer) Мастер удаленных приложений RemoteApp (RemoteApp Wizard) также отображает страницу Настройка пакета распространения (Configure Distribution Package)

со вторым набором опций. Во-первых, вы можете указать для устанавливаемого приложения RemoteApp размещение значков ярлыков. Значки ярлыков можно разместить на рабочем столе пользователя и в папке меню Пуск (Start), присвоив ей имя по своему усмотрению. Во-вторых, вы можете отконфигурировать приложение RemoteApp, чтобы оно запускалось каждый раз при открытии файла, расширение которого сопоставлено с этим приложением. (Используйте эту опцию лишь в том случае, если на компьютерах клиентов отсутствуют локально установленные версии программы.)

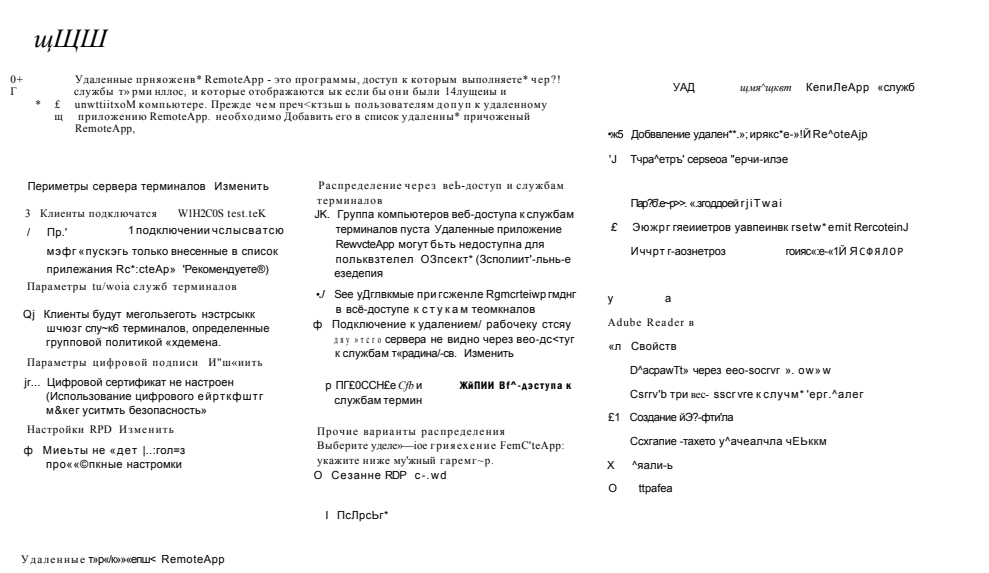


Рис. 4-28. Создание установщика Windows для приложения RemoteApp

СОВЕТ Подготовка к экзамену

Для сдачи сертификационного экзамена 70-643 вам нужно помнить, что эти две опции значков ярлыков и сопоставлений файловых расширений на странице Настройка пакета распространения (Configure Distribution Package) становятся доступными только при создании пакета установщика Windows приложения RemoteApp.

На рис. 4-29 показана страница Настройка пакета распространения (Configure Distribution Package) Мастера удаленных приложений RemoteApp (RemoteApp Wizard).

Как и в случае с RDP-файлами, вы можете распространять пакеты установщика Windows среди клиентов с помощью SMS, System Center Configuration Manager и групповой политики. В качестве альтернативы файлы можно распространять по электронной почте или через общий сетевой ресурс.

СОВЕТ Подготовка к экзамену

Одно нз преимуществ публикации приложений через Веб-доступ к службам терминалов (TS Web Access) состоит в том, что изменения свойств приложений RemoteApp немедленно регистрируются клиентами. Тем не менее если вы распространили приложение RemoteApp через файлы RDP или MSJ и хотите изменить его свойства, чтобы, например, клиентам требовалось подключаться к нему через шлюз служб терминалов, вам придется заново создать эти файлы и распространить их среди пользователей.

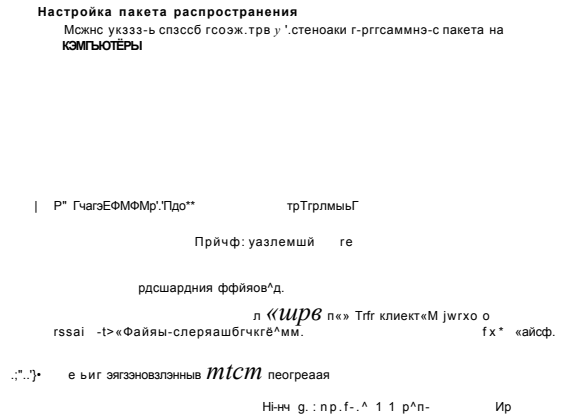


Рис. 4-29. Конфигурирование опций распространения пакета установщика Windows

Проверьте себя

1. Можно ли отконфигурировать Веб-доступ к службам терминалов (TS Web Access) для отображения приложений RemoteApp, найденных на различных серверах организации?
2. Укажите единственную опцию развертывания приложений RemoteApp, которая позволяет установить значки ярлыков приложения в меню Пуск (Start).

Ответы

1. Нет, нельзя. Веб-доступ к службам терминалов отображает ресурсы, размещенные на одном сервере.
2. Создание пакета установщика Windows (MSI-файл). Вы можете развернуть MSI-файлы посредством групповой политики, чтобы значки ярлыков в меню Пуск (Start) устанавливались автоматически.

Практикум. Публикация приложений с помощью диспетчера RemoteApp

В этом наборе упражнений вы опубликуете приложение тремя способами. Во-первых, вы разрешите пользователям запускать удаленное приложение в веб-странице. Во-вторых, вы создадите и распространите RDP-файл удаленного приложения. И наконец, создадите и распространите пакет установщика системы Windows.

Упражнение 1. Установка службы роли Веб-доступ к службам терминалов

Самый простой способ публикации приложения RemoteApp состоит в использовании компонента Веб-доступ к службам терминалов (TS Web Access). В этом упражнении вы подготовите сервер терминалов для публикации приложений, установив службу роли Веб-доступ к службам терминалов (TS Web Access).

1. Войдите на сервер Server2 в качестве администратора домена Contoso.com.
2. Откройте Диспетчер сервера (Server Manager).
3. В дереве консоли диспетчера сервера разверните узел Роли (Roles) и выберите Службы терминалов (Terminal Services).
4. В области Службы ролей (Role Services) панели сведений щелкните ссылку Добавление служб ролей (Add Role Services). Откроется страница Выбор служб ролей (Select Role Services) мастера Добавление служб ролей (Add Role Services Wizard).
5. В списке доступных служб ролей установите флажок Веб-доступ к службам терминалов (TS Web Access).

   На этом этапе может открыться диалоговое окно (Add Role Services) с предложением установить службы ролей, требуемые для компонента Веб-доступ к службам терминалов.
6. Если откроется диалоговое окно Добавление служб ролей (Add Role Services), щелкните кнопку Добавить требуемые службы ролей (Add Required Role Services).
7. На странице Выбор служб ролей (Select Role Services) щелкните кнопку Далее (Next).
8. Если откроется страница Веб-сервер (IIS) (Web Server (IIS)) прочитайте весь текст и щелкните кнопку Далее (Next).
9. Если откроется страница Выбор служб ролей (Select Role Services), прочитайте всю информацию и щелкните кнопку Далее (Next).
10. На странице Подтвердите выбранные элементы (Confirm Installation Selections) щелкните кнопку Установить (Install). Во время установки компонентов будет отображаться страница Ход выполнения установки (Installation Progress). По завершении установки откроется страница Результаты установки (Installation Results).
11. На странице Результаты установки (Installation Results) щелкните кнопку Закрыть (Close).

Упражнение 2. Публикация приложения для веб-доступа к службам терминалов

В этом упражнении вы добавите программу MS Paint в список приложений RemoteApp диспетчера удаленных приложений служб терминалов.

1. Войдите на сервер Server2 в качестве администратора домена Contoso.com.
2. Щелкните кнопку Пуск (Start), откройте Администрирование (Administrative Tools), затем откройте Службы терминалов (Terminal Services) и щелкните Диспетчер удаленных приложений RemoteApp служб терминалов.
3. В панели Действия (Actions) диспетчера RemoteApp щелкните действие Добавление удаленных приложений RemoteApp (Add RemoteApp Programs).
4. На странице приветствия Мастера удаленных приложений RemoteApp (RemoteApp Wizard) щелкните кнопку Далее (Next).
5. На странице Выберите программы для добавления в список удаленных приложений RemoteApp (Choose Programs To Add To The RemoteApp Programs List) выберите в списке программу Paint и щелкните кнопку Далее (Next).
6. На странице Просмотр параметров (Review Settings) щелкните кнопку Готово (Finish). Программа Paint появится в списке Удаленные приложения RemoteApp (RemoteApp Programs) диспетчера RemoteApp.

   Обратите внимание на то, что в столбце Веб-доступ к службам терминалов (TS Web Access) для этого приложения указано состояние Да (Yes).
7. Переходите к упражнению 3.

Упражнение 3. Запуск удаленного приложения через веб-доступ к службам терминалов

В этом упражнении вы запустите приложение Paint через веб-доступ к службам терминалов.

1. Войдите на сервер Serverl в качестве администратора домена Contoso.com.
2. Откройте Internet Explorer.
3. В меню Сервис (Tools) выберите Свойства обозревателя (Internet Options) и перейдите на вкладку Безопасность (Security).
4. На вкладке Безопасность (Security) диалогового окна Свойства обозревателя выберите зону Местная интрасеть (Local Intranet) и щелкните кнопку Узлы (Sites).
5. В диалоговом окне Местная интрасеть добавьте веб-сайт *http://server2.contoso.com* и *https://server2.contoso.com*, затем щелкните кнопку Закрыть (Close).
6. В диалоговом окне Свойства обозревателя (Internet Options) щелкните кнопку OK.
7. В адресную строку Internet Explorer введите *https://seruer2.contoso.com/ts* и нажмите клавишу Enter.

8. В окне сообщения Предупреждение безопасности (Security Alert) щелкните ОК. Откроется страница Веб-доступ к службам терминалов (TS Web Access). При выборе заглавия Удаленные приложения RemoteApp (RemoteApp Programs) в главной области веб-страницы отобразится значок Paint.
9. Щелкните значок Paint. Откроется окно с предупреждением RemoteApp.
10. Прочитайте весь текст предупреждения и щелкните кнопку Подключить (Connect).
11. В окне Безопасность Windows (Windows Security) введите учетные данные доменного администратора и щелкните ОК. Через минуту откроется окно Paint.
12. В меню Файл (File) щелкните команду Сохранить (Save). Откроется окно Сохранить как (Save As). Ответьте на следующие вопросы.

    Где по умолчанию сохраняется файл: на Serverl или Server2? Почему?

    Ответ: На Server2, поскольку программа запускается на Server2.
13. В окне Сохранить как (Save As) щелкните кнопку Отмена (Cancel) и закройте окно Paint.

Упражнение 4. Создание общего дистрибутивного ресурса

В этом упражнении вы создадите общий дистрибутивный ресурс с доступом чтения для всех пользователей домена. Общий ресурс будет использоваться для распространения RDP-файлов и пакетов установщиков служб терминалов.

1. Войдите на сервер Server2 в качестве администратора домена Contoso.com.
2. Создайте папку TS Apps в корне диска С.
3. Щелкните правой кнопкой мыши папку TS Apps и примените команду Общий доступ (Share) из контекстного меню.

    Откроется окно Общий доступ к файлу (File Sharing).
4. В текстовое поле введите *Пользователи домена* и щелкните кнопку Добавить (Add).

    Группа Пользователи домена (Domain Users) появится в списке Имя (Name) с уровнем разрешений Читатель (Reader).
5. Щелкните кнопку Общий доступ (Share).

    В окне Общий доступ к файлу (File Sharing) появится сообщение о назначении общего доступа к папке.
6. Щелкните кнопку Готово (Done).

Упражнение 5. Создание RDP-файла опубликованного приложения

В этом упражнении вы создадите RDP-файл программы WordPad и сохраните его в общем дистрибутивном ресурсе TS Apps.

1. Войдите на сервер Server2 в качестве администратора домена Contoso.com и откройте Диспетчер удаленных приложений RemoteApp служб терминалов (TS RemoteApp Manager).

    В панели Действия (Actions) диспетчера RemoteApp щелкните действие Добавление удаленных приложений RemoteApp (Add RemoteApp Programs).

С помощью Мастера удаленных приложений RemoteApp (RemoteApp Wizard) добавьте программу WordPad в список Удаленные приложения RemoteApp (RemoteApp Programs), как описано в упражнении 2.

2. В списке удаленных приложений RemoteApp выберите программу WordPad и в области Прочие варианты распределения (Other Distribution Options) диспетчера RemoteApp щелкните ссылку Создание RDP-файла (Create .RDP File). Запустится Мастер удаленных приложений RemoteApp (RemoteApp Wizard).
3. На странице приветствия мастера щелкните кнопку Далее (Next).
4. На странице Назначение параметров пакета (Specify Package Settings) прочитайте весь текст и щелкните кнопку Обзор (Browse).
5. В диалоговом окне Обзор папок (Browse For Folder) найдите и выберите папку TS Apps в корне диска C. Щелкните OK.
6. На странице Назначение параметров пакета (Specify Package Settings) диспетчера RemoteApp щелкните кнопку Далее (Next).
7. На странице Просмотр параметров (Review Settings) щелкните кнопку Готово (Finish).
8. Переходите к упражнению 6.

Упражнение 6. Запуск удаленного приложения с помощью локального RDP-файла

В этом упражнении вы скопируете RDP-файл из общего дистрибутивного ресурса на Serverl, а затем используете этот RDP-файл для запуска удаленного приложения.

1. Войдите на сервер Serverl в качестве администратора домена Contoso.com.
2. В поле Начать поиск (Start Search) меню Пуск (Start) введите *\\Server2* и нажмите клавишу Enter. В обозревателе Windows откроется окно Server2.
3. В окне Server2 дважды щелкните общий сетевой ресурс TS Apps.
4. Из общего ресурса TS Apps скопируйте RDP-файл с именем wordpad на рабочий стол Serverl.
5. Закройте все открытые окна на Serverl. а затем дважды щелкните файл wordpad на рабочем столе Serverl. Откроется окно с предупреждением RemoteApp.
6. Прочитайте текст предупреждения и щелкните кнопку Подключить (Connect).
7. В окне Безопасность Windows (Windows Security) введите учетные данные администратора домена. Щелкните OK.
8. Через минуту программа WordPad откроется на Serverl.
9. Закройте все открытые окна.

Упражнение 7. Создание пакета установщика Windows удаленного приложения RemoteApp для распространения

В этом упражнении, где требуется доступ в Интернет, вы загрузите и установите программу Microsoft Office Word Viewer из центра загрузок Microsoft,

а затем добавите это приложение в список удаленных приложений RemoteApp. Далее вы создадите пакет установщика Windows для распространения среди пользователей в сети.

ПРИМЕЧАНИЕ Использование альтернативной программы
В этом упражнении приложение Word Viewer используется лишь для примера. Вы можете выбрать любую устанавливаемую программу вместо Word Viewer.

1. Войдите на сервер Serverl в качестве администратора домена Contoso.com.
2. С помощью Internet Explorer подключитесь к Центру загрузок Microsoft по адресу *http://www.7nicrosoft.com/downloads.* На сайте Центра загрузок Microsoft найдите программу Word Viewer.
3. Загрузите Microsoft Office Word Viewer с веб-сайта.
4. Установите Word Viewer на Server2.
5. После установки приложения откройте Диспетчер удаленных приложений RemoteApp служб терминалов (TS RemoteApp Manager).
6. В панели Действия (Actions) диспетчера RemoteApp щелкните действие Добавление удаленных приложений RemoteApp (Add RemoteApp Programs).
7. С помощью Мастера удаленных приложений RemoteApp (RemoteApp Wizard) добавьте приложение Microsoft Office Word Viewer в список Удаленные приложения RemoteApp (RemoteApp Programs), как это описано в упражнении 2. После завершения работы мастера приложение Microsoft Office Word Viewer появится в списке удаленных приложений RemoteApp диспетчера RemoteApp.
8. Выберите в списке приложение Microsoft Office Word Viewer и в разделе Прочие варианты распределения (Other Distribution Options) диспетчера RemoteApp щелкните ссылку Создание пакета установщика Windows (Create Windows Installer Package).
9. На странице приветствия мастера удаленных приложений RemoteApp щелкните кнопку Далее (Next).
10. На странице Назначение параметров пакета (Specify Package Settings) прочитайте весь текст и щелкните кнопку Обзор (Browse).
11. В диалоговом окне Обзор папок (Browse For Folder) найдите и выберите папку TS Apps в корне диска С. Щелкните ОК.
12. На странице Назначение параметров пакета (Specify Package Settings) щелкните кнопку Далее (Next).
13. На странице Настройка пакета распространения (Configure Distribution Package) прочитайте весь текст, установите флажок Рабочий стол (Desktop) и щелкните кнопку Далее (Next).
14. На странице Просмотр параметров (Review Settings) щелкните кнопку Готово (Finish).
15. Переходите к упражнению 8.

Упражнение 8. Установка удаленного приложения

В этом упражнении вы используете пакет установщика Windows, созданный в упражнении 7, чтобы установить программу Word Viewer в качестве удаленного приложения.

1. Войдите на сервер Serverl в качестве администратора домена Contoso.com.
2. В поле Начать поиск (Start Search) меню Пуск (Start) введите *\\Server2* и нажмите клавишу Enter. В обозревателе Windows откроется окно Server2.
3. В окне Server2 дважды щелкните общий сетевой ресурс TS Apps.
4. Из общего ресурса TS Apps скопируйте пакет установщика Windows (MSI-файл) с именем WORDVIEW на рабочий стол Serverl.
5. Закройте все открытые окна Serverl, а затем дважды щелкните файл WORDVIEW на рабочем столе Serverl. По окончании установки программы на рабочем столе появится новый ярлык RDP-файла с именем Microsoft Office Word Viewer.
6. Дважды щелкните ярлык Microsoft Office Word Viewer. Появится окно предупреждения RemoteApp.
7. Прочитайте весь текст предупреждения и щелкните кнопку Подключить (Connect).
8. В окне Безопасность Windows (Windows Security) введите учетные данные администратора домена. Через некоторое время откроется программа Word Viewer с диалоговым окном Открыть (Open), где будет предложено указать файл Word.
9. Закройте все открытые окна и выйдите с серверов Serverl и Server2.

Резюме

- Компонент Удаленные приложения RemoteApp служб терминалов (TS RemoteApp) позволяет запускать приложения через Службы терминалов (Terminal Services) и работать с ними таким же образом, как с локально установленными программами. Удаленные приложения RemoreApp удобно использовать в ситуациях, где пользователям требуется удаленно получать доступ к приложениям или просто не хватает оборудования или программного обеспечения, необходимого для запуска приложения.
- Программа, опубликованная через TS RemoteApp, называется удаленным приложением TS RemoteApp. Существует три способа публикации удаленных приложений RemoteApp: через страницу Веб-доступ к службам публикации (TS Web Access), через RDP-файлы и через пакеты установщика Windows (Windows Installer).
- Установку приложений для публикации на сервере терминалов нужно выполнять в режиме сервера TS-Install. Установка в этом режиме позволяет приложению поддерживать множество пользователей.
- Основным средством, используемым для управления и настройки приложений RemoteApp, является Диспетчер удаленных приложений RemoteApp служб терминалов (TS RemoteApp Manager).

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных в ходе занятия 3. Эти вопросы представлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы
Ответы и пояснения к каждому их варианту размещены в разделе «Ответы» в конце книги.

1. Как обеспечить гарантию того, что приложение, установленное на компьютере с запущенными службами терминалов, сможет поддерживать множество пользователей?
   А. Использовать команду *Chglogon.*
   Б. Использовать команду *Chguser.*
   В. Использовать команду *Qappsrv.*
   Г. Использовать команду *Mstsc.*
2. Вы недавно создали и распространили RDP-файлы определенного приложения RemoteApp. Однако это приложение работает медленно, и вы хотите выполнить его миграцию на более мощный сервер. Как обеспечить гарантию того, что пользователи смогут подключаться к приложению RemoteApp после его миграции? (Укажите два варианта. Каждый ответ представляет готовое решение.)
   А. Создать для нового сервера терминалов новый сайт Веб-доступ к службам терминалов (TS Web Access) и опубликовать приложение на новом сайте.
   Б. Вновь создать RDP-файл приложения RemoteApp после миграции и распространить файл среди пользователей.
   В. Модифицировать свойства существующего RDP-файла и распространить его среди пользователей.
   Г. В диспетчере удаленных приложений RemoteApp на старом сервере терминалов изменить параметры компонента Сервер терминалов (Terminal Server), чтобы имя представляло новый сервер терминалов.

Закрепление материала главы

Для того чтобы попрактиковаться и закрепить знания, приобретенные в ходе изучения представленного в данной главе материала, вам необходимо:

- ознакомиться с резюме главы;
- повторить используемые в главе основные термины;
- выполнить задания лабораторной работы, которые моделируют реальные ситуации, требующие применения полученных знаний;
- выполнить рекомендуемые упражнения;
- сдать пробный экзамен с помощью тестов.

Резюме главы

- Свойства клиента служб терминалов можно настроить с помощью опций компонента Подключение к удаленному рабочему столу (Remote Desktop Connection) или параметров объекта групповой политики.
- Для управления пользовательскими сеансами на сервере терминалов используется Диспетчер служб терминалов (Terminal Services Manager, TSM). С помощью диспетчера TSM можно отображать информацию о пользователях, подключенных к серверу терминалов, отслеживать пользовательские сеансы, а также выполнять такие административные задачи, как завершение и отключение сеансов пользователей.
- Сервер шлюза служб терминалов (TS Gateway) позволяет авторизованным пользователям подключаться к серверам терминалов, расположенным за брандмауэром. Сервер шлюза служб терминалов обеспечивает конфиденциальность сеансов TS-клиентов, выполняя шифрование с помощью протокола SSL. Для настройки шлюза служб терминалов и управления им используется Диспетчер шлюза служб терминалов (TS Gateway Manager).
- Компонент Удаленные приложения RemoteApp служб терминалов (TS RemoteApp) позволяет публиковать приложения, запущенные на сервере терминалов, чтобы запускать их на стороне клиента. Компонент TS RemoteApp можно использовать в случаях, когда пользователям требуется удаленный доступ к приложениям или в организации просто не хватает оборудования и программного обеспечения, необходимого для запуска приложения. Для настройки TS RemoteApp и управления им используется Диспетчер удаленных приложений RemoteApp служб терминалов (TS RemoteApp Manager).
- Вы можете публиковать приложения RemoteApp через Веб-доступ к службам терминалов (TS Web Access), RDP-файлы или пакеты установщика Windows (Windows Installer).

Основные термины

Проверьте, знаете ли вы, что означают перечисленные ниже термины (свои ответы можно сверить с определениями, содержащимися в конце книги):

- Центр сертификации;
- сертификат;
- сеанс консоли;
- домашняя папка;
- HTTPS;
- режим TS-Install;
- публикация приложения;
- самозаверяющий сертификат;
- SSL;

- TSCAP:
- шлюз служб терминалов;
- TS RAP:
- TS RemoteApp:
- Веб-доступ к службам терминалов;
- пользовательский профиль.

Лабораторная работа

Для выполнения следующих заданий используйте знания, полученные при изучении этой главы. Правильные ответы вы сможете найти в разделе «Ответы» в конце книги.

Задание 1. Управление сеансами служб терминалов

Вы являетесь администратором компьютера TS1, на котором запущена система Windows Server 2008. На компьютере TS1 запущены Службы терминалов (Terminal Services) и несколько приложений. На протяжении дня к TS1 подключается множество пользователей, и вы отвечаете за управление пользовательскими сеансами на сервере.

1. Пользователь сообщил, что его сеанс TS на сервере TS1 завис. Какие команды можно использовать для определения ID и завершения сеанса?
2. Новый пользователь сообщил о проблемах, связанных с работой приложения на сервере TS1. Поскольку он работает в другом здании, вы хотите показать ему, как работать с приложением, не посещая физически его рабочее место. Как выполнить эту задачу?

Задание 2. Публикация приложений

Ваша компания недавно отконфигурировала сервер Server1 для управления бизнес-приложением Appl. На Server1 запущена система Windows Server 2008 и Службы терминалов (Terminal Services). Вы являетесь членом команды, занимающейся тестированием и публикацией приложения в Windows Server 2008. Ваша первая цель состоит в публикации приложения Appl для всех пользователей домена Contoso.com.

1. После установки приложения Appl на Server1 ваша команда решила публиковать Appl на рабочих столах пользователей. Вы не хотите, чтобы пользователи для запуска удаленного приложения копировали файлы из общего ресурса. Какой метод или методы развертывания вы могли бы порекомендовать?
2. Вы желаете, чтобы пользователи видели приложение в меню Пуск (Start), а также чтобы при открытии файла, расширение которого сопоставлено с Appl, нужная программа запускалась автоматически. Как лучше выполнить эту задачу?
3. Вы хотите сделать приложение Appl доступным в виде удаленной программы RemoteApp для пользователей вне корпоративной сети. Как можно выполнить

эту задачу? (Предполагается, что ваша организация располагает брандмауэром и сетью по периметру, в которой размещены публичные серверы.)

Рекомендуемые упражнения

Чтобы успешно справиться с экзаменационными заданиями, выполните следующие упражнения.

Развертывание инфраструктуры служб терминалов

В этих упражнениях вы развернете сервер терминалов, шлюз служб терминалов и удаленное приложение RemoteApp.

- **Упражнение 1** Установите Windows Server **2008** и Службы терминалов (Terminal Services) на сервере организации. В режиме TS-Install установите приложение на сервере, а затем добавьте это приложение в список Удаленные приложения RemoteApp (RemoteApp Programs) Диспетчера удаленных приложений RemoteApp служб терминалов (TS RemoteApp Manager). Установите на том же сервере компонент Веб-доступ к службам терминалов (TS Web Access), а затем подключитесь к странице Веб-доступ к службам терминалов с еще одного компьютера. Запустите приложение RemoteApp со страницы Веб-доступ к службам терминалов.
- **Упражнение 2** Разверните на втором сервере организации Шлюз служб терминалов (TS Gateway). Используйте на первом сервере Диспетчер удаленных приложений RemoteApp служб терминалов (TS RemoteApp Manager) для создания RDP-файла того же приложения. Настройте этот RDP-файл для указания нового адреса шлюза служб терминалов. Экспортируйте сертификат сервера шлюза служб терминалов на клиентский компьютер (при необходимости), а затем с помощью RDP-файла на клиентском компьютере запустите приложение RemoteApp через шлюз.

Просмотр веб-вещания

Выполняя это упражнение, вы ознакомитесь с интересной информацией о службах терминалов Windows Server2008.

- **Упражнение 1** Просмотрите веб-вещание «Windows Server **2008** Terminal Services RemoteApp and Web Access» Дэвида Хана (David Hanna) па прилагаемом к книге CD-диске в папке Webcasts или посетите сайт *http://msevents.mcrosoft.com* и найдите событие **1032355810.**

Выполнение виртульной лабораторной работы

В этих упражнениях вы займетесь настройкой инфраструктуры Службы терминалов (Terminal Services) в сети и ее управлением.

- **Упражнение 1** Посетите страницу *http://msevents.microsoft.com* и выполните поиск события 1032345540. Пройдите регистрацию и выполните лабораторную работу «TechNet Virtual Lab: Managing Terminal Services Gateway and RemoteApps in Microsoft Windows 2008».
- **Упражнение 2** Посетите страницу *http://msevents.microsoft.com* и выполните поиск события 1032347559. Пройдите регистрацию и выполните лабораторную работу «TechNet Virtual Lab: Centralized Application Access with Windows Server 2008».

Пробный экзамен

На прилагаемом к книге компакт-диске представлено несколько вариантов тренировочных тестов. Проверка знаний выполняется только по одной или же по всем экзаменационным темам сертификационного экзамена 70-643. Тестирование можно организовать таким образом, чтобы оно проводилось как экзамен, или же настроить его на изучение — в этом случае вы сможете после каждого своего ответа на вопрос просматривать правильные ответы и объяснения.

ПРИМЕЧАНИЕ Пробный экзамен

Подробнее о пробном экзамене рассказано во введении к данной книге.

ГЛАВА 5

Установка и настройка веб-приложений

Занятие 1. Установка роли веб-сервера (IIS) 230

Занятие 2. Настройка Internet Information Services 257

Современные веб-сайты обеспечивают функциональность многих локально установленных клиентских приложений. Эти приложения предоставляют доступ к базам данных в общественных средах и интрасетях, позволяют пользователям настроить их работу.

Веб-приложения и веб-службы используют множество различных стандартов, протоколов и технологий разработок.

Операционная система Windows Server 2008 содержит готовую платформу веб-служб Internet Information Services (IIS) 7.0, которая может поддерживать веб-содержимое и веб-приложения различных типов. Компонент IIS 7.0 обеспечивает значительные улучшения в управлении, расширяемости и стабильности, а также обратную совместимость для поддержки миллионов веб-сайтов с предыдущими версиями IIS.

В этой главе вы изучите принципы установки и настройки в Windows Server 2008 ролей Веб-сервер (IIS) и Сервер приложений (Application Server). Исходя из требований своей среды вы сможете включить многочисленные компоненты и службы. Излагаемая здесь информация поможет вам также развернуть и настроить IIS в производственных средах.

Темы экзамена:

- Настройка веб-приложений.
- Управление веб-сайтами.
- Управление Internet Information Services (IIS).

Требования

Для выполнения упражнений этой главы должна быть установлена система Windows Server 2008 на Server2.contoso.com.

ПРИМЕЧАНИЕ Альтернативная установка

Вы можете выполнить большинство упражнений еще на одном компьютере Windows Server 2008, однако вам может потребоваться внести некоторые изменения в процесс. Кроме того, разные выпуски Windows Server 2008 отличаются в отношении лицензирования, включая базовую архитектуру роли веб-сервера (IIS).

Реальный мир

Анил Десаи

Успешной ли будет установка сервера, часто зависит от того, насколько его конфигурация соответствует потребностям пользователей и разработчиков.

Если некоторые компоненты отсутствуют, приложения не будут запускаться должным образом. Если в систему включено слишком много компонентов, они могут оказать отрицательное влияние на безопасность, совместимость и производительность. Поэтому нужно, как говорится, сделать все правильно. В подобной ситуации коммуникации играют важную роль.

Во многих IT-подразделениях нет согласованности между командами разработчиков приложений (например, веб-разработчиками) и системными администраторами, отвечающими за их развертывание и поддержку. Довольно часто бывает, что функции каждой из команд в организации определены нечетко, вследствие чего трудно разобраться, кто отвечает за итоговую конфигурацию продукта.

Однако эти проблемы можно решить. Системные администраторы должны четко сформулировать требования к веб-приложениям, которые они поддерживают. А веб-разработчики могут сразу учитывать требования и предложения потенциальной конфигурации производственных серверов.

Здесь огромное значение приобретает написание технической документации. И наконец, нельзя забывать о конечных пользователях. Независимо от того, являются ли они сотрудниками вашей организации, важно понимать, с какой целью они посещают ваши веб-сайты. В решении этих задач вам может помочь маркетинговое исследование.

Занятие 1. Установка роли веб-сервера (IIS)

Хотя включение IIS и связанных компонентов обычно представляет собой довольно простую процедуру, нужно знать архитектуру, компоненты и доступные возможности платформы. На этом занятии вы изучите модульную архитектуру IIS и принципы конфигурирования компьютера Windows Server 2008 в качестве веб-сервера.

Изучив материал этого занятия, вы сможете:

- •S Описать архитектуру IIS 7.0, включая новые компоненты.
- S Определить назначение роли сервера приложений.
- S Описать назначение служб ролей, связанных с ролью веб-сервера (IIS).
- •S Установить роль веб-сервера (IIS), а также добавлять и удалять службы ролей.
- S Выполнять установку роли веб-сервера (IIS) из командной строки, а также автоматизированную установку.

Расчетная продолжительность занятия составляет 45 мин.

Безопасность веб-сервера

Веб-сервер IIS 7.0 содержит набор компонентов и опций для поддержки веб-служб и приложений различных типов.

Использование утилиты Диспетчер сервера (Server Manager) упрощает процесс установки IIS, а также компонентов и опций веб-сервера. Системному администратору, отвечающему за развертывание IIS с учетом различных требований, перед установкой ролей веб-сервера и сервера приложений важно изучить структуру IIS. В настоящем разделе описаны опции развертывания платформы IIS.

К СВЕДЕНИЮ Другие компоненты IIS

Платформа IIS помимо поддержки веб-приложений, которым посвящена эта глава, обеспечивает компоненты сервера для протоколов File Transfer Protocol (FTP) и Simple Mail Transfer Protocol (SMTP). Информация о других компонентах содержится в главе 7.

Веб-стандарты и протоколы

Чтобы понять назначение и функции платформы IIS, нужно вначале изучить используемые веб-приложениями протоколы и стандарты. Изначально для коммуникаций с веб-службами используется протокол HTTP (Hypertext Transfer Protocol), который обеспечивает модель запроса-отклика для коммуникаций с другими компьютерами в сети. Для получения доступа к трафику HTTP используется протокол TCP/IP (Transmission Control Protocol/Internet Protocol), основанный на сетевых подключениях. Поскольку веб-трафик играет важную роль, большинство организаций разрешают своим пользователям получать доступ в Интернет через TCP-порт 80 — порт HTTP по умолчанию.

Протокол HTTP не запоминает состояния и не обеспечивает встроенный механизм отслеживания коммуникаций между клиентами и серверами. Каждый запрос должен включать сведения, идентифицирующие запрашивающую сторону, а также другую информацию, которая может потребоваться для выполнения транзакции.

Веб-стандарты и протоколы также включают методы защиты данных, передаваемых между компьютерами. По умолчанию HTTP-трафик передается незашифрованным потоком, который можно без труда декодировать. Хотя такой подход вполне приемлем при получении пользователями доступа к публичному содержимому, многим веб-сайтам и приложениям требуется передавать информацию между клиентами и серверами в защищенном виде. В качестве распространенного примера можно привести сайт обработки денежных поступлений, который принимает данные кредитных карточек через Интернет. Протокол HTTPS (HTTP Secure) обеспечивает поддержку шифрования HTTP-трафика. По умолчанию подключения HTTPS используют для коммуникаций TCP-порт 443, хотя вы можете указать и любой другой порт. Для шифрования чаще всего используются такие механизмы, как SSL (Secure Sockets Layer) и TLS (Transport Layer Security). Естественно, можно также использовать и другие механизмы шифрования, особенно в интрасетях.

Веб-стандарты и протоколы обеспечивают согласованный метод обмена информацией между компьютерами. Изначальная спецификация веб-страниц выполняется с помощью протокола HTML (Hypertext Markup Language). Формат HTML-страниц на основе тегов позволяет разработчикам использовать технологии для создания содержимого таким образом, чтобы оно принималось различными веб-браузерами. Инструменты разработок могут быть самыми разными, начиная с текстовых редакторов, например программа Блокнот (Notepad) системы Microsoft Windows, и заканчивая полнофункциональными средами разработок наподобие платформы Microsoft Visual Studio.

Протоколы HTTP и HTML были предназначены для организации базовых коммуникаций и служб презентации. Современные веб-приложения включают компоненты, обеспечивающие выполнение комплексных функций с использованием данных стандартов. Активные веб-сайты создаются веб-разработчиками на основе таких платформ разработок, как ASP.NET (компонент структуры Microsoft .NET Framework). Эти сайты могут отслеживать пользовательские сеансы, а также обеспечивать доступ к базам данных и другой хранящейся в среде информации.

ПРИМЕЧАНИЕ Стандарты Интернета

Более подробные сведения о стандартах Интернета и Веб можно найти на веб-сайте World Wide Web Consortium (W3C) по адресу *http://www.w3.org,* а также на веб-сайте Internet Engineering Task Force (IETF) по адресу *http://www.ietf.org*. Оба сайта содержат официальную спецификацию и описание основных протоколов Интернета.

Сценарии с использованием веб-сервера

Изначальное преимущество использования веб-содержимого и веб-приложений состоит в их доступности для множества различных клиентских компьютеров. На компьютерах пользователей не нужно устанавливать и конфигурировать какое-либо программное обеспечение, как для стандартных приложений. По-

скольку современные операционные системы включают в себя или поддерживают стандартные веб-браузеры, например Windows Internet Explorer, большинство пользователей уже располагают основными клиентскими средствами для получения доступа к веб-содержимому. IT-персонал и разработчики программного обеспечения могут использовать различные технологии представления содержимого и развертывания приложений для внутренних и внешних пользователей.

Платформа IIS предназначена для поддержки различных сценариев. Далее приведены некоторые примеры.

- **Публичные веб-сайты** Многие бизнес-требования к обмену информацией в Интернете довольно просты. Например, небольшая организация может предоставить контактную информацию и сведения о своих услугах на простом веб-сайте.
- **Интернет-магазины** Электронная торговля в Интернете позволяет поставщикам рекламировать и продавать различную продукцию. Интернет-магазины обеспечивают функциональность корзины покупок, обработку заказов, а также поддержку потребителей.
- **Сценарии интрасети** Веб обеспечивает для всех пользователей в организации простой метод получения доступа и представления содержимого. Такие задачи компании, как создание отчетов о затратах или доходах, можно выполнять в онлайновом режиме, если нет необходимости в непосредственном контакте с персоналом организации.
- **Производственные приложения** Часто при разработке бизнес-приложений необходимо обеспечить возможность их развертывания и управления их установкой на стороне клиента. Для решения таких задач многие организации создают внутренние приложения, доступ к которым осуществляется через веб-браузер. Можно привести самые разные примеры таких приложений, начиная с сайта, выполняющего одну функцию, и заканчивая распределенными производственными системами.
- **Интернет-приложения** Пользователи могут получать доступ к своей электронной почте и создавать документы, Fie устанавливая приложения на свои компьютеры. Распределенные организации и команды также могут использовать преимущества защищенного доступа к корпоративным приложениям из Интернета.
- **Сценарии экстрасети** Для получения услуг организации часто вступают в партнерские отношения с другими компаниями. В сценарии экстрасети пользователи вне организации могут получать доступ к информации. В данном случае важную роль играет безопасность, и веб-приложения обеспечивают стандартный метод, с помощью которого пользователи могут получать доступ к нужной информации.
- **Веб-хостинг** Многие компании предлагают услуги по размещению информации на веб-сайтах. Эти компании запускают на одном физическом сервере большое количество веб-сайтов, обеспечивая безопасность, быстродействие и стабильность.

Большинство организаций развертывают IIS в нескольких ролях. Важно отметить, что требования к компонентам и опциям зависят от конкретного развертывания.

СОВЕТ Подготовка к экзамену
При изучении компонентов и опций платформы IIS имеет смысл рассмотреть сценарии, в которых эти компоненты могут потребоваться для выполнения технических или бизнес-требований. При сдаче сертификационного экзамена 70-643 вам могут задать вопрос, для ответа на который потребуется знать специфические требования и уметь определять на их основе соответствующую опцию или компонент.

Далее мы рассмотрим компоненты и службы, которые поддерживаются платформой IIS.

Новые компоненты IIS

Платформа IIS предоставляет один из самых популярных веб-серверов для публичных и частных веб-сайтов. Версия IIS 7.0 системы Windows Server 2008 включает множество новых компонентов и обеспечивает повышение быстродействия в различных сферах деятельности. Далее описаны основные области применения улучшений платформы.

- **Администрирование** Неудобство в работе с предыдущими версиями IIS было связано с большим количеством страниц свойств и диалоговых окон. В IIS 7.0 включены новые инструменты администрирования, предназначенные для более эффективного управления множеством опций и параметров. Пользовательский интерфейс разработан с учетом требований как веб-разработчиков, так и системных администраторов.
- **Безопасность** По умолчанию роль веб-сервера (IIS) включена лишь в базовый набор функций. Даже двоичные файлы неиспользуемых компонентов недоступны в стандартных папках операционной системы. Системные администраторы должны явным образом включать дополнительные службы и компоненты. Такой подход позволяет снизить фронт атак IIS и упростить управление. Кроме того, в сам продукт включены функции автоматического определения распространенных попыток хакинга. (Раньше для включения этого компонента нужно было устанавливать утилиту URLScan.)
- **Диагностика и устранение неполадок** Поскольку веб-службы являются ключевым компонентом инфраструктуры организаций, важно иметь возможность быстро обнаруживать и устранять неполадки в работе этих служб. В IIS 7.0 включены новые компоненты, позволяющие выявлять ошибки и получать сведения, необходимые для их устранения.
- **Централизованное управление конфигурацией** Многие организации поддерживают десятки, а то и сотни инсталляций IIS. Для выполнения требований расширяемости и производительности часто приходится развертывать множество веб-серверов с практически одинаковыми параметрами конфигурации. В предыдущих версиях IIS было довольно сложно управлять этими конфигурациями без подключения к каждому серверу. Версия IIS 7.0 предо-

ставляет администраторам упрощенный метод совместного использования данных конфигурации с помощью веб-ферм. Для обеспечения безопасности учетных записей IIS создается согласованный набор учетных записей пользователей, включая глобально уникальные идентификаторы (GUID) и разрешения. Администраторы могут использовать конкретные имена и параметры учетных записей при создании сценариев и автоматизации распространенных процессов. В IIS 7.0 также включена значительно улучшенная поддержка командной строки.

- **Поддержка делегирования** Довольно часто возникает необходимость разделить задачи администрирования веб-серверов из соображений безопасности или удобства управления. В IIS 7.0 обеспечена возможность реализации гранулированных разрешений конфигурации безопасности с целью поддержки веб-сред и конфигураций производственного уровня.
- **Обратная совместимость** Подавляющее большинство веб-сайтов и приложений, созданных для предыдущих версий IIS, совместимо с IIS 7.0. Кроме того, для таких приложений обеспечиваются средства управления IIS 6.0.

В целом в платформе IIS 7.0 устранены распространенные проблемы, с которыми приходилось сталкиваться в предыдущих версиях IIS. Далее в этой главе мы рассмотрим различные компоненты IIS и многочисленные усовершенствования платформы.

К СВЕДЕНИЮ IIS в Windows Vista

Платформа IIS 7.0 была вначале внедрена для операционной системы Windows Vista. Поскольку архитектура ядра IIS в Windows Vista аналогична архитектуре ядра в Windows Server 2008, веб-разработчики могут использовать аналогичные среды на рабочих станциях и своих производственных серверах. Однако следует отметить, что существуют отличия в принципах работы некоторых компонентов этих платформ и в условиях лицензирования. Более подробные сведения о них можно найти на веб-сайте Microsoft Internet Information Services по адресу *http://www.microsoft.com/iis/*.

Компоненты и опции IIS

Платформа IIS имеет модульную архитектуру на основе компонентов. В самой простой конфигурации базовые функции HTTP обеспечиваются компонентом Веб-сервер (Web server). IIS содержит множество компонентов и функций, поддерживающих содержимое и приложения различных типов. В большинстве схем развертывания требуются лишь некоторые из этих компонентов и функций. Поэтому администраторы могут включать только те из них, которые нужны для работы их веб-приложений.

Хотя модульная архитектура требует, чтобы системные администраторы явным образом включали нужные компоненты, она обеспечивает многочисленные преимущества.

- **Улучшенная безопасность** Каждая включенная служба или компонент потенциально увеличивает фронт атак сервера IIS. В частности, сказанное

относится к общедоступным серверам, которые могут являться целями атак или попыток неавторизованного доступа.

Например, уязвимость в конкретном типе расширения IIS может быть использована для выполнения неавторизованных действий на сервере. Поэтому, включая лишь те компоненты и службы, которые необходимы для содержимого и приложений, администраторы могут значительно снизить эти угрозы.

- **Повышение быстродействия** Установка и включение ненужных компонентов на сервере IIS приводит к расходованию системных ресурсов. Если администратор будет включать лишь те компоненты, которые требуются для работы, ресурсы сервера можно будет резервировать для использования другими приложениями. Таким образом обеспечивается более высокая производительность и расширяемость.
- **Возможность настройки конфигураций серверов** Как уже отмечалось ранее в этой главе, организации используют IIS в различных сценариях развертывания. При этом требования безопасности и функциональности могут существенно отличаться. Модульная архитектура позволяет системным администраторам настраивать каждое развертывание на основе требований. Например, требования безопасности для внутренних веб-серверов и серверов в Интернете часто значительно отличаются. Администраторы могут независимо включать необходимые компоненты для каждого типа сервера. В этом разделе вы изучите компоненты и опции платформы IIS.

ВАЖНО! Сведения от команды IIS

Команда IIS корпорации Microsoft создала веб-сайт, который содержит различные руководства, технические статьи и другую информацию о работе с платформой IIS. На нем вы можете найти подробные сведения о множестве доступных компонентов и функций IIS. На сайте есть ссылки на загружаемые файлы и информацию о продуктах, работающих с платформой IIS. Члены команды IIS также разместили собственные блоги с информацией на основе своего опыта. Главная страница расположена по адресу *http://www.iis.net*.

Сервер приложений

Одним из исходных преимуществ платформы Windows является поддержка широкого набора технологий разработки приложений. Современные приложения могут зависеть от возможностей коммуникации. Например, распределенное приложение часто должно создавать и осуществлять транзакции и управлять ими на нескольких сайтах с использованием различных служб в распределенной сети. Разработка такого типа функциональности может оказаться довольно сложной задачей. Разработчики приложений могут значительно экономить время и силы, используя преимущества компонентов, уже доступных на платформах операционных систем.

Роль Сервер приложений (Application Server) в системе Windows Server 2008 служит для поддержки различных технологий разработки приложений. Она основана на технологии .NET Framework 3.0 и включает поддержку других коммуникаций и возможностей презентаций. Хотя роль Сервер приложений не

зависит непосредственно от роли Веб-сервер (IIS) (Web Server (IIS)), распределенные приложения ASP.NET или Windows Communication Foundation (WCF) требуют использования обеих ролей.

ПРИМЕЧАНИЕ Подготовка к экзамену
Роль Сервер приложений (Application Server) помимо поддержки ASP.NET и других служб, доступных для роли Веб-сервер (IIS) (Web Server (IIS)), обеспечивает дополнительную функциональность. Если для работы конкретного веб-приложения или веб-службы вам не требуется роль Сервер приложений, ее устанавливать нет необходимости. Например, основные приложения ASP.NET будут запускаться и без включенной на сервере роли сервера приложений.

Вы можете установить роль Сервер приложений (Application Server) с помощью Мастера добавления ролей (Add Roles Wizard) в Диспетчере сервера (Server Manager). При добавлении этой роли вам будет предоставлена возможность определить дополнительные службы ролей, которые планируется включить. Далее описаны эти компоненты.

- **Ядро сервера приложений (Application Server Foundation)** Этот компонент необходим для роли сервера приложений. Он включает поддержку технологии развертывания приложений .NET Framework 3.0 и управления ими. Основными компонентами этой технологии являются WCF, Windows Presentation Foundation (WPF) и Windows Workflow Foundation (WF).
- **Поддержка веб-сервера (IIS) (Web Server (IIS) Support)** Роль Сервер приложений (Application Server) можно интегрировать с ролью Веб-сервер (IIS) (Web Server (IIS)), чтобы обеспечить для веб-приложений доступ к дополнительным функциям. При выборе этой опции вам будет предложено автоматически установить IIS, если данный компонент еще не установлен.
- **Доступ к сети COM+ (COM+ Network Access)** Стандарт Component Object Model (COM) позволяет разработчикам приложений получать доступ к различным элементам кода приложения. Технология COM+ обеспечивает возможность удаленной активизации кода приложения в сети (или получения доступа). Этот компонент может потребоваться для работы распределенных приложений COM+ с множеством уровней функциональности.
- **Совместное использование TCP-порта (TCP Port Sharing)** Потенциальная задача управления при работе в распределенных средах состоит в поддержке множества серверных приложений на одном компьютере. Обычно каждому приложению требуется собственный TCP-порт для реагирования на входящие запросы. Данный компонент позволяет множеству приложений совместно использовать один порт, что упрощает конфигурацию сервера и брандмауэра.
- **Поддержка служб активации процессов Windows (Windows Process Activation Service Support)** Служба активации процессов Windows (Windows Process Activation Service) обеспечивает возможность получения доступа к сервисам приложений в сети с помощью различных типов протоколов и служб. Этот компонент может использоваться самим сервером IIS для поддержки дополнительных протоколов и методов коммуникаций.

- Распределенные транзакции (Distributed Transactions) Приложениям, использующим распределенные транзакции, для координации деятельности перед внесением перманентных изменений требуется множество серверов и приложений. С помощью этого компонента можно включить входящие и исходящие удаленные транзакции и поддержку стандарта WS-Atomic Transactions для всб-служб.

Чтобы определить необходимые компоненты сервера приложений, вам следует согласовать требования с разработчиками веб-приложений.

Правильно выполняемое определение и согласование требований всб-сервера позволит повысить уровень совместного сотрудничества системных администраторов, разработчиков и поддерживаемых пользователей. С точки зрения IT-персонала, использование технологии IIS обеспечит организации преимущество во всех сферах деятельности.

Службы ролей IIS 7.0

Службы ролей определяют конкретные компоненты и опции платформы IIS, доступные для использования на локальном веб-сервере. После установки IIS 7.0 на компьютере Windows Server 2008 компоненты можно добавлять с помощью Диспетчера сервера (Server Manager).

При использовании диспетчера сервера откроется диалоговое окно, показанное на рис. 5-1.

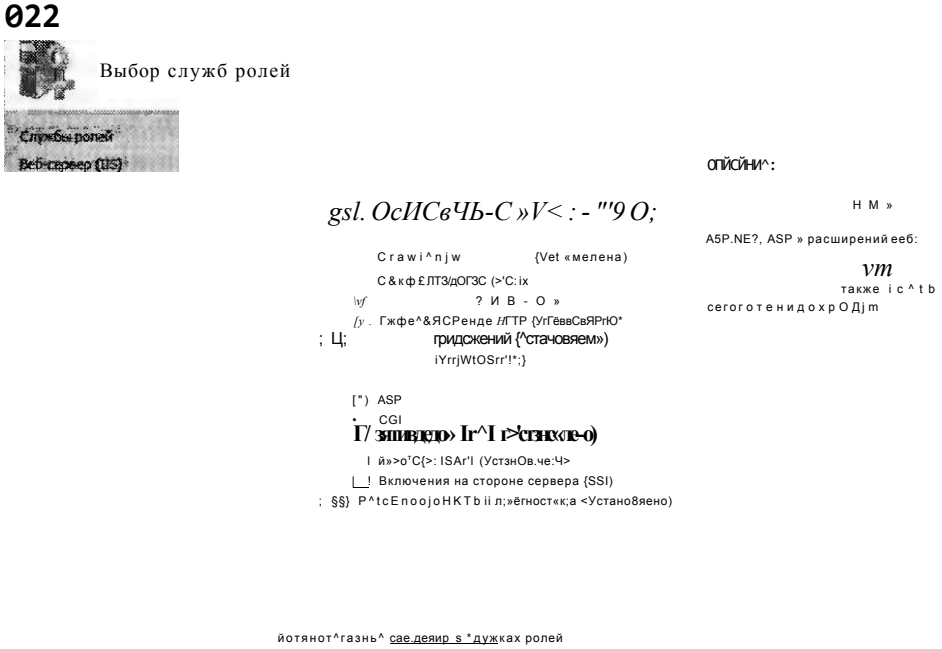


Рис. 5-1. Управление службами ролей веб-сервера в диспетчере сервера

Службы ролей IIS разбиты на несколько категорий:

- Основные возможности HTTP (Common HTTP Features);
- Разработка приложений (Application Development);
- Работоспособность и диагностика (Health and Diagnostics);
- Безопасность (Security);
- Быстродействие (Performance);
- Средства управления (Management Tools);
- Служба FTP-публикации (FTP Publishing Service).

На верхнем уровне иерархии расположен Веб-сервер (Web Server). Этот элемент представляет основные службы IIS, требующиеся для опциональных компонентов, которые также можно установить. Элементы Средства управления (Management Tools) и Служба FTP-публикации (FTP Publishing Service) можно установить независимо от элемента Веб-сервер (Web Server). Каждая область содержит связанные компоненты и опции. Работа некоторых элементов зависит от других служб ролей.

Если перед выбором элемента не определять его зависимости, будет предоставлена возможность автоматической установки необходимых ролей служб, как показано на рис. 5-2.

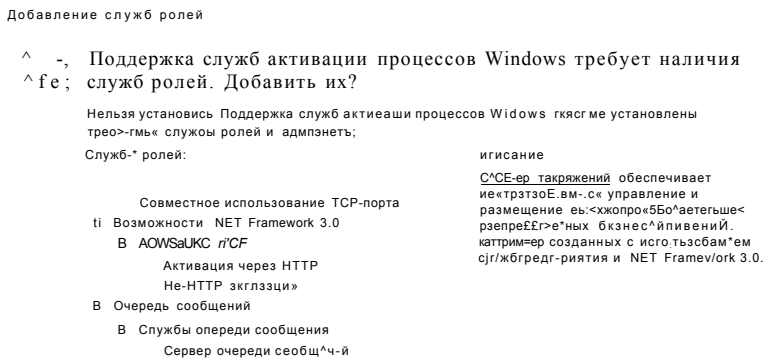


Рис. 5-2. Включение зависимостей ролей при добавлении службы ролей

СОВЕТ Подготовка к экзамену

Отметим, что добавляемые службы ролей становятся доступными для использования вашими веб-сайтами и приложениями, однако иногда требуется дополнительное конфигурирование. Например, при включении определенных опций проверки подлинности они не будут применяться автоматически ко всем вашим веб-сайтам. При сдаче сертификационного экзамена 70-643 следует помнить, что добавление службы роли Веб-сервер (Web Server) может являться лишь одним из этапов согласования требований решения.

Службы ролей IIS по умолчанию

Как уже отмечалось ранее, в конфигурацию по умолчанию включен ограниченный набор функций. Такая конфигурация устанавливается с целью обслуживания ограниченного статического содержимого, если нет необходимости в обеспечении дополнительной безопасности и средств разработки. Во многих случаях может потребоваться включение дополнительных опций.

В табл. 5-1 перечислены службы ролей, которые включаются при добавлении на компьютер роли Веб-сервер (IIS) (Web Server (IIS)).

Табл. 5-1. Службы ролей по умолчанию в роли Веб-сервер (IIS)

Группа/Категория	Компоненты
Основные возможности HTTP (Common HTTP Features)	Статическое содержимое (Static Content) Стандартный документ (Default Document) Обзор каталогов (Directory Browsing) Ошибки HTTP (HTTP Errors)
Работоспособность и диагностика (Health and Diagnostics)	Ведение журнала HTTP (HTTP Logging) Монитор запросов (Request Monitor)
Безопасность (Security)	Фильтрация запросов (Request Filtering)
Быстродействие (Performance)	Сжатие статического содержимого (Static Content Compression)
Средства управления (Management Tools)	Консоль управления IIS (IIS Management Console)

В следующих разделах мы рассмотрим назначение этих служб, а также многих опциональных служб ролей.

Основные возможности HTTP

Самой важной функцией роли Веб-сервер (IIS) (Web Server (IIS)) является обслуживание веб-страниц HTML с помощью протокола HTTP. В группе Основные возможности HTTP (Common HTTP Features) доступны для установки следующие компоненты.

- **Статическое содержимое (Static Content)** Эта функциональность позволяет обслуживать статические веб-страницы с помощью HTTP. Самыми распространенными типами содержимого являются статические страницы HTML и рисунки. Файлы со статическим содержимым обычно непосредственно пересылаются пользователям без выполнения обработки на стороне сервера.
- **Стандартный документ (Default Document)** Этот компонент позволяет IIS автоматически возвращать определенный файл для веб-сайта, если он не запрошен явным образом в URL. Например, если пользователь пытается подключиться к сайту *http://www.contoso.com,* веб-сервер может возвращать в качестве отклика файл default.htm.
- **Обзор каталогов (Directory Browsing)** В IIS включена функциональность, обеспечивающая листинг основных каталогов для пользователей. Этот ком-

понент отправляет информацию о файлах и папках на веб-сайте на веб-браузер клиента. Поскольку пользователи имеют возможность получать доступ к загрузке всех файлов, для которых указаны соответствующие разрешения, обычно этот компонент отключен для общедоступных веб-сайтов. Если при включении компонента Стандартный документ (Default Document) навден стандартный документ, пользователи не увидят окно обзора каталогов.

- **Ошибки HTTP (HTTP Errors)** По умолчанию большинство веб-браузеров автоматически отображают сообщения об ошибках для пользователей. Если, например, страница не найдена на сервере или сервер перегружен, веб-браузер отобразит эту информацию для пользователя. Чтобы обеспечить удобство работы пользователя, IIS можно отконфигурировать для автоматического возвращения настраиваемых страниц с сообщениями об ошибках в случае возникновения проблем. Страницы с сообщениями об ошибках могут включать контактные данные администратора веб-сайта и другую информацию.
- **Перенаправление HTTP (HTTP Redirection)** Протокол HTTP поддерживает метод перенаправления запроса с одного сайта на другой. Веб-сервер можно настроить для автоматической отправки пользователю запроса перенаправления HTTP при получении доступа к определенному сайту. Перенаправление запросов удобно использовать в ситуациях с переименованием URL веб-сайта или когда для получения доступа к одному и тому же содержимому назначено множество URL.

Все эти основные возможности HTTP можно добавлять для сайтов, однако поведение каждого веб-сайта IIS зависит от его содержимого и параметров конфигурации.

Разработка приложений

Хотя некоторые веб-сайты используют лишь статическое содержимое, для работы производственных сайтов требуется динамическая поддержка веб-серверов и веб-приложений. В IIS обеспечена поддержка различных возможностей и технологий для соответствия этим требованиям.

Далее приведен список служб ролей Разработка приложений (Application Development).

- **ASP.NET** Основной платформой разработок веб-серверов Microsoft является ASP.NET. Она основана на технологии .NET Framework и обеспечивает мощную и гибкую инфраструктуру разработок для выполнения распространенных задач проектирования веб-сайтов. Эта платформа содержит встроенную поддержку управления доступом к базам данных, методы обеспечения безопасности и проверки подлинности, а также функции стабильности и расширяемости.
- **Расширяемость .NET (.NET Extensibility)** Программная платформа Microsoft .NET Framework.может использоваться для модификации набора функций веб-сервера IIS. Эта служба ролей позволяет разработчикам получать доступ к управлению именными пространствами IIS и объектами для конструирования логики, взаимодействующей с запросами веб-серверов.
- **ASP** Технология ASP (Active Server Page) является предшественницей платформы ASP.NET. Она обеспечивала упрощенный метод разработки веб-

приложений с использованием сценариев. Сценарии ASP запускаются на веб-сервере и генерируют содержимое HTML, которое передается пользователю обратно через IIS. В основном поддержка ASP предназначена для обеспечения обратной совместимости с приложениями, которые еще не перенесены на платформу ASP.NET.

- **CGI** Общий интерфейс шлюза (Common Gateway Interface, CGI) представляет собой стандарт, определяющий метод передачи веб-серверами информации программным сценариям. Он требуется для работы некоторых компонентов на стороне сервера, в частности тех, которые предназначены для запуска на множестве платформ веб-серверов. Поддержка CGI требуется на веб-сервере таким языкам веб-разработок, как PHP:Hypertext Preprocessor. В IIS 7.0 включены компоненты, значительно повышающие быстродействие обработки CGI.
- **Расширения ISAPI (ISAP1 extensions)** В IIS обеспечена поддержка стандарта расширения ISAPI (Internet Server Application Programming Interface). Создавая расширения ISAPI, веб-разработчики могут создавать собственные обработчики содержимого, которые будут взаимодействовать с каждым аспектом конвейера веб-запросов. Стандарт ISAPI предназначен для обеспечения расширяемости с целью поддержки множества одновременно покупаемых запросов.
- **Фильтры ISAPI (ISAPI filters)** Эти фильтры представляют собой настраиваемый код, который можно создавать для обработки специфических запросов веб-сервера. Их логика может принимать сведения о веб-запросе и возвращать соответствующее содержимое в зависимости от логики на стороне сервера. В IIS осуществляются попытки сопоставить веб-запросы с соответствующим фильтром ISAPI для обработки его типа содержимого. Установка этой службы ролей позволяет разработчикам добавлять в IIS настраиваемые фильтры ISAPI.
- **Включения на стороне сервера (SSI) (Server Side Includes)** Веб-разработчики часто используют возможность внедрения определенного распространенного содержимого во все свои веб-страницы. В качестве примеров можно привести заголовок сайта, элементы навигации и нижние колонтитулы сайтов. Служба ролей Включения на стороне сервера (SSI) позволяет веб-серверу включать другие элементы содержимого при генерировании запроса веб-сервера. Из соображений безопасности этот компонент по умолчанию отключен. Тем не менее он может потребоваться для работы сайтов, на которых не используются другие технологии веб-разработок (например, ASP.NET).

При планировании развертывания коммерческих веб-сайтов определите дополнительные компоненты, которые следует включить для обеспечения их функциональности. Обычно эти сведения можно получить от группы или организации разработчиков веб-приложений.

Работоспособность и диагностика

Хотя основная функциональность веб-серверов может показаться довольно простой, во время обработки стандартных веб-запросов нужно выполнять мно-

жество операций. Организации, использующие свои веб-серверы для получения доступа к критически важной информации и системам, должны применять методы изоляции и устранения неполадок и всех возникающих проблем. Службы ролей, включенные в компонент Работоспособность и диагностика (Health and Diagnostics), предназначены для содействия администраторам и разработчикам в сборе и анализе информации о веб-запросах.

Одной из распространенных задач, связанных с мониторингом веб-сайтов, является управление генерируемым объемом информации. Процесс записи подробных сведений обо всех запросах может значительно влиять на быстродействие производственных систем. Для решения этой проблемы в IIS 7.0 реализованы улучшенные возможности сбора сведений о запросах и настройки типов собираемых данных. Компонент Работоспособность и диагностика (Health and Diagnostics) включает в себя следующие службы ролей.

- **Ведение журнала HTTP (HTTP Loggings)** Базовая функция ведения журнала в IIS состоит в сохранении информации HTTP-запроса в текстовых файлах на сервере. Ведение журнала HTTP обеспечивает также набор параметров по умолчанию для ведения журнала запросов. Детали можно настроить в свойствах каждого веб-сайта. По умолчанию файлы журнала сохраняются в папку %SystemDrive%\Inetpub\Logs\LogFiles. На рис. 5-3 показан список полей, которые можно включить в файлы журнала.

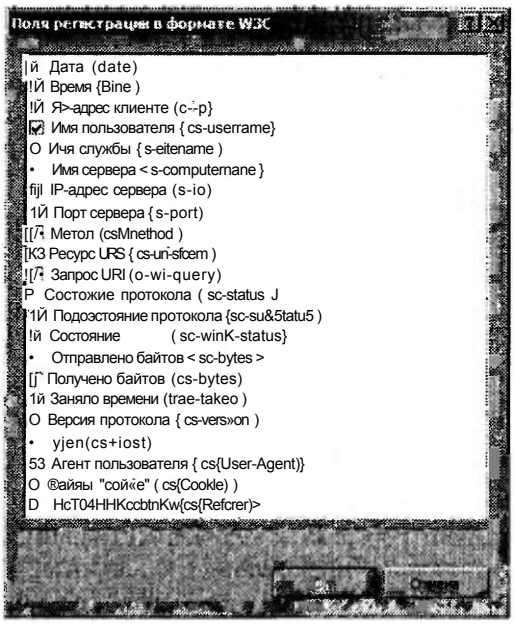


Рис. 5-3. Настройка опций ведения журнала

- **Средства ведения журналов (Logging Tools)** Необработанные журналы запросов **HTTP** довольно сложно просматривать и анализировать вручную. На загруженных веб-серверах эти файлы могут быстро вырасти до угрожающих размеров. Поскольку содержимое, как правило, организовано в виде

одной строки на запрос, администраторам может потребоваться выполнить поиск в тысячах строк для извлечения нужной информации. Служба ролей Средства ведения журналов (Logging Tools) обеспечивает простые утилиты для получения доступа к данным файлов журналов и для их анализа.

- **Монитор запросов (Request Monitor)** Основная сложность диагностики проблем производительности на веб-сервере заключается в определении текущей активности. Компонент Монитор запросов (Request Monitor) позволяет администраторам определять текущие выполняемые запросы на веб-сервере. Таким образом, администраторы могут выявить потенциальную причину замедления работы или зависания запросов.
- **Слежение (Tracing)** При возникновении ошибки на веб-сервере или снижении его производительности нужно собрать как можно больше информации о возникшей проблеме. К сожалению, детали, касающиеся всех запросов, хранить непрактично из соображений быстродействия. Слежение позволяет IIS сохранять детальные сведения обо всех запросах с ошибками. Этот компонент сохраняет в памяти информацию о выполнении запросов вплоть до их успешной обработки. В случае ошибки результаты запроса можно сохранить на веб-сервере для последующего анализа.
- **Особое протоколирование (Custom Logging)** Компонент Ведение журнала HTTP (HTTP Logging) по умолчанию обеспечивает хранение информации о веб-запросах в текстовом формате. Хотя этот формат вполне может соответствовать основным требованиям большинства веб-сайтов и служб, организации могут также с помощью этого компонента создавать собственные модули COM. Разработчикам потребуется создать модуль ведения журнала, а затем зарегистрировать его с помощью IIS для хранения данных. Такой подход обеспечивает максимальную гибкость при определении типов записываемых данных.
- **Ведение журнала ODBC (ODBC Logging)** Хотя хранение данных в текстовом файле является вполне эффективным методом ведения журнала запросов, это усложняет анализ производительности веб-сервера и отчетность. Служба ролей Ведение журнала ODBC (ODBC Logging) позволяет приложениям сохранять данные веб-запросов в любом формате, который поддерживается подключением ODBC (Open Database Connectivity). В качестве примеров можно привести такие серверы реляционных баз данных, как Microsoft SQL Server и файловые форматы Microsoft Excel. Важно отметить, что запись данных в журналы ODBC может создать на веб-сервере значительные нагрузки, связанные с обработкой и сохранением данных.

Веб-администраторы часто используют программы анализа журналов с целью обработки текстовых файлов журналов с информацией о запросах. Эти сведения можно использовать для устранения проблем (таких как ошибочные ссылки или отсутствующее содержимое), а также для анализа трафика и популярности конкретных веб-страниц.

Безопасность

Обеспечение безопасности веб-сайтов, веб-приложений и веб-служб играет первостепенную роль для всех веб-серверов. В зависимости от конкретной

конфигурации развертывания и использования организации могут включать обширный набор механизмов обеспечения безопасности. Далее приведен список служб ролей Безопасность (Security), доступных в IIS:

- Обычная проверка подлинности (Basic Authentication);
- Windows-проверка подлинности (Windows Authentication);
- Дайджест-проверка подлинности (Digest Authentication);
- Проверка подлинности с сопоставлением сертификата клиента (Client Certificate Mapping Authentication);
- Проверка подлинности с сопоставлением сертификата клиента IIS (IIS Client Certificate Mapping Authentication);
- Проверка подлинности URL (URL Authentication);
- Фильтрация запросов (Request Filtering);
- Ограничения IP-адресов и доменов (IP and Domain Restrictions).

Выбор и реализация этих механизмов обеспечения безопасности описаны в главе 6.

Быстродействие

Все типы веб-серверов должны обеспечивать возможность обслуживания большого количества запросов в заданный интервал времени. В IIS включены многочисленные архитектурные компоненты, обеспечивающие эффективное выполнение веб-запросов. Кроме того, службы ролей Быстродействие (Performance) включают две дополнительные опции, описанные далее.

- **Сжатие статического содержимого (Static Content Compression)** Протокол HTTP обеспечивает метод, с помощью которого статические веб-страницы (например, файлы HTML) можно сжимать перед отправкой на клиентские веб-браузеры. Веб-браузер разархивирует эту информацию и выполнит прорисовку (рендеринг) страницы. Этот метод позволяет значительно экономить пропускную способность с минимальной нагрузкой CPU на стороне клиента и сервера. Кроме того, в IIS включена возможность хранения в памяти статического содержимого, к которому достаточно часто запрашивается доступ. Эта возможность позволяет повысить быстродействие и обеспечить расширяемость. Данный компонент включен по умолчанию и работает автоматически, если веб-браузеры пользователей поддерживают сжатие содержимого HTTP.
- **Сжатие динамического содержимого (Dynamic Content Compression)** Динамическое содержимое обычно представляет собой различную информацию, отправляемую разным пользователям. Поскольку динамическое содержимое часто изменяется для каждого запроса веб-сервера, сжатие данных может создать значительную нагрузку на сервер. По умолчанию сжатие динамического содержимого отключено, однако его можно добавить с целью снижения нагрузки на пропускную способность веб-приложений.

В целом ограничение пропускной способности играет большую роль, чем ограничение мощностей обработки на современных серверах. Поэтому рекомендуется включить сжатие статического содержимого, если у организации нет особых причин для его отключения.

Средства управления

Компонент Средства управления (Management Tools) обеспечивает возможность определять программы, которые будут доступны для работы с IIS. По умолчанию вместе с ролью Веб-сервер (IIS) (Web Server (IIS)) из средств управления устанавливается лишь основной административный инструмент Консоль управления IIS (IIS Management Console).

Этот инструмент обеспечивает графический метод конфигурирования веб-служб IIS и управления ими. Вы можете удалить Консоль управления IIS, если собираетесь удаленно управлять сервером или если этого требует корпоративная политика безопасности.

Другими ценными инструментами компонента Средства управления (Management Tools) являются инструмент Сценарии и средства управления IIS (IIS Management Scripts and Tools), который позволяет осуществлять администрирование IIS в командной строке, а также инструмент Служба управления (Management Service), позволяющий осуществлять удаленное администрирование IIS с помощью Консоли управления IIS.

Одной из важных задач проектирования IIS 7.0 является обеспечение поддержки веб-приложений IIS 6.0.

Хотя многие приложения можно непосредственно перенести в IIS 7.0, в новую версию в качестве служб ролей включены компоненты, обеспечивающие обратную совместимость:

- Совместимость управления IIS 6 (IIS 6 Management Compatibility);
- Совместимость метабазы IIS 6 (IIS 6 Metabase Compatibility);
- Совместимость WMI в IIS 6 (IIS 6 WMI Compatibility);
- Службы сценариев IIS 6 (IIS 6 Scripting Tools);
- Консоль управления IIS 6 (IIS 6 Management Console).

Более подробно вы изучите эти компоненты и принципы их использования на занятии 2.

Установка роли Веб-сервер (IIS)

Несмотря на многочисленные компоненты и опции, доступные для роли Веб-сервер (IIS) (Web Server (IIS)), установка соответствующих опций является довольно простой задачей. Добавление этой роли является основой для обеспечения функциональности веб-сервера. Компоненты IIS также требуются для работы нескольких других компонентов и опций Windows Server 2008. Для добавления роли сервера используется Мастер добавления ролей (Add Roles Wizard) в Диспетчере сервера (Server Manager), как показано на рис. 5-4.

Мастер добавления ролей (Add Roles Wizard) автоматически проанализирует конфигурацию локального компьютера и определит дополнительные службы ролей, которые нужно установить. Например, если Служба активации процессов Windows (Windows Process Activation Service) еще не установлена, вам будет предложено установить ее.

На этапе установки веб-сервера (IIS) отображается некоторая вводная информация об использовании IIS, а также сведения об установке WSRM с целью поддержки быстродействия на случай, если компьютер будет выполнять множество ролей.

Рис. 5-4. Выбор роли Веб-сервер (IIS) (Web Server (IIS)) в мастере добавления ролей

На странице Выбор служб ролей (Select Role Services) можно определить компоненты IIS, которые будут инсталлированы в процессе установки роли, как показано на рис. 5-5.

Опции по умолчанию обеспечивают минимальный набор компонентов ядра роли веб-сервера. Как будет описано далее в этой главе, вы также можете добавлять и удалять службы ролей после включения роли Веб-сервер **(IIS)** (Web Server **(IIS)).** Поскольку работа некоторых компонентов роли зависит от других компонентов, при выборе элемента вам может быть предложено добавить эти зависимости.

На странице Подтвердите выбранные элементы (Confirm Installation Selections) отображается список выбранных параметров конфигурации н служб ролей.

Процесс установки запускается щелчком кнопки Установить (Finish). В зависимости от выбранных служб ролей процесс установки может выполняться довольно долго и требовать перезагрузки сервера. После перезагрузки Мастер добавления ролей (Add Roles Wizard) продолжит выполнение с последней конечной точки. И наконец, на странице Результат выполнения установки (Installation Results), показанной на рис. 5-6, отобразится список установленных компонентов и дополнительная информация

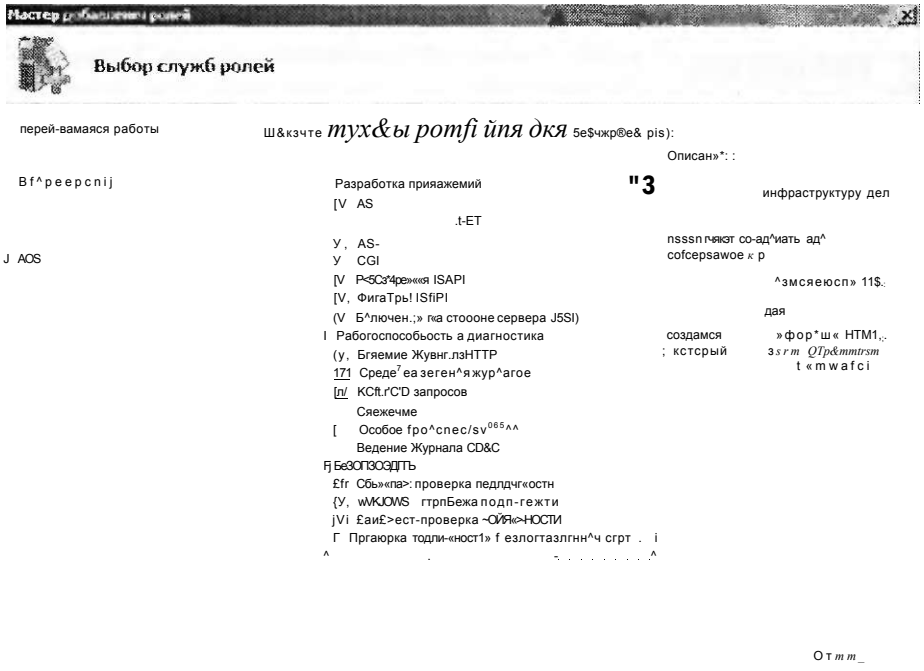


Рис. 5-5. Выбор служб ролей Веб-сервер (IIS) (Web Server (IIS)

ESSI

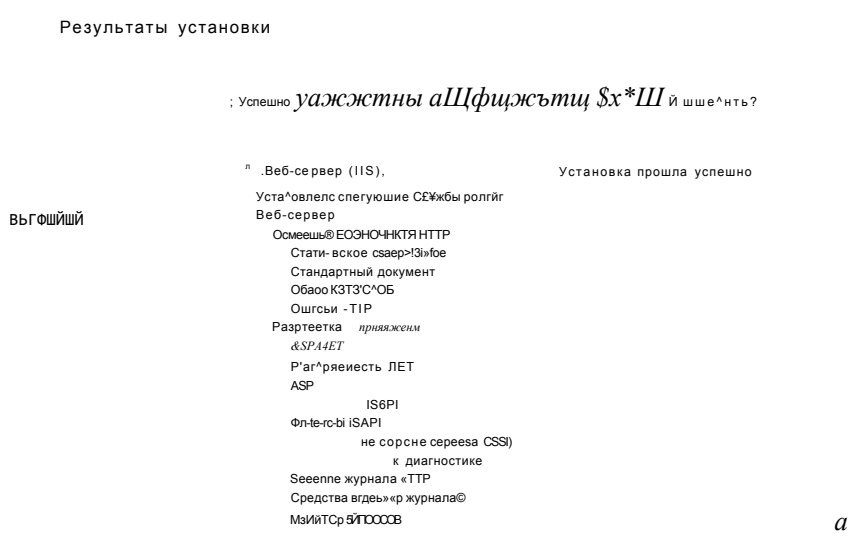


Рис. 5-6. Просмотр результатов установки роли Веб-сервер (IIS) (Web Server (IIS)

Проверка установки IIS с помощью диспетчера сервера

После установки IIS в вашем распоряжении имеется несколько методов проверки корректности работы процессов веб-сервера. Первый метод состоит в использовании Диспетчера сервера (Server Manager). Разверните раздел Роли (Roles), а затем щелкните роль Веб-сервер (IIS) (Web Server (IIS)) для просмотра сведений. Па странице отобразится информация обо всех событиях, которые требуют вашего внимания. Кроме того, здесь будут перечислены установленные службы с указанием их текущего состояния, как показано на рис. 5-7. Список включенных элементов зависит от установленных служб ролей и зависимостей. Компонент Служба веб-публикаций (World Wide Publishing Service, W3SVC) является основным инструментом, который отвечает за реагирование на веб-запросы.

Диспетчер сервера также отображает информацию о службах, установленных для роли Веб-сервер (IIS), как показано на рис. 5-8. Для внесения изменений в конфигурацию можно использовать ссылки Добавить службы ролей (Add Role Services) и Удалить службы ролей (Remove Role Services).

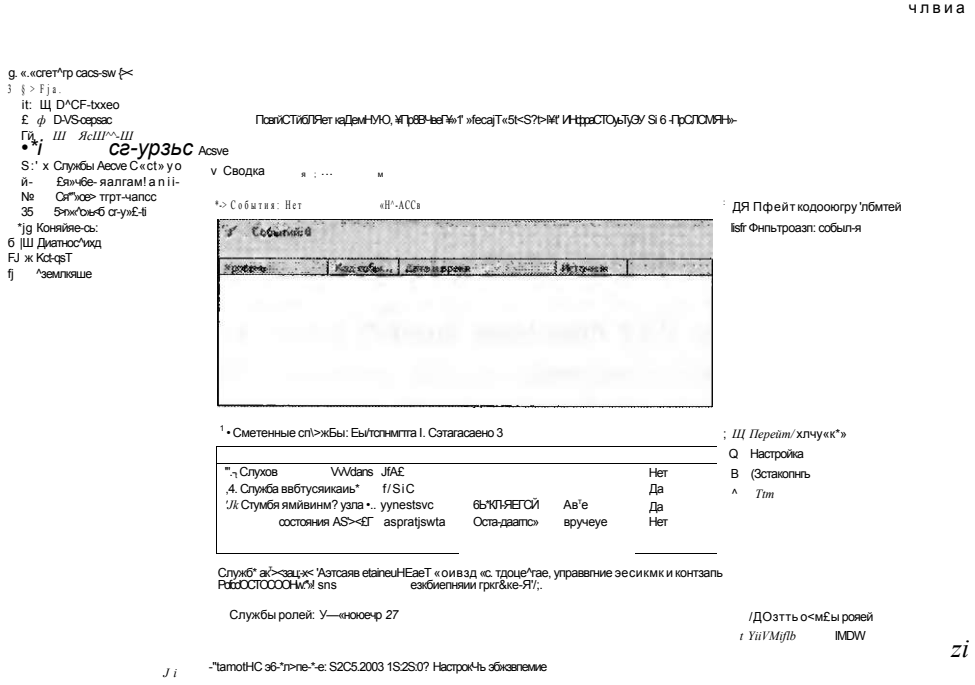


Рис. 5-7. Просмотр состояния роли Веб-сервер (IIS) (Web Server (IIS)) в диспетчере сервера

И наконец, в разделе Ресурсы и поддержка (Resources And Support) представлены рекомендации и другая подробная информация, которая может оказаться полезной при первой настройке IIS и роли веб-сервера на компьютере. Более подробно эти опции описаны в занятии 2. В указанном разделе также

представлены ссылки на множество онлайновых ресурсов с информацией об использовании IIS.

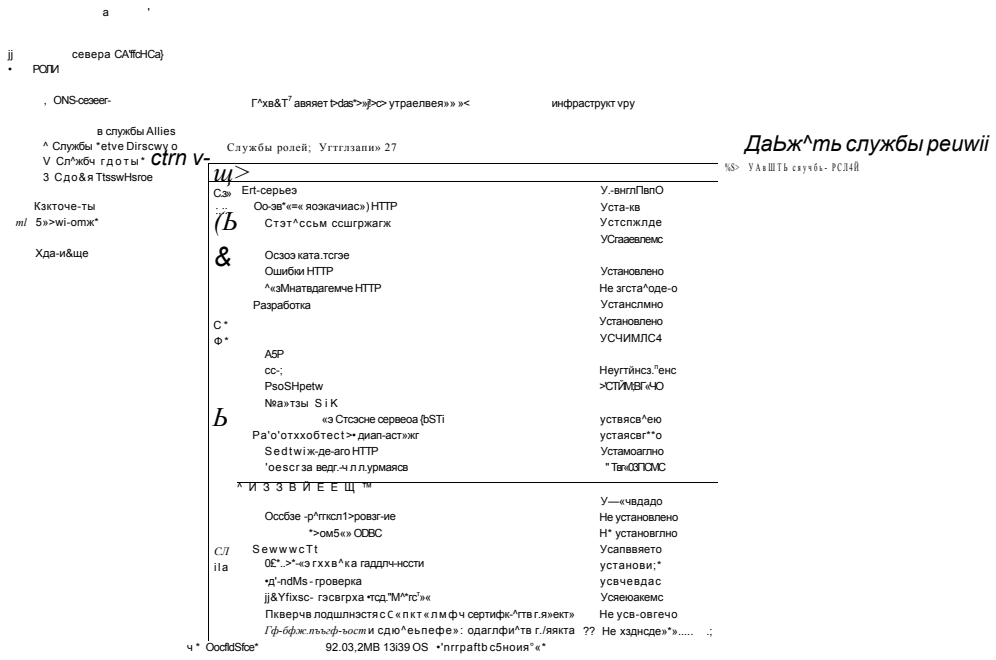


Рис. 5-8. Список установленных служб ролей в диспетчере сервера

Проверка установки IIS с помощью Internet Explorer

При добавлении роли веб-сервера (IIS) на компьютер Windows Server 2008 автоматически создается веб-сайт, который по умолчанию настроен на прослушивание запросов на HTTP-порте 80. По умолчанию этот сайт размещен в папке %SystemDrive%\Inetpub\wwwroot. Содержимое по умолчанию включает в себя лишь статическую HTTP-страницу и файл изображения.

Поскольку назначение IIS состоит в обслуживании веб-страниц, один из способов проверки работы заключается в запуске веб-браузера и подключении к локальному компьютеру. Вы можете использовать встроенный локальный псевдоним http://localhost или полное имя компьютера (например, http://serverl.contoso.com). В любом случае откроется страница приветствия по умолчанию, как показано на рис. 5-9. При выборе языка выполняется автоматическое перенаправление на веб-сайт *http://www.iis.net,* если, конечно, сервер располагает доступом в Интернет.

Вам также следует попытаться получить доступ к веб-сайту IIS с удаленного компьютера. Просто откройте любой веб-браузер и подключитесь к полностью указанному адресу веб-сервера. Если вам не удается подключиться, причиной могут являться ошибки разрешения имен DNS (Domain Name System) или конфигурация брандмауэра.

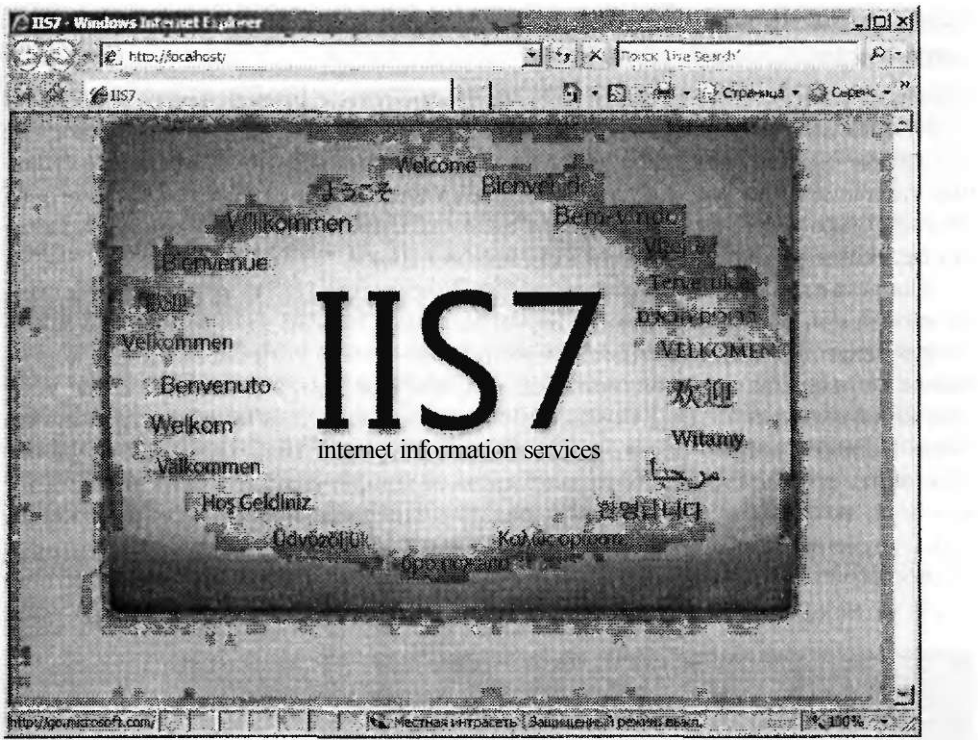


Рис. 5-9. Веб-сайт IIS по умолчанию

Управление службами ролей

Модульная архитектура IIS позволяет быстро и без труда добавлять и удалять службы ролей после установки роли Веб-сервер (IIS) (Web Server (IIS)) на компьютер Windows Server 2008. Основной причиной изменения конфигурации службы ролей является необходимость в поддержке нового типа веб-приложения или веб-службы. Вы также можете удалять службы, которые больше не нужны, в частности в случае изменения технических требований. Поскольку удаление или добавление службы ролей влияет на конфигурацию всего сервера, перед выполнением операции следует учесть потенциальные эффекты на всех веб-сайтах сервера.

Для добавления или удаления службы откройте Диспетчер сервера (Server Manager), разверните раздел Роли (Roles), щелкните правой кнопкой мыши Веб-сервер (IIS) (Web Server (IIS)) и примените соответственно команду Добавить службы ролей (Add Role Services) или Удалить службы ролей (Remove Role Services). В открывшемся диалоговом окне будут показаны установленные компоненты — напротив их названий будут установлены флажки. Если флажок сброшен, это означает, что элемент не установлен. Напротив названий уже установленных компонентов службы ролей флажки не активны.

При добавлении или удалении служб ролей появляется окно подтверждения, после чего запускается процесс. Если требуется перезагрузка компьютера, процесс настройки возобновляется автоматически при следующем входе на сервер.

Использование командной строки и опций автоматизированной установки

Организациям, использующим IIS, часто требуется развертывать множество различных инсталляций IIS. Хотя вы можете выполнять этот процесс локально на каждом сервере, довольно часто более эффективный способ состоит в создании сценариев или команд для выполнения необходимых действий. Существует несколько методов выполнения автоматизированной установки, а также инсталляции с использованием командной строки.

Для установки роли Веб-сервер (IIS) (Web Server (IIS)) из командной строки можно использовать утилиту ServerManagerCmd.exe. Например, при запуске команды *ServerManagerCmd.exe-install Web-Server* устанавливаются компоненты веб-сервера по умолчанию. Для просмотра ролей и компонентов, установленных на локальном компьютере, можно также использовать команду *ServerManagerCmd.exe-query,* как показано на рис. 5-10. Эту команду удобно применять для быстрого сбора всех данных конфигурации и определения изменений, которые нужно внести с целью поддержки нового веб-приложения. Для получения более подробной информации об использовании этой утилиты в командную строку введите команду *ServerManagerCmd.exe -?*. Данную утилиту также можно использовать для добавления и удаления компонентов WSRM.

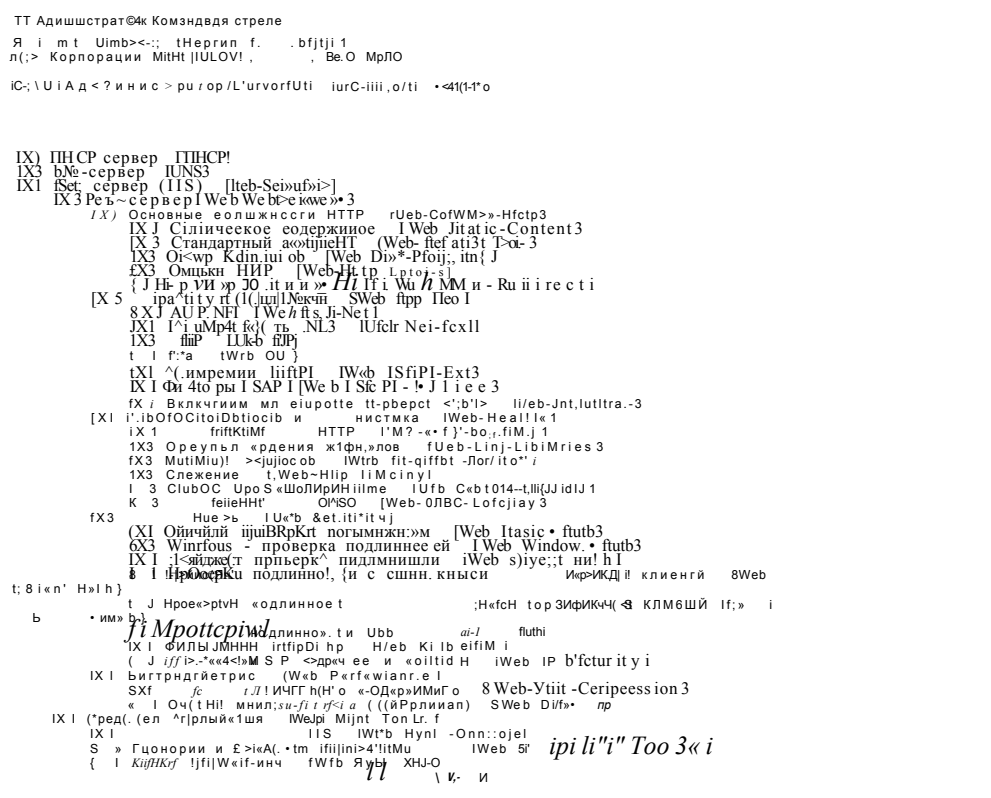


Рис. 5-10. Просмотр списка установленных служб ролей и компонентов с помощью утилиты ServerManagerCmd.exe

Для установки роли веб-сервера (JIS) из командной строки можно также использовать утилиту Диспетчер пакетов Windows (Windows Package Manager, PkgMgr.exe). Для храпения данных о компонентах и опциях, которые следует включить в установку I IS. диспетчер пакетов Windows использует XML-файл. Чтобы получить более подробные сведения, в командную строку введите команду *PkgMgr.exe -?*.

На занятии 2 вы изучите другие утилиты и команды, которые можно использовать для конфигурирования IIS из командной строки или сценариев.

Удаление роли Веб-сервер (IIS)

Если вам больше не нужна роль веб-сервера для компьютера Windows Server 2008, вы можете удалить IIS и все связанные компоненты с помощью команды Удалить роли (Remove Roles) в Диспетчере сервера (Server Manager). Однако не забывайте, что веб-сервер может потребоваться для работы различных компонентов и функций операционной системы. На рис. 5-11 показана страница Подтверждение выборов для удаления (Confirm Removal Selections).

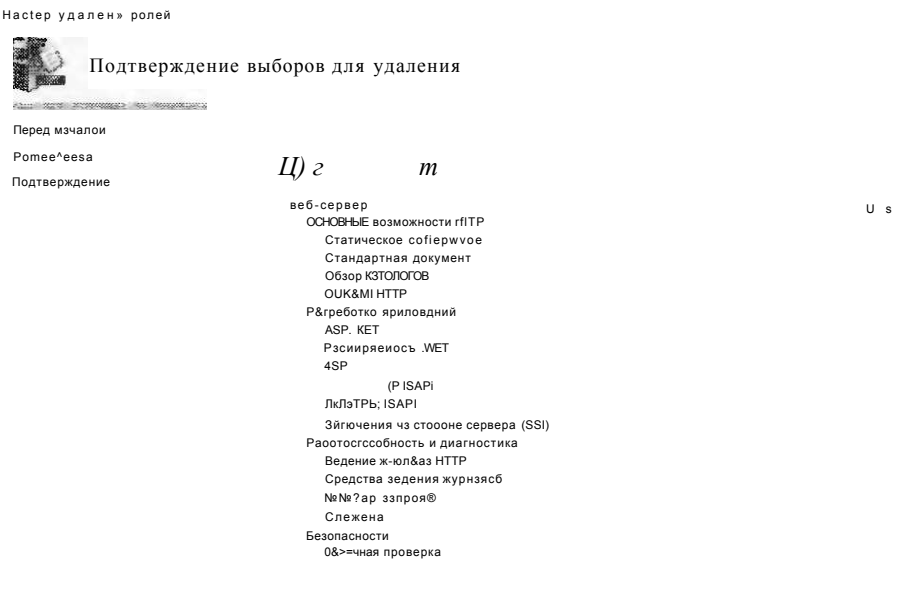


Рис. 5-11. Подтверждение удаления роли Веб-сервер (IIS) (Web Server (IIS))

В зависимости от того, какие установлены компоненты, в процессе удаления может потребоваться перезагрузить компьютер. После перезагрузки процесс возобновится автоматически при следующем входе пользователя на компьютер.

В результате удаления роли Веб-сервер (IIS) (Web Server (IIS)) будут удалены все двоичные файлы и службы ролей, связанные с веб-сервером. Базовая конфигурация сервера, включая список веб-сайтов и их параметров, будет

сохранена в случае переустановки роли веб-сервера. Реальное содержимое веб-сайтов нельзя удалить автоматически. Если вы планируете навсегда удалить веб-службы с сервера, вручную удалите все оставшиеся веб-страницы и данные, которые больше не нужны.

Диспетчер системных ресурсов Windows

Для любого сервера важно, чтобы работа основных служб не прерывалась при загрузке системы. По умолчанию большинство служб в Windows Server 2008 запускается с одинаковым уровнем приоритета. Диспетчер системных ресурсов Windows (Windows Resource Manager, WSRM) позволяет администраторам назначать приоритеты различным системным процессам, таким как IIS. Хотя диспетчер WSRM не требуется для запуска IIS, он может пригодиться в определенных ситуациях. Например, администраторы могут создавать Политики выделения ресурсов (Resource Allocation Policies) для определения ограничений CPU и памяти, чтобы гарантировать реагирование системы даже в случае высокой степени нагрузки, как показано на рис. 5-12.

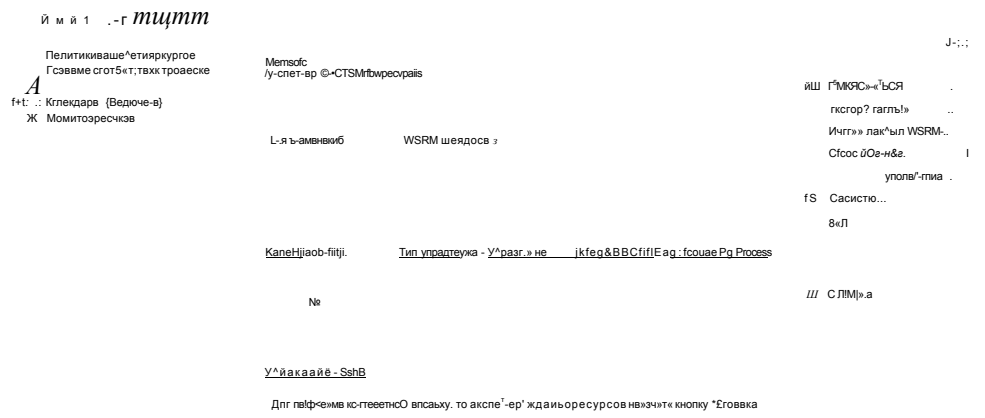


Рис. 5-12. Диспетчер системных ресурсов Windows (WSRM)

Диспетчер WSRM можно добавить на компьютер Windows Server 2008 с по мощью Диспетчера сервера (Server Manager). Для запуска процесса щелкнит правой кнопкой мыши элемент Диспетчер сервера (Server Manager) и приме ните команду Добавить компоненты (Add Features). Запустится Мастер добав ления компонентов (Add Features Wizard), с помощью которого можно добавит компонент Диспетчер системных ресурсов Windows (Windows Resource Mana

ger). Дополнительную информацию о диспетчере WSRM можно найти в Справке и поддержке Windows (Windows Help And Support).

Проверьте себя

1. С помощью каких двух методов можно проверить, успешно ли прошла установка роли Веб-сервер (IIS)?
2. Когда в роль Веб-сервер (IIS) можно добавлять службы ролей?

Ответы

1. Диспетчер сервера (Server Manager) можно использовать для проверки установки и запуска служб, а Internet Explorer или другой веб-браузер можно применять для проверки реагирования веб-сайта по умолчанию.
2. Службы ролей можно добавить во время изначального добавления роли, а также после включения роли Веб-сервер (IIS).

Практикум. Установка и проверка роли Веб-сервер (IIS)

В предложенных далее упражнениях вы выполните установку роли Веб-сервер (IIS) (Web Server (IIS)) на сервере server2.contoso.com.

Упражнение 1. Установка роли Веб-сервер (IIS)

В этом упражнении вы выполните установку роли веб-сервера IIS лишь с основными службами ролей по умолчанию.

1. Войдите на сервер server2.contoso.com с использованием учетной записи члена группы локальных администраторов.
2. Откройте Диспетчер сервера (Server Manager). Щелкните правой кнопкой мыши элемент Роли (Roles), а затем примените команду Добавить роли (Add Roles), чтобы открыть Мастер добавления ролей (Add Roles Wizard). На странице Перед началом работы (Before You Begin) щелкните кнопку Далее (Next).
3. На странице Выбор ролей сервера (Select Server Roles) выберите роль Веб-сервер (IIS) (Web Server (IIS)). При необходимости добавьте все требуемые зависимости. Щелкните кнопку Далее (Next).
4. На странице Веб-сервер (IIS) (Web Server (IIS)) прочитайте вводную информацию о работе с IIS. Для получения подробной информации о веб-сервере IIS и связанных компонентах можно воспользоваться ссылками в разделе Дополнительные сведения (Additional Information). Щелкните кнопку Далее (Next). Выбор по умолчанию на странице Выбор служб ролей (Selcet Role Services) включает основные компоненты роли Веб-сервер (IIS). Вы можете получить более подробные сведения о каждом элементе в списке, выделив его и прочитав текст в правой части страницы. Для большинства элементов имеются ссылки на дополнительные источники информации. Поскольку в этом упражнении вы добавляете лишь компоненты по умолчанию, оставьте опции по умолчанию и щелкните кнопку Далее (Next). Список опций, выбранных по умолчанию, приведен в табл. 5-1.

5. На странице Подтвердите выбранные элементы (Confirm Installation Selections) проверьте выбор служб ролей. При желании вы можете отправить эти данные на печать, отослать по электронной почте или сохранить. Для запуска процесса установки щелкните кнопку Установить (Install).
6. После завершения процесса установки проверьте установленные роли и службы на странице Результаты установки (Installation Results) и щелкните кнопку Закрыть (Close).
7. Закройте Диспетчер сервера (Server Manager).

Упражнение 2. Тестирование IIS

В этом упражнении вы проверите установку роли Веб-сервер (IIS) (Web Server (IIS)), добавленной на сервер server2.contoso.com в упражнении 1. В частности, для проверки работы IIS вы используете Диспетчер сервера (Server Manager) и Internet Explorer.

1. Войдите на сервер server2.contoso.com с использованием учетной записи члена группы локальных администраторов.
2. Откройте Диспетчер сервера (Server Manager). Разверните элемент Роли (Roles) и щелкните роль Веб-сервер (IIS) (Web Server (IIS)). Будет выведена итоговая информация о роли веб-сервера. В разделе События (Events) отображаются все важные сообщения, связанные с ролью Веб-сервер (IIS).
3. В разделе Системные службы (System Services) проверьте запуск Службы веб-активаций (World Wide Web Publishing Service, W3SVC). Здесь также будет указана Служба поддержки узла приложений (Application Host Helper Service, apphostsvc) и Служба активации Windows (Windows Process Activation Service). Если одна из этих служб остановлена, щелкните ее и запустите.
4. В разделе Службы ролей (Role Services) просмотрите список установленных элементов и проверьте установку всех опций по умолчанию. (Список служб ролей по умолчанию приведен в табл. 5-1 занятия 1.)
5. Закройте Диспетчер сервера (Server Manager) и откройте Internet Explorer. В адресную строку введите *http://localh.ost* и нажмите клавишу Enter. Должна открыться страница приветствия IIS по умолчанию.
6. В адресную строку Internet Explorer введите URL-адрес *http://server2.contoso.com* и нажмите клавишу Enter. Должна открыться страница приветствия IIS по умолчанию. Закройте Internet Explorer.
7. Закройте Диспетчер сервера (Server Manager).

Резюме

- Роль Веб-сервер (IIS) (Web Server (IIS)) позволяет предоставить доступ к содержимому веб-сайта с использованием протокола HTTP.
- Роль Сервер приложений (Application Server) обеспечивает поддержку приложений, для работы которых требуются компоненты .NET Framework 3.0, COM+ и распределенные транзакции.
- Диспетчер системных ресурсов Windows (Windows System Resource Manager, WSRM) можно использовать для назначения правил выделения ресурсов различным рабочим процессам и службам, например IIS.

- Службы ролей IIS 7.0 включают компоненты, предназначенные для разработки приложений, обеспечения работоспособности и диагностики, быстродействия и управления.
- Диспетчер сервера (Server Manager) можно использовать для добавления роли Веб-сервер (IIS) (Web Server (IIS)) и управления службами ролей.
- Установку IIS можно проверить с помощью диспетчера сервера или путем открытия веб-сайта по умолчанию в Internet Explorer.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний после изучения материала занятия 1. Если вы предпочитаете электронную форму вопросов, обратитесь к прилагаемому к книге компакт-диску.

ПРИМЕЧАНИЕ Ответы

Ответы на вопросы и пояснения к каждому варианту ответа размещены в разделе «Ответы» в конце книги.

1. Будучи системным администратором, вы пытаетесь устранить проблему, связанную с получением доступа к веб-сайту на компьютере Windows Server 2008. Раньше пользователи могли получать доступ к этому веб-сайту по адресу *http://hr.contoso.com*. Однако теперь при попытке получить доступ появляется сообщение о том, что Internet Explorer не может отобразить страницу. Какие действия нужно предпринять для устранения этой ошибки.
   А. С помощью диспетчера сервера добавить роль Ошибки HTTP (HTTP Errors).
   Б. С помощью диспетчера сервера проверить запуск службы веб-публикаций (World Wide Web Publishing Service).
   В. Проверить конфигурацию веб-браузеров пользователей.
   Г. С помощью диспетчера сервера добавить службу ролей Ведение журнала HTTP (HTTP Logging).
   Д. В диспетчере сервера щелкнуть роль Веб-сервер (IIS) и проверить запуск службы IIS Admin Service.

Занятие 2. Настройка Internet Information Services

После установки роли Веб-сервер (IIS) (Web Server (IIS)) вам может потребоваться заняться созданием веб-сайтов и управлением ими, а также включить определенные компоненты, необходимые для работы приложений. Детали выполнения этих задач зависят от типа веб-служб и принципа использования IIS. В частности, вам следует учесть миграцию веб-сайтов из предыдущих версий IIS, а также необходимость управления множеством сайтов и приложений на одном сервере. Для упрощения администрирования в IIS включено несколько удобных средств и методов управления. На этом занятии вы изучите методы управления веб-сайтами и параметрами сервера для роли Веб-сервер (IIS) в Windows Server 2008.

К СВЕДЕНИЮ Безопасность IIS

Возможность управлять параметрами и разрешениями безопасности имеет очень важное значение для производственных веб-серверов. Настоящее занятие посвящено настройке веб-приложений и компонентов, не связанных с. безопасностью. Более подробные сведения о методах проверки подлинности и авторизации содержатся в главе 6.

Изучив материал этого занятия, вы сможете:

- С помощью утилиты Диспетчер служб IIS (IIS Manager) подключаться и управлять параметрами сервера для роли веб-сервера.
- Создавать и настраивать параметры веб-сайтов, включая связывание сайтов.
- Создавать новые веб-приложения на веб-сайтах и осуществлять управление ими.
- Описывать назначение пулов приложений и управлять параметрами пула приложений для веб-сайтов и веб-приложений.
- Создавать виртуальные каталоги и осуществлять управление ими.
- Использовать утилиту AppCmd.exe для выполнения распространенных задач администрирования веб-сервера IIS.
- Описать принципы управления IIS 7.0 параметрами конфигурации в файлах ApplicationHost.config и Web.config.
- Обеспечить поддержку миграции приложений из IIS 6.0.

Расчетная продолжительность занятия составляет 60 мин.

Средства управления IIS

Как вы уже знаете из занятия 1, в IIS включено множество компонентов и опций, которые можно использовать для выполнения различных технических и бизнес-требований. Утилита Диспетчер служб IIS (Internet Information Services (IIS) Manager) является основным средством, используемым для настройки веб-сайтов и их параметров, а также для управления ими. Эта программа устанавливается автоматически при добавлении роли Веб-сервер (IIS) (Web Server (IIS)) на компьютер Windows Server 2008 с использованием опций по умолчанию. Утилиту Диспетчер служб IIS (IIS Manager) можно запустить из группы программ Администрирование (Administrative Tools). На рис. 5-13 представлен пользовательский интерфейс этой утилиты.

По умолчанию диспетчер служб IIS будет подключаться к локальному серверу. Он позволяет внести изменения в конфигурацию сервера и другие параметры этого компьютера. Диспетчер служб IIS предназначен для получения большого объема информации с использованием простых и согласованных компонентов пользовательского интерфейса. В левой панели показана информация о сервере, к которому вы подключены. Вы можете развернуть эти узлы для просмотра сведений о веб-сайтах и других объектах на данном сервере.

Некоторые элементы содержат дополнительные команды, которые можно открыть, щелкнув имя объекта правой кнопкой мыши.

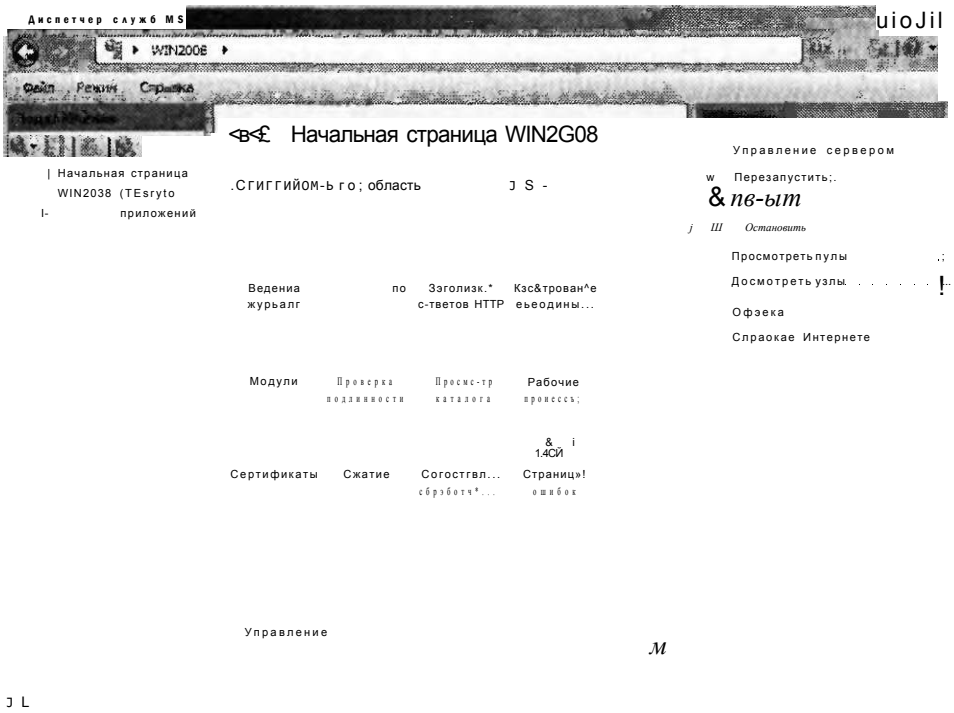


Рис. 5-13. Использование диспетчера служб IIS для подключения к локальному серверу

Просмотр возможностей

Центральная панель содержит сведения и опции, связанные с выбранным элементом в левой панели. В нижней части панели можно выбрать один из двух основных режимов просмотра. При выборе режима Просмотр возможностей (Features View) отобразится список всех доступных параметров, которые можно настроить для выбранного элемента. Список элементов зависит от ролей, добавленных в конфигурацию сервера. Раскрывающийся список Сгруппировать по (Group By) позволяет указать метод отображения различных элементов с помощью следующих опций.

- **Без группирования (No Grouping)** Все элементы отображаются в алфавитном порядке в одном списке.
- **Категория (Category)** Элементы группируются на основе их функциональных областей (например. Быстродействие (Performance) и Безопасность (Security)).
- **Область (Area)** Элементы группируются по областям конфигурации, на которые они влияют.

На рис. 5-14 показаны элементы, отображаемые при выборе сервера в левой панели и метода группирования по категории. Помимо этих опций вы можете отображать элементы, используя опции Сведения (Details), Значки- (Icons), Плитка (Tiles) и Список (List). Общая раскладка аналогична раскладке обозревателя Windows. Она предназначена для группирования и отображения большого количества параметров, чтобы администраторам было легче осуществлять управление. Двойным щелчком компонента загружается отдельная страница опций, где можно модифицировать параметры этого компонента.

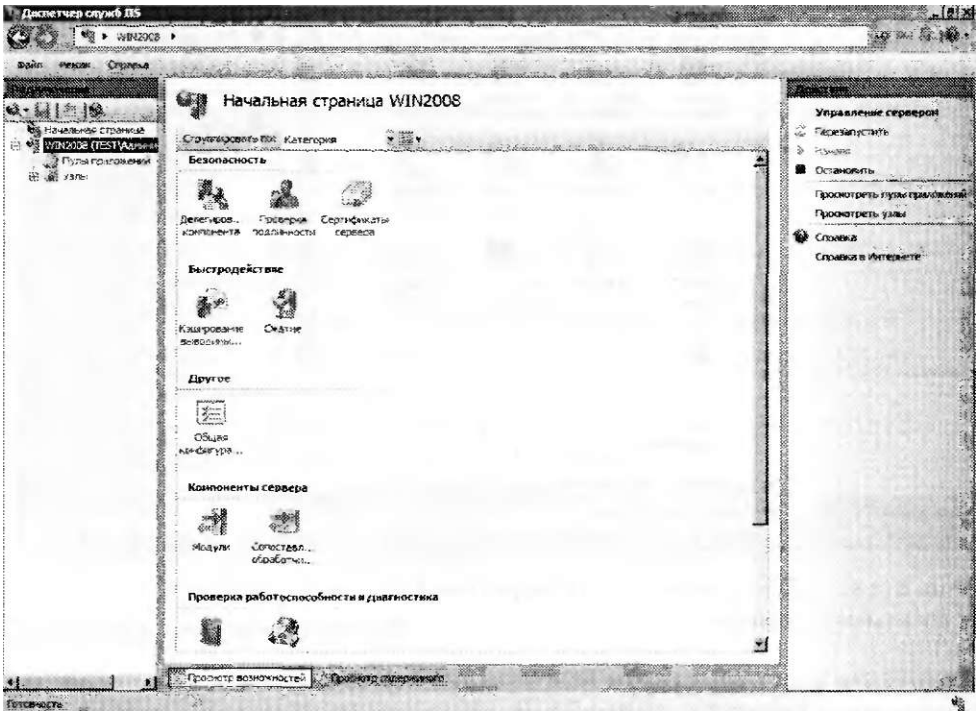


Рис. 5-14. Просмотр элементов конфигурации диспетчера служб IIS, сгруппированных по категории

СОВЕТ Подготовка к экзамену

Изучение множества компонентов и опций платформы IIS может оказаться очень долгим процессом, особенно если вы не знакомы с разработкой и управлением Веб. Тем не менее, как говорится, лучше один раз увидеть, чем сто раз услышать. Эта концепция относится также к опциям и параметрам, которые нужно изучить для сдачи сертификационного экзамена 70-643. По этой причине на данном занятии используется большое количество мгновенных снимков экрана. Мы рекомендуем при подготовке к экзамену открыть и просмотреть различные страницы свойств для множества компонентов и служб ролей. Это поможет вам выбирать оптимальные способы выполнения требований и решения задач как на экзамене, так и в реальных средах.

Просмотр содержимого

Режим Просмотр содержимого (Content View) используется для просмотра файлов и папок веб-сайта. Подробности отображаются в формате обозревателя Windows с возможностью фильтрации и группирования списка файлов, как показано на рис. 5-15.

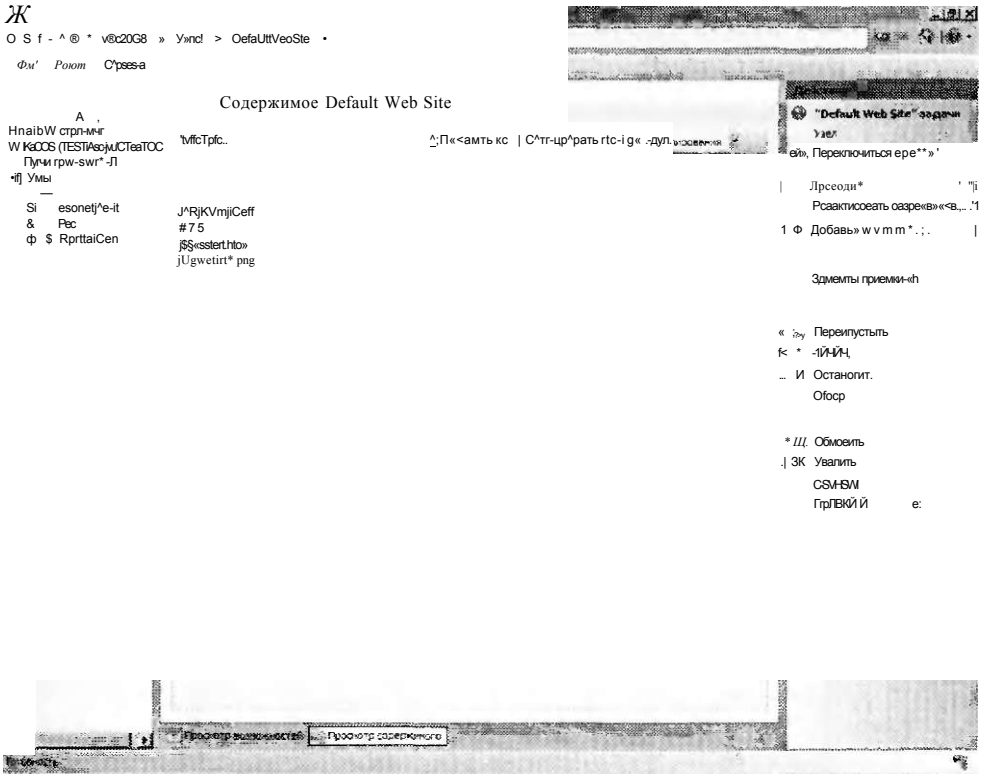


Рис. 5-15. Просмотр содержимого в диспетчере служб IIS

Просмотр содержимого удобно использовать для управления содержимым сайта, а не его параметрами. Этот режим просмотра аналогичен представлению по умолчанию средств управления предыдущих версий IIS.

К СВЕДЕНИЮ Переход с IIS 6.0

Если вы переходите на версию IIS 7.0 с версии IIS 6.0, вся используемая функциональность будет сохранена. Грубо говоря, режим Просмотр возможностей (Features View) заменяет страницы свойств, которые можно было конфигурировать на веб-сервере IIS 6.0. В режиме Просмотр содержимого (Content View) отображается информация о файлах и папках каждого выбранного веб-сайта и каталога — равно как на правой панели в IIS 6.0. Назначение IIS 7.0 — обеспечить организацию обширного набора опций, не создавая головной боли для системных администраторов.

Панель действий

В правой части пользовательского интерфейса утилиты Диспетчер служб IIS (IIS Manager) находится панель Действия (Actions). Отображаемые в ней команды зависят от контекста. Например, при выборе веб-сайта отобразятся действия, которые выполняются для его просмотра, а также остановки, запуска и перезапуска (рис. 5-16). Кроме того, при изменении параметров определенных компонентов в панели действий обычно отображаются ссылки Применить (Accept) и Отмена (Cancel).

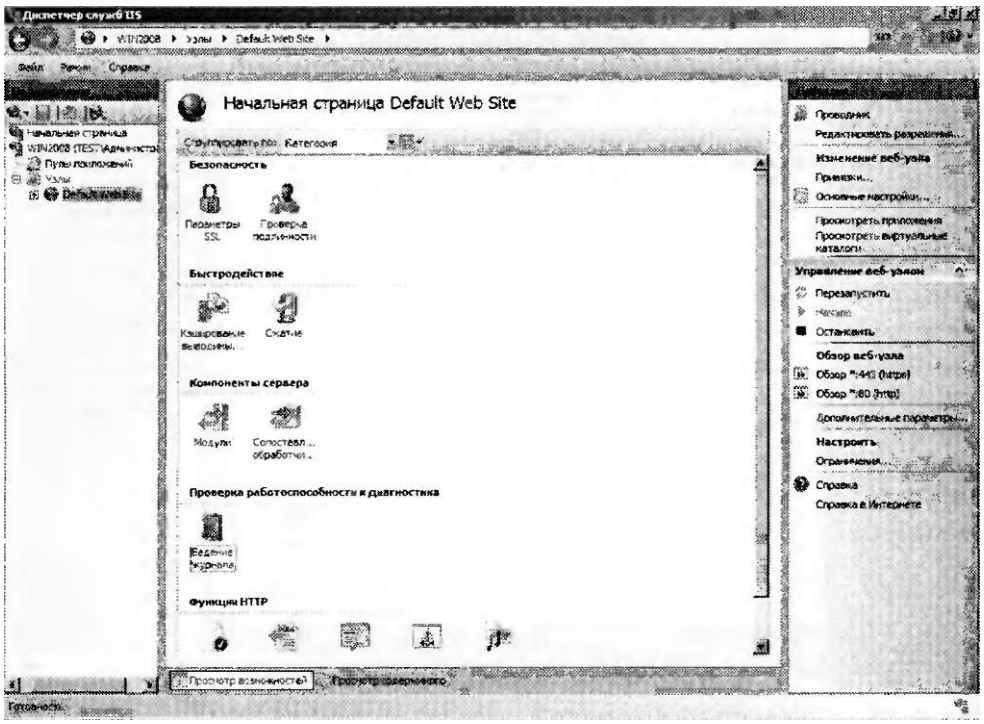


Рис. 5-16. Просмотр команд управления веб-сайтом в панели Действия диспетчера служб IIS

Создание и настройка веб-сайтов

Хотя некоторые веб-серверы могут содержать лишь один веб-сайт, чаще всего на одном сервере IIS размещается множество различных веб-служб и приложений. Перед изучением принципов администрирования IIS важно выяснить, как работают компоненты и объекты веб-сервера.

Сайты и привязка сайтов

Веб-сайты представляют собой контейнеры высшего уровня, обеспечивающие доступ к веб-содержимому. Каждому веб-сайту должен быть сопоставлен физический путь на сервере. Обычно этот путь содержит корневую папку для всего содержимого, которое будет доступно пользователям.

Конфигурация веб-сайта указывает протоколы, порты и другие параметры, которые используются для подключения к веб-серверу. Эта информация называется данными *привязки сайта.* Каждый сайт может располагать множеством связываний на основе требований сервера. В привязке сайта можно указать следующие детали.

- **Тип (Type)** Указывает протокол, который будет использоваться для подключения к веб-серверу. По умолчанию назначаются типы HTTP и HTTPS.

ПРИМЕЧАНИЕ Поддержка других протоколов

Одно из преимуществ WAS состоит в том, что эта структура позволяет IIS 7.0 создавать сайты, использующие другие протоколы помимо HTTP и HTTPS. Однако в этой главе (и на сертификационном экзамене) мы будем работать с двумя самыми распространенными протоколами веб-серверов. При поддержке распределенных приложений, использующих WCF, помните, что сайты IIS могут поддерживать прямые TCP-подключения и другие методы коммуникаций.

- **IP-адрес (IP Address)** Список адресов IPv4 и IPv6, на которые будет реагировать сервер. Если сервер настроен с использованием нескольких IP-адресов, для реагирования на каждый адрес можно отконфигурировать различные веб-сайты. Помимо выбора IP-адресов администраторы могут выбрать опцию Все неназначенные (All Unassigned), чтобы разрешить веб-сайту отвечать на запрос на любом интерфейсе без явного порта и привязки протоколов.
- **Порт (Port)** Указывает TCP-порт, на котором сервер будет выполнять прослушивание. По умолчанию для HTTP-подключений назначается порт 80. Пользователи, которым требуется доступ к веб-сайтам на альтернативных портах, должны указать номер порта в URL. Например, URL-адрес *http:// Serverl.contoso.com:5937*будет пытаться подключиться к веб-серверу Serverl. contoso.com с использованием протокола HTTP на TCP-порте 5937. Для TCP-портов используются номера в диапазоне от 1 до 65535. Обычно многие номера портов до 1024 резервируются для использования распространенными приложениями, однако никаких технических ограничений по их использованию для веб-сайтов не существует.
- **Имя узла (Host Name)** Этот текстовый параметр позволяет множеству веб-сайтов совместно использовать один тип протокола, IP-адрес и номер порта, а пользователям — подключаться к различным веб-сайтам. В этом методе выполняется интерпретация информации заголовка узла в HTTP-запросе. Администраторы сайтов могут настроить свои параметр **DNS,** чтобы разрешить множеству доменных имен указывать один IP-адрес. Данные доменного имени затем используются веб-сервером для определения веб-сайта, к которому пытается подключиться пользователь, а также для генерирования ответа с соответствующего сайта.

Важно не забывать, что комбинация параметров привязки должна быть уникальной для каждого веб-сайта, управляемого IIS. Например, два веб-сайта не могут отвечать с использованием одного протокола, IP-адреса, порта и параметров имени узла. Несмотря на то что вы можете создать множество сайтов

с одинаковыми параметрами привязки, IIS не позволит этим сайтам запускаться одновременно.

Управление веб-сайтом по умолчанию

Изначально роль Веб-сервер (IIS) (Web Server (IIS)) включает сайт по умолчанию Default Web Site. Этот сайт настроен для реагирования па запросы с использованием протоколов HTTP (порт 80) и HTTPS (порт 443). Для просмотра списка привязок в диспетчере служб IIS щелкните правой кнопкой мыши узел Default Web Site и примените команду Изменить привязки (Edit Bindings), чтобы открыть окно, показанное на рис. 5-17. Для открытия этого окна можно также использовать ссылку Привязки (Bindings) в панели Действия (Actions).

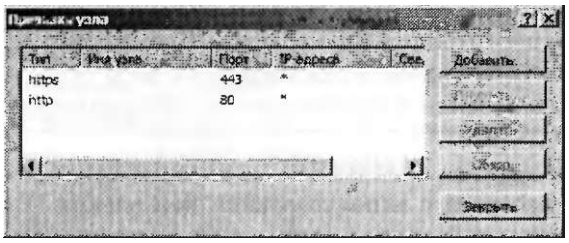


Рис. 5-17. Привязки сайта Default Web Site

При запуске веб-браузера и подключении к URL (например, *http://server2. contoso.com)* IIS получает запрос на HTTP-порт 80 и возвращает содержимое с соответствующего веб-сайта.

Чтобы добавить новую привязку для сайта Default Web Site, в диалоговом окне Привязки узла (Site Binding) щелкните кнопку Добавить (Add). В этом окне можно указать тип протокола, IP-адрес и данные порта, а также опциональное имя узла, как показано на рис. 5-18. Если вы попытаетесь добавить привязку узла, которая уже используется, то получите уведомление с напоминанием о том, что привязки должны быть уникальными.

5 =

3 |'C.1C.0.!Cc

'fSM^VJftfK

Рис. 5-18. Добавление новой привязки узла Default Web Site

Добавление веб-сайтов

Чтобы добавить новый веб-сайт в IIS, в Диспетчере служб IIS (IIS Manager) щелкните правой кнопкой мыши контейнер Узлы (Sites) и примените команду Добавить веб-узел (Add Web Site). На рис. 5-19 показаны доступные опции для создания нового сайта.

Помимо указания привязки протокола по умолчанию для сайта вам потребуется указать имя сайта — логическое имя, которое будет невидимым для пользователей сайта. По умолчанию Диспетчер служб IIS (IIS Manager) создаст новый пул приложений с тем же именем, которое указано для веб-сайта.

Вы также можете выбрать существующий пул приложений, щелкнув кнопку Выбрать (Select). Назначение пулов приложений мы рассмотрим далее на этом занятии.

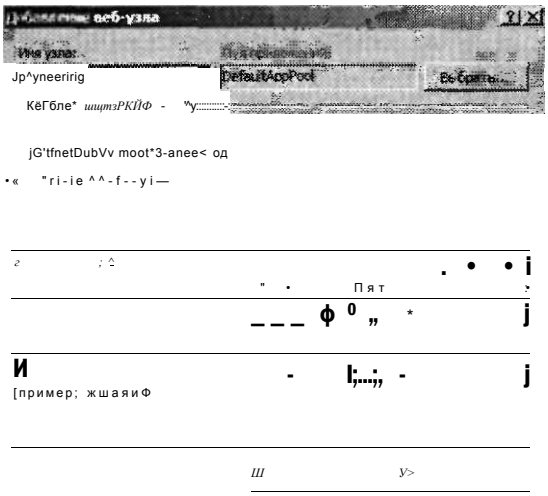


Рис. 5-19. Добавление нового веб-сайта с помощью диспетчера служб IIS

В разделе Каталог содержимого (Content Directory) можно указать полный физический путь к корневой папке веб-сайта. По умолчанию для веб-содержимого IIS назначается корневая папка %SystemDrive%\Inetpub\wwwroot. В этой папке размещаются исходные файлы веб-сайта по умолчанию. Для хранения содержимого нового веб-сайта следует создать новую папку (по этому пути или другому). С помощью кнопки Подкл. как (Connect As) можно указать параметры безопасности, которые будут использоваться IIS для получения доступа к содержимому. По умолчанию задается параметр Сквозная проверка подлинности (Pass-Through Authentication), который означает использование контекста безопасности запрашивающего веб-пользователя. Безопасность содержимого веб-сайтов мы рассмотрим в главе 6.

Последний флажок в окне позволяет указать немедленный запуск сайта после щелчка ОК. При этом, если информация привязки веб-сайта уже используется, вы увидите соответствующее предупреждение (рис. 5-20).

Когда вы щелкнете ОК, новый веб-сайт появится в левой панели диспетчера служб IIS. Веб-сайты можно запускать и останавливать по отдельности, выбирая их и применяя команды панели Действия (Actions). Вы также можете щелкнуть имя сайта правой кнопкой мыши и выбрать команду Управление веб-узлом (Manage Web Site). Остальные параметры, например привязки узлов,

также можно модифицировать в любое время. Таким образом, вы можете создавать, реконфигурировать и останавливать сайты по отдельности, не затрагивая другие сайты на сервере. Помимо основных параметров сайта существуют также параметры конфигурации, которые можно определить на уровне сайта.

ШШ

Привязка "^ЗО;* назначена другому узлу. Тесле назначения уточу узлу той мне привязки будет возможен запуск только одного из веб-узлоб. Добавить привязку вторично'

1 д* ; s

Рис. 5-20. Попытка создать новый веб-сайт путем дублирования информации привязки

Настройка ограничений для веб-сайта

Параметры Ограничения для веб-узла (Web Site Limits) назначают максимальное использование полосы пропускания и максимальное количество подключений, которые MoiyT поддерживаться веб-сайтом. Эти параметры позволяют системным администраторам запретить одному или нескольким сайтам на сервере использовать всю полосу пропускания сети или слишком много ресурсов. Чтобы настроить ограничения для веб-сайта, выберите соответствующий сайт и щелкните команду Ограничения (Limits) в панели Действия (Actions). На рис. 5-21 показаны параметры по умолчанию для нового веб-сайта.

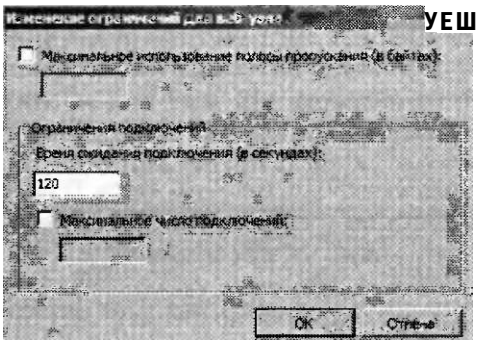


Рис. 5-21. Настройка ограничений использования полосы пропускания и количества пользовательских подключений для веб-сайта

Опция Максимальное использование полосы пропускания (Limit Bandwidth Usage), которая изначально отключена, позволяет ввести максимальное число байтов в секунду, которое будет поддерживать веб-сервер. В случае превышения этого значения веб-сервер дросселирует отклики путем добавления временной задержки.

В разделе Ограничения подключений (Connection Limits) можно указать максимальное количество пользовательских подключений, которое будет под-

держивать сайт. Каждое пользовательское подключение автоматически завершается, если в течение указанного количества секунд не поступил новый запрос. (По умолчанию назначено 120 с, или 2 мин.) Кроме того, вы можете указать максимальное количество подключений для сайта. В случае превышения этого количества пользователи, пытающиеся создать новое подключение, будут получать сообщение об ошибке с информацией о занятости сервера.

Настройка ведения журнала

Еще одним параметром уровня сайта является Ведение журнала (Logging). Чтобы открыть эти свойства, выберите соответствующий веб-сайт и в режиме Просмотр возможностей (Features View) дважды щелкните элемент Ведение журнала (Logging).

На рис. 5-22 показаны опции ведения журнала по умолчанию.

Рис. 5-22. Настройка параметров ведения журнала для веб-сайта

Доступные опции в этом окне зависят от того, какие службы ролей установлены на веб-сервере. По умолчанию каждый новый сайт конфигурируется для хранения текстовых файлов журнала в папке %SystemDrive%\Inetpub\Logs\LogFile на локальном сервере. Каждому веб-сайту будет назначаться собственная папка, и каждая такая папка будет содержать один или несколько файлов журнала. Вы можете выбирать разные форматы файлов журнала, однако по умолчанию назначается формат W3C. Этот стандарт можно использовать для сравнения данных журнала с различных платформ веб-серверов. Щелкнув

кнопку Выбрать поля (Select Fields), вы можете определить, какие данные следует сохранять в журнале. Поля, назначенные по умолчанию, обеспечивают баланс между быстродействием и объемом полезной информации. Добавление полей может повлиять на быстродействие веб-сервера и увеличить размер файлов журнала.

На загруженных веб-серверах файлы журналов быстро приобретают большие размеры. Поскольку файлы журналов создаются в текстовом формате, объемные файлы часто с трудом поддаются анализу. В разделе Переход на новый файл журнала (Log File Rollover) можно указать метод и время создания нового файла журнала. По умолчанию новый файл журнала создается ежедневно. Вы также можете использовать лишь один файл журнала. Хотя анализ файлов журнала теоретически можно выполнять в таком текстовом редакторе, как Блокнот (Notepad), для этого чаще применяются специальные утилиты.

Веб-приложения

Во многих сценариях работы веб-сервера для поддержки одного сайта часто обеспечивается доступ к содержимому различных типов. Веб-приложения создаются в структуре веб-сайтов с целью указания физического пути к набору файлов содержимого. Например, сайт онлайновых новостей может включать два разных веб-приложения: одно для зарегистрированных пользователей и еще одно для незарегистрированных пользователей. Каждое веб-приложение может указывать отдельную физическую папку на компьютере, чтобы сервер IIS мог определить метод обработки запросов. Веб-приложения также могут использовать другие методы обеспечения доступа к одному содержимому (например, к новостям) на обоих сайтах.

Создание веб-приложений

Новые веб-приложения можно без труда создавать с помощью Диспетчера служб IIS (IIS Manager). Щелкните правой кнопкой мыши веб-сайт, в котором хотите создать веб-приложение, а затем примените команду Добавить приложение (Add Application). На рис. 5-23 показаны доступные опции. Первой опцией является псевдоним, который можно использовать для сайта. Это имя, которое пользователи будут вводить в URL для подключения к содержимому. Например, если в веб-сайте по умолчанию создано новое веб-приложение с псевдонимом Engineering, посетители будут использовать такой URL, как *http://serverl.contoso.com/Engineering* для получения доступа к содержимому. Параметры пула приложений мы рассмотрим далее на этом занятии.

Опция Физический путь (Physical Path) позволяет указать панку, в которой можно хранить содержимое для веб-приложения. Обычно папка в файловой системе должна быть уникальной и не должна использоваться совместно с другими веб-приложениями. Как и в случае с процессом создания сайта, вы сможете оставить параметр по умолчанию Сквозная проверка подлинности (Pass-Through Authentication) или щелкнуть кнопку Подкл. как (Connect As), чтобы указать имя пользователя и пароль. Щелкнув кнопку Тест настроек (Test Settings), вы можете проверить работу соединения с текущими параметрами.

В диалоговом окне Проверка соединения (Test Connection), приведенном на рис. 5-24, указано, что в случае применения параметров по умолчанию Диспетчер служб IIS (IIS Manager) не сможет проверить разрешения проверки подлинности. (Проверку подлинности и авторизацию мы рассмотрим в главе 6.) Причина состоит в том, что перед попыткой пользователя получить доступ к содержимому не был определен конкретный пользовательский контекст.

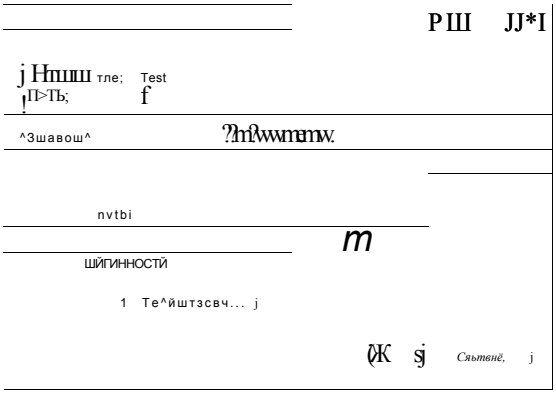


Рис. 5-23. Добавление нового веб-приложения в веб-сайт

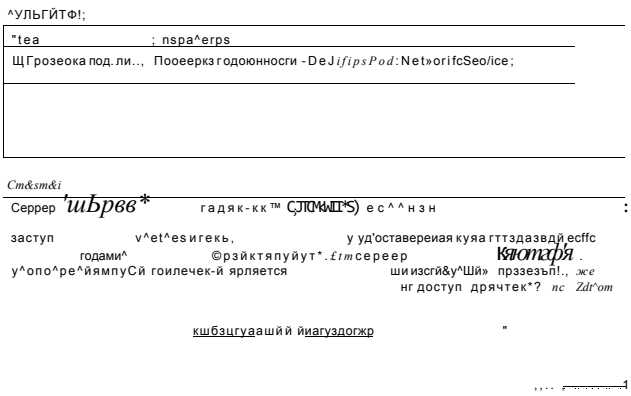


Рис. 5-24. Проверка параметров подключения физического пути при создании нового веб-приложения

Чтобы завершить процесс создания веб-приложения, щелкните ОК. Новое веб-приложение появится в объекте сайта в левой панели диспетчера служб US. Теперь для веб-приложения можно модифицировать и другие параметры с помощью режима Просмотр возможностей (Features View).

Управление параметрами веб-приложений

По умолчанию многие параметры для нового веб-приложения автоматически наследуются от веб-сайта, в котором создается веб-приложение. Таким образом,

вы можете без труда использовать для каждого нового сайта одинаковые параметры по умолчанию. В большинстве случаев вы также можете заменить параметры на уровне веб-приложения в соответствии с требованиями к приложению. Для этого дважды щелкните любой элемент в режиме Просмотр возможностей (Feature View) и внесите соответствующие изменения на уровне веб-приложения. Большинство этих параметров заменят параметры по умолчанию, назначенные для родительского сайта.

Пулы приложений

Изначально при управлении веб-серверами следует позаботиться о потенциальном негативном влиянии работы одного веб-сайта или приложения на другие сайты и приложения.

Такие проблемы, как утечка памяти или дефекты приложений, могут привести к значительному снижению быстродействия или полному отказу многих веб-приложений. Пулы приложений предназначены для изоляции различных сайтов друг от друга вместе с их внутренними ошибками и другими проблемами. Внутри каждого пула приложений рабочие процессы отвечают за выполнение веб-запросов. Каждый пул приложений содержит собственный набор рабочих процессов, так что один пул приложений никак не может влиять на процессы другого. Пулы приложений можно также независимо запускать и останавливать.

По умолчанию IIS включает пулы приложений Classic.NET AppPool и DeafultAppPool, а также пул приложений с именем, как у приложения. Пул Classic. NET AppPool используется для поддержки приложений Microsoft .NET Framework 2.0 с использованием классического (Classic) режима управляемого конвейера (Managed Pipeline Mode) (режим, в котором код .NET может использовать методы перехвата и реагирования на запросы, обрабатываемые в IIS). Пул приложений DefaulAppPool используется для поддержки сайта Default Web Site. Он также поддерживает Microsoft .NET Framework 2.0, однако использует новый встроенный (Integrated) режим управляемого конвейера (Managed Pipeline Mode). Режимы конвейера мы рассмотрим более подробно далее на этом занятии.

По умолчанию Диспетчер служб IIS (IIS Manager) создает для нового вебсайта новый пул приложений. Отметим, что пул приложений получит такое же имя, как и у сайта. Эту методику рекомендуется использовать, поскольку она позволяет процессам в каждом веб-сайте запускаться независимо от других. При создании нового веб-приложения можно выбрать любой доступный пул приложений.

Создание пулов приложений

Диспетчер служб IIS (IIS Manager) включает объект Пулы приложений (Application Pools), который позволяет управлять пулами приложений на веб-сервере. По умолчанию щелчком этого объекта отображаются все существующие пулы приложений на сервере с их текущим состоянием и параметрами, как показано на рис. 5-25.

Чтобы создать новый пул приложений, щелкните правой кнопкой мыши объект Пулы приложений (Application Pools) и примените команду Добавить пул приложений (Add Application Pool). Откроется окно опций, показанное на рис. 5-26. Опция Имя (Name) используется системными администраторами для идентификации назначения пула приложений. Если вы создаете этот объект для поддержки конкретного веб-сайта, включите в имя сведения для идентификации. Выбор опций Версии среды .NET Framework (.NET Framework version) зависит от доступных версий .NET Framework на локальном компьютере. По умолчанию предлагаются варианты Платформа .NET Framework версия 2.0 (.NET Framework 2.0) и Без управляемого кода (No Managed Code). При выборе последнего варианта функциональность .NET не будет доступна для веб-приложений, входящих в этот пул.

Режим управляемого конвейера (Managed Pipeline Mode) определяет метод, который будет поддерживаться для кода перехвата и модификации обработки веб-запросов. Классический режим (Classic) конвейера поддерживает приложения ASP.NET, написанные для предыдущих версий IIS и зависящие от интеграции с событиями конвейера запросов. Встроенный режим (Integrated) обеспечивает более высокий уровень быстродействия и функциональности для приложений ASP.NET. Этот метод рекомендуется использовать для веб-приложений, которые не зависят непосредственно от классического режима конвейера. И наконец, вы можете указать в этом окне немедленный запуск создаваемого пула приложений.

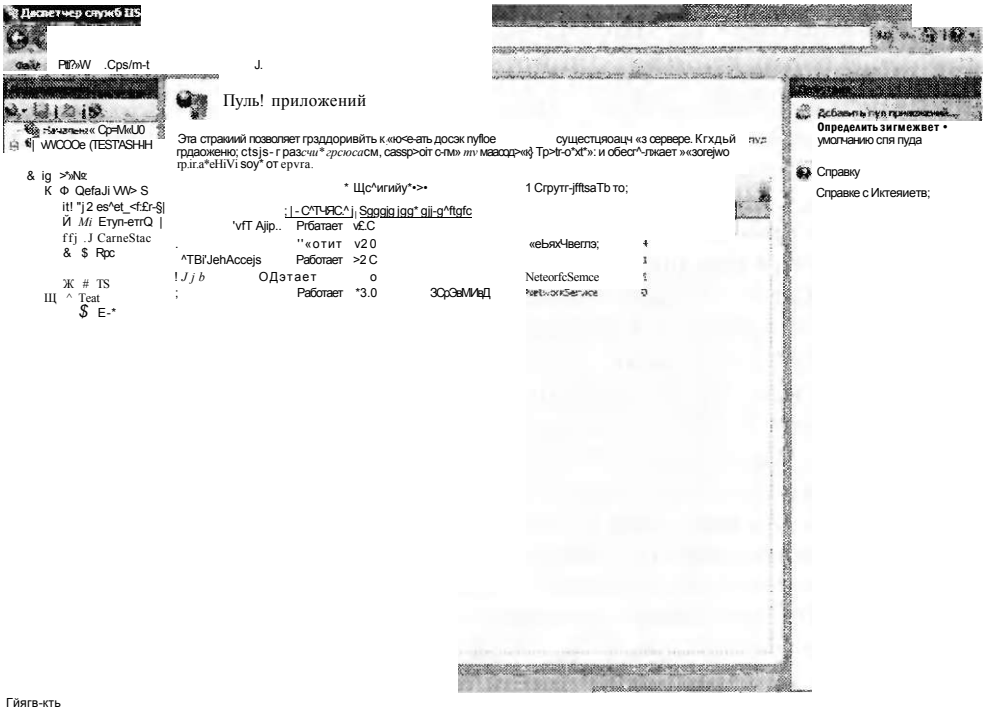


Рис. 5-25. Управление пулами приложений в диспетчере служб IIS

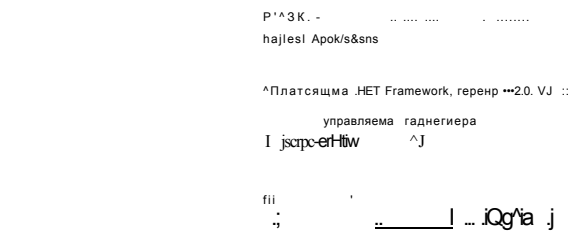


Рис. 5-26. Создание нового пула приложений

Управление пулами приложений

Каждый пул приложений на веб-сервере может запускаться и останавливаться независимо. При остановке пула приложений прекращается обработка запросов всеми приложениями, входящими в данный пул. Пользователи, пытающиеся подключиться к содержимому этих сайтов, будут получать код ошибки HTTP 503 «Служба недоступна» (Service Unavailable). Поэтому перед остановкой пула следует выяснить, какими приложениями он используется. Для этого в Диспетчере служб IIS (IIS Manager) щелкните правой кнопкой мыши пул приложений и примените команду Просмотреть приложения (View Applications).

Настройка параметров перезапуска

Альтернативой остановке пула приложений является его перезапуск с помощью команды Перезапуск (Recycle) в панели Действия (Actions). При выполнении этой команды IIS автоматически сбрасывает текущий рабочий процесс после выполнения им существующих запросов. Преимущество состоит в том, что пользователи не замечают сбоя службы на компьютере — просто рабочий процесс будет быстрее заменен новым. Перезапуск пулов приложений обычно выполняется в случае утечки памяти или значительной нагрузки на ресурсы. Довольно часто реальной причиной такой проблемы является дефект или какая-то неполадка в коде приложения. Идеальное решение состоит в устранении исходной проблемы. Однако с помощью команды Перезапуск (Recycle) вы сможете хотя бы определить признаки ошибки.

В некоторых случаях можно автоматически перезапускать рабочий процесс на основе ограничений использования ресурсов или временных ограничений. Чтобы открыть эти свойства, щелкните команду Перезапуск (Recycle) в разделе Изменить пул приложений (Edit Application Pool) панели Действия (Actions). Откроется окно, показанное на рис. 5-27.

Изначально для изменения параметров перезапуска доступны опции раздела Через фиксированные промежутки времени (Fixed Intervals) или По достижении максимального объема памяти (Memory Based Maximums). Оптимальные опции зависят от того, какие проблемы вы пытаетесь устранить или предотвратить. Слишком частый перезапуск пулов приложений может снизить быстродействие. Тем не менее, если в работе веб-приложения имеются серьезные проблемы, рекомендуется устранять их посредством перезапуска рабочих процессов, чтобы пользователи не замечали зависания или ошибки на веб-сайте.

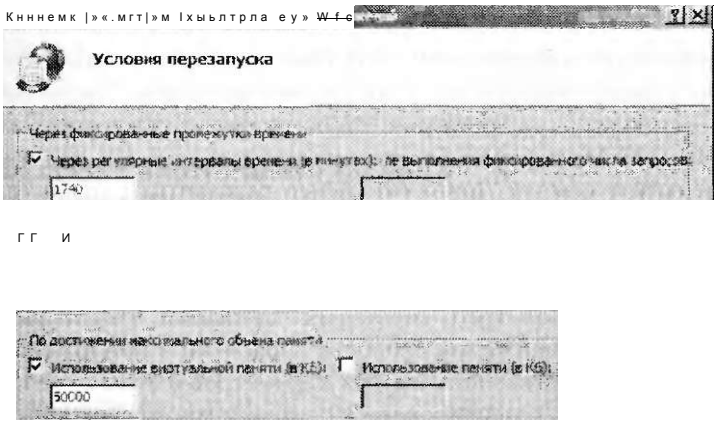


Рис. 5-27. Настройка параметров перезапуска пула приложений

Отслеживание событий пула приложений также играет важную роль в обеспечении стабильной работы веб-ссрвера и его приложений. Например, при назначении ограничений максимального объема памяти следует выяснить, как часто выполняется перезапуск пула приложений. На рис. 5-28 показана открывающаяся на следующем этапе настройки страница Записываемые в журнал события перезапуска (Recycling Events To Log), в которой можно определить записываемые события. Для перехода к этой странице щелкните кнопку Далее (Next) на странице, показанной на рис. 5-27.

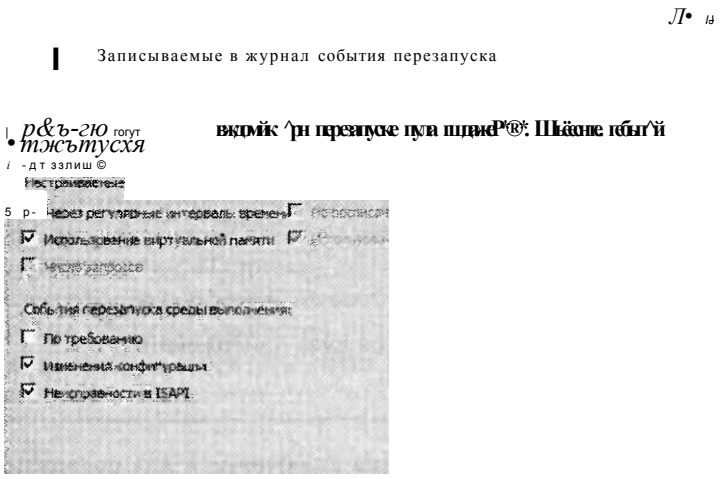


Рис. 5-28. Выбор событий перезапуска для записи в журнал

Настройка дополнительных параметров пула приложений

Помимо основных параметров конфигурации и опций перезапуска для пула приложений системные администраторы могут настроить дополнительные параметры контроля поведения рабочих процессов. Чтобы открыть эти параметры, в Диспетчере служб IIS (IIS Manager) выберите пул приложений и в панели Действия (Actions) щелкните ссылку Дополнительные параметры (Advanced Settings). Откроется окно, показанное на рис. 5-29.

Опции в этом окне позволяют указать детальные параметры использования ресурсов процессора и памяти. В принципе вам не следует изменять эти параметры вручную, если у вас нет для этого серьезных оснований. Некоторые модификации могут сказаться на снижении скорости обработки в приложениях, входящих в данный пул. При изменении других параметров в этом окне на отдельный пул приложений может резервироваться слишком много системных ресурсов.

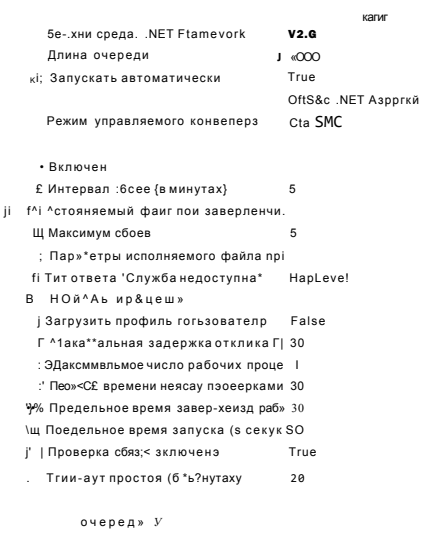


Рис. 5-29. Настройка дополнительных параметров пула приложений

Виртуальные каталоги

Общим требованием для всех веб-сайтов является включение в них содержимого из папок, размещенных вне исходной структуры папок веб-сайта. Например, множеству веб-сайтов, совместно использующих один набор изображений, может потребоваться доступ к указателю на отдельный путь, через который все веб-сайты смогут получать доступ к файлам. Для обеспечения этой возможное-

ти используются виртуальные каталоги, которые можно создавать на уровне веб-сайта или в конкретном веб-приложении. Виртуальные каталоги включают псевдоним (который используется в URL запроса) и указывают путь к физическому размещению в файловой системе.

Создание виртуального каталога

Процесс создания виртуального каталога аналогичен созданию веб-приложения. В Диспетчере служб IIS (IIS Manager) щелкните правой кнопкой соответствующий родительский веб-сайт или веб-приложение и примените команду Добавить виртуальный каталог (Add Virtual Directory). Для виртуального каталога можно указать псевдоним (например, Изображения), а также параметры проверки подлинности и физический путь к виртуальному каталогу. Когда на этот псевдоним приходит запрос, IIS автоматически выполняет поиск размещения запрашиваемого содержимого в файловой системе.

Сравнение виртуальных каталогов и веб-приложений

Хотя параметры виртуального каталога аналогичны параметрам веб-приложения, принципы их использования отличаются. Веб-приложения, как правило, предназначены для поддержки исполняемого кода Веб (например, приложения, написанные с помощью ASP.NET). Они запускаются в изолированном пространстве процессов с использованием архитектуры WAS. Стабильность WAS также позволяет веб-приложениям отвечать на запросы с помощью других протоколов помимо HTTP и HTTPS (если, конечно, эти протоколы установлены и настроены на локальном сервере). Виртуальные же каталоги изначально используются для указания статического содержимого, которое хранится в альтернативных размещениях файловой системы.

Веб-приложения и виртуальные каталоги формируют полный URL, который используется для получения доступа к веб-сайту. Их можно также сделать вложенными с целью обеспечения доступа к содержимому на множестве уровней веб-сайта. Выбор параметров зависит от требований к веб-приложению, которое вы планируете поддерживать.

ВАЖНО! Стремление к простоте в конфигурации

Функциональность и гибкость, которая обеспечивается веб-приложениями и виртуальными каталогами, важна как для администраторов веб-серверов, так и для веб-разработчиков. Следует стремиться к максимально простой и интуитивной конфигурации. Например, хотя оба типа объектов можно вложить друг в друга, сложная структура вложенных элементов может запутать, особенно если некоторые объекты совместно используют одни имена. Таким образом, создавая и проектируя структуру сайта, следует не забывать о четком управлении всеми его элементами.

Управление из командной строки

В целом выполнять административные задачи на нескольких серверах IIS с помощью консоли Диспетчер служб IIS (IIS Manager) относительно просто. Тем не менее для внесения одинаковых изменений на множестве различных серверов

или для автоматизации процесса настройки целесообразнее использовать сценарии и утилиты командной строки. В IIS включена исполняемая команда *AppCmd.exe,* обеспечивающая простой способ выполнения распространенных операционных задач. Ее реальные параметры сопоставляются со структурой веб-сайтов, веб-приложений и виртуальных каталогов IIS.

Файл AppCmd.exe содержится в папке %SystemRoot%\System32\inetsrv. Для получения данных справки запустите команду *appcmd*/? (рис. 5-30). Этот же переключатель можно использовать для получения дополнительных сведений о других командах. Далее приведен общий синтаксис этой команды:

Appcmd.exe *Команда Объект "Имя_объекта" /параметр:значение*

Рис. 5-30. Данные справки утилиты AppCmd.exe

Командные опции

Для выполнения задач с объектами с помощью утилиты AppCmd.exe используется простой набор из следующих команд.

- List Возвращает информацию об указанном объекте.
- **Add** Создает новый объект с указанным типом. Дополнительные детали можно добавлять с помощью параметров и значений.

- **Delete** Удаляет указанный объект (например, веб-сайт или веб-прнложение).
- **Set** Изменяет параметры объекта в соответствии с указанными параметрами и значениями.
- **Start/Stop** Доступна для объектов, которые поддерживают эти действия (таких как веб-сайт).

При выполнении каждой операции (из файла сценария или командной строки) в строку всегда нужно добавлять *AppCmd.exe.*

Объекты

В стандартной инструкции AppCmd вам может потребоваться указать тип и имя объекта, над которым выполняется операция. Далее приведен список типов объектов, поддерживаемых утилитой AppCmd.exe:

- App (веб-приложение);
- AppPoll (пул приложений);
- Backup (архивы конфигурации сервера);
- Config (сведения конфигурации сервера);
- Module;
- Request;
- Site (веб-сайт);
- Trace;
- VDir (виртуальный каталог);
- WP (рабочий процесс).

Чтобы получить подробные сведения о параметрах и значениях, применяемых к объекту, после команды добавьте -?.

```
Appcmd site -?
```

Примеры команды

С помощью утилиты AppCmd.exe можно без труда перечислять и создавать параметры конфигурации IIS. В табл. 5-2 приведены некоторые распространенные команды и указано их назначение.

Табл. 5-2. Примеры команд утилиты AppCmd.exe

Команда	Назначение
AppCmd list site	Возвращает список веб-сайтов на локальном сервере
AppCmd add site./name:TestSite01	Добавляет новый веб-сайт TestSiteOl
AppCmd add vdir /app.name:"Default Web Site/" /path:/Images/physical Path:"C:\Inetpub\ wwwroot\images"	Добавляет новый виртуальный каталог с псевдонимом Images и указывает заданный физический путь в файловой системе
AppCmd list request	Возвращает список текущих запущенных запросов веб-сервера
AppCmd list config	Возвращает все сведения о текущей конфигурации веб-сервера в формате XML

СОВЕТ Подготовка к экзамену

При подготовке к сертификационному экзамену 70-643 вам не обязательно запоминать все опции и параметры командной строки для таких утилит, как AppCmd.exe. Вам нужно знать лишь базовый синтаксис и типы выполняемых операций. Нет лучшего способа ознакомиться с командами, чем реальное выполнение таких действий, как создание сайтов и изменение параметров конфигурации. Таким образом вы сможете идентифицировать варианты выбора ответов при сдаче экзамена.

Windows PowerShell

Помимо утилиты AppCmd.exe администраторы веб-серверов могут использовать командную оболочку и язык сценариев Microsoft Windows PowerShell. Оболочка Windows PowerShell включена в Windows Server 2008 в виде компонента, который по умолчанию отключен. Чтобы включить Windows PowerShell, откройте Диспетчер сервера (Server Manager), щелкните правой кнопкой мыши узел Компоненты (Features) в левой панели и примените команду Добавить компоненты (Add Feature). Выберите компонент Windows PowerShell и щелкните кнопку Далее (Next), чтобы установить его. После установки компонент можно запустить из группы программ Windows PowerShell 1.0 в меню Пуск (Start). Оболочка Windows PowerShell позволяет создавать мощные сценарии для выполнения многих распространенных административных операций.

К СВЕДЕНИЮ Windows PowerShell

Хотя в данной книге нет полного описания принципов использования PowerShell и темы сертификационного экзамена 70-643, вы можете найти сведения об использовании PowerShell для управления IIS, выполнив поиск Powershell на сайте *http://www.iis.net*. На странице *http://www.microsoft.com/technet/scriptcenter/hubs/msh.mspx* веб-сайта Windows PowerShell приведены примеры создания новых сценариев от Microsoft TechNet Scripting.

Выполнение автоматизации с использованием .NET Framework

Многие веб-разработчики хорошо знакомы с принципами работы .NET Framework. Поэтому им удобно управлять IIS с помощью стандартного кода .NET. В IIS 7.0 предоставлены два именных пространства .NET, которые можно использовать для программного управления параметрами конфигурации IIS.

- **Microsoft.Web.Administration** Это именное пространство обеспечивает объекты и методы, которые удобно использовать для управления параметрами веб-сайта и для их изменения. Оно изначально спроектировано для внесения изменений в конфигурацию веб-сервера IIS.
- **Microsoft.Web.Management** Хотя пользовательский интерфейс Диспетчер служб IIS (IIS Manager) обеспечивает простой доступ к наиболее часто используемым функциям, для выполнения специфических задач в некоторых

средах может потребоваться создать собственные оснастки расширения. Именное пространство Microsoft.Web.Management включает объекты и методы, позволяющие разработчикам расширять функциональность пользовательского интерфейса средств управления IIS. Эти дополнения затем можно настроить для запуска в автономной среде или интегрировать со встроенной утилитой Диспетчер служб IIS (IIS Manager) для быстрого доступа.

Разработка приложений с использованием .NET Framework не входит в темы сертификационного экзамена 70-643, однако следует знать, что эти возможности доступны для автоматизации задач настройки и управления. Дополнительную информацию об этих и других именных пространствах можно найти по адресу *http://msdn2.microsoft.com/en-us/library/aa388745.aspx.*

Управление файлами конфигурации веб-сервера

Настройку параметров конфигурации на одном или нескольких серверах проще всего выполнять с помощью графических инструментов. Однако администраторам часто требуется настраивать множество веб-серверов. Помимо Диспетчера служб IIS (IIS Manager) и связанных с ним инструментов для настройки параметров веб-сервера можно также использовать файлы конфигурации XML. Кроме того, сохраняя параметры в отдельном файле, вы можете без труда архивировать и восстанавливать параметры в других экземплярах установки IIS. На этом занятии мы рассмотрим файлы хранения параметров конфигурации веб-сервера и веб-сайта.

Файл ApplicationHost.config

Все параметры конфигурации, определяемые для локального веб-сервера IIS, хранятся в текстовом XML-файле ApplicationHost.config. По умолчанию этот файл расположен в папке %SystemDrive%\Inetpub\History. В нее входит набор подпапок, каждая из которых содержит копию файла ApplicationHost.config. Служба поддержки узла приложений (Application Host Helper Service), которая включается по умолчанию при установке роли Веб-сервер (IIS) (Web Server (IIS)), автоматически создает периодические резервные копии параметров конфигурации локального веб-сервера. В этом процессе автоматически создается новая папка и копия файла ApplicationHost.config. В подпапке содержится файл, который используется для описания и интерпретации параметров в файлах конфигурации.

Файл ApplicationHost.config можно открывать и модифицировать с помощью стандартного текстового редактора (такого как Блокнот Windows (Windows Notepad)) или приложения, предназначенного для работы с XML-файлами (например, Visual Studio).

Содержимое организовано в иерархии с различными параметрами и опциями, которые можно конфигурировать в IIS, как показано на рис. 5-31. Перед внесением изменений непосредственно в файл конфигурации не забудьте создать его резервную копию, поскольку изменения могут привести к возникновению ошибок в IIS.

Рис. 5-31. Просмотр файла ApplicationHost.config в Internet Explorer

Восстановление файла AppllicationHost.config

Для возврата конфигурации IIS в предыдущее состояние с помощью автоматически создаваемых архивных файлов ранний файл конфигурации можно вручную скопировать на место рабочего файла. Активная версия файла ApplicationHost.config представлена в папке %SystemRoot%\System32\Inetsrv\Config. Для выполнения отката конфигурации IIS найдите версию файла ApplicationHost.config, которую вы хотите использовать, и скопируйте ее поверх текущего файла. Имейте в виду, что для применения изменений может потребоваться перезапустить веб-сервер и Диспетчер служб IIS (IIS Manager). Кроме того, настоятельно рекомендуется скопировать текущий файл конфигурации в архив на случай, если он понадобится в будущем.

Файлы Web.config

Одной из распространенных проблем, связанных с управлением веб-приложениями и веб-сайтами, является сохранение параметров при перемещении сайтов между серверами. В предыдущих версиях IIS часто приходилось вручную воссоздавать параметры для корректной работы сайта.

В версии IIS 7.0 используется иерархический подход к созданию параметров конфигурации и к управлению ими. Помимо параметров уровня сервера, определяемых в файле ApplicationHost.config, системные администраторы и веб-разработчики могут включать и другие параметры в файлы Web.config.

Файлы Web.config можно размещать в корневой папке веб-сайта или веб-приложения. Эти файлы могут содержать параметры, заменяющие параметры по умолчанию уровня сервера, включенные в файл ApplicationHost.config. Форматы файлов и опций аналогичны. По умолчанию новый файл Web.config создается автоматически при добавлении нового веб-сайта или веб-приложения. Параметры по умолчанию наследуются от параметров уровня сервера, если вы не измените их сами. Ниже приведена иерархия файлов конфигурации.

1. Хост (ApplicationHost.config).
2. Сайт (Web.config).
3. Приложение (Web.config).

Параметры в файлах на более низких уровнях иерархии могут заменять параметры, определенные на родительских уровнях. Преимущество такого подхода состоит в том, что данные конфигурации включаются автоматически при копировании всей папки веб-содержимого еще на один сервер или в другое размещение на том же сервере.

СОВЕТ Подготовка к экзамену

При внесении изменений в конфигурацию IIS и веб-приложений следует знать, на какие элементы структуры сайта должны повлиять эти изменения. Если цель состоит в модификации всех веб-сайтов, вносите изменения в файл ApplicationHost.config уровня сервера. В противном случае изменения лучше вносить на уровне сайта или приложения.

Миграция веб-сайтов и веб-приложений

Наличие файлов Web.config в папках веб-приложений и веб-сайтов значительно упрощает процесс миграции веб-сайтов на различные серверы или в другие физические размещения. Для большинства приложений требуется лишь, чтобы в новое место были скопированы или перемещены все файлы в соответствующих папках.

Затем в Диспетчере служб IIS (IIS Manager) можно воссоздать все дополнительные веб-сайты, веб-приложения и виртуальные каталоги. Тем не менее следует тщательно протестировать мигрированное веб-приложение. В некоторых случаях несовместимость параметров на уровне сервера и на уровне приложения или другие проблемы могут привести к непредвиденным последствиям. Однако в целом процесс перемещения и копирования веб-сайтов выполняется просто и без труда.

Архивация и восстановление данных конфигурации с помощью утилиты AppCmd.exe

Важным аспектом администрирования веб-сервера является обеспечение защиты конфигурации сервера от потери данных. Поскольку параметры конфигурации IIS автоматически сохраняются в папке %SystemDrive%\Inetpub\History, эта папка должна быть включена в политику архивации файловой системы. Кроме того, важно архивировать веб-сайты и веб-приложения для быстрого

восстановления в случае сбоя. Однако вам придется довольно часто вручную создавать архивы параметров конфигурации. Например, если вам нужно перенести данные конфигурации в другой экземпляр установки IIS или обеспечить защиту от нежелательных изменений, вы можете создать резервные копии параметров конфигурации по требованию.

Утилиту AppCmd.exe можно использовать для создания архивной копии параметров конфигурации IIS и ее сохранения в текстовом файле. Эта утилита обеспечивает простые возможности для создания и восстановления резервной копии. Далее приведен синтаксис стандартной команды добавления новой архивной копии.

```
AppCmd add backup "Имя_файла"
```

Если вы не укажите имя для создаваемого архива, будет сгенерировано имя файла с временной меткой. Файл будет создан в той же папке, откуда запускается утилита AppCmd, однако его легко переместить или скопировать в другое место.

Восстановление данных конфигурации из резервной копии выполняется с помощью следующей команды:

```
AppCmd restore backup "Имя_файла"
```

Этот процесс восстановит конфигурация веб-сервера IIS в соответствии с параметрами, включенными в файл резервной копии.

Для просмотра списка резервных копий можно использовать следующую команду:

```
AppCmd list backups
```

Вы увидите список всех созданных файлов резервных копий. Работа всех этих команд архивации и восстановления показана на рис. 5-32.

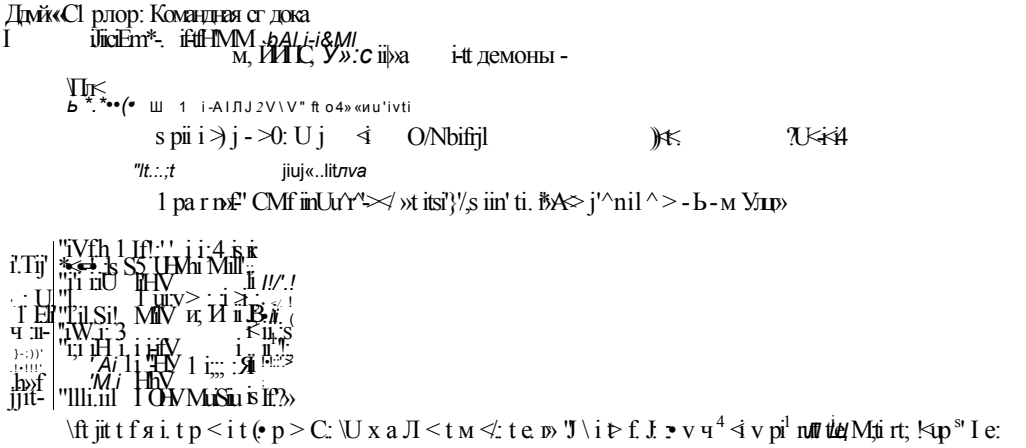


Рис. 5-32. Архивация и восстановление параметров конфигурации IIS с помощью утилиты AppCmd.exe

Использование централизованной конфигурации для ферм серверов

В процессе размещения организациями веб-сайтов и веб-приложений важную роль играет возможность повышения быстродействия, расширяемости и надежности. Для веб-группы серверов часто используется конфигурация *фермы веб-серверов* (Web server farm). В этой конфигурации многие веб-серверы настроены для обеспечения доступа к одному содержимому. Как правило, эти веб-серверы располагают одинаковыми параметрами конфигурации и либо хранят локальные копии веб-сайтов и приложений, либо получают к ним доступ из общего ресурса.

Для системных администраторов управление большими группами веб-серверов может оказаться довольно хлопотным делом. При необходимости внести в конфигурацию изменения приходится вручную назначать их на множестве компьютеров. Даже при автоматизации и использовании сценариев можно управлять лишь несколькими серверами.

Для поддержки сценария серверной фермы в IIS 7.0 множество веб-серверов может совместно использовать данные конфигурации, которые хранятся в централизованном общем ресурсе.

Первый этап процесса создания совместно используемой конфигурации состоит в экспорте параметров конфигурации на отдельный сервер IIS. В принципе вы будете конфигурировать этот сервер с использованием всех параметров, которые требуется применять на других серверах. Затем в Диспетчере служб IIS (IIS Manager) щелкните имя сервера и в режиме Просмотр возможностей (Features View) дважды щелкните элемент Общая конфигурация (Shared Configuration). Для экспорта параметров конфигурации в панели Действия (Actions) щелкните команду Выполняется экспорт конфигурации (Export Configuration), чтобы открыть окно, показанное на рис. 5-33. Вы можете указать путь сохранения файлов конфигурации. Чтобы обеспечить защиту уязвимой информации в файлах конфигурации, вы должны ввести и подтвердить пароль ключей шифрования. Этот пароль потребуется вводить для просмотра параметров конфигурации в файле. Если вы планируете хранить файлы конфигурации в сети, можете также использовать опцию Подключить как (Connect As) и указать учетные данные.

Второй этап процесса — размещение совместно используемого файла конфигурации в таком месте, которое будет доступно для всех веб-серверов. Обычно лучше всего использовать общую сетевую папку на надежном сервере. Выяснив путь к файлам, вы можете использовать опции компонента Общая конфигурация (Shared Configuration). Вначале установите флажок Включить общую конфигурацию (Enable Shared Configuration), как показано на рис. 5-34.

После этого вы сможете указать параметр Физический путь (Physical Path). Вы можете использовать локальное размещение файловой системы или сетевой UNC-путь (например, \\Server1\WebConfig). В поля Имя пользователя (User Name) и Пароль (Password) можно ввести учетные данные безопасности, которые будут использоваться IIS для подключения к указанному ранее физическому пути.

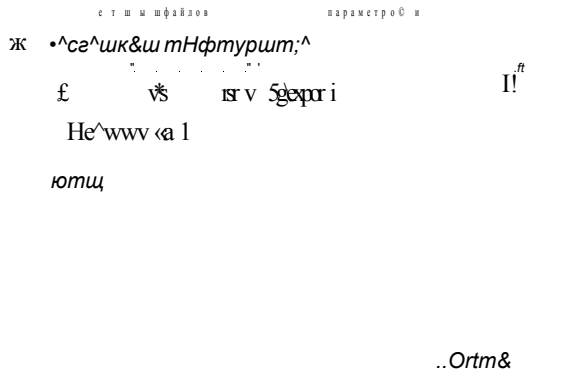


Рис. 5-33. Экспорт данных конфигурации IIS

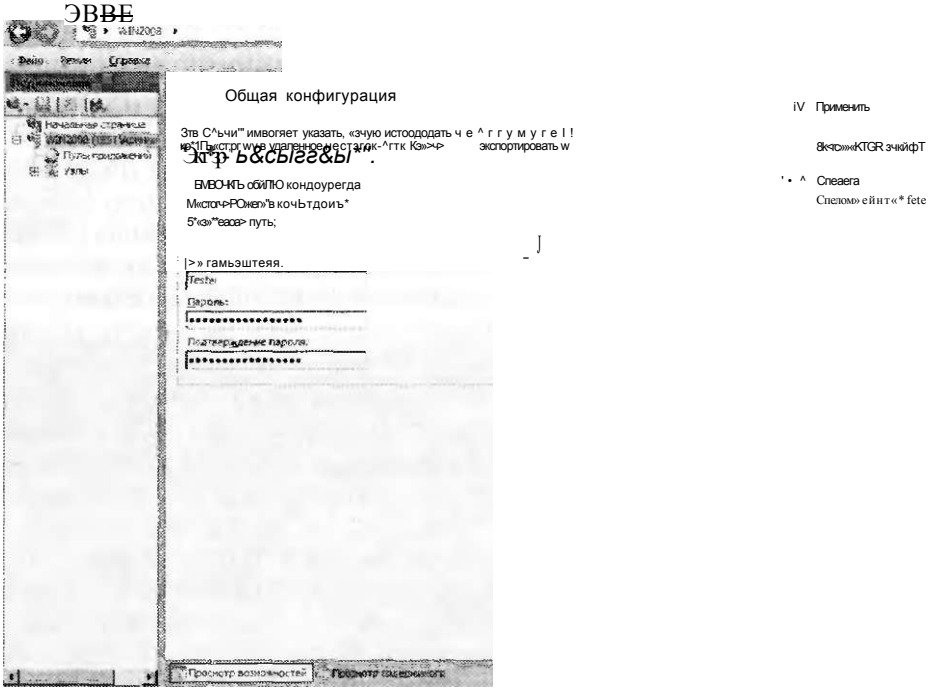


Рис. 5-34. Включение общей конфигурации для веб-сервера IIS

Для сохранения параметров в напели Действия (Actions) щелкните команду Применить (Apply). Вам будет предложено ввести пароль ключей шифрования для файлов конфигурации. После импорта данных конфигурации потребуется перезагрузить Диспетчер служб IIS (IIS Manager) с целью применения изменений конфигурации. Позже вы можете отключить параметры общей конфигура-

ции, сбросив флажок Включить общую конфигурацию (Enable Shared Configuration). Тогда веб-сервер снова станет использовать локально определенные параметры конфигурации.

СОВЕТ Создание корпоративных ферм серверов
Возможность совместного использования параметров множеством веб-серверов удобно применять для установки ферм веб-серверов IIS. Однако общие данные конфигурации являются лишь частью общей конфигурации фермы веб-серверов. Помимо всего прочего требуется развернуть и синхронизировать обновление содержимого, управление состоянием сеансов, управление безопасностью, реализацию балансировки нагрузки и реагирование на события обработки отказов. Для решения этих задач существует много отличных методов. Тем не менее к участию в процессе проектирования стратегии горизонтального масштабирования всегда нужно привлекать веб-разработчиков и системных администраторов.

Миграция с версии IIS 6.0

Многие веб-разратботчики используют предыдущие версии IIS для поддержки своих веб-приложений и веб-сайтов. Версия IIS 6.0, включенная в Windows Server 2003, обеспечивала более совершенные возможности по сравнению с предыдущими версиями. В версии IIS 7.0 значительно расширена функциональность, повышены быстродействие и надежность, улучшены возможности управления. При использовании новых возможностей важной задачей остается обеспечение обратной совместимости с существующими приложениями, разработанными для IIS 6.0.

Для веб-сайтов и веб-приложений, которые изначально используют статическое содержимое, процесс миграции на IIS 7.0 не составляет проблемы. Требуется лишь переместить содержимое и воссоздать все связанные параметры уровня сайта или приложения. Однако следует учитывать дополнительные опции и обратить внимание на нюансы для других типов приложений, например таких как ASP.NET, использующих архитектурные компоненты IIS 6.0. В этом разделе мы рассмотрим миграцию веб-приложений на платформу IIS 7.0.

Обновление Windows Server 2003 и IIS 6.0

Один из способов перемещения веб-приложений на Windows Server 2008 состоит в обновлении компьютера Windows Server 2003. В процессе обновления Windows Server 2003 до Windows Server 2008 автоматически вносятся изменения, обеспечивающие совместимость со старыми приложениями. Например, в обновление включается большинство служб ролей, опционально добавленных в стандартную установку роли Веб-сервер (IIS) (Web Server (IIS)). Более того, в новой версии можно использовать средства и компоненты управления IIS 6.0. Выполняя обновление до Windows Server 2008 и IIS 7.0, проверьте, какие из установленных компонентов можно удалить и какие нужно удалить. Обязательно, как и при любой миграции, тщательно протестируйте функциональность своих веб-сайтов перед повторным развертыванием.

Еще один способ обновления до IIS 7.0 состоит в выполнении миграции веб-сайтов вручную, путем копирования содержимого в новую установку Windows Server 2008.

В этой методике существующее содержимое переносится на новый сервер, а веб-сайты и веб-приложения требуется конфигурировать заново.

Совместимость средств управления IIS 6

Некоторые веб-сайты и веб-приложения могут включать код приложения, который использует архитектуру IIS 6.0 для управления запросами. В качестве примеров приведем веб-приложения, для которых требуется обеспечить доступ к базе данных конфигурации IIS 6.0 и совместимость со старыми методами сценариев. Кроме того, некоторым приложениям может требоваться доступ к предыдущим версиям консоли управления.

По умолчанию компоненты, обеспечивающие обратную совместимость, в Windows Server 2008 автоматически не устанавливаются. Чтобы обеспечить обратную совместимость, с помощью Диспетчера сервера (Server Manager) нужно добавить службы ролей для роли Веб-сервер (IIS) (Web Server (IIS)). При этом доступны следующие опции.

- **Совместимость управления IIS 6 (IIS 6 Management Compatibility)** Этот компонент обеспечивает поддержку двух компонентов сценариев и администрирования IIS 6.0: базовый объект Admin (Admin Base Object (ABO)) и интерфейс Active Directory Services Interface (ADSI). Веб-приложениям, которые используют эти технологии, данные компоненты потребуются для корректной работы. Кроме того, для включения других опций совместимости IIS 6.0 требуется служба ролей Совместимость управления IIS 6 (IIS 6 Management Compatibility).
- **Совместимость метабазы IIS 6 (IIS 6 Metabase Compatibility)** В IIS 6.0 использовалась база данных конфигурации (так называемая метабаза) для хранения параметров сервера и другой информации. В IIS 7.0 эта метабаза заменена новыми типами файлов конфигурации в формате XML, как например файлы ApplicationHost.config и Web.config. Веб-приложения IIS 6.0 могли запрашивать метабазу для управления параметрами IIS. Для поддержки этих приложений требуется включить службу роли Совместимость метабазы IIS 6.
- **Совместимость WMI в IIS 6 (IIS 6 WMI Compatibility)** Инструментарий управления WMI (Windows Management Instrumentation) представляет собой программный интерфейс, позволяющий коду приложения запрашивать параметры IIS и управлять ими с помощью сценариев или инструментов WMI. Эта служба ролей обеспечивает совместимость, позволяющую применять на веб-серверах IIS 7.0 команды IIS 6.0, использующие WMI.
- **Службы сценариев IIS 6 (IIS 6 Scripting Tools)** Включив эту службу ролей, веб-разработчики и системные администраторы могут переносить сценарии IIS 6.0 на платформу IIS 7.0. Службы сценариев IIS 6 обеспечивают поддержку объектов ADO (ActiveX Data Objects) и интерфейса ADSI.

- **Консоль управления IIS 6 (IIS 6 Management Console)** Системные администраторы, которые хотят удаленно управлять инсталляциями IIS 6.0, могут установить на Windows Server 2008 консоль управления IIS 6. Эта консоль обеспечивает лишь подключение к серверам IIS 6.0 и не может подключаться к веб-серверу Windows Server 2008.

В общем эти средства и компоненты помогут обеспечить поддержку функциональности предыдущих версий приложений IIS 6.0 в Windows Server 2008.

Режимы интеграции ASP.NET

В IIS 7.0 улучшены возможности платформы разработок ASP.NET. В предыдущих версиях IIS обработка ASP.NET выполнялась через модуль кода IS API. Хотя эта методика прекрасно работает, существуют некоторые серьезные ограничения. В IIS 7.0 интеграция ASP.NET улучшена путем более плотного внедрения обработки веб-страниц ASP.NET в конвейер запросов веб-сервера. Эта новая архитектура обеспечивает несколько преимуществ, включая более строгий контроль обработки запросов и возможность использования компонентов ASP.NET для типов содержимого, не относящегося к динамическим веб-страницам.

Все приложения ASP.NET могут использовать преимущества нового режима конвейера с интеграцией .NET (.NET Integrated Mode) в IIS 7.0. Однако приложениям, использующим архитектуру IIS 6.0 для перехвата и модификации запросов, потребуется поддержка классического режима конвейера. Режим обработки можно настроить путем изменения параметров или конфигурации пула приложений.

Проверьте себя

1. Как избежать возникновения проблем, связанных с производительностью или использованием ресурсов множества веб-сайтов, которые запущены на одном веб-сервере IIS?
2. Как создать резервную копию данных конфигурации веб-сервера IIS перед ее изменением?

Ответы

1. Каждый веб-сайт нужно настроить для запуска в отдельном пуле приложений. Таким образом вы сможете свести к минимуму вероятность возникновения конфликтов приложений.
2. Утилита AppCmd.exe обеспечивает команды для создания и восстановления резервных копий параметров конфигурации IIS.

Практикум. Настройка параметров IIS и управление ими

В предложенных далее упражнениях вы создадите веб-сайты и веб-приложения на сервере Server2.contoso.com и протестируете процессы архивации и восстановления параметров конфигурации. Предполагается, что вы уже установили на компьютер роль Веб-сервер (IIS) (Web Server (IIS)) со службами ролей

по умолчанию. (Более подробная информация о добавлении роли представлена в упражнении 1 занятия 1.) Для выполнения упражнения 2 требуется закончить упражнение 1, поскольку создаваемый веб-сайт будет использоваться для тестирования процессов архивации и восстановления.

Упражнение 1. Создание веб-сайтов и веб-приложений

В этом упражнении вы используете Диспетчер служб IIS (IIS Manager) для создания нового веб-сайта на локальном сервере. Поскольку веб-сайт по умолчанию (Default Web Site) уже отконфигурирован для использования стандартных портов HTTP и HTTPS, вы укажете альтернативные данные привязки узла. Вы также создадите новое веб-приложение с тестовой веб-страницей для проверки отклика сервера.

1. Войдите на сервер Server2.contoso.com с использованием локальных административных учетных данных.
2. Прежде чем создавать новый веб-сайт, создайте в файловой системе папки содержимого. В проводнике Windows укажите путь %SystemDrive\Inetpub\wwwroot на системном диске компьютера.
3. В папке Wwwroot создайте новую папку Contoso. В папке Contoso создайте папку WebAppOl. Вы будете использовать эти папки как физические пути для веб-сайта и веб-приложения, которые создадите далее.
4. Скопируйте файлы Iisstart.htm и Welcome.png из папки Wwwroot в папку Contoso. Файл Iisstart.htm переименуйте в Default.htm.
5. В папке %SystemDrive%\Inetpub\wwwroot\Contoso\WebAppOl создайте новый текстовый файл Default.htm. Введите в него приведенный ниже код и сохраните файл.

```
<html>
<title>Web Application 01</title>
<body>
<hl>Welcome to Web Application 01.<hl>
</body>
</html>
```

6. В группе программ Администрирование (Administrative Tools) запустите Диспетчер служб IIS (IIS Manager).
7. Если вам будет предложено подключиться к серверу, подключитесь к локальному компьютеру.
8. Разверните объект локального компьютера и контейнер Узлы (Sites), чтобы просмотреть список существующих веб-сайтов. Вы увидите сайт Default Web Site, установленный при добавлении роли Веб-сервер (IIS) на компьютер.
9. Для создания нового веб-сайта щелкните контейнер Узлы (Sites) правой кнопкой мыши и примените команду Добавить веб-узел (Add Web Site).
10. Введите для нового веб-сайта имя *Contoso Test Site*. Заметьте, что по умолчанию создается и автоматически выбирается пул приложений с тем же именем. В данном упражнении вы используете этот новый пул приложений,

однако вы также имеете возможность щелкнуть кнопку Выбрать (Select) и выбрать для нового веб-сайта существующий пул.

11. В поле Физический путь (Physical Path) укажите папку %SystemDrive%\Inetpub\wwwroot\Contoso, созданную ранее. Примите параметр безопасности по умолчанию Сквозная проверка подлинности (Pass-Through Authentication) и щелкните кнопку Тест настроек (Test Settings). Отметим, что IIS может выполнить проверку подлинности, однако не выполняет авторизацию, поскольку эта информация неизвестна до тех пор, пока пользователь не попытается получить доступ к сайту.
12. Для того чтобы вернуться к диалоговому окну Добавление веб-узла (Add Web Site), щелкните кнопку Закрыть (Close).
13. В разделе Привязка (Binding) укажите следующие параметры:
    - Протокол: HTTP;
    - IP-адрес: Все неназначенные (All Unassigned);
    - Порт: 8000;
    - Имя узла: пусто.
14. Убедитесь, что выбрана опция Запустить веб-узел немедленно (Start Web Site Immediately), и щелкните OK для создания и автоматического запуска нового веб-сайта.
15. В левой панели Диспетчера служб IIS (IIS Manager) щелкните новый созданный объект Contoso Test Site. Отметим, что в панели Действия (Actions) представлены команды для работы с веб-сайтом. Для проверки корректности конфигурации сайта щелкните команду Обзор *:8000 (http) (Browse *:8000 (http)). Internet Explorer автоматически запустится и подключится к сайту *http://Server2:8000.contoso.com*. В веб-браузере вы должны увидеть содержимое стартовой страницы IIS по умолчанию. После этого закройте Internet Explorer.
16. Чтобы создать новое веб-приложение, в Диспетчере служб IIS (IIS Manager) щелкните правой кнопкой мыши элемент Contoso Test Site и примените команду Добавить приложение (Add Application).
17. В поле Псевдоним (Alias) введите для приложения псевдоним *TestApp*. В поле Физический путь (Physical Path) введите физический путь %SystemDrive%\Inetpub\wwwroot\Contoso\WebApp01. Обратите внимание на то, что для пула приложений будет выбрана опция DefaultAppPool.
18. Щелкните кнопку Выбрать (Select), чтобы указать пул приложений Contoso Test Site. Оставьте все остальные параметры по умолчанию и щелкните OK, чтобы создать новое веб-приложение.
19. В левой панели Диспетчера служб IIS (IIS Manager) вы увидите новое веб-приложение TestApp в объекте Contoso Test Site. Чтобы проверить содержимое этого приложения, выберите элемент Testltem и щелкните кнопку Просмотр содержимого (Content View) в нижней части центральной панели диспетчера служб IIS. Вы увидите файл по умолчанию default.htm, созданный ранее.

20. Чтобы протестировать веб-приложение, в разделе Управление приложением (Manage Application) панели Действия (Actions) щелкните кнопку Обзор (Browse). Запустится Internet Explorer и подключится к файлу *http://Server2:8000.contoso.com/TestApp/default.htm.* В строке заголовка будет указано имя Web Application 01 и отображено приветствие, сохраненное в HTML-файле. После этого закройте Internet Explorer.
21. Закройте диспетчер служб IIS.

Упражнение 2. Архивация и восстановление параметров конфигурации IIS

В этом упражнении вы выполните архивацию данных конфигурации IIS с помощью утилиты AppCmd.exe. Затем вы с помощью диспетчера служб IIS удалите объект Contoso Test Site, созданный в упражнении 1, и для восстановления конфигурации веб-сайта вновь используете утилиту AppCmd.exe.

1. Войдите на сервер Server2.contoso.com с использованием локальных административных учетных данных.
2. Щелкните меню Пуск (Start), затем кнопку Выполнить (Run) и введите *cmd,* чтобы открыть окно командной строки.
3. Измените текущую рабочую папку на папку с утилитой AppCmd.exe с помощью команды *cd %SystemRoot%\Windows\System32\Inetsrv.*
4. Чтобы создать новую резервную копию параметров конфигурации IIS, в командную строку введите следующее:

   ```
   Appcmd add backup "IISBackupOl"
   ```

5. Для проверки того, была ли создана резервная копия, введите следующую команду:

   ```
   Appcmd list backups
   ```

   Вы должны увидеть в списке элемент IISBackupOl. (Если вы создавали другие резервные копии параметров конфигурации, они также отобразятся в этом списке.)
6. Оставьте окно командной строки открытым и запустите Диспетчер служб IIS (IIS Manager).
7. Подключитесь к локальному серверу и разверните контейнер Узлы (Sites). Щелкните правой кнопкой мыши объект Contoso Test Site и примените команду Удалить (Remove). Для подтверждения операции удаления щелкните кнопку Да (Yes). Сайт и его веб-приложение будут удалены.
8. Вернитесь к окну командной строки и введите следующую команду для восстановления конфигурации IIS из ранее созданной резервной копии:

   ```
   AppCmd restore backup "IISBackupOl"
   ```

9. После выполнения команды закройте окно командной строки и вернитесь к Диспетчеру служб IIS (IIS Manager).
10. Для обновления содержимого консоли щелкните правой кнопкой мыши контейнер Узлы (Sites) и примените команду Обновить (Refresh). Вы увидите объект Contoso Test Site. Отметим, что при удалении веб-сайта содер-

жимое, хранящееся в файловой системе, не удаляется, так что сайт должен быть доступен для использования. В некоторых случаях после выполнения процесса восстановления может потребоваться закрыть Диспетчер служб IIS (IIS Manager) и вновь открыть консоль.

11. Закройте диспетчер служб IIS.

Резюме

- Диспетчер служб IIS (IIS Manager) обеспечивает интегрированный пользовательский интерфейс для управления параметрами, компонентами и веб-содержимым IIS.
- Привязки веб-сайтов указывают протокол, IP-адрес, порт и заголовки сайта. Системные администраторы могут настроить ограничения полосы пропускания, количеств пользовательских подключений и параметры учетных данных для каждого веб-сайта.
- Пулы приложений обеспечивают независимость и изоляцию множества веб-сайтов и веб-приложений, запущенных на одном сервере IIS.
- Системные администраторы и веб-разработчики могут использовать утилиту AppCmd.exe для выполнения распространенных задач управления IIS из командной строки.
- Параметры конфигурации сервера IIS должны хранится в файле ApplicationHostxonfig. Эти параметры могут быть заменены параметрами из файлов Web.config, которые размещены в папках содержимого.
- Windows Server 2008 включает многочисленные компоненты для обеспечения обратной совместимости с целью управления серверами IIS 6.0 и поддержки приложений, разработанных для версии IIS 6.0.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных при изучении материалов занятия 2. Если вы предпочитаете электронную форму вопросов, обратитесь к прилагаемому к книге компакт-диску.

ПРИМЕЧАНИЕ Ответы

Ответы и пояснения к каждому их варианту размещены в разделе «Ответы» в конце книги.

1. Вы, являясь системным администратором, отвечаете за управление веб-сервером Windows Server 2008. В настоящее время на сервере нет настроенных веб-сайтов. Вам требуется отконфигурировать на сервере два веб-приложения: EngineeringApp и SalesApp. Оба приложения должны быть доступны на HTTP-порте 80 без использования заголовков узла. Кроме того, вы должны позаботиться о том, чтобы одно веб-приложение не влияло на быстродействие и стабильность другого. Какие два действия следует предпринять для выполнения этих требований?

   А. Создать один веб-сайт, содержащий оба веб-приложения.

   Б. Создать два веб-сайта — по одному для каждого веб-приложения.

В. Назначить обоим веб-приложениям один пул приложений.
Г. Назначить каждому приложению собственный пул приложений.

2. Вы являетесь системным администратором и отвечаете за управление веб-сервером Windows Server 2008. Вы не создавали вручную резервные копии параметров конфигурации IIS. Недавно веб-разработчик сообщил, что он случайно удалил два веб-сайта из конфигурации IIS. Оба веб-сайта содержали несколько веб-приложений. Вы убедились, что эти веб-сайты не отображаются при открытии диспетчера служб IIS и контейнера Узлы (Sites). Вы также убедились, что содержимое для двух веб-сайтов все еще находится в папке C:\WebSites. Опрашивая других веб-разработчиков, вы выяснили, что больше никакие изменения не вносились в конфигурацию IIS. Какие из приведенных ниже действий следует предпринять для быстрого восстановления двух отсутствующих веб-сайтов и связанных параметров?

А. Вручную воссоздать два веб-сайта, а затем воссоздать связанные веб-приложения.
Б. Вручную модифицировать файл веб-сервера ApplicationHost.config и добавить параметры веб-сайтов и веб-приложений.
В. Восстановить конфигурацию IIS с помощью утилиты AppCmd.
Г. Скопировать предыдущую версию файла ApplicationHost.config из папки %SystemDrive%\Inetpub\wwwroot\History поверх текущей активной версии файла ApplicationHostxonfig.

Закрепление материала главы

Для приобретения практических навыков и закрепления знаний, полученных в ходе изучения материала данной главы, вам необходимо:

- просмотреть резюме главы;
- повторить основные термины;
- выполнить задания лабораторной работы, которые моделируют реальные ситуации, требующие применения полученных знаний;
- выполнить рекомендуемые упражнения;
- сдать пробный экзамен с помощью тестов.

Резюме главы

- Роль Веб-сервер (IIS) (Web Server (IIS)) в Windows Server 2008 предназначена для поддержки веб-сайтов и веб-приложений.
- Роль Веб-сервер (IIS) предоставляет множество служб ролей, связанных с обеспечением безопасности, быстродействия, обратной совместимости и возможности выполнять диагностику.
- Диспетчер служб IIS (IIS Manager) используется для создания веб-сайтов, веб-приложений, пулов приложений и виртуальных каталогов, а также для управления ими.
- Управление IIS можно осуществлять с помощью утилиты командной строки AppCmd.exe, оболочки Windows PowerShell и структуры .NET Framework.

- Windows Server 2008 обеспечивает несколько методов поддержки обратной совместимости для приложений, разработанных на основе IIS предыдущих версий.

Основные термины

Проверьте, знаете ли вы, что означают перечисленные ниже термины (свои ответы можно сверить с определениями, содержащимися в конце книги):

- AppCmd.exe;
- пулы приложений;
- файл ApplicationHostxonfig;
- ASP.NET;
- HTTP (Hypertext Transfer Protocol);
- HTTPS (Hypertext Transfer Protocol Secure);
- Диспетчер служб IIS;
- IIS (Internet Information Services);
- SSL (Secure Sockets Layer);
- привязка узла;
- TLS (Transport Layer Security);
- Роль сервера Веб-сервер (IIS);
- фермы веб-серверов;
- файлы Web.config;
- Windows PowerShell;
- Диспетчер системных ресурсов Windows (WSRM).

Лабораторная работа

Выполнение следующих заданий потребует от вас применения знаний, полученных во время изучения этой главы. Правильные ответы вы сможете найти в разделе «Ответы» в конце книги.

Задание 1. Администрирование веб-сервера IIS

Вы являетесь системным администратором в организации и отвечаете за управление различными веб-серверами. Каждый веб-сервер поддерживает множество веб-приложений. Основные требования включают обеспечение стабильности и быстродействия всех веб-приложений. Кроме того, вы должны упростить административные задачи для серверов. Руководство организации требует, чтобы в случае сбоя оборудования в результате изменений содержимого сайтов или конфигурации потери данные были ограничены информацией лишь за последние четыре часа. Веб-разработчик сообщил, что ему требуется вносить множество изменений в параметры IIS на одном тестовом веб-сервере.

1. Как упростить конфигурацию всех серверов с учетом того, что на них должны использоваться одинаковые параметры?
2. Какое содержимое следует включить в процесс архивации?

3. Какие два способа можно применять для отката конфигурации на тестовом сервере в случае внесения случайных или нежелательных изменений?

Задание 2. Управление множеством веб-сайтов

Вы являетесь системным администратором и отвечаете за управление 15 веб-сайтами на одном веб-сервере Windows Server 2008. Из соображений безопасности, для поддержки стабильности и быстродействия вам необходимо предотвратить влияние проблем, возникающих в одном веб-приложении, на другие приложения. Кроме того, несколько различных веб-приложений требуется отконфигурировать для отклика на HTTP-порте 80 и HTTP-порте 443 с использованием одного публичного IP-адреса. Одно из веб-приложений ASP.NET изначально предназначено для IIS 6.0 и использует преимущества дополнительных компонентов для обработки запросов.

1. Как свести к минимуму вероятность того, что ошибки в одном веб-приложении повлияют на работу других веб-приложений на одном сервере?
2. Какие параметры конфигурации соответствуют требованиям подключения HTTP и HTTPS по умолчанию?
3. Каким образом можно обеспечить поддержку веб-приложения IIS 6.0 на веб-сервере Windows Server 2008?

Рекомендуемые упражнения

Чтобы успешно справиться с экзаменационными заданиями, выполните следующие упражнения.

Управление веб-приложениями

Выполняя предлагаемые упражнения, вы сможете попрактиковаться в создании веб-приложений с помощью диспетчера служб IIS и утилит командной строки, а также в управлении ими.

- **Упражнение 1** Для корректной работы веб-приложения часто приходится выполнять многочисленные требования и включать различные компоненты. По возможности загрузите примеры веб-приложений и разверните их в IIS с помощью различных параметров для пулов приложений и других опций. Хорошей стартовой точкой для загрузки приложений ASP.NET является сайт Microsoft ASP.NET Starter Kit, размещенный по адресу *http://www.asp.net/downloads/starter-kits/*. Кроме того, если в вашей организации уже есть веб-сайты или приложения, попытайтесь установить их в тестовой среде.
- **Упражнение 2** После ознакомления с концепциями использования диспетчера служб IIS для создания веб-сайтов и управления ими попытайтесь выполнить те же действия из командной строки. Используйте утилиту AppCmd.exe для выполнения следующих операций:
  - создание нового веб-сайта с уникальными параметрами привязки узла;
  - создание множества веб-приложений в новом веб-сайте;
  - добавление виртуальных каталогов, которые указывают размещения файловой системы вне папки сайта или веб-приложения по умолчанию;
  - архивация и восстановление параметров конфигурации IIS;
  - удаление тестовых сайтов и других созданных объектов.

Если вам требуется создать много сайтов на нескольких веб-серверах, для автоматизации процесса вы можете скомбинировать множество команд в пакетном файле.

Пробный экзамен

На прилагаемом к книге компакт-диске представлено несколько вариантов тренировочных тестов. Проверка знаний выполняется по одной или же по всем экзаменационным темам сертификационного экзамена 70-643. Тестирование можно организовать таким образом, чтобы оно проводилось как экзамен, или же настроить его на обучение — в этом случае вы сможете после каждого своего ответа на вопрос просматривать правильные ответы и объяснения.

ПРИМЕЧАНИЕ Пробный экзамен

Подробнее о пробном экзамене рассказано во введении к данной книге.

ГЛАВА 6

Управление безопасностью веб-сервера

Занятие 1. Настройка безопасности IIS 298

Занятие 2. Контроль доступа к веб-службам 324

С точки зрения системных администраторов, одна из основных задач управления веб-серверами состоит в обеспечении высокого стандарта безопасности. Безопасность имеет важное значение для всех IT-областей, особенно для информации и приложений, доступных большому числу пользователей.

В этой главе вы изучите принципы конфигурирования безопасности веб-сервера Windows Server 2008. Занятие I посвящено обеспечению безопасности доступа к Internet Information Services 7.0 (IIS 7). Будут рассмотрены принципы конфигурирования разрешений удаленного управления, повышения уровня безопасности сервера путем отключения или удаления ненужных компонентов и опций. На занятии 2 вы изучите методы проверки подлинности и авторизации, а также способы повышения уровня безопасности посредством использования сертификатов сервера и ограничений IP-адресов.

Темы экзамена:

- Настройка веб-приложений.
- Управление веб-сайтами.
- Управление Internet Information Services.
- Настройка безопасности SSL.
- Настройка аутентификации и разрешений веб-сайта.

Требования

Для выполнения упражнений в этой главе вам потребуется следующее.

- Установленная роль сервера Веб-сервер (IIS) (Web Server (IIS)) на сервере Server2.contoso.com с использованием опций по умолчанию для этой роли сервера. Если вы в предыдущих упражнениях создали дополнительные веб-сайты или веб-приложения, можете оставить их на этом сервере.

- Возможность создавать веб-сайты и веб-приложения и управлять ими, как описано в главе 5.

Реальный мир

Анил Десаи

Основной целью системных администраторов, которые отвечают за управление доступом к веб-службам, является сведение к минимуму вероятности неавторизованного доступа и неправильного использования приложений или данных. Понятие «фронт атаки» означает возможности подключения к серверу с использованием различных способов. Один из основных способов обеспечения безопасности сервера состоит в снижении фронта атаки. Инфраструктура IIS поддерживает веб-приложения, использующие различные технологии. Если определенные веб-приложения не требуют применения конкретной технологии (например, поддержку Microsoft .NET Framework), вы можете снизить вероятность неавторизованного доступа к системе, отключив данный компонент.

Еще одна стратегия, связанная с безопасностью веб-сервера, заключается в обеспечении глубинной защиты. В этой технологии используется многоуровневая система безопасности. Опции безопасности включают аутентификацию, авторизацию, разрешения файловой системы и другие параметры, обеспечивающие множество барьеров в получении доступа. Эти механизмы безопасности позволяют лишь авторизованным пользователям получать доступ к системе. Кроме того, в случае некорректной настройки или взлома одного из уровней безопасности другие параметры безопасности могут ограничить неавторизованный доступ или воспрепятствовать ему.

Часто параметрами безопасности управлять довольно сложно. Если системные администраторы не установят соответствующие разрешения, это приведет к снижению уровня безопасности систем. В IIS используется иерархическая система расположения объектов, таких как веб-сайты и веб-приложения, что упрощает организацию параметров и содержимого. Например, вы можете применить параметры безопасности на уровне сервера, для конкретных веб-сайтов и веб-приложений или непосредственно в виртуальных каталогах, физических файлах и папках.

В целом применение разрешений на более высоких уровнях иерархии упрощает администрирование. На рис. 6-1 показано, каким образом такие объекты, как веб-сервер, веб-сайты, веб-приложения и т. д., классифицированы во вложенных связях «родитель-потомок». Параметры объектов более высокого уровня (например, веб-сайта) будут автоматически применены ко всем объектам на более низких уровнях (например, ко множеству веб-приложений). Администраторы могут затем заменять параметры конкретных веб-приложений, используя любой метод в зависимости от требований. Конечным результатом реализации такой стратегии конфигурирования является обеспечение высокого уровня безопасности при минимальных усилиях администратора.

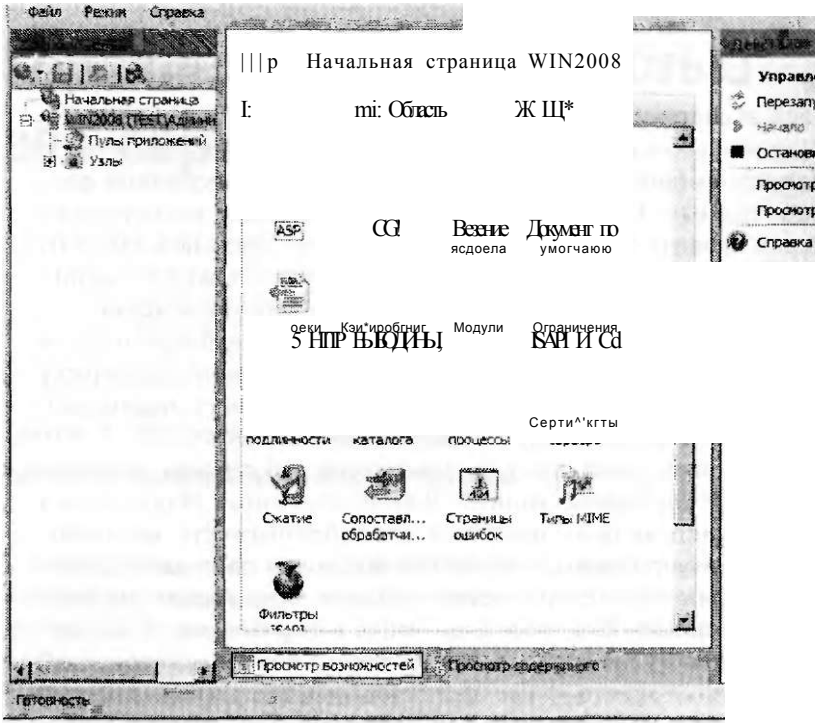


Рис. 6-1. Иерархия объектов в диспетчере служб IIS

СОВЕТ Подготовка к экзамену

Хотя на сертификационном экзамене 70-643 может и не быть вопросов, касающихся общих концепций и методик обеспечения безопасности, вам следует знать рекомендуемые технологии глубинной защиты и снижения фронта атаки веб-сервера. Довольно часто оптимальным решением для сценария является применение различных методов обеспечения безопасности в наиболее подходящей комбинации.

Занятие 1. Настройка безопасности 113

Инфраструктура IIS изначально функционирует как сервер для веб-служб. Поскольку безопасность веб-содержимого имеет большое значение, существует множество промышленных стандартов безопасности, поддерживаемых в IIS 7.0, которые вы должны знать. На этом занятии будут рассмотрены принципы конфигурирования безопасности роли Веб-сервер (IIS) и ее компонентов, а также управления безопасностью. Вначале вы узнаете, как определить разрешения администраторов на веб-серверах, изучите способы расширения возможностей администрирования IIS для других пользователей и веб-разработчиков в орга-

низации с помощью параметров удаленного управления и делегирования. Затем вы изучите способы повышения уровня безопасности путем настройки обработчиков запросов и других параметров с целью сведения к минимуму угроз, связанных с выполнением нежелательного (либо вредоносного) кода и содержимого.

Изучив материал этого занятия, вы сможете:

- Описать архитектуру системы безопасности IIS, включая встроенные учетные записи.
- Включать компоненты удаленного управления для веб-серверов IIS.
- Конфигурировать пользователей диспетчера служб IIS (IIS Manager), разрешения и делегирование для распределенного администрирования.
- Управлять обработчиками запросов и сопоставлениями обработчиков для снижения фронта атак веб-сервера.

Расчетная продолжительность занятия составляет 60 мин.

Учетные записи безопасности IIS 7.0

При добавлении роли Веб-сервер (IIS) (Web Server (IIS)) на компьютер Windows Server 2008 в конфигурацию сервера вносится много изменений и дополнений, как описано в главе 5. В предыдущих версиях IIS для каждой установки использовались учетные записи служб, основанные на имени сервера. Поскольку учетные записи и их идентификаторы безопасности SID (Security Identifier) отличались друг от друга, копирование веб-содержимого и параметров между веб-серверами выполнялось в несколько шагов.

В IIS 7.0 на каждом компьютере с веб-сервером Windows Server 2008 используется стандартная учетная запись IUSRS и локальная группа безопасности IIS_IUSRS. Управление паролями учетных записей выполняется таким образом, что администраторам не нужно их отслеживать.

СОВЕТ Подготовка к экзамену

Веб-службы представляют собой программы, позволяющие серверу хранить, создавать и доставлять информацию с помощью стандартных методов и протоколов, например HTTP. В контексте IIS 7.0 используется статическое содержимое веб-сайтов и веб-приложения, включенные в конфигурацию сервера. При сдаче экзамена под термином «веб-службы» следует понимать любую функциональность IIS.

Управление разрешениями файловой системы

Для реализации системы безопасности администраторы веб-серверов должны иметь возможность определять содержимое, требующее защиты. Они также должны иметь возможность указывать пользователей и группы, которым разрешен доступ к защищенному содержимому. Управление параметрами разрешений

для веб-содержимого осуществляется с помощью разрешений файловой системы NTFS. Администрирование этих параметров можно выполнять напрямую с помощью проводника Windows (Windows Explorer). Вы также можете щелкнуть правой кнопкой мыши отдельный объект в иерархии диспетчера служб IIS (IIS Manager) и применить команду Редактировать разрешения (Edit Permissions). Как показано на рис. 6-2, параметры разрешений определяют пользователей и группы, которые могут получать доступ к содержимому, а также разрешения доступа. В IIS эти разрешения используются для определения учетных данных, которые требуется предоставить для выполнения запроса веб-клиента.

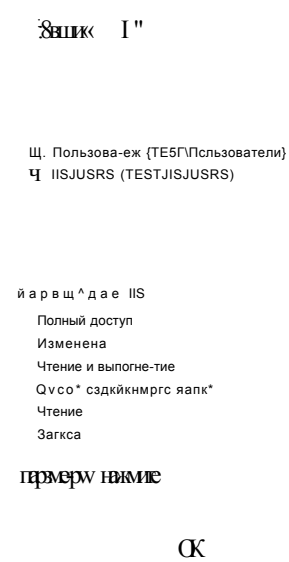


Рис. 6-2. Разрешения для папки веб-сайта Engineering

Настройка компонентов администрирования 113

При добавлении роли веб-сервера (IIS) на компьютер Windows Server 2008 конфигурация по умолчанию позволяет осуществлять лишь локальное администрирование на сервере. Таким образом повышается уровень безопасности, поскольку пользователи других компьютеров не могут с помощью диспетчера служб IIS вносить изменения в конфигурацию сервера. Хотя этот подход оптимален для небольших сред, системные администраторы довольно часто предпочитают использовать Диспетчер служб IIS (IIS Manager) для удаленной настройки сервера.

Во многих средах управление веб-сайтами и веб-приложениями осуществляется группой системных администраторов. При крупномасштабных развертываниях ответственность за один веб-сервер часто несут несколько администраторов. Например, один сервер IIS может управлять несколькими важными веб-приложениями, причем администрирование каждого приложения выполняется отдельной персоной или группой. Если организация обеспечивает для

подписчиков доступ к серверу IIS, подписчикам нужно разрешить управлять определенным веб-содержимым и компонентами. В этом случае подписчики выполняют роль удаленных администраторов для определенных элементов серверов. Удаленное администрирование удобно применять в тех ситуациях, когда существует большое количество администраторов и управление осуществляется из множества местоположений.

Чтобы разрешить удаленным администраторам управлять IIS, вы должны вначале включить на сервере удаленное управление. Затем вы можете определить и отконфигурировать пользователей диспетчера служб IIS. Делегирование позволяет указать действия, которые могут выполнять удаленные администраторы.

Включение удаленного управления

Для включения удаленного управления на локальный сервер с помощью Диспетчера сервера (Server Manager) нужно добавить службу ролей Служба управления IIS (IIS Management Service). В папке Роли (Roles) щелкните правой кнопкой мыши роль Веб-сервер (ITS) (Web Server (IIS)) и примените команду Добавить службы ролей (Add Role Services). Добавьте роль Служба управления IIS (IIS Management Service) из раздела Средства управления (Management Tools) доступных служб ролей.

Служба удаленного управления использует стандартное подключение HTTP или HTTPS. По умолчанию коммуникации осуществляются через порт 8172. Если трафик на этом порте разрешен всеми брандмауэрами и устройствами обеспечения сетевой безопасности, удаленные администраторы смогут управлять своими серверами IIS через локальное сетевое подключение или Интернет.

После добавления службы ролей Сценарии и средства управления IIS (IIS Management Service) в роль Веб-сервер (IIS) (Web Server (IIS)) вы можете использовать Диспетчер служб IIS (IIS Manager) для включения удаленною управления. Для этого откройте Диспетчер служб IIS (IIS Manager) и в левой панели выберите объект веб-сервера. Затем в режиме Просмотр возможностей (Features View) в разделе Управление (Management) дважды щелкните элемент Службы управления (Management Service), чтобы открыть окно, представленное на рис. 6-3.

Изначально флажок Разрешить удаленные подключения (Enable Remote Connections) не установлен. Чтобы разрешить пользователям диспетчера подключаться к IIS по сети, следует его установить. В разделе Удостоверяющие учетные данные (Identity Credentials) можно ука.шгь проверку подлинности с использованием лишь учетных данных Windows (по умолчанию) или также включить реквизиты диспетчера IIS.

В разделе Подключения (Connections) можно указать IP-адреса и порты для служб управления. По умолчанию службы отвечают на запросы всех доступных IP-адресов па порте 8172. Если на веб-сервере отконфигурировано множество сетевых подключений или IP-адресов, для повышения уровня безопасности следует ограничить подключения удаленного доступа конкретным адресом. В разделе Сертификаты SSL (SSL Certificate) можно выбрать один из сертификатов SSL, отконфигурированный на локальном сервере. Вы также можете настроить путь запросов к журналу управления. По умолчанию указан путь %SystemDrive%\Inetpub\Logs\WMSvc.

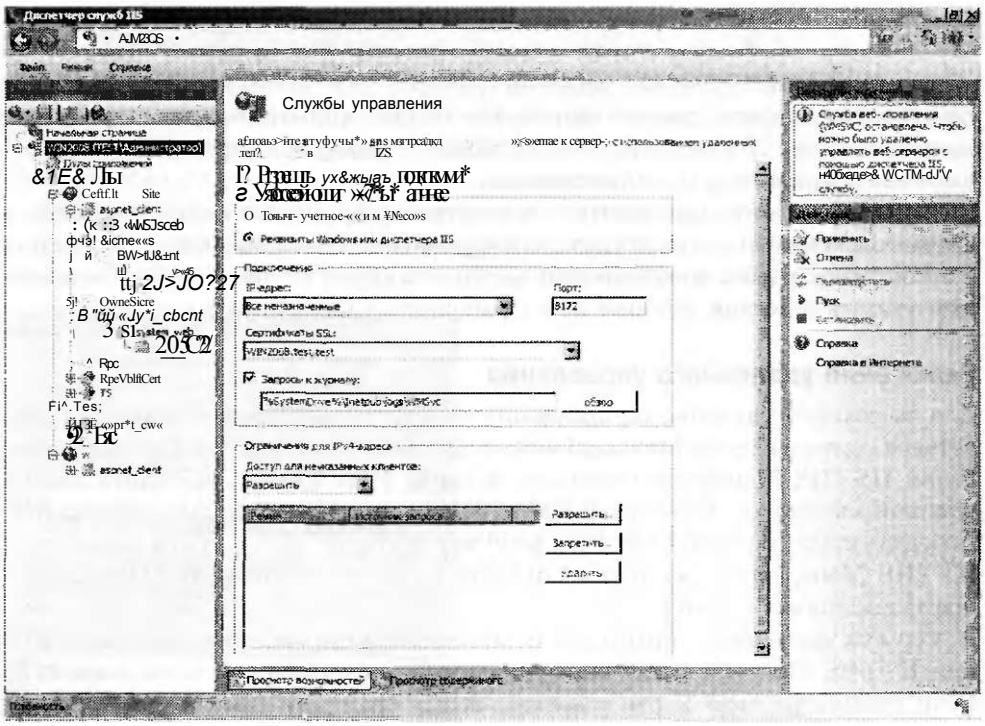


Рис. 6-3. Настройка служб управления в диспетчере служб IIS

И наконец, в разделе Ограничения для IPv4-адреса (IPv4 Address Restrictions) можно ограничить число компьютеров, которым разрешено удаленно подключаться к IIS, повысив таким образом уровень безопасности. Как показано на рис. 6-4, правила настраиваются на основе конкретного I Pv4-адреса или диапазона адресов (который определяется комбинацией IP-адреса и маски подсети).

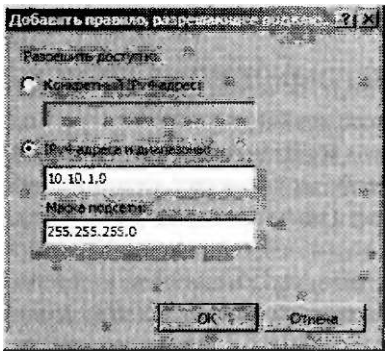


Рис. 6-4. Настройка ограничений 1Ру4-адреса для службы управления в диспетчере IIS

С помощью раскрывающегося списка Доступ для неуказанных клиентов (Access For Unspecified Clients) можно разрешить или запретить IP-адреса без записей. Затем для определения разрешенных IP-адресов можно создать запись

Разрешить (Allow) или Запретить (Deny). Эти опции удобнее всего использовать для управления группой компьютеров, на которых будет осуществляться администрирование веб-служб.

Поскольку служба веб-управления по умолчанию остановлена, для разрешения удаленных подключений в панели Действия (Actions) нужно щелкнуть команду Пуск (Start). Для внесения изменений в конфигурацию требуется остановить службу веб-управления.

Пользователи диспетчера IIS

Чтобы подключаться к веб-серверу Windows Server 2008 с помощью Диспетчера служб IIS (IIS Manager), пользователи должны располагать необходимыми разрешениями. Пользователи, которые входят на компьютер Windows Server 2008 с административными привилегиями, автоматически получают необходимые разрешения для выполнения всех доступных задач на сервере. Для пользователей других типов, например удаленных системных администраторов, требуется определить метод управления разрешениями.

По умолчанию роль Веб-сервер (IIS) (Web Server (IIS)) позволяет назначать разрешения с использованием лишь проверки подлинности Windows. Это означает, что все администраторы, осуществляющие управление IIS, должны располагать учетными данными и разрешениями Windows. Проверка подлинности Windows (Windows Authentication) оптимальна для сред, в которых все администраторы веб-серверов принадлежат одному домену. Пользователям, вошедшим в домен, не нужно вручную вводить учетные данные при подключении к серверу с помощью диспетчера I IS, поскольку они располагают необходимыми разрешениями. Проверку подлинности Windows удобно применять и для создания локальных или доменных учетных записей для всех администраторов, которым требуется доступ к диспетчеру IIS.

В некоторых случаях создавать локальные или доменные учетные записи для каждого потенциального администратора IIS непрактично. Например, компании, управляющие веб-службами, могут содержать сотни пользователей, которым требуется обеспечить возможность управления их серверами. В таких средах каждый пользователь обычно может модифицировать конкретные параметры своего веб-сайта. Эти пользователи не должны иметь доступ к веб-сайтам других пользователей. Кроме того, их возможности часто ограничиваются лишь изменением определенных параметров. Для поддержки таких сценариев требуется выбрать опцию Реквизиты Windows или диспетчера IIS (Windows Credentials Or IIS Manager Credentials). Включив в службах управления эту опцию, вы сможете создавать комбинации пользовательских имен и паролей исключительно для управления IIS. Эти реквизиты потом предоставляются другим пользователям и администраторам, чтобы они могли подключаться к веб-серверу без указания учетной записи Windows каждого пользователя.

Создание пользователей диспетчера IIS

Утилита Диспетчер служб IIS (IIS Manager) позволяет определить пользователей, которым разрешено подключаться и администрировать веб-сайты и веб-службы.

1. Откройте Диспетчер служб IIS (IIS Manager) и в левой панели выберите нужный сервер.

2. В режиме Просмотр возможностей (Features View) щелкните в разделе Управление (Management) элемент Пользователи диспетчера IIS (IIS Manager Users). По умолчанию локальные пользователи IIS не определены.
3. Чтобы создать нового пользователя, вначале щелкните в панели Действия (Actions) команду Открытие функции (Open Feature), а затем в панели действий щелкните команду Добавить пользователя (Add User). Вам будет предложено указать имя пользователя и пароль, как показано на рис. 6-5. Эти параметры определяются в IIS локально, так что здесь не нужно вводить полное имя пользователя в соответствии с доменными правилами именования.

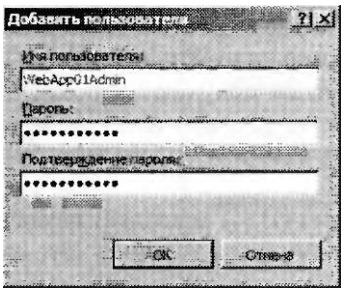


Рис. 6-5. Добавление пользователя диспетчера IIS

Помимо настройки разрешений для пользователей диспетчера IIS вы можете определять удаленно подключаемых пользователей с помощью параметров членства в группах. Пользователи, которым разрешено входить на локальный компьютер и работать с диспетчером IIS, смогут выполнять те же операции с удаленного компьютера.

Определение разрешений управления IIS

До сих пор мы обсуждали включение удаленного управления и способы назначения пользователей, которым разрешено осуществлять администрирование веб-сервера с помощью диспетчера IIS. Далее потребуется определить разрешения для удаленных администраторов. В некоторых случаях удаленному администратору бывает необходимо предоставить полпый административный доступ к веб-серверу. В других ситуациях может понадобиться ограничить доступ лишь конкретными неб-гаитамн или веб-прпложеипямп. Разрешения диспетчера IIS можно конфигурировать на уровне неб слита п приложения. Однако рлзрешенн» нельзя конфигурировать непосредственно па уровне сервера. Эта мера предосторожности гарантирует, что пользователям разрешается модифицировать параметры лишь конкретных веб-сайтов и веб-приложений, к которым им нужно иметь доступ.

Для управления разрешениями выберите веб-сайт или веб-приложение, а затем в режиме Просмотр возможностей (Features View) в разделе Управление (Management) щелкните элемент Разрешения диспетчера IIS (IIS Manager Permissions). IIo умолчанию новым пользователям диспетчера IIS не назначаются разрешения для подключения к конкретному веб-сайту или веб-нриложению. Чтобы разрешить новому пользователю подключения на выбранном уровне, в панели Действия (Actions) вначале щелкните команду Открытие функции

(Open Features), а затем в этой же панели щелкните команду Разрешить пользователю (Allow User). В открывшемся окне можно указать пользователя Windows или Диспетчера IIS (IIS Manager) (если принимаются реквизиты диспетчера IIS), как показано па рис. 6-6. В случае использования учетных данных системы Windows можно выбрать существующего пользователя или группу, определенную ранее в домене (если сервер является членом домена) или же локально.

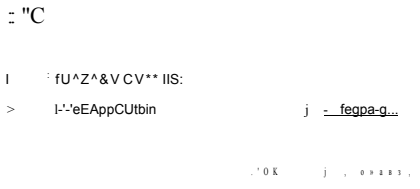


Рис. 6-6. Разрешение пользователю осуществлять администрирование веб-сайта

Пользователи, удаленно подключающиеся к ITS. могут получать доступ лишь к определенным веб-сайтам и веб-приложениям. По умолчанию разрешения объектов более высокого уровня автоматически наследуются объектами на более низких уровнях. Вы также можете использовать в панели Действия (Actions) команду Запретить пользователю (Deny User) для явного запрета доступа на конкретных уровнях.

Чтобы упростить схему администрирования, осуществляемого множеством пользователей, при управлении разрешениями веб-сайта используются две команды. Команда Показать всех пользователей (Show All Users) отображает список всех пользователей IIS. Команда Показать только пользователей узлов (Show Only Site Users) отображает лишь тех пользователей, которые имеют доступ к сайту.

Настройка делегирования компонента

Возможность определения пользователей и разрешений позволяет управлять администрированием на основе структуры содержимого сайта. Однако важно также определить компоненты, которые могут просматриваться и конфигурироваться пользователями. Например, вы можете разрешить администратору веб-сервера подключаться к веб-сайту Default Web Site и запретить изменять параметры проверки подлинности. Делегирование — это процесс, с помощью которого администраторы определяют компоненты IIS для просмотра и изменения пользователями.

Параметры делегирования компонента по умолчанию изначально определены в IIS на уровне сервера. Чтобы получить доступ к этим параметрам с помощью диспетчера IIS, в левой панели выберите объект веб-сервера и в режиме Просмотр возможностей (Features View) щелкните в разделе Управление (Management) элемент Делегирование компонента (Feature Delegation). Откроется окно, показанное на рис. 6-7.

Список элементов, доступных для делегирования, включает все компоненты, добавленные для роли Веб-сервер (IIS) (Web Server (IIS)) и служб ролей. Чтобы изменить параметр для компонента, выберите его в списке и используйте команды в разделе Задать делегирование компонента (Set Feature Delegation) панели Действия (Actions). Для большинства компонентов доступны команды Только чтение (Read Only) или Чтение и запись (Read/Write). Кроме того, для некоторых элементов доступны команды Разрешение на чтение и запись (Configuration Read/Write) или Разрешение только на чтение (Configuration Read Only). Эти настройки позволяют веб-разработчикам указать параметры в файлах конфигурации или управлять ими на основе параметров баз данных. Параметр Делегирование отсутствует (Not Delegated) означает, что компонент нельзя делегировать и конфигурировать на более низких уровнях. Чтобы быстро определить конфигурацию всех параметров, можно также использовать опцию Делегирование (Delegation) в раскрывающемся списке Группировать по (Group By), как показано на рис. 6-8.

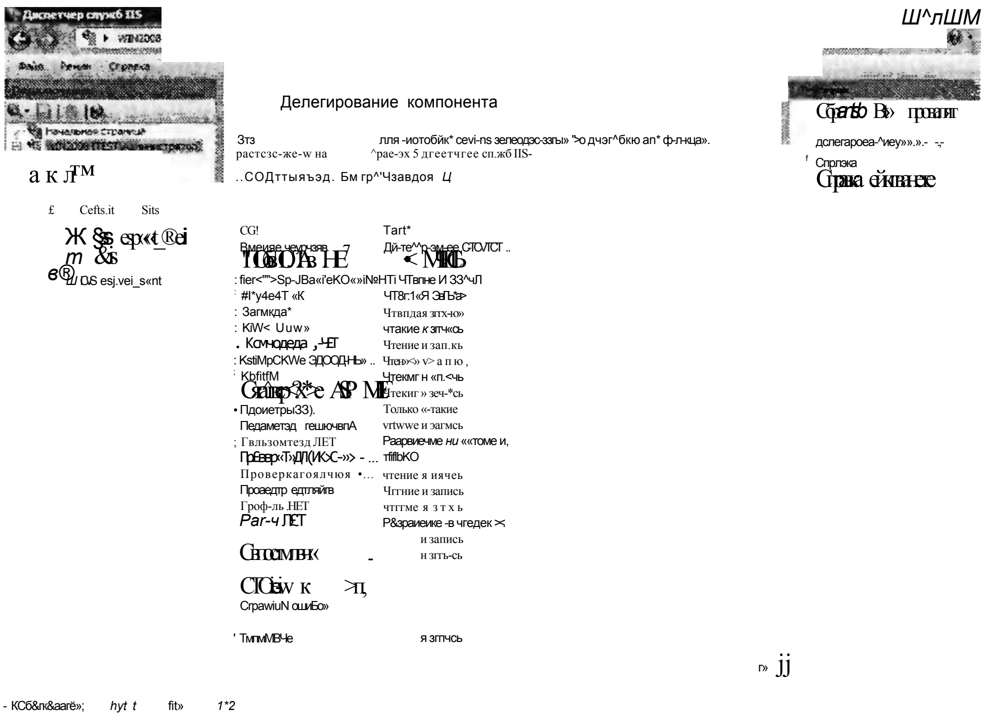


Рис. 6-7. Делегирование компонентов веб-сервера IIS

Параметры, определяемые на уровне сервера, по умолчанию автоматически применяются ко всем дочерним веб-сайтам и приложениям. В некоторых случаях может потребоваться ограничить делегирование компонентов на уровне сайта. Для этого в панели Действия (Actions) щелкните команду Пользовательское делегирование узла (Custom Site Delegation). Откроется окно Пользовательское делегирование узла (Custom Site Delegation) (рис. 6-9), где можно выбрать конкретные сайты, к которым нужно применить параметры делегирования.

Команда Копировать делегирование (Copy Delegation) позволяет копировать текущие выбранные параметры на один или несколько веб-сайтов сервера. Для быстрого возврата исходных значений групп параметров можно также использовать команды Сброс до унаследованного состояния (Reset To Inherited) и Сбросить все делегирование (Reset All Delegation) в панели Действия (Actions). Параметры делегирования компонентов используются для определения элементов конфигурации системы, которые будут доступны удаленным пользователям, подключающимся к серверу с помощью Диспетчера служб IIS (IIS Manager).

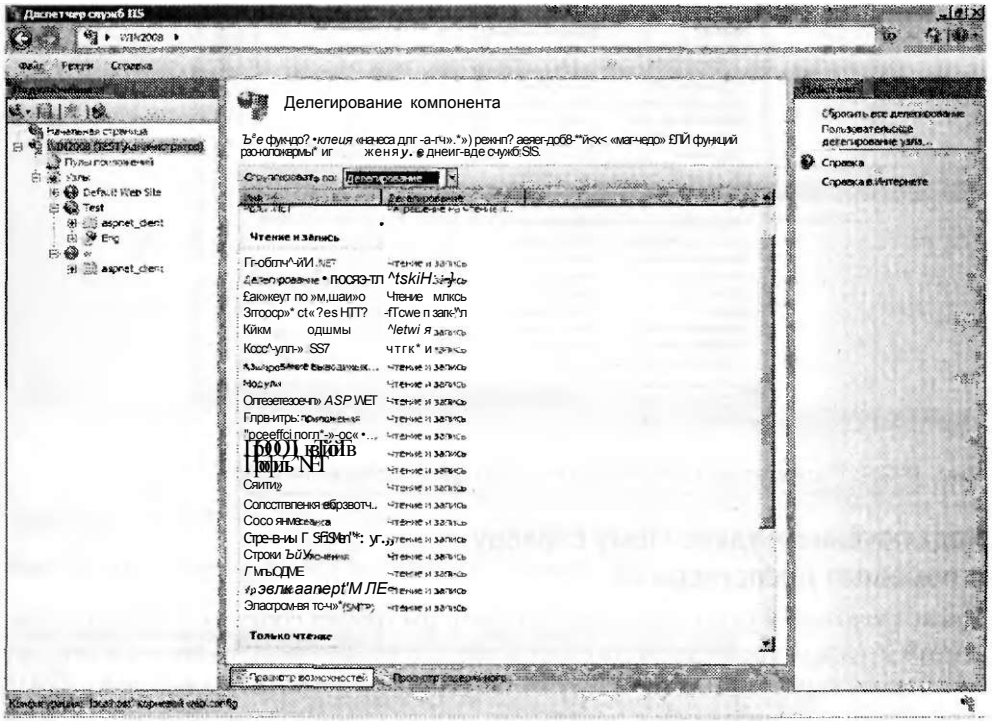


Рис. 6-8. Параметры конфигурации делегирования компонентов, сгруппированные по опции делегирования

ПРИМЕЧАНИЕ

При реализации системы безопасности удаленного управления следует учитывать конкретные требования администрирования. Некоторые параметры, например Пользователи диспетчера IIS (IIS Manager Users) и Делегирование компонента (Feature Delegation), можно конфигурировать лишь на уровне веб-сервера. Таким образом, эти параметры применимы для всех объектов расположенных ниже уровней. В качестве альтернативы Разрешения диспетчера IIS (IIS Manager Permissions) можно конфигурировать для конкретных веб-сайтов и веб-приложений. Такой подход позволяет реализовать гранулированную систему безопасности для тех пользователей, которым требуется доступ лишь к ограниченным наборам элементов веб-сервера.

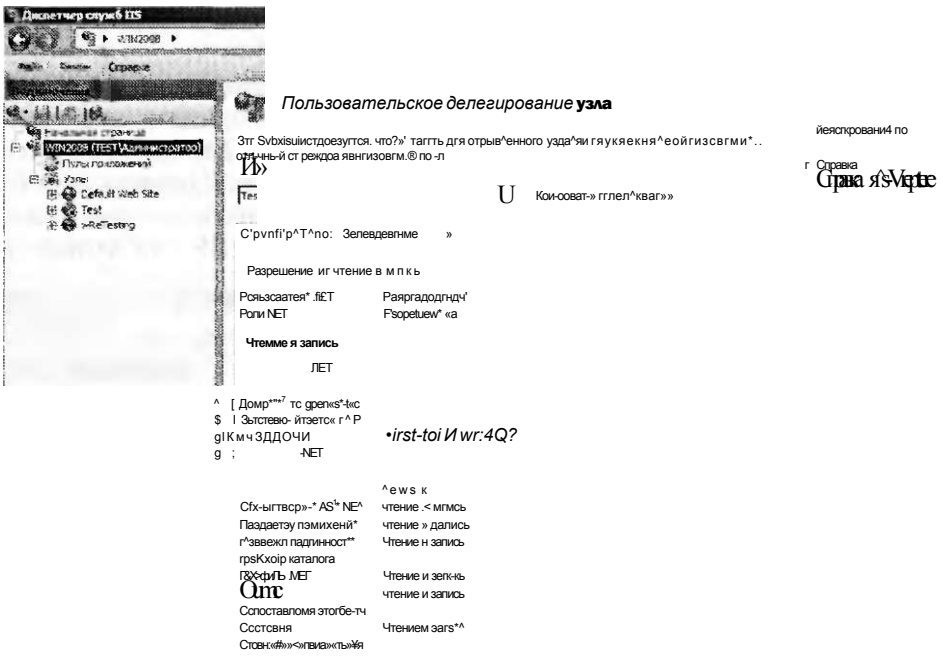


Рис. 6-9. Параметры пользовательского делегирования узла

Подключение к удаленному серверу с помощью диспетчера IIS

После включения удаленного управления и настройки соответствующих разрешений и параметров удаленные пользователи смогут подключаться к серверу с помощью консоли Диспетчер служб IIS (IIS Manager). Для подключения к IIS и проверки конфигурации с локального или удаленного компьютера, где установлена консоль Диспетчер служб IIS, используется элемент Начальная страница (Start Page) диспетчера IIS или меню Файл (File). Как показано на рис. 6-10, удаленные пользователи смогут подключаться к серверу на одном из нескольких уровней.

В рассматриваемом окне доступны следующие команды:

- Подключиться к серверу (Connect To A Server);
- Подключиться к узлу (Connect To A Site);
- Подключиться к приложению (Connect To An Application).

На рис. 6-11 показаны опции, доступные при непосредственном подключении к веб-приложению.

Для установки подключения удаленным администраторам потребуется указать учетные данные (включая пользовательское имя и пароль). В случае успешного соединения удаленные администраторы увидят в левой панели диспетчера IIS новый объект. Для отслеживания соединений эти администраторы также могут именовать и переименовать эти подключения.

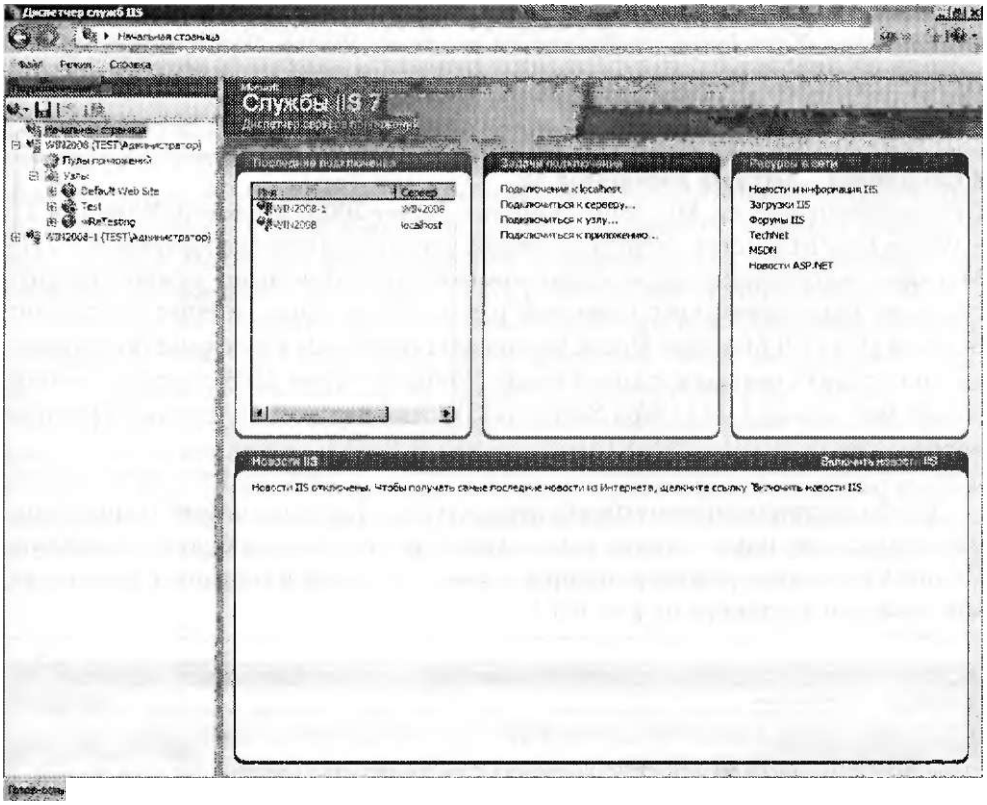


Рис. 6-10. Подключение к удаленному серверу IIS

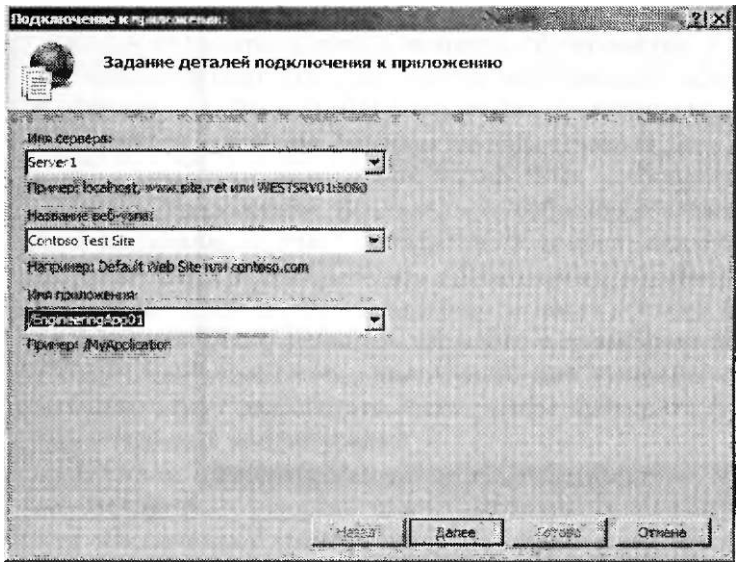


Рис. 6-11. Создание подключения к веб-приложению

Элементы, доступные для управления, зависят от параметров делегирования компонентов. Хотя будут отображаться все те же значки, удаленные администраторы не смогут вносить и сохранять изменения в конфигурацию отдельных элементов.

К СВЕДЕНИЮ Загрузка диспетчера IIS

Пользователи систем Microsoft Windows Server 2003, Microsoft Windows XP и Windows Vista могут загрузить копию консоли Диспетчер служб IIS (IIS Manager) и установить ее на своих компьютерах. Для этого нужно посетить страницу *http://www.iis.net/downloads* и выполнить поиск Internet Information Services (IIS) 7.0 Manager. После установки программы удаленные пользователи смогут подключаться к компьютеру Windows Server 2008 с установленной ролью Веб-сервер (IIS) (Web Server (IIS)), для которой включено удаленное управление.

Для большинства параметров будет доступна страница конфигурации с подробными сведениями, однако сами элементы управления будут отключены. Поэтому удаленные администраторы не смогут вносить и сохранять изменения, как показано в примере на рис. 6-12.

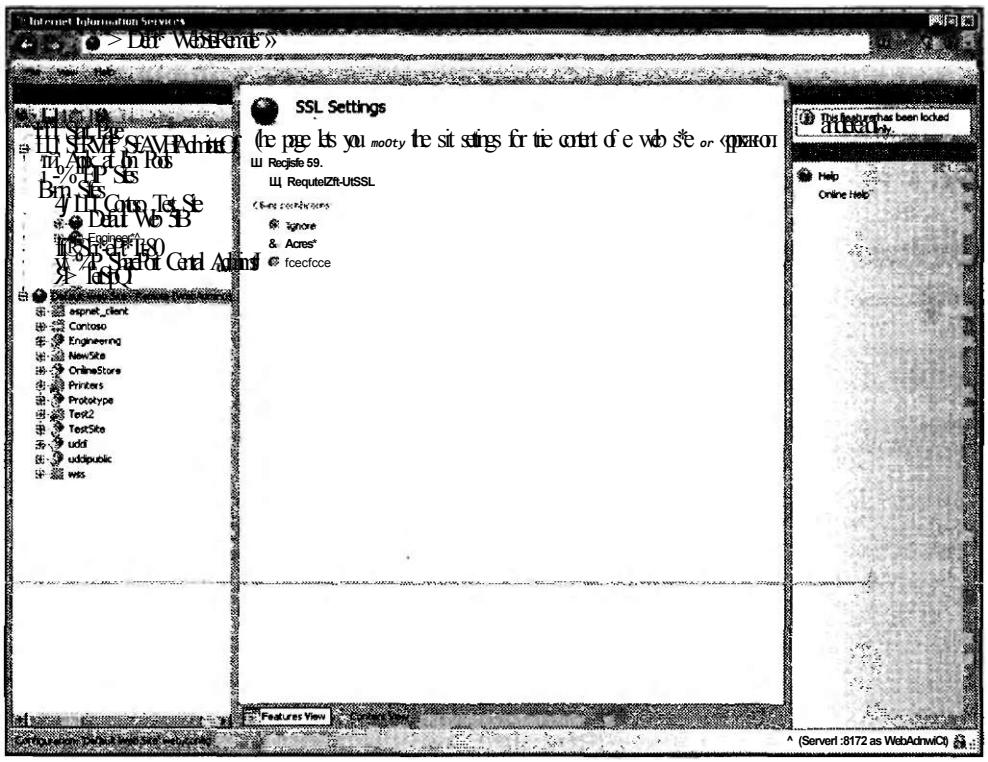


Рис. 6-12. Просмотр параметров SSL, отключенных в делегировании компонентов

Управление обработчиками запросов

Для обеспечения поддержки различных технологий веб-приложений архитектура IIS позволяет включать и отключать обработчики запросов. Обработчики запросов представляют собой программы, которые могут обрабатывать веб-запросы и генерировать отклики, возвращаемые затем клиентам. Веб-серверы и веб-приложения можно конфигурировать с использованием собственных наборов обработчиков запросов в зависимости от типов содержимого, которые требуется поддерживать. Например, веб-приложение можно настроить для поддержки статического содержимого (например, HTML), а также веб-страниц ASP.NET.

Преимущество такого подхода состоит в том, что веб-разработчики могут выбирать технологии, в наибольшей степени соответствующие их задачам. Однако в отношении безопасности это является недостатком. При конфигурировании IIS с использованием множества обработчиков запросов увеличивается фронт атак. Уязвимость в любом включенном обработчике запросов может привести к получению неавторизованного доступа или к возникновению других проблем. Поэтому системным администраторам рекомендуется включать лишь те обработчики запросов, которые планируется использовать. В этом разделе мы рассмотрим включение и отключение обработчиков запросов.

Реальный мир

Анил Десаи

Веб-разработчики и системные администраторы часто назначают слишком много разрешений на своих веб-серверах. Мотивация довольно проста: таким образом проще обеспечить полный доступ ко всем компонентам и параметрам. Нередко системные администраторы не знают нюансов безопасности веб-приложений, а веб-разработчики не осознают важность сведения к минимуму фронта атак производственных веб-серверов. В конечном результате уровень безопасности снижается, и возникает угроза неавторизованного доступа. Как же найти решение проблемы?

Самым важным аспектом определения идеальных параметров безопасности является общение. Администраторы серверов должны согласовывать с веб-разработчиками список конкретных требований для производственных приложений. Вначале целесообразно составить предварительный производственный контрольный список, включающий сведения о назначаемых пользователях, необходимых обработчиках IIS, требованиях проверки подлинности и безопасности доступа. Веб-разработчики должны понимать важность сведения к минимуму количества служб и разрешений для своих приложений. Для выполнения этих задач обе команды могут разработать тесты, чтобы проверить функциональность и безопасность конфигурации.

В целом опыт веб-разработчиков и администраторов веб-серверов основан на деятельности в различных технических областях. Такие отличия обеспечивают преимущества до тех пор, пока обе группы понимают важность реализации системы безопасности производственного сервера.

Сопоставления обработчиков запросов

Когда веб-сервер получает запрос, IIS посредством сопоставлений обработчиков запросов определяет тип обработчика, который нужно использовать для обработки текущего запроса. Сопоставление обработчиков содержит следующую информацию.

- **Операции** Запросы HTTP включают операции, определяющие тип запроса. В качестве самых распространенных операций указываются операция GET, используемая для получения информации с веб-сервера, и операция POST, которая также может включать информацию, отправляемую с клиентского браузера на веб-сервер.
- **Расширение запроса** Как правило, веб-серверы возвращают обширный набор типов содержимого. Самыми распространенными типами информации являются стандартные HTML-страницы, а также изображения в формате .jpg и .gif. В IIS данные файловых расширений из HTTP-запроса могут использоваться для определения типов содержимого, которое потребуется обработать. Например, файловым расширением веб-страниц ASP.NET по умолчанию является .aspx. Запросы страниц .aspx автоматически сопоставляются с обработчиком запросов ASP.NET. На большинстве платформ веб-разработок используются собственные правила для расширений. Разработчики также могут создавать новые расширения и обеспечивать для них соответствующие сопоставления.
- **Информация обработчика** Сопоставление обработчика включает сведения о конкретном обработчике запросов, который должен вызываться в IIS с учетом выполняемой операции или расширения запроса. Наличие этих сведений можно обеспечить различными способами, включая указание полного пути к исполняемому файлу или имени программы, предназначенной для обработки запроса.

Помимо конкретных сопоставлений обработчиков на основе параметров IIS обеспечивает возможность возврата содержимого с помощью обработчика по умолчанию.

Сопоставление обработчика StatisFile отконфигурировано для реагирования на запросы, которые не сопоставляются с существующими файлами. Конкретный ответ зависит от параметров веб-приложения. Если для веб-приложения или виртуального каталога указан документ по умолчанию, то в ситуациях, где в URL не указан файл, будет возвращаться этот документ. Например, в ответ на запрос *http://Server1.contoso.com/TestSite* будет автоматически возвращен документ default.htm (если таковой существует).

Если документа по умолчанию не существует или отключен сам компонент, обработчик StaticFile проверит возможность просматривать каталог. Если этот компонент включен, в ответ на запрос будет возвращен список всего содержимого папки.

И наконец, если ни один из этих методов не может обеспечить выполнение запроса, пользователь получит сообщение о запрете на просмотр каталога с кодом ошибки HTTP 403.14 «Веб-сервер сконфигурирован таким образом, чтобы не формировать списка содержимого каталога» (The Web Server Is Configured To Not List The Contents Of This Directory), показанное на рис. 6-13.

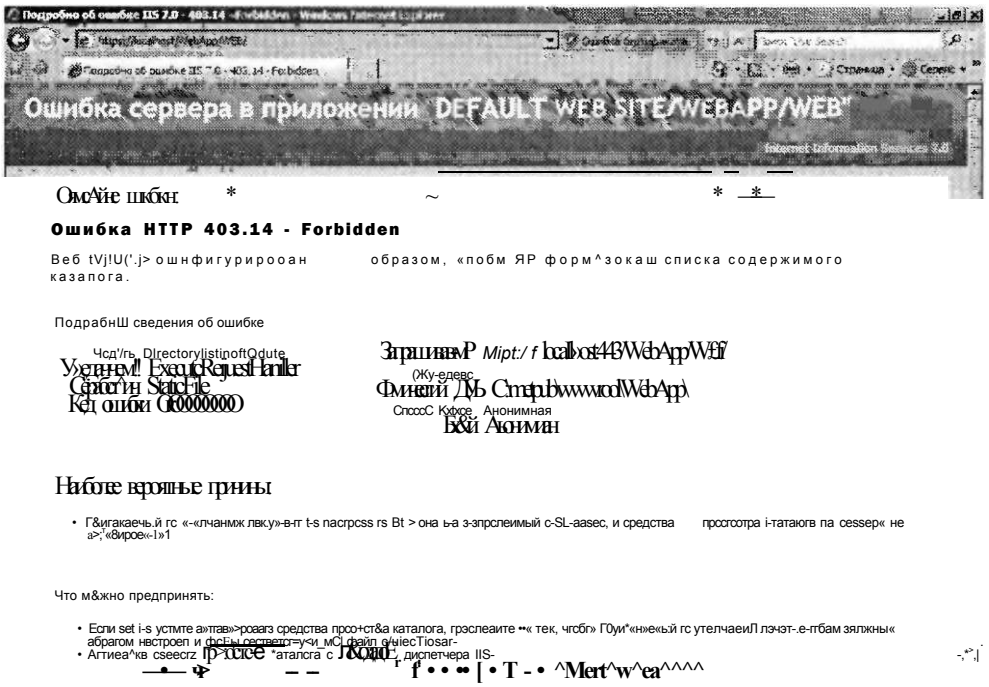


Рис. 6-13. Страница ошибки HTTP 403.14

К СВЕДЕНИЮ Локальные и удаленные сообщения об ошибках

Из соображений безопасности IIS обеспечивает один тип сообщений для веб-пользователей, получающих доступ к серверу с локального компьютера, и еще один тип сообщений для пользователей, получающих удаленный доступ. Таким образом, потенциально уязвимая информация не будет отображаться для пользователей удаленных веб-браузеров, а системные администраторы и веб-разработчики по-прежнему будут получать ценную информацию для устранения неполадок.

Настройка сопоставлений обработчиков

При добавлении роли Веб-сервер (IIS) (Web Server (IIS)) на компьютер Windows Server 2008 для веб-сервера и веб-сайта Default Web Site определяется набор сопоставлений обработчиков по умолчанию. Новые веб-сайты и веб-прнложения также конфигурируются с набором сопоставлений обработчиков по умолчанию. Кроме того, при добавлении служб ролей для веб-сервера (IIS) в конфигурацию могут быть автоматически добавлены дополнительные сопоставления обработчиков.

Для настройки сопоставлений обработчиков можно использовать Диспетчер служб IIS (IIS Manager). После подключения к IIS вы должны выбрать уровень настройки сопоставлений. Сопоставления можно конфигурировать на следующих уровнях:

- веб-сервер;
- веб-сайты;

- веб-приложения;
- виртуальные каталоги;
- веб-папки.

Дочерние элементы в иерархии автоматически наследуют сопоставления обработчиков. Например, дочерний элемент автоматически наследует для нового веб-приложения сопоставления обработчиков по умолчанию из конфигурации родительского веб-сайта. Параметры на нижерасположенных уровнях заменяют параметры на уровнях выше. Таким образом, конкретное веб-приложение может поддерживать определенный тип файлового содержимого (например, страницы ASP.NET), а другие приложения и родительский веб-сайт могут поддерживать лишь статическое содержимое. Для просмотра сопоставлений обработчиков, отконфигурированных на конкретном уровне, щелкните соответствующий объект в левой панели Диспетчера служб IIS (IIS Manager). Затем в режиме Просмотр возможностей (Features View) выберите в центральной панели элемент Сопоставления обработчиков (Handler Mappings). На рис. 6-14 показаны сопоставления обработчиков, определенные для веб-сайта.

В сведения включена вся информация обо всех сопоставлениях обработчиков, определенных на выбранном уровне. Имя включает информацию о самом обработчике запросов. В качестве примеров можно привести обработчики StaticFile и ASPClassic. Для встроенных сопоставлений обработчиков назначены имена по умолчанию, однако администраторы могут указывать имена для создаваемых сопоставлений. В столбце Путь (Path) указаны конкретные расширения запросов, для которых используется данный обработчик.

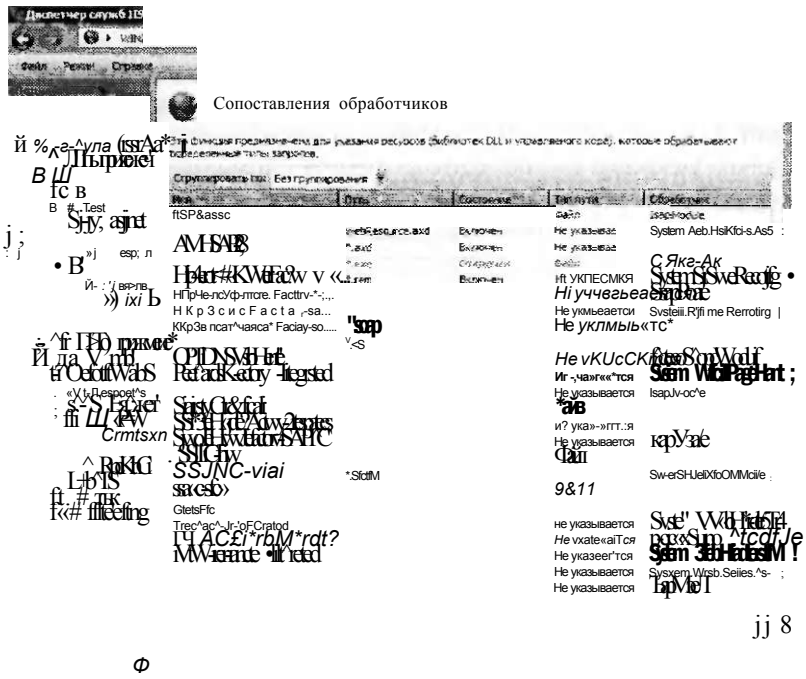


Рис. 6-14. Сопоставления обработчиков для веб-сайта

В столбце Состояние (State) указано, включен или отключен обработчик. Если обработчик отключен, обработка запросов, соответствующих этому сопоставлению, не будет выполняться. В столбце Обработчик (Handler) отображаются сведения о вызываемой программе. И наконец, в столбце Тип элемента (Entry Type) указано наследование сопоставлением обработчика от родительского объекта или тип наследования Локальный (Local), который определяется непосредственно для этого объекта.

Раскрывающийся список Сгруппировать по (Group By) можно использовать для просмотра сопоставлений обработчиков на основе различных критериев. В столбце Тип элемента (Entry Type) указано, какие параметры унаследованы от родительских объектов и какие обработчики отконфигурированы непосредственно для выбранного объекта. Группирование по критерию Состояние (State) позволяет быстро определить включенные и отключенные сопоставления обработчиков и фронт атак для каждого компонента веб-сервера.

Удаление сопоставлений обработчиков

Для обеспечения безопасности веб-содержимого имеет смысл удалять все обработчики запросов, которые не требуется использовать в работе. Чтобы удалить сопоставление обработчика, щелкните его и в панели Действия (Actions) выберите команду Удалить (Remove). После его удаления обработка запросов типов содержимого, для которых использовался этот обработчик, не будет выполняться. Например, на рис. 6-15 показан результат, возвращаемый на локальный веббраузер в случае удаления обработчика запросов StaticFile для веб-приложения.

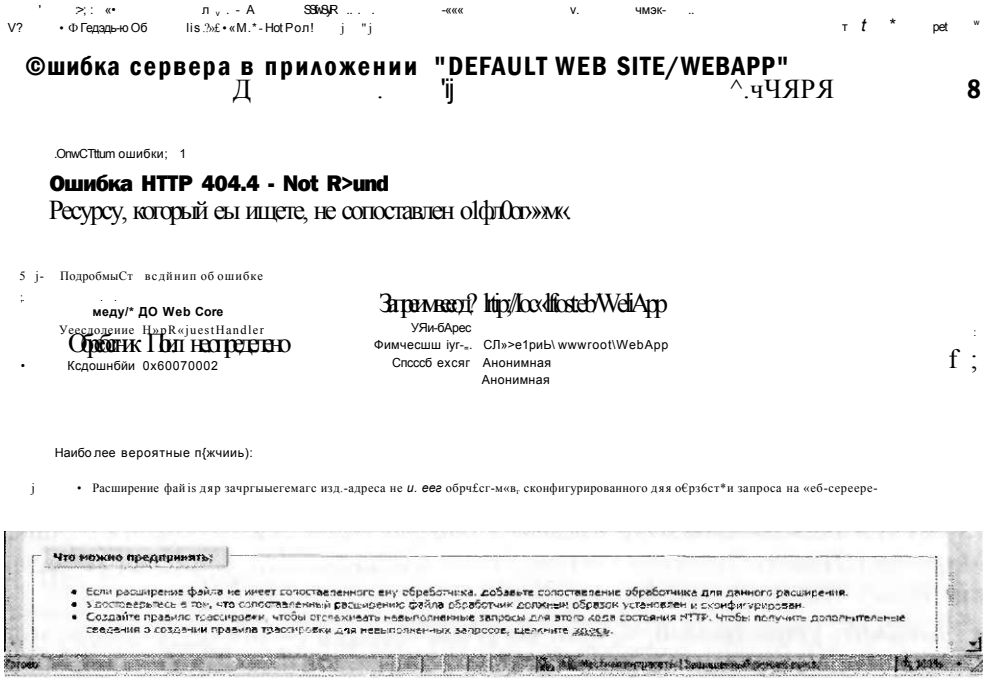


Рис. 6-15. Страница ошибки обработчика запроса

В данном случае файл запроса default.htm находится в папке веб-приложения. Однако из-за отсутствия доступного обработчика запросов для файлового расширения .htm обработка запроса выполняться не может. Веб-браузер получит сообщение о том, что запрашиваемого файла не существует.

Управление наследованием обработчиков

Наследование параметров сопоставлений обработчиков может значительно упростить администрирование серверов с множеством веб-сайтов и веб-приложений. В целом конфигурировать сопоставления обработчиков по возможности следует на самом высоком уровне. Например, если вы уверены, что ни одному из веб-приложений конкретного веб-сайта не потребуется отвечать на запросы файлового расширения .soap, это сопоставление обработчика можно удалить на уровне веб-сайта. Как мы уже говорили ранее, из соображений безопасности следует свести к минимуму количество включенных обработчиков и количество их типов.

По умолчанию объекты на более низких уровнях веб-сервера могут заменять параметры сопоставлений обработчиков, унаследованные от родительских объектов. Иногда может даже потребоваться запретить обработку некоторых типов запросов на всем сервере независимо от параметров веб-сайтов и веб-приложений. Для этого можно блокировать конфигурацию обработчика запросов. Для блокировки конфигурации в Диспетчере служб IIS (IIS Manager) щелкните объект веб-сервера, а затем дважды щелкните элемент Сопоставления обработчиков (Handler Mappings). Выберите сопоставление обработчика, которое вы хотите блокировать, а затем в панели Действия (Actions) щелкните команду Блокировка (Lock).

Для параметров сопоставлений обработчиков можно также вернуть значения по умолчанию. Для этого в панели Действия (Actions) диспетчера служб IIS щелкните команду Вернуться к унаследованным (Revert To Inherited). При выполнении этого действия будут восстановлены сопоставления родительского объекта и потеряны все локально определенные сопоставления обработчиков.

Добавление сопоставлений обработчиков

Архитектура IIS позволяет системным администраторам добавлять новые сопоставления обработчиков на основе конкретных требований. Например, если вам нужно обеспечить поддержку файлового типа с расширением .mypage, вы можете добавить обработчик для этого типа. Кроме того, веб-разработчики могут создавать собственные программы для управления любыми новыми типами запросов.

Чтобы добавить сопоставление обработчика, выберите соответствующий объект, а затем в режиме Просмотр возможностей (Features View) диспетчера служб IIS дважды щелкните элемент Сопоставления обработчиков (Handler Mappings). Панель Действия (Actions) содержит несколько опций для добавления новых типов обработчиков запросов, которые описаны далее.

- **Добавить управляемый обработчик (Add Managed Handler)** Управляемый обработчик выполняет обработку запросов на основе библиотеки кодов .NET. Выбрать существующие модули кодов .NET, зарегистрированные на локаль-

ном сервере позволяет Параметр Тип (Type) (рис. 6-16). Все эти типы принадлежат к именному пространству System.Web.

- Добавить сопоставление сценария (Add Script Map) Сопоставления сценариев используются для пересылки обработки запросов в библиотеку DLL (Dynamic Link Library) или исполняемый файловыйгтип (.exe). Эти типы программ предназначены для обработки данных запросов и генерирования ответа для IIS с целыо отправки его конечному пользователю.

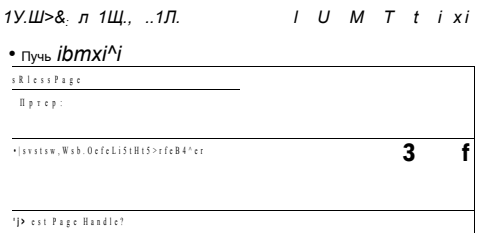


Рис. 6-16. Добавление управляемого обработчика для веб-сайта

- Добавление сопоставления сценария с подстановочными знаками (Add Wildcard Script Map) Сопоставления сценариев с подстановочными знаками используются для указания обработчика по умолчанию для типов документов, которыми нельзя управлять с помощью других обработчиков. Опция Исполняемый файл (Executable Path) указывает файл .dll или .exe, предназначенный для обработки запросов.
- Добавить сопоставление модуля (Add Module Mapping) Модули представляют собой программы, предназначенные для интеграции с конвейером обработки запросов ГIS. Они могут обеспечивать обширный набор функции п включены ь службы ролей, устанавливаемые по умолчанию и выборочно для роли Веб-сервер (IIS) (Web Server (IIS)). В качестве примеров можно привести модуль FastCGIModule, предназначенный для обработки сценариев на основе спецификации CGI (Common Gateway Interface), и модуль StaticCompressionModule, который сжимает статическое содержимое HTML для экономии полосы пропускания. Помимо указания модуля для обработки администраторы могут определить опциональный исполняемый файл или библиотеку .dll, которая будет использоваться мри обработке запросов, как показано на рис. 6-17.

При добавлении нового обработчика запросов вам будет предложено указать данные пути запроса. Вы можете использовать подстановочные знаки или указать список конкретных файлов. В качестве примеров можно привести путь *.mypage (для реагирования на запросы всех файлов с этим расширением) и Config.mypage (для реагирования на запросы этого конкретного имени файла).

Параметр Имя (Name) можно использовать с целью идентификации назначения сопоставления обработчика для других разработчиков и администраторов.

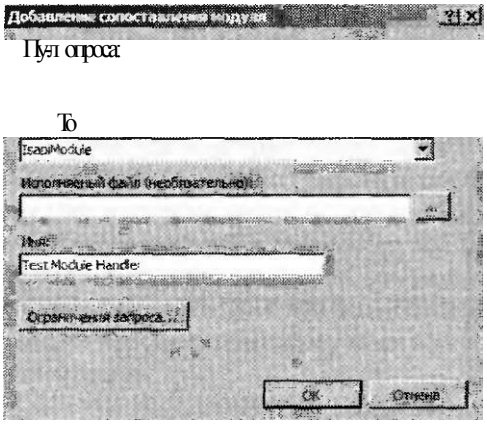


Рис. 6-17. Добавление сопоставления модуля для веб-приложения

Настройка ограничений запроса

Помимо указания путей и файловых имен, которым будут сопоставляться конкретные обработчики запросов, с помощью ограничений запроса можно внедрить безопасность IIS. Чтобы открыть доступные опции, в диалоговом окне добавления сопоставления щелкните кнопку Ограничения запроса (Request Restrictions). Опции ограничения запроса распределены по трем вкладкам Сопоставление (Mapping), Команды (Verbs) и Доступ (Access).

Вкладку Сопоставление (Mapping) можно использовать для указания вызова обработчика при сопоставлении запроса с файлом, каталогом или и с тем, и с другим. По умолчанию обработчик автоматически вызывается при запросах файлов и каталогов. Вы можете ограничить вызов обработчика лишь при запросе файлов или каталогов, чтобы, к примеру, обработчик отвечал на запросы документов по умолчанию или на явные запросы файлов.

Вкладку Команды (Verbs), показанную на рис. 6-18, можно использовать для указания команд HTTP-запросов, на которые будет реагировать обработчик. Хотя самыми распространенными типами команд являются операции GET и POST, для запроса других сведений на веб-сервере некоторые приложения могут использовать другие команды (например HEAD). По умолчанию обработчику запросов будут пересылаться все типы команд. Если вам требуется использовать для разных команд различные обработчики или вы хотите применять сопоставление обработчиков лишь к определенным типам запросов, можете воспользоваться опцией Одна из следующих команд (One Of The Following Verbs).

И наконец, на вкладке Доступ (Access) указаны разрешения доступа, которые будут предоставлены обработчику запросов. Из соображений безопасности следует свести к минимуму типы доступа обработчика. По умолчанию указан доступ Сценарий (Script), который применим к большинству типов исполняв-

мых обработчиков. Существуют также опции доступа Нет (None), Чтение (Read), Запись (Write) и Выполнение (Execute).

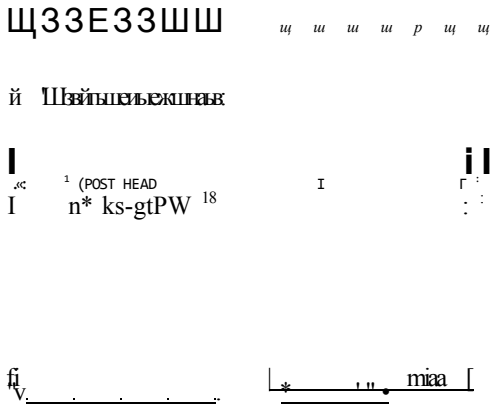


Рис. 6-18. Ограничения команд запросов для сопоставления обработчика

Настройка разрешений функции

Разрешения функции указывают типы действий, которые может выполнять обработчик запросов. Чтобы настроить эти параметры, дважды щелкните элемент Сопоставления обработчиков (Handler Mappings), а затем в панели Действия (Actions) щелкните команду Изменение разрешений функции (Edit Feature Permissions). Откроется окно, показанное на рис. 6-19.

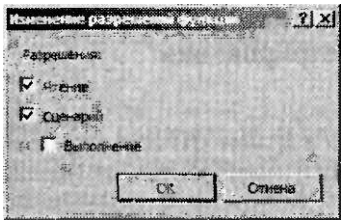


Рис. 6-19. Настройка разрешений функции для обработчика запросов

В окне представлены следующие три опции разрешений.

- Чтение (Read) Разрешает обработчику читать файлы, хранящиеся внутри файловой системы.
- Сценарий (Script) Разрешает обработчику выполнять основные сценарии па сервере.
- Выполнение (Execute) Разрешает обработчику при обработке запроса запускать на компьютере файлы с исполняемым программным кодом (как например, .dll или .exe). Для включения этого разрешения должно быть также включено разрешение Сценарий (Script).

По умолчанию для новых сопоставлений обработчиков включены разрешения Чтение (Read) и Сценарий (Script).

Проверьте себя

1. Какие шаги следует предпринять, чтобы разрешить пользователям удаленно управлять IIS с помощью консоли Диспетчер служб IIS (IIS Manager)?
2. Назовите два способа управления пользователями, которые могут осуществлять удаленное администрирование IIS?

Ответы

1. Чтобы разрешить удаленное управление, нужно добавить службу ролей Служба управления IIS (IIS Management Service) и разрешить удаленные подключения в элементе Службы управления (Management Service).
2. Служба управления IIS (IIS Management Service) может выполнять проверку подлинности пользователей с помощью учетных данных Windows (Windows Authentication) или реквизитов диспетчера IIS (IIS Manager Credentials).

Практикум. Управление параметрами безопасности IIS

В предложенных далее упражнениях вы выполните действия, необходимые для управления безопасностью компьютера Windows Server 2008 с установленной ролью Веб-сервер (IIS) (Web Server (IIS)). В частности, вы включите удаленное администрирование и отконфигурируете сопоставления обработчиков. Предполагается, что на сервере Server2.contoso.com уже установлена роль Веб-сервер (IIS) с опциями по умолчанию и вы знаете, как добавлять службы ролей.

Упражнение 1. Настройка удаленного администрирования и управление им

В этом упражнении вы используете функции Службы управления IIS (IIS Management Service), чтобы разрешить пользователю подключаться к компьютеру. Вначале вам потребуется установить службу ролей Служба управления IIS (IIS Management Services). Затем вы создадите нового пользователя с применением реквизитов диспетчера IIS и настроите разрешения доступа к сайту Default Web Site. И наконец, вы подключитесь к IIS с использованием новой учетной записи и проверите разрешения и параметры делегирования компонентов. Последние шаги можно выполнять локально на сервере Server2 или на еще одном компьютере Windows Vista или Windows Server 2008 с установленной консолью Диспетчер служб IIS (IIS Manager). Предполагается, что вы выполняете шаги локально на сервере Server2.

1. Войдите на сервер Server2 в качестве пользователя с административными привилегиями.
2. С помощью Диспетчера сервера (Server Manager) добавьте службу ролей Служба управления IIS (IIS Management Service) в роль Веб-сервер (IIS) (Web Server (IIS)). Затем закройте Диспетчер сервера (Server Manager).
3. Откройте Диспетчер служб IIS (IIS Manager) и подключитесь к локальному серверу (Server2).

4. В левой панели щелкните объект сервера, а затем в режиме Просмотр возможностей (Features View) дважды щелкните элемент Службы управления (Management Service).
5. На странице Службы управления (Management Service) должно отображаться сообщение о том, что служба веб-управления не запущена. Эта мера необходима для внесения изменений в конфигурацию. Установите флажок Разрешить удаленные подключения (Enable Remote Connections).
6. В разделе Удостоверяющиеся учетные данные (Identity Credentials) выберите опцию Реквизиты Windows или диспетчера IIS (Windows Credentials Or IIS Manager Credentials), чтобы позже иметь возможность создавать пользователей диспетчера IIS. Оставьте все остальные параметры по умолчанию. Отметим, что службы управления по умолчанию будут реагировать на запросы порта 8172.
7. С помощью команды Пуск (Start) в панели Действия (Actions) запустите службу управления сервером. Имейте в виду, что вы не сможете модифицировать параметры запущенной службы.
8. Вернитесь в режим Просмотр возможностей (Features View), щелкнув кнопку Назад (Back) в верхней панели инструментов.
9. Дважды щелкните элемент Пользователи диспетчера IIS (IIS Manager Users), чтобы просмотреть список пользователей, которым разрешен доступ к системе. Отметим, что по умолчанию этот список пуст.
10. Чтобы создать нового пользователя диспетчера IIS, в панели Действия (Actions) щелкните команду Добавить пользователя (Add User). Укажите имя пользователя *WebAdminOI* и пароль *1w3b!admin.* (Всегда используйте строгие пароли.) Для создания нового пользователя щелкните ОК и убедитесь, что он появился в списке Пользователи диспетчера IIS (IIS Manager Users).
11. В левой панели диспетчера IIS щелкните объект Default Web Site. Затем в режиме Просмотр возможностей (Features View) дважды щелкните в области Управление (Management) элемент Разрешения диспетчера IIS (IIS Manager Permissions).
12. Щелкните действие Разрешить пользователю (Allow User). В качестве типа пользователей выберите Диспетчер служб IIS (IIS Manager) и введите в текстовое поле имя *WebAdminOI.* Щелкните ОК.
13. В диспетчере служб IIS щелкните объект Server2, а затем в режиме Просмотр возможностей (Features View) дважды щелкните в области Управление (Management) элемент Делегирование компонента (Feature Delegation). В раскрывающемся списке Сгруппировать по (Group By) выберите критерий Делегирование (Delegation). Обратите внимание на компоненты в списке, которым назначено делегирование Только чтение (Read Only). В последующих шагах вы попытаетесь изменить Параметры SSL (SSL Settings), чтобы проверить делегирование этого компонента.
14. В левой панели диспетчера служб IIS щелкните элемент Начальная страница (Start Page). В центральной панели щелкните ссылку Подключиться к узлу (Connect To A Site).

15. В поле Имя сервера (Server Name) введите имя *Server2.contoso.com.* В поле Название веб-узла (Site Name) введите имя Default Web Site. Щелкните кнопку Далее (Next).
16. В поле Имя пользователя (Username) введите имя *WebAdminOI,* а в поле Пароль (Password) введите пароль *1w3b!admin.* Щелкните кнопку Далее (Next).
17. В качестве имени подключения введите *Default Web Site - Test* и щелкните кнопку Готово (Finish). После выполнения подключения в левой панели диспетчера служб IIS появится новый элемент — Default Web Site - Test. Для администрирования это подключение можно щелкнуть, как в случае с локальным подключением по умолчанию. Тем не менее отметим, что новое подключение отображает лишь содержимое сайта Default Web Site. Вы будете располагать только теми разрешениями, которые назначены пользователю WebAdminOI.
18. Чтобы проверить параметры делегирования компонентов, в режиме Просмотр возможностей (Features View) щелкните в области SSL элемент Параметры SSL (SSL Settings).
19. При желании вы можете удалить новое подключение в диспетчере служб IIS, щелкнув его правой кнопкой мыши и применив команду Удаление подключения (Remove Connection).
20. Закройте Диспетчер служб IIS (IIS Manager).

Упражнение 2. Управление сопоставлениями обработчиков

В этом упражнении вы займетесь настройкой сопоставлений обработчиков для веб-приложения и управлением ими. Вначале вы проверите корректность отображения содержимого для веб-пользователей. Затем вы отключите сопоставление обработчика запросов и убедитесь, что содержимое более недоступно. И наконец, для восстановления доступа к содержимому вы вернете унаследованные параметры сопоставлений обработчиков.

1. Войдите на сервер Server2 в качестве пользователя с административными привилегиями.
2. С помощью проводника Windows найдите каталог %SystemDrive%\Inetpub\Wwwroot. Создайте копию файла Iisstart.htm и укажите для нее имя *Iisstart.test.* Отметим, что вам может потребоваться сбросить флажок Скрывать расширения для зарегистрированных типов файлов (Hide Extensions For Well Known File Types) на вкладке Вид (View) диалогового окна Свойства папки (Folder Options). Для этого в меню Упорядочить (Organize) примените команду Свойства папок и поиска (Folder And Search Options).
3. Закройте Проводник Windows (Windows Explorer).
4. Откройте Диспетчер служб IIS (IIS Manager) и подключитесь к локальному серверу.
5. В левой панели диспетчера служб IIS выберите объект Default Web Site. В панели Действия (Actions) щелкните команду Обзор *:80(http) (Browse *:80(http)). Запустится Internet Explorer, и он подключится к содержимому для сайта по умолчанию. Отметим, что отобразится документ по умолчанию (в данном случае файл Iisstart.htm), и страница будет содержать тип изображения .png.

6. В Internet Explorer модифицируйте URL для запроса страницы iisstart.test. Например, можно ввести полный URL *http://Server1/iisstart.test*. Отметим, что несмотря на наличие файла, вы получите код ошибки HTTP 404.3. Это означает, что для обработки запроса недоступен обработчик.
7. Закройте Internet Explorer.
8. В Диспетчере служб IIS (IIS Manager) дважды щелкните элемент Сопоставления обработчиков (Handler Mappings). Вы увидите список всех обработчиков по умолчанию, зарегистрированных в системе.
9. Для создания нового сопоставления щелкните ссылку Добавить сопоставление модуля (Add Module Mapping). В поле Путь запроса (Request Path) введите **.test*. В раскрывающемся списке Модуль (Module) выберите модуль StaticFileModule. В поле Имя (Name) введите название *Test Page Handler*. Оставьте остальные параметры по умолчанию и щелкните ОК для создания сопоставления. Веб-сервер обработает файлы с расширением .test.
10. Откройте Internet Explorer, а затем откройте страницу Iisstart.page с помощью того же URL, который использовали в шаге 5. Отметим, что на этот раз вы увидите пустую страницу без сообщения об ошибке. Это означает, что новое созданное сопоставление обработчика функционирует должным образом.
11. Закройте Internet Explorer.
12. В Диспетчере служб IIS (IIS Manager) вернитесь к элементу Сопоставления обработчиков (Handler Mappings) для объекта Default Web Site, а затем в панели Действия (Actions) щелкните команду Вернуться к унаследованным (Revert To Inherited). Для подтверждения изменений щелкните кнопку Да (Yes). Будут восстановлены сопоставления обработчиков по умолчанию и удалено сопоставление Test Page Handler, созданное в предыдущем шаге.
13. Закройте Диспетчер служб IIS (IIS Manager).

Резюме

- Для обеспечения безопасности IIS следует внедрить реализацию глубинной защиты и снизить фронт атак.
- Для управления системой безопасности в IIS 7.0 используются встроенные учетные записи пользователей и группы.
- Удаленное управление в IIS можно включить, добавив службу ролей Служба управления IIS (IIS Management Service).
- Управление возможностями удаленного администрирования можно осуществлять путем создания пользователей, назначения разрешений и настройки делегирования компонентов.
- Сопоставления обработчиков запросов определяют типы содержимого, разрешенные IIS для отдельного компонента в иерархии.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных в ходе занятия 1. Эти вопросы представлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы
Ответы и пояснения к каждому их варианту размещены в разделе «Ответы» в конце книги.

1. Вы являетесь системным администратором и отвечаете за безопасность веб-сервера Windows Server 2008. Вы создали новый веб-сайт Contoso Intranet, который будет содержать семь веб-приложений. Один из разработчиков приложений сообщил вам, что для его нового веб-приложения требуется новый обработчик запросов с использованием созданной библиотеки .NET. Как выполнить эти требования, обеспечив максимальный уровень безопас-" ности для сервера?
   А. Добавить новый управляемый обработчик для веб-сайта Contoso Intranet.
   Б. Добавить новый управляемый обработчик для конкретного веб-приложения, которому он требуется.
   В. Добавить новое сопоставление модуля для веб-сайта Contoso Intranet.
   Г. Добавить новое сопоставление модуля для конкретного веб-приложения, которому он требуется.
2. Как системный администратор вы отвечаете за управление веб-сервером Windows Server 2008. Недавно ваша организация установила новый веб-сайт IIS, доступ к которому будут получать пользователи вне организации. Консультанты должны иметь возможность подключаться к этому веб-сайту с помощью диспетчера служб IIS. Политика безопасности организации не позволяет создавать доменные или локальные учетные записи для этих пользователей. Вы пытаетесь использовать для веб-сайта компонент Разрешения диспетчера IIS (IIS Manager Permissions). Однако, щелкнув команду Разрешить пользователю (Allow User), вы можете выбрать лишь пользователей Windows. Как решить эту проблему?
   А. Убедиться в том, что запущен компонент Службы управления (Management Service).
   Б. Заново отконфигурировать разрешения файловой системы для корневого каталога веб-сайта.
   В. Заново отконфигурировать Службы управления (Management Service) и в качестве удостоверяющих учетных данных выбрать Реквизиты Windows или диспетчера IIS (Windows And IIS Manager Credentials).
   Г. Проверить параметры Проверка подлинности (Authentication) для веб-сайта.

Занятие 2. **Контроль доступа к веб-службам**

Как правило, конфигурация развертывания веб-серверов бывает самой разной. Одни серверы обеспечивают содержимое, которое должно быть общедоступным в Интернете, другие — содержимое веб-приложений, доступное только для ограниченного набора пользователей. Администрация веб-сервера должна располагать возможностью определения пользователей, которые могут подключаться к веб-службе. После того как пользователи подтвердят свою идентичность, доступ к типам содержимого должен осуществляться на основе правил.

На этом занятии вы изучите принципы конфигурирования проверки подлинности и авторизации для обеспечения защиты веб-содержимого в IIS. Ввиду множества стандартов и методик обеспечения безопасности для веб-служб важно знать, как выбрать оптимальный стандарт для сценария. Вы также изучите использование таких компонентов, как Ограничения по 1Py4-адресам и именам домена (IPv4 Address And Domain Restrictions) для дальнейшего обеспечения безопасности веб-служб.

Изучив материал этого занятия, вы сможете:

- Описать опции проверки подлинности, доступные для веб-служб IIS.
- Настроить опции проверки подлинности для веб-сервера, веб-сайта и веб-приложения.
- Осуществлять реализацию и управление правилами авторизации (Authorization Rules) для ограничения доступа к конкретному веб-содержимому.
- Настроить сертификаты сервера и включить функциональность SSL (Secure Sockets Layer) для сервера IIS.
- Создавать ограничения по 1Py4-адресам и именам домена (IPv4 Address And Domain Restrictions) для ограничения доступа к веб-серверу IIS и управлять созданными ограничениями.
- Конфигурировать уровни доверия .NET (.NET Trust Levels) на основе требований конкретных веб-приложений.

Расчетная продолжительность занятия составляет 75 мин.

Управление проверкой подлинности IIS

Проверка подлинности, или аутентификация, — это процесс подтверждения своей идентичности пользователем или компьютером. При работе с такими веб-серверами, как IIS, параметры и опции проверки подлинности определяют, каким образом пользователи будут предоставлять свои учетные данные для получения доступа к содержимому веб-сервера. В IIS реализованы многочисленные методы обеспечения безопасности содержимого. По умолчанию анонимным пользователям разрешен доступ к содержимому новых веб-сайтов, веб-приложений и виртуальных каталогов. Это означает, что пользователям не потребуется предоставлять данные аутентификации для извлечения информации. На этом занятии вы изучите режимы проверки подлинности, поддерживаемые в IIS, и принципы их конфигурирования.

Анонимная проверка подлинности

При работе с веб-серверами многих типов пользователи должны иметь возможность получать доступ хотя бы к странице по умолчанию или некоторому содержимому без прохождения проверки подлинности. При включении роли Веб-сервер (IIS) (Web Server (IIS)) с опциями по умолчанию для сайта Default Web Site и его содержимого включается анонимная проверка подлинности. Эта проверка проводится для обеспечения доступа к содержимому, предназначенному

для всех пользователей, подключающихся к веб-серверу. В качестве примера можно привести веб-страницу IIS по умолчанию для сайта Default Web Site. При получении запроса содержимого IIS автоматически использует конкретную идентичность для обработки запроса. По умолчанию в анонимной проверке подлинности используется встроенная учетная запись IUSR, как показано на рис. 6-20. Пока эта пользовательская учетная запись располагает разрешением доступа к содержимому (на основе разрешений NTFS), обработка запроса будет выполняться автоматически.

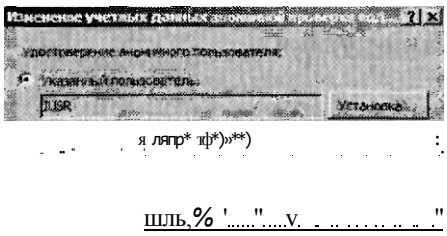


Рис. 6-20. Изменение учетных данных анонимной проверки подлинности

Команду Установка (Set) можно использовать с целью обеспечения пользовательского имени и пароля для другой учетной записи. Ее удобно применять в случаях использования разных разрешений NTFS для различного веб-содержимого. И наконец, параметр Удостоверение пула приложений (Application Pool Identity) указывает IIS использовать те же учетные данные, которые применяются к пулу приложений для веб-сайта или веб-приложения.

Если всем пользователям должно быть доступно все содержимое веб-сервера, никакой дополнительной конфигурации проверки подлинности не потребуется. Однако обычно доступ к некоторому содержимому сервера все же ограничивается. FlanpuMep, сервер интрасети может включать веб-приложение или виртуальный каталог, предназначенный только для отдела кадров. Для ограничения доступа к содержимому можно использовать разрешения NTFS. Если учетные данные, отконфигурированные для анонимной проверки подлинности, не позволяют получить доступ к содержимому, данные не будут автоматически возвращаться пользователю. Обычно для обеспечения возможности доступа к содержимому для авторизованных пользователей включается один из других методов проверки подлинности.

ПРИМЕЧАНИЕ Упрощение системы защиты содержимого

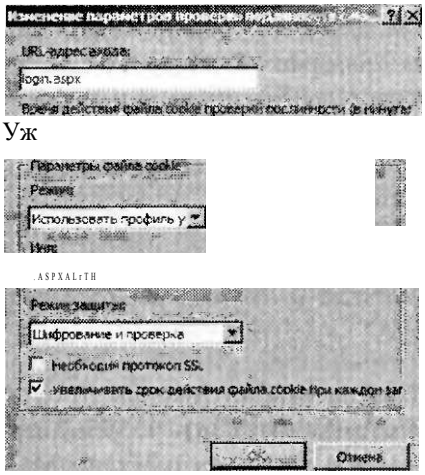
Па всех веб-серверах есть некоторое содержимое, доступ к которому не должны получать все пользователи. В качестве примеров можно привести содержимое системных папок (например, папка Windows) и исходный код приложений, который хранится внутри папок с веб-содержимым. Значения Запретить (Deny) для разрешений NTFS гарантируют, что пользователи не смогут применять анонимные учетные данные для получения доступа к содержимому. Если вы для такой проверки подлинности при получении доступа к различному содержимому используете множество учетных записей, лучше всего будет создать группу, содержащую эти учетные записи. Затем вы сможете запретить разрешения для группы, что позволит существенно упростить администрирование.

Проверка подлинности с помощью форм

Распространенная методика обеспечения безопасности состоит в использовании стандартных форм HTTP для передачи учетных данных. В проверке подлинности с помошыо форм используется ответ HTTP 302 Вход-перенаправление (Login/Redirect), перенаправляющий пользователей на страницу входа в систему. Как правило, на странице входа пользователи могут указать имя и пароль. После ввода на странице входа выполняется подтверждение учетных данных. В случае успешного подтверждения учетных данных пользователи перенаправляются к содержимому, которое запрашивали. По умолчанию данные формы пересылаются в незашифрованном формате. Для обеспечения безопасности передачи учетных данных следует включить шифрование с иомощыо SSL или TLS.

Проверка подлинности с помощью форм чаще всего применяется в Интернете по причине отсутствия каких-либо требований к веб-браузеру. Веб-разработчики, как правило, создают собственные страницы входа в систему. Подтверждение данных входа часто выполняется в соответствии с данными учетных записей, которые хранятся в реляционной базе данных (для интернет-сайтов), или доменом служб каталогов Active Directory.

Параметры по умолчанию для проверки подлинности с помощью форм используются веб-приложениями ASP.NET. Параметры проверки подлинности с помощью форм можно изменять (рис. 6-21). Основным параметром является URL-адрес входа (Login URL). Он указывает имя веб-страницы, на которую будут направляться пользователи при попытках получить доступ к защищенному содержимому.



Уж

Рис. 6-21. Настройка параметров проверки подлинности с помощью форм

После предоставления пользователем учетных данных для проверки подлинности при выполнении каждого запроса с веб-браузера на веб-сервер пересылаются данные cookies. Таким образом, клиент может удостовериться в проверке подлинности веб-сервером. Файлы cookies необходимы по причине того, что протокол HTTP не запоминает состояния. В разделе Параметры файла cookie

(Cookie Settings) можно настроить режим использования сайтом файлов cookies. Опция Режим (Mode) располагает следующими значениями:

- Не использовать файлы cookie (Do Not Use Cookies);
- Использовать файлы cookie (Use Cookies);
- ш Автовыбор (Auto Detect);
- Использовать профиль устройства (Use Device Profile).

Выбор оптимального параметра зависит от требований веб-браузера (например, должны ли пользователи веб-сайта включить поддержку файлов «cookies») и требований веб-приложения или содержимого.

Проверка подлинности с запросом

Пользователи, которые получают доступ к защищенным веб-сайтам в Интернете, обычно вводят пользовательское имя и пароль или выполняют такие действия, как размещение онлайновых заказов. В IIS поддерживаются три метода обеспечения безопасности для пользователей, которые пытаются получить доступ к веб-содержимому, защищенному с помощью разрешений файловой системы. Каждый из этих трех методов отправляет пакет-запрос HTTP 401, в котором пользователю предлагается предоставить учетные данные. Далее описаны эти методы.

- **Обычная проверка подлинности (Basic Authentication)** Пересылка пакета-запроса проверки подлинности веб-пользователям с применением стандартного метода, поддерживаемого всеми веб-браузерами. Основной недостаток обычной проверки подлинности состоит в том, что предоставляемые пользователям данные кодируются, но не шифруются. Это означает, что в случае перехвата информации можно без труда получить пользовательское имя и пароль. Для безопасной передачи данных проверки подлинности следует обеспечить безопасность сети (например, в среде центра данных) или включить шифрование с использованием протокола SSL или TLS.
- **Сжатая проверка подлинности Дайджест (Digest Authentication)** При такой проверке подлинности для обеспечения метода защищенной передачи учетных данных используется протокол HTTP 1.1. Для аутентификации пользователя используется контроллер домена Windows. Потенциальный недостаток такой проверки подлинности состоит в том, что веб-браузеры клиентов должны поддерживать протокол HTTP 1.1. Текущие версии распространенных браузеров поддерживают этот метод, так что сжатую проверку подлинности можно использовать для Интернета и интрасетей.
- **Проверка подлинности Windows (Windows Authentication)** Обеспечивает защищенную проверку подлинности, которую легко администрировать. . В ней протокол аутентификации NTLM или Kerberos применяется для подтверждения реквизитов пользователей в соответствии с доменом Windows или локальной базой данных безопасности. Проверка подлинности Windows изначально предназначена для использования в интрасетях, где клиенты и веб-серверы являются членами одного домена. Для упрощения администрирования системные администраторы могут управлять доступом к содержимому с помощью доменных учетных записей Active Directory.

Один из важных нюансов методов проверки подлинности с запросом связан с их взаимодействием с анонимной проверкой подлинности. Чтобы от пользователей требовался ввод учетных данных перед получением доступа к веб-содержимому, нужно отключить анонимную проверку подлинности. Если анонимная проверка подлинности останется включенной, содержимое, не защищенное с помощью разрешений файловой системы, будет автоматически доступно для пользователей без аутентификации. Кроме того, вы не сможете включить для одного содержимого оба метода проверки подлинности с помощью форм и с использованием пакетов-запросов.

Олицетворение ASP.NET

Олицетворение представляет собой метод обеспечения безопасности, где обработка веб-запроса IIS выполняется с использованием данных безопасности учетной записи конкретного пользователя или пользователя, получающего доступ к сайту. В случае отключения олицетворения ASP.NET (по умолчанию) контекст безопасности для обработки запросов зависит от учетной записи, используемой веб-приложением. Включив олицетворение, вы сможете указать пользовательскую учетную запись для определения контекста безопасности (рис. 6-22). Чтобы указать пользовательское имя и пароль, щелкните кнопку Установка (Set).

Для настройки олицетворения ASP.NET можно также использовать опцию Прошедший проверку пользователь (Authenticated User). Данный параметр указывает, что для предоставления доступа к содержимому будут использоваться разрешения безопасности пользователя, прошедшего проверку подлинности (с применением еще одной опции аутентификации). Этот параметр удобно использовать вместе с разрешениями файловой системы для конкретных пользователей и групп. Такой способ проверки подлинности лучше всего применять в средах с поддержкой относительно небольшого количества пользователей, например веб-серверы иитрасети уровня отдела.

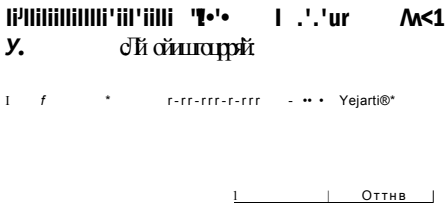


Рис. 6-22. Настройка параметров олицетворения ASP.NET

Проверка подлинности с помощью клиентских сертификатов

Помимо других методов проверки подлинности в 11S обеспечена поддержка клиентских сертификатов, подтверждающих идентичность веб-пользователя. Для поддержки этого метода пользователи должны установить на своих компьютерах сертификаты безопасности. При получении запроса защищенного содержимого IIS автоматически подтверждает идентичность клиента, запрашивая данные сертификата.

Существует три основных режима использования клиентских сертификатов.

- **Сопоставления -«один-один»** В этой конфигурации веб-сервер должен содержать копию клиентского сертификата, используемого каждым компьютером, который будет получать доступ к конкретному содержимому. Для подтверждения запроса сервер сравнивает свою копию сертификата с копией, предоставленной клиентом.
- **Сопоставления -«множество-один»** Довольно часто управлять сертификатами всех возможных веб-пользователей на сервере непрактично. Сопоставления «множество-к-одному» зависят от веб-сервера, выполняющего проверку подлинности с применением определенной информации из клиентского сертификата. В качестве распространенного примера можно привести подтверждение данных организации в сертификате для обеспечения гарантии того, что запрашивающий пользователь входит в доверенную компанию.
- **Сопоставления Active Directory** Службы сертификации Active Directory (Active Directory Certificate Services) могут значительно упростить создание клиентских сертификатов и управление ими. Для включения этого метода организация должна вначале установить собственную инфраструктуру на основе сертификатов.

Этот метод чаще всего используется в средах, где системные администраторы управляют компьютерами конечных пользователей, поскольку требовать сертификаты для общедоступных веб-сайтов и приложений в Интернете попросту нецелесообразно.

Требования проверки подлинности

Управление проверкой подлинности IIS осуществляется обработчиками и модулями. Конкретные опции проверки подлинности для веб-сервера зависят от установленных служб ролей веб-сервера (IIS). Далее приведен список доступных служб ролей:

ш Обычная проверка подлинности (Basic Authentication);

- Windows - проверка подлинности (Windows Authentication);
- Дайджест - проверка подлинности (Digest Authentication);
- Проверка подлинности с сопоставлением сертификата клиента (Client Certificate Mapping Authentication);
- Проверка подлинности с сопоставлением сертификата клиента IIS (IIS Client Certificate Mapping Authentication).

Для того чтобы добавить или удалить службу ролей, связанную с безопасностью (рис. 6-23), откройте Диспетчер сервера (Server Manager), разверните узел Роли (Roles), щелкните правой кнопкой мыши Веб-сервер (IIS) (Web Server (IIS)) и примените команду Добавить службы ролей (Add Role Services) или Удалить службы ролей (Remove Role Services). Поскольку службы ролей влияют на доступные опции проверки подлинности всего веб-сервера, определите требования всех веб-приложений и веб-содержимого на сервере.

Помимо параметров служб ролей для каждого метода проверки подлинности требуется конкретный модуль, как описано в табл. 6-1. Более подробная информация об управлении модулями представлена в разделе «Управление обработчиками запросов» этой главы.

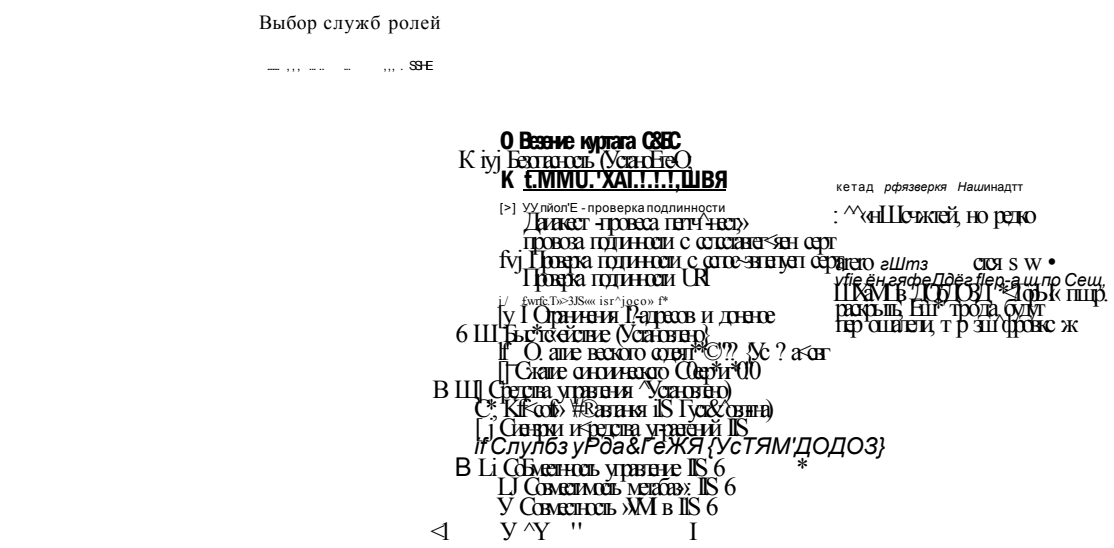


Рис. 6-23. Просмотр установленных служб ролей, связанных с проверкой подлинности

Табл. 6-1. Методы проверки подлинности IIS и их требования

Проверка подлинности	Требуемые модули
Анонимная	Anonymous AuthM odule
Олицетворение ASP.NET	ManagedEngine
Обычная	BasicAuthModule TokenCacheModule
Клиентские сертификаты	HsClientCertificatelVIappinglVIodule
Клиентские сертификаты (Сопоставление Active Directory)	CertificateMappingAuthenticationModule
Дайджест	DigestAuthModule
Формы	FormsAuthenticationModule
Windows	WindovvsAuthenticationModule

Настройка параметров проверки подлинности

С помощью иерархии веб-объектов IIS можно определять параметры конфигурации. Параметры проверки подлинности можно конфигурировать для объектов на следующих уровнях:

- веб-сервер;
- веб-сайты;

- веб-приложения;
- виртуальные каталоги;
- физические папки и отдельные файлы.

Параметры проверки подлинности, определяемые на более высоких уровнях (как, например, для веб-приложения), будут автоматически использоваться для объектов нижерасположенных уровней. Этот метод упрощает управление параметрами для множества веб-сайтов, веб-приложений и их содержимого.

Чтобы с помощью Диспетчера служб IIS (IIS Manager) отконфигурировать параметры проверки подлинности, в левой панели выберите соответствующий объект и в режиме Просмотр возможностей (Features View) дважды щелкните элемент Проверка подлинности (Authentication). На рис. 6-24 показаны опции проверки подлинности по умолчанию для объекта Default Web Site.

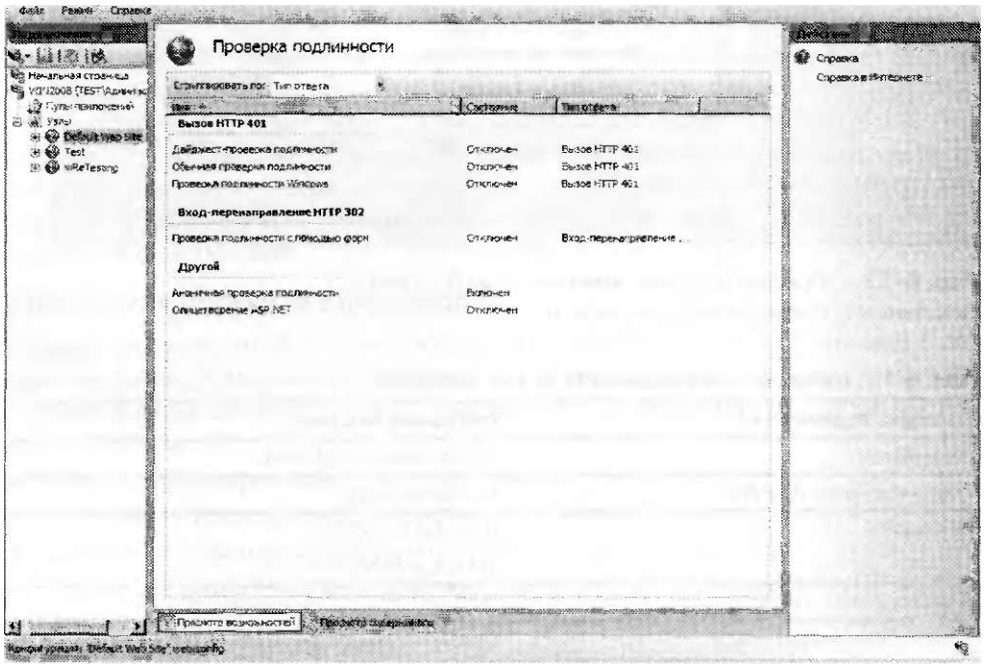


Рис. 6-24. Просмотр опций проверки подлинности для объекта Default Web Site в диспетчере служб IIS

По умолчанию отобразится полный список доступных опций проверки подлинности, сгруппированных по используемому типу ответа. Каждый метод можно включать и отключать с помощью команд Включить (Enable) и Отключить (Disable) в панели Действия (Actions). Кроме того, некоторые опции проверки подлинности обеспечивают дополнительные команды. По умолчанию при включении или отключении опции проверки подлинности этот параметр будет применен ко всем объектам и содержимому иерархии IIS на более низких уровнях. Вы можете изменять такое поведение, явным образом включая и отключая методы проверки подлинности на более низких уровнях.

Для проверки параметров проверки подлинности доступ к содержимому всегда следует тестировать с помощью веб-браузера. В некоторых случаях для проверки подлинности может потребоваться использовать второй компьютер. Например, если вы уже подключены к компьютеру Windows Server 2008 как член группы администраторов и хотите протестировать проверку подлинности Windows, подключение следует выполнять на еще одном компьютере в среде, чтобы автоматическая проверка подлинности не повлияла на результаты тестирования.

Управление правилами авторизации URL

Авторизация представляет собой метод, с помощью которого системные администраторы могут определить ресурсы и содержимое, доступные для конкретных пользователей. Подтверждение идентичности пользователя выполняется во время проверки подлинности. После подтверждения идентичности правила авторизации определяют действия, которые разрешено выполнять пользователю или компьютеру. В IIS реализованы методы обеспечения безопасности для содержимого различных типов с применением авторизации на основе URL. Поскольку запросы веб-содержимого выполняются, как правило, с использованием URL, включающего полный путь к запрашиваемому содержимому, вы без труда можете конфигурировать параметры авторизации с помощью Диспетчера служб IIS (IIS Manager).

Создание правил авторизации URL

Для выполнения авторизации URL должен быть включен модуль UrlAuthorizationModule. Правила авторизации можно конфигурировать на уровне веб-сервера, для конкретных веб-сайтов, веб-приложений или файлов (в зависимости от полного пути URL). Правила авторизации URL используют наследование, так что объекты на нижерасположенных уровнях наследуют параметры авторизации родительских объектов (если их не заменить явным образом).

Для настройки параметров авторизации выберите в левой панели Диспетчера служб IIS (IIS Manager) соответствующий объект и в режиме Просмотр возможностей (Features View) дважды щелкните элемент Правила авторизации (Authorization Rules). На рис. 6-25 показан пример набора правил, отконфигурированных для веб-сайта.

Существует два типа правил: Разрешить (Allow) и Запрет (Deny). Новые правила можно создавать с помощью команд Добавить разрешающее правило (Add Allow Rule) и Добавить запрещающее правило (Add Deny Rule) в панели Действия (Actions). Опции для обоих типов аналогичны (рис. 6-26). При создании нового правила определяются пользователи, к которым применяется правило. Для этого можно использовать следующие опции:

ш Все пользователи (All Users);

- Все анонимные пользователи (All Anonymous Users);
- Указанные роли или группы пользователей (Specific Roles Or User Groups);
- Указанные пользователи (Specific Users).

При указании пользователей или групп, к которым будет применено правило, соответствующие имена можно ввести в списке с разделительными запятыми.

Конкретные пользователи и группы определяются с помощью поставщиков ролей .NET. Этот стандартный компонент доступен для веб-разработчиков ASP.NET. Разработчики могут создавать собственные роли и пользовательские учетные записи, а также определять разрешения в своих приложениях. Обычно информация о пользователях и ролях хранится в реляционной базе данных или службе каталогов, например Active Directory.

Рис. 6-25. Правила авторизации для веб-сайта

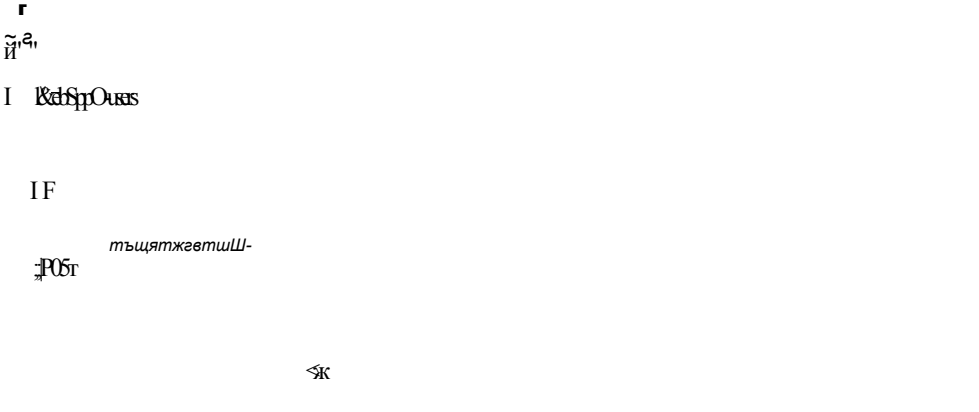


Рис. 6-26. Создание нового разрешающего правила для веб-приложения

Помимо выбора пользователей и ролей правило авторизации можно конфигурировать на основе указанных команд HTTP. Например, если правило требуется применить только для команд POST (которые, как правило, используются для передачи информации с веб-браузера на веб-сервер), в конфигурацию правила следует добавить лишь команду POST.

Управление наследованием правил

Как уже говорилось ранее в этом разделе, правила авторизации автоматически наследуются объектами на более низких уровнях. Такой подход удобно использовать в случае иерархической организации веб-сайта и веб-содержимого на основе назначенных пользователей и групп. В столбце Тип элемента (Entry Type) указано, унаследовано ли правило с более высокого уровня или определено локально. Диспетчер служб IIS (IIS Manager) не позволяет создавать дублирующие правила. Вы можете удалять правила на любом уровне, включая типы элементов Унаследовано (Inherited) и Локальный (Local).

Настройка сертификатов сервера

Для обеспечения безопасности требуется проверить идентичность веб-сервера, а затем защитить коммуникации между веб-клиентом и веб-сервером. Во многих сетях, особенно в Интернете, обеспечение защищенных коммуникаций для передачи уязвимых данных является ключевой задачей. Сертификаты сервера предназначены для обеспечения дополнительной безопасности веб-служб. В IIS обеспечена встроенная поддержка для создания сертификатов сервера и управления ими, а также для включения зашифрованных коммуникаций. В настоящем разделе мы рассмотрим принципы конфигурирования и включения этих опций.

Сертификаты сервера

Сертификаты сервера представляют метод, с помощью которого веб-сервер может подтвердить свою идентичность для клиентов, которые пытаются получить к нему доступ. Основной способ обеспечения такой функциональности состоит в создании иерархии доверенных центров сертификации (Certificate Authority, CA). В Интернете подтверждение серверов и генерирование сертификатов обеспечивается множеством сторонних организаций. Если пользователи доверяют этим организациям, они также должны иметь возможность расширить доверие для подтвержденных веб-сайтов. Организации также могут создавать собственные центры сертификации для внутренних серверов. Это позволяет системным администраторам подтверждать развертывания новых серверов с использованием механизма обеспечения безопасности.

Процесс получения сертификата сервера состоит из трех основных этапов.

- **Генерирование запроса сертификата** На веб-сервере создается запрос вместе с текстовым файлом, содержащим информацию о запросе в зашифрованном формате. Запрос сертификата уникальным образом идентифицирует веб-сервер.
- **Представление запроса сертификата в центре сертификации** Запрос сертификата передается в центр сертификации (с помощью защищенного веб-сайта или по электронной почте). Затем центр сертификации проверяет данные запроса и создает доверенный сертификат сервера.

- Получение и установка сертификата на веб-сервере Центр сертификации возвращает сертификат запрашивающей стороне (обычно в виде небольшого текстового файла). Затем этот файл можно импортировать в конфигурацию веб-сервера для включения защищенных коммуникаций.

К СВЕДЕНИЮ Сертификаты клиента и сертификаты сервера
Технологию на основе сертификатов можно использовать па веб-сервере несколькими способами. Сертификаты клиента используются для проверки доступа к веб-серверу путем подтверждения клиентов. В этом случае клиент располагает сертификатом, который может подтвердить сервер. Такой способ мы обсуждали ранее па этом занятии. Сертификаты сервера устанавливаются на компьютерах с веб-серверами с целью подтверждения их идентичности для веб-клиентов и включения защищенных коммуникаций. Сертификаты клиентов, как правило, используются в интрасетях и экстрасетях, а сертификаты сервера применяются для обеспечения безопасности веб-серверов всех типов.

Создание запроса сертификата Интернета

Для получения сертификата с целью его применения на веб-сервере IIS используется Диспетчер служб IIS (IIS Manager). Чтобы начать этот процесс, подключитесь к веб-серверу Windows Server 2008 и в режиме Просмотр возможностей (Features View) дважды щелкните элемент Сертификаты сервера (Server Certificates). Откроется окно, показанное на рис. 6-27.

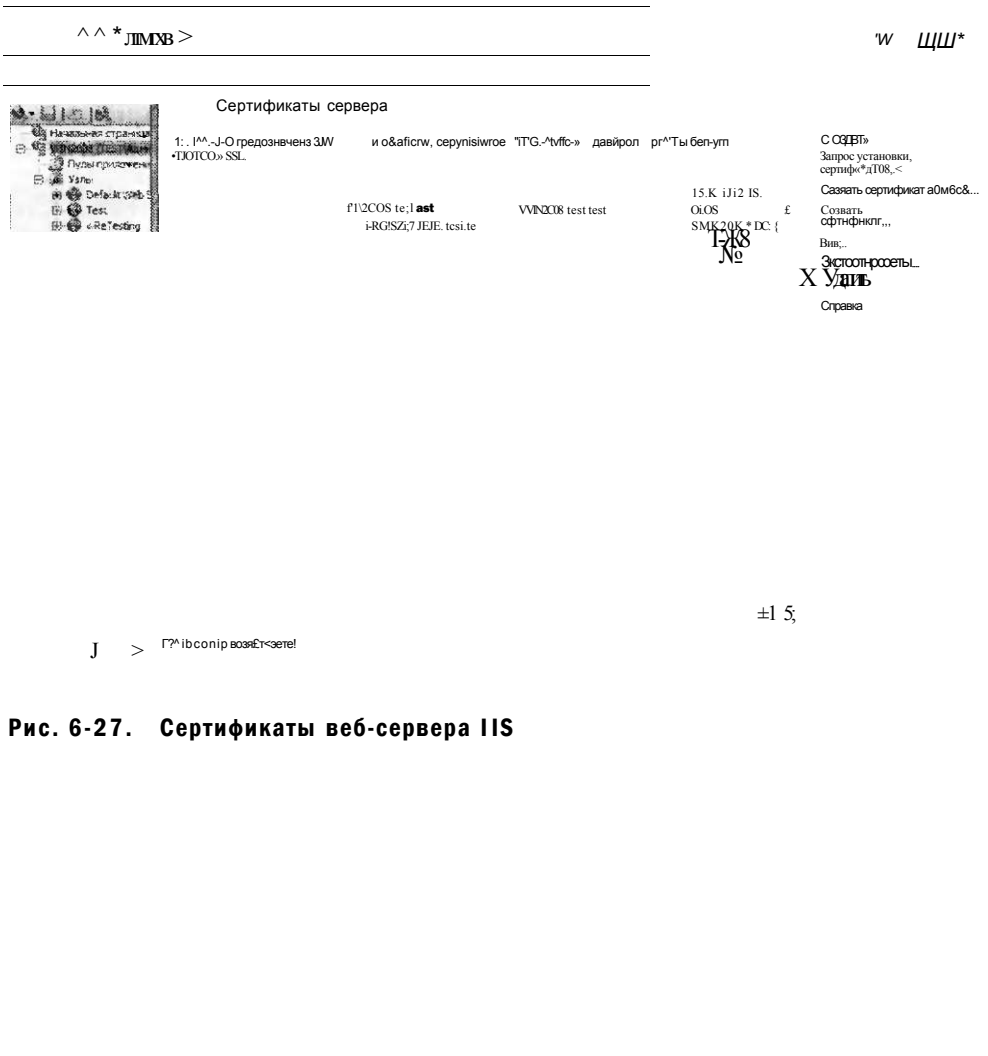


Рис. 6-27. Сертификаты веб-сервера IIS

Отметим, что запросы сертификатов генерируются лишь на уровне веб-сервера, но не для таких объектов, как веб-сайты и веб-приложения.

В зависимости от конфигурации локального сервера некоторые сертификаты уже могут быть включены по умолчанию. В панели Действия (Actions) находятся команды для создания новых сертификатов.

Для создания запроса сертификата щелкише команду Создать запрос сертификата (Create Certificate Request). Как показано на рнс. 6-28, вам потребуется указать информацию о запрашивающей организации.

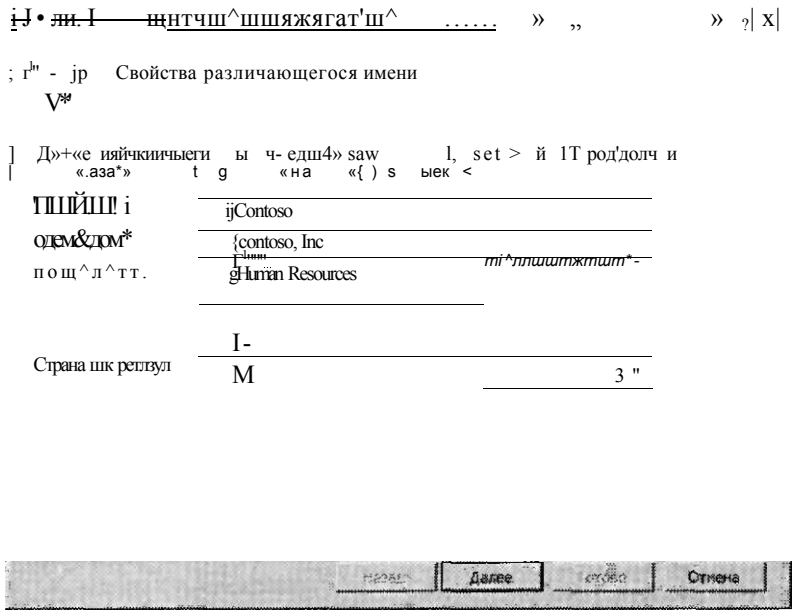


Рис. 6-28. Свойства различающегося имени

Эта информация будет использоваться центром сертификации для принятия решения о выдаче сертификата. Поэтому она должна быть точной. Например, в поле Организация (Organization) следует указать полное официальное название запрашивающей компании. В поле Полное имя (Common Name), как правило, указывается доменное имя, которое будет использоваться вместе^ сертификатом.

На втором этапе создания запроса сертификата требуется выбрать метод шифрования, который будет использоваться для обеспечения безопасности запроса сертификата, как показано на рис. 6-29. Для параметра Поставщик служб шифрования (Cryptographic Service Provider) следует выбрать метод, приемлемый для центра сертификации. (Поставщик по умолчанию Microsoft RSA SChannel Cryptographic Provider приемлем для большинства сторонних центров сертификации.) Параметр Длина ключа (Bit Length) указывает степень строгости шифрования. Чем больше длина ключа, тем больше времени потребуется для обработки, однако при этом обеспечивается гораздо более высокий уровень безопасности.

На следующем этапе запрос сертификата сохраняется в файле. Вы можете указать полный путь и имя файла для сохранения запроса. Запрос сохраняется в текстовом файле, содержащем зашифрованную информацию.

Далее требуется представить запрос сертификата в центре сертификации. Обычно веб-сайт издателя требует выгрузить запрос сертификата или скопировать и вставить содержимое запроса на защищенный веб-сайт. Издатель также запрашивает дополнительную информацию, такую как сведения об организации и оплате услуги.

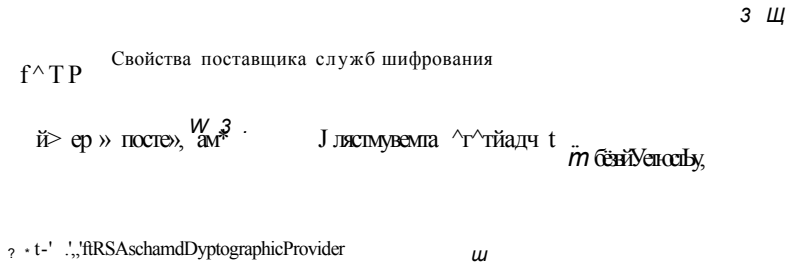


Рис. 6-29. Свойства поставщика служб шифрования

Запрос установки сертификата Интернета

Время обработки запроса сторонним центром сертификации может быть различным. После обработки и утверждения запроса центр сертификации пересылает ответ по электронной почте или через свой веб-сайт.

Этот ответ можно затем сохранить в текстовом файле и предоставить его в IIS для завершения процесса. Для этого в режиме Просмотр возможностей (Features View) дважды щелкните элемент Сертификаты сервера (Server Certificates), выберите соответствующий запрос и в панели Действия (Actions) примените команду Запрос установки сертификатов (Complete Certificate Request). Вам будет предложено указать путь и имя файла ответа вместе с понятным именем, которое будет использоваться для администрирования, как показано на рис. 6-30.

Для ответа обычно используется имя файла с расширением .cer, однако вы также можете указать любой тип стандартного текстового файла.

Если запрос сертификата соответствует ответу, сертификат будет импортирован в конфигурацию IIS.

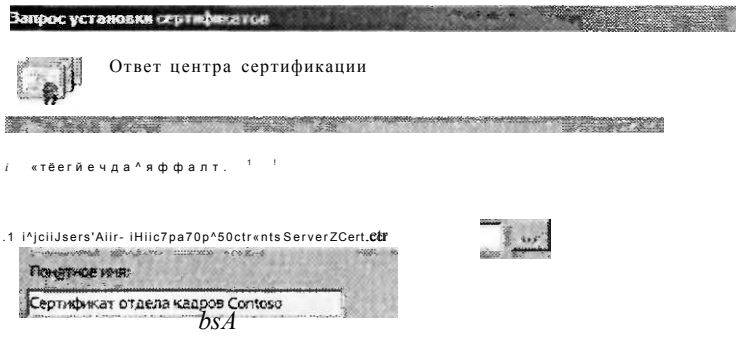


Рис. 6-30. Завершение процедуры создания запроса сертификата

Создание сертификатов других типов

Помимо стандартной процедуры запроса для создания сертификатов можно использовать еще две команды в панели Действия (Actions) для компонента Сертификаты сервера (Server Certificates).

Команда Создать сертификат домена (Create Domain Certificate) генерирует запрос внутреннего центра сертификации. Обычно эта процедура используется в организациях с собственной .инфраструктурой служб сертификации. Вместо того чтобы быть отправленным стороннему центру сертификации, запрос пересылается на внутренний сервер.

На рис. 6-31 показаны доступные опции. В текстовое поле Локальный центр сертификации (Specify Online Certificate Authority) нужно ввести путь и имя внутреннего сервера CA. В поле Понятное имя (Friendly Name) можно ввести описание назначения сертификата.

ПРИМЕЧАНИЕ Службы сертификации Active Directory

В Windows Server 2008 включена роль Службы сертификации Active Directory (Active Directory Certificate Services), позволяющая администраторам создавать собственную инфраструктуру безопасности на основе сертификатов. Реализация этих служб не входит в темы сертификационного экзамена 70—643 и не описана в данной книге. Более подробные сведения о настройке служб сертификации можно найти на странице Microsoft TechNet Active Directory Certificate Services по адресу *http://technet2.7nicrosoft.com/windowsseiTier2008/en/seiTier-7nanager/activedirectoryceitificateseivices.mspx.*

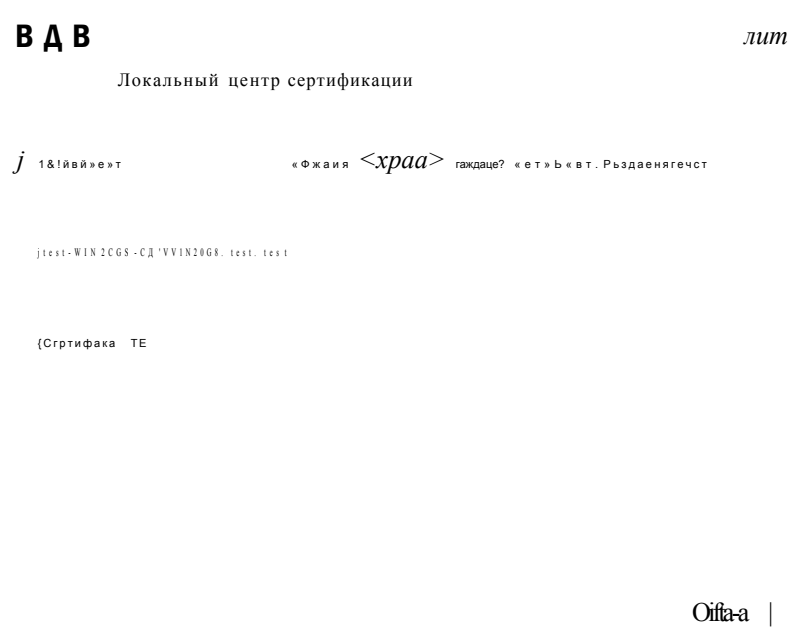


РИС. 6-31. Параметры локального центра сертификации для создания сертификата домена

Создание самозаверяющих сертификатов

Процесс создания сертификатов и управления ими обычно требует затрат на получение сертификата от доверенного стороннего центра сертификации. Хотя это необходимо для обеспечения безопасности в производственных средах, в средах разработок и тестирования используется более простой метод. С помощью самозаверяющих сертификатов функциональность инфраструктуры сертификации можно протестировать путем создания локальных сертификатов. Самозаверяющие сертификаты создаются в обход центров сертификации с применением команды Создать самозаверяющий сертификат (Create Self-Signed Certificate) в панели Действия (Actions). Диалоговое окно создания самозаверяющего сертификата показано на рис. 6-32.

В отличие от сертификатов других типов для самозаверяющего сертификата не нужно указывать сведения об организации. Объясняется это тем, что сам сертификат создается незамедлительно на локальном компьютере. При этом изначальный недостаток самозаверяющих сертификатов состоит в том, что пользователи, которые получают доступ к веб-серверу с использованием защищенного подключения, получат предупреждение о том, что сертификат не был выпущен доверенным центром сертификации. Именно это предупреждение показано на рис. 6-33.

Хотя обычно это не является проблемой в тестовых средах, тем не менее использовать самозаверяющие сертификаты для производственных веб-серверов не рекомендуется.

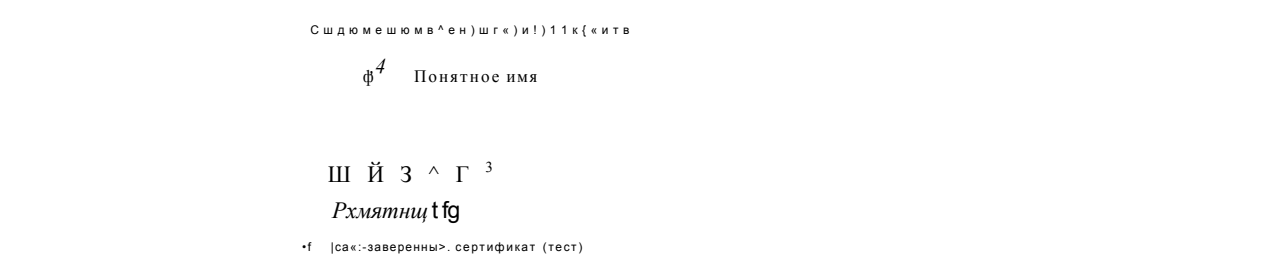


Рис. 6-32. Создание самозаверяющего сертификата

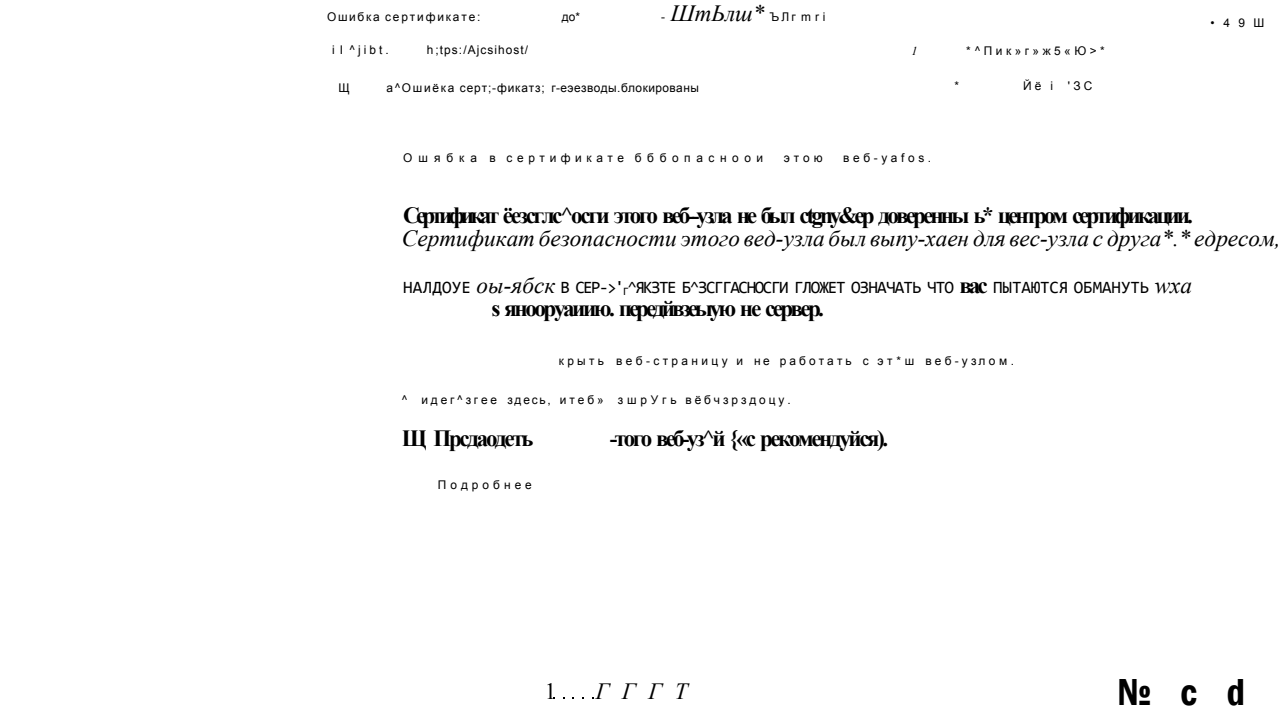


Рис. 6-33. Страница ошибки сертификата, открывающаяся при получении доступа к серверу, на котором используется самозаверяющий сертификат

Просмотр сведений о сертификате

Содержимое сертификата сервера включает различные сведения и свойства. Для того чтобы просмотреть эту информацию, дважды щелкните элемент в списке Сертификаты сервера (Server Certificates) для веб-сервера. Откроется показанное на рис. 6-34 диалоговое окно Сертификат (Certificate) с информацией о сертификате сервера. На вкладке Общие (General) указаны данные об издателе сертификата. Для сертификатов Интернета здесь отображается имя доверенного стороннего центра сертификации. Кроме того, для сертификатов указан срок действия.

На вкладке Состав (Details) указаны дополнительные свойства сертификата, включая метод шифрования. На вкладке Путь сертификации (Certification Path) отображается вся иерархия доверия для сертификата. В средах, располагающих центрами сертификации на нескольких уровнях, такую иерархию удобно применять для отслеживания всех используемых доверительных связей. Для того, чтобы сертификат был действительным, все уровни иерархии должны быть доверенными.

Веб-пользователи могут также просматривать данные безопасности сертификатов для подтверждения идентичности веб-сервера или организации. В Internet Explorer пользователи могут щелкнуть веб-страницу правой кнопкой мыши и применить команду Свойства (Properties). На вкладке Путь сертификации (Certification Path) можно просмотреть состояние сертификата и другие сведения (рис. 6-35).

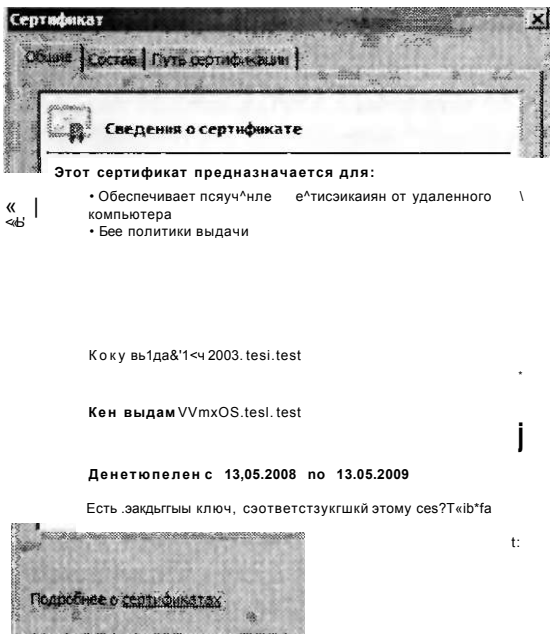


Рис. 6-34. Основные сведения о сертификате сервера

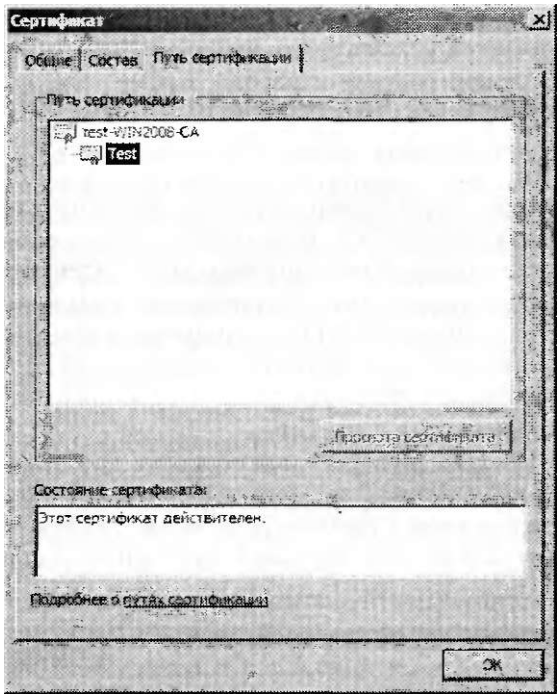


Рис. 6-35. Сведения о сертификате

Импорт и экспорт сертификатов

После установки на веб-сервере сертификат можно экспортировать в файл. Для этого в Диспетчере служб TIS (IIS Manager) щелкните сертификат правой кнопкой мыши и примените команду Экспортировать (Export). Затем вы можете указать папку для экспорта и имя файла с паролем, чтобы сертификат не могли установить неавторизованные пользователи (рис. 6-36). По умолчанию файлы экспортированных сертификатов используют расширение .pfx. Однако вы можете использовать любое иное расширение. Содержимое экспортированного сертификата шифруется, а для защиты также используется указанный пароль.

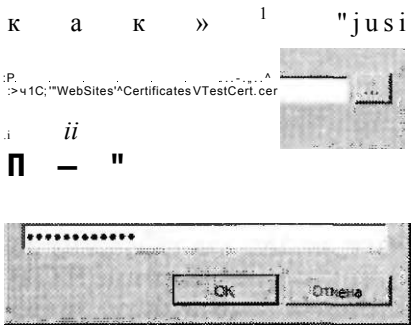


Рис. 6-36. Экспорт сертификата сервера с помощью диспетчера служб IIS

Для импорта сертификата в панели Действия (Actions) щелкните команду Импортировать (Import). Вам потребуется указать место хранения файла экспортированного сертификата в файловой системе и пароль. Кроме того, вы можете разрешить экспорт этого сертификата в дальнейшем.

Включение Secure Sockets Layer

После добавления сертификата сервера на веб-сервер IIS можно включить соединения с использованием SSL. Подключения SSL используют сертификаты для подтверждения идентичности веб-сервера. После подтверждения идентичности пользователи могут создавать защищенные подключения, применяя протокол HTTP Secure (IITTPS). По умолчанию HTTPS-подключепия используют TCP-порт 443. Чтобы модифицировать или включить протокол IITTPS для веб-сайта, требуется отконфигурпровать привязки узла. (Подробные сведения о настройке привязок узла содержатся в главе 5.)

С помощью Диспетчера служб IIS (IIS Manager) можно также требовать SSL-подключения для конкретных веб-сайтов. Для этого выберите веб-сайт, веб-ириложепие или каталог, а затем в режиме Просмотр возможностей (Features View) щелкните элемент Параметры SSL (SSL Settings). Доступные опции показаны на рис. 6-37.

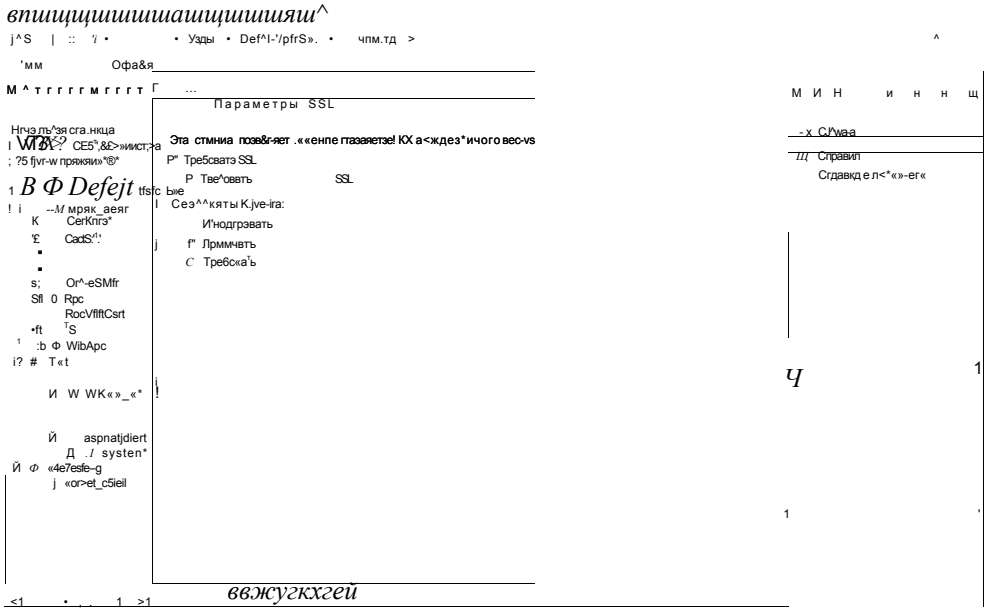


Рис. 6-37. Настройка параметров SSL для веб-приложения

С помощью флажков можно указать, требуется ли SSL для получения доступа к этому содержимому. Если этот флажок установлен, стандартные HTTP-подключения не разрешаются. При желании вы можете указать, будут ли сертификаты клиента игнорироваться, приниматься пли требоваться.

В целом сертификаты сервера и SSL обеспечивают стандартный метод защиты веб-подключений и содержимого веб-сервера. Поддержка сертификатов

сервера и SSL часто требуется для веб-серверов всех типов, содержащих уязвимую информацию.

Настройка ограничений по IP-адресам и именам домена

Хотя некоторые веб-серверы конфигурируются с целью обеспечения открытого доступа ко всему содержимому, довольно часто доступ требуется ограничить лишь конкретными группами пользователей. По умолчанию IIS конфигурируется для приема запросов всех подключений на основе параметров связывания узла, таких как IP-адрес и TCP-порт. С помощью Диспетчера служб IIS (IIS Manager) системные администраторы могут в дальнейшем ограничить доступ к веб-сайтам, реагируя лишь на запросы, исходящие из конкретных IP-адресов или доменов.

Первый шаг состоит в выборе уровня, на котором требуется назначить ограничения. Компонент Ограничения по 1Ру4-адресам и именам домена (IPv4 Address And Domain Restrictions) доступен на уровне сервера, сайта, веб-приложения, виртуального каталога и папки. Рекомендуется назначать ограничения на самом высоком уровне, где будут применяться параметры. Например, если все веб-приложения отдельного веб-сайта должны реагировать на запросы лишь от одного домена, конфигурируйте параметры запросов па уровне сайта. По умолчанию IIS ис включает никаких ограничений. Чтобы отконфигурировать параметры запросов, в левой панели Диспетчера служб IIS (IIS Manager) выберите соответствующий объект и в режиме Просмотр возможностей (Features View) дважды щелкните элемент Ограничения по IPvi-адресам и именам домена (IPv4 Address And Domain Restrictions). На рис. 6-38 показаны доступные параметры.

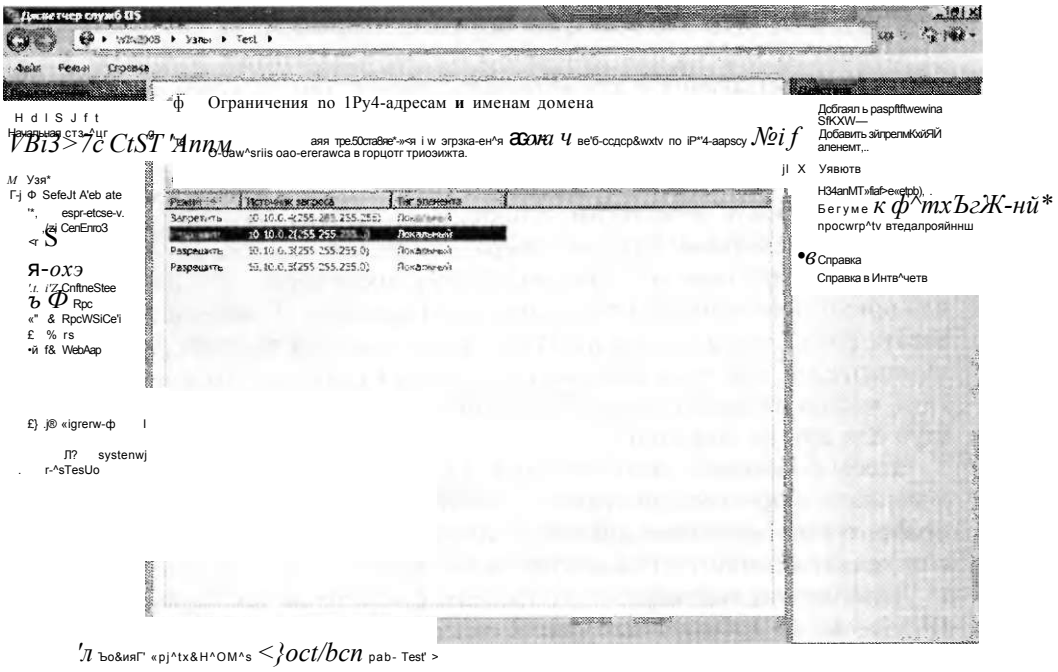


Рис. 6-38. Ограничения по 1Ру4-адресам и именам домена для веб-сайта

Добавление запрещающих и разрешающих элементов

Существует два основных типа элементов, которые можно добавлять в конфигурацию компонента Ограничения по 1Ру4-адресам и именам домена (IPv4 Address And Domain Restrictions). Разрешающие элементы указывают IP-адреса, которые могут получать доступ к веб-содержимому. Запрещающие элементы определяют адреса, которые не могут получать доступ к содержимому. При настройке ограничений IP-адресов можно указать отдельный IP-адрес или диапазон IP-адресов, как показано на рис. 6-39.

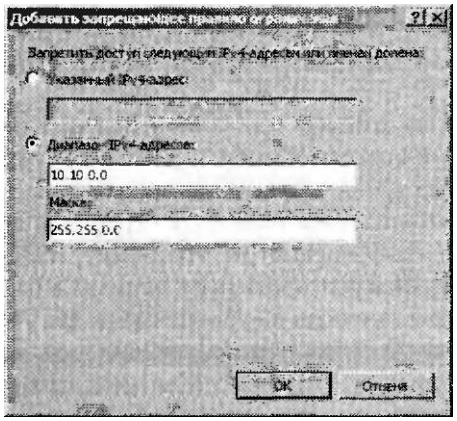


Рис. 6-39. Добавление ограничения по IP-адресам для веб-сайта

Для указания диапазона можно ввести исходный IP-адрес и маску подсети. Отдельные IP-адреса или диапазоны можно исключить с помощью дополнительных разрешающих и запрещающих правил. Тем не менее следует придерживаться простой конфигурации с целью упрощения процессов администрирования и управления.

Отдельные адреса удобно указывать лишь в тех случаях, когда доступ к сайту требуется лишь нескольким пользователям или доступ к содержимому требуется лишь нескольким другим серверам, например в средах, которые поддерживают распределенные веб-приложения на стороне сервера, не предназначенные для прямого пользовательского доступа. Диапазоны IP-адресов удобно использовать в тех случаях, когда доступ к среде требуется группам пользователей и компьютеров. Так, если пользователи отдела кадров расположены в одной подсети, можно разрешить доступ для этой подсети и в то же время запретить доступ для других подсетей.

Чтобы определить, назначен ли для адреса доступ, IIS оценивает все разрешающие и запрещающие правила. Приоритет запрещающих правил выше, чем приоритет разрешающих правил. Если пользователям запрещен доступ к сайту, они увидят страницу, показанную на рис. 6-40.

Дополнительный параметр определяет поведение по умолчанию для всех IP-адресов, не добавленных явно в список разрешающих н запрещающих элементов. По умолчанию 11S автоматически разрешает доступ с этих адресов. Чтобы изменить этот параметр, в панели Действия (Actions) щелкните коман-

ду Изменить параметры (Edit Feature Settings) и для параметра Доступ для неуказанных клиентов (Access For Unspecified Clients) выберите значение Запретить (Deny), как показано на рис. 6-41.

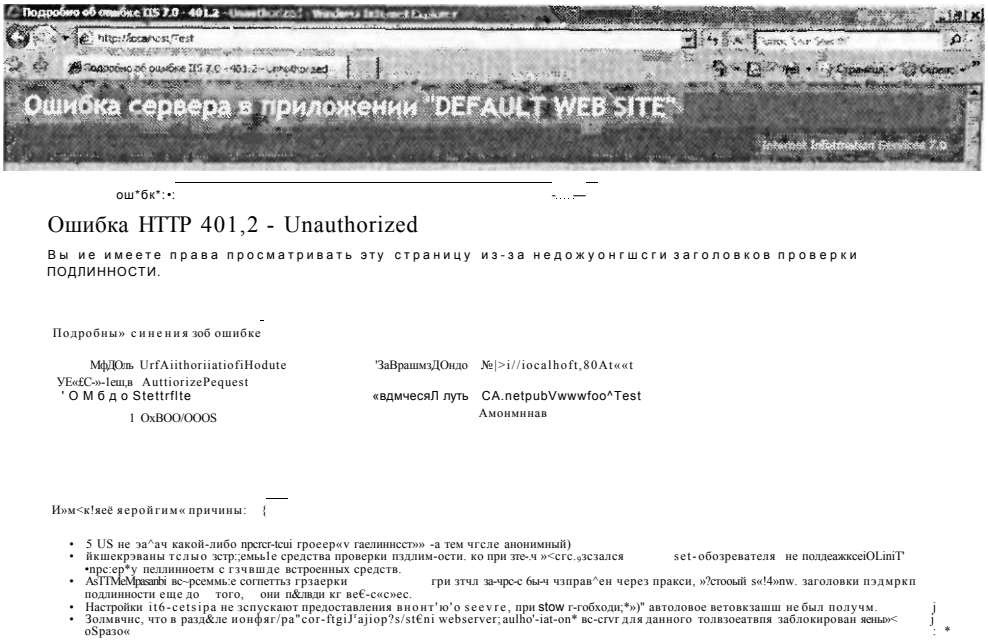


Рис. 6-40. Сообщение об ошибке, возвращаемое клиенту из-за ограничений доступа к сайту

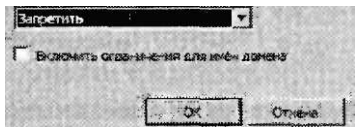


Рис. 6-41. Настройка параметров ограничений по 1Ру4-адресам и именам домена

Добавление доменных ограничений

Управлять доступом к веб-службам с помощью IP-адресов удобно при работе со списком хорошо известных входящих клиентов. Такая ситуация типична для интрасети и внутренней сетевой среды, где сетевые администраторы могут конфигурировать и управлять диапазонами IP-адресов. В других типах сценариев веб-серверов, например публичных веб-серверов или экстрасетей, управление диапазонами IP-адресов отнимает много времени и не является эффективным.

Альтернативой использованию ограничений на основе IP-адресов являются ограничения на основе доменных имен. Этот метод зависит от операции обратного просмотра или реверсивного поиска (reverse lookup) доменной системы именования DNS (Domain Name System). Когда пользователь пытается подключиться к IIS, веб-сервер выполняет реверсивный поиск DNS для разрешения IP-адреса запрашивающей стороны в доменное имя. Затем IIS с помощью этого доменного имени определяет, следует ли пользователю предоставлять доступ. Доменные ограничения по умолчанию отключены, поскольку они могут весьма значительно влиять на быстродействие сервера. Каждый запрос потребуется разрешать, что добавит значительную дополнительную нагрузку при обработке. Кроме того, указанные ограничения могут создать значительную нагрузку инфраструктуры DNS-сервера. Тем не менее с точки зрения управления эта возможность иногда может оказаться довольно полезной (особенно в мелкомасштабных сценариях).

Чтобы включить ограничения доменных имен, откройте для веб-сайта компонент Ограничения по 1Ру4-адресам и именам домена (IPv4 Address And Domain Restrictions), в панели Действия (Actions) щелкните команду Изменить параметры (Edit Feature Settings) и в окне, изображенном на рис. 6-41, установите флажок Включить ограничения для имен домена (Enable Domain Name Restrictions). На рис. 6-42 показано предупреждение, которое появляется при включении этой функции.

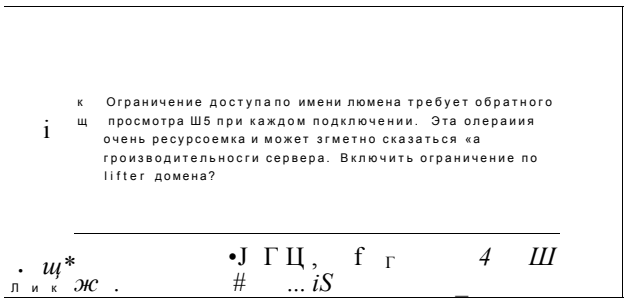


Рис. 6-42. Предупреждение, которое появляется при включении ограничений для имен домена

После включения ограничений для имен домена вы можете использовать команды Добавить разрешающий элемент (Add Allow Entry) и Добавить запрещающий элемент (Add Deny Entry), чтобы отконфигурировать правила. Как показано на рис. 6-43, в этих диалоговых окнах появится дополнительный параметр — Имя домена (Domain Name).

Как мы уже говорили ранее, поведение по умолчанию для запрещающих и разрешающих ограничений наследуется дочерними объектами от родительских. Если вы внесете явные изменения в параметры такого объекта, как веб-приложения, то для сброса параметров на этом уровне можете использовать команду Вернуться к унаследованным (Revert To Inherited), представленную в панели Действия (Actions). Унаследованные параметры будут зависеть от родительской иерархии.

СОВЕТ Подготовка к экзамену

Ограничения IP-адресов и доменных имен могут повысить общий уровень безопасности IIS, однако они не являются заменой управлению проверкой подлинности и параметрами авторизации. Используйте эти ограничения, если можете ограничить источник входящих запросов относительно небольшой группой пользователей и компьютеров. В целом ограничения IP-адресов и доменных имен следует использовать как часть общей стратегии безопасности веб-сервера.

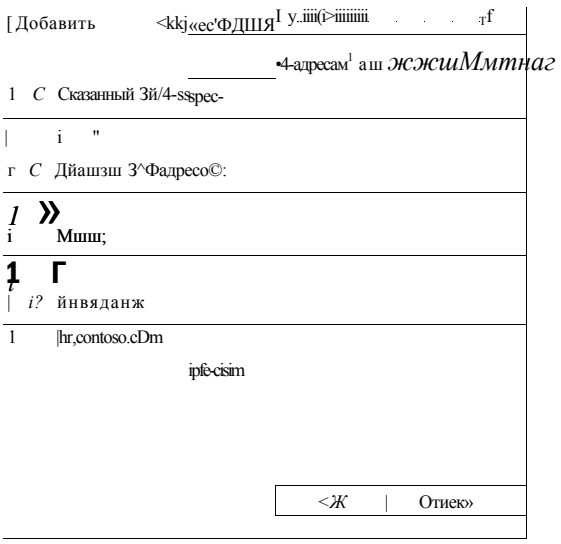


Рис. 6-43. Добавление ограничения имени домена для веб-сайта

Настройка уровней доверия .NET

Для реализации приложений веб-разработчиками технология .NET Framework обеспечивает строгий набор компонентов, включая веб-приложения (на основе платформы ASP.NET) и другие компоненты управляемого кода. С их помощью можно без труда создавать приложения .NET, которые смогут выполнять различные операции на компьютере. Однако из соображений безопасности важно ограничить разрешения, предоставляемые приложению .NET. Вредоносный или дефектный код может привести к возникновению самых разных проблем, начиная с неавторизованиого доступа к данным и заканчивая удалением содержимого.

Чтобы системные администраторы могли эффективно управлять разрешениями на производственных серверах, IIS поддерживает политику прав доступа кода Code Access Security (CAS). Политики CAS можно использовать для определения доступных операций в коде приложения .NET. Существует два основных типа конфигурации. Полное доверие обеспечивает для кода приложения ASP.NET все разрешения на компьютере. Для обеспечения совместимости этот параметр используется по умолчанию для приложений, созданных на основе .NET Framework 1.0, 1.1 и 1.2.

Уровни ограниченного доверия

Другой опцией политики CAS является ограниченное доверие, в котором ограничиваются действия, выполняемые приложениями .NET. Эти опции доступны для приложений, спроектированных на основе .NET Framework 1.1 и .NET Framework 2.0. При использовании ограниченного доверия включаются только те разрешения, которые необходимы для работы конкретного веб-приложения.

Уровни доверия можно конфигурировать на различных уровнях иерархии объектов веб-сервера, включая следующие:

- веб-сервер;
- веб-сайты;
- веб-приложения;
- виртуальные каталоги и физические папки.

Как и в случае с другими параметрами безопасности, уровни доверия, определенные на родительских уровнях иерархии веб-сервера, автоматически применяются к дочерним объектам. В принципе параметры уровней доверия .NET следует определять на самом высоком уровне в иерархии веб-сервера. Например, если веб-приложения отдельного веб-сайта не должны располагать полным набором прав доступа, эти параметры можно отконфигурировать на уровне сайта. Позже вы можете задать исключения, назначая необходимые параметры уровней доверия .NET конкретным веб-приложениям или папкам.

Уровни доверия .NET

Структура .NET Framework содержит много компонентов и операций, которые потенциально могут создавать проблемы безопасности на веб-сервере. Для обеспечения упрощенного метода настройки и применения параметров доверия в IIS определено пять встроенных уровней, которые можно применять к объектам IIS. Конкретные параметры для каждого уровня определены в различных файлах .config. (Более подробные сведения об использовании файлов конфигурации находятся в главе 5.) Параметры в этих файлах можно просматривать и модифицировать с помощью редактора XML или текстового редактора. В табл. 6-2 описаны уровни доверия и их параметры.

Табл. 6-2. Уровни доверия .NET

Уровень доверия .NET	Имя файла .config	Описание	Ограниченные действия
Full (internal)	N/A	Обеспечивает полный набор разрешений для приложения ASP.NET	N/A
High	Web_hightrust.config	Обеспечивает доступ к большинству действий на сервере и предназначен для надежных и протестированных веб-приложений	Вызов неуправляемого кода. Вызов обслуживаемых компонентов. Запись в журнал событий. Получение доступа к службам организации сообщений. Получение доступа к источникам данных ODBC, OLEDB и Oracle

Уровень доверия .NET	Имя файла .config	Описание	Ограниченные действия
Medium	Web_medium-trust.config	Обеспечивает дополнительные ограничения для веб-приложений, которым не требуется получать доступ к файловой системе или реестру	Получение доступа к файлам вне каталога приложения. Получение доступа к реестру. Обращения к сети или веб-службам
Low	Weblowtrust.config	Более высокая степень ограничений возможностей приложения	Запись в файловую систему. Вызов метода Assert (метод, который часто используется для тестирования кодов приложений)
Minimal	Web_minimal-trust.config	Разрешает лишь выполнение и запрещает доступ к другим ресурсам компьютера	Выполнение действий, для которых требуются дополнительные разрешения помимо выполнения (Execute)

СОВЕТ Подготовка к экзамену

При подготовке к сертификационному экзамену 70-643 ознакомьтесь с назначением каждого уровня доверия .NET. Вам не нужно запоминать конкретные ограничения, следует лишь помнить, какие типы операций рассматриваются как небезопасные. В отношении ограничений уровни доверия являются кумулятивными. Например, уровень Low добавляет дополнительные ограничения к уровню Medium и остальным вышерасположенным уровням. При сдаче экзамена перед выбором оптимального уровня доверия следует определить требования веб-приложения.

По умолчанию назначается уровень доверия Full (internal), который обеспечивает максимальную совместимость, но и является максимально уязвимым в отношении безопасности. По возможности назначайте более низкие уровни доверия .NET, чтобы код приложения запускался с минимальным набором разрешений. Довольно часто для определения требований и выполнения полного тестирования на различных уровнях безопасности нужно взаимодействовать с веб-разработчиками.

Настройка уровней доверия .NET

Для конфигурирования уровней доверия .NET с помощью Диспетчера служб IIS (IIS Manager) выберите объект, параметры которого вы хотите настроить, а затем в режиме Просмотр возможностей (Features View) дважды щелкните элемент Уровни доверия .NET (.NET Trust Levels). Откроется окно, показанное на рис. 6-44. Для того, чтобы изменить параметр, в раскрывающемся списке выберите соответствующий уровень и в панели Действия (Actions) щелкните команду Применить (Apply). Назначенный уровень доверия будет применен ко всем приложениям ASP.NET, запущенным на выбранном уровне в иерархии веб-сервера, а также ко всем дочерним объектам (если их параметры не заменить явным образом).

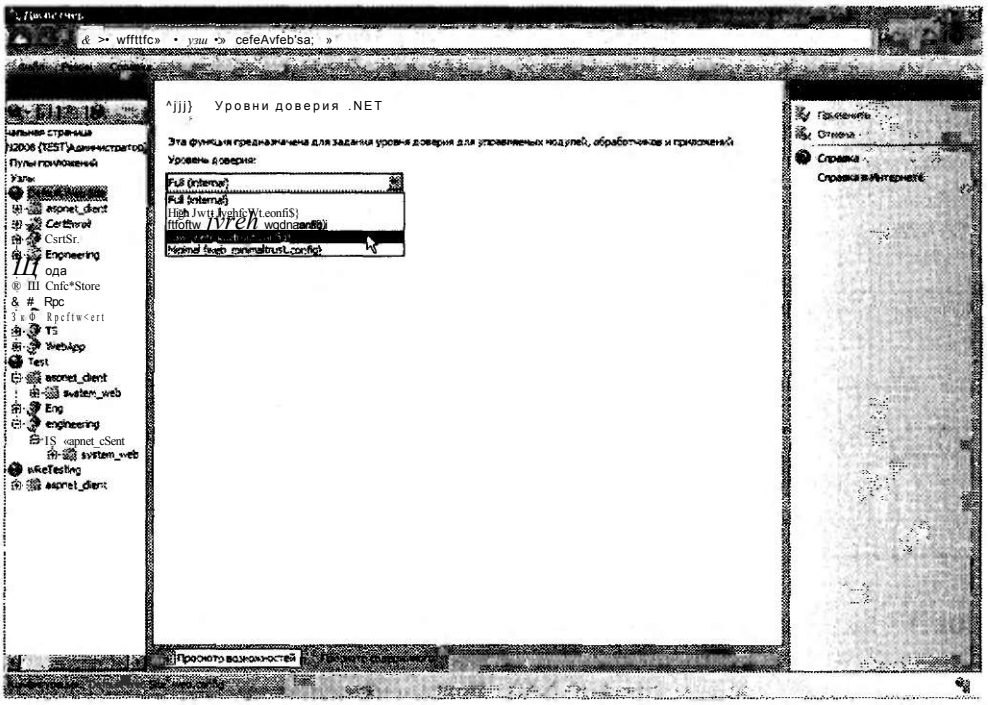


Рис. 6-44. Уровни доверия .NET для веб-сайта

Проверьте себя

1. Как управлять доступом пользователей к содержимому, не требуя какой-либо проверки подлинности?
2. Перечислите требования для включения SSL на веб-сервере IIS, который будет доступен в Интернете.
3. Как ограничить доступ к веб-приложению IIS лишь для ограниченного набора компьютеров?

Ответы

1. Если включена анонимная проверка подлинности, то при определении содержимого, для доступа к которому требуются учетные данные, IIS использует параметры разрешений файловой системы NTFS.
2. Чтобы обеспечить безопасность SSL для интернет-подключений, получите сертификат безопасности от доверенного стороннего центра сертификации и установите его на веб-сервере. Затем вы сможете включить SSL с помощью привязок узлов HTTPS.
3. Для того чтобы указать компьютеры, которые должны располагать доступом к веб-серверу IIS, можно использовать ограничения по IP-адресам. Вы также можете использовать и другие методы, включая применение клиентских сертификатов.

Практикум. Безопасность веб-серверов и веб-содержимого

В предложенных далее упражнениях вы займетесь обеспечением безопасности конкретного веб-содержимого. Предполагается, что у вас установлена роль Веб-сервер (IIS) (Web Server (IIS)) с параметрами по умолчанию и вы знаете, как добавлять службы ролей.

Упражнение 1. Управление параметами проверки подлинности и их тестирование

В этом упражнении вы настроите и проверите различные параметры проверки подлинности.

1. Войдите на сервер Server2 в качестве пользователя с административными привилегиями.
2. С помощью Диспетчера сервера (Server Manager) добавьте для роли Веб-сервер (IIS) (Web Server (IIS)) следующие службы ролей:
   - Обычная проверка подлинности (Basic Authentication);
   - Windows — проверка подлинности (Windows Authentication);
   - Дайджест — проверка подлинности (Digest Authentication);
   - Проверка подлинности URL (URL Authentication);
   - Ограничения IP-адресов и доменов (IP and Domain Restrictions).
3. Закройте Диспетчер сервера (Server Manager).
4. Откройте Диспетчер служб IIS (IIS Manager) и в левой панели выберите объект Default Web Site. В режиме Просмотр возможностей (Features View) дважды щелкните элемент Проверка подлинности (Authentication). Отметим, что в параметрах по умолчанию включена лишь анонимная проверка подлинности.
5. Щелкните объект Default Web Site, а затем в панели Действия (Actions) щелкните команду Обзор *:80(http) (Browse *:80(http)). Убедитесь, что отображается начальная страница IIS по умолчанию. Оставьте веб-браузер открытым и вернитесь к диспетчеру служб IIS.
6. В режиме Просмотр возможностей (Features View) вновь дважды щелкните элемент Проверка подлинности (Authentication). Выберите Проверку подлинности Windows (Windows Authentication), а затем в панели Действия (Actions) щелкните команду Включить (Enable).
7. Вернитесь к Internet Explorer и обновите веб-страницу. Отметим, что вам не будет предложено указать учетные данные для проверки подлинности. Причина состоит в том, что для сайта все еще включена анонимная проверка подлинности.
8. Вернитесь к Диспетчеру служб IIS (IIS Manager), выберите Анонимную проверку подлинности (Anonymous Authentication), а затем в панели Действия (Actions) щелкните команду Отключить (Disable).
9. Вернитесь к Internet Explorer и обратите внимание, что на этот раз для получения доступа к сайту вам будет предложено указать учетные данные. Введите пользовательское имя и пароль, а затем щелкните ОК, чтобы убедиться в загрузке сайта. При желании вы можете указать недействительные учетные

данные (например, несуществующую учетную запись) и убедиться в невозможности получения доступа к сайту. Затем закройте Internet Explorer.

10. Чтобы восстановить исходные параметры проверки подлинности, вернитесь к диспетчеру служб IIS. Отключите проверку подлинности Windows и включите анонимную проверку подлинности.

И.Закройте Диспетчер служб IIS (IIS Manager).

Упражнение 2. Настройка сертификатов сервера

В этом упражнении вы создадите самозаверяющий сертификат для сервера Server2.contoso.com. Затем вы потребуете включить SSL для получения доступа к сайту Default Web Site и с помощью Internet Explorer протестируете используемые параметры.

1. Войдите на сервер Server2 в качестве пользователя с административными привилегиями.
2. Откройте Диспетчер служб IIS (IIS Manager) и в левой панели выберите объект сервера.
3. В режиме Просмотр возможностей (Features View) дважды щелкните в области IIS элемент Сертификаты сервера (Server Certificates). Отметим, что в зависимости от ролей и служб ролей, установленных на локальном сервере, в открывшемся окне уже могут присутствовать некоторые сертификаты.
4. В панели Действия (Actions) щелкните команду Создать самозаверенный сертификат (Create Self-Signed Certificate).
5. Введите для сертификата имя *Test Local SSL Certificate и* щелкните OK. Новый сертификат должен появиться в списке сертификатов сервера.
6. Для просмотра свойств нового сертификата щелкните его правой кнопкой мыши и примените команду Вид (View). Обратите внимание на сведения об издателе (имя сервера) и на сроки действия сертификата. (Срок действия новых сертификатов истекает через год.)
7. На вкладке Путь сертификации (Certification Path) будет отображен лишь сам сертификат. Это означает, что он не был издан доверенным центром сертификации. По этой причине данный сертификат не годится для получения пользователями доступа к общественным сетям, таким как Интернет. Щелкните OK.
8. В диспетчере служб IIS щелкните правой кнопкой мыши объект Default Web Site и примените команду Изменить привязки (Edit Binding). Выберите тип привязки HTTPS и щелкните кнопку Изменить (Edit). В списке Сертификаты SSL (SSL Certificate) выберите созданный ранее Test Local SSL Certificate. Для сохранения изменений щелкните OK, а затем щелкните кнопку Закрыть (Close).
9. В режиме Просмотр возможностей (Features View) дважды щелкните элемент Параметры SSL (SSL Settings). Установите флажок Требовать SSL (Require SSL) и щелкните команду Применить (Apply).
10. Щелкните кнопку Назад (Back), чтобы вернуться к режиму просмотра возможностей для объекта Default Web Site. В панели Действия (Actions) щелк-

ните команду Обзор *:80(http) (Browse *80:(http)). Запустится Internet Explorer, и он попытается подключиться к сайту с использованием HTTP-подключения (не SSL). Отметим, что вы получите сообщение об ошибке «Страница, к которой вы пытаетесь обратиться, защищена с помощью протокола SSL» (The page you are trying to access is secure with Secure Sockets Layer (SSL)). Закройте Internet Explorer.

11. В Диспетчере служб IIS (IIS Manager) щелкните в панели Действия (Actions) команду Обзор *:443(https) (Browse *:443(https)). На этот раз вы получите сообщение об ошибке в сертификате безопасности веб-сайта. Причина заключается в том, что самозаверяющий сертификат не был издан доверенным центром сертификации.
12. Чтобы все же получить доступ к сайту, щелкните ссылку Продолжить открытие этого веб-узла (Continue To This Website). Обратите внимание на то, что адресная строка будет окрашена в красный цвет и появится сообщение Ошибка сертификата (Certificate Error). Тем не менее содержимое сайта будет доступным.
13. Закройте Internet Explorer.
14. В Диспетчере служб IIS (IIS Manager) выберите объект Default Web Site, дважды щелкните элемент Параметры SSL (SSL Settings) и сбросьте флажок Требовать SSL (Require SSL). Для сохранения изменений в панели Действия (Actions) щелкните команду Применить (Apply).
15. Закройте Диспетчер служб ITS (IIS Manager).

Резюме

- Анонимная проверка подлинности обеспечивает доступ к содержимому сайта, не требуя учетных данных пользователей.
- Проверку подлинности с помощью форм удобно применять для публичных веб-сайтов и приложений, которые управляют собственной безопасностью.
- Правила авторизации URL могут определять пользователей и группы, располагающие доступом к содержимому веб-сайта.
- Чтобы включить в Интернете зашифрованные соединения с использованием протокола SSL, администраторы веб-серверов могут использовать сертификаты сервера Интернета.
- Для тестирования и разработок администраторы могут создавать самозаверяющие сертификаты сервера.
- Ограничения по IP-адресам и именам домена можно использовать для ограничения доступа к веб-содержимому.
- Уровни доверия .NET ограничивают набор разрешений для управляемого кода на веб-сервере.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных в ходе занятия 2. Эти вопросы представлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы
Ответы и пояснения к каждому их варианту размещены в разделе «Ответы» в конце книги.

1. Вы являетесь администратором веб-сервера IIS и реализуете параметры проверки подлинности для нового веб-сайта. В соответствии с требованиями для веб-сайта Human Resources пользователи должны предоставлять учетные данные для получения доступа к сайту. Доступ к сайту разрешен лишь пользователям с учетными записями в домене Active Directory организации. Вы уже отконфигурировали разрешения файловой системы для содержимого на основе соответствующих параметров. Вы также хотите повысить уровень безопасности сайта. Какие два действия следует предпринять для выполнения этих требований?
   А. Включить проверку подлинности Windows.
   Б. Включить обычную проверку подлинности.
   В. Отключить анонимную проверку подлинности.
   Г. Включить анонимную проверку подлинности.
2. Вы являетесь системным администратором и устраняете неполадку, связанную с получением доступа к веб-серверу Windows Server 2008. Ранее еще один администратор создал и установил на компьютере сертификат сервера. Пользователи сообщают, что они могут подключаться к сайту с помощью протокола HTTP, однако при попытках подключиться с помощью HTTPS получают предупреждение в Internet Explorer. Вы хотите позволить пользователям подключаться с помощью обоих протоколов — HTTP и HTTPS. Вы пытаетесь получить доступ к сайту с помощью экземпляра Internet Explorer на самом сервере и для подключений HTTPS получаете то же самое предупреждение. Как устранить эту проблему?
   А. Изменить привязку узла, чтобы включить соединения на порте 443.
   Б. Изменить для веб-сайта параметры SSL и установить флажок Требовать SSL (Require SSL).
   В. Получить и установить существующий сертификат безопасности.
   Г. Заново настроить параметры брандмауэров клиентов, чтобы включить трафик на порте 443.

Закрепление материала главы

Для того чтобы попрактиковаться и закрепить знания, приобретенные в ходе изучения представленного в данной главе материала, вам необходимо:

- ознакомиться с резюме главы;
- повторить основные термины, используемые в главе;
- выполнить задания лабораторной работы, которые моделируют реальные ситуации, требующие применения полученных знаний;
- выполнить рекомендуемые упражнения;
- сдать пробный экзамен с помощью тестов.

Резюме главы

- Администраторы веб-серверов должны сосредоточиться на реализации глубинной защиты и уменьшении фронта атак IIS, используя такие возможности, как сопоставления обработчиков запросов.
- Управление удаленным администрированием в IIS можно осуществлять путем конфигурирования пользователей, разрешений и делегирования компонентов для служб управления.
- Администраторы сервера могут управлять доступом к веб-серверу с помощью параметров проверки подлинности, правил авторизации URL, сертификатов сервера, а также ограничений по IP-адресам и именам домена.

Основные термины

Проверьте, знаете ли вы, что означают перечисленные ниже термины (свои ответы можно сверить с определениями, содержащимися в конце книги):

- олицетворение ASP.NET;
- фронт атак;
- центр сертификации;
- проверка подлинности с помощью сертификата клиента;
- глубинная защита;
- доменные ограничения (IIS);
- делегирование компонента (IIS);
- сопоставления обработчиков (IIS);
- реквизиты диспетчера IIS;
- запрос сертификата Интернета (IIS);
- ограничения по IP-адресам (IIS);
- службы управления IIS;
- модули (IIS);
- уровни доверия .NET;
- обработчики запросов;
- самозаверяющий сертификат;
- сертификаты сервера;
- правила авторизации URL.

Лабораторная работа

В следующих заданиях вы займетесь обеспечением безопасности IIS.

Задание 1. Настройка удаленного управления для IIS

Вы являетесь системным администратором и отвечаете за управление четырьмя веб-серверами Windows Server 2008. Для подключения ко всем серверам вы хотите использовать один экземпляр Диспетчера служб IIS (IIS Manager). Кроме того, трем другим системным администраторам также нужно управлять

серверами. Один из этих администраторов является независимым консультантом и не располагает учетной записью домена Windows или локального пользователя. Вы хотите создать для этого консультанта пользовательское имя и пароль и ограничить его права лишь управлением IIS. Вы также хотите, чтобы все остальные администраторы, кроме вас, могли лишь просматривать, но не могли изменять параметры компонентов Документ по умолчанию (Default Document) и Просмотр каталога (Directory Browsing).

1. Какой самый простой метод следует использовать для управления параметрами всех веб-серверов с помощью диспетчера служб IIS?
2. Как назначить пользовательское имя и пароль для удаленного системного администратора?
3. Как запретить остальным пользователям диспетчера служб IIS модификацию компонентов Документ по умолчанию (Default Document) и Просмотр каталога (Directory Browsing)?

Задание 2. Повышение уровня безопасности веб-сайта

Вы являетесь системным администратором и отвечаете за безопасность производственного веб-сервера Windows Server 2008 и управление им. Сервер доступен в Интернете и содержит восемь веб-сайтов. Каждый сайт содержит как минимум по одному веб-приложению. Веб-приложение Customer Database содержит веб-приложение ASP.NET 2.0, которому требуется доступ к удаленному серверу баз данных. Еще одно приложение Service Desk содержит статическое содержимое, большая часть которого должна быть доступна пользователям. Однако доступ к папке Admin должны получать лишь конкретные пользователи. И наконец, для приложения Contoso Central нужно реализовать новое требование, которое состоит в том, что все подключения должны быть зашифрованы.

1. Какой уровень доверия .NET следует отконфигурировать для приложения Customer Database?
2. Как отконфигурировать параметры безопасности для папки Admin приложения Service Desk?
3. Как отконфигурировать шифрование подключений к приложению Contoso Central?

Рекомендуемые упражнения

Чтобы успешно справиться с экзаменационными заданиями, выполните следующие упражнения.

Реализация безопасности веб-сервера

В следующих упражнениях вы примените методы обеспечения безопасности веб-серверов, веб-сайтов, веб-приложений IIS.

- **Упражнение 1** Содержимое веб-сайта может содержать копии файла Iisstart.htm и других файлов HTML. Поместите некоторые файлы в папки и создайте сценарии защиты содержимого. Используйте разрешения файловой

системы, параметры проверки подлинности и правила авторизации URL, чтобы лишь определенные пользователи могли получать доступ к сайту. Например, создайте в веб-приложении новую подпапку с именем Secure-Documents. Разместите соответствующие ограничения, чтобы для получения доступа к содержимому пользователям требовалось указывать учетные данные. Кроме того, протестируйте изменения сопоставлений обработчиков. Например, удалите для веб-сайта сопоставление обработчика StaticFile и проверьте результат с помощью Internet Explorer. Для новых файловых типов вы также можете добавить собственные настраиваемые сопоставления обработчиков (например, для файлов с расширением .secure).

- **Упражнение 2** Попрактикуйтесь в использовании различных компонентов безопасности для обеспечения поддержки администраторов веб-сервера с помощью различных уровней ограничений. Протестируйте приведенные ниже опции.
  - Создание пользователей диспетчера служб IIS.
  - Назначение разрешений диспетчера служб IIS для управления доступом администраторов к веб-сайтам и веб-приложениям.
  - Назначение разрешений для пользователей, которые не являются администраторами и располагают учетными записями Windows.
  - Создание ограничений по IP-адресам для управления компьютерами, которые могут администрировать IIS.
  - Использование делегирования компонентов для управления модификацией параметров с помощью диспетчера служб IIS.

  Для эффективного тестирования параметров рекомендуется использовать удаленный компьютер Windows Vista или Windows Server 2008 с установленным диспетчером IIS 7.0.
- **Упражнение 3** Просмотрите следующие сведения и ресурсы с дополнительной информацией об IIS.
  - Трансляция «Secure, Simplified Web Publishing Using Internet Information Services 7.0 (Level 300)» Роберта МакМюррея (Robert McMurray) в папке Webcasts на прилагаемом к книге CD-диске. Эту веб-трансляцию также можно найти, посетив сайт *http://msevents.microsoft.com* и выполнив поиск ID события 1032352159.
  - Веб-трансляция «Securing and Tuning Internet Information Services 7.0 (Level 300)» Назима Лала (Nazim Lala), которая находится в папке Webcasts на прилагаемом CD-диске. Эту веб-трансляцию также можно найти, посетив сайт *http://msevents.microsoft.com* и выполнив поиск ID события 1032352141.
  - Веб-сайт Microsoft Internet Information Services по адресу *http://www.microsoft.com/iis.*
  - Веб-сайт IIS.Net по адресу *http://www.iis.net.*
  - Веб-трансляции IIS 7 по адресу *http://www.iis.net/default.aspx?tabid=2&subtabid=24.*
  - Сайт IIS 7 Virtual Lab по адресу *http://virtuallabs.iis.net.*

Пробный экзамен

На прилагаемом к книге компакт-диске представлено несколько вариантов тренировочных тестов. Проверка знаний выполняется только по одной или же по всем экзаменационным темам сертификационного экзамена 70-643. Тестирование можно организовать таким образом, чтобы оно проводилось как экзамен, или же настроить его на изучение — в этом случае вы сможете после каждого своего ответа на вопрос просматривать правильные ответы и объяснения.

ПРИМЕЧАНИЕ Пробный экзамен

Подробнее о пробном экзамене рассказано во введении к данной книге.

ГЛАВА 7

Настройка служб FTP и SMTP

Занятие 1. Конфигурирование FTP **361**

Занятие 2. Конфигурирование SMTP **398**

В платформе Internet Information Services (IIS) реализованы возможности совместного использования информации несколькими протоколами. Протокол FTP (File Transfer Protocol) обеспечивает стандартный метод, с помощью которого компьютеры могут передавать файлы и другие типы данных.

Этот протокол используется во внутренних сетях и Интернете для выгрузки и загрузки содержимого. Протокол SMTP (Simple Mail Transfer Protocol) обеспечивает стандартный метод передачи сообщений электронной почты. Он часто используется веб-приложениями для отправки сообщений на электронные адреса пользователей.

В этой главе вы изучите принципы конфигурирования указаных служб в Windows Server 2008. На занятии 1 мы обсудим, как установить и сконфигурировать FTP, на занятии 2 рассмотрим установку и конфигурирование SMTP.

Темы экзамена:

- Настройка FTP-сервера.
- Настройка SMTP.

Требования

Для выполнения упражнений этой главы потребуется следующее:

- Знание основ конфигурирования IIS, включая добавление роли Веб-сервер (IIS) и опциональных служб ролей. Эти сведения содержатся в главе 5.
- Роль Веб-сервер (IIS), установленная на сервере Server2.contoso.com с опциями по умолчанию. Если в предыдущих упражнениях вы создали дополнительные веб-сайты и веб-приложения, можете оставить их на сервере.

Занятие 1. Конфигурирование FTP

В Windows Server 2008 поддерживаются две версии FTP-серверов. Служба FTP-публикации (FTP Publishing Service), включенная в Windows Server 2008,

обеспечивает те же функции, которые были доступны в IIS 6.0 системы Windows Server 2003. Это версия FTP 6. Вы также можете загрузить и установить новую, версию продукта — FTP 7.

Обе версии обеспечивают возможности установки FTP-сайтов, позволяющих пользователям без труда выгружать и загружать файлы. В FTP 7 обеспечивается также улучшенная безопасность и расширенные административные возможности. На этом занятии мы обсудим, как установить обе версии FTP на компьютере Windows Server 2008.

СОВЕТ Подготовка к экзамену

В период написания данной книги корпорация Microsoft планировала включить FTP 6 в первоначальную версию сертификационного экзамена 70-643. Однако со временем на экзамене могут появиться вопросы по версии FTP 7. Хотя основные возможности и функциональность этих двух версий аналогичны, FTP 7 обеспечивает много новых возможностей и использует версию диспетчера служб IIS системы Windows Server 2008.

Реальный мир

Анил Десаи

Работая консультантом в области информационных технологий, я часто сталкивался с конфигурацией сервера и служб, параметры которой были настроены с нарушением важнейших правил, в частности принципов безопасности.

В ряде случаев системные администраторы, будучи занятыми другими делами, не располагали временем для корректной настройки служб. Часто им просто не хватало опыта и знания принципов реализации. И каждый раз наблюдалась аналогичная картина: службы развертывались без обеспечения безопасности.

Если вы отвечаете за развертывание новых компонентов и служб, от которых зависит дополнительная функциональность, вы должны учитывать возможные последствия таких изменений. Отличным примером подобного случая является реализация FTP-сервера. Сайты FTP обеспечивают метод, с помощью которого пользователи могут выгружать и загружать данные по сети.

При организации доступа к ним в Интернете или внешних сетях очень важно, чтобы лишь авторизованные пользователи получали доступ к серверу. Для обеспечения безопасности можно использовать такие опции конфигурации, как методы проверки подлинности, зашифрованные подключения, параметры авторизации и домашние каталоги пользователей. Эти возможности мы рассмотрим на занятии 1.

Уделите внимание изучению принципов обеспечения безопасности при установке таких сетевых служб, как FTP-серверы. Если вам не хватает времени на безопасное развертывание сервера, возможно, лучше его вообще не развертывать.

Изучив материал этого занятия, вы сможете:

- S Установить и отконфигурировать Службу FTP-публикации (FTP Publishing Service) на компьютере Windows Server 2008.
- •S С помощью FTP 6 создать и отконфигурировать новый FTP-сайт.
- •S Администрировать FTP 7 с помощью диспетчера служб IIS.
- S Конфигурировать привязки FTP-сайта для веб-сайта IIS 7.
- •S Управлять параметрами FTP 7, включая параметры SSL, проверку подлинности, авторизацию и изоляцию пользователей.

Расчетная продолжительность занятия составляет 60 мин.

Установка службы FTP-публикации

Служба FTP-публикации (FTP Publishing Service) (FTP 6) включена для роли Веб-сервер (IIS) (Web Server (IIS)) в качестве опциональной службы ролей. Эту службу можно добавить на сервер с помощью Диспетчера сервера (Server Manager). Первый метод состоит в выборе службы ролей Служба FTP-публикации (FTP Publishing Service) при добавлении роли Веб-сервер (IIS) на компьютер. Если вы уже установили роль Веб-сервер (IIS), для добавления нужного элемента используйте команду Добавить службы ролей (Add Role Services) (рис. 7-1).

ШШ2.

Выбор служб ролей

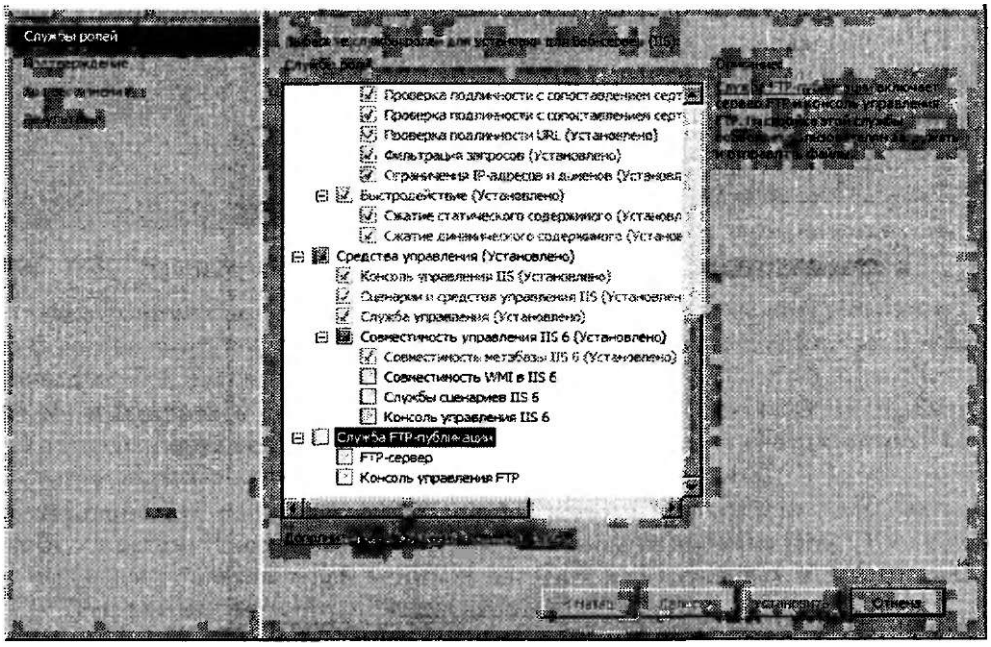


Рис. 7-1. Установка FTP 6 на компьютер Windows Server 2008

Компонентами службы FTP-публикации (FTP Publishing Service) являются две службы ролей. Системная служба FTP-сервер (FTP Server) обеспечивает доступ к FTP-сайтам, а Консоль управления FTP (FTP Management Console) используется для создания FTP-сайтов с помощью диспетчера служб IIS 6.0 и управления ими.

Удаление службы FTP-публикации

Если вам больше не нужен сервер для обеспечения доступа через FTP, вы можете удалить службу FTP-публикации. Кроме того, если вы планируете установить FTP 7, рекомендуется вначале удалить службу FTP-публикации с компьютера. Таким образом вы предотвратите потенциальные конфликты портов и другие проблемы совместимости конфигурации.

Службу FTP-публикации (FTP Publishing Service) можно удалить с помощью Диспетчера сервера (Server Manager). В левой панели разверните узел Роли (Roles), щелкните правой кнопкой мыши Веб-сервер (IIS) (Web Server (IIS)) и примените команду Удалить службы ролей (Remove Role Services). Чтобы отключить на сервере функции FTP-публикации, удалите Службу FTP-публикации (FTP Publishing Service) и ее опциональные компоненты. Отметим, что при этом содержимое FTP-папок не будет удалено из файловой системы компьютера.

Настройка FTP-сайтов с помощью диспетчера служб IIS 6.0

Для управления FTP-сервером можно использовать Диспетчер служб IIS 6.0 (IIS 6.0 Manager), который содержится в группе программ Администрирование (Administrative Tools). Чтобы просмотреть конфигурацию локального сервера, разверните объект сервера и папку FTP-узлы (FTP Sites). По умолчанию Служба FTP-публикации (FTP Publishing Service) устанавливает FTP-сайт Default FTP Site, как показано на рис. 7-2.

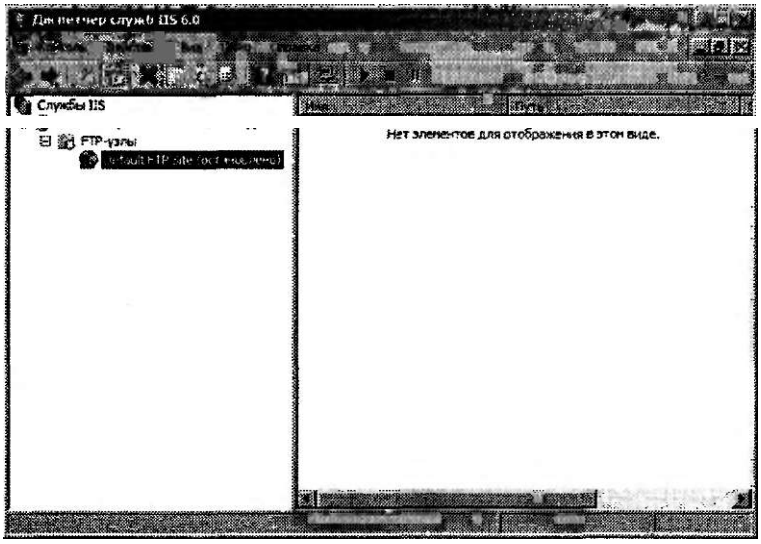


Рис. 7-2. Конфигурирование нового FTP-сайта в диспетчере служб 115 6.0

В этом разделе вы изучите принципы создания FTP-сайтов и управления их конфигурацией с помощью диспетчера служб IIS 6.0.

Создание FTP-сайта

Вы можете создать множество FTP-сайтов, которые будут прослушивать запросы на различных портах и IP-адресах. Чтобы в диспетчере служб IIS 6.0 создать новый FTP-сайт, щелкните правой кнопкой мыши папку FTP-узлы (FTP Sites), выберите команду Создать (New) и щелкните FTP-узел (FTP Site). Запустится Мастер создания FTP-узла (FTP Site Creation Wizard). На первой странице мастера (после приветствия) вам будет предложено ввести описание FTP-сайта. Такое описательное имя поможет вам идентифицировать сайт при администрировании.

На странице Настройка IP-адреса и порта (IP Address And Port Settings), показанной на рис. 7-3, можно указать IP-адрес и TCP-порт для данного FTP-сайта. По умолчанию сервер отвечает на запросы со всех не указанных [P-адресов, используя порт по умолчанию 21. Для одновременной работы FTP-сайтов каждому сайту на сервере требуется назначить уникальную комбинацию IP-адреса и порта.

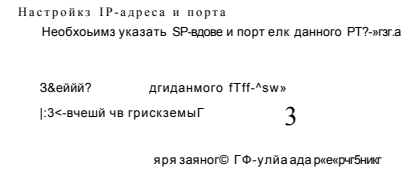


Рис. 7-3. Настройка IP-адреса и порта для нового FTP-сайта

На странице Изоляция пользователя FTP (FTP User Isolation) можно указать содержимое, к которому пользователи будут получать доступ, как показано на рис. 7-4. Здесь имеются следующие опции.

- Не изолировать пользователей (Do Not Isolate Users) Этот параметр позволяет всем пользователям получать доступ ко всему содержимому FTP-сайта, включая папки, созданные другими пользователями.
- Изолировать пользователей (Isolate Users) Для каждого пользователя будет автоматически создаваться папка с именем пользователя. Эта опция запрещает пользователям получать доступ к другим папкам и каталогам на FTP-сервере.
- Изолировать пользователей, используя Active Directory (Isolate Users Using Active Directory) Этот параметр позволяет определить корневой

каталог FTP и параметры изоляции в службах каталогов Active Directory. Для входа на сервер пользователи должны располагать доменными учетными записями Active Directory, Кроме того, должен существовать указанный пользователем путь к папке.

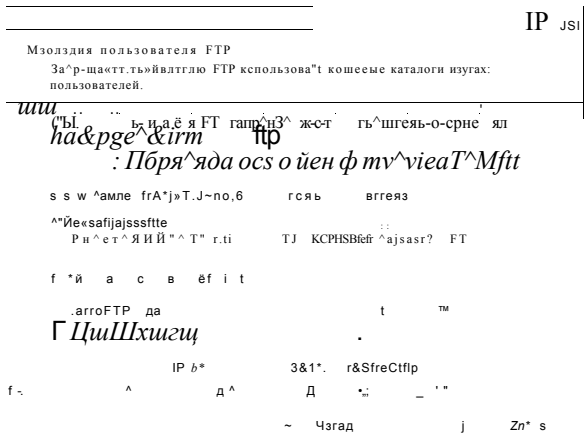


Рис. 7-4. Параметры изоляции пользователя FTP для нового FTP-сайта

На странице Корневой каталог FTP-узла (FTP Site Home Directory) следует указать путь к корневому каталогу FTP-сайта в файловой системе. Как правило, каждый FTP-сайт располагает собственным уникальным корневым каталогом. Сайту Default FTP Site сопоставлена папка %SystemDrive%\Inetpub\Ftproot. На странице Разрешения на доступ к FTP-узлу (FTP Site Access Permissions) мастера создания FTP-сайта для пользователей можно указать разрешение на чтение или запись файлов на сервере. При выборе лишь разрешений чтение пользователи смогут выгружать данные на сервер, но не смогут их загружать с сервера. Разрешения на запись требуются для добавления файлов на сайт. Если пользователи должны лишь выгружать файлы на сервер, но не должны загружать их с сервера, па этой странице можно указать лишь разрешение на запись без чтения.

Новый FTP-сайт будет создан после того, как вы щелкнете кнопку Готово (Finish) на последней странице Мастера создания FTP-узла (FTP Site Creation Wizard). Затем вы сможете управлять этим сайтом и его параметрами с помощью Диспетчера служб IIS 6.0 (IIS 6.0 Manager). FTP-сайты, отконфигурированные с помощью Службы FTP-публикации (FTP Publishing Service), можно независимо останавливать, запускать и приостанавливать. При остановке работы FTP-сайта входящие подключения не разрешаются.

Настройка свойств FTP-сайта

Чтобы отконфигурировать параметры для FTP-сайта, в Диспетчере служб IIS 6.0 (IIS 6.0 Manager) щелкните правой кнопкой мыши объект сайта и примените команду Свойства (Properties). На вкладке FTP-узел (FTP Site) можно изменить параметры IP-адреса и порта для FTP-сайта, как показано на рис. 7-5. Чтобы изменения вступили в силу, нужно перезапустить FTP-сайт.

В области Подключения FTP-узла (FTP Site Connections) можно указать ограничения для подключений. По умолчанию разрешается до 100 ООО подключений со временем ожидания до 120 с. Если вы хотите ограничить полосу пропускания и ресурсы, используемые конкретными сайтами в службе FTP-нубликации, можете указать нужные параметры в этой области.

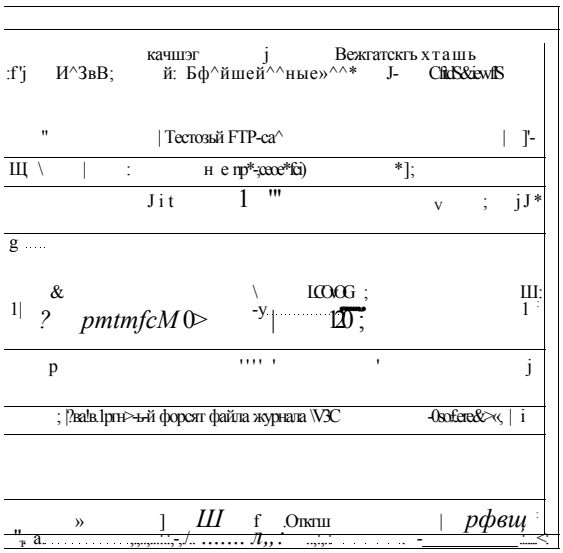


Рис. 7-5. Просмотр параметров FTP-сайта в диспетчере служб IIS 6.0

ВАЖНО! Ограничения подключений

К FTP-серверам, особенно серверам в Интернете, часто предпринимаются попытки неавторизованного доступа. Пользователи иногда подключаются к незащищенному FTP-серверу с целью обеспечения доступа к их собственному выгруженному содержимому для других пользователей. Такие параметры, как ограниченное количество подключений, позволят гарантировать использование сайта лишь авторизованными пользователями. Например, если к сайту будут получать доступ лишь несколько пользователей, уменьшите число подключений, заданное по умолчанию. Хотя ограничения подключений не являются заменой методов обеспечения безопасности, они могут помочь избежать определенных проблем, связанных с неправильным использованием сайта.

В области Вести журнал (Enable Logging) щелкните кнопку Свойства (Properties), чтобы открыть диалоговое окно Свойства ведения журнала (Logging Properties). В нем можно указать временной период для создания новых файлов журнала и место их хранения, как показано на рис. 7-6. С помощью свойств на вкладке Дополнительно (Advanced) можно также указать, какие данные следует записывать в журнал. Чем больше информации добавляется в журнал, тем большими будут размеры его файлов. Файлы журнала представляют собой обычные текстовые файлы, которые можно открыть в таком текстовом редакторе, как Блокнот (Notepad) Windows.

Щелкнув кнопку Текущие сеансы (Current Sessions) на вкладке FTP-узел (FTP Site), вы сможете просмотреть текущих пользователей, подключенных к серверу. Эту информацию удобно использовать для устранения потенциальных проблем производительности и отслеживания текущего использования сайта.

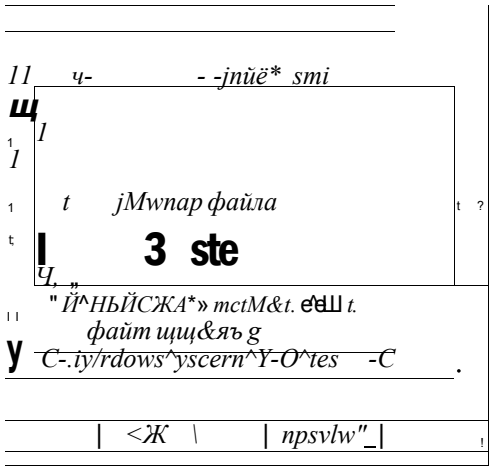


Рис. 7-6. Свойства ведения журнала для FTP-сайта

Настройка безопасных учетных записей

Когда пользователи подключаются к FTP-серверу с применением анонимных учетных данных, для обработки запросов выгрузки и загрузки Служба FTP-публикации (FTP Publishing Service) использует разрешения, назначенные конкретной учетной записи. По умолчанию применяются разрешения IUSR_*MachineName* (где *MachineName* — имя локального компьютера). Па вкладке Безопасные учетные записи (Security Accounts) можно указать другое пользовательское имя и пароль, как показано на рис. 7-7.

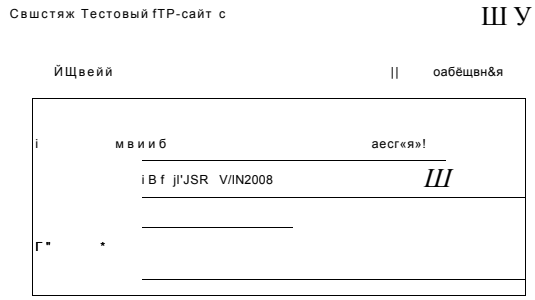


Рис. 7-7. Настройка безопасных учетных записей для FTP-сайта

Если установить флажок Разрешить только анонимные подключения (Allow Only Anonymous Connections), разрешения всех пользователей сайта будут ограничены указанной учетной записью независимо от предоставления ими действительных учетных данных Windows.

Сообщения FTP-сервера

На вкладке Сообщения (Messages) можно ввести текст, который будет отображаться для пользователя. Заголовок (Banner) появляется перед входом пользователя на FTP-сайт. Здесь вы можете указать сведения о сайте и контактные данные, как показано на рис. 7-8. Приветствие (Welcome) отображается после успешной проверки подлинности пользователя на сервере. Сообщение Выход (Exit) отображается после завершения пользователем подключения, а сообщение Максимальное число подключений (Maximum Connections) — в случае выполнения FTP-сервером максимального количества подключений, указанного на вкладке FTP-узел (FTP Site).

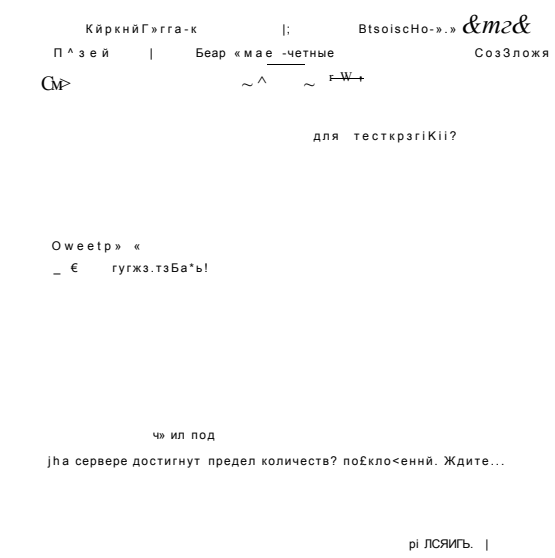


Рис. 7-8. Настройка сообщений FTP-сайта

Настройка опций корневого каталога

На вкладке Корневой каталог (Home Directory) можно указать размещение корневого каталога FTP-сайта в файловой системе, как показано на рис. 7-9. Опция по умолчанию Каталог данного компьютера (A Directory Located On This Computer) позволяет указать путь к локальной папке. Вы можете назначить для папки разрешения чтения, записи, а также указать, следует ли записывать в журнал сведения о посещении этой папки. В области Стиль вывода каталогов (Directory Listing Style) можно указать формат файловых списков, возвращаемых FTP-клиенту.

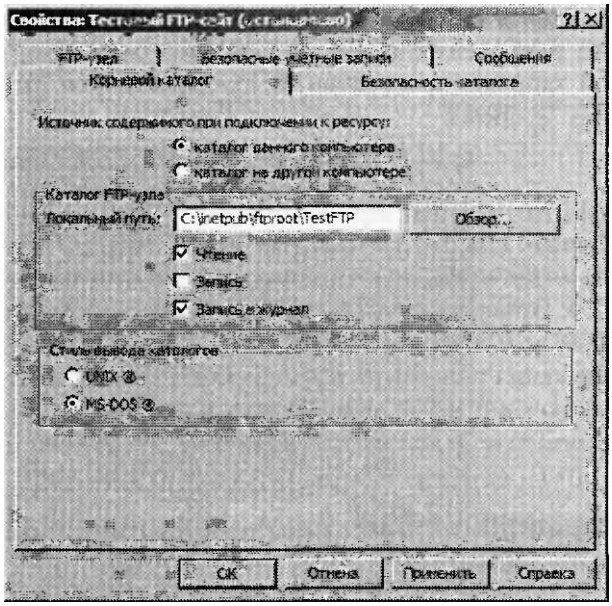


Рис. 7-9. Настройка корневого каталога для FTP-сайта

Корневой каталог можно также использовать на любом другом компьютере. Эта опция позволяет множеству FTP-серверов обеспечивать доступ к одному содержимому. Выбрав опцию Каталог на другом компьютере (A Directory Located On Another Computer), вы сможете указать сетевой путь UNS (Universal Naming Convention) к содержимому (например, \\Server1\FTPData\). Щелкнув кнопку Подключиться как (Connect As), вы сможете указать пользовательское имя и пароль, которые будут применяться для получения доступа к содержимому (рис. 7-10).

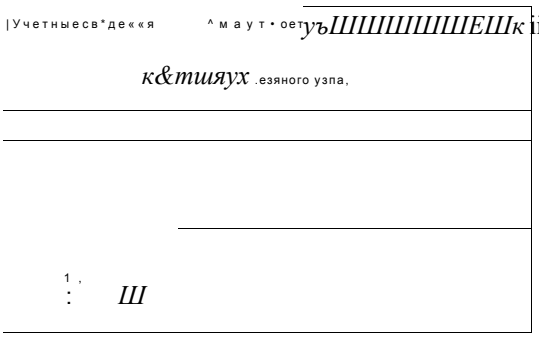


Рис. 7-10. Настройка учетных сведений для доступа к сетевому каталогу FTP-сайта

По умолчанию для подтверждения доступа к данным используются учетные данные пользователя, прошедшего проверку подлинности. Вы можете назначить учетную запись для тестирования и подтверждения разрешений независимо от учетных данных пользователей.

Управление параметрами безопасности каталога

Доступ к FTP-сайту можно ограничить на основе данных IPv4-адресов. Эти параметры находятся на вкладке Безопасность каталога (Directory Security), показанной на рис. 7-11. По умолчанию доступ к сайту смогут получать все компьютеры. Чтобы изменить эти настройки, нужно добавить новые записи для конкретных компьютеров или групп компьютеров и выбрать параметр Разрешен доступ (Granted Access) или Запрещен (Denied Access).

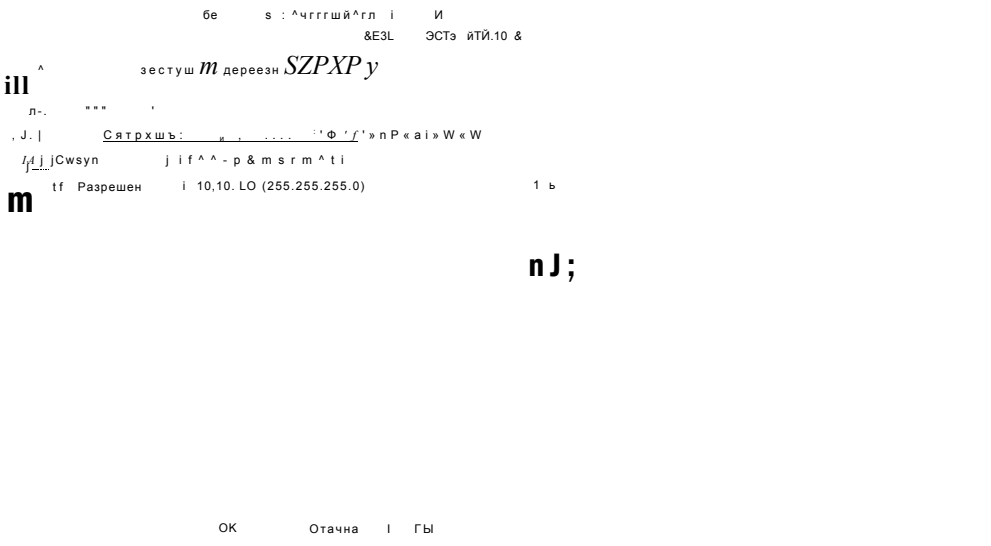


Рис. 7-11. Настройка безопасности каталога FTP-сайта

Установка FTP 7 и управление им

Для Windows Server 2008 корпорация Microsoft предоставила обновленную версию служб FTP. Чтобы включить FTP 7, нужно вручную загрузить и установить службу FTP-публикации Microsoft для IIS 7.0. Необходимые файлы и инструкции по установке можно получить в разделе Downloads веб-сайта Microsoft Internet Information Services (IIS) по адресу *http://www.iis.net/downloads/*. Не запускайте версии FTP 6 и FTP 7 на одном компьютере одновременно, поскольку могут возникнуть конфликты конфигурации сайта и портов. Чтобы избежать таких проблем, перед установкой FTP 7 удалите FTP 6 с компьютера, как описано ранее в этом занятии.

Основным средством администрирования FTP 7 является Диспетчер служб IIS (IIS Manager). Системные администраторы могут использовать диспетчер служб IIS для настройки служб HTTP и FTP с помощью одного административного интерфейса.

После загрузки и установки FTP 7 вы можете запустить Диспетчер служб IIS (IIS Manager) и отконфигурировать параметры сервера. На рис. 7-12 показаны доступные опции FTP для сайта Default Web Site.

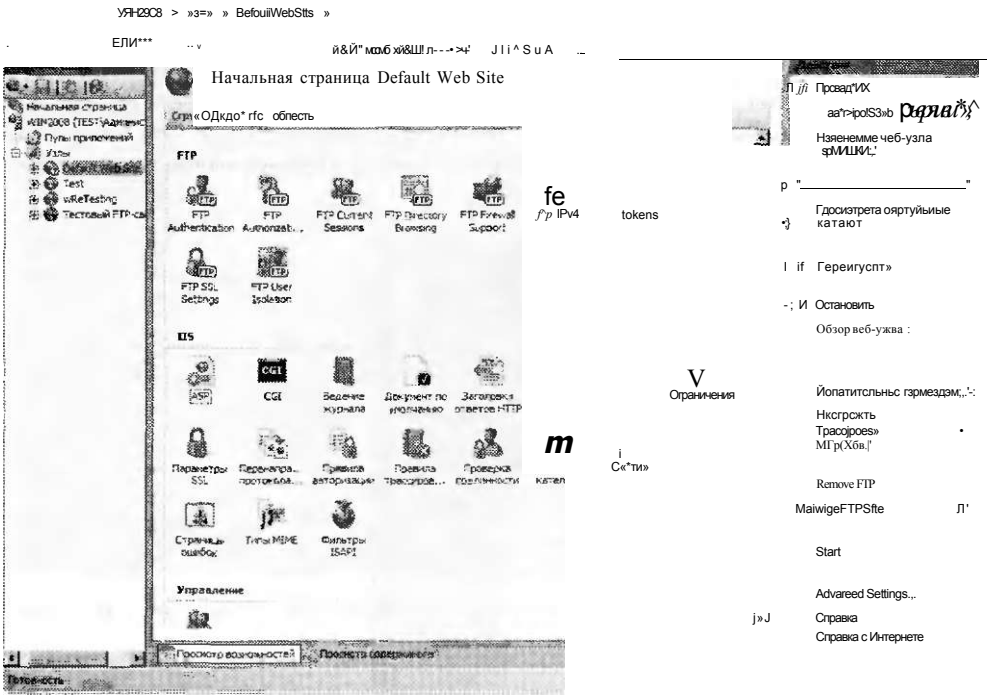


Рис. 7-12. Опции FTP для сайта Default Web Site в диспетчере служб IIS

Управление FTP-сайтами

После установки и настройки FTP 7 для создания и конфигурирования FTP-сайтов можно использовать Диспетчер служб IIS (IIS Manager). В этом разделе описано, как создавать новые FTP-сайты и добавлять функциональность FTP для существующих веб-сайтов.

Создание FTP-сайта

Новые FTP-сайты можно создавать для поддержки различных групп пользователей и обеспечения доступа к разным наборам файлов. Чтобы создать FTP-сайт, в левой панели Диспетчера служб IIS (IIS Manager) щелкните правой кнопкой мыши объект сервера или папку Узлы (Sites), примените команду Add FTP Site (Добавить FTP-узел), и будет запущен Мастер добавления FTP-узла (Add FTP Site Wizard). На первой странице вам будет предложено указать имя для сайта, как показано на рис. 7-13. Это имя будет использоваться в административных целях.

Поэтому если вы планируете управлять множеством FTP-сайтов на одном сервере, им следует присваивать описательные имена. В поле Physical Path (Физический путь) следует ввести путь к корневому каталогу для FTP-сайта. Вы можете выбрать любую из папок, однако чаще всего используется подпапка в каталоге %SystemDrive%\Inetpub.

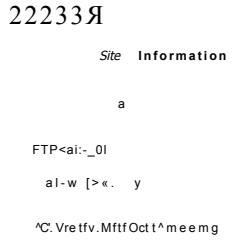


Рис. 7-13. Добавление нового FTP-сайта с помощью диспетчера служб IIS

На второй странице мастера можно указать привязки и параметры SSL для нового FTP-сайта, как показано на рис. 7-14. Для параметров привязки используются следующие опции.

- IP Address (IP-адрес) По умолчанию FTP-сайт настроен для реагирования на все входящие запросы на любом сетевом адаптере или IP-адресе. Если на компьютере установлено множество сетевых адаптеров или на одном адаптере отконфигурировано множество IP-адресов, вы можете указать конкретный адрес в раскрывающемся списке.
- Port (Порт) TCP-порт FTP-сайта. По умолчанию для FTP-коммуникаций назначается порт 21. Если выбрать другой порт, пользователям FTP потребуется настроить свое клиентское программное обеспечение FTP для подключения, указав номер порта сервера.
- Виртуальный узел (Virtual Host) С помощью имен виртуальных узлов администраторы могут создать множество веб-сайтов на одном IP-адресе и порте. Для определения сайта, к которому подключается пользователь, эти имена используют записи DNS (Domain Name System). Чтобы указать, к какому сайту требуется подключиться, пользователи могут также включать имя виртуального хоста в учетные данные.
- Автоматический запуск FTP-узла (Start FTP Site Automatically) Если установить этот флажок, FTP-сайт будет запускаться автоматически при каждой перезагрузке компьютера или перезапуске службы FTP. Если вы планируете запускать FTP-сайт вручную но требованию, сбросьте флажок.

Вы также можете выбрать сертификат SSL и указать, разрешение (Apply) или требование (Require) подключения SSL (Secure Socket Protocol) для этого FTP-сайта. Более подробно данные опции описаны далее в этом разделе.

На странице Данные проверки подлинности и авторизации (Authentication And Authorization Information) нужно указать параметры проверки подлинности и авторизации для нового FTP-сайта, как показано на рис. 7-15.

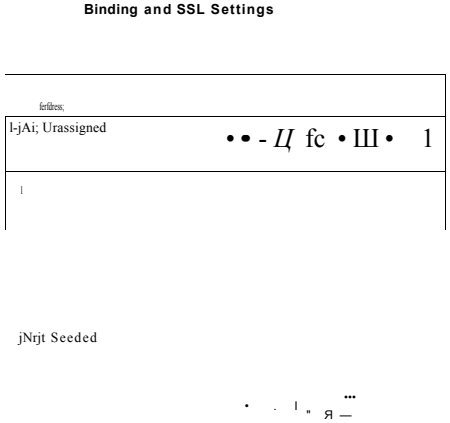


Рис. 7.14. Настройка параметров привязок и SSL для нового FTP-сайта

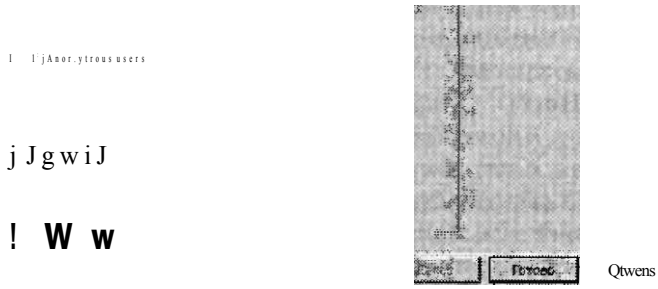


Рис. 7-15. Настройка параметров проверки подлинности и авторизации для нового FTP-сайта

Когда вы щелкнете кнопку Finish (Готово), новый FTP-сайт будет создан и добавлен в левую панель диспетчера служб IIS. Выбрав объект FTP-сайта, вы сможете использовать команды в панели Действия (Actions) для запуска, перезапуска и остановки FTP-сайта. В центральной панели Диспетчера служб IIS (IIS Manager) отобразится также список всех опций конфигурации FTP-сайта, как показано на рис. 7-16.

Рис. 7-16. Просмотр опций FTP в диспетчере служб IIS

Файлы конфигурации FTP 7

Все параметры конфигурации сайтов FTP 7 хранятся в XML-файлах с расширением .config. Эти параметры можно просматривать и редактировать с помощью текстового редактора. Параметры уровня сервера для веб-сайтов и FTP-сайтов хранятся в файле ApplicationHost.config. Более подробные сведения об использовании этих файлов конфигурации и создании резервных копий содержатся в главе 5.

Создание виртуальных каталогов

Содержимое FTP-сайта можно без труда организовать в физических папках. Например, вы можете создать иерархию папок для различных типов приложений и данных. Однако в некоторых случаях может потребоваться обеспечить доступ к содержимому, размещенному вне корневого каталога FTP. Для этого можно создать виртуальные каталоги. Виртуальные каталоги представляют собой указатели размещения папок. Их можно вкладывать в другие виртуальные каталоги или физические папки. Располагая соответствующими разрешениями, пользователи будут видеть виртуальный каталог как физическую папку. Однако все операции выгрузки и загрузки будут направляться на физическую папку. Виртуальные каталоги удобно применять для совместного использования содержимого на множестве физических сайтов, а также в тех случаях, если вы не хотите перемещать или копировать данные в корневой каталог FTP.

Чтобы создать новый виртуальный каталог, в левой панели диспетчера служб IIS щелкните родительской объект правой кнопкой мыши и примените команду Добавить виртуальный каталог (Add Virtual Directory). Откроется диалоговое окно Добавление виртуального каталога (Add Virtual Directory), показанное на рис. 7-17. Название узла (Site Name) и Путь (Path) указывают место, где будет создан виртуальный каталог. Псевдоним (Alias) папки будет отображаться для пользователей сайта. В поле Физически! путь (Physical Path) следует ввести полный физический путь к содержимому, которое вы хотите сделать доступным.

Л У Ш - » х

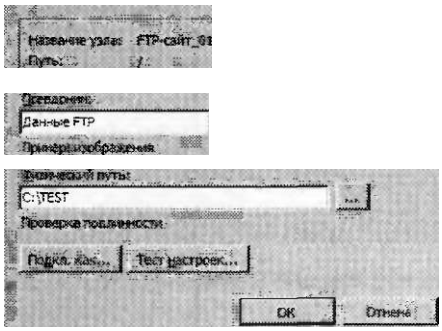


Рис. 7-17. Добавление нового виртуального каталога для FTP-сайта

По умолчанию для определения разрешений доступа пользователей к содержимому виртуальные каталоги будут использовать сквозную проверку подлинности (Pass-Through Authentication). Это означает, что пользовательская учетная запись, которая применяется для входа, должна располагать разрешениями для папки с содержимым. Такое поведение можно изменить, щелкнув кнопку Подкл. как (Connect As) и выбрав опцию Указании»! пользователь (Specific User). Вы можете указать пользовательское имя и пароль конкретной учетной записи. Если выбрать опцию Указанный пользователь (Specific User), все запросы данных, хранящихся по указанному физическому пути, будут выполняться в контексте безопасности этого пользователя.

Настройка дополнительных свойств FTP-сайта

Помимо стандартных свойств, доступных в режиме Просмотр возможностей (Features View) диспетчера служб IIS, для FTP-сайта можно отконфигурировать опции Advanced Settings (Дополнительные параметры). Чтобы открыть эти опции, в панели Действия (Actions) щелкните команду Advanced Settings (Дополнительные параметры). На рис. 7-18 показаны доступные опции и их значения по умолчанию.

Область Behavior (Поведение) содержит опции для тонкой настройки параметров FTP-сайта. В области Connections (Подключения) можно управлять временем ожидания каналов данных (в секундах), а также максимальным числом подключений. Эти параметры удобно применять для управления производительностью перегруженных веб-серверов и FTP-серверов. В области File Handling (Управление файлами) можно указать опции частичной выгрузки и разрешить сеансу выполнять операции во время выгрузки данных.

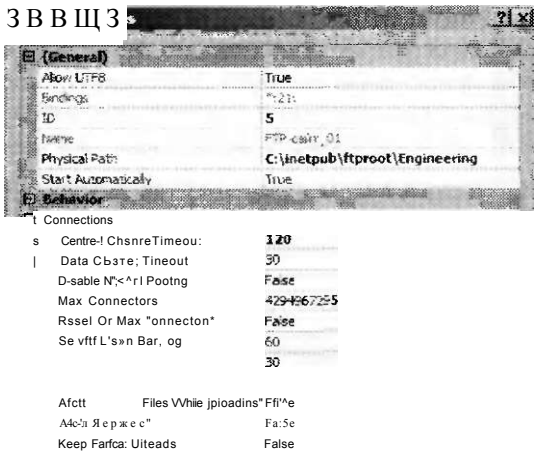


Рис. 7-18. Конфигурирование дополнительных параметров FTP-сайта

Управление привязками FTP-сайта

В FTP 7 администраторы веб-сайтов могут использовать упрощенный метод управления содержимым с помощью FTP. В предыдущих версиях FTP администраторам требовалось вручную конфигурировать новый сайт или виртуальные каталоги для получения доступа к содержимому веб-сайта. Теперь чтобы обеспечить автоматический доступ для FTP-клиентов, можно добавить для веб-сайта новую привязку FTP-сайта. Такие привязки удобно использовать, чтобы разрешать удаленным администраторам и веб-разработчикам получать доступ к конкретным веб-сайтам и модифицировать их содержимое.

Для добавления новой FTP-привязки в диспетчере служб IIS выберите веб-сайт и в панели Действия (Actions) щелкните команду Привязки (Binding). Чтобы создать новую привязку узла, щелкните кнопку Добавить (Add). Откроется окно, показанное на рис. 7-19.

В диалоговом окне Добавление привязки узла (Add Site Binding) можно выбрать тип привязки FTP. Затем, чтобы определять разрешения доступа пользователей к FTP-сайту, вы можете ввести данные IP-адреса, порта и имени хоста. После добавления FTP-привязки в режиме Просмотр возможностей (Features View) диспетчера служб IIS вы увидите группу команд для FTP. Их можно использовать для модификации параметров привязок FTP-сайта точно таким же образом, как и в случае с автономным веб-сайтом. В панели Действия (Actions) также появится новый раздел Manage FTP Site (Управление FTP-узлом). FTP-сайт, являющийся частью веб-сайта, можно запускать, останавливать и перезапускать независимо от веб-сайта.

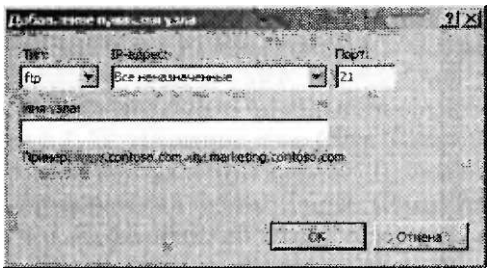


Рис. 7-19. Добавление для веб-сайта новой привязки FTP-сайта

ВАЖНО! Номера FTP-портов и безопасность
Изменив порт 21, назначаемый по умолчанию, можно повысить уровень безопасности конфигурации FTP-сервера. Случайные хакеры часто пытаются подключаться к этому порту в поисках незащищенных FTP-серверов. Тем не менее принцип «безопасность через незнание» (Security through obscurity) редко оправдывает себя. Сокрытие деталей работы FTP-сервера не поможет решить самые важные вопросы безопасности. Всегда используйте вместе с привязками узлов другие возможности для обеспечения безопасности, например параметры брандмауэра, проверки подлинности и правила авторизации.

Управление безопасностью FTP-пользователя

С помощью FTP-серверов пользователи могут выгружать и загружать уязвимые данные. Вы можете использовать несколько методов управления доступом пользователей к конкретному содержимому. В этом разделе рассматриваются параметры проверки подлинности, авторизации и изоляции пользователей.

Настройка опций проверки подлинности

С помощью компонента Проверка подлинности (Authentication) для FTP-сайта можно определить доступ пользователей к содержимому сайта. Существует несколько встроенных методов управления проверкой подлинности. Для конфигурирования этих параметров в Диспетчере служб IIS (IIS Manager) выберите объект FTP-сайта и в режиме Просмотр возможностей (Features View) дважды щелкните компонент FTP Authentication (Проверка подлинности FTP). На рис. 7-20 показан пример опций проверки подлинности. Панель Действия (Actions) позволяет включать и отключать различные опции проверки подлинности. С помощью команды Edit (Изменить) в этой панели можно указать дополнительные параметры для выбранного метода проверки подлинности.

Анонимная проверка подлинности (Anonymous Authentication) позволяет всем пользователям, которые подключаются к сайту, получать доступ к содержимому независимо от предоставляемых учетных данных. Этот метод следует использовать в тех случаях, если вы планируете назначить доступ к содержимому для всех посетителей FTP-сайта или если для ограничения доступа к сайту вы используете другие методы обеспечения безопасности. Когда FTP-пользователь посылает запрос чтения или записи данных, для подтверждения разрешений анонимная проверка подлинности применит учетную запись указанного

пользователя. По умолчанию для этой пели используется встроенная учетная запись IUSR. Вы можете назначить конкретную учетную запись Windows, щелкнув команду Edit (Изменить) в панели Действия (Actions). Для выполнения анонимной проверки подлинности можно также указать идентичность конкретного пользователя, как показано на рис. 7-21.

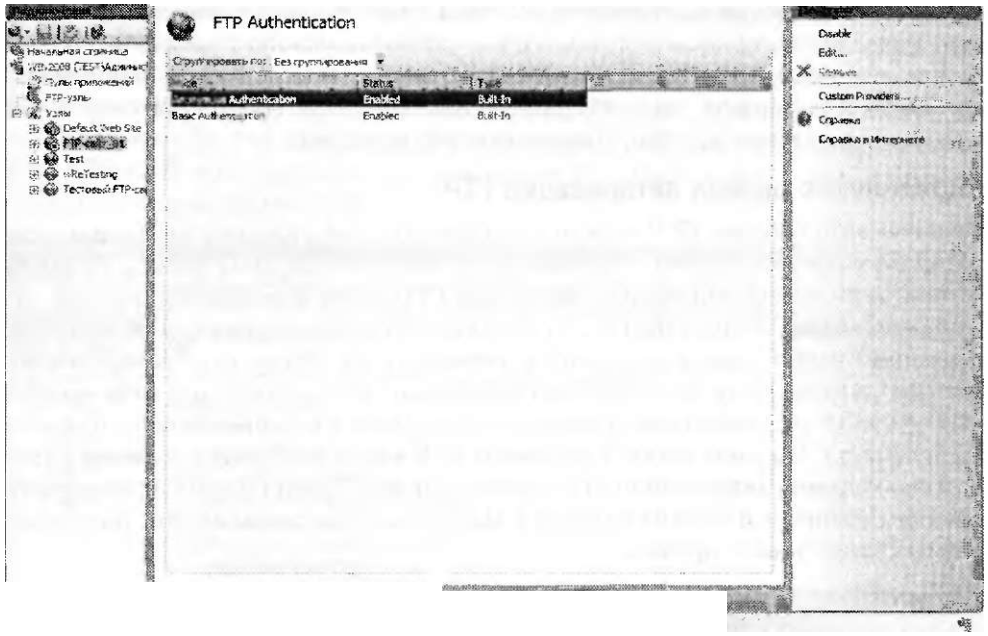


Рис. 7-20. Параметры проверки подлинности для FTP-сайта

ugir

8 ^ttser.^ffias

- |SUSR

:S

CcnЙггT' pfts *SWGfgi*

Рис. 7-21. Изменение параметров учетных данных для анонимной проверки подлинности

Вы также можете применить два других метода проверки подлинности, щелкнув команду Custom Providers (Настраиваемые поставщики) в панели Действия (Actions). Проверка подлинности диспетчера IIS (IIS Manager Auth) конфигурирует веб-сайт для применения учетных данных пользователя диспетчера служб IIS. Этот метод удобно использовать для ограничения доступа

к FTP-сайту конкретных пользователей, не располагающих учетными записями Windows на локальном FTP-сервере. Перед использованием этого метода проверки подлинности нужно установить и включить Службу управления IIS (IIS Management Service). Более подробные сведения о создаиии пользователей диспетчера служб IIS и управлении ими содержатся в главе 6. Аналогично учетным данным обычной проверки подлинности (Basic Authentication) пользовательское имя и пароль передаются между FTP-клиентом и FTP-сервером в открытом виде.

В методе проверки подлинности ASP.NET (AspNetAuth) используется структура управления пользователями .NET. Этот метод удобно применять при создании веб-сайта ASP.NET, который подтверждает учетные данные пользователя. Чтобы подтвердить доступ и разрешения для сайта, веб-приложения часто используют учетные данные, хранящиеся в базе данных.

Определение правил авторизации FTP

Правила авторизации FTP можно использовать для указания пользователей, которым разрешен доступ к конкретному содержимому FTP-сайта. Правила авторизации можно определить на уровне FTP-сайта или для конкретных логических и виртуальных папок. Эти возможности обеспечивают гибкость в реализации правил гранулированной авторизации на основе типа содержимого, которое должно быть доступно пользователям. Существует два типа правил авторизации: разрешающие правила (Allow Rules) и запрещающие правила (Deny Rules). По умолчанию для нового FTP-сайта нет предварительно определенных правил авторизации. Для создания новых правил можно использовать команды в панели Действия (Actions). На рис. 7-22 показаны опции, доступные при создании нового правила.

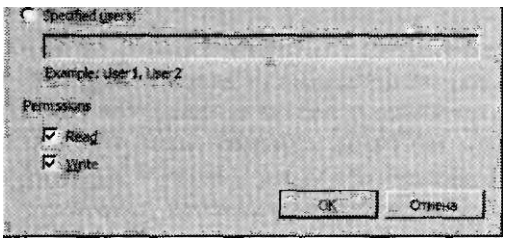


Рис. 7-22. Добавление нового правила авторизации

Разрешающие и запрещающие правила применяются к пользователям следующих типов:

- All Users (Все пользователи);
- All Anonymous Users (Все анонимные пользователи);

- Specified Roles Or User Groups (Указанные роли или группы пользователей);
- Specified Users (Указанные пользователи).

После выбора пользователей или групп, к которым будет применено правило, вы можете указать для пользователей разрешения чтения, записи либо чтения и записи.

Настройка опций изоляции пользователей FTP

При управлении разрешениями доступа и параметрами FTP-сервера часто требуется обеспечить для отдельных пользователей собственные папки и каталоги. Пользователи должны иметь возможность выгружать и загружать файлы из своих папок и не должны получать доступ к папкам других пользователей. Компонент Изоляция пользователей FTP (FTP User Isolation) позволяет отконфигурировать эти параметры. В Диспетчере служб IIS (IIS Manager) выберите FTP-сайт и дважды щелкните компонент FTP User Isolation, чтобы открыть окно, показанное на рис. 7-23.

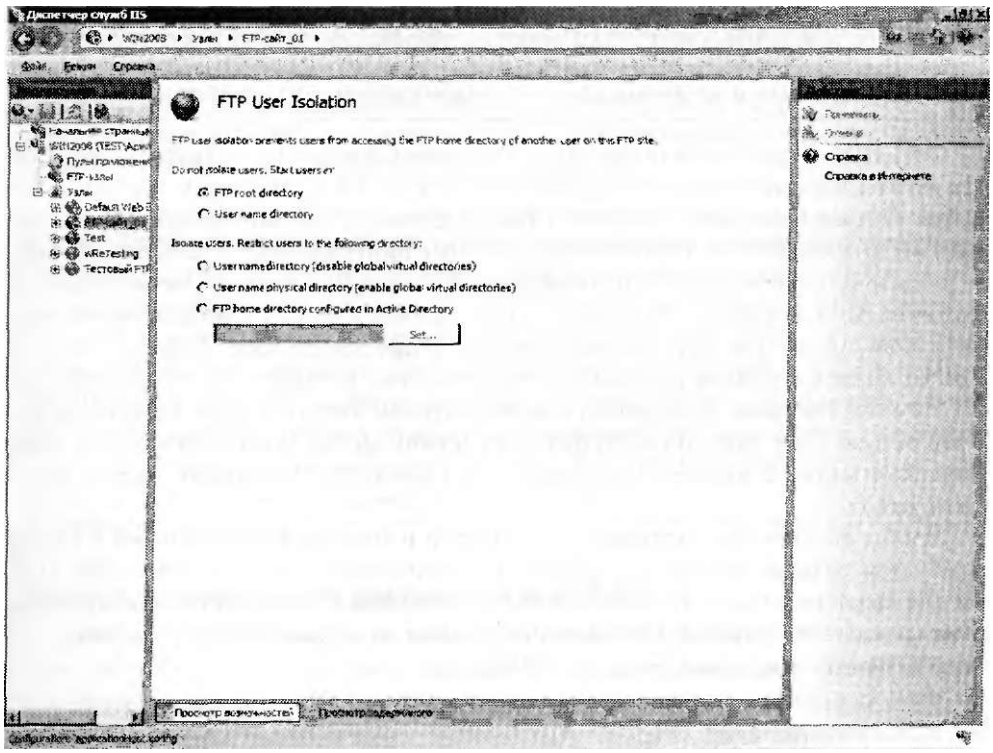


Рис. 7-23. Опции изоляции пользователей FTP

По умолчанию в этом окне назначена опция FTP root directory (Корневой каталог FTP). При выборе этой опции на сервере пользователи направляются в корневой каталог FTP, определяемый при создании FTP-сайта. Эту опцию удобнее всего использовать для обеспечения всем пользователям доступа к одному содержимому. Затем для определения разрешений конкретных папок можно применить правила авторизации.

При использовании опции User name directory (Корневой каталог пользователя) каждому пользователю назначается собственный корневой каталог с именем пользователя. Если имени папки конкретного пользователя не существует, пользователь будет помещен в корневой каталог FTP-сайта. Помните, что этот параметр не является заменой механизмов безопасности (по крайней мере если он используется сам по себе). Если на FTP-сайте разрешена анонимная проверка подлинности, вы можете создать для этих пользователей папку Default.

СОВЕТ Подготовка к экзамену
Параметрами безопасности FTP можно управлять с помощью различных компонентов, в частности Проверка подлинности (Authentication), Авторизация (Authorization) и Ограничения по 1РУ4-адресам и именам домена (IPv4 Address And Domain Restrictions). При реализации системы безопасности FTP-сайта лучше всего использовать комбинации этих компонентов. Например, параметры изоляции пользователя FTP можно использовать для определения файлов и содержимого, к которому будут иметь доступ пользователи. Затем для ограничения доступа к конкретному содержимому можно применить правила авторизации FTP. Помните об этом при обеспечении безопасности производственных FTP-серверов и во время сдачи сертификационного экзамена 70-643.

Остальные три опции позволяют обеспечить изоляцию пользователей FTP. Их можно использовать для ограничения доступа к конкретным папкам FTP-сайта. Опция User name directory (disable global virtual directories) (Корневой каталог пользователя (отключить глобальные виртуальные каталоги)) помещает пользователей в назначенный корневой каталог на основе учетной записи, применяемой для входа. Пользователь не сможет перейти к родительской папке и поэтому не сможет получать доступ к другим папкам. Пользователь не сможет просматривать глобальные виртуальные каталоги, определенные для FTP-сайта. Вы можете разрешить пользователям доступ к этим каталогам, выбрав опцию User name physical directory (enable global virtual directories) (Физическая папка с именем пользователя (включить глобальные виртуальные каталоги)).

Чтобы обеспечить поддержку параметров изоляции пользователей FTP, потребуется создать соответствующую структуру папок для пользователей. Папка для каждого пользователя может быть размещена в физическом или виртуальном каталоге на сервере. Путь к папке зависит от нескольких переменных.

- **FTPRoot** Корневой каталог FTP-сайта.
- **UserName** Имя пользователя, прошедшего проверку подлинности, которое было указано клиентом.
- **UserDomain** Имя домена Windows, используемое для подтверждения учетных данных, — имя локального FTP-сервера либо имя домена Active Directory (если сервер является членом домена).

Создаваемый путь к конкретной папке зависит от параметров проверки подлинности сайта и типа пользователя, который пытается получить доступ к содержимому. В табл. 7-1 приведен список размещений папок по умолчанию для каждого типа учетной записи.

Табл. 7-1. Размещения папок FTP по умолчанию для пользовательских учетных записей

Тип учетной записи пользователя FTP	Размещение корневого каталога
Анонимные пользователи	%FTPRoot%\LocalUser\Public
Локальные учетные записи Windows	%FTPRoot%\LocalUser\%UserName%
Доменные учетные записи Windows	%FTPRoot%\%UserDomain%\%UserName%
Учетные записи диспетчера IIS или ASP.NET	%FTPRoot%\LocalUser\%UserName%

Последней опцией изоляции пользователя FTP является опция FTP Home Directory Configured In Active Directory (Корневой каталог FTP в службе каталогов Active Directory). Такой тип изоляции можно использовать для определения FTP-папок пользователей в службе каталогов Active Directory с помощью переменных FTPRoot и FTPDir. Эти свойства существуют в доменах Active Directory с версией не ниже Windows Server 2003. (Для доменов Windows Server 2000 эти свойства можно добавить вручную.) Щелкнув кнопку Set (Задать), вы можете указать учетные данные, которые будут использоваться для подключения к Active Directory. Когда пользователь входит на FTP-сервер, сервер пытается получить эти свойства для пользователя. Если свойства существуют и путь к папке действителен, пользователь будет размещен в этой папке. В противном случае он не получит доступа к серверу.

ПРИМЕЧАНИЕ Создание учетных записей пользователей с помощью сценариев
Создание отдельных папок для множества пользовательских учетных записей может отнимать много времени и сил. Удачным решением в этой ситуации является использование сценариев. Вы можете получить список учетных записей пользователей с помощью самых разных методов, включая VBScript и Microsoft Windows PowerShell. Затем эту информацию можно использовать для выполнения команд, которые создадут необходимые папки. Более подробные сведения о сценариях можно найти на сайте Microsoft TechNet Script Center по адресу *http://www.microsoft.com/technet/scriptcenter*.

Настройка разрешений диспетчера служб IIS

Во многих средах существует множество администраторов, которые должны подключаться к FTP-серверам и содержимому для администрирования. Например, провайдер Веб и FTP может назначать отдельных администраторов для каждого FTP-сайта. С помощью компонента Разрешения диспетчера IIS (IIS Manager Permissions) вы можете разрешить другим пользователям получать доступ к сайту. Команда Разрешить пользователю (Allow User) позволяет добавить нового пользователя, определенного в Диспетчере служб IIS (IIS Manager) или на основе учетной записи Windows. После этого авторизованные пользователи могут с помощью диспетчера служб IIS на своих компьютерах подключаться к серверу FTP 7. Более подробные сведения о настройке разрешений диспетчера IIS содержатся в главе 6.

Настройка сетевой безопасности FTP

В FTP 7 реализованы многочисленные методы разрешения доступа к FTP-сайту только для авторизованных пользователей. В этом разделе речь пойдет об использовании SSL, параметров брандмауэра и ограничений по IP-адресам для управления доступом к FTP-сайтам.

Настройка параметров SSL для FTP-сайта

По умолчанию все коммуникации по каналам управления и каналам данных между FTP-сервером и клиентом осуществляются в открытом виде. Это является серьезной угрозой безопасности, особенно при обеспечении доступа FTP в Интернете. Например, если во время проверки подлинности будут перехватываться пакеты данных, имя пользователя и пароль могут быть извлечены и применены для получения доступа к сайту.

Администраторы могут шифровать коммуникации между сервером FTP 7 и FTP-клиентом с помощью стандарта FTP over SSL, который еще называется FTP/S или FTPS. Для модификации этих параметров в диспетчере служб IIS выберите соответствующий FTP-сайт и дважды щелкните компонент FTP SSL Settings (Параметры FTPS). Откроется окно, показанное на рис. 7-24.

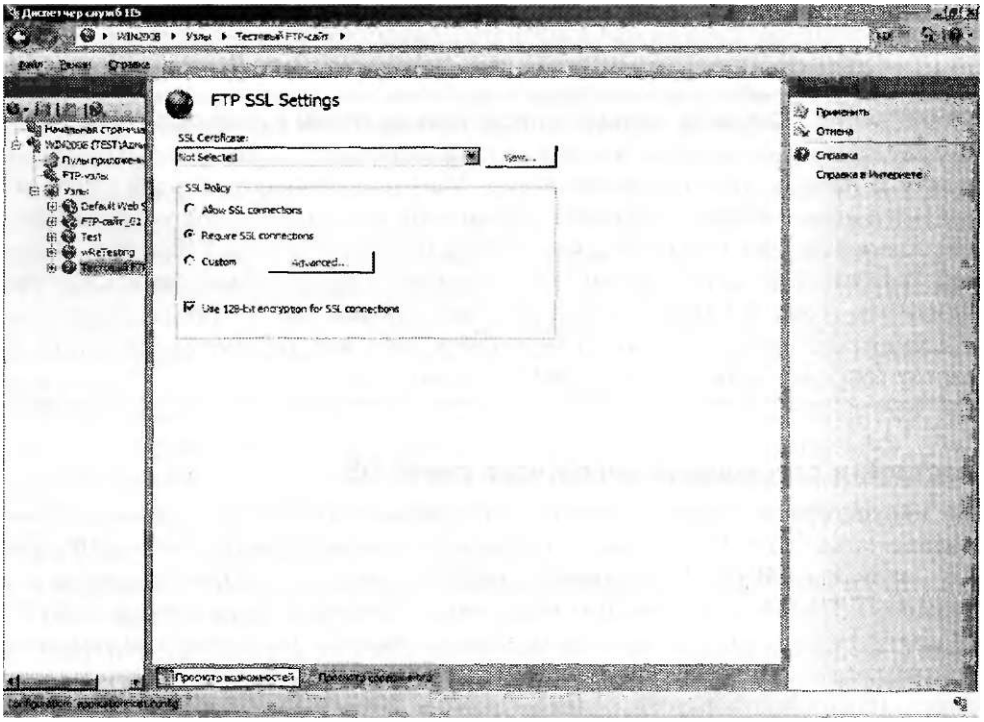


Рис. 7-24. Настройка параметров FTPS с помощью диспетчера служб IIS

Первый параметр позволяет указать сертификат SSL, который будет использоваться FTP-сайтом. Более подробно о создании и получении сертификатов SSL рассказывалось в главе 6. В области SSL Policy (Политика SSL) содержат-

ся три опции. При выборе опции Allow SSL Connections (Разрешить SSL-подключения) пользователи смогут подключаться к серверу с использованием SSL-подключений, но при этом смогут также выполнять незашифрованные подключения. При выборе опции Require SSL Connections (Требовать SSL-подключения) все пользователи должны будут применять SSL и не смогут устанавливать незашифрованные подключения, а опция Custom (Настроить) позволяет указать различные правила для управляющего канала (Control Channel) и канала данных (Data Channel), как показано на рис. 7-25. Эти опции можно использовать для уменьшения степени влияния шифрования на производительность. Например, требуя шифрование только для учетных данных, вы сможете запретить передачу пользовательских имен и паролей в открытом виде и разрешить выполнение и передачу других управляющих команд и данных без шифрования.

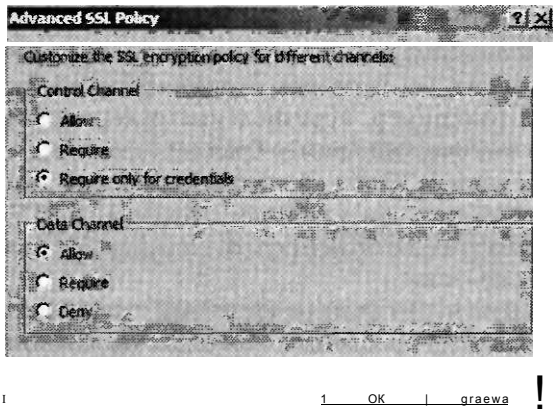


Рис. 7-25. Настройка дополнительной политики SSL для FTP-сайта

По умолчанию в шифровании FTPS будет использоваться ключ длиной 40 бит. Таким образом, для большинства сценариев будет поддерживаться соответствующий уровень безопасности без значительного влияния на производительность CPU. Для повышения строгости шифрования (и нагрузки CPU) вы можете установить флажок Use 128-Bit Encryption For SSL Connections (Использовать 128-битовое шифрование для SSL-подключений).

ПРИМЕЧАНИЕ Стандарты безопасности FTP
Стандарт Secure Shell (SSH) можно также использовать для обеспечения безопасности FTP-коммуникаций. Комбинация этих технологий иногда именуется как Secure FTP или SFTP. Системы безопасности на основе SSH не поддерживаются в Windows Server 2008 и FTP 7, однако вы можете столкнуться с этим стандартом в другом программном обеспечении FTP-сервера или опциях подключений FTP-клиентов.

Как правило, пользователи будут конфигурировать свои параметры SSL в своем программном обеспечении FTP-клиента. При попытке создать новое

подключение пользователь получит сообщение, в котором он сможет просмотреть сертификат и принять сертификат SSL, установленный для FTP-сервера.

Управление опциями брандмауэра FTP

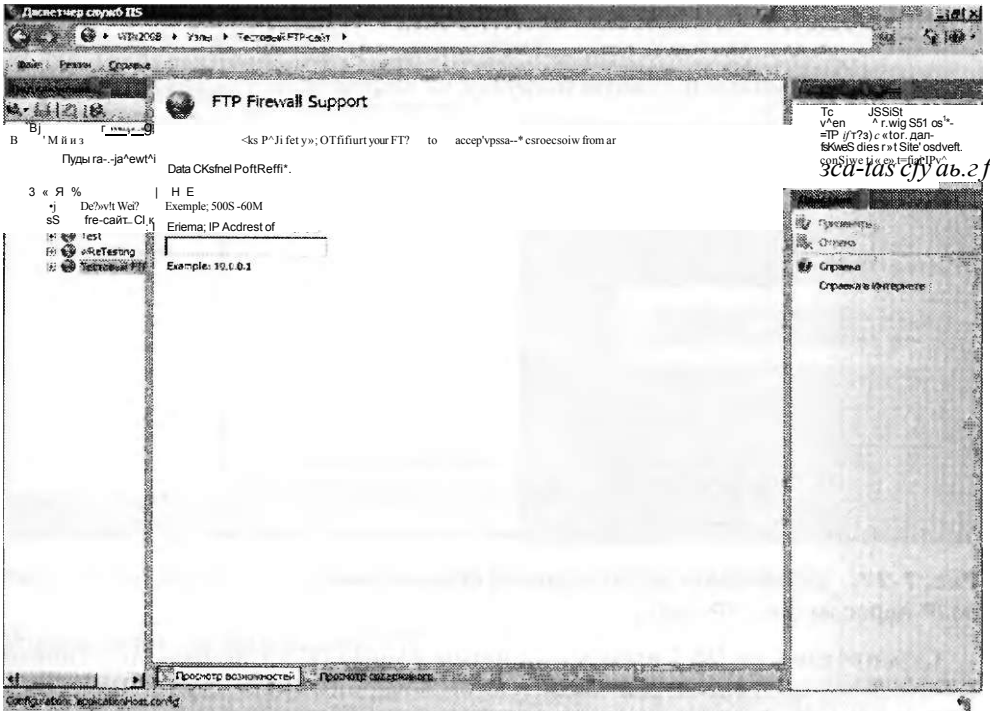
Для получения доступа к FTP-серверу брандмауэры должны разрешать передачу сетевого трафика для канала данных и управляющего канала. Когда пользователи подключаются к веб-серверу, исходное подключение создается с использованием порта, который указан в адресе. (Если номер порта не указан, используется порт 21 по умолчанию.) Однако передавая по каналу данных такую информацию, как списки каталогов и файлы, FTP-сервер может отвечать с помощью диапазона номеров портов. Если эти порты закрыты на брандмауэре, пользователи не смогут получить доступ ко всей функциональности сайта.

ПРИМЕЧАНИЕ Устранение распространенных неполадок FTP-подключений
Распространенная проблема FTP-подключений связана с получением доступа к FTP-серверу через брандмауэр. Так, пользователи могут подключаться к FTP-серверу и предоставлять учетные данные для проверки подлинности, однако при попытке выполнения действия (например, перечисления содержимого папки) они не получают ответ. Это классический пример брандмауэра, ограничивающего коммуникации по каналу данных. Один из способов решения этой проблемы состоит в том, чтобы включить пассивные FTP-подключения на FTP-клиенте. Второй способ — реконфигурирование брандмауэра. Помните об этом при устранении неполадок FTP-подключений.

Вы можете избежать возникновения этой проблемы с помощью компонента FTP Firewall Support (Поддержка брандмауэра FTP) в диспетчере служб IIS, который показан на рис. 7-26. В FTP 7 обеспечена поддержка FTP-подключений в пассивном режиме, позволяющая указать порты, на которых FTP-сервер будет отвечать на запросы.

Параметр Data Channel Port Range (Диапазон портов канала данных) позволяет указать диапазон портов, которые будут использоваться для передачи ответов клиентам. Следует указывать порты в диапазоне от 1024 до 65 535. Параметр External IP Address Of Firewall (Внешний IP-адрес брандмауэра) позволяет FTP-серверу определить адрес, с которого будет осуществляться отправка пакетов. Его удобно использовать для поддержки сценариев с SSL-шифрованием.

СОВЕТ Подготовка к экзамену
Для настройки реагирования FTP-сайта на FTP-команды и запросы используйте параметры компонента FTP Firewall Support. Он не вносит изменения непосредственно в конфигурацию брандмауэра системы Windows Server 2008 или других устройств в сети. Терминология иногда может сбивать с толку. При сдаче сертификационного экзамена 70-643 не забудьте отконфигурировать параметры FTP Firewall Support, чтобы они могли «работать» с параметрами брандмауэра. Кроме того, вам может потребоваться вручную изменить конфигурацию брандмауэра.



зса-tas cfy ab.z feey-aii.

Рис. 7-26. Конфигурирование опции поддержки брандмауэра FTP

Реализация ограничений по IP-адресам и именам домена

Вы можете повысить уровень безопасности FTP-сервера, ограничив сетевые адреса, с которых можно получать доступ к конкретным FTP-сайтам или папкам. Для управления этими параметрами в Диспетчере служб IIS (IIS Manager) выберите FTP-сайт или папку, а затем дважды щелкните компонент FTP IPv4 Address And Domain Restrictions (Ограничения FTP по 1Ру4-адресам н именам домена). В панели Действия (Actions) есть две команды для управления правилами: Add Allow Entry (Добавить разрешающее правило) и Add Deny Entry (Добавить запрещающее правило). Правила на основе IP-адресов позволяют указать отдельный IP-адрес или диапазон IP-адресов, определяемый с помощью маски подсети (рис. 7-27).

С помощью команды Edit Feature Settings (Изменить параметры) в панели Действия (Actions) можно указать действие по умолчанию для IP-адресов, которые не соответствуют существующим правилам. Параметр по умолчанию Allow (Разрешить) указывает, что этим IP-адресам будет разрешено подключаться. Выбрав опцию Deny (Запрет), вы можете разрешить доступ лишь тем клиентам, для которых установлены разрешающие правила.

Ограничения доменных имен можно также включить в диалоговом окне Edit Feature Settings (Изменить параметры). Ограничения доменных имен основаны на системе именования DNS. Хотя ими управлять иногда проще, чем правилами для IP-адресов, эти ограничения могут значительно влиять на быстродействие.

Причина такого недостатка заключается в том, что для оценки правил выполняется операция обратного поиска DNS, которая может занимать много времени и создавать дополнительную нагрузку на инфраструктуру DNS.

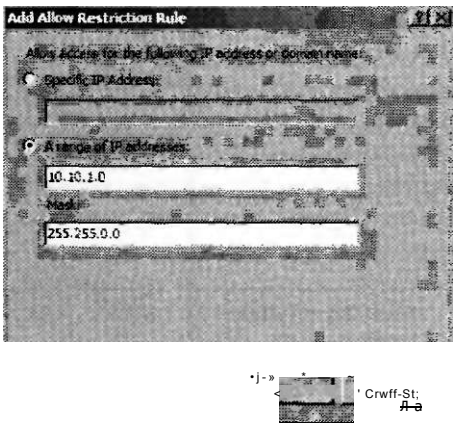


Рис. 7-27. Добавление нового правила ограничения по IP-адресам для FTP-сайта

Ограничения по 1Py4-адресам и именам домена (IPv4 Address And Domain Restrictions) автоматически наследуются дочерними объектами. Например, ограничения, определенные на уровне FTP-сайта, автоматически применяются ко всем папкам сайта. Вы можете изменить это поведение, создав явные правила для конкретных папок и виртуальных каталогов. Для удаления всех специфических параметров используется команда Revert To Parent (Вернуться к унаследованным) в панели Действия (Actions).

Управление параметрами FTP-сайта

В FTP 7 включены возможности мониторинга и повышения комфорта пользователей. В этом разделе вы изучите данные опции конфигурации, а также способы отслеживания использования FTP-сайта.

Мониторинг текущих сеансов FTP

Компонент FTP Current Sessions (Текущие сеансы FTP) для FTP-сайта можно использовать для отслеживания текущих пользователей, которые подключены к серверу (рис. 7-28). Он отображает следующие сведения:

- User Name (Имя пользователя);
- Client IP Address (IP-адрес клиента);
- Session Start Time (Время запуска сеанса);
- Current Command (Текущая команда);
- Previous Command (Предыдущая команда);
- Command Start Time (Время запуска команды);
- Bytes Sent (Передано байтов);
- Bytes Received (Принято байтов);
- Session ID (ID сеанса).

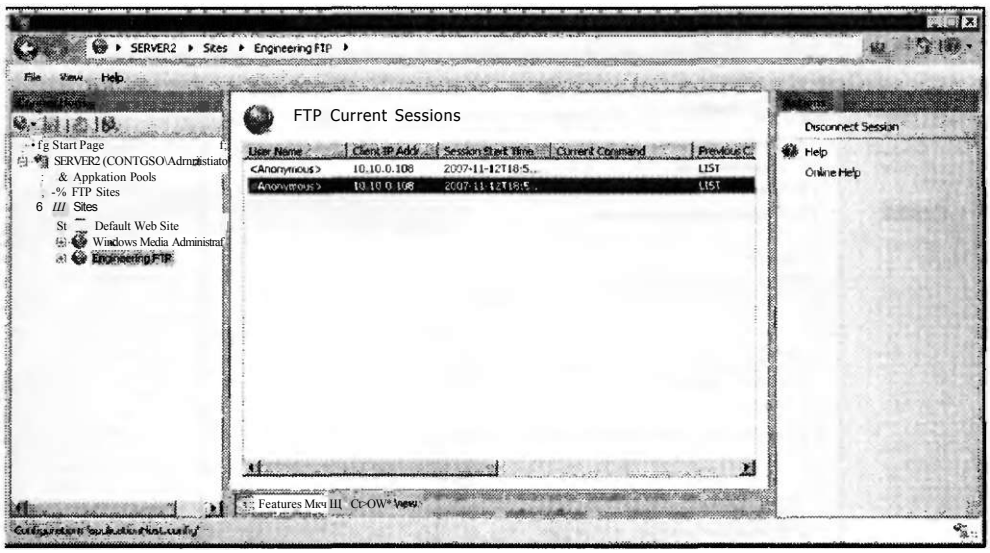


Рис. 7.28. Просмотр текущих сеансов FTP в диспетчере служб IIS

Управление сообщениями FTP

Компонент FTP Messages (Сообщения FTP) можно использовать для определения текстовых сообщений, которые будут пересылаться клиенту. Вы можете определить следующие типы текстовых сообщений.

- **Banner (Заголовок)** Это сообщение пользователь получает при подключении к FTP-сайту.
- **Welcome (Приветствие)** Отображается после успешной проверки подлинности пользователя на FTP-сайте.
- **Exit (Выход)** Отображается после завершения подключения пользователем и передается непосредственно перед закрытием подключения.
- **Maximum Connections (Максимальное число подключений)** Это сообщение отображается в случае, когда на сервере достигнуто максимальное количество подключений и пользователь не может получить доступ к сайт}'.

FTP-сообщения часто включают предупреждения, связанные с использованием сайта, а также могут содержать контактные данные для администраторов сайта, как показано на рис. 7-29.

В области Message Behavior (Поведение сообщений) можно изменить поведение заголовка, например, чтобы скрыть сведения о назначении сайта, пока пользователи не пройдут проверку подлинности. Опция Support User Variables In Messages (Поддержка пользовательских переменных в сообщениях) позволяет использовать в сообщениях следующие строковые значения:

- Bytes Received;
- BytesSent;
- SessionID;
- SiteName;
- UserName.

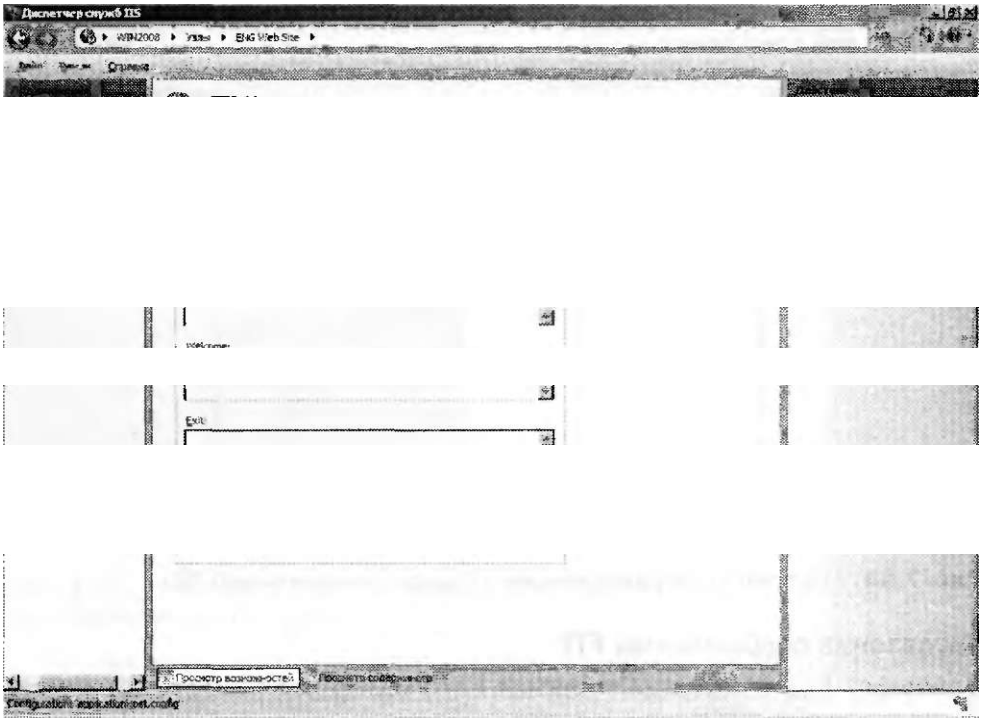


Рис. 7-29. Настройка FTP-сообщений для FTP-сайта

Отметим, что если переменная заключена в символы процентов (например, %UserName%), FTP-сервер автоматически подставит в переменную соответствующее значение.

Настройка ведения журнала FTP

В FTP 7 можно автоматически создавать файлы журналов, отслеживающих использование FTP-сайта. По умолчанию эти сведения хранятся в текстовых файлах, которые помещаются в папку %SystemDrive%\Inetpub\Logs\LogFiIes. Для каждого FTP-сайта, создаваемого на локальной машине, создаются отдельные папки. Для модификации параметров файлов журнала можно использовать компонент FTP Logging (Ведение журнала FTP).

С помощью команды Select W3C Fields (Выбрать поля W3C) указываются типы данных, которые будут отслеживаться при выполнении каждой команды или запроса на FTP-сервере. На рис. 7-30 показаны опции по умолчанию, предназначенные для обеспечения баланса между подробной информацией, производительностью и размером файлов журнала.

В области Log File. Rollover (Создание нового файла журнала) можно указать, когда следует создавать новые файлы журналов. Для управления FTP-серверами во множестве временных поясов также можно использовать опцию Use Local Time For File Naming And Rollover (Использовать локальное время для создания и именования файлов). С помощью команды View Logs (Просмотр журналов) в панели Действия (Actions) открывается папка, содержащая файлы журнала FTP. Эти файлы представляют собой текстовые документы, содержащие разде-

ленные запятыми значения. Их можно просмотреть в программе Блокнот Windows (Windows Notepad) или с помощью программного обеспечения для анализа журналов от сторонних производителей. Следует регулярно просматривать журнал FTP-сервера, чтобы определять неавторизованные действия или нежелательное использование сайтов.

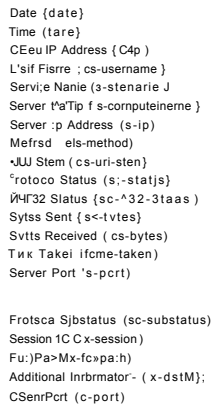


Рис. 7-30. Выбор полей для включения в файлы журнала FTP

Настройка просмотра каталога

Одной из самых распространенных команд, отправляемых FTP-клиентами, является запрос просмотра каталога. Обычно программное обеспечение FTP-клиентов автоматически выполняет команду LIST каждый раз при изменении пользователем текущей рабочей папки. Эти опции можно настроить, выбрав сайт в диспетчере служб IIS и дважды щелкнув компонент FTP Directory Browsing (Просмотр каталога FTP), как показано на рис. 7-31. В области Directory Listing Style (Стиль просмотра каталога) можно указать стиль MS-DOS (по умолчанию) или UNIX для возвращаемой информации. Данный параметр определяет предоставление этих сведений для FTP-клиента. Большинство FTP-клиентов могут обрабатывать оба формата.

В области Directory Listing Options (Опции просмотра каталога) можно указать типы сведений, которые будут включены в просмотр каталога. Если установлен флажок Virtual Directories (Виртуальные каталоги), пользователю будут возвращаться названия виртуальных каталогов. Чтобы скрыть названия виртуальных каталогов от пользователей, сбросьте этот флажок. При выборе опции Available Bytes (Доступно байт) возвращается объем свободного дискового пространства для FTP-сайта. В случае включения дисковых квот будет возвращаться объем свободного дискового пространства для текущего подключенного пользователя. Если установлен флажок Four-Digit Years (Годы из четырех знаков), вся информация будет возвращаться в четырех символах, а не в двух.

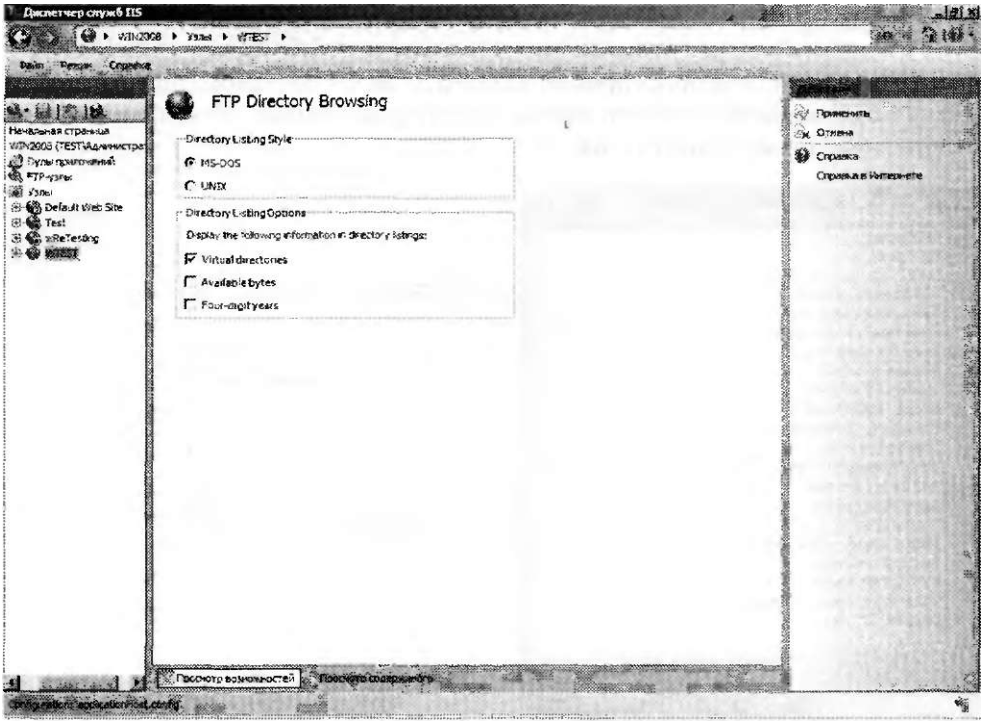


Рис. 7-31. Настройка параметров просмотра каталога FTP

Программное обеспечение FTP-клиента

Для подключения к FTP-серверу пользователи могут применять FTP-клиенты нескольких типов. Операционные системы Windows содержат утилиту командной строки FTP, обеспечивающую текстовые функции для подключения к FTP-серверу. Ее удобно использовать при выполнении простых операций и тестирования функциональности веб-сайтов. Команды FTP также можно поместить в пакетный файл для автоматизации таких операций, как передача резервных файлов на удаленный сервер.

Кроме того, для подключения к FTP-сайту можно использовать веб-браузер с возможностями FTP, такой как Windows Internet Explorer (рис. 7-32). Для URL применяется стандартный синтаксис Лр://Имя_сервера. В URL также можно указать учетные данные и порт, применив следующий синтаксис:

```
ftp://Имя_пользователя:Пароль:Имя_сервера:Порт/Путь
```

URL-адреса FTP удобно использовать для получения быстрого доступа к файлам с веб-сайтов. Важно отметить, что по умолчанию все коммуникации осуществляются с использованием незашифрованных подключений.' Поэтому URL-адреса FTP следует использовать лишь при работе с FTP-сайтами, предназначенными для анонимных пользователей.

Для графического доступа к FTP-сайту можно также использовать проводник Windows (Windows Explorer), как показано на рис. 7-33. Этот метод позволяет применять знакомые команды и функции, например операции перетаски-

вания и вставки. Для подключения просто введите URL-адрес FTP в адресную строку проводника Windows. Если вы уже подключились к FTP-сайту, вы также можете использовать команду Открыть FTP-узел (Open FTP Site) из меню Страница (Page) обозревателя Internet Explorer. Хотя возможности управления файлами и папками ограничены, с помощью данного метода к содержимому FTP могут подключаться даже неопытные пользователи.

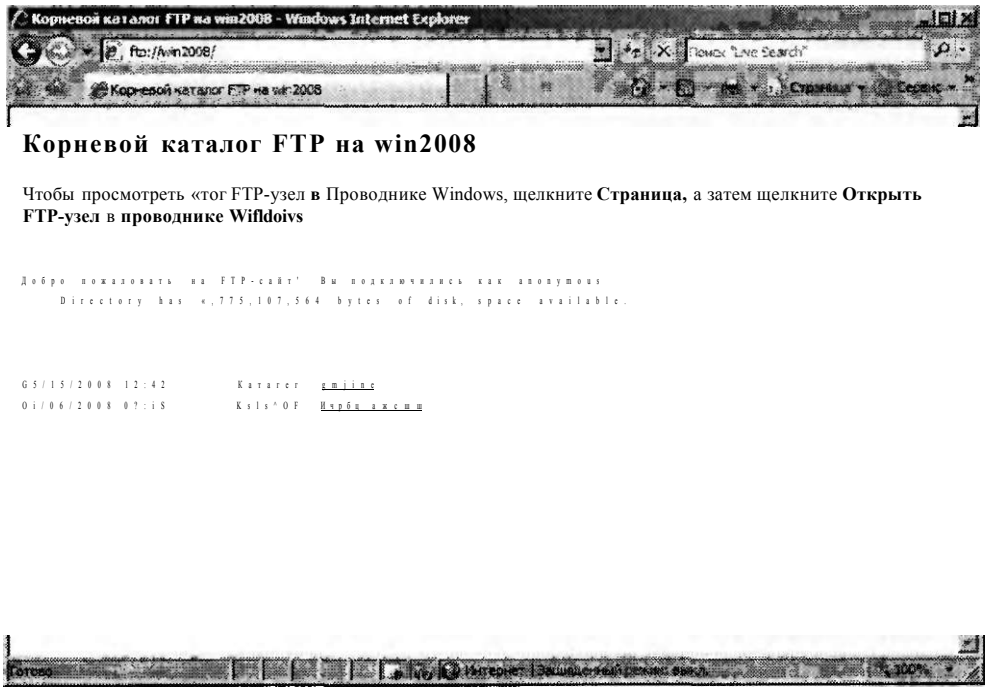


Рис. 7-32. Подключение к FTP-сайту с помощью Internet Explorer 7

Проверьте себя

1. Как в FTP 7 проще всего запретить отдельной группе пользователей получать доступ к конкретной папке FTP-сайта?
2. Каким образом можно добиться того, чтобы учетные данные, передаваемые на FTP-сайт в Интернете с использованием обычной проверки подлинности, шифровались во время передачи?

Ответы

1. Чтобы назначить конкретные разрешения для папки FTP-сайта, можно использовать правила авторизации FTP.
2. С помощью FTP 7 нужно включить для FTP-сайта стандарт FTP Over SSL (FTPS). При этом требуется получить SSL-сертификат сервера, а затем требовать SSL, по крайней мере при передаче учетных данных на сервер.

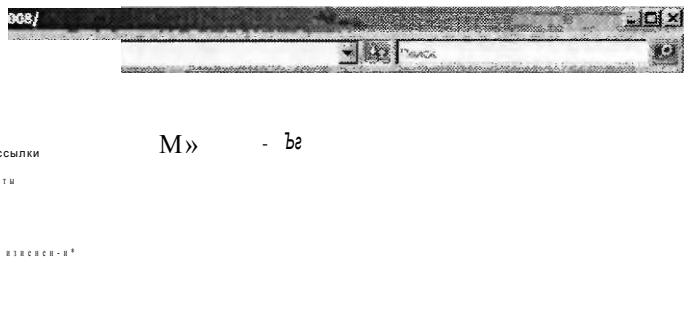


Рис. 7-33. Использование проводника **Windows** для **получения доступа к FTP-сайту**

Практикум. Настройка и тестирование FTP

В предложенных далее упражнениях вы настроите FTP-сайт с помощью версий FTP 6 и FTP 7. Затем вы подключитесь к новому сайту с помощью утилиты командной строки FTP.

Упражнение 1. Использование FTP 6 для создания нового веб-сайта

В этом упражнении вы с помощью FTP 6 создадите новый веб-сайт. Вы начнете упражнение с включения FTP 6. Предполагается, что вы установили роль Веб-сервер (IIS) (Web Server (IIS)) с опциями по умолчанию, но еще не установили службу ролей Служба FTP-публикации (FTP Publishing Service).

1. Войдите на сервер Server2 в качестве пользователя с административными привилегиями.
2. Откройте Диспетчер сервера (Server Manager). Разверните узел Роли (Roles), щелкните правой кнопкой мыши роль Веб-сервер (IIS) (IIS Web Server) и примените команду Добавить службы ролей (Add Role Services).
3. На странице Выбор служб ролей (Select Role Services) выберите Службу FTP-публикации (FTP Publishing Service). Отметим, что вместе с ней будут автоматически установлены службы ролей FTP-сервер (FTP Server) и Консоль управления FTP (FTP Management Console). Щелкните кнопку Далее (Next).
4. На странице Подтвердите выбранные элементы (Confirm Installation Selections) щелкните кнопку Установить (Install) для запуска процесса установки. После завершения установки щелкните кнопку Готово (Finish).

5. В Диспетчере сервера (Server Manager) проверьте, чтобы для роли Веб-сервер (IIS) была установлена Служба FTP-публикации (FTP Publishing Service). Закройте диспетчер сервера.
6. Для настройки FTP-сервера в группе программ Администрирование (Administrative Tools) запустите Диспетчер служб IIS 6.0 (IIS 6.0 Manager).
7. Разверните узел Server2 и откройте папку FTP-узлы (FTP Sites). Обратите внимание на то, что объект Default FTP Site существует, но не запускается автоматически.
8. Щелкните правой кнопкой мыши объект Default FTP Site и примените команду Свойства (Properties). Просмотрите параметры на вкладке FTP-узел (FTP Site). По умолчанию FTP-сайт отвечает на все неуказанные IP-адреса на TCP-порте 21.
9. Перейдите на вкладку Корневой каталог (Home Directory) и просмотрите параметры размещения корневого каталога FTP-сайта в файловой системе. По умолчанию корневой каталог расположен в папке %SystemDrive%\Inetpub\Ftproot. Для содержимого папки по умолчанию включено только разрешение Чтение (Read).
10. Щелкните ОК, чтобы закрыть диалоговое окно Свойства: Default FTP Site (Default FTP Site Properties).
11. Далее для тестирования функциональности FTP вы создадите некоторые файлы. С помощью проводника Windows откройте корневой каталог FTP-сайта и создайте новую папку FTPContents. В этой папке создайте новый текстовый файл TestFile.txt. Закройте проводник Windows.
12. В Диспетчере служб IIS 6.0 (IIS 6.0 Manager) щелкните правой кнопкой мыши объект Default FTP Site и примените команду Пуск (Start), чтобы запустить сайт Default FTP Site. Далее вы используете утилиту командной строки FTP для проверки конфигурации FTP-сайта.
13. В меню Пуск (Start) щелкните элемент Командная строка (Command Prompt), чтобы открыть окно командной строки. Для подключения к локальному FTP-серверу введите команду FTP Server2. Отметим, что вам не потребуется указывать номер порта, поскольку сервер по умолчанию привязан к TCP-порту 21.
14. В строку Пользователь (User) введите имя вашей учетной записи Windows. Затем в строку Пароль (Password) введите пароль. В строку FTP введите *dir* и нажмите клавишу Enter, чтобы извлечь список файлов в корневом каталоге сайта Default FTP Site. Вы должны увидеть папку FTPContents, созданную в шаге 11.
15. Для изменения активной папки введите *cd FTPContents.* Для просмотра списка файлов введите команду *dir.* Для загрузки копии файла, созданного ранее в локальной рабочей папке, введите команду *get TestFile.txt.*
16. Чтобы закрыть командную строку FTP, введите команду *quit.* Затем закройте окно командной строки.
17. Закройте Диспетчер служб IIS 6.0 (IIS 6.0 Manager).

Упражнение 2. Использование FTP 7 для добавления привязки FTP-узла

В этом упражнении вы с помощью FTP 7 и Диспетчера служб IIS (IIS Manager) создадите новую привязку для сайта Default FTP Site. Перед тем как приступать к упражнению, нужно удалить версию FTP 6, если она установлена на сервере Server2.contoso.com, затем загрузить и установить FTP 7 по адресу *http://www.iis.net/downloads*.

1. Войдите на сервер Server2 в качестве пользователя с административными привилегиями.
2. Откройте Диспетчер служб IIS (IIS Manager) и подключитесь к локальному серверу.
3. В левой панели щелкните правой кнопкой мыши объект Default Web Site и примените команду Изменить привязки (Edit Bindings). В диалоговом окне Привязки узла (Site Bindings) щелкните кнопку Добавить (Add).
4. В диалоговом окне Добавление привязки узла (Add Site Binding) выберите в раскрывающемся списке Тип (Type) тип привязки FTP. Используйте параметр IP-адреса Все неназначенные (All Unassigned) и порт 21 по умолчанию. Поле Имя узла (Host Name) оставьте пустым. Чтобы добавить привязку узла, щелкните OK.
5. Проверьте, создана ли новая привязка узла для FTP-протокола на порте 21. Чтобы закрыть диалоговое окно Привязки узла (Site Bindings), щелкните кнопку Закрыть (Close).
6. Чтобы просмотреть FTP-опции для сайта Default Web Site, в меню Режим (View) Диспетчера служб IIS (IIS Manager) щелкните кнопку Обновить (Refresh). Появится область FTP с опциями настройки FTP. В панели Действия (Actions) появятся также команды для управления FTP-сайтом.
7. В области Manage FTP Site (Управление FTP-узлом) панели Действия (Actions) щелкните команду Advanced Settings (Дополнительные параметры). Отметим, что параметр Physical Path (Физический путь) сопоставлен с корневым каталогом сайта Default Web Site (%SystemDrive%\Inetpub\Wwwroot). Щелкните OK.
8. В режиме Просмотр возможностей (Features View) диспетчера служб IIS дважды щелкните компонент FTP Authentication (Проверка подлинности FTP). Отметим, что по умолчанию проверка подлинности не включена. Включите опции Basic Authentication (Обычная проверка подлинности) и Anonymous Authentication (Анонимная проверка подлинности), выбрав каждую по-очереди и применив команду Enable (Включить) в панели Действия (Actions).
9. Чтобы вернуться к режиму Просмотр возможностей (Features View), щелкните кнопку Назад (Back) или объект Default Web Site.
10. Откройте компонент FTP SSL Settings (Параметры FTP SSL). Отметим, что по умолчанию сервер использует опцию Require SSL Connections (Требовать SSL-подключения). Задайте опцию Alow SSL Connections (Разрешать SSL-подключения). При желании вы можете выбрать в раскрывающемся списке сертификат SSL. Для сохранения изменений щелкните команду Применить (Apply).

11. Далее вы используете утилиту командной строки FTP для тестирования доступа к FTP-сайту. Откройте окно командной строки, выбрав ее в меню Пуск (Start). Чтобы подключиться к локальному FTP-серверу, введите команду *FTP Server2.* Номер порта вам не потребуется указывать, поскольку сервер по умолчанию привязан к TCP-порту 21.
12. В строку Пользователь (User) введите имя вашей учетной записи Windows. Затем в строку Пароль (Password) введите пароль. В строку FTP введите *dir* и нажмите клавишу Enter, чтобы извлечь список файлов корневого каталога сайта Default FTP Site. При желании вы можете использовать команды *GET* и *PUT* для загрузки и выгрузки файлов. Затем для выхода из командной строки FTP введите команду *quit.* Закройте окно командной строки.
13. Закройте Диспетчер IIS (IIS Manager).

Резюме

- Чтобы управлять FTP-сайтами с помощью FTP 6, для роли Веб-сервер (IIS) (Web Server (IIS)) нужно добавить Службу FTP-публикации (FTP Publishing Site).
- Диспетчер служб IIS 6.0 (IIS 6.0 Manager) можно использовать для создания параметров сайтов FTP 6 и управления ими.
- Чтобы в Windows Server 2008 использовать FTP 7, нужно загрузить и установить отдельный пакет программного обеспечения.
- В FTP 7 обеспечены многочисленные улучшения по сравнению с версией FTP 6, в том числе поддержка зашифрованных SSL-подключений, упрощенной конфигурации с использованием Диспетчера служб IIS (IIS Manager) и возможность создания привязок FTP для веб-сайтов.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных в ходе занятия 1. Эти вопросы представлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы

Ответы и пояснения к каждому их варианту размещены в разделе «Ответы» в конце книги.

1. Вы являетесь системным администратором Windows Server 2008 и отвечаете за конфигурирование службы FTP-публикации для использования техническими сотрудниками организации. Серверу присвоено имя FTPServerOl. Некоторые пользователи сообщают, что они могут получить доступ к большинству файлов на FTP-сайте, но не могут получить доступ к содержимому папки Drawings. Вы убедились, что учетные записи этих пользователей располагают соответствующими разрешениями файловой системы для этой папки. Вы хотите свести к минимуму набор разрешений для всех пользователей. Какие из следующих изменений следует внести, чтобы пользователи могли получать доступ к этой папке?

   A. Изменить разрешения учетной записи IUSR_FTPServer01 для папки Drawings.

Б. Создать новые ограничения по TCP/IP-адресам для пользователей, которые не могут получать доступ к папке Drawings,

В. Отключить опцию Разрешать только анонимные подключения (Allow Only Anonymous Connections).

Г. Добавить пользователей в локальную группу администраторов на сервере FTPServer2.

2. Вы являетесь системным администратором и недавно установили и настроили FTP 7 на компьютере Windows Server 2008. Вы включили для сервера опцию FTP Over SSL (FTPS) и получили сертификат SSL из доверенного стороннего центра сертификации. В последнее время FTP-сайт стал использоваться намного интенсивнее, и пользователи стали жаловаться на заметное снижение быстродействия. Вы хотите отконфигурировать параметры SSL, чтобы шифровать только учетные данные и команды, а не сведения, связанные с файлами. Вы также хотите оптимизировать шифрование. Какие из следующих изменений следует внести в систему? (Выберите два варианта. Каждый отдельный вариант является частью полного ответа.)

А. Применить политику Allow SSL Connections (Разрешить SSL-подключения).

Б. Сбросить флажок Use 128-bit Encryption For SSL Connection (Использовать 128-разрядный SSL).

В. Применить политику Require SSL Connections (Требовать SSL-подключения).

Г. Применить собственную политику SSL (Custom SSL Policy).

Занятие 2. **Конфигурирование SMTP**

Компонент SMTP (Simple Mail Transfer Protocol) системы Windows Server 2008 позволяет передавать сообщения электронной почты. Стандарт SMTP обеспечивает согласованный метод, с помощью которого серверы могут отправлять сообщения. Его можно использовать для внутреннего трафика электронной почты или коммуникаций в Интернете. Отдельные пользователи и приложения часто используют функции SMTP для отправки уведомлений и другой информации. На этом занятии мы обсудим, как включить и отконфигурировать SMTP-сервер в Windows Server 2008.

Изучив мвтериал этого занятия, вы сможете:

- Включить SMTP-сервер в Windows Server 2008.
- Создать виртуальный SMTP-сервер.
- Конфигурировать параметры IP-адресов и портов для виртуального SMTP-сервера.
- Обеспечивать безопасность SMTP-служб путем настройки параметров проверки подлинности для входящих и исходящих подключений.
- Тестировать SMTP-службы с помощью клиентского приложения электронной почты.

Расчетная продолжительность занятия составляет 45 мин.

Установка сервера SMTP

Компонент Сервер SMTP (SMTP Server) системы Windows Server 2008 позволяет поддерживать много приложений и сетевых подключений для отправки больших объемов данных в сообщениях. Например, веб-приложение может использовать SMTP для отправки пользователям уведомлений электронной почты. Стандарт SMTP предназначен для отправки электронных сообщений, которые может принимать такой сервер сообщений, как Microsoft Exchange Server. Сообщения также можно хранить в файловой системе, чтобы к ним могли получать доступ другие приложения. Пользователи, как правило, получают эти сообщения, подключаясь к своим почтовым ящикам на сервере сообщений с помощью таких протоколов, как Post Office Protocol (POP).

Вы можете установить сервер SMTP на компьютере Windows Server 2008 с помощью Диспетчера сервера (Server Manager). Для этого щелкните правой кнопкой мыши объект Компоненты (Features) и примените команду Добавить компоненты (Add Features). Для SMTP-сервера существуют некоторые зависимости, как показано на рис. 7-34.

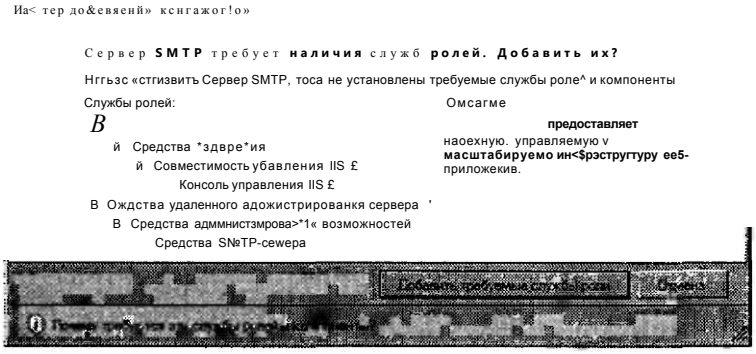


Рис. 7-34. Зависимости сервера SMTP

Удаление сервера SMTP также выполняется с помощью диспетчера сервера. Для этого щелкните правой кнопкой мыши объект Компоненты (Features) и примените команду Удалить компоненты (Remove Features). После удаления сервера SMTP вы не сможете использовать сервер для обмена электронными сообщениями.

Настройка служб SMTP

После установки сервера SMTP на компьютер Windows Server 2008 для настройки служб SMTP можно использовать Диспетчер служб IIS 6.0 (IIS 6.0 Manager). Откройте Диспетчер служб IIS 6.0 и разверните объект сервера. При добавлении сервера SMTP в конфигурацию автоматически добавляется сайт по умолчанию SMTP Virtual Server #1.

Создание виртуального сервера SMTP

Виртуальный сервер SMTP можно создать в системе Windows Server 2008 с помощью Мастера создания виртуального SMTP-сервера (New SMTP Virtual

Server Wizard). Каждый виртуальный сервер располагает собственным набором параметров конфигурации с независимым управлением. Чтобы с помощью диспетчера служб IIS 6.0 создать виртуальный сервер SMTP, щелкните объект сервера правой кнопкой мыши, выберите меню Создать (New) и щелкните опцию Виртуальный SMTP-сервер (SMTP Virtual Server). На первой странице мастера вам будет предложено ввести имя для виртуального сервера. Следует использовать описательное имя, указывающее назначение виртуального сервера, поскольку в пользовательском интерфейсе диспетчера служб IIS 6.0 будут идентифицироваться различные серверы.

На странице Выберите IP-адрес (Select IP Address) выберите IP-адрес для виртуального сервера SMTP. Если на сервере установлено множество физических сетевых адаптеров или IP-адресов, вы можете выбрать конкретный адрес в раскрывающемся списке. Таким образом вы сможете ограничить доступ к SMTP-серверу для обеспечения безопасности. Например, если один или несколько IP-адресов доступны в Интернете, вы можете запретить серверу отвечать по этому адресу. По умолчанию используется параметр IP-адреса Все неназначенные (All Unassigned), то есть виртуальный сервер SMTP будет отвечать по всем IP-адресам, отконфигурированным на сервере.

Еще одна причина изменения IP-адреса состоит в том, что два виртуальных сервера SMTP не могут запускаться одновременно, если им присвоен один IP-адрес и порт. По умолчанию SMTP-подключения используют порт 25. Если вы попытаетесь создать новый виртуальный SMTP-сервер, используя ту же комбинацию IP-адреса и номера порта, то получите сообщение об ошибке, как показано на рис. 7-35. В данном случае вы можете продолжить создание сервера, однако позже вам придется модифицировать параметры для его запуска.

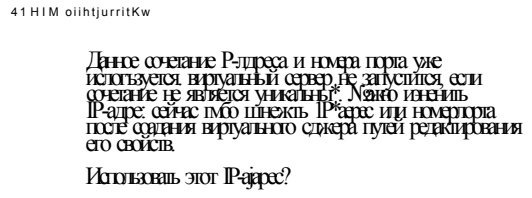


Рис. 7-35. Предупреждение конфигурации SMTP

На странице Выберите корневой каталог (Select Home Directory) укажите размещение корневого каталога виртуального SMTP-сервера в файловой системе, как показано на рис. 7-36. В ней будут храниться файлы сообщений и другие данные.

На странице (Default Domain) следует указать полное имя домена, на запросы которого будет отвечать виртуальный сервер SMTP. Обычно используется доменное имя DNS, например hr.contoso.com. После завершения работы мастера создания виртуального SMTP-сервера новый сервер появится в панели диспетчера служб IIS 6.0. Затем вы сможете получить доступ к свойствам сервера и внести дополнительные изменения в конфигурацию.

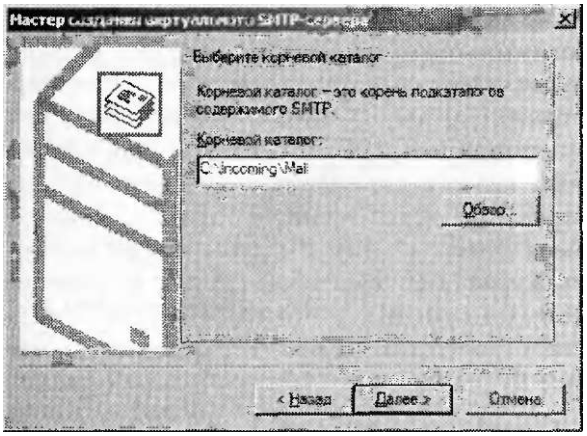
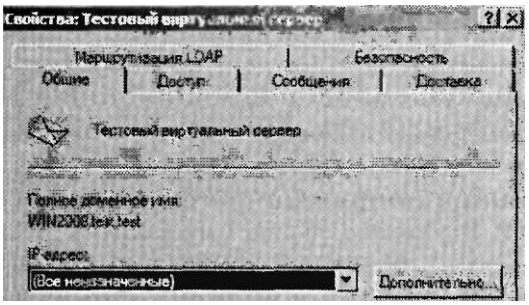


Рис. 7-36. Указание размещения корневого каталога нового виртуального сервера SMTP в файловой системе

Настройка основных параметров сервера SMTP

Для получения доступа к параметрам конфигурации виртуального сервера SMTP щелкните его правой кнопкой мыши в Диспетчере служб IIS 6.0 (I1S 6.0 Manager) и примените команду Свойства (Properties). На вкладке Общие (General) можно указать параметры сетевых подключений сервера SMTP, как показано на рис. 7-37.



jit ~

— r - r

III • 'fefffffiiT&MIi^'/jdwWfiZ ..

b '...

Рис. 7-37. Настройка основных параметров виртуального сервера SMTP

В раскрывающемся списке можно выбрать IP-адрес или параметр Все неназначенные (All Unassigned). Щелкнув кнопку Дополнительно (Advanced), вы можете отконфигурировать несколько идентификаторов для виртуального сервера. Щелкнув кнопку Дополнительно (Advanced), вы также можете изменить номер порта, на котором можно получать доступ к SMTP-серверу. На вкладке Общие (General) можно ограничить число подключений и назначить для них время ожидания. Конфигурирование этих ограничений способствует повышению быстродействия перегруженных серверов SMTP. Вы также можете использовать опцию Включить ведение журнала (Enable Logging) для сохранения данных о сообщениях, пересылаемых с помощью этого виртуального SMTP-сервера. Щелкнув кнопку Свойства (Properties), вы можете указать место хранения файлов журнала. На вкладке Дополнительно (Advanced) можно указать типы данных, которые будут включены в файл журнала. Эти файлы можно просматривать с помощью стандартного текстового редактора, такого как Блокнот Windows (Windows Notepad). При ведении журнала на перегруженных SMTP-серверах может снизиться производительность и увеличиться объем используемого дискового пространства.

Безопасность доступа к виртуальному серверу SMTP

Для предотвращения нежелательного использования виртуальных серверов SMTP важно отконфигурировать правила доступа для отправки соответствующих сообщений. Через незащищенные серверы SMTP приходит большое количество ненужной коммерческой электронной почты — так называемый спам. Правилами использования виртуального сервера SMTP можно управлять с помощью свойств на вкладке Доступ (Access), показанной на рис. 7-38.

Щелкнув кнопку Проверка подлинности (Authentication), вы можете определить, каким образом потенциальные пользователи виртуального сервера SMTP должны проходить проверку подлинности. Доступные опции показаны на рис. 7-39. По умолчанию назначен Анонимный доступ (Anonymous Access), то есть пользователям не нужно указывать свои учетные данные при подключении к виртуальному серверу SMTP. Эту опцию удобно использовать в тех случаях, если вы применяете другие методы (например, брандмауэры или безопасные сетевые подключения) для предотвращения неавторизованного доступа к серверу.

При выборе опции Обычная проверка подлинности (Basic Authentication) пользователям потребуется передавать на виртуальный сервер SMTP имя и пароль. По умолчанию эти учетные данные передаются в открытом виде и, следовательно, могут быть перехвачены. Вы можете включить шифрование Transport Layer Security (TLS) для передачи сообщений. Для создания зашифрованных подключений протокол TLS использует сертификаты. Для проверки учетных данных интегрированная проверка подлинности Windows использует стандартные учетные записи Windows. Этот метод лучше всего применять для приложений, которые будут использоваться одной учетной записью Windows или когда все потенциальные пользователи сервера SMTP располагают учетными записями домена Active Directory.

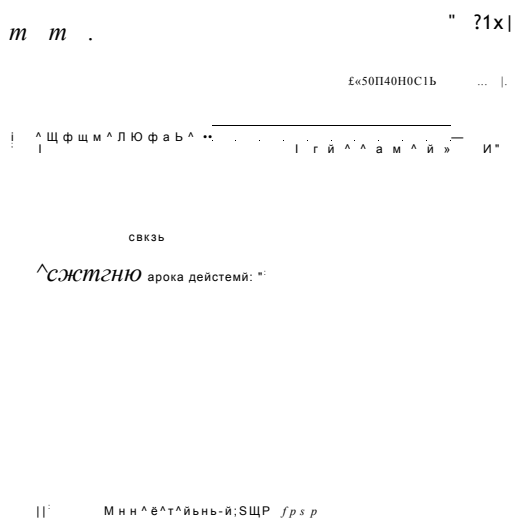


Рис. 7-38. Настройка параметров доступа для виртуального сервера SMTP

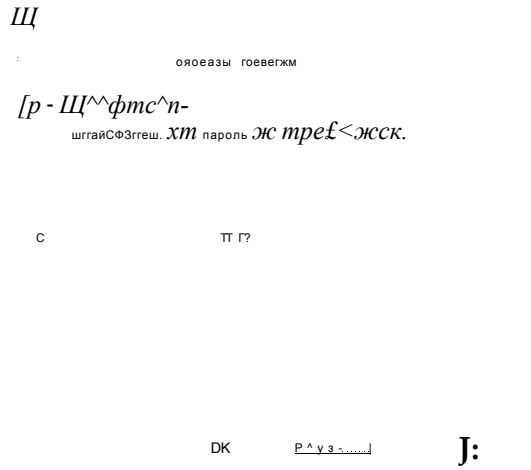


Рис. 7-39. Управление методами проверки подлинности для виртуального сервера SMTP

Помимо настройки методов проверки подлинности вы можете ограничить доступ к виртуальному серверу SMTP по IP-адресам или именам домена, чтобы лишь авторизованные сетевые клиенты могли использовать SMTP-службы. Чтобы добавить эти ограничения, на вкладке Доступ (Access) окна Свойства

(Properties) виртуального сервера SMTP щелкните кнопку Подключение (Connection). Вы сможете указать, какие компьютеры могут получать доступ к данному серверу.

При выборе опции Только компьютеры из списка ниже (Only The List Below) доступ к серверу смогут получать лишь те компьютеры, которые соответствуют отконфигурированным правилам. Эту опцию следует использовать в средах, где все клиентские компьютеры являются членами одной или нескольких сетей. При выборе опции Все компьютеры, кроме списка ниже (All Except The List Below) добавляемые правила будут применяться к компьютерам, которым запрещено использовать виртуальный сервер SMTP. Щелкнув кнопку Добавить (Add), вы можете создать новое правило конфигурации, как показано на рис. 7-40.

При создании ограничений можно указать или отдельный IP-адрес, или диапазон адресов.

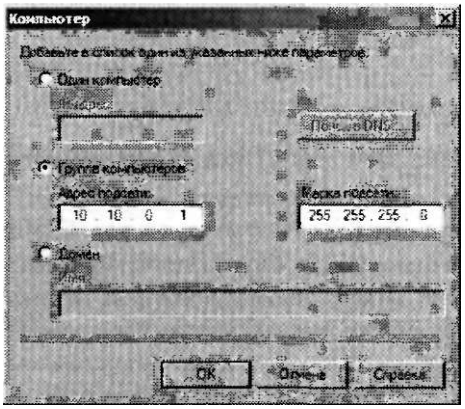


Рис. 7-40. Создание нового правила контроля подключений для виртуального сервера SMTP

Команду Поиск в DNS (DNS Lookup) можно использовать для поиска конкретного IP-адреса по имени домена. В случае выбора опции Домен (Domain) при попытках компьютера подключиться сервер SMTP будет выполнять операцию реверсивного, или обратного, поиска. В этой операции выполняется попытка разрешения IP-адреса входящего подключения в имя DNS. Если включить эту опцию, производительность может снизиться по причине выполнения множества запросов DNS.

В нижней части вкладки Доступ (Access) находится область Ограничения ретрансляции (Relay Restrictions). Ретрансляция SMTP выполняется при отправке сообщения по адресам, не входящим в домен виртуального сервера. Ретрансляция представляет собой распространенный метод, используя который спамеры могут с помощью незащищенных виртуальных серверов SMTP пересылать спам.

Опция Ограничения ретрансляции (Relay Restrictions) позволяет указать компьютеры, которые могут ретранслировать сообщения через SMTP-сервер, как показано на рис. 7-41. По умолчанию ретрансляцию могут осуществлять все пользователи и компьютеры, успешно прошедшие проверку подлинности.

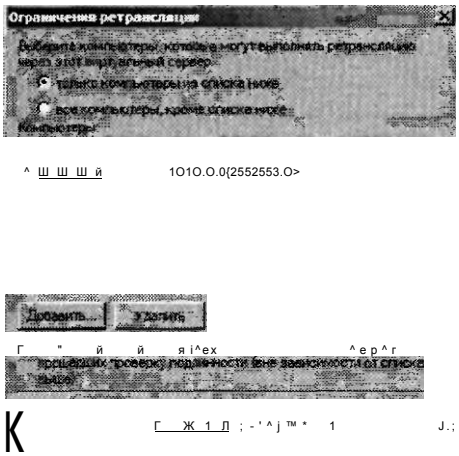


Рис. 7-41. Настройка ограничений ретрансляции SMTP

ВАЖНО! Сдерживание спама

Помимо снижения нагрузки незащищенных сетей защита виртуального сервера SMTP от неавторизованного доступа необходима и по другим причинам. Многие утилиты для борьбы со спамом будут поддерживать список известных незащищенных серверов SMTP и добавлять его в список блокировок. Все сообщения, отправляемые через незащищенный сервер SMTP, могут помечаться как спам, что затруднит обеспечение коммуникаций пользователей и приложений с лицами вне организации. При установке нового виртуального сервера SMTP выделите время для защиты конфигурации. Кроме того, для определения потенциального неавторизованного использования сервера важно регулярно просматривать параметры конфигурации SMTP и файлов журнала.

Настройка сообщений

На вкладке Сообщения (Messages) диалогового окна свойств виртуального сервера SMTP можно конфигурировать ограничения для сообщений, пересылаемых через сервер, как показано на рис. 7-42. Первые две опции позволяют указать максимальный размер сообщения (включая вложения) и максимальный объем данных, которые можно пересылать на сервер в одном подключении. Вы можете ограничить количество сообщений, отправляемых в каждом подключении, а также ограничить количество получателей сообщения. Все эти методы содействуют защите сервера от нежелательного доступа и позволяют снизить нагрузку на такие ресурсы, как полоса пропускания.

Распространенными причинами ошибок сообщений являются некорректные адреса и доменные имена, вводимые отправителем. В поле Отправлять копию отчета о недоставке на адрес (Send Copy Of Non-Delivery Report To) можно указать адрес электронной почты, на который будет пересылаться недоставленная почта. В поле Каталог сообщений с ошибками (Badmail Directory) указан путь к папке, по которому будут пересылаться данные сообщения. Эти сообщения или файлы можно просматривать для проверки недоставленной почты.

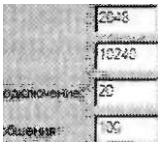


Рис. 7-42. Настройка параметров сообщений для виртуального сервера SMTP

Свойства доставки

При осуществлении коммуникаций в Интернете проблемы сетевой маршрутизации и сбои сервера могут приводить к неполадкам службы. Стандарт SMTP был разработан как надежный метод доставки сообщений. Серверы SMTP автоматически сохраняют копии сообщений, пытаясь переслать их по назначению. Если конечный сервер недоступен, сервер SMTP попытается повторить операцию. Этим поведением можно управлять с помощью свойств на вкладке Доставка (Delivery), как показано на рис. 7-43. Исходящие правила (Outbound) определяют интервалы, через которые сервер будет пытаться транслировать передачу сообщения в случае сбоя.

Вы также можете настроить Уведомление о задержке (Delay Notification) и Время ожидания (Expiration Timeout) ка для входящих, так и для исходящих подключений.

Для передачи по месту назначения серверы SMTP обычно пересылают сообщения через другие серверы SMTP. Администраторы могут конфигурировать свои серверы SMTP для требования проверки подлинности перед ретрансляцией сообщения. Щелкнув кнопку Безопасность исходящих подключений (Outbound Security), вы можете указать метод проверки подлинности, который будет использоваться при подключении еще к одному серверу SMTP.

Щелкнув кнопку Исходящие подключения (Outbound Connections), вы сможете указать ограничение количества подключений к другим серверам SMTP и время ожидания.

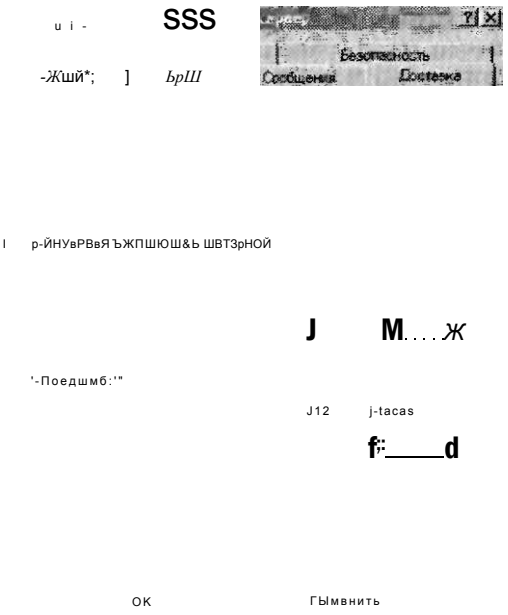


Рис. 7-43. Параметры по умолчанию для свойств доставки виртуального сервера SMTP

Щелчком кнопки Дополнительно (Advanced) открывается окно с описанными далее дополнительными опциями для управления сообщениями на виртуальном сервере SMTP.

- Максимальное количество прыжков **(Maximum Hop Count)** Когда сообщения передаются на сервер SMTP, само сообщение включает подсчет прыжков для записи числа передач с одного сервера на другой. Когда для сообщения будет достигнуто максимальное число прыжков, сообщение будет помечено как недоставленное.
- Домен маскировки **(Masquerade Domain)** При использовании этого параметра сервер SMTP автоматически переписывает имя домена из адреса От (From), используемого для исходящих сообщений. Этот параметр позволяет обеспечивать для исходящих сообщений постоянное доменное имя.
- Полное доменное имя **(Fully Qualified Domain Name)** Это поле содержит DNS-адрес виртуального сервера SMTP в соответствии с записями Address (A) и Mail Exchanger (MX). В общем каждый сервер SMTP должен иметь уникальное полное доменное имя, включающее имя сервера (например, Server01.mail.contoso.com).
- Промежуточный узел **(Smart Host)** Если для этого параметра определить имя сервера или IP-адрес, маршрутизация всех сообщений с этого виртуального сервера SMTP будет выполняться через указанный сервер. Данная опция часто используется в средах, где сообщения множества внутренних серверов передаются через указанный сервер SMTP, имеющий доступ в Интернет. Использование промежуточного узла позволяет снизить нагрузку на полосу пропускания и повысить уровень безопасности, поскольку доступ

к внешним сетям потребуется лишь определенным серверам. Если установить флажок Выполнять попытку прямой доставки перед отправкой на промежуточный узел (Attempt Direct Delivery Before Sending To Smart Host), локальный сервер SMTP будет пытаться подключиться напрямую к конечному серверу SMTP. Если попытка не удастся, сообщение будет передано на назначенный промежуточный узел.

- **Выполнять обратный писк в DNS для входящих сообщений (Perform Reverse DNS Lookup On Incoming Messages)** Если установить этот флажок, сервер SMTP будет выполнять обратный поиск в DNS для проверки соответствия домена пользователя IP-адресу в заголовке сообщения. Включив эту опцию, вы сможете предотвратить неавторизованную передачу на сервер SMTP сообщений, в которых используются несоответствующие данные заголовков.

Включение маршрутизации LDAP

Протокол LDAP (Lightweight Directory Access Protocol) является основным стандартом, с помощью которого программное обеспечение служб каталогов может осуществлять коммуникации. В качестве примеров таких служб можно привести Active Directory и Exchange Server. На вкладке Маршрутизация LDAP (LDAP Routing) можно включить маршрутизацию LDAP и настроить виртуальный сервер SMTP для использования запросов LDAP с целью разрешения адресов в электронных сообщениях. С помощью опций конфигурации можно указать схему LDAP для сервера SMTP и адрес сервера. Вы также можете указать параметры проверки подлинности для подключения к серверу LDAP и выполнения запросов.

Управление разрешениями безопасности

На вкладке Безопасность (Security) можно указать пользователей Windows, которым разрешается управлять виртуальным сервером SMTP, как показано на рис. 7-44.

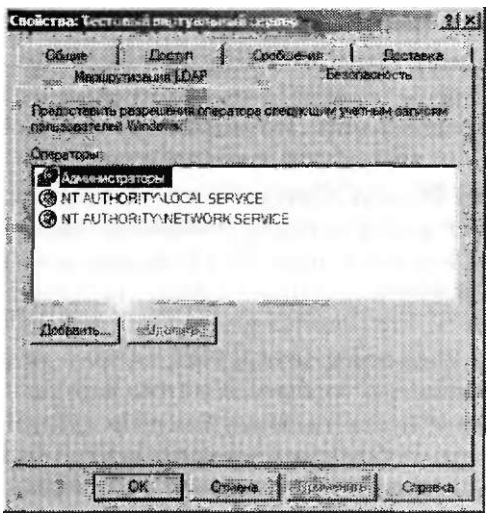


Рис. 7-44. Настройка параметров безопасности виртуального сервера SMTP

В списке перечислены пользователи, которых следует определять как операторов. Операторы располагают разрешениями на изменение конфигурации виртуального сервера SMTP. По умолчанию в список включена группа Администраторы (Administrators), а также встроенные учетные записи Local Service и Network Service. Щелкнув копку Добавить (Add), вы можете включить в список операторов дополнительных пользователей или дополнительные группы.

Мониторинг виртуальных серверов SMTP

Существует несколько способов отслеживания виртуальных серверов SMTP. С помощью компонента Текущие сеансы (Current Sessions) Диспетчера служб IIS 6.0 (IIS 6.0 Manager) можно наблюдать за всеми текущими подключениями к серверу SMTP. В случае ретрансляции сообщений или проблем производительности на сервере эти сведения можно использовать для определения источника трафика сообщений.

Вы также можете отслеживать множество счетчиков производительности Windows объекта Сервер (Server), включая следующие:

- Процент локальных получателей (% Recipients Local);
- Процент удаленных получателей (% Recipients Remote);
- Текущее количество входящих подключений (Inbound Connections Current);
- Всего байтов сообщений (Message Bytes Total);
- Доставлено сообщений (сообщения/с) (Messages Delivered/sec);
- Отправка сообщений (сообщения/с) (Messages Sent/sec);
- Всего исходящих подключений (Outbound Connections Total);
- Всего ошибок подключений (Total Connection Errors).

Помимо отслеживания использования сервера следует периодически проверять недоставленные сообщения. По умолчанию эти сообщения сохраняются в корневом каталоге, определенном для сервера SMTP. Сервер по умолчанию SMTP Virtual Serer#l использует каталог %SystemDrive%\Inetpub\Mailroot. В этой папке содержатся следующие подпапки.

- **Badmail** Сообщения, которые не были доставлены из-за проблем адресации или безопасности.
- **Drop** Хранилище всех входящих сообщений SMTP.
- **Pickup** Хранилище сообщений, ожидающих обработки еще одной программой или службой.
- **Queue** Сообщения, ожидающие доставки.

Кроме того, если согласно конфигурации сервера недоставленные сообщения пересылаются конкретной учетной записи, вам следует регулярно просматривать эти сообщения.

Использование виртуального сервера SMTP

Доступ к виртуальным серверам SMTP можно получать несколькими способами. Системные администраторы могут использовать утилиту командной строки Telnet, чтобы напрямую подключаться к серверу SMTP и отправлять команды или создавать сообщения. Однако самыми распространенными источниками сообщений SMTP являются приложения конечных пользователей и веб-приложения.

Утилита Telnet

К серверу SMTP можно подключиться напрямую с помощью команды *Telnet*. Для этого на компьютер можно добавить опциональный компонент Клиент Telnet (Telnet Client) системы Windows Server 2008. После добавления этого компонента вы можете использовать в командной строке команду *Telnet* для подключения к виртуальному серверу SMTP. Затем вы можете использовать команды для выполнения таких действий, как отправка сообщений. Утилита Telnet используется лишь для диагностики и устранения неполадок. Конечные пользователи предпочитают отправлять и получать электронные сообщения с помощью графических приложений.

ПРИМЕЧАНИЕ Устранение неполадок с помощью утилиты Telnet

Более подробные сведения об устранении неполадок SMTP с помощью утилиты Telnet можно найти в статье справки и поддержки Microsoft по адресу *http://support.microsoft.com/kb/323350/*.

Использование клиентского приложения для обмена сообщениями

Конечные пользователи чаще всего отправляют электронные сообщения с помощью клиентских приложений электронной почты. Примерами таких приложений служат Microsoft Outlook, Почта Windows (Windows Mail) (включено в операционную систему Windows Vista) и Outlook Express (Windows XP). Инструкции по установке таких приложений могут быть разными, однако пользователям обычно требуется следующая информация для настройки своих серверов SMTP:

- адрес или имя узла сервера SMTP;
- порт сервера SMTP;
- данные проверки подлинности SMTP (если требуется проверка подлинности).

Настройка параметров SMTP для ASP.NET

Многим веб-приложениями требуется возможность отправлять электронные сообщения пользователям. Для выполнения этой задачи веб-приложению нужна информация о доступном сервере SMTP. С помощью Диспетчера служб IIS (IIS Manager) эти параметры можно отконфигурировать для приложения ASP.NET, запущенного на сервере IIS 7. Для этого в левой панели выберите веб-сервер, веб-сайт или веб-приложение, а затем дважды щелкните компонент Электронная почта (SMTP) (SMTP E-Mail), чтобы открыть окно, показанное на рис. 7-45.

СОВЕТ Подготовка к экзамену

Не путайте параметры электронных сообщений SMTP в диспетчере служб IIS и параметры виртуальных серверов SMTP в диспетчере служб IIS 6.0. Параметры IIS 7 используются лишь с целью обеспечения информации для веб-приложения и не вносят изменений в конфигурацию виртуального сервера SMTP. Для модификации параметров и разрешения сервера SMTP нужно использовать диспетчер служб IIS 6.0.

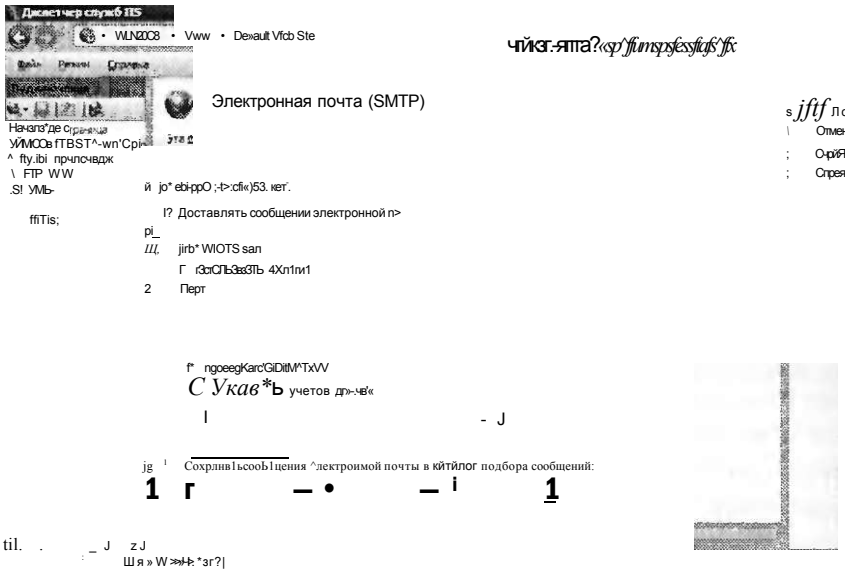


Рис. 7-45. Настройка параметров электронной почты SMTP для веб-сайта IIS 7

Веб-приложения могут запрашивать информацию каждый раз при необходимости отправить электронные сообщения, ослабляя таким образом конфигурацию развертывания. Доступны перечисленные далее опции. Адрес электронной почты (E-Mail Address) будет указан в поле От (From) сообщения. Параметры SMTP-сервера и порта (Port) определяют детали подключения к доступному виртуальному серверу SMTP. Параметры проверки подлинности (Authentication) можно указать в случае, если сервер SMTP требует передачу учетных данных. И наконец, опция Сохранять сообщения электронной почты в каталог подбора сообщений (Store E-Mail In Pickup Directory) является альтернативой пересылки сообщений на сервер SMTP. При использовании этой опции исходящие сообщения будут храниться в виде отдельных файлов в указанной папке.

Проверьте себя

1. Какой параметр следует изменить, чтобы позволить пользователям SMTP отправлять большие вложения с помощью виртуального сервера SMTP?
2. Как отконфигурировать виртуальный сервер SMTP, чтобы на пего мог отправлять сообщения лишь один веб-сервер?

Ответы

1. Свойства на вкладке Сообщения (Messages) позволяют настроить ограничения для размера сообщений в килобайтах.
2. Вы можете включить опции Подключение (Connection) на вкладке Доступ (Access) диалогового окна свойств виртуального сервера SMTP. Следует модифицировать параметры для разрешения одного IP-адреса (адресов) веб-сервера.

Практикум. Конфигурирование и тестирование служб SMTP

В предложенных далее упражнениях вы попрактикуетесь во включении служб SMTP на компьютере Windows Server 2008.

Упражнение 1. Создание нового виртуального сервера SMTP

В этом упражнении вы с помощью диспетчера служб IIS 6.0 создадите виртуальный SMTP-сервер. Предполагается, что вы еще не установили компонент Сервер SMTP (SMTP Server).

1. Войдите на сервер Server2/contoso.com как пользователь с правами администратора.
2. Откройте Диспетчер сервера (Server Manager). Щелкните правой кнопкой мыши узел Компоненты (Features) и примените команду Добавить компоненты (Add Features).
3. Выберите компоненты Сервер SMTP (SMTP Server) и Клиент Telnet (Telnet Client) и щелкните кнопку Далее (Next).
4. На странице Подтвердите выбранные элементы (Confirm Installation Selections) щелкните кнопку Установить (Install), чтобы начать процесс установки. После завершения установки щелкните кнопку Закрыть (Close).
5. Закройте диспетчер сервера. В группе программ Администрирование (Administrative Tools) запустите Диспетчер служб IIS 6.0 (IIS 6.0 Manager).
6. Разверните объект Server2 (Локальный компьютер) и обратите внимание, что для него уже создан сервер SMTP Virtual Server#l.
7. Щелкните правой кнопкой мыши объект Server2, выберите меню Создать (New) и примените команду Виртуальный SMTP-сервер (New SMTP Virtual Server).
8. В поле Имя (Name) введите имя *Contoso SMTP* и щелкните кнопку Далее (Next).
9. Для параметра Выберите IP-адрес (Select IP Address) оставьте значение по умолчанию и щелкните кнопку Далее (Next). Прочитайте предупреждение и щелкните кнопку Да (Yes) для продолжения. Вы разрешите этот конфликт позже.
10. В проводнике Windows (Windows Explorer) создайте в корне системного диска новую папку с именем Mail. Укажите путь к этой папке для корневого каталога (например, C:\Mail).
11. В поле Домен (Domain) введите имя *mail.contoso.com* и щелкните кнопку Готово (Finish). Новый виртуальный сервер SMTP с именем Contoso SMTP появится в левой панели диспетчера служб IIS 6.0.
12. Щелкните правой кнопкой мыши объект Contoso SMTP и примените команду Свойства (Properties).
13. На вкладке Общие (General) щелкните кнопку Дополнительно (Advanced), чтобы открыть список IP-адресов и номеров портов для виртуального сервера SMTP. Выберите в списке IP-адрес (IP Address) параметр Все неназначенные (All Unassigned) и щелкните кнопку Правка (Edit).

14. Для параметра TCP-порт (TCP Port) укажите номер 2525 и щелкните OK. Таким образом будет разрешен конфликт с виртуальным сервером SMTP, созданным по умолчанию. Трижды щелкните OK, чтобы закрыть диалоговые окна и сохранить параметры.
15. В Диспетчере служб IIS 6.0 (IIS 6.0 Manager) щелкните правой кнопкой мыши виртуальный сервер Contoso SMTP и примените команду Пуск (Start).
16. После выполнения этого практического упражнения вы можете использовать клиента электронной почты для подключения к серверу SMTP и отправки сообщения. Вы можете попытаться отправить сообщение по ошибочному адресу электронной почты (например, *Recipient@mail.test)* и проверить поведение сервера SMTP.
17. Закройте Диспетчер служб IIS 6.0 (IIS 6.0 Manager). При желании вы можете удалить сервер SMTP на сервере Server2.

Резюме

- Компонент Сервер SMTP (SMTP Server) можно включить в Windows Server 2008 с помощью Диспетчера сервера (Server Manager).
- Каждый виртуальный сервер SMTP должен использовать уникальное сочетание IP-адреса и номера порта.
- Настроив методы проверки подлинности, можно требовать, чтобы пользователи, подключающиеся к серверу SMTP, предоставляли учетные данные.
- Ограничения ретрансляции (Relay Restrictions) можно использовать для уменьшения объема незатребованных коммерческих сообщений электронной почты.
- Конфигурацию виртуального сервера SMTP можно протестировать с помощью клиентского приложения электронной почты.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных в ходе занятия 2. Эти вопросы представлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы

Ответы и пояснения к каждому их варианту размещены в разделе «Ответы» в конце книги.

1. Вы являетесь системным администратором и отвечаете за настройку SMTP-сервера Windows Server 2008. Для отправки уведомлений веб-приложения ContosoOrderManagement ваша организация в настоящее время использует виртуальный сервер SMTP, созданный по умолчанию. Недавно вы заметили, что на виртуальный сервер SMTP приходит много сообщений от других компьютеров и пользователей. Какие два метода можно использовать для предотвращения неавторизованного доступа к SMTP-серверу? (Укажите два варианта. Каждый вариант является частью полного ответа.)
   A. Включить обычную проверку подлинности (Basic Authentication).

Б. Отконфигурировать промежуточный узел для использования виртуальным сервером SMTP.

В. Добавить правило управления подключениями для ограничения IP-адресов, которые могут использовать сервер SMTP.

Г. Модифицировать параметры на вкладке Безопасность (Security) диалогового окна свойств виртуального сервера SMTP.

2. Вы являетесь системным администратором и отвечаете за управление SMTP-сервером Windows Server 2008. Недавно пользователи стали жаловаться, что в определенное время дня в веб-приложении, которое запущено на том же сервере, возникает проблема быстродействия. Вы подозреваете, что проблема связана с нагрузкой на сервер SMTP. Какой из следующих методов следует использовать для отслеживания производительности виртуального сервера SMTP?

А. Компонент Текущие сеансы (Current Sessions) диспетчера служб IIS 6.0.

Б. Счетчики производительности SMTP-сервера в оснастке Системный монитор (Performance Monitor).

В. Журнал Приложение (Application) в оснастке Просмотр событий Windows (Windows Event Viewer).

Г. Содержимое папки Badmail виртуального сервера SMTP.

Закрепление материала главы

Для того чтобы попрактиковаться и закрепить знания, приобретенные в ходе изучения представленного в данной главе материала, вам необходимо:

- ознакомиться с резюме главы;
- повторить используемые в главе основные термины;
- выполнить задания лабораторной работы, которые моделируют реальные ситуации, требующие применения полученных знаний;
- выполнить рекомендуемые упражнения;
- сдать пробный экзамен с помощью тестов.

Резюме главы

- В Windows Server 2008 можно установить компонент Служба FTP-публикации (FTP Publishing Service (FTP 6)), чтобы позволить пользователям выгружать и загружать файлы.
- В Windows Server 2008 можно установить версию FTP 7, чтобы обеспечить новые возможности, в частности интеграцию с привязками веб-сайтов, администрирование с помощью диспетчера служб IIS (IIS Manager) и поддержку стандарта FTP Over SSL (FTPS).
- Служба SMTP позволяет Windows Server 2008 выполнять безопасную маршрутизацию сообщений электронной почты для других серверов и пользователей.

Основные термины

Проверьте, знаете ли вы, что означают перечисленные ниже термины (свои ответы можно сверить с определениями, содержащимися в конце книги):

- File Transfer Protocol (FTP);
- FTP-клиент;
- FTP-сервер;
- FTP Over SSL;
- изоляция пользователя FTP;
- домен маскировки;
- ограничения ретрансляции;
- Simple Mail Transfer Protocol (SMTP);
- промежуточный узел;
- виртуальный сервер SMTP.

Лабораторная работа

В следующих заданиях вы примените полученные знания о конфигурировании параметров FTP и SMTP в Windows Server 2008.

Задание 1. Реализация сайта Secure FTP

Вы являетесь системным администратором и обеспечиваете для веб-разработчиков возможности управления веб-приложениями на тестовом сервере. Некоторые из этих пользователей являются консультантами и не располагают учетными записями в домене Active Directory вашей организации. Вы хотите обеспечить для них возможность доступа и модификации содержимого конкретных веб-сайтов. Вы также хотите свести к минимуму административную работу, которую требуется выполнить, чтобы обеспечить такую конфигурацию. Согласно политике безопасности компании такие учетные данные, как пользовательские имена и пароли, не должны пересылаться в незашифрованном виде.

1. Какую версию FTP-сервера следует использовать для обеспечения такой конфигурации?
2. Как обеспечить шифрование пересылаемых учетных данных?
3. Какой самый простой метод можно использовать для обеспечения FTP-доступа к существующим веб-сайтам?

Задание 2. Настройка виртуального сервера SMTP

Вы являетесь системным администратором и отвечаете за обеспечение безопасности виртуального сервера SMTP в Windows Server 2008. На сервере, где размещен виртуальный SMTP-сервер, установлены два физических сетевых адаптера, подключенных к отдельным сетям. Согласно требованиям безопасности SMTP-сервер должен отвечать лишь по одному из этих IP-адресов и только на порте 8937. Пользователи и приложения, которым требуется доступ к SMTP-серверу, должны предоставлять учетные данные. Недавно пользователи стали жаловаться, что они не могут пересылать вложения с объемом больше

2 Мбайт. Вы хотите разрешить пересылать через сервер вложения с объемом до 10 Мбайт.

1. Как отконфигурировать виртуальный сервер SMTP, чтобы он отвечал лишь на конкретные сетевые запросы?
2. Как отконфигурировать сервер, чтобы для отправки сообщений SMTP требовалось предоставлять учетные данные?
3. Как изменить максимальный дозволенный размер сообщений?

Рекомендуемые упражнения

Чтобы успешно справиться с экзаменационными заданиями, выполните следующие упражнения.

Работа со службами FTP и SMTP

Выполняя предлагаемые упражнения, вы научитесь использовать в Windows Server 2008 службы FTP и SMTP.

- **Упражнение 1** В этом упражнении вы сможете на практике ознакомиться с новыми возможностями FTP 7 для Windows Server 2008.
  1. Загрузите пакет FTP 7 по адресу *http://www.iis.net.doTemloads* и установите его на компьютер Windows Server 2008.
  2. С помощью Диспетчера служб IIS (IIS Manager) создайте для объекта Default Web Site новую привязку FTP-сайта.
  3. Отконфигурируйте различные параметры изоляции пользователя FTP (FTP User Isolation) и для проверки используйте клиентское приложение FTP. Обратите внимание на размещение папок по умолчанию в зависимости от каждого параметра, а также на то, какие папки доступны для пользователей.
  4. Включите шифрование FTP Over SSL (FTPS), создав самозаверяющий сертификат SSL. Для проверки функциональности используйте совместимое клиентское FTP-приложение.
- **Упражнение 2** В этом упражнении вы протестируете и отконфигурируете службу SMTP в Windows Server 2008.
  1. На компьютере Windows Server 2008 установите компонент Сервер SMTP (SMTP Server).
  2. Модифицируйте параметры виртуального сервера SMTP, созданного по умолчанию, чтобы при отправке сообщений требовать обычную проверку подлинности.
  3. Протестируйте конфигурацию SMTP-сервера, отправив через него электронное сообщение с помощью такого клиентского приложения, как Почта Windows (Windows Mail), Outlook или Outlook Express,
  4. Попытайтесь отправить тестовое электронное сообщение на неправильный или несуществующий адрес электронной почты. Попробуйте найти это сообщение в папке Badmail сервера SMTP. Кроме того, проверьте, можете ли вы получать недоставленные и ошибочные сообщения электронной почты.

Пробный экзамен

На прилагаемом к книге компакт-диске представлено несколько вариантов тренировочных тестов. Проверка знаний выполняется только по одной или же по всем экзаменационным темам сертификационного экзамена 70-643. Тестирование можно организовать таким образом, чтобы оно проводилось как экзамен, или же настроить его на изучение — в этом случае вы сможете после каждого своего ответа на вопрос просматривать правильные ответы и объяснения.

ПРИМЕЧАНИЕ Пробный экзамен

Подробнее о пробном экзамене рассказано во введении к данной книге.

ГЛАВА 8

Настройка служб Windows Media 2008

Занятие 1. Настройка служб Windows Media 419

Многим организациям требуется эффективно доставлять цифровое мультимедийное содержимое пользователям. Аудио- и видеофайлы часто доступны для сотрудников и внешних пользователей. Например, организация может хранить на сервере интрасети архивные версии встреч компании и других презентаций. Некоторые организации обеспечивают для пользователей аудио- и видеосодержимое в соответствии со схемой своей деятельности. Однако процесс отправки информации мультимедиа по сети и Интернету может оказывать существенное влияние на пропускную способность и ресурсы сервера.

В Windows Server 2008 обеспечены возможности эффективного потокового мультимедиа для пользователей через общественные и частные сети. Из этой главы вы узнаете, как установить и отконфигурировать роль сервера потокового мультимедиа (Media Services) для обеспечения доступа к различным типам содержимого. Вы также изучите способы обеспечения защиты цифрового содержимого с помощью DRM (Digital Rights Management).

К СВЕДЕНИЮ Получение компонента Windows Media Services

Роль Windows Media Services представляет собой загружаемую надстройку Windows Server 2008. Более подробные сведения о получении этого продукта содержатся на веб-сайте Windows Media Servers по адресу *http://www.microsoft.com/windowsmedia/forpros/server/server.aspx* (русская версия находится по адресу *http://www.jnicrosoft.cojn/downloads/details.aspx?displaylang^ru&FajnilyID=9ccf6312-723b-4577-be58- 7caab2e 1c5b 7).*

Темы экзамена:

- Настройка сервера Windows Media.
- Настройка средств защиты авторских прав DRM (Digital Rights Management).

Требования

Для выполнения упражнений этой главы на сервере Server2.Contoso.com должна быть установлена роль Веб-сервер (IIS) (Web Server (IIS)).

Занятие 1. Настройка служб Windows Media

Роль Службы потокового мультимедиа (Streaming Media Services) в Windows Server 2008 обеспечивает большой выбор возможностей управления аудио- и видеосодержимым и его представления для пользователей. Кроме того, она включает административные средства и опции конфигурации, соответствующие многим техническим и бизнес-требованиям. На этом занятии вы узнаете, как включить и отконфигурировать сервер Windows Media, а также изучите методы повышения возможностей расширяемости, производительности, безопасности и стабильности.

Изучив материал этого занятия, вы сможете:

- Установить роль Службы потокового мультимедиа (Streaming Media Services) на компьютере Windows Server 2008.
- Настроить параметры служб потокового мультимедиа.
- Создать пункты публикации для доставки широковещательного аудио- и видеосодержимого для пользователей по запросам.
- Настроить параметры проверки подлинности и авторизации для защиты доступа к содержимому.
- Включить компоненты кэширования и прокси для повышения производительности и стабильности служб сервера Windows Media.
- Описать, как можно реализовать DRM (Digital Rights Management) для защиты интеллектуальной собственности.

Расчетная продолжительность занятия составляет 60 мин.

Службы Windows Media

Технические требования для обеспечения доступа к аудио- и видеосодержимому могут значительно отличаться от требований к другим типам содержимого. Роль Веб-сервер (IIS) может обеспечить пользователям доступ ко многим типам файлов. Например, вы можете позволить пользователям загружать файлы Windows Media Audio (.wma) и Windows Media Video (.wmv), обеспечив для них соответствующие URL и разрешения доступа. Недостаток этой технологии состоит в том, что пользователям, как правило, нужно загрузить весь файл перед воспроизведением. Поэтому они вынуждены ожидать завершения загрузки, что не делает их работу комфортной. В результате многие пользователи попросту отменяют загрузку файла. Когда пользователи запрашивают большие видео- и аудиофайлы, веб-серверы пытаются отправить эту информацию как можно быстрее. Таким образом, снижается производительность сервера для других пользователей и ограничивается общая расширяемость. Кроме того, когда пользователи решают отказаться от загрузки всего файла, ресурсы, используемые в процессе загрузки, расходуются впустую.

Все эти проблемы стали причиной создания специализированной службы для работы с содержимым мультимедиа. Изначально роль Службы потокового мультимедиа (Streaming Media Services) в Windows Server 2008 предназначена для обеспечения доступа к потоковым аудио- и видеоданным через стандартные протоколы коммуникаций, например протоколы Интернета. Доступ к мультимедиа можно обеспечить в интрасети и на общественных веб-сайтах. Во многих случаях веб-приложение включает ссылки, позволяющие пользователям быстро локализовать и запустить требуемое содержимое. Обычно воспроизведение содержимого начинается через несколько секунд, а сервер мультимедиа может автоматически дросселировать пропускную способность сети на основе скорости клиентского подключения и требуемого качества. Для защиты содержимого можно также использовать Технические средства защиты авторских прав DRM (Digital Rights Management).

Доставка транслируемого и предварительно записанного содержимого

С помощью служб потокового мультимедиа Windows (Windows Media Services) пользователи могут получать доступ к двум основным типам содержимого. Широковещательная трансляция, как правило, используется для таких событий, как спортивное обозрение, музыкальные концерты и презентации. Источником трансляции обычно является сервер или камера с поддержкой стандарта Windows Media Encoder. Этот тип содержимого запускается в конкретное время, причем все пользователи принимают одно видео- и аудиосодержимое. Поскольку данные отправляются по мере их генерирования, пользователи не могут приостановить, перемотать вперед или запустить заново содержимое трансляции. Тем не менее данные трансляции можно архивировать, чтобы пользователи могли потом получать к ним доступ по требованию.

Предварительно записанное содержимое запрашивается пользователем по требованию. В качестве примеров можно привести библиотеку обучающих и музыкальных видеоклипов, телевизионных передач и другого содержимого, доступного по запросу. При запросе содержимого службы потокового мультимедиа незамедлительно начинают его отправку. Как только на клиентском компьютере будет буферизован достаточный объем потоковых данных, начнется воспроизведение. Процесс буферизации часто занимает всего несколько секунд, так что воспроизведение потоковых данных начинается довольно быстро. Разработчики содержимого могут также создавать веб-страницы, включающие вложенный проигрыватель мультимедиа, обеспечивающий быстрый доступ к содержимому и связанной информации. Кроме того, пользователи могут остановить или приостановить воспроизведение запрашиваемого по требованию содержимого, перемотать его вперед или назад.

Одноадресный и многоадресный потоки мультимедиа

При обеспечении доступа к потоковому аудио- и видеосодержимому очень важно снизить уровень требований к пропускной способности сети. Клиенты и серверы часто имеют ограничения, которые могут снизить возможности масштабирования и количество пользователей, получающих доступ к мультимедиа. Службы потокового мультимедиа Windows (Windows Media Services) обеспечивают два метода отправки данных клиентам.

Одноадресный поток основан на прямом подключении между клиентскими компьютерами и сервером мультимедиа. Этот подход чаще всего используется в сценариях, где пользователи должны иметь возможность запуска воспроизведения любого содержимому по требованию. Поскольку содержимое отправляется каждому клиенту отдельно, пользователи могут приостановить, повторить или быстро перемотать вперед содержимое в своих проигрывателях. Основной недостаток одноадресного потока мультимедиа состоит в том, что он может занимать значительную часть полосы пропускания.

При использовании многоадресного потока мультимедиа многие клиенты могут одновременно подписаться на один и тот же поток с сервера. Требования к пропускной способности сервера в данном случае минимальны, поскольку информация отправляется лишь один раз. Если сетевая инфраструктура поддерживает многоадресную маршрутизацию и распространение, клиенты смогут получать содержимое без необходимости в прямом подключении к серверу. Многоадресные потоки удобнее всего использовать для доставки транслируемого широковещательного мультимедиа, поскольку пользователи не смогут управлять воспроизведением потока. Многоадресную потоковую передачу удобно также применять во внутренних корпоративных сетях, где администраторы могут обеспечить ее поддержку в инфраструктуре.

Протоколы передачи данных

Поставщики содержимого должны обеспечивать возможности доступа и быстродействие в своих службах потокового мультимедиа. Службы потокового мультимедиа Windows (Windows Media Streaming) поддерживают различные протоколы в зависимости от возможностей клиентов и сетей. Протокол RTSP (Real-Time Streaming Protocol) обеспечивает эффективный метод передачи аудио- и видеосодержимого на компьютеры проигрывателем Windows Media не ниже версии 9. Протокол RTSP может использовать протокол UDP (User Datagram Protocol, RTSPU), если он поддерживается клиентом и сетью. Если протокол UDP не поддерживается, RSTP может использовать протокол TCP (RTSPT). По умолчанию для подключений используется TCP-порт 554, однако вы можете изменить этот номер в соответствии с требованиями брандмауэра.

Потоковые службы мультимедиа Windows могут также использовать для потоковой передачи данных протокол HTTP, обеспечивая поддержку клиентов и сетей, не поддерживающих протокол RTSP. По умолчанию данные передаются на HTTP-порт 80, однако номер порта можно изменить во избежание конфликтов с ролью Веб-сервер (IIS). Чтобы упростить процесс подключения, службы потокового мультимедиа Windows используют механизм автоматической смены протокола. Этот механизм может автоматически определять оптимальный тип подключения для отдельного клиента проигрывателя мультимедиа и через него передавать данные.

Установка служб потокового мультимедиа

Службы Windows Media (Windows Media Services) представляют собой опциональную роль сервера, которую следует загрузить с сайта Microsoft. Пакет загрузки можно найти на сайте Центр загрузки Microsoft, выполнив поиск по фразе «Службы Windows Media 2008 для Windows Server 2008». На сайте пред-

ставлены сведения по установке роли сервера служб потокового мультимедиа с помощью диспетчера сервера. Чтобы начать процесс, откройте Диспетчер сервера (Server Manager), щелкните правой кнопкой мыши узел Роли (Roles) и примените команду Добавить роли (Add Roles). В списке вы увидите Службы потокового мультимедиа (Streaming Media Services), как показано на рис. 8-1.

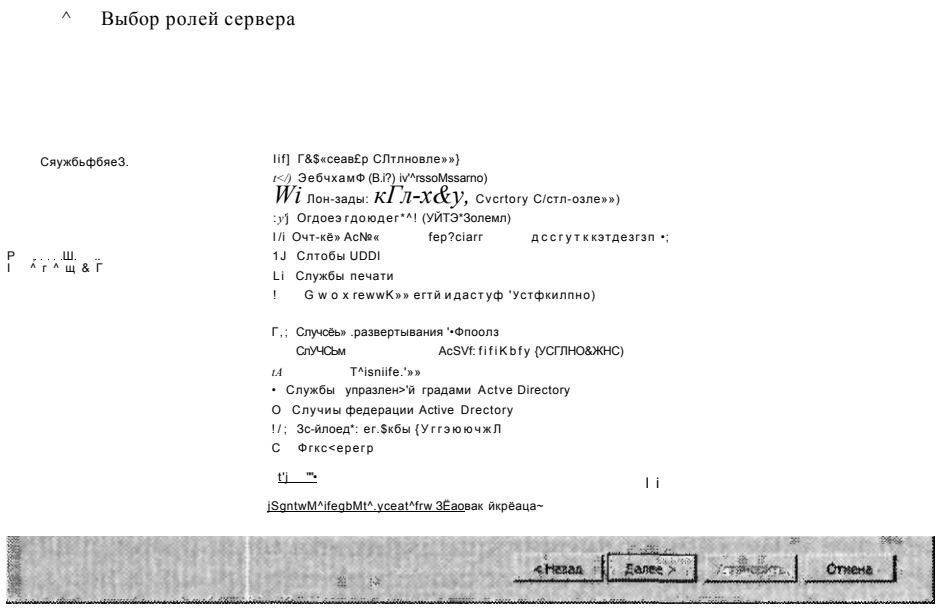


Рис. 8-1. Добавление служб потокового мультимедиа с помощью диспетчера сервера

Роль Службы потокового мультимедиа (Streaming Media Services) включает следующие службы ролей.

- **Сервер Windows Media (Windows Media Server)** При установке этого флажка на компьютере будут установлены основные службы потокового мультимедиа и консоль. Эту службу ролей нужно установить для обеспечения возможности потоковой передачи аудио и видео клиентам с локального сервера.
- **Веб-администрирование (Web-Based Administration)** Службы потокового мультимедиа также включают опциональную веб-конфигурацию и управление веб-сайтом для поддержки тех же функций, что и консоль служб потокового мультимедиа по умолчанию. Для работы этого компонента на локальном компьютере следует включить роль Веб-сервер (IIS) (Web Server (IIS)).
- Агент ведения журнала **(Logging Agent)** Этот компонент работает с веб-серверами и захватывает информацию о потоках аудио и видео. Для него требуется установить роль Веб-сервер (IIS). Если установить веб-сервер (IIS) на том же компьютере, где установлена служба ролей Службы Windows Media (Windows Media Services), потребуется изменить HTTP-порт по умолчанию для сайта Default Web Site, иначе возникнет конфликт привязок.

На странице Выберите протоколы передачи данных (Select Data Transfer Protocols) можно указать протоколы, которые будут включены по умолчанию. Если вы ранее установили роль Веб-сервер (IIS) и привязали ее к HTTP-порту 80, то вы не сможете выбрать на этой странице протокол HTTP (Hypertext Transfer Protocol), как показано на рис. 8-2. Вы сможете реконфигурировать и включить HTTP после добавления роли.

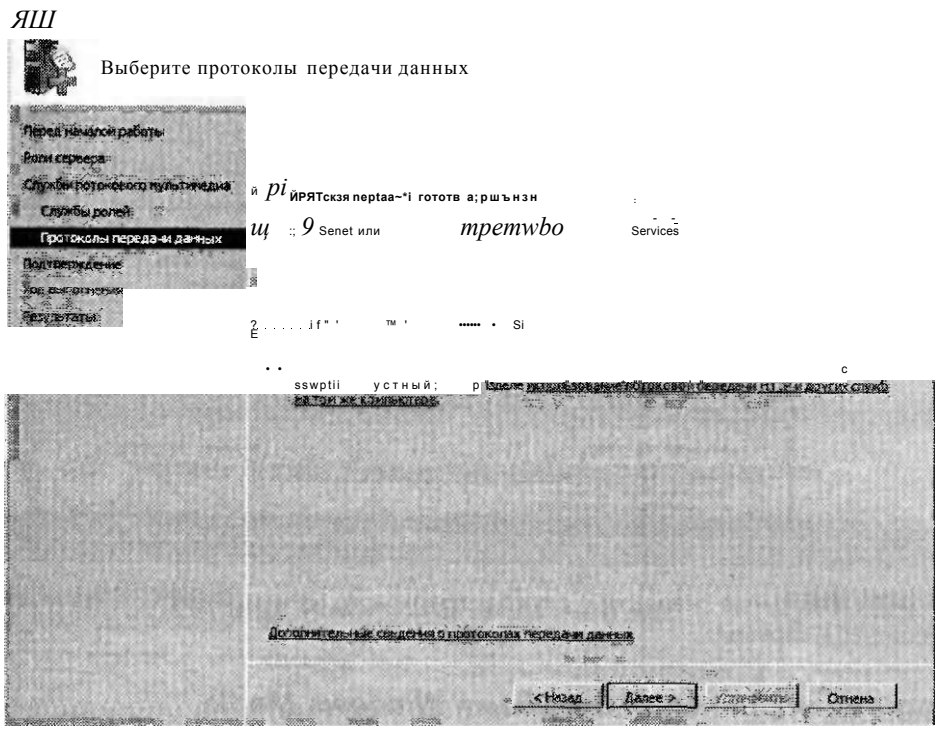


Рис. 8-2. Настройка протоколов передачи данных для служб потокового мультимедиа

Помимо этих служб ролей консоль Службы Windows Media (Windows Media Services) обеспечивает возможности тестирования доступа к содержимому с использованием проигрывателя Windows Media (Windows Media Player). Для того чтобы проигрыватель Windows Media был доступен для использования, вы должны с помощью Диспетчера сервера (Server Manager) установить компонент Возможности рабочего стола (Desktop Experience). Этот компонент является опциональным. Его не обязательно использовать, если вы не планируете тестировать потоковую передачу мультимедиа на локальном компьютере Windows Server 2008.

После установки Служб потокового мультимедиа (Streaming Media Services) дополнительные сведения можно просмотреть с помощью Диспетчера сервера (Server Manager). Для этого разверните объект Роли (Roles) и выберите Службы потокового мультимедиа (Streaming Media Services), как показано на рис. 8-3. Все ошибки, записанные в журналы событий Windows, отображаются в области События (Events). В области Ресурсы и поддержка (Resources And Support)

представлены различные рекомендации относительно конфигурации и развертывания потокового мультимедиа.

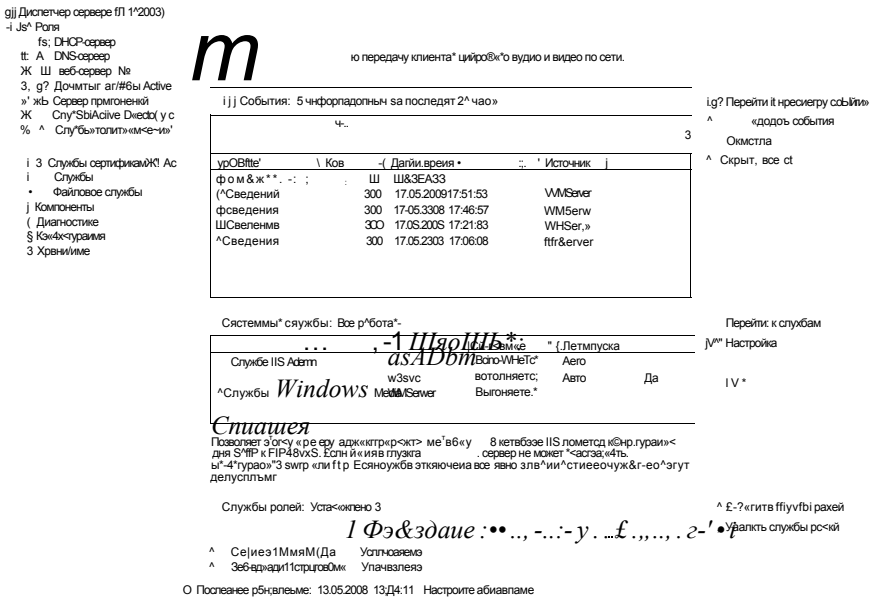


Рис. 8-3. Просмотр сведений о службах потокового мультимедиа в диспетчере сервера

Средства управления службами Windows Media

Службы Windows Media (Windows Media Services) содержат два основных административных инструмента. Консоль Службы Windows Media (Windows Media Services) можно запустить из группы программ Администрирование (Administrative Tools). Консоль Службы Windows Media показана па рис. 8-4.

Если вы установите компонент Веб-администрирование (Web-Based Administration), то сможете также отконфнгурировать службы Windows Media с помощью веб-браузера. По умолчанию веб-caiiTy Windows Media Administration назначается HTTP-порт 8080. Этот веб-сайт можно запускать, останавливать и реконфигурировать с помощью Диспетчера служб IIS (IIS Manager), как показано на рис. 8-5.

После запуска сайта доступ к нему можно получить, запустив Службы Windows Media (Веб) (Windows Media Services (Web)) из группы программ Администрирование (Administrative Tools) или указав URL сайта в веб-браузере. Привязки сайта по умолчанию не включают привязку SSL, так что вы можете получить предупреждение, показанное на рис. 8-6. Более подробные сведения о настройке и включении протокола SSL (Secure Sockets Layer) для веб-сайта содержатся в главе 6. Вы можете продолжить администрирование сайта и без использования SSL-подключения.

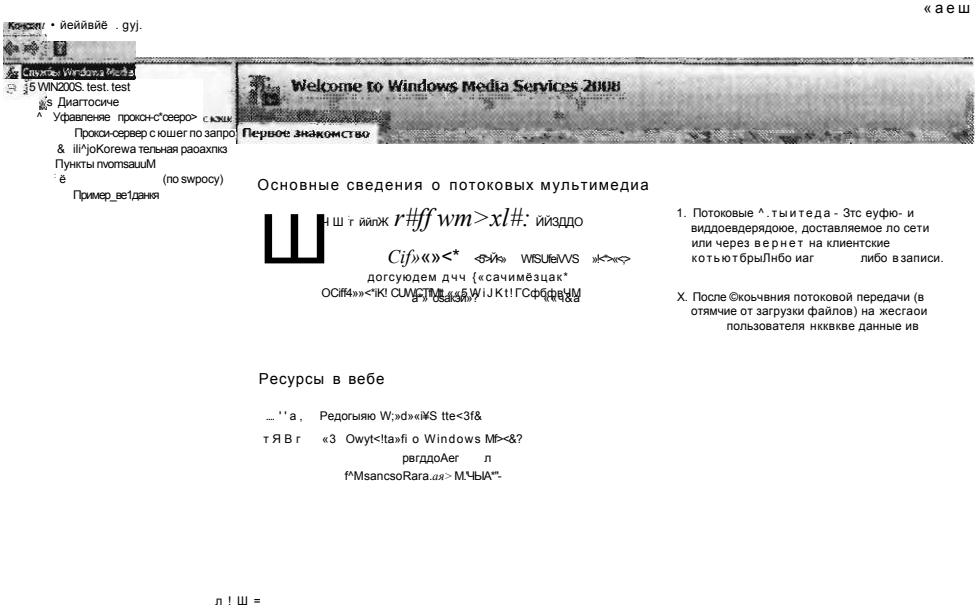


Рис. 8-4. Консоль Службы Windows Media (Windows Media Services)

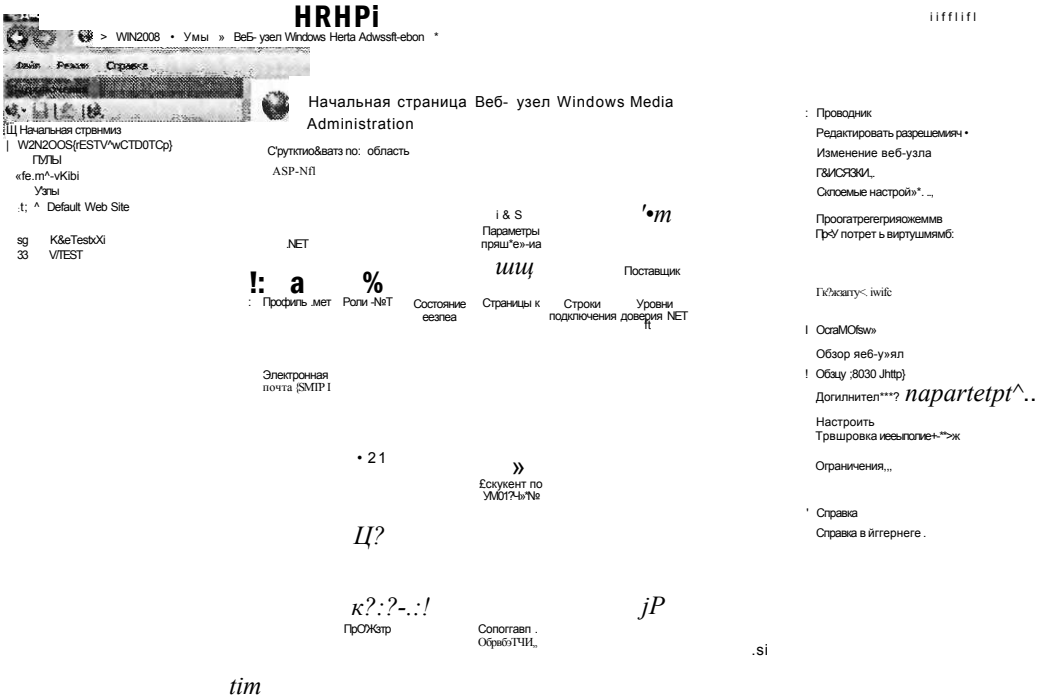


Рис. 8-5. Просмотр сайта Windows Media Administration с помощью диспетчера служб IIS

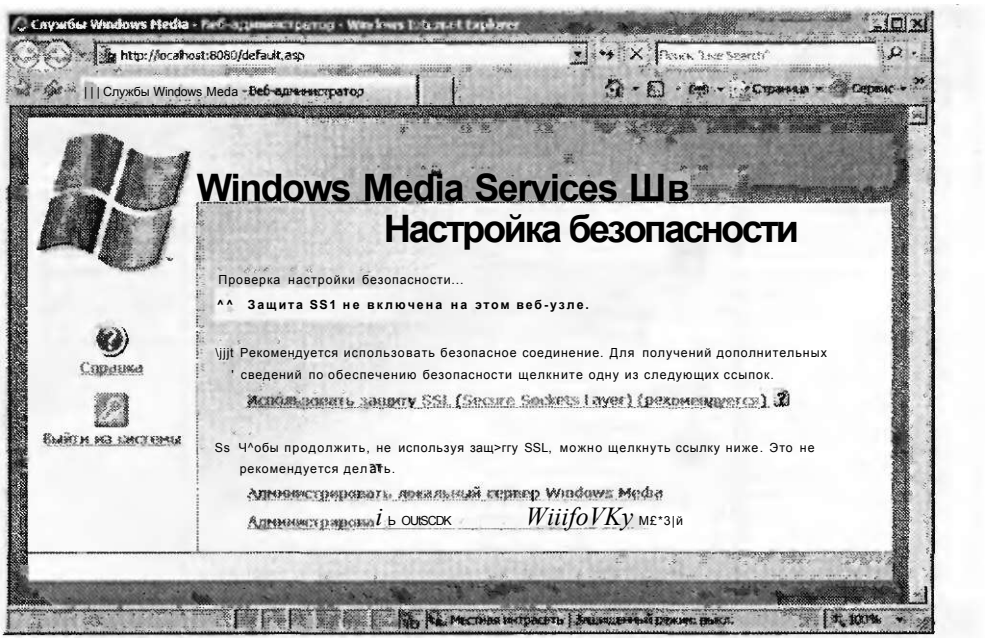


Рис.8-6. Предупреждение настройки безопасности служб Windows Media

Веб-сайт Windows Media Administration, показанный на рис. 8-7, похож на консоль Службы Windows Media (Windows Media Services), имеющую те же компоненты и функции.

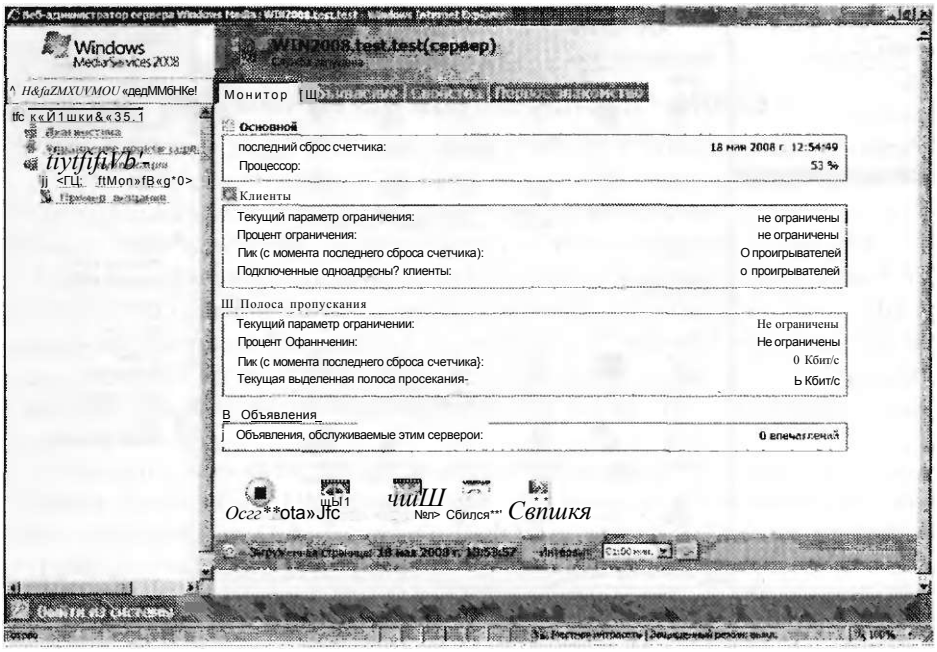


Рис. 8-7. Веб-сайт Windows Media Administration

Веб-страницы обновляются автоматически через регулярные интервалы времени. Администрирование веб-сайта удобно применять для удаленного управления.

Далее на этом занятии пойдет речь об использовании консоли Службы Windows Media (Windows Media Services). Тем не менее многие операции можно выполнять с помощью веб-сайта Windows Media Administration.

Управление пунктами публикации

Пункты публикации используются для определения размещений и типов содержимого, доступного для пользователей консоли Службы Windows Media (Windows Media Services). При установке роли Службы потокового мультимедиа (Streaming Media Services) автоматически создается пункт публикации по умолчанию <По умолчанию> (по запросу) <Default> (on-demand). Эта папка расположена в каталоге %SystemDrive%\Wmpub\Wmroot. Она содержит набор мультимедийных файлов по умолчанию, включая примеры видеофайлов Windows Media Video (.wmv), списки воспроизведения и файлы изображений.

Создание нового пункта публикации

Для обеспечения доступа к новому содержимому с помощью консоли Службы Windows Media (Windows Media Services) можно создать новый пункт публикации. Щелкните правой кнопкой мыши объект Пункты публикации (Publishing Points) в левой панели консоли и примените команду Добавить пункт публикации (мастер) (Add Publishing Point (Wizard)). На странице приветствия Мастера добавления пункта публикации (Add Publishing Point Wizard) щелкните кнопку Далее (Next). На странице Имя пункта публикации (Publishing Point Name) будет предложено указать имя для нового пункта публикации, как показано на рис. 8-8. Следует ввести короткое описательное имя, поскольку оно будет использоваться как часть URL, указываемого клиентами для подключения к содержимому.

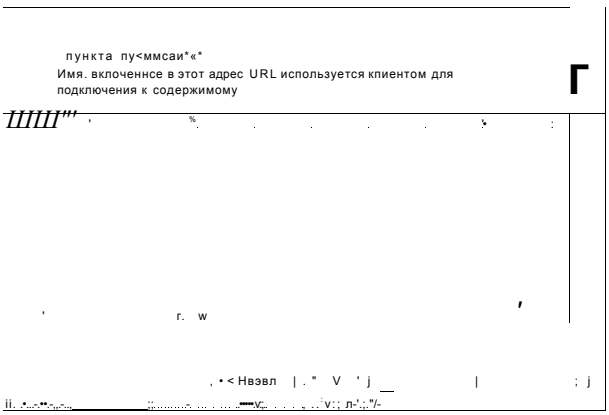


Рис. 8-8. Назначение имени новому пункту публикации

На странице Тип содержимого (Content Type) мастера необходимо указать тин содержимого, которое будет доступно в этом пункте публикации, как показано на рис. 8-9. Вы можете выбрать один из следующих параметров:

- Кодировщик (прямой поток) (Encoder) (A Live Stream);

Список воспроизведения (совокупность файлов и прямых потоков данных, объединяемых в непрерывный поток) (Plavlist (A Mix Of Files And/Or Live Streams That You Сап Combine Into A Continuous Stream);

Один файл (удобен для широкого вещания архивированного файла) (One File (Useful For A Broadcast Of An Archived File);

Файлы (мультимедиа или списки воспроизведения) в каталоге (удобен для представления доступа для воспроизведения по запросу с помощью одного пункта публикации) (Files (Digital Media Or Products) In A Directory (Useful For Providing Access For On-Demand Playback Through A Single Publishing Point)).

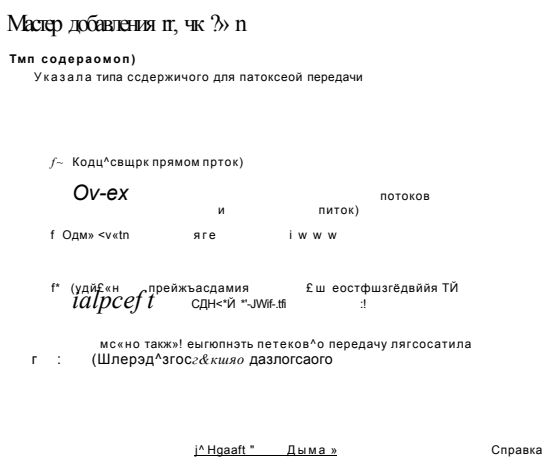


Рис. 8-9. Выбор типа содержимого для новой точки публикации

На странице Тип пункта публикации (Publishing Point Type) можно выбрать Широковещательный пункт публикации (Broadcast Publishing Point) или Пункт публикации по запросу (On-Demand Publishing Point), как показано на рис. 8-10. Один из параметров на этой странице может быть недоступен — это зависит от опции, выбранной на предыдущей странице.

На странице Параметры передачи для широковещательных пунктов публикации (Delivery Options For Broadcast Publishing Points) можно указать Одноадресную (Unicast) или Многоадресную (Multicast) передачу содержимого, как показано на рис. 8-11. По умолчанию выбрана одноадресная передача, которая подходит для большинства приложений, однако использует всю полосу пропускания. Для сетей с поддержкой многоадресной передачи данных можно выбрать Многоадресную (Multicast) передачу содержимого. При выборе многоадресной передачи можно также применить автопереключение в одноадресный режим (Unicast Rollover), обеспечивающее одноадресную передачу для клиентов, которые не могут подключиться к многоадресному потоку.

При создании пункта публикации, обеспечивающего доступ к файлам, откроется также страница Каталог (Directory Location), показанная на рис. 8-12. В поле Папка (Location Of Directory) указывается корневая папка, в которой будет размещено содержимое. В этой папке нужно хранить все аудио- и видеофайлы, которые должны быть доступны для пользователей.

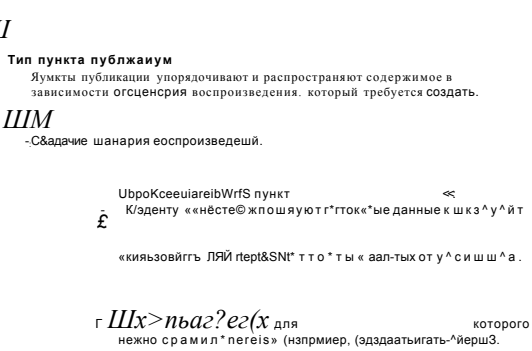


Рис. 8-10. Выбор типа пункта публикации

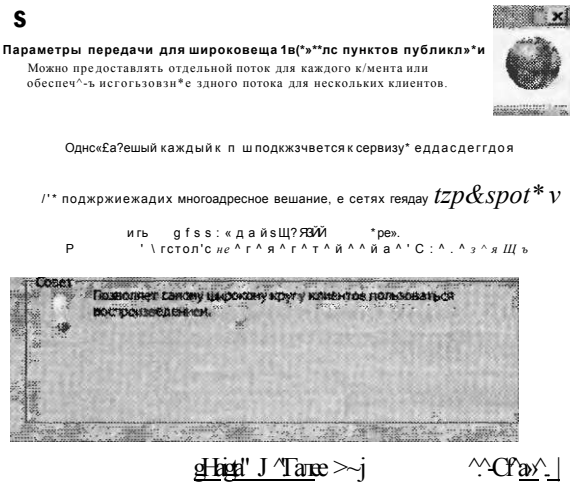


Рис. 8-11. Выбор параметра передачи для широковещательных пунктов публикации

Опция Включить доступ к содержимому каталога с помощью подстановочных знаков (Enable Access To Directory Content Using Wildcards) (она доступна при создании пункта публикации по запросу) позволяет пользователям получать прямой доступ к любому файлу, размещенному в корневой папке. Для этого они могут вручную модифицировать URL, если им известно имя нужного файла.

Эту опцию удобно использовать для работы с большим количеством файлов, для которых требуются прямые ссылки. Тем не менее если вы хотите, чтобы пользователи получали доступ лишь к файлам, которые вы явно сделали доступными, отключите этот параметр.

На странице Воспроизведение содержимого (Content Playback) представлены опции управления порядком воспроизведения содержимого в каталоге или списке воспроизведения:

- Повтор (содержимое воспроизводится непрерывно) (Loop (Content Plays Continuously));
- В случайном порядке (содержимое воспроизводится в случайном порядке) (Shuffle (Content Plays Randomly)).

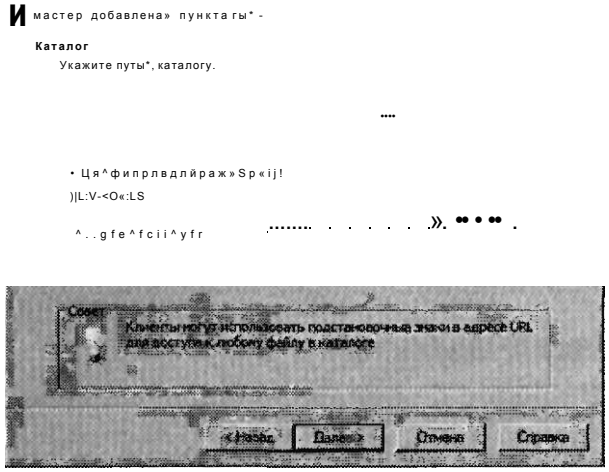


Рис. 8-12. Выбор каталога для нового пункта публикации

При выборе кодировщика прямого потока на странице Адрес URL кодировщика (Encoder URL) будет предложено указать URL кодировщика, обеспечивающего воспроизведение содержимого мультимедиа, как показано на рис. 8-13. Этот URL должен включать полный путь и номер порта сервера, на котором запущен кодировщик служб Windows Media.

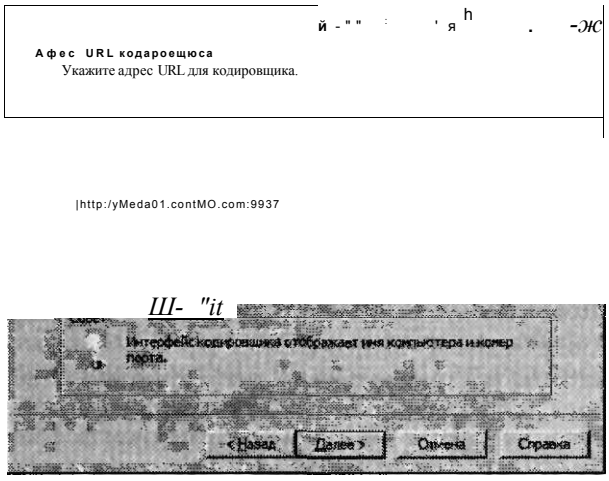


Рис. 8-13. Указание URL кодировщика при создании широковещательного пункта публикации

На странице Журнал одноадресного вещания (Unicast Logging) мастера добавления пункта публикации можно включить регистрацию данных о клиентах, получающих содержимое точки публикации в виде одноадресного потока. На странице (Publishing Point Summary) представлен список параметров, выбранных на предыдущих страницах, как показано на рис. 8-14. На последней странице мастера содержится важная информация о URL, который будет использоваться для получения доступа к пункту публикации, как показано на рис. 8-15. На этой странице также можно выбрать различные файлы, обеспечивающие для пользователей доступ к содержимому. Мы опишем их далее в этом разделе.

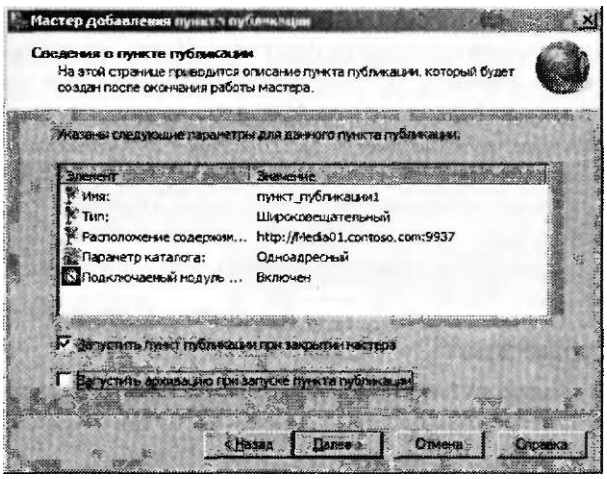


Рис. 8-14. Итоговые параметры создаваемого пункта публикации

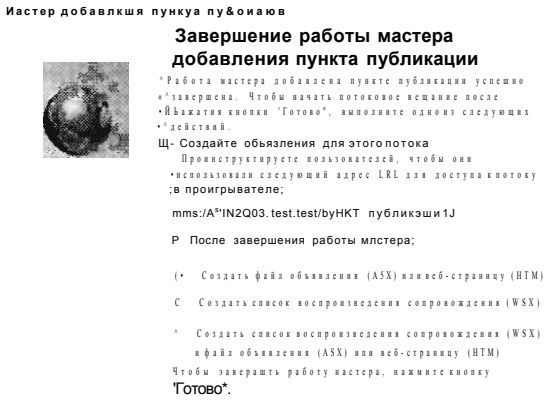


Рис. 8-15. Завершение работы мастера добавления пункта публикации

Администрирование пунктов публикации

Состоянием пунктов публикации можно управлять с помощью консоли Службы Windows Media (Windows Media Services). Для управления состоянием

пункта публикации и выполнения других административных функций щелкните соответствующий объект правой кнопкой мыши. Далее приведен список доступных команд:

- Запустить (Start);
- Остановить (Stop);
- Разрешить новые подключения (Allow New Connections);
- Запретить новые подключения (Deny New Connections);
- Дублировать (Duplicate);
- Переименовать (Rename);
- Удалить (Remove).

Отдельные пункты публикации можно запускать и останавливать независимо. Вы также можете использовать команду Дублировать (Duplicate) для создания нового пункта публикации (с новым именем и URL) иа основе параметров существующего пункта публикации. В случае запрета новых подключений содержимое пункта публикации становится недоступным для новых пользователей, однако для уже подключенных пользователей потоковая передача информации продолжается. При использовании команды Остановить (Stop) выполняется отключение всех активных пользователей п завершение всех потоков пункта публикации.

Наблюдение за пунктами публикации

На вкладке Монитор (Monitor) пункта публикации представлен обзор текущих подключений и статистика текущего использования содержимого, как показано на рис. 8-16.

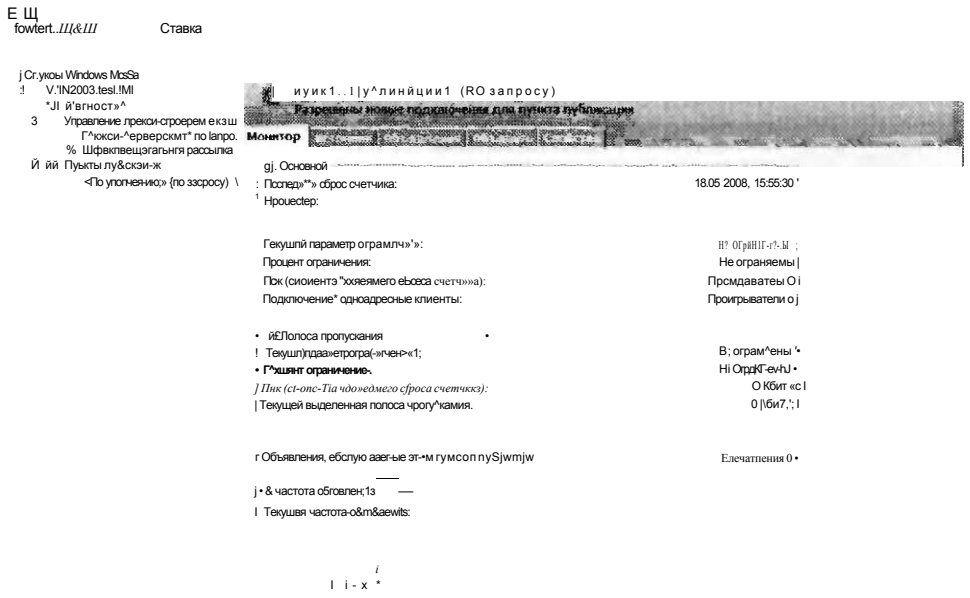


Рис. 8-16. Мониторинг активности пункта публикации с использованием консоли служб Media Services

По умолчанию обновление окна выполняется каждые 3 с. Для возврата исходных значений всех счетчиков с кумулятивным накоплением значений можно использовать команду Сбросить все счетчики (Reset All Counters), которая представлена в виде значка в нижней части окна.

Настройка параметров источника

Для указания доступных для пользователей файлов мультимедиа каждый пункт публикации должен располагать исходной информацией. Как уже говорилось в предыдущем разделе, вы можете указать сведения по умолчанию при создании нового пункта публикации с помощью Мастера добавления пункта публикации (Add Publishing Point Wizard). Для внесения изменений в параметры источника можно также использовать консоль Службы Windows Media (Windows Media Services). Для этого выберите пункт публикации и перейдите на вкладку Источник (Source), показанную на рис. 8-17.

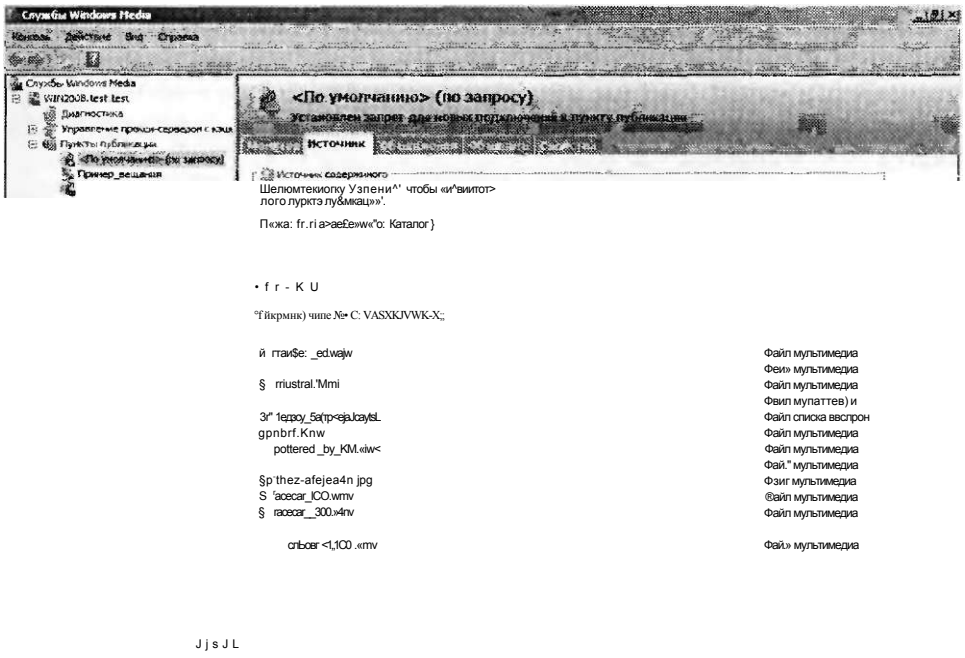


РИС. 8-17. Настройка параметров источника для пункта публикации по запросу

Опции и сведения на этой странице зависят от тина созданного пункта публикации. Например, пункт публикации, обеспечивающий доступ к прямому потоку широковещания, будет располагать информацией о URL источника потока, а пункты публикации по запросу включают список воспроизведения и сведения о размещениях файлов. Параметры на вкладке Источник (Source) обеспечивают быстрый способ модификации доступного для пользователей типа содержимого без необходимости создания нового пункта публикации. Вы можете выделить видео и щелкнуть кнопку Пробный поток (Test Stream) для получения доступа к мультимедиа, используя для воспроизведения содержимого Windows Media Player или Windows Internet Explorer.

Создание объявлений

После подготовки нового пункта публикации для сервера Windows Media вам потребуется обеспечить доступ к содержимому для пользователей. С помощью консоли Службы Windows Media можно создавать объявления, представляющие собой метод создания ссылок и списков воспроизведения для обеспечения доступа к содержимому. В последнем шаге мастера можно автоматически создать соответствующие типы объявлений, включая следующие:

- Создать файл объявления (ASX) или веб-страницу (HTM) (Create An Announcement File (.asx) Or Web Page (.htm));
- Создать список воспроизведения сопровождения (WSX) (Create A Wrapper Playlist (.wsx));
- Создать список воспроизведения сопровождения (WSX) и файл объявления (ASX) или веб-страницу (HTM) (Create A Wrapper Playlist (.wsx) And Announcement File (.asx) Or Web Page (.htm)).

В зависимости от выбранной опции мастер предоставит один или несколько параметров. Параметры объявлений существующего пункта публикации можно просмотреть и модифицировать, выбрав пункт публикации в консоли Службы Windows Media (Windows Media Services) и открыв вкладку Объявить (Announce), показанную на рис. 8-18.

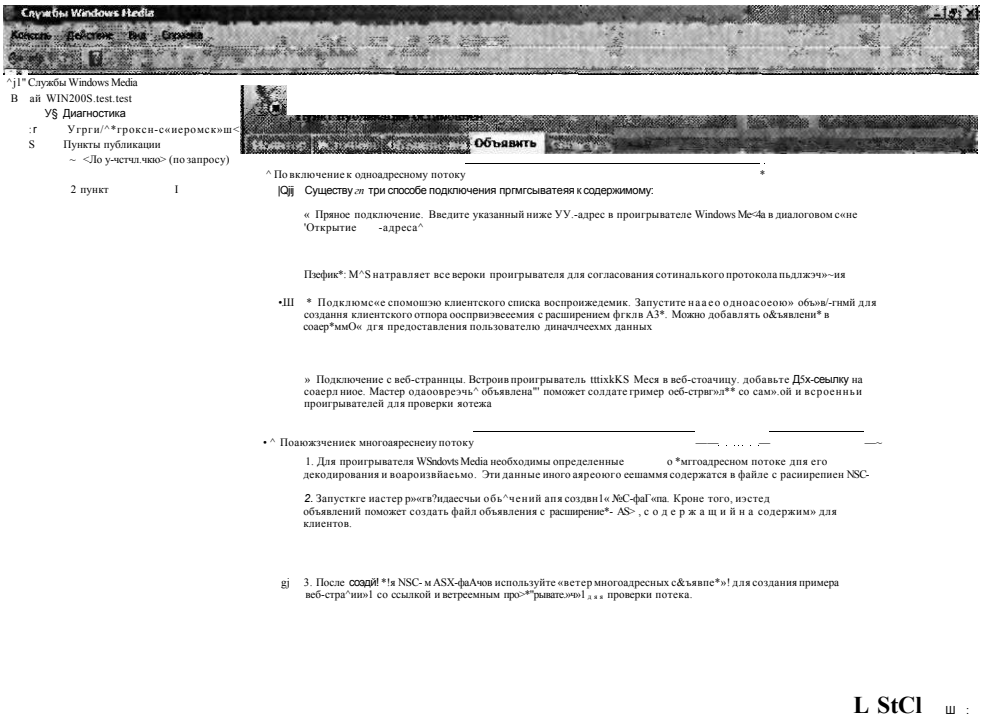


Рис. 8-18. Параметры вкладки Объявить (Announce) для пункта публикации

Сведения объявлений можно использовать в собственных веб-страницах (например, создав тег, который непосредственно ссылается на пункт публика-

ции). Вы также можете обеспечить ссылки на файлы списков воспроизведения или само сопровождение.

Мастер создания сопровождения

Мастер создания сопровождения (Create Wrapper Wizard) позволяет создать список воспроизведения сопровождения, как показано на рис. 8-19.

шшшшшш&ашшшшшшшШШшшшшшш'.М

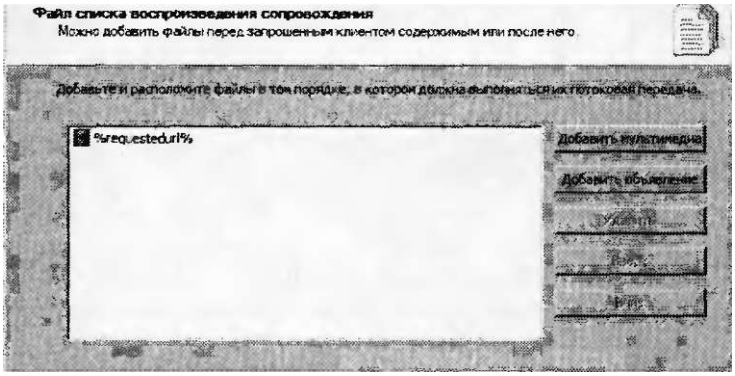


Рис. 8-19. Окно мастер создания сопровождения

Чтобы добавить новые файлы или другие типы содержимого, щелкните кнопку Добавить мультимедиа (Add Media). Откроется окно, которое представлено на рис. 8-20.

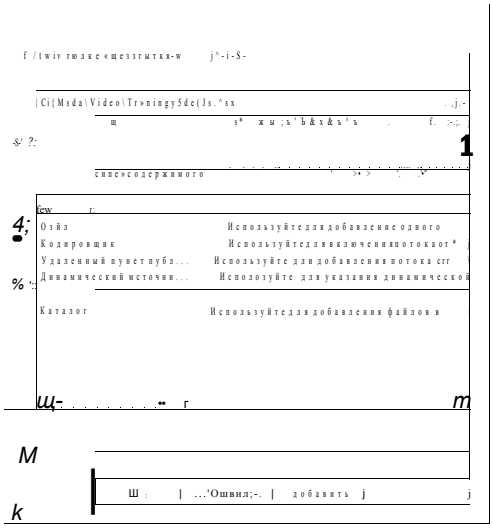


Рис. 8-20. Добавление мультимедиа в список воспроизведения сопровождения

Данные в этом окне могут быть представлены другими пунктами публикации и могут включать смесь содержимого по запросу и прямого потока кодировщика.

После выбора соответствующей опции вам будет предложено указать место хранения файла .vvsx. Обычно этот файл следует помещать в корневую нанку пункта публикации, чтобы он был доступен для пользователей. Вы также можете скопировать или переместить этот файл в другое место, например в корневую папку веб-сайта.

Мастер одноадресных объявлений

При выборе одноадресной доставки потокового содержимого для настройки соответствующих опций можно использовать Мастер одноадресных объявлений (Unicast Announcement Wizard). По умолчанию перед одноадресным URL стоит префикс mms (например, mms://Server2.contoso.com/Media). Клиентские проигрыватели мультимедиа, например Проигрыватель Windows Media (Windows Media Player), автоматически связываются с этим типом URL. чтобы воспропз ведение содержимого могло запускаться автоматически, после того как пользователь щелкнет соответствующую гиперссылку на веб-странице. На странице мастера Сохранить параметры объявления (Save Announcement Options) можно указать место сохранения файла объявления ASX, как показано па рис. 8-21. 1lo умолчанию файл сохраняется в корневой папке объекта Default Web Site роли сервера Веб-сервер (IIS) (Web Server (IIS)).

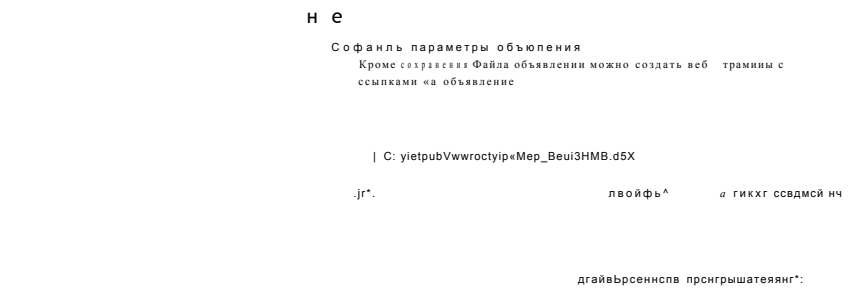


Рис. 8-21. Сохранение файлов объявлений

На этой странице мастера можно также создать веб-страницу HTML со встроенным проигрывателем и ссылкой на содержимое. При использовании этого метода веб-разрабогчики могут с помощью тегов HTML и проигрывателя мультимедиа включать собственный код. Позже вы сможете загружать эту веб-страницу прямо в Internet Explorer. Если у вас установлен Проигрыватель Windows Media (Windows Media Player), вы сможете протестировать объявление путем воспроизведения видео, как показано па рис. 8-22. Если вы планируете поместить ссылку на мультимедиа в существующую веб-страницу, .можете установить флажок Скопировать в буфер синтаксис для встроенного проигрывателя на веб-странице (Copy The Syntax For Embedding A Player In A Web Page To The Clipboard).

На странице мастера Изменение метаданных объявления (Edit Announcement Metadata) можно указать сведения заголовка и автора содержимого, а также авторское право. Эта информация будет автоматически передаваться на проигрыватели пользователей.

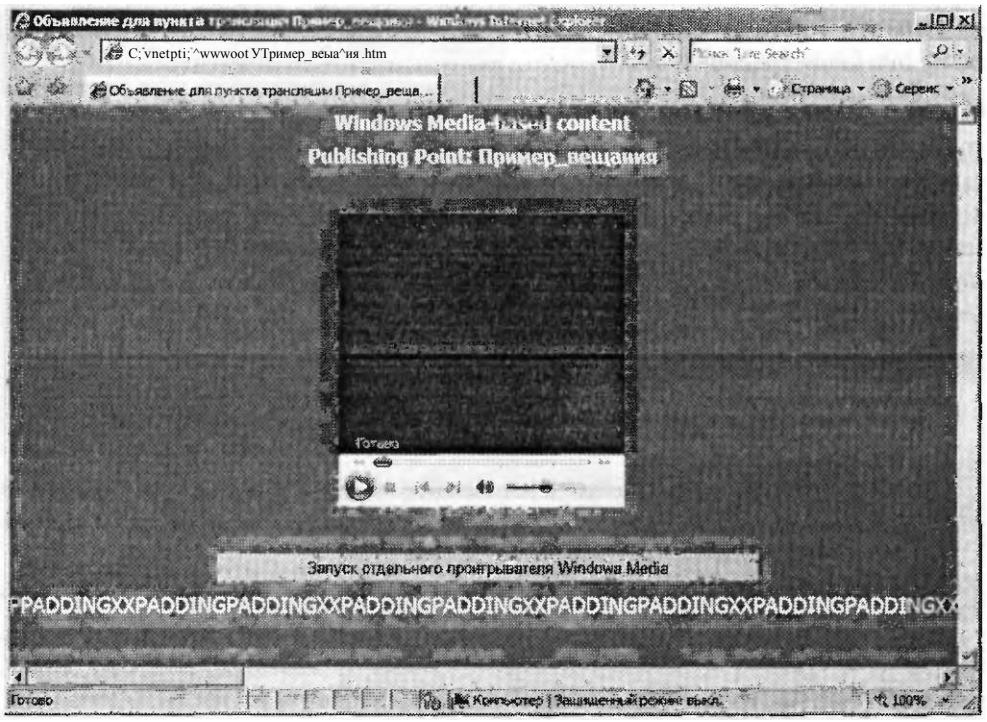


Рис. 8-22. Проверка веб-страницы объявления, созданной с помощью мастера одноадресных объявлений

Для проверки выбранных параметров можно использовать кнопки в окне Проверочное одноадресное объявление (Test Unicast Announcement). Это окно, показанное на рис. 8-23, открывается автоматически после завершения работы Мастера одноадресных объявлений (Unicast Announcement Wizard).

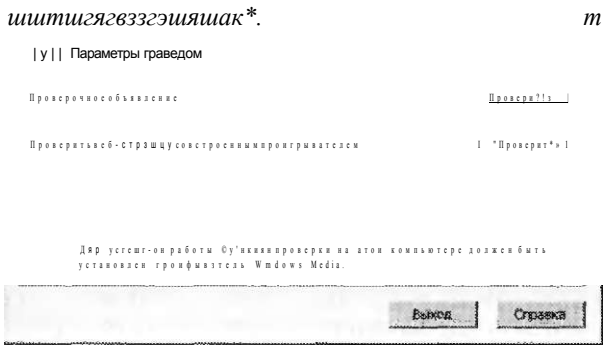


РИС. 8-23. Проверка одноадресных объявлений

Первая кнопка Проверить обеспечивает прямой доступ к списку воспроизведения. Щелчком этой кнопки открывается Проигрыватель Windows Media (Windows Media Player) и начинается воспроизведение содержимого. Щелчком второй кнопки Проверить (Test), находящейся напротив опции Проверить веб-страницу со встроенным проигрывателем (Test Web Page With Embedded Player), запускается Internert Explorer, в который загружается тестовая веб-страница (если она была создана).

Мастер многоадресных объявлений

При настройке пунктов публикации, поддерживающих многоадресное широковещание потоков мультимедиа, для создания необходимых файлов можно использовать Мастер многоадресных объявлений (Multicast Announcement Wizard). На странице Указание файлов для создания (Specify Files To Create) можно выбрать метод обеспечения ссылок для многоадресного потока, как показано на рис. 8-24.

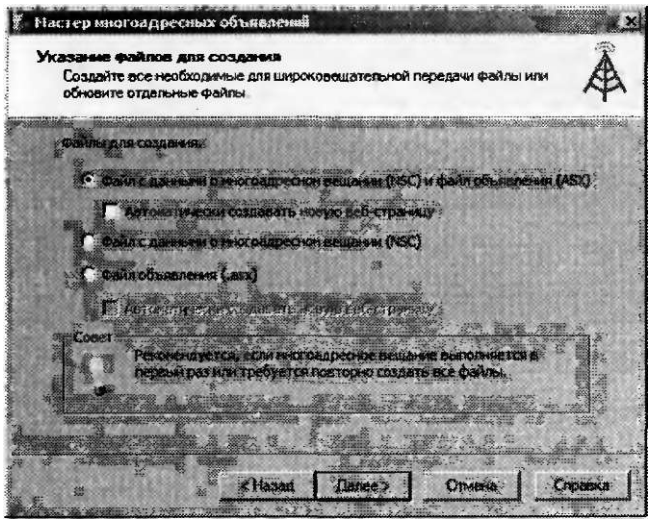


Рис. 8-24. Создание многоадресного объявления

Опция по умолчанию Файл с данными о многоадресном вещании (NSC) и файл объявления (ASX) (Multicast Information File (.nsc) And Announcement File (.asx)) создает все необходимые файлы для обеспечения доступа к содержимому. Вы также можете по отдельности создавать или воссоздавать файлы NSC и ASX. Если установить флажок Автоматически создавать новую веб-страницу (Automatically Create A Web Page), будет генерироваться HTML-файл, включающий ссылку на многоадресное содержимое.

На странице Форматы потока (Stream Formats) можно определить потоки, которые будут доступны в объявлении. Вы можете обеспечить доступ к различным потокам в разных пунктах публикации на том же или другом сервере Службы Windows Media (Windows Media Services). Щелкните кнопку Добавить (Add), чтобы открыть диалоговое окно Добавление форматов потоков (Add Stream Formats), показанное на рис. 8-25. В поле Папка содержимого (Location Of Content) можно непосредственно указать аудио- или видеофайл, либо ука-

зать размещение кодировщика прямого потока мультимедиа. Вы также можете ссылаться на поток из другого пункта публикации. Когда вы щелкнете кнопку Далее (Next), Мастер многоадресных объявлений (Multicast Announcement Wizard) автоматически попытается проверить ссылки на указанное содержимое.

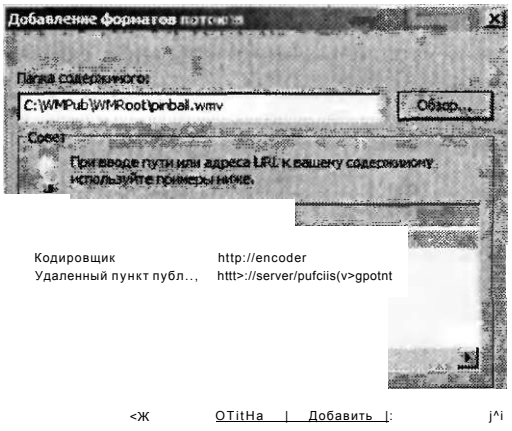


Рис. 8-25. Добавление форматов потоков с помощью мастера многоадресных объявлений

На странице Сохранение файлов многоадресных объявлений (Save Multicast Announcement Files) указаны физические пути, по которым будут сохраняться выбранные файлы (рис. 8-26). По умолчанию выбрана корневая папка объекта Default Web Site, создаваемого при установке роли Веб-сервер (IIS) (Web Server (IIS)). Тем не менее вы можете изменить размещения файлов, чтобы объявления были доступны еще на одном веб-сайте.

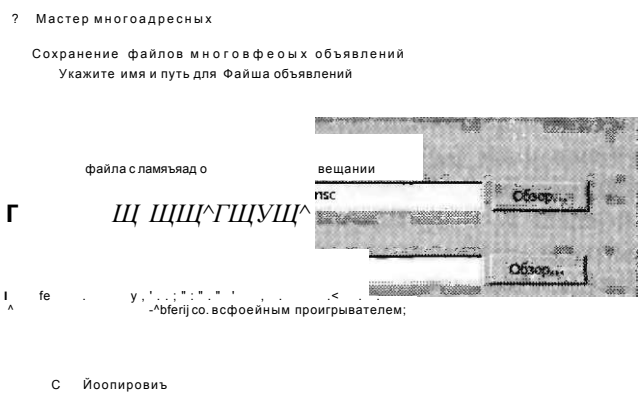


Рис. 8-26. Выбор размещений для хранения файлов объявлений широковещания в файловой системе

Объявление может ссылаться на веб-сервер или общий сетевой ресурс, где хранится файл NSC с данными широковещания. Нужную опцию можно выбрать на странице Указание URL-адреса файла данных о многоадресном вещании (Specify URL To Multicast Information File), как показано на рис. 8-27. В случае использования общего сетевого ресурса учетные записи служб Windows Media должны располагать разрешениями чтения файла. Опцию Сетевой ресурс (Network Share) удобно применять для централизованного создания файлов данных широковещания и управления ими.

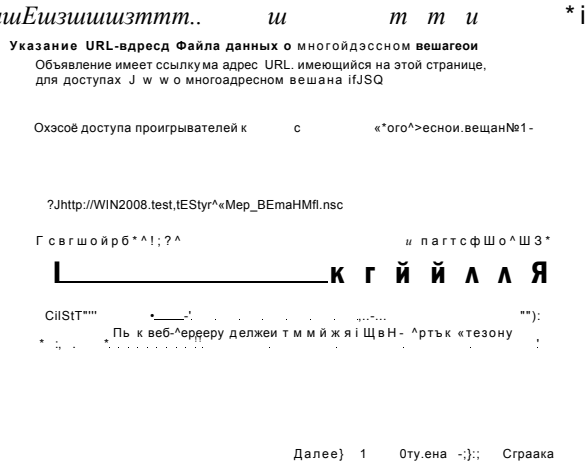


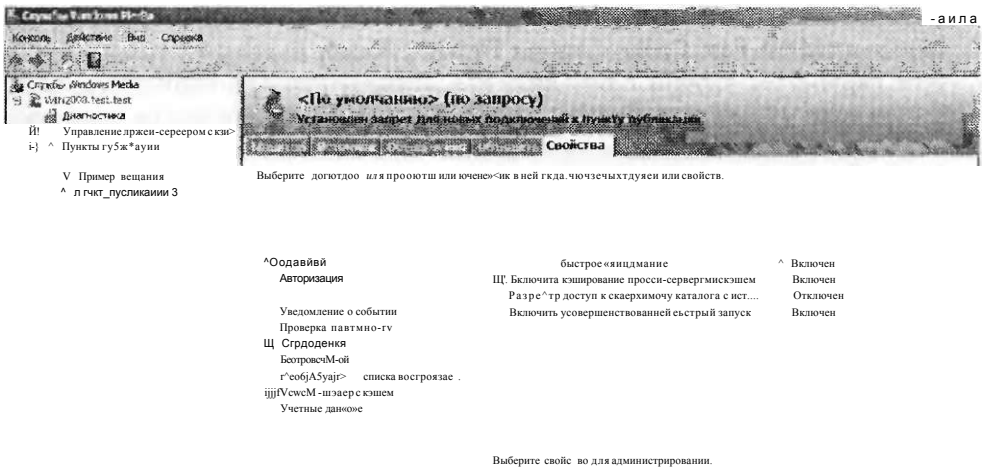
Рис. 8-27. Выбор размещений файлов данных широковещания

Поскольку многоадресные потоки предназначены для обеспечения доступа к прямому широковещанию, поток аудио или видео не будет доступен для автоматического повтора воспроизведения. Опция Да (Yes) на странице Архивация содержимого (Archive Content) используется для автоматического создания архивного видеофайла, доступ к которому можно будет получить после завершения прямого потока широковещания.

После завершения работы Мастера многоадресных объявлений (Multicast Announcement Wizard) сгенерированные файлы п параметры можно протестировать точно таким же образом, как и при работе с Мастером одноадресных объявлений (Unicast Announcement Wizard). Например, вы можете загрузить веб-страницу, содержащую встроенный проигрыватель для прямого широковещания. Следует, однако, отметить, что если прямой поток запущен из указанного кодировщика, вы не сможете просмотреть файлы мультимедиа.

Настройка свойств пункта публикации

Для настройки возможностей и опций, доступных для каждого пункта публикации, Службы Windows Media (Windows Media Services) используют модульную архитектуру. Чтобы открыть эти параметры, в консоли Службы Windows Media выберите пункт публикации и откройте вкладку Свойства (Properties). Доступные опции показаны на рис. 8-28.



ш ш к ш* I о ш

Рис. 8-28. Свойства пункта публикации по запросу

Список категорий и их параметров по умолчанию в значительной степени зависит от опций, которые использовались при создании пункта публикации.

Например, категория Ограничения (Limits) содержит многочисленные опции для управления полосой пропускания и производительностью, в том числе и следующие:

- Ограничить подключения проигрывателя (Limit Player Connections);
- Ограничить подключения исходящего распределения (Limit Outgoing Distribution Connections);
- Ограничить среднюю полосу пропускания проигрывателя (Кбит/с) (Limit Aggregate Player Bandwidth (Kbps));
- Ограничить среднюю полосу пропускания исходящего распределения (Кбит/с) (Limit Aggregate Outgoing Distribution Bandwidth (Kbps));
- Ограничение пропускной способности на подключение проигрывателя (Кбиг/с) (Limit Bandwidth Per Player Connection (Kbps));
- Ограничение пропускной способности на исходящее подключение распространения (Кбит/с) (Limit Bandwidth Per Outgoing Distribution Bandwidth (Kbps));
- Ограничение пропускной способности для функции быстрого запуска для каждого подключения проигрывателя (Кбиг/с) (Limit Fast Start Bandwidth Per Player Connection (Kbps));

- Ограничить скорость представления содержимого функции быстрого кэширования (Limit Fast Cache Content Delivery Rate).

Эти параметры удобно применять для управления использованием сети, особенно если многие компоненты служб Windows Media стремятся использовать одни и те же ресурсы или на одном сервере запущено много пунктов публикации. Свойства, которые связаны с безопасностью, мы обсудим далее на этом занятии.

Управление параметрами рекламы

Для многих поставщиков содержимого реклама аудио и видео является значительным источником доходов. Консоль Службы Windows Media (Windows Media Services) можно использовать для автоматического создания рекламных объявлений и управления ими. Для просмотра и модификации параметров выберите пункт публикации и откройте вкладку Объявления (Advertising), показанную на рис. 8-29.

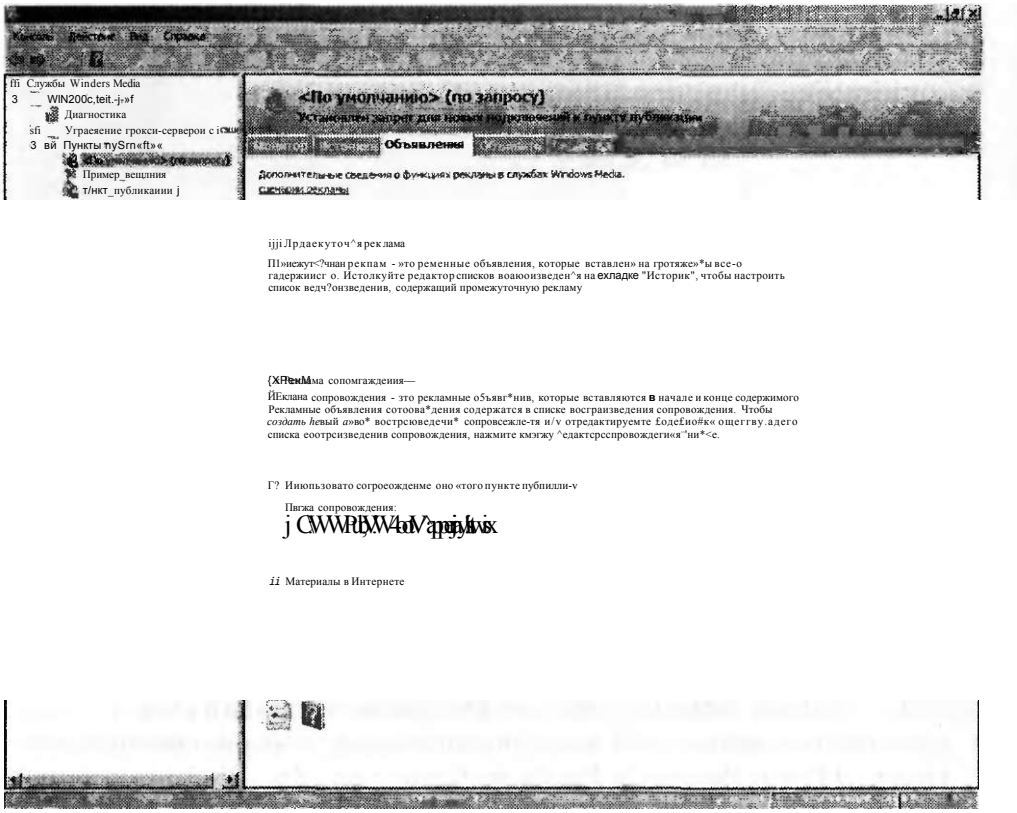


Рис. 8-29. Настройка рекламных объявлений для пункта публикации

Рекламные объявления можно включать вручную с помощью соответствующих файлов в списке воспроизведения. Однако этот процесс довольно утомителен, особенно в тех случаях, когда пользователи могут получать доступ к аудио- и видеофайлам из одного нункта публикации.

Существует три основных метода рекламы.

- **Рекламные заголовки (Banner ads)** Многие веб-страницы, ссылающиеся на содержимое аудио и видео, могут включать рекламу на исходных веб-страницах. Например, в центре страницы может отображаться широковещание видео, окруженное статическими рекламными заголовками. Для реализации этого метода никаких особых параметров конфигурации применять не требуется.
- **Реклама сопровождений (Wrapper ads)** Стандартным требованием для многих организаций является возможность автоматического воспроизведения конкретного аудио- или видеоклипа до или после получения доступа к любому потоковому содержимому. Например, служба видеоновостей может включать короткую видеозаставку при получении пользователем доступа к мультимедиа. Реклама сопровождений содержится в списках воспроизведения сопровождения. Эти рекламные объявления могут автоматически воспроизводиться во время прямого широковещания, чтобы пользователи, подключившиеся к уже запущенному потоку, также наслаждались рекламой.
- **Промежуточная реклама (Interstitial ads)** Эти рекламные объявления воспроизводятся в разные моменты на протяжении воспроизведения всего потокового содержимого. Например, сетевой телевизионный ретранслятор может запускать новую рекламу после воспроизведения четырех видеофайлов по запросу. Эти рекламные объявления можно определить вручную путем модификации параметров списков воспроизведения на вкладке Источник (Source) свойств пункта публикации. Отредактировав списки воспроизведения вручную, вы получите тот же результат.

На вкладке Объявления (Advertising) также есть ссылка на центр партнеров Windows Media (Windows Media Partner Center). Компании, перечисленные на этом сайте, предлагают технологию DRM (Digital Rights Management) и такие услуги, как централизованное распределение рекламы.

Настройка безопасности служб Windows Media

Как и при работе с доступными в сети другими типами содержимого, важно, чтобы доступ к потоковому аудио и видео получали лишь авторизованные пользователи. Некоторые организации обеспечивают содержимое только для оплативших услугу или зарегистрированных пользователей, ограничивая использование полосы пропускания сети.

Неавторизованным пользователям также может не разрешаться прямой доступ к содержимому или загрузке и дальнейшему распространению файлов мультимедиа. Службы Windows Media (Windows Media Services) обеспечивают несколько методов безопасности Служб потокового мультимедиа (Streaming Media Services). По умолчанию параметры безопасности могут быть определены на уровне сервера. Эти параметры будут автоматически применены ко всем пунктам публикации на сервере. Тем не менее вы можете изменять параметры для отдельных пунктов публикации. В этом разделе описаны параметры проверки подлинности, авторизации и разрешения, которые доступны на вкладке Свойства (Properties) пункта авторизации.

Настройка проверки подлинности

По умолчанию новые пункты публикации наследуют параметры безопасности, определенные на уровне сервера. Конкретные параметры для различных типов содержимого можно определить в категории (Authentication) вкладки Свойства (Properties) пункта публикации, показанной на рис. 8-30.

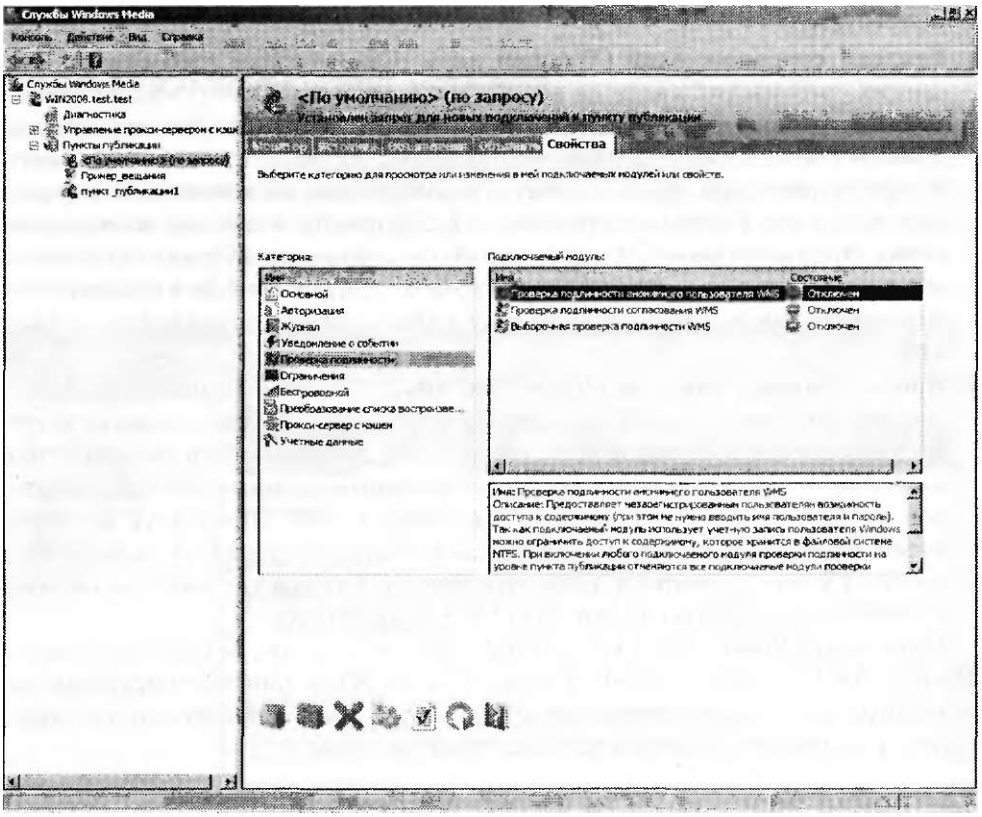


Рис. 8-30. Параметры проверки подлинности для пункта публикации

Проверку подлинности пользователей можно выполнять с помощью трех методов. При использовании метода Проверка подлинности анонимного пользователя WMS (WMS Anonymous User Authentication) службы Windows Media пе будут предлагать пользователям указать свои учетные данные. Тем не менее если включить этот метод, пользователи смогут получать доступ к содержимому, предназначенному лишь для пользовательской учетной записи с разрешениями файловой системы NTFS. По умолчанию применяется пользовательская учетная запись в формате WM **USII**mmСервера, которая автоматически создается при установке роли сервера Службы потокового мультимедиа (Streaming Media Services). Чтобы изменить параметры учетной записи, дважды щелкните модуль Проверка подлинности анонимного пользователя WMS (WMS Anonymous User Authentication) и укажите соответствующее пользовательское имя

и пароль. Анонимную проверку подлинности удобно использовать для предоставления всем пользователям сервера мультимедиа доступа к одной коллекции содержимого.

Метод Проверка подлинности согласования WMS (WMS Negotiate Authentication) используется в основном для поддержки пользователей Интернета. Для запросов и получения учетных данных по сети этот метод применяет протокол HTTP. Из соображений безопасности он пересылает не реальный пароль, а хэш, который можно использовать для подтверждения подлинности пользователя.

Настройка опций авторизации

В категории свойств Авторизация (Authorization) сервера Службы Windows Media (Windows Media Services) или пункта публикации определены методы проверки разрешений пользователей перед получением доступа к содержимому. Здесь представлены три опции, как показано па рис. 8-31.

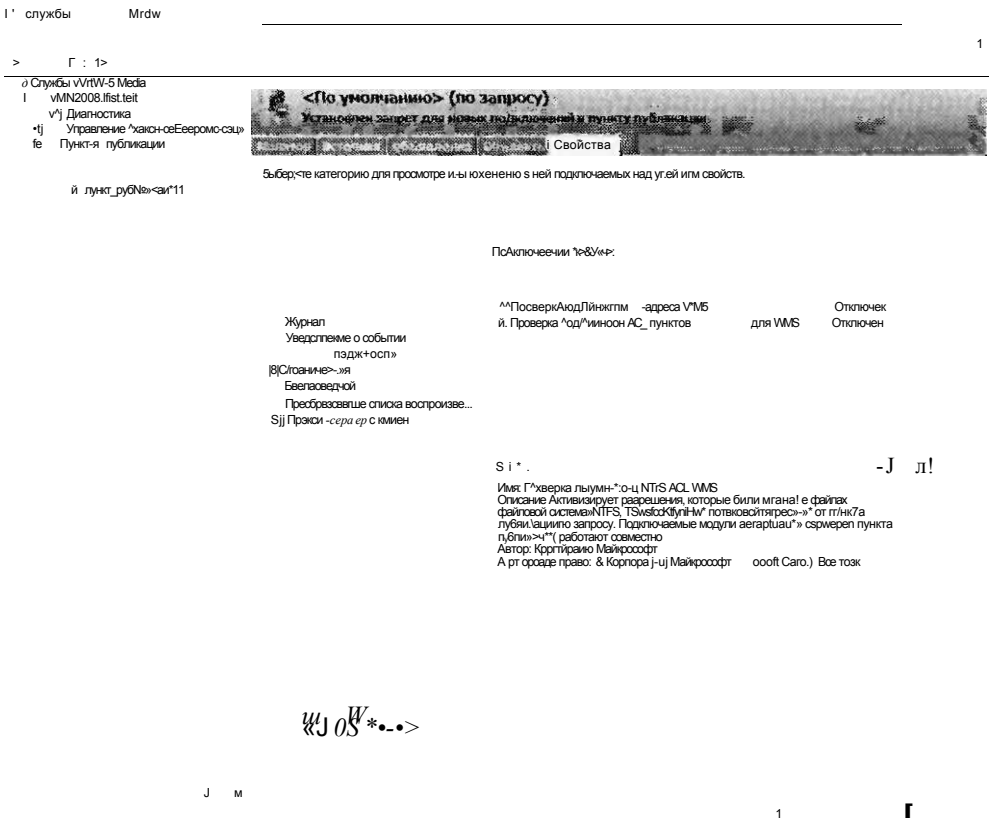


Рис. 8-31. Методы авторизации для пункта публикации

Модуль Проверка подлинности NTFS ACL WMS (WMS NTFS ACL Authentication) используется для определения разрешений доступа пользователя

к файлам разрешения файловой системы NTFS. Если включена лишь анонимная проверка подлинности, то при включении данного метода учетная запись анонимного пользователя должна располагать соответствующими разрешениями доступа к содержимому. В случае предоставления пользователем своих учетных данных перед передачей потока выполняется проверка действующих разрешений этого пользователя.

Некоторые инсталляции служб Windows Media предназначены для использования лишь определенной группой компьютеров. Например, организация может обеспечивать видеоконференции компании, для получения доступа к содержимому которых всем пользователям требуется подключаться к локальной сети (LAN) организации. С помощью модуля Проверка подлинности IP-адреса WMS (WMS IP Address Authorization) администраторы могут указать IP-адреса, с которых разрешен доступ к содержимому, как показано на рис. 8-32.

По умолчанию параметры могут быть отконфигурированы для автоматического разрешения или запрета подключений, которые не перечислены явно в имеющемся списке.

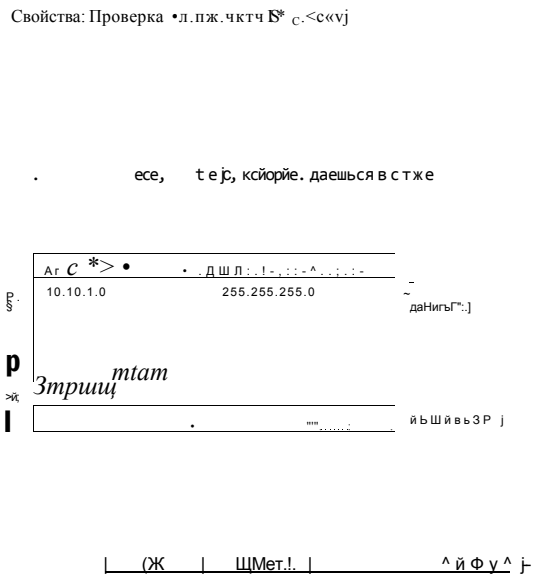


Рис. 8-32. Настройка проверки подлинности IP-адреса WMS

Модуль Проверка подлинности ACL пунктов публикации для WMS (WMS Publishing Points ACL Authentication) можно использовать для определения пользователей и групп, которым будет разрешен доступ к пункту публикации, как показано на рис. 8-33.

Для получения доступа к содержимому пользователи должны располагать хотя бы разрешениями чтения. По умолчанию группа Все (Everyone) располагает этими разрешениями доступа к содержимому. Для обеспечения возможностей модификации содержимого пункта публикации пользователям и группам можно назначить разрешение Запись (Write) или Создание (Create)

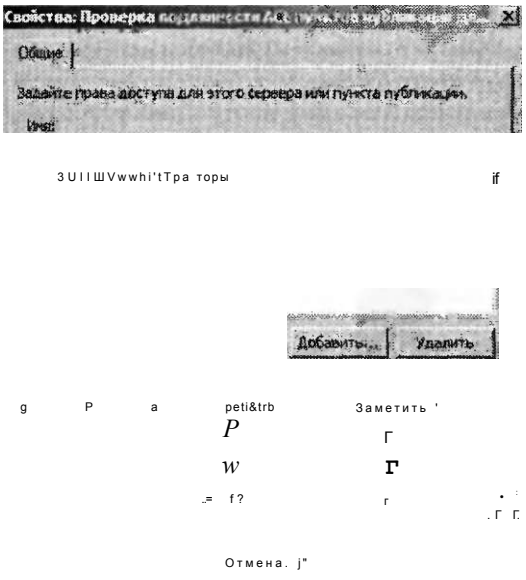


Рис. 8-33. Настройка параметров авторизации модуля проверки подлинности ACL пунктов публикации для WMS

Разрешения веб-сервера

Существует еще один метод обеспечения безопасности доступа к потоковому аудио- и видеосодержимому, в котором не задействованы Службы Windows Media (Windows Media Services). Для обеспечения безопасности ссылок и другого содержимого можно использовать опции прав доступа и безопасности роли Веб-сервер (IIS) (Web Server (IIS)). Например, ссылки и списки воспроизведения можно отображать лишь для зарегистрированных пользователей, которые применяют безопасное SSL-подключение. Более подробные сведения о настройке параметров безопасности IIS содержатся в главе 6.

Управление прокси-сервером с кэшем

При обеспечении поддержки большого количества пользователей пропускной способностью сети и ресурсами сервера довольно сложно управлять с помощью одного лишь сервера Службы Windows Media (Windows Media Services). Этот сервер сам по себе часто может являться наиболее критическим элементом п создавать проблемы производительности для клиентов. Кроме того, при сбое сервера может быть утерян доступ к аудио- и видеоданным. Для решения этих проблем можно использовать возможности кэш/прокси серверов.

С помощью таких методов, как кэширование и представительство (proxying), Службы Windows Media (Windows Media Services) могут транслировать потоковые данные с одного пункта публикации пользователям, которым нужна эта информация. При использовании кэширования сервер Windows Media копирует содержимое исходного сервера и локально сохраняет его. Кэш-сервер получает данные из источника и передает их прямо клиенту. Прокси-серверы

используют множество компьютеров с запущенными службами Windows Media, которые передают запросы другим серверам потокового мультимедиа. Типичный пример конфигурации серверов показан на рис. 8-34.

В этой схеме исходный сервер обеспечивает прямой доступ лишь для дистрибутивных серверов. В свою очередь дистрибутивные серверы затем могут передавать потоковые данные клиентам. Таким образом снижается нагрузка на сеть и ресурсы исходного сервера Windows Media, а пользователи могут подключаться к серверам на основе конфигурации своих сетей.

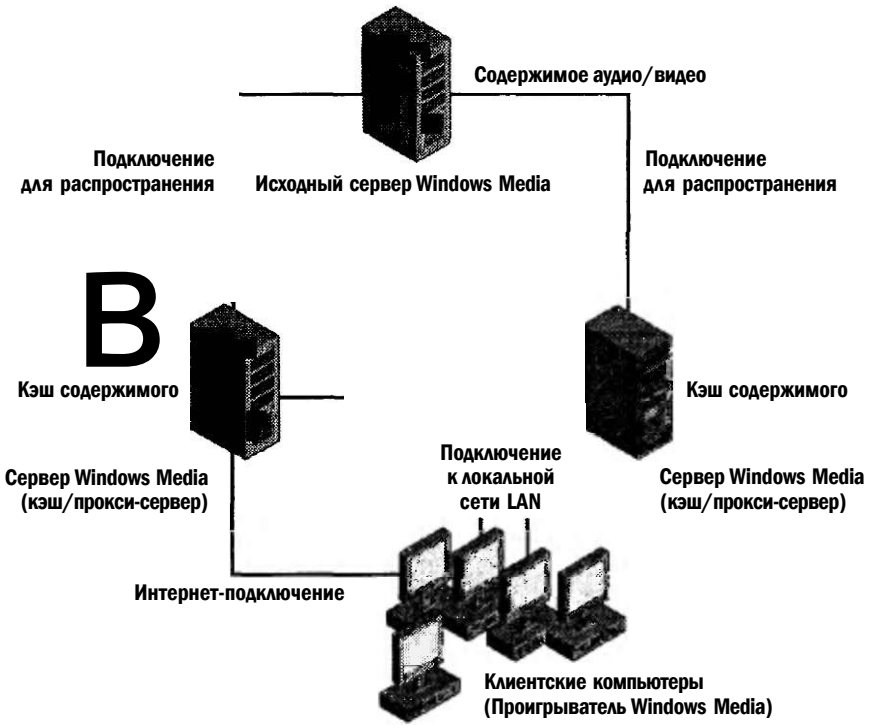


Рис. 8-34. Использование кэш/прокси-серверов для повышения расширяемости и производительности

Включение параметров кэш/прокси-серверов

По умолчанию Управление прокси-сервером с кэшем (Cache/Proxy Management) отключено в новой инсталляции компонента Службы потокового мультимедиа (Streaming Media Services). Чтобы включить эту функцию для сервера, откройте консоль Службы Windows Media (Windows Media Services) и выберите объект сервера. Затем на вкладке Свойства (Properties) откройте категорию Управление прокси-сервером с кэшем (Cache/Proxy Management). Щелкните правой кнопкой мыши Подключаемый модуль WMS Cache Proxy и примените команду Включить (Enable). Чтобы открыть опции конфигурации кэша и прокси-сервера, дважды щелкните модуль WMS Cache Proxy.

ПРИМЕЧАНИЕ Подготовка к экзамену
При использовании компонента Службы Windows Media (Windows Media Services) один сервер может выполнять множество ролей. Например, он может обеспечивать доступ к пунктам публикации по запросу и пунктам публикации прямого потока широковещания, а также представлять запросы и кэшировать содержимое для других серверов. На этом занятии используются упрощенные понятия исходных серверов и кэш/прокси-серверов. С учетом схемы вашей сети или требований сертификационного экзамена вы можете отконфигурировать один сервер для выполнения всех этих функций.

Настройка параметров кэширования

На вкладке Кэш (Cache) можно указать путь к каталогу кэша и ограничения архивирования (рис. 8-35). Для снижения нагрузки на исходный сервер кэш/прокси-сервер будет пытаться сохранять как можно больше информации. По умолчанию для кэширования не назначены никакие ограничения, однако если вы кэшируете данные для больших объемов содержимого, рекомендуется установить некоторые ограничения.

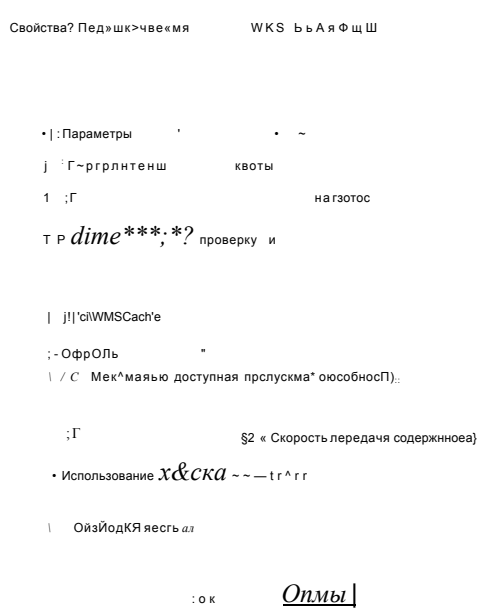


Рис. 8-35. Настройка параметров кэширования для сервера Windows Media

В области Скорость кэширования (Caching Speed) указана скорость передачи данных с исходного сервера. Если выбрать опцию Максимально доступная пропускная способность (Maximum Available Bandwidth), кэш/прокси-сервер будет пытаться передавать содержимое с исходного сервера, используя пропускную способность файла. Эта опция удобна в случае, если доступом к одному исходному серверу располагает множество серверов кэширования.

На вкладке Prestuff представлены опции заполнения кэша мультимедиа кэш/прокси-сервера, даже если пользователи не запрашивают содержимое (рис. 8-36). Их удобно использовать для первоначального заполнения содержимого сервера перед вводом в производство (когда нагрузка будет значительно выше). При выборе первой опции информация извлекается из потока. Вам потребуется указать полный URL к пункту публикации на исходном сервере. Вы также можете ограничить пропускную способность, используемую для заполнения содержимого (операция prestuff).

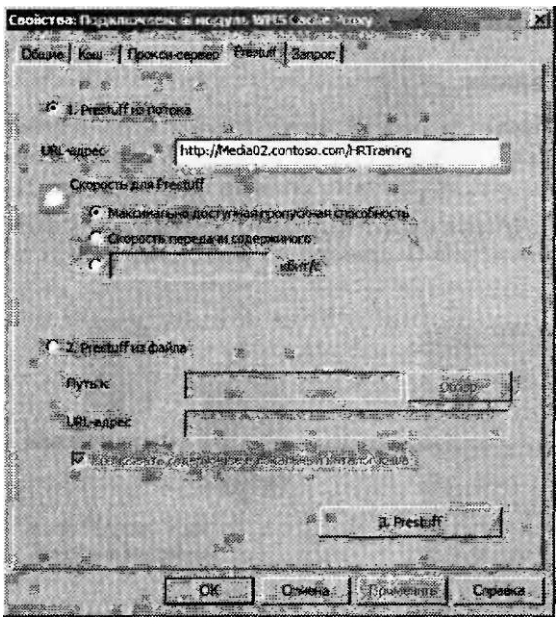


Рис. 8-36. Настройка параметров заполнения содержимого для сервера кэширования

Чтобы снизить сетевую нагрузку при передаче больших объемов данных, можно также загрузить данные prestuff из файла. В поле Путь к содержимому (Content Path) можно указать локальное размещение файловой системы или сетевой путь. В поле URL-адрес (Stream URL) указываются файлы из существующего пункта публикации. Для запуска операции заполнения содержимого prestuff щелкните кнопку Prestuff.

К СВЕДЕНИЮ Тестирование инфраструктуры служб Windows Media

При планировании передачи потокового мультимедиа для большого количества пользователей для тестирования инфраструктуры служб Windows Media имеет смысл создать некоторую нагрузку. Корпорация Microsoft разработала симулятор нагрузки Windows Media Load Simulator для службы Windows Media Services 9 Series. Этот бесплатный инструмент используется для генерирования нагрузки и имитации пользовательской активности. Данный симулятор и другие утилиты можно найти на странице Windows Media Services 9 Series Tools and Add-ins по адресу *http://www.microsoft.corn/iemdowsmedia/forpros/seme/tools.aspx.*

Настройка параметров прокси

Для снижения нагрузки исходного сервера сервер Windows Media может также представлять запросы от клиентов.

На вкладке Прокси-сервер (Proxy) представлены параметры для трех режимов прокси, описанных далее.

- **Прокси-сервер (Proxy)** Этот режим, в котором сервер представляет содержимое для клиентов, используется по умолчанию. Сервер отображается для клиента как исходный сервер Windows Media.
- **Перенаправление прокси (Proxy Redirect)** При выборе этого режима клиентские запросы перенаправляются на еще один прокси-сервер в той же сети. Чаще всего данный режим применяется в схемах конфигурации с балансировкой нагрузки для перенаправления всех пользователей на определенный сервер с доступным содержимым.
- **Обратный прокси-сервер (Reverse Proxy)** При использовании этого режима входящие запросы перенаправляются в указанный пункт публикации. Обратный прокси-сервер выполняет проверку подлинности пользователя и запрашивает содержимое на исходном сервере.

В общем, используя прокси-серверы, вы можете повысить возможность расширяемости пункта распределения содержимого сервера Windows Media.

Настройка параметров кэш/прокси для пунктов публикации

Включив и отконфигурировав на соответствующих серверах Управление прокси-сервером с кэшем (Cache/Proxy Management), вы можете использовать Службы Windows Media (Windows Media Services) для настройки параметров кэширования. Для этого выберите пункт публикации и откройте вкладку Свойства (Properties). Категория Прокси-сервер с кэшем (Cache/Proxy) содержит свойства, определяющие кэширование информации. Для широковещательных пунктов публикации доступен параметр Срок действия разделения потока (Stream Splitting Expiration). Он указывает время, в течение которого можно получить доступ к содержимому перед запросом исходного сервера для проверки обновлений содержимого. С той же целью используется свойство Срок действия кэша (Cache Expiration) пунктов публикации по запросу. По умолчанию для обоих параметров задано значение 86 400 с (24 ч).

Мониторинг кэш/прокси-серверов

В раздел Управление прокси-сервером с кэшем (Cache/Proxy Management) консоли Службы Windows Media (Windows Media Services) включены два объекта. Эти объекты используются для наблюдения за текущей производительностью и использованием прокси. Сведения, отображаемые в разделах Прокси-сервер с кэшем по запросу (Cache/Proxy On-Demand) и Широковещательная рассылка прокси-сервера с кэшем (Cache/Proxy Broadcast), зависят от типа пункта публикации на исходном сервере. Этими параметрами можно управлять независимо. Например, вы можете запретить новые подключения к содержимому по запросу и разрешать новым клиентам получать доступ к потокам широковещания. На вкладке Монитор (Monitor) представлены данные статистики и конфигурации (рис. 8-37).

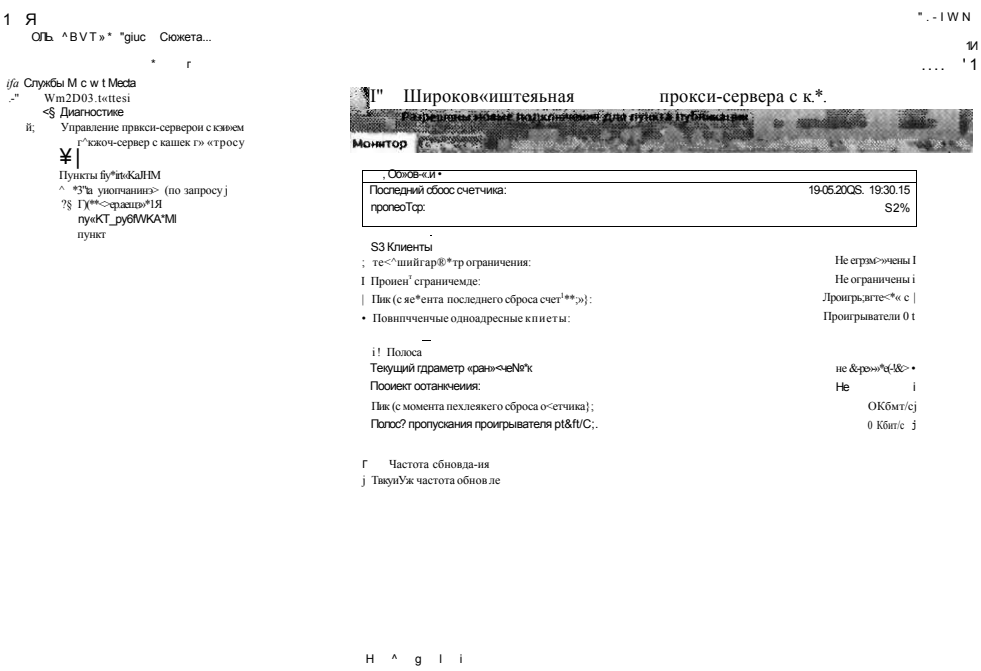


Рис. 8-37. Наблюдение за параметрами и производительностью прокси-сервера с кэшем

Обеспечение защиты мультимедиа с помощью DRM

Организациям, обеспечивающим ценное содержимое для своих пользователей, требуются гарантии того, что эта информация используется должным образом. Например, если пользователь может сохранить копию видеофайла на своем компьютере, ему нельзя разрешать передавать эту копию другим пользователям или размещать ее на веб-сайте без разрешения поставщика содержимого. Технические средства защиты авторских прав Digital Rights Management (DRM) позволяют поставщикам и создателям содержимого ограничивать распространение своей информации. Защиту содержимого можно обеспечить несколькими способами.

Сторонний партнер DRM

Службы Windows Media (Windows Media Services) предоставляют расширяемую архитектуру, позволяющую добавлять подключаемые модули для обеспечения функциональности DRM. Эти модули поставляются сторонними организациями, работающими в области защиты содержимого. Более подробные сведения о таких организациях можно найти па веб-сайте Microsoft Windows Media DRM Partners по адресу *http://www.microsoft.com/windows/wifidowsmedia/forpros/drm/9series/providers.aspx.*

Службы управления правами Active Directory

В Windows Server 2008 включена роль Службы управления правами Active Directory (Active Directory Tights Management Services, AD RMS). Эта роль сервера позволяет компьютеру Windows Server 2008 выпускать лицензии для создания и защиты такого содержимого, как файлы мультимедиа и документы. Для использования этой инфраструктуры приложения, создающие содержимое, должны быть совместимы с RMS. В качестве примеров таких совместимых приложений можно привести Microsoft Office System 2003 и Microsoft Office 2007. Функции RMS также можно применять в Internet Explorer. Более подробные сведения о службах AD RMS находятся на веб-сайте Microsoft TechNet по адресу *http://technet.microsoft.com.*

Другие методы обеспечения защиты содержимого

Существуют и другие методы обеспечения защиты цифрового аудио- и видеосодержимого. Например, для разрешения доступа к содержимому лишь зарегистрированным пользователям вы можете реализовать веб-авторизацию и проверку подлинности. Для предотвращения доступа к файлам содержимого можно также использовать такие устройства сетевой безопасности, как брандмауэры. В целом для реализации DRM используется несколько компонентов, которые следует отконфигурировать для разрешения доступа к содержимому лишь авторизованным пользователям.

Проверьте себя

1. Какой тип пункта публикации следует создать, чтобы позволить пользователям выбирать и получать потоки данных из большой библиотеки аудио- и видеофайлов?
2. Как повысить расширяемость пункта публикации служб Windows Media на сервере, где часто возникают сетевые перегрузки?

Ответы

1. Пункт публикации по запросу позволяет пользователям запрашивать мультимедиа в любое время, а также перематывать вперед, приостанавливать воспроизведение и повторно воспроизводить содержимое.
2. Для снижения нагрузки на сервер следует отконфигурировать дополнительные кэш/прокси-серверы служб потокового мультимедиа.

Практикум. Настройка служб Windows Media

В предложенных далее упражнениях вы установите и отконфигурируете роль Службы потокового мультимедиа (Streaming Media Services) на компьютере Windows Server 2008. Перед выполнением упражнения 2 необходимо выполнить упражнение 1.

Упражнение 1. Установка служб потокового мультимедиа

В этом упражнении вы с помощью диспетчера сервера добавите службы потокового мультимедиа на сервер Server2.contoso.com. Предполагается, что вы уже загрузили и установили требуемый пакет обновления Службы Windows Media

(Windows Media Services), как описано в разделе «Установка служб потокового мультимедиа» ранее в этой главе. На локальном компьютере также должна быть установлена роль Веб-сервер (IIS) (Web Server (IIS)). Если вы еще не установили их, вам будет предложено добавить необходимую роль и службы ролей в процессе установки служб потокового мультимедиа.

1. Войдите на сервер Server2 как пользователь с административными привилегиями.
2. Откройте Диспетчер сервера (Server Manager), щелкните правой кнопкой мыши объект Роли (Roles) и примените команду Добавить роли (Add Roles). На странице Перед началом работы (Before You Begin) щелкните кнопку Далее (Next).
3. На странице Выбор ролей сервера (Select Server Roles) выберите Службы потокового мультимедиа (Streaming Media Services), после чего щелкните кнопку Далее (Next).
4. Прочитайте описание служб потокового мультимедиа и щелкните кнопку Далее (Next). Отметим, что, щелкая ссылки в области Описание (Description), вы сможете прочитать дополнительные сведения об этой службе ролей.
5. На странице Выбор служб ролей (Select Role Services) выберите три службы: Сервер Windows Media (Windows Media Server), Веб-администрирование (Web-Based Authentication) и Агент ведения журнала (Logging Agent). Щелкните кнопку Далее (Next).
6. На странице Выберите протоколы передачи данных (Select Data Transfer Protocols) оставьте параметры по умолчанию. Отметим, что вы не сможете добавить протокол HTTP, если существующий веб-сайт уже привязан к HTTP-порту 80 на локальном сервере. Щелкните кнопку Далее (Next).
7. Если будет предложено, выполните инструкции для добавления необходимых компонентов роли Веб-сервер (IIS) (Web Server (IIS)). Более подробные сведения об этой роли и ее службах содержатся в главе 5.
8. Просмотрите итоговые сведения о выбранных компонентах и щелкните кнопку Установить (Install). После завершения процесса установки щелкните кнопку Закрыть (Close).
9. В Диспетчере сервера (Server Manager) разверните объект Роли (Roles) и выберите Службы потокового мультимедиа (Streaming Media Services). Прочитайте сведения в областях События (Events), Системные службы (System Services), Службы ролей (Role Services) и Справка и поддержка (Resources And Support). Закройте Диспетчер сервера.
10. В группе программ Администрирование (Administrative Tools) запустите Службы Windows Media (Windows Media Services). Консоль автоматически подключится к локальному серверу Windows Media. Вы можете развернуть объект сервера и просмотреть конфигурацию по умолчанию. После этого закройте консоль Службы Windows Media.
11. Откройте Проводник Windows (Windows Explorer) и найдите папку %SystemDrive%\Wmpub. Просмотрите содержимое по умолчанию, размещенное в этой папке. Папка wmroot содержит образцы файлов, которые можно использовать для тестирования.
12. Закройте Проводник Windows и выйдите с сервера.

Упражнение 2. Создание и проверка нового пункта публикации

В этом упражнении вы создадите новый пункт публикации служб Windows Media. Пункт публикации будет обеспечивать доступ по запросу к нескольким образцам файлов мультимедиа, включенным в роль Службы потокового мультимедиа (Streaming Media Services). Затем вы протестируете доступ к содержимому, подключившись к видеофайлу с помощью Internet Explorer. Для выполнения тестов на локальном компьютере нужно установить компонент Возможности рабочего стола (Windows Desktop Experience).

1. Войдите на сервер Server2 как пользователь с административными привилегиями.
2. Откройте Проводник Windows (Windows Explorer) и создайте копию папки wmroot в каталоге %SystemDrive%\Wmpub. Задайте для копии папки имя ContosoVideos. Эта папка будет играть роль корневого каталога нового пункта публикации. После этого закройте Проводник Windows.
3. В группе программ Администрирование (Administrative Tools) откройте консоль Службы Windows Media (Windows Media Services).
4. Разверните объект Server2, щелкните правой кнопкой мыши Пункты публикации (Publishing Points) и примените команду Добавить пункт публикации (мастер) (Add Publishing Point (Wizard)).
5. Для запуска Мастера добавления пункта публикации (Add Publishing Point Wizard) щелкните кнопку Далее (Next).
6. На странице Имя пункта публикации (Publishing Point Name) введите имя ContosoVideos. Щелкните кнопку Далее (Next).
7. На странице Тип содержимого (Content Type) выберите параметр Файлы (мультимедиа или списки воспроизведения) (Files (Digital Media Or Playlists)) и щелкните кнопку Далее (Next).
8. На странице Тип пункта публикации (Publishing Point Type) выберите сценарий Пункт публикации по запросу (On-Demand Publishing Point). Этот сценарий позволит пользователям подключаться ко всем доступным видеофайлам (при наличии соответствующих разрешений), а также управлять воспроизведением во время приема потока. Щелкните кнопку Далее (Next).
9. На странице Каталог (Directory Location) укажите путь к папке, созданной в шаге 2. Установите флажок Включить доступ к содержимому каталога с помощью подстановочных знаков (Enable Access To Directory Content Using Wildcards). В результате пользователи смогут вручную вводить имя видеофайла для получения прямого доступа на сервере. Щелкайте кнопку Далее (Next).
10. На странице Воспроизведение содержимого (Content Playback) оставьте опции по умолчанию и щелкните кнопку Далее (Next).
11. На странице Журнал одноадресного вещания (Unicast Logging) оставьте опцию по умолчанию и щелкните кнопку Далее (Next).
12. На странице Сведения о пункте публикации (Publishing Point Summary) проверьте выбранные параметры и щелкните кнопку Далее (Next).

13. На последней странице Мастера добавления пункта публикации (Add Publishing Point Wizard) оставьте опции по умолчанию и щелкните кнопку Готово (Finish).
14. После создания пункта публикации автоматически откроется Мастер одноадресных объявлений (Unicast Announcement Wizard). Щелкните кнопку Далее (Next).
15. На странице Каталог по запросу (On-Demand Directory) щелкните кнопку Обзор (Browse) и выберите файл serversideplaylist.wsx в папке, созданной в шаге 2. Щелкните кнопку Далее (Next).
16. На странице Доступ к содержимому (Access The Content) запомните URL, который можно использовать для доступа с содержимому. Вы примените этот URL для проверки объявления. Щелкните кнопку Далее (Next).
17. На странице Сохранить параметры объявления (Save Announcement Options) оставьте путь по умолчанию. Он указывает размещение объекта Default Web Site, установленного вместе с ролью Веб-сервер (IIS) (Web Server (IIS)). Кроме того, установите флажок для создания веб-страницы с параметрами по умолчанию. Щелкните кнопку Далее (Next).
18. На странице Изменение метаданных объявления (Edit Announcement Metadata) введите заголовок Contoso Training. Щелкните кнопку Далее (Next).
19. На последней странице Мастера одноадресных объявлений (Unicast Announcement Wizard) установите флажок Проверить файлы после закрытия мастера (Test Files When This Wizard Finishes) и щелкните кнопку Готово (Finish).
20. В диалоговом окне Проверочное одноадресное объявление (Test Unicast Announcement) щелкните первую кнопку Проверить (Test), чтобы непосредственно проверить объявление. Должен запуститься Проигрыватель Windows Media (Windows Media Player) и автоматически воспроизвести видеофайл из пункта публикации. После воспроизведения видео закройте проигрыватель Windows Media.
21. В диалоговом окне Проверочное одноадресное объявление (Test Unicast Announcement) щелкните вторую кнопку Проверить (Test). Затем закройте консоль Службы Windows Media (Windows Media Services).

Резюме

- Службы Windows Media (Windows Media Services) предназначены для обеспечения пользователям доступа к прямым потокам аудио- и видеовещания и потокам по запросу.
- Роль сервера Службы потокового мультимедиа (Streaming Media Services) включает административные инструменты MMC и Веб.
- При использовании многоадресной передачи потоков в сети можно снизить требования пропускной способности.
- На сервере Windows Media можно создать множество пунктов публикации для обеспечения доступа к различным типам содержимого.

- Прокси-серверы с кэшем могут повысить производительность и расширяемость серверов Windows Media.
- Безопасный доступ к пунктам публикации можно обеспечить с помощью параметров подключаемых модулей Авторизация (Authorization) и Проверка подлинности (Authentication).
- Технические средства защиты авторских прав DRM (Digital Rights Management) позволяют поставщикам и создателям содержимого защищать свою интеллектуальную собственность, контролируя использование мультимедиа.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных в ходе занятия 1. Эти вопросы представлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы

Ответы и пояснения к каждому их варианту размещены в разделе «Ответы» в конце книги.

1. Вы являетесь системным администратором Windows Server 2008 и отвечаете за настройку роли Службы потокового мультимедиа (Streaming Media Services). Ваша организация желает обеспечить для своих сотрудников доступ к многочисленным обучающим видеофайлам. Сотрудники должны иметь возможность приостанавливать и перематывать содержимое. Кроме того, пользователи должны получать доступ к содержимому, лишь подключаясь к локальной сети LAN компании. Какие действия следует предпринять? (Укажите два действия. Каждое действие является частью полного ответа.)

   А. Создать новый широковещательный пункт публикации.

   Б. Создать новый пункт публикации по запросу.

   В. Включить для пункта публикации модуль Проверка подлинности IP-адреса WMS (WMS IP Address Authorization).

   Г. Включить для пункта публикации модуль Проверка подлинности согласования WMS (WMS Negotiate Authentication).

   Д. Включить для пункта публикации модуль Проверка подлинности NTFS ACL WMS (WMC NTFS ACL Authorization).

2. Вы являетесь администратором сервера Windows Media и отвечаете за настройку роли Службы потокового мультимедиа (Streaming Media Services) для получения доступа в Интернет. В настоящее время в папке, используемой четырьмя пунктами публикации на сервере, содержится 200 больших видеофайлов. Вы хотите предоставить пользователям доступ лишь к 100 файлам с обучающим видео. Вы создали новый пункт публикации по запросу, использующий папку с видео в качестве своего корневого каталога. Вы также хотите свести к минимуму объем дискового пространства, используемого для хранения файлов на сервере. Пользователи должны получать доступ по за-

просу к любому обучающему видео из этих 100 файлов, не указывая свои учетные данные. Какое из следующих действий следует предпринять?

А. С помощью Мастера одноадресных объявлений (Unicast Announcement Wizard) создать страницу HTML, обеспечивающую доступ к содержимому.

Б. Включить для веб-сайта модуль Проверка подлинности NTFS ACL WMS (WMS NTFS ACL Authentication) и назначить соответствующие разрешения файловой системы.

В. Скопировать обучающее видео в еще одну папку и модифицировать корневой каталог пункта публикации.

Г. Отключить для пункта публикации модуль Проверка подлинности анонимного пользователя WMS (WMS Anonymous User Authentication).

Д. Создать новый список воспроизведения сопровождения (Wrapper Playlist), включающий только обучающее видео.

3. Вы являетесь системным администратором Windows Server 2008 и отвечаете за обеспечение доступа к большому количеству видеофайлов для зарегистрированных пользователей общественного веб-сайта организации. Все видеофайлы расположены в папке D:\Public\Videos. Разработчики содержимого часто создают и модифицируют видео в этой папке. Недавно пользователи стали жаловаться на низкую производительность при получении доступа к видео в рабочее время. В это время на сервере Windows Media, управляющем содержимым, интенсивно используют ресурсы процессора и пропускной способности сети. Вы хотите как можно быстрее решить проблему производительности. Какое из следующих действий следует предпринять для решения проблемы?

А. Скопировать обучающее видео еще в одну папку на сервере Windows Media.

Б. Установить на дополнительных серверах роль Службы потокового мультимедиа (Streaming Media Services) и отконфигурировать их как серверы кэширования.

В. Установить на дополнительных серверах роль Службы потокового мультимедиа (Streaming Media Services) и отконфигурировать их как прокси-серверы.

Г. В свойствах пункта публикации включить параметр Ограничить подключения исходящего распределения (Limit Outgoing Distribution Connections).

Закрепление материала главы

Для того чтобы попрактиковаться и закрепить знания, приобретенные в ходе изучения представленного в данной главе материала, вам необходимо:

- ознакомиться с резюме главы;
- повторить используемые в главе основные термины;
- выполнить задания лабораторной работы, которые моделируют реальные ситуации, требующие применения полученных знаний;
- выполнить рекомендуемые упражнения;
- сдать пробный экзамен с помощью тестов.

Резюме главы

- Службы потокового мультимедиа (Streaming Media Services) в Windows Server 2008 обеспечивают расширяемый метод доставки пользователям широковещательного содержимого аудио и видео, а также аудио и видео по запросу.
- Сервер Windows Media может управлять множеством пунктов публикации, обеспечивающим доступ к различным типам содержимого.
- Для повышения производительности сервера Windows Media можно отконфигурировать Серверы кэширования и прокси.

Основные термины

Проверьте, знаете ли вы, что означают перечисленные ниже термины (свои ответы можно сверить с определениями, содержащимися в конце книги):

- Службы управления правами Active Directory (AD RMS);
- Технические средства защиты авторских прав DRM;
- промежуточная реклама;
- пункты публикации;
- Real-Time Streaming Protocol (RTSP);
- Службы потокового мультимедиа (роль сервера);
- утилита Windows Media Load Simulator 9 Series;
- рекламные объявления сервера Windows Media;
- широковещание сервера Windows Media;
- кэш/прокси-сервер Windows Media;
- список воспроизведения сервера Windows Media;
- подключаемые модули сервера Windows Media;
- Службы Windows Media;
- Многоадресная передача сервера Windows Media;
- Одноадресная передача сервера Windows Media;
- Рекламные объявления сопровождения списков воспроизведения.

Лабораторная работа

В следующих заданиях вы примените знания, полученные в этой главе. Ответы находятся в разделе Ответы» в конце книги.

Задание 1. Защита содержимого потокового мультимедиа

Вы являетесь системным администратором и работаете в компании, предоставляющей услуги обучения в области IT. Недавно руководство компании решило обеспечить доступ к обучающим видеофайлам для зарегистрированных студентов определенного курса. Пользователи должны получать доступ лишь к обучающим видеофайлам, имеющим отношение к изучаемому ими материалу. Студенты располагают учетными записями Windows в домене Active Directory организации. Они должны иметь возможность в любое время получать доступ

ко всем видеофайлам и управлять воспроизведением. Перед воспроизведением целого видеофайла должен запускаться короткий вводный заголовок.

1. Какой тип пункта публикации следует создать для обеспечения доступа к мультимедиа?
2. Как ограничить доступ студентов лишь обучающими видеофайлами?
3. Какой самый простой метод можно применить для запуска вводных заголовков перед каждым видеофайлом?

Задание 2. Повышение производительности и расширяемости сервера Windows Media

Ваша организация обеспечивает доступ к потоковому аудио пользователям Интернета, оплатившим эту услугу. Вы отконфигурировали один компьютер Windows Server 2008 с ролью Потоковые службы мультимедиа (Streaming Media Services). Изначально этот сервер мог выполнять запросы пользователей. Однако недавно на сервере было зарегистрировано еще несколько тысяч пользователей, и некоторые из них жалуются на медленное воспроизведение и другие проблемы производительности в определенное время дня. Из соображений безопасности и управления вы хотите избежать перемещения или копирования аудио вручную с текущего сервера Windows Media. Ваша организация также планирует в следующем месяце транслировать музыкальный концерт и обеспечить как можно больше клиентских подключений.

1. Какой тип пункта публикации следует создать для трансляции музыкального события?
2. Как снизить требования пропускной способности, не включая дополнительные серверы Windows Media?
3. Как отконфигурировать дополнительные серверы Windows Media для повышения расширяемости?

Рекомендуемые упражнения

Чтобы успешно справиться с экзаменационными заданиями, выполните следующие упражнения.

Настройка служб Windows Media

Работая над упражнениями этого раздела, вы можете попрактиковаться в конфигурировании и управлении ролью Потоковые службы мультимедиа (Streaming Media Services) в Windows Server 2008, а также в создании новых пунктов публикации на сервере Windows Media.

- **Упражнение 1** Создайте пункт публикации по запросу и предоставьте доступ к списку воспроизведения, включающему множество аудио- и видеофайлов. Вы можете использовать образцы файлов мультимедиа, включенные в роль сервера Службы потокового мультимедиа (Streaming Media Services).

  Отконфигурируйте один из видеофайлов для автоматического воспроизведения, создав рекламное объявление сопровождения перед передачей содержимого пользователям.

С помощью веб-браузера запустите воспроизведение содержимого, чтобы проверить его доступность. Если в вашем распоряжении имеется несколько компьютеров, попытайтесь одновременно получить на них доступ к видео, чтобы проверить работу множества одновременных подключений.

  - Откройте вкладку Монитор (Monitor) и просмотрите статистику воспроизведения содержимого.

- **Упражнение 2** Установите роль сервера Службы потокового мультимедиа (Streaming Media Services) на двух компьютерах Windows Server 2008. Отконфигурируйте на одном из серверов пункт публикации по запросу.
  Используйте утилиту Windows Media Load Simulator для тестирования производительности и расширяемости сервера Windows Media. Попытайтесь имитировать большое количество подключений и просмотрите статистику доступа на вкладке Монитор (Monitor) свойств пункта публикации.
  Для пункта публикации, созданного на первом сервере Windows Media, отконфигурируйте второй сервер Windows Media как кэш/прокси-сервер.
  Повторите тесты Windows Media Load Simulator для проверки производительности и выясните, с какого сервера выполняется потоковая передача содержимого.

  При желании отконфигурируйте ограничения в свойства пункта публикации и проверьте результаты тестов Windows Media Load Simulator.

Пробный экзамен

На прилагаемом к книге компакт-диске представлено несколько вариантов тренировочных тестов. Проверка знаний выполняется только по одной или же по всем экзаменационным темам сертификационного экзамена 70-643. Тестирование можно организовать таким образом, чтобы оно проводилось как экзамен, или же настроить его на изучение — в этом случае вы сможете после каждого своего ответа на вопрос просматривать правильные ответы и объяснения.

ПРИМЕЧАНИЕ Пробный экзамен

Подробнее о пробном экзамене рассказано во введении к данной книге.

ГЛАВА 9

Настройка служб Windows SharePoint Services

Занятие 1. Настройка служб Windows SharePoint Services и управление ими 462

Операционная система сервера может содействовать выполнению задач пользователей посредством поддержки совместной работы. Службы Microsoft Windows SharePoint Services (WSS) предназначены для обеспечения пользователей технологией совместного сотрудничества, модификации и обсуждения различных типов содержимого. Они предоставляют возможности централизованного создания распространенных типов информации, включая объявления, задачи и напоминания. Разработчики приложений также могут использовать WSS в качестве платформы для собственных веб-приложений. Операционная система Windows Server 2008 поддерживает Windows SharePoint Services в качестве роли сервера, которую можно быстро развернуть в производственной среде. В этой главе мы обсудим настройку WSS, включая установку новых сайтов SharePoint, управление ими и управление операциями сервера SharePoint.

Темы экзамена:

- Настройка опций сервера Microsoft Windows SharePoint Services.
- Настройка интеграции электронной почты Windows SharePoint Services.

Требования

Для выполнения упражнений этой главы вам потребуется следующее.

- Роль Веб-сервер (IIS) (Web Server (IIS)), добавленная на сервер Server2.contoso.com с опциями по умолчанию. Более подробные сведения об установке этой роли содержатся в главе 5.

Занятие 1. Настройка служб Windows SharePoint Services и управление ими

Основное назначение WSS стоит в обеспечении среды для совместной работы пользователей с общими данными и документами. Организации могут исполь-

зовать WSS как основу веб-сайта интрасети компании или совместной работы с информацией. Пользовательский веб-интерфейс обеспечивает доступ в организации с помощью веб-браузеров. Многие приложения, такие как пакет Microsoft Office, обеспечивают интеграцию с WSS для редактирования документов управления. Платформу WSS могут также использовать разработчики для создания собственных веб-приложений в соответствии с конкретными бйзнес-требованиями.

Поскольку платформа WSS позволяет использовать множество различных сценариев, после ее установки важно отконфигурировать многочисленные опции и параметры. Установив роль Windows SharePoint Services с помощью веб-приложения центра администрирования SharePoint (SharePoint Central Administration Web-site), можно внести несколько изменений в конфигурацию.

На этом занятии вы изучите опции и возможности WSS, а также принципы их применения.

К СВЕДЕНИЮ Установка Windows SharePoint Services

Во время написания этой книги корпорация Microsoft продолжала работу над Windows SharePoint Services 3.0 для Windows Server 2008. По умолчанию роль WSS не включена в Windows Server 2008. Ее нужно загрузить и установить отдельно. Многие разделы главы написаны в соответствии с поведением текущей версии WSS 3.0. Однако в финальный выпуск операционной системы могут вноситься изменения. При подготовке к сертификационному экзамену 70-643 следует помнить, что темы экзамена посвящены настройке WSS на основе требований, а не на основе инсталляции продукта. Более подробные сведения о загрузке и установке Windows SharePoint Services на компьютер Windows Server 2008 можно найти на странице Windows SharePoint Services TechCenter сайта Microsoft Technet по адресу *http://tecImet.microsoft.com/en-us/windowsserver/sharepoint/default.aspx.*

Изучив материал этого занятия, вы сможете:

- Описать назначение Windows SharePoint Services.
- Понять различие между автономным развертыванием и развертыванием WSS на ферме серверов.
- Выполнять задачи конфигурирования WSS с помощью веб-приложения Центр администрирования SharePoint (SharePoint Central Administration Web-site).
- Управлять параметрами операций WSS, связанными с безопасностью, электронной почтой и ведением журнала.
- Выполнять операции резервного копирования и восстановления для сайтов SharePoint.
- Развертывать и конфигурировать новые сайты SharePoint.
- Управлять параметрами веб-приложений для сайтов SharePoint.

Расчетная продолжительность занятия составляет 60 мин.

Службы Windows SharePoint Services

В Windows Server 2008 включена поддержка версии Службы Windows SharePoint Services (WSS) 3.0. Пользователи взаимодействуют с WSS с помощью веб-сайтов, управление которыми осуществляется через Internet Information Services (IIS). Хотя настройкой исходной конфигурации сервера обычно занимаются IT-профессионалы, опытные пользователи вполне могут поддерживать содержимое и информацию на сайтах WSS. Например, отдел или группа в организации может создать собственный сайт портала или рабочее пространство для осуществления коммуникаций с другими отделами и группами, управляя следующими функциями и типами информации:

- объявления;
- общие документы;

  календари:

  задачи;

  коллективное обсуждение;

  ссылки;

  контактные данные.

  На рис. 9-1 показан пользовательский интерфейс WSS.

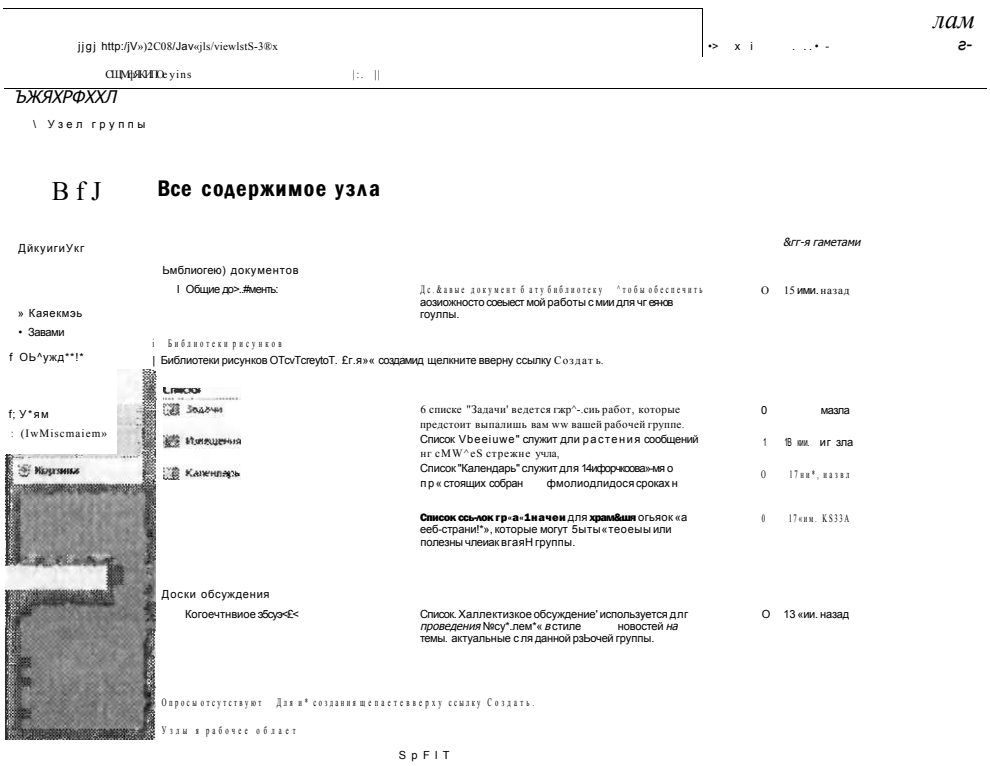


Рис. 9-1. Получение доступа к сайту Windows SharePoint Services с помощью веб-браузера

Пользователи могут непосредственно управлять всей этой информацией и обеспечивать ее защиту путем применения разрешения безопасности. Для получения уведомлений об изменениях содержимого, а также для обмена данными с WSS можно использовать электронную почту. Возможности оповещения о присутствии также могут содействовать совместному сотрудничеству распределенных команд с использованием программ мгновенного обмена сообщениями и других приложений. В WSS также обеспечены возможности расширяемости, позволяющие разработчикам приложений проектировать новую функциональность. В целом эти возможности позволяют группам и подразделениям совместно сотрудничать и использовать общую информацию.

ПРИМЕЧАНИЕ Другие продукты SharePoint Services
Версию Службы Windows SharePoint Services 3.0 можно также бесплатно загрузить для платформы Windows Server 2003 SP1. Кроме того, корпорация Microsoft предлагает полнофункциональный продукт Microsoft Office SharePoint Server 2007. Сервер SharePoint Server 2007 обеспечивает дополнительные возможности, в частности поддержку пользовательских профилей, сквозную проверку подлинности, личные сайты и много других функций. Более подробные сведения об этих технологиях можно найти по адресу *http://www.microsoft.com/sharepoint/default.mspx*.

Опции развертывания WSS

Платформа WSS поддерживает разнообразные сценарии. Для системного администратора важно обеспечить баланс между легкостью в развертывании и такими возможностями, как расширяемость. Для соответствия различным требованиям в WSS включены две опции развертывания: автономная конфигурация и конфигурация фермы серверов. Нужную опцию можно выбрать при добавлении роли Службы Windows SharePoint Services. В этом разделе мы обсудим различные способы развертывания SharePoint.

Развертывание WSS в автономной конфигурации

Самый простой метод установки и запуска WSS состоит в использовании конфигурации одного сервера. При выборе автономной конфигурации WSS использует один сервер, который управляет всеми необходимыми компонентами и службами на локальном компьютере.

06i4Ho взаимодействие с WSS осуществляется через веб-браузер. Для управления основным пользовательским сайтом WSS и веб-сайтом SharePoint Central Administration нужно установить IIS. Для работы архитектуры WSS на компьютер также требуется установить компонент .NET Framework 3.0. Для хранения данных в автономной конфигурации используется Внутренняя база данных Windows (Windows Internal Database). В этой базе данных хранятся данные операционной системы, включая содержимое WSS. Сама база данных основана на технологии Microsoft SQL Server.

Запустив все эти службы на одном компьютере, вы сможете очень быстро выполнить установку и развертывание. Помимо ролей сервера и компонентов, которые добавляются автоматически, отсутствуют дополнительные системные

требования или этапы настройки системы. Дополнительная установка выполняется с помощью веб-сайта SharePoint Central Administration.

Основной недостаток автономной конфигурации состоит в том, что она не поддерживает множество серверов для расширения в больших средах.

Развертывание WSS в конфигурации фермы серверов

Во многих организациях возможности совместного сотрудничества являются важным элементом инфраструктуры. Поскольку WSS обеспечивает много полезных компонентов, расширяемость играет важную роль. Архитектура WSS позволяет системным администраторам отделять функциональность клиентской части системы (веб-сайты пользователей и администрации) от серверного хранилища данных (база данных WSS). Эта опция развертывания называется *конфигурацией фермы серверов*.

В ферме серверов множество серверов клиентской части системы WSS могут подключаться к серверу базы данных, который управляет копиями всех документов, параметров и связанных данных. Такая инфраструктура позволяет организациям повысить производительность и обеспечить возможности доступа в самых различных сценариях. Например, она позволяет создать сценарий экстрасети для сторонних пользователей и организаций (таких как бизнес-партнеры и консультанты). Кроме того, удаленные офисы могут использовать собственные серверы WSS для повышения производительности и обеспечения возможностей доступа.

Основные системные требования аналогичны требованиям автономной конфигурации служб Windows SharePoint Services за исключением базы данных Windows Internal Database.

Для развертывания в конфигурации фермы серверов на компьютере с версией Microsoft SQL Server 2000 или SQL Server 2005 уже должна существовать база данных SharePoint. Хотя в ходе этого процесса выполняются дополнительные шаги, с его помощью администраторы организации могут установить базы данных и использовать для управления ими существующий экземпляр SQL Server.

В процессе стандартной установки на компьютере SQL Server вначале нужно установить и отконфигурировать требуемые базы данных. В зависимости от требований безопасности и производительности SQL Server можно установить и отконфигурировать на одном из компьютеров с запущенными службами WSS. На следующем шаге установки роль Службы Windows SharePoint Services добавляется на все клиентские серверы. Хотя дополнительные серверы можно добавить позже, лучше всего добавить эту роль на все серверы, входящие в исходную конфигурацию развертывания. Веб-сайт SharePoint Central Administration будет установлен и отконфигурирован на первом сервере, который входит в ферму серверов.

В целом развертывание фермы серверов обеспечивает расширенную конфигурацию WSS, и для его осуществления требуется дополнительное планирование и координация.

СОВЕТ Подготовка к экзамену

При подготовке к сертификационному экзамену 70-643 важно понимать технические отличия между автономным развертыванием и конфигурацией фермы серверов служб Windows SharePoint Services. Конфигурация фермы серверов включает дополнительные зависимости и такие требования, как доступ к SQL Server. Если вы не знакомы с принципами использования SQL Server, займитесь установкой и конфигурированием автономного развертывания WSS. Все остальные этапы конфигурирования, за исключением исходной установки, аналогичны.

В целом развертывание фермы серверов обеспечивает расширенную конфигурацию WSS, и для его осуществления требуется дополнительное планирование и координация.

Мастер настройки продуктов и технологии SharePoint

После добавления основных ролей клиентской стороны сервера WSS администраторы могут использовать Мастер настройки продуктов и технологии SharePoint (SharePoint Products And Technologies Configuration Wizard) для дальнейшей настройки опций сервера. В процессе конфигурировании выполняется установка базы данных WSS и веб-серверов (рис. 9-2). Этот мастер можно также использовать для отмены установки WSS в случае недоступности сайта или возникновения ошибок. При работе с конфигурацией фермы серверов потребуется указать размещение и учетные данные для сервера базы данных, который будет использоваться в ферме.

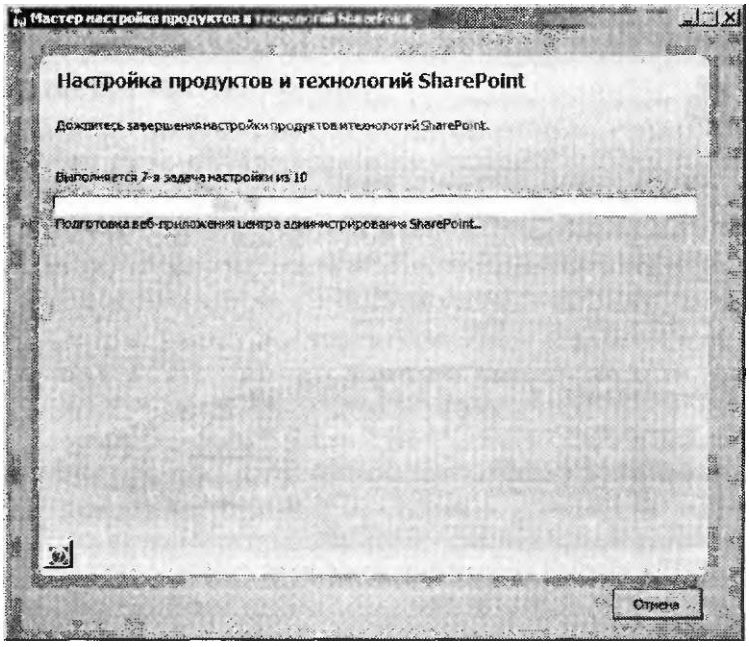


Рис. 9-2. Окно мастера настройки продуктов и технологии SharePoint

ПРИМЕЧАНИЕ

Хотя WSS можно установить и использовать в Windows Server 2008, согласно условиям лицензирования в этой операционной системе можно создавать только общественные интернет-сайты. Поэтому вы не можете использовать веб-выпуск для создания порталов или сайтов в средах интра/экстрасетей. Кроме того, вы не можете развернуть автономную конфигурацию WSS с помощью этого выпуска. Более подробные сведения о выпусках можно найти на веб-сайте Microsoft Windows Server 2008 по адресу *http://www.microsoft.com/windows-setver2008/default.mspx.*

Проверка установки WSS

После завершения установки роли Службы Windows SharePoint Services (WSS) параметры можно проверить с помощью Диспетчера сервера (Server Manager) и Windows Internet Explorer. На этом занятии вы узнаете, как гарантировать доступ к сайту.

Проверка ролей и параметров сервера

Для получения общей картины конфигурации роли сервера Windows SharePoint Services откройте Диспетчер сервера (Server Manager), разверните объект Роли (Roles), щелкните (Windows SharePoint Services), и вы сможете просмотреть информацию о состоянии WSS (рис. 9-3).

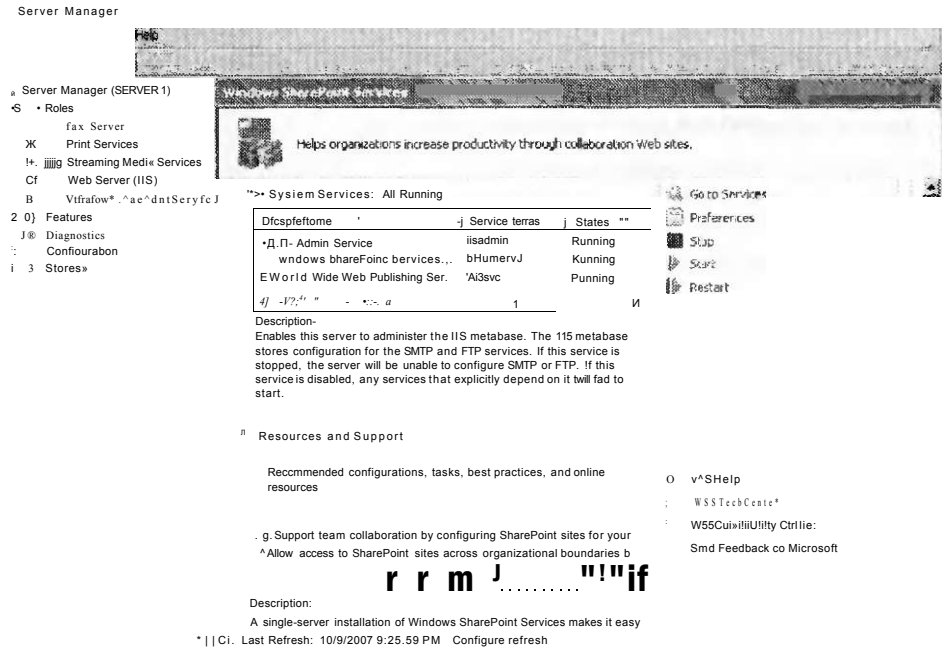


Рис. 9-3. Использование диспетчера сервера для просмотра информации о роли Windows SharePoint Services

В разделе События (Events) указаны сведения журнала событий, связанные с WSS. Периодически просматривайте эту информацию для определения ошибок конфигурации, которые требуют вашего внимания.

В разделе Системные службы (System Services) указаны основные системные службы, связанные с WSS. В случае автономной установки па один сервер вы увидите несколько служб, описанных в табл. 9-1. При желании вы можете запускать и останавливать отдельные службы.

Табл. 9-1. Системные службы WSS

Отображаемое имя	Имя службы	Описание
Служба [IS Admin (IIS Admin Service)	iisadmin	Используется для хранения данных конфигурации, связанных с параметрами SMTP и FTP, и управления этими данными
Служба Windows SharePoint Services Timer	SPTimerv3	Используется для выполнения запланированных задач и отправки уведомлений, откоифигурированных на (SharePoint Central Administration Web site). Если служба остановлена, работа с запланированными задачами н сообщениями выполняться не будет
Служба веб-публикашш (World Wide Web Publishing Service)	W3SVC	HTTP-сервер IIS, позволяющий веб-сайвм SharePoint принимать подключения и обрабатывать запросы. Если остановить эту службу, пользователи и администраторы не смогут подключаться к WSS с помощью веб-браузера

В разделе Ресурсы и поддержка (Resources And Support) диспетчера сервера предоставлены дополнительные сведения о параметрах конфигурации WSS.

Проверка веб-сайтов WSS

Как уже говорилось ранее в этой главе, при добавлении роли Windows SharePoint Services на компьютер в процессе установки создается два новых веб-сайта.

- **SharePoint-80** Основной веб-сайт, к которому пользователи WSS будут получать доступ с помощью веб-браузеров (рис. 9-4). По умолчанию он отвечает на запросы порта 80. После создания сайта пользователи могут получать доступ к WSS с помощью адреса *1шр://Имя_сервера.*
- **Центр администрирования SharePoint v3 (SharePoint Central Administration v3)** Этот веб-сайт позволяет администраторам SharePoint конфигурировать опции WSS, например параметры электронной почты, пользовательские разрешения и параметры отдельных сайтов SharePoint.

Отметим, что в процессе установки роли сервера будут автоматически остановлены все другие сайты IIS, откоифигурированные для использования порта 80 на локальном сервере. Это необходимо по причине того, что ITS не позволяет одновременно запускать множество сайтов на одном ИТТР-порте без использования уникальных заголовков узла. Если локальный сервер управляет еще одним веб-сайтом или веб-приложением, может потребоваться изменить их параметры портов, чтобы пользователи могли получать доступ. Более подробные сведения о настройке 1IS содержатся в главе 5.

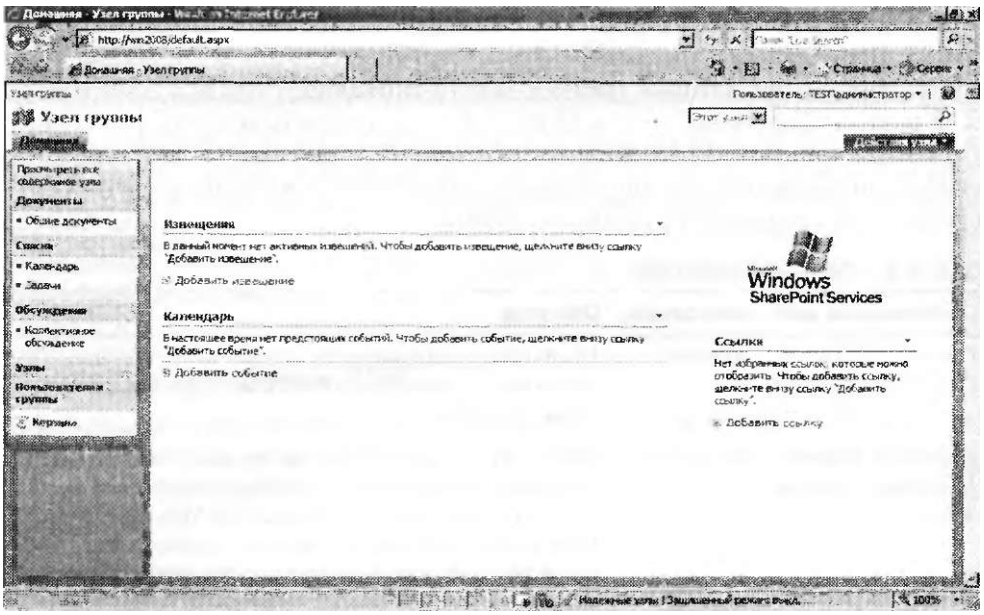


Рис. 9-4. Веб-сайт SharePoint

Проверьте себя

1. Какие существуют зависимости ролей и компонентов в установке автономной конфигурации (один сервер) служб Windows SharePoint Services?
2. Опишите преимущества установки служб Windows SharePoint Services в конфигурации фермы серверов.

Ответы

1. Для роли WSS требуются компоненты .NET Framework 3.0, роль Веб-сервер (IIS), компонент Служба активации Windows (Windows Process Activation Service) и компонент Внутренняя база данных Windows (Windows Internal Database).
2. Конфигурация фермы серверов позволяет множеству веб-серверов WSS подключаться к серверам баз данных. Таким образом обеспечиваются возможности расширяемости для крупномасштабных развертываний или поддержки сценариев с использованием экстрасетей.

Центр администрирования SharePoint

Основным инструментом системного администрирования WSS является веб-сайт Центр администрирования SharePoint (SharePoint Central Administration). Если роль сервера Windows SharePoint Services была добавлена с опциями по умолчанию, доступ к этому сайту можно получить, открыв браузер и набрав адрес *Иир://Имя_сервера:11омер порта.* В сайт включены разделы для управ-

ления конфигурацией сервера и выполнения важных задач, таких как создание новых сайтов для пользователей.

Выполнение административных задач

При первом подключении к сайту открывается список административных задач. По умолчанию расположение элементов в списке зависит от приоритета каждой задачи. В списке представлены следующие задачи:

- Первоочередные сведения — щелкните эту ссылку для получения инструкций по развертыванию (READ FIRST — Click this link for deployment instructions);
- Параметры входящей электронной почты (Incoming e-mail settings);
- Параметры исходящей электронной почты (Outgoing e-mail settings);
- Создание узлов SharePoint (Create SharePoint sites);
- Настройка параметров рабочих процессов (Configure workflow settings);
- Учетная запись для пула приложений центра администрирования должна быть уникальной (Central Administration application pool account should be unique);
- Параметры сбора данных диагностики (Diagnostic logging settings);
- Добавление защиты от вирусов (Add antivirus protection).

Перед тем как разрешить пользователям подключаться к веб-сайту SharePoint, рекомендуется выполнить эти задачи. Для просмотра сведений о каждой задаче щелкните ссылку. Вы увидите дополнительные сведения, связанные с опциями конфигурации (рис. 9-5).

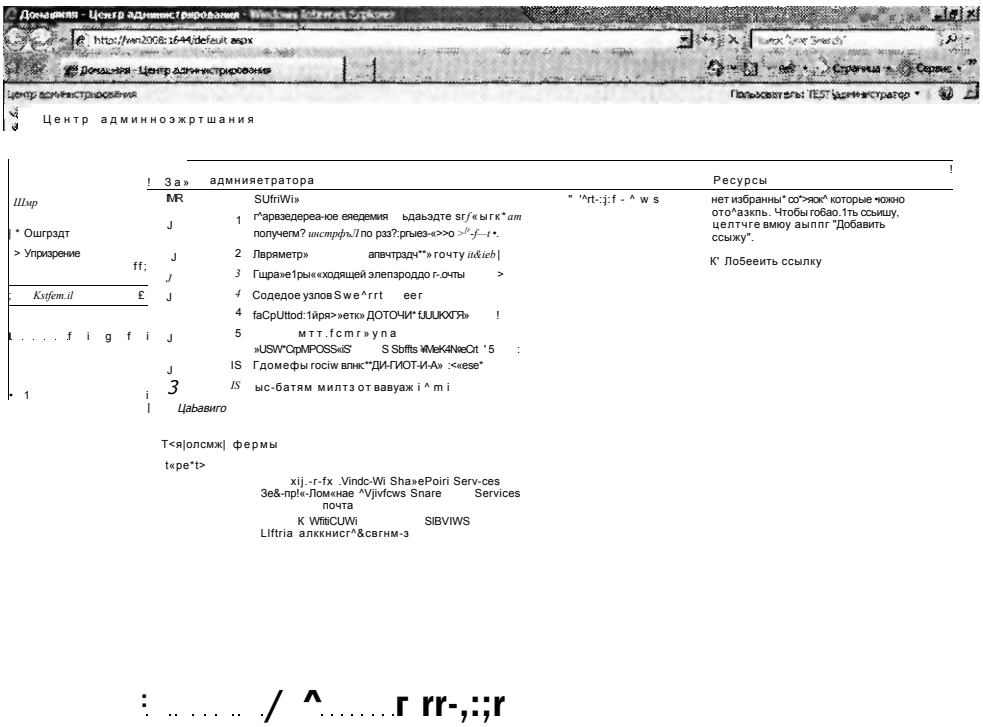


Рис. 9-5. Просмотр сведений об административной задаче на веб-сайте центра администрирования SharePoint

Выполненную задачу можно удалить, чтобы она не отображалась в списке. Отметим, что в разделе Действия (Actions) для некоторых элементов представлены прямые ссылки на соответствующие страницы конфигурации. Эти страницы также можно открывать вручную.

Навигация на веб-сайте центра администрирования SharePoint

Хотя в списке Задачи администратора (Administrator Tasks) представлены самые распространенные операции, выполняемые в процессе развертывания, веб-сайт Центр администрирования SharePoint (SharePoint Central Administration) содержит много дополнительных опций. Веб-сайт разбит на две основные области. Одна из них — вкладка Операции (Operations), где представлены ссылки и задачи, связанные с конфигурированием и управлением WSS, как показано на рис. 9-6.

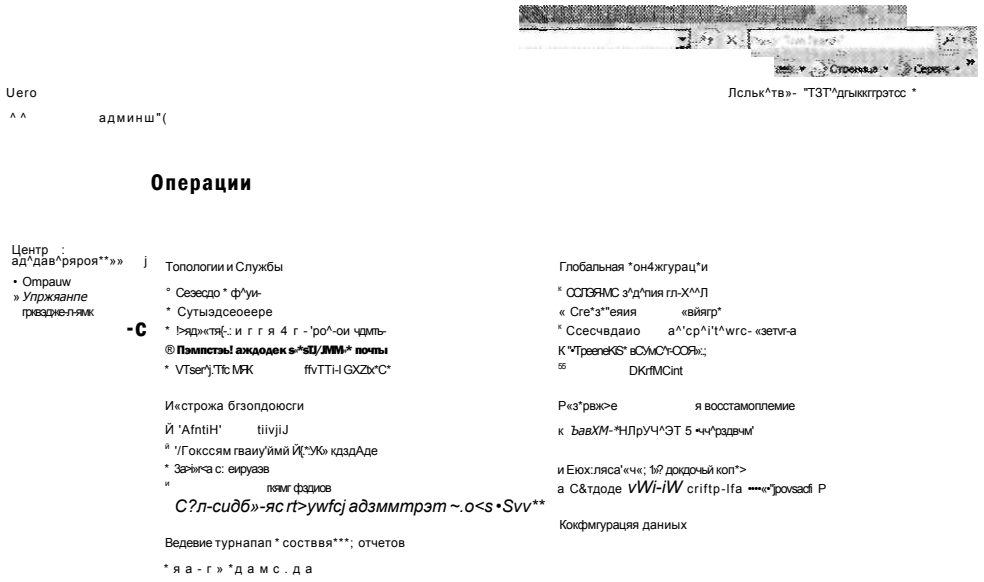


Рис. 9-6. Операции в центре администрирования SharePoint

Далее описаны разделы вкладки Операции (Operations).

- **Топология и службы (Topology and Services)** Определяет конфигурацию фермы серверов и управляет параметрами электронной почты.
- **Настройка безопасности (Security Configuration)** Управляет учетными записями служб, параметрами антивирусной защиты и другими параметрами безопасности.
- **Ведение журналов и составление отчетов (Logging and Reporting)** Позволяет администраторам включать ведение журналов для устранения неполадок и наблюдения за статистикой использования сайтов.

- **Глобальная конфигурация (Global Configuration)** Параметры, связанные с запланированными заданиями, управляющими решениями и сопоставлениями веб-сайтов для узла WSS.
- **Резервное копирование и восстановление (Backup and Restore)** Обеспечивает возможности создания резервных копий, восстановления из резервных копий и наблюдения за состоянием заданий резервного копирования.
- **Конфигурация данных (Data Configuration)** Позволяет администраторам указывать сведения подключения для сервера баз данных, который будет использоваться службами WSS.

Второй областью веб-сайта Центр администрирования SharePoint (SharePoint Central Administration) является вкладка Управление приложениями (Application Management), показанная на рис. 9-7.

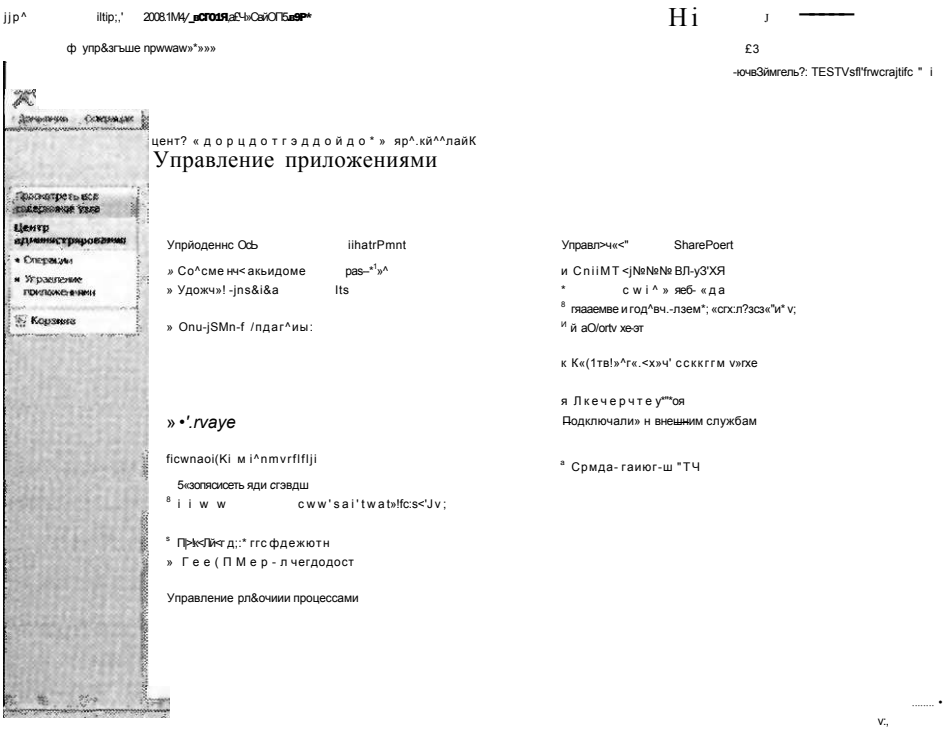


Рис. 9-7. Управление приложениями в центре администрирования SharePoint

Эти параметры, описанные далее, связаны с созданием веб-приложений SharePoint и управлением ими.

- **Управление приложениями SharePoint (SharePoint Web Application Management)** Параметры для создания новых веб-приложений и конфигурирования параметров других приложений.
- **Безопасность приложений (Application Security)** Параметры для конфигурирования параметров безопасности, включая разрешения и методы проверки подлинности для веб-приложения.

- **Управление рабочими процессами (Workflow Management)** Опции для конфигурирования параметров рабочих процессов.
- **Управление узлами SharePoint (SharePoint Site Management)** Задачи, связанные с созданием и удалением коллекций сайтов SharePoint, а также управлением ими.
- **Подключения к внешним службам (External Service Connections)** Опции Средства просмотра HTML (HTML Viewer), Преобразования документов (Document Conversions) и Центра записей (Records Center).

Хотя некоторые из этих опций могут показаться аналогичными опциям на вкладке Операции (Operations), важно отметить, что задачи, представленные на вкладке Управление приложениями (Application Management), связаны с конкретными сайтами WSS и не относятся к конфигурации на уровне сервера WSS. Многие из этих параметров мы рассмотрим более подробно на протяжении данного занятия.

СОВЕТ Подготовка к экзамену

Хороший способ изучения опций конфигурации, доступных на веб-сайте Центр администрирования SharePoint (SharePoint Central Administration), состоит в использовании каждой ссылки. Во многих разделах представлены описания и дополнительные сведения, которые могут помочь определить нужные опции для вашего развертывания. Ознакомившись с каждым параметром, вы сможете лучше подготовиться к сертификационному экзамену 70-643.

Управление операциями SharePoint

После установки и запуска WSS пользователи могут сами выполнять множество задач, связанных с содержимым. Перед тем как разрешить пользователям получать доступ к сайту, вам следует просмотреть и при необходимости изменить некоторые административные параметры. На этом занятии вы изучите основные функции и параметры, связанные с управлением сервером WSS.

Управление параметрами безопасности

Важный аспект безопасности состоит в обеспечении гарантии запуска приложений и служб с минимальным набором разрешений согласно техническим и бизнес-требованиям. При добавлении на компьютер роли сервера Windows SharePoint Services на локальный сервер добавляются несколько служб. Каждая служба использует учетную запись по умолчанию. Параметры по умолчанию для автономной конфигурации описаны в табл. 9-2.

Табл. 9-2. Параметры учетных записей по умолчанию для служб Windows SharePoint Services

Имя службы	Учетная запись по умолчанию	Тип запуска
Windows SharePoint Services Administration	Локальная система (Local System)	Вручную
Windows SharePoint Services Search	Local Service	Вручную
Windows SharePoint Services Timer	Network Service	Авто

Имя службы	Учетная запись по умолчанию	Тип запуска
Windows SharePoint Services Tracing	Local Service	Авто
Windows SharePoint Services VSS Writer	Локальная система (Local System)	Вручную

Параметры учетной записи службы можно изменить в консоли Службы (Services), однако рекомендуется конфигурировать параметры на веб-сайте Центр администрирования SharePoint (SharePoint Central Administration). На рис. 9-8 показана задача Учетные записи служб (Service Accounts).

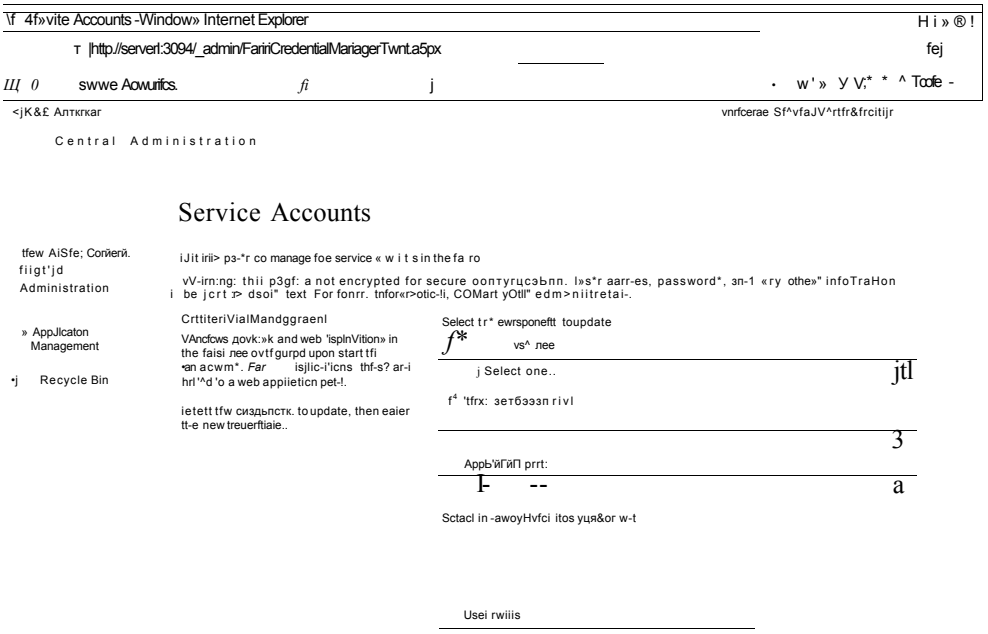


Рис. 9-8. Параметры управления учетными записями в центре администрирования SharePoint

По умолчанию каждый сайт SharePoint отконфигурирован в собственном пуле приложений. (Более подробные сведения о пулах приложений IIS содержатся в главе 5.) Параметры безопасности каждого сайта можно изменить, назначив встроенную учетную запись (например, Network Service или Local Service) или указав пользовательское имя и пароль.

В некоторых случаях могут потребоваться конкретные локальные или доменные учетные записи, скажем, если сайт должен получать доступ к другим серверам в среде.

Одной из потенциальных угроз, связанных с совместной работой в сетевых средах, является возможность выгрузки на сервер нежелательных или инфицированных вирусами файлов. Хотя WSS не содержит встроенную антивирусную программу, для автоматического сканирования передаваемых данных можно использовать стороннее антивирусное приложение.

Кроме того, уровень безопасности можно повысить с помощью опции Заблокированные типы файлов (Blocked File Types), как показано на рис. 9-9.

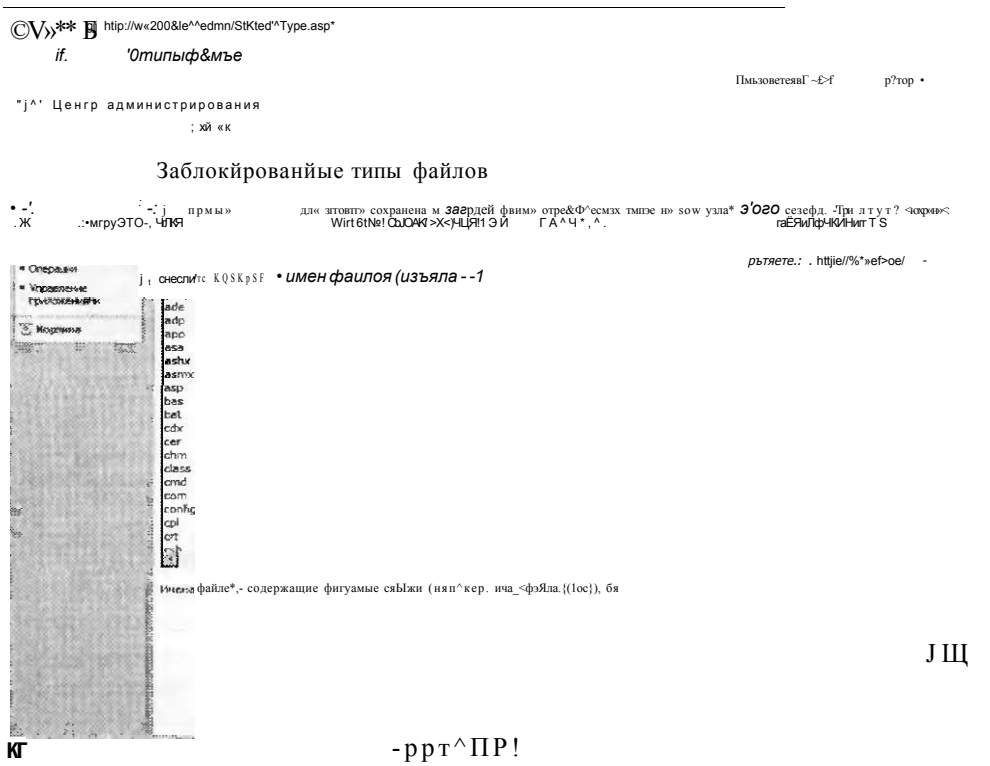


РИС. 9-9. Заблокированные типы файлов в центре администрирования SharePoint

Эти ограничения гарантируют выгрузку лишь файлов определенных типов. Например, многие распространенные форматы сценариев (такие как VBScript) блокируются по умолчанию. Хотя пользователи могут менять расширения файлов, эти параметры не позволяют загружать и автоматически выполнять файлы таких типов.

Настройка параметров электронной почты

Для передачи и получения сообщений службы WSS используют протокол электронной почты SMTP. Хотя вы можете указать сервер электронной почты и адресные данные в процессе установки роли сервера Windows SharePoint Services, это делать не обязательно. Вам также может потребоваться изменить

параметры после установки WSS в соответствии с изменениями в сетевом окружении. Ссылка Параметры исходящей электронной почты (Outgoing E-Mail Settings) на вкладке Операции (Operations) позволяет добавлять и изменять эти сведения, как показано на рис. 9-10.

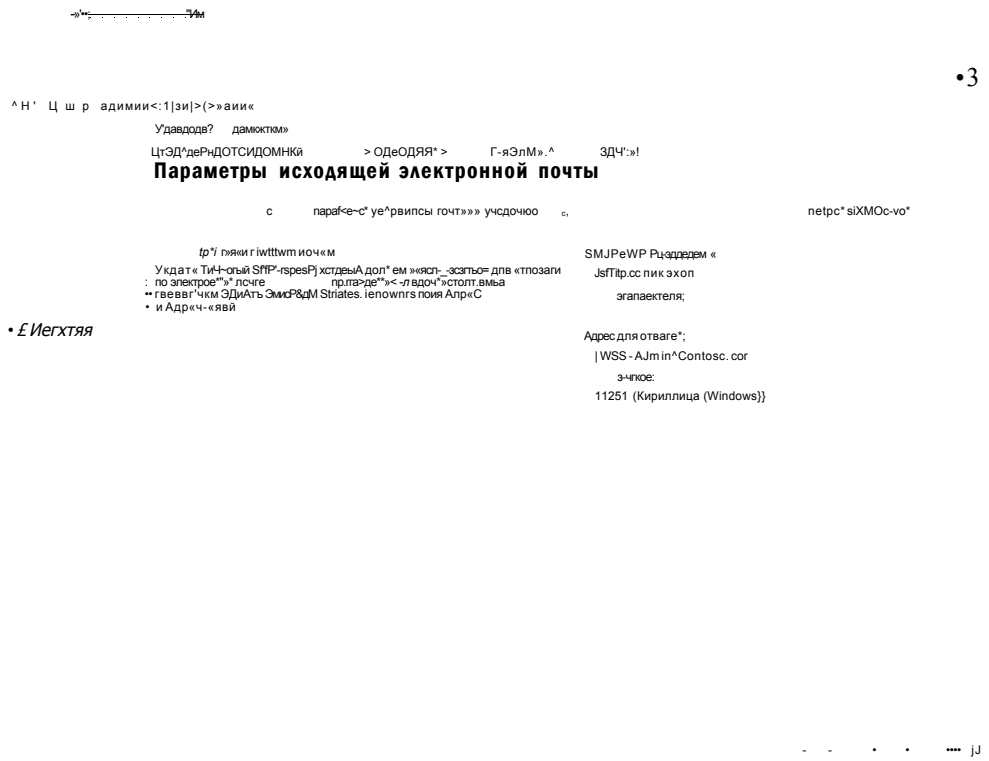


Рис. 9-10. Параметры исходящей электронной почты для WSS

Помимо отправки электронной почты WSS позволяет получать электронные сообщения от пользователей. По умолчанию эта функция отключена. Чтобы включить ее, щелкните ссылку Параметры входящей электронной почты (Incoming E-Mail Settings). На рис. 9-11 показаны доступные опции.

После включения входящей электронной почты для сервера WSS для приема входящих сообщений можно отконфигурировать библиотеки документов. Для этого откройте сайт SharePoint, а затем откройте библиотеку документов Общие документы (Shared Documents). В меню Параметры (Settings) выберите опцию Библиотека документов: параметры (Document Library Settings) и в разделе Обмен информацией (Communications) щелкните ссылку Параметры входящей электронной почты (Incoming E-Mail Settings). На странице Параметры входящей электронной почты: Общие документы (Incoming E-Mail Settings: Shared Documents) представлены параметры включения электронной почты и обработки вложений, как показано на рис. 9-12.

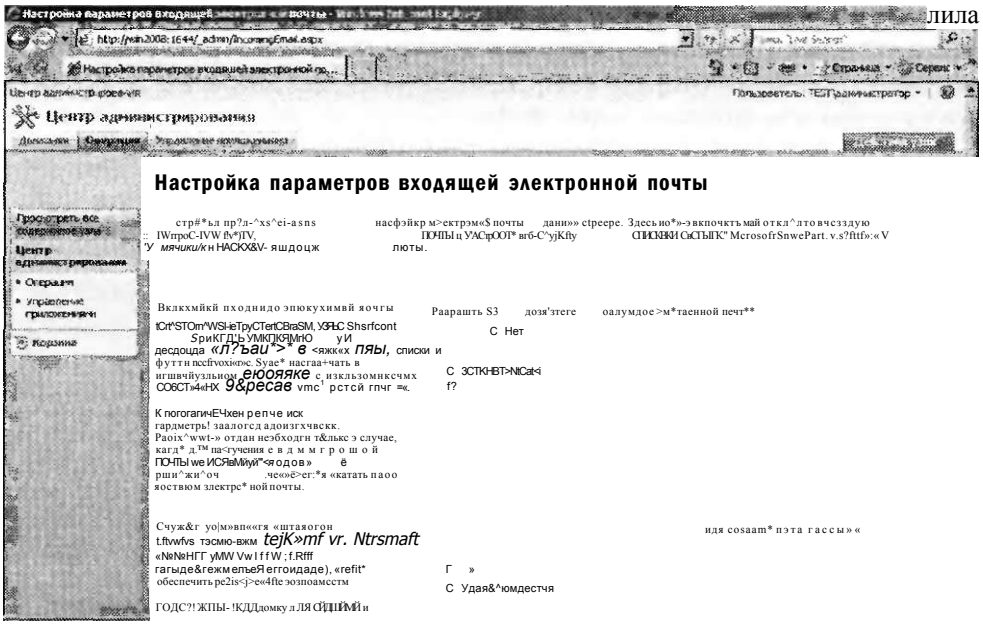


Рис. 9-11. Параметры входящей электронной почты для WSS

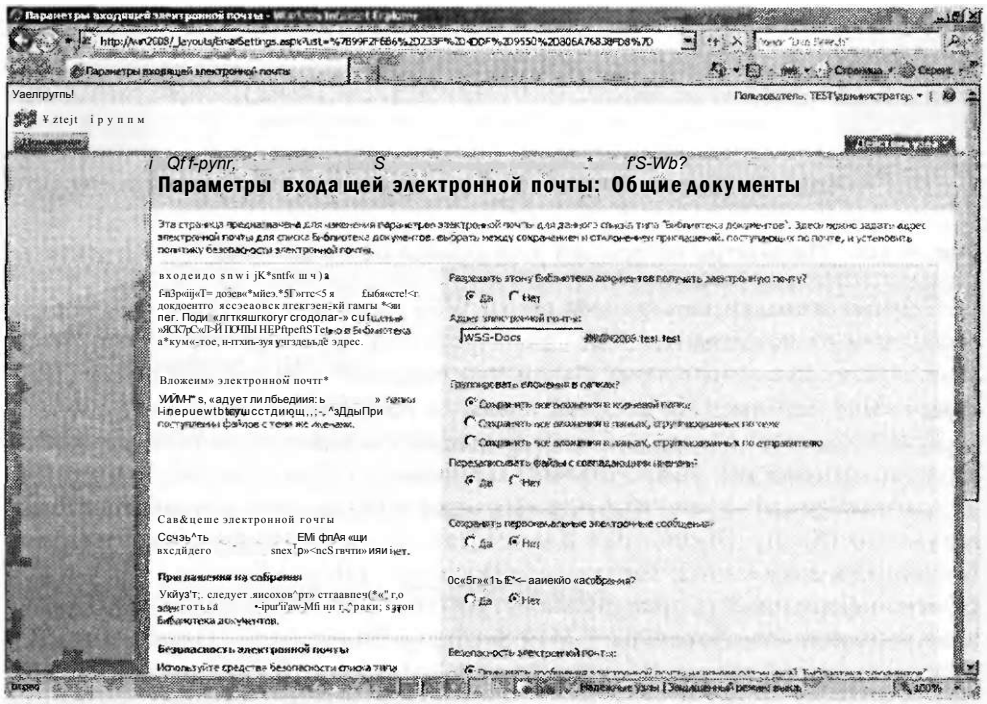


Рис. 9-12. **Параметры входящей электронной почты для библиотеки Общие документы (Shared Documents)**

Управление параметрами ведения журнала

Системные администраторы должны обеспечивать для WSS преимущества встроенной функциональности ведения журнала и составления отчетов. На странице Сбор данных диагностики (Diagnostic Logging), показанной на рис. 9-13, представлены опции для управления записью событий. По умолчанию сбор отчетов об ошибках включен. Эти отчеты создаются автоматически в случае возникновения ошибок WSS. В качестве примеров таких ошибок можно привести сбои оборудования, отсутствие критически важных файлов или неполадки конфигурации программного обеспечения.

Поскольку перегруженные сайты SharePoint могут генерировать большое количество событий, в разделе Регулирование событий (Event Throttling) можно указать типы записываемой информации.

В раскрывающемся списке категорий представлено много типов событий, за которыми можно вести наблюдение, начиная с сообщений, связанных с базой данных, и заканчивая сведениями об элементах управления Веб. Параметры можно изменить для одной или всех категорий. Сведения об ошибках можно записывать в журнал событий Windows (который можно открыть в приложении Просмотр событий (Event Viewer) или в Диспетчере сервера (Server Manager)) или хранить в файлах журнала трассировки.

Рис. 9-13. **Управление параметрами сбора данных диагностики в центре администрирования SharePoint**

Раскрывающийся список Событие наименьшей важности для занесения в журнал событий (Least Critical Event To Report To The Event Log) содержит следующие опции:

- Нет (None);
- Ошибка (Error);
- Предупреждение (Warning);
- Не удалось выполнить аудит (Audit Failure);
- Успешное выполнение аудита (Audit Success);
- Сведения (Information).

Раскрывающийся список Событие наименьшей важности для занесения в журнал отслеживания (Least Critical Event To Report To The Trace Log) содержит такие опции:

- Нет (None);
- Непредвиденный (Unexpected);
- Контролируемый (Monitorable);
- Высокий (High);
- Средний (Medium);
- Подробный (Verbose).

Хотя в большинстве случаев удобно применять параметры по умолчанию, эти опции могут помочь в устранении специфических неполадок. Например, если вы подозреваете потенциальную неполадку стабильности работы категории Резервное копирование и восстановление (Backup And Restore), то можете отконфигурировать запись в журнал детальной информации о таких событиях. И наконец, в разделе Журнал трассировки (Trace Log) можно указать количество создаваемых файлов журнала и число минут на использование файла журнала. С помощью этих опций можно обеспечить баланс между использованием дискового пространства и возможностями управления файлами журналов. По умолчанию файлы журналов размещены в папке %Program Files%\Common Files\Microsoft Shared\Web Server Extensions\12\Logs.

Обработка сведений об использовании

Системные администраторы могут отслеживать использование сайтов SharePoint. С помощью этих сведений можно определять, является ли производительность оптимальной либо в конфигурацию требуется внести изменения. Из соображений производительности функция Обработка сведений об использовании (Usage Analysis Processing) по умолчанию отключена. Вы можете включить обработку сведений об использовании и отконфигурировать параметр Местоположение файлов журнала (Log File Location) согласно требуемому уровню отслеживания.

Помимо хранения полезной информации службы WSS обеспечивает возможность автоматической обработки сведений об использовании в указанное время. Пользователи с соответствующими разрешениями могут просматривать отчеты об использовании сайтов на определенных узлах SharePoint.

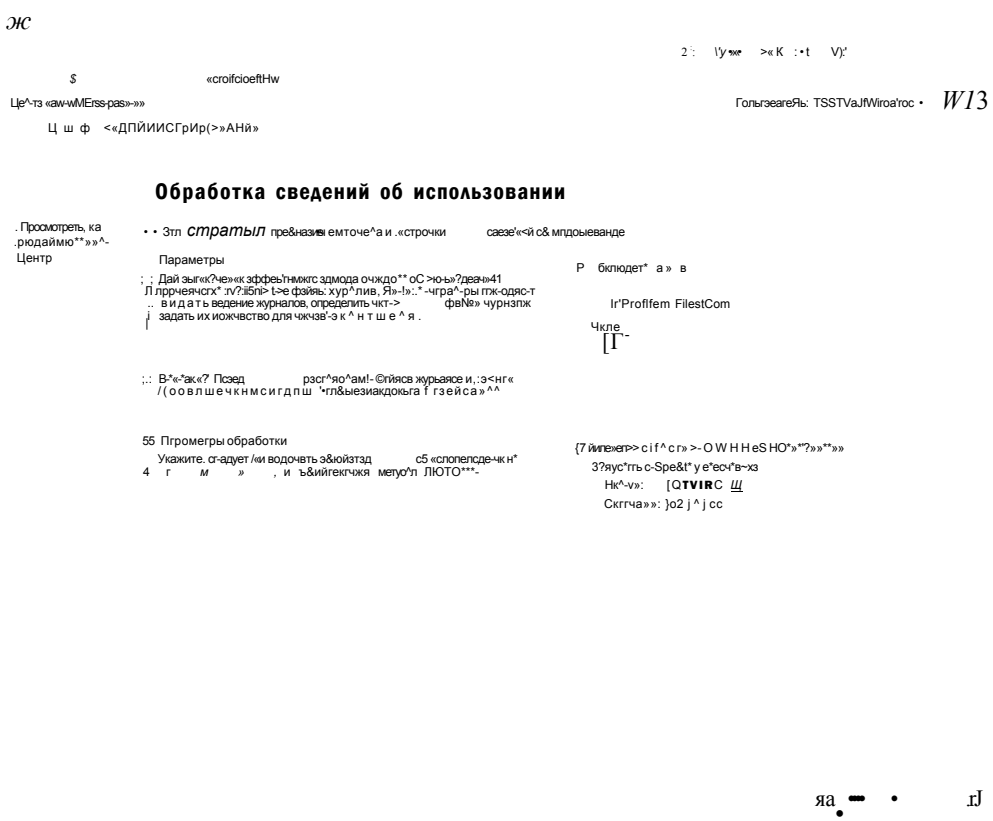


Рис. 9-14. Обработка сведений об использовании в центре администрирования SharePoint

Определения заданий

Для хранения данных службы WSS используется Внутренняя база данных Windows (Windows Internal Database) в автономной конфигурации и база данных SQL Server в конфигурации фермы серверов.

Информацию в этих базах данных следует регулярно проверять, чтобы удалять ненужные сведения и поддерживать общую производительность. Сведения о запланированных заданиях можно просмотреть, щелкнув ссылку Определения заданий таймера (Timer Job Definitions) на вкладке Операции (Operations). Как показано на рис. 9-15, вы можете щелкать отдельные задания, чтобы включать и отключать их.

Для просмотра истории выполнения заданий на вкладке Операции (Operations) щелкните ссылку Состояние задания таймера (Time Job Status). На этой странице отображается название (должность) каждого выполняемого задания с указанием времени запуска задания и состояние выполнения (успех или ошибка). Эту информацию следует регулярно просматривать для определения потенциальных проблем.

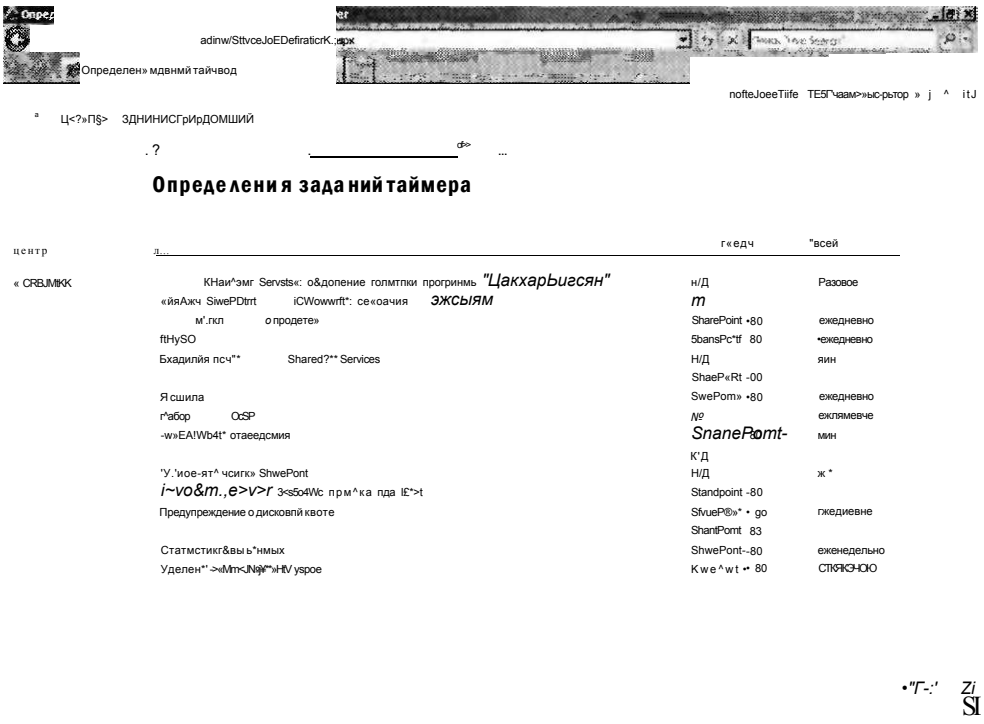


Рис. 9-15. Определения заданий таймера в центре администрирования SharePoint

Управление WSS с помощью утилиты stsadm

Хотя веб-сайт Центр администрирования SharePoint (SharePoint Central Administration) обеспечивает интуитивный и дружественный пользователю способ управления параметрами конфигурации, выполнение распространенных операций на множестве серверов WSS отнимает много времени. Для автоматизации этой задачи в WSS включена утилита командной строки stsadm.exe. Она используется для выполнения таких распространенных задач, как создание или удаление сайтов SharePoint и создание резервных копий. Переключатель командной строки help можно использовать для получения дополнительных сведений о синтаксисе и операциях, которые может выполнять утилита. Окно утилиты stsadm.exe показано на рис. 9-16.

По умолчанию утилита командной строки stsadm находится в папке %ProgramFiles%\Common Files\Microsoft Shared\Web Server Extensions\12\BIN.

СОВЕТ Подготовка к экзамену

Вам может показаться странным то, что основная утилита командной строки для администрирования служб Windows SharePoint Services (WSS) носит имя stsadm. Такое ее имя объясняется тем, что предыдущие версии WSS назывались SharePoint Team Services (STS). При сдаче сертификационного экзамена этот факт поможет вам вспомнить назначение данной утилиты командной строки.

Утилиту stsadm удобно использовать для выполнения одинаковых или похожих задач на множестве компьютеров WSS или для создания сценариев выполнения распространенных операций. Ее также удобно запускать в случае отсутствия веб-доступа к сайту Центр администрирования SharePoint (SharePoint Central Administration).

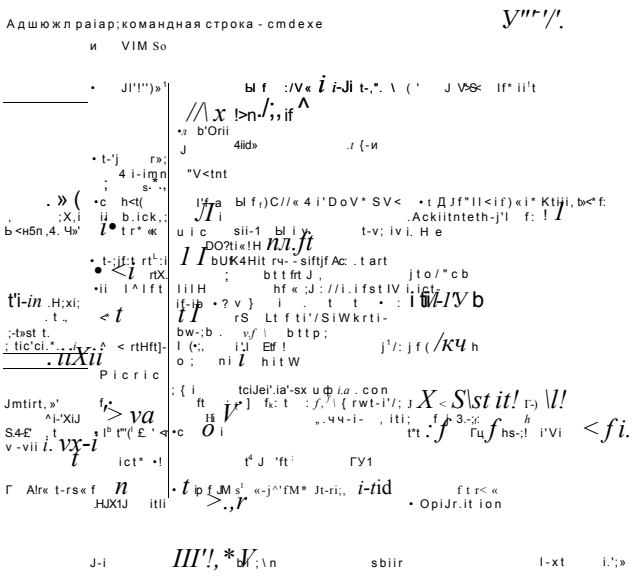


Рис. 9-16. Просмотр справочных сведений утилиты командной строки stsadm.exe

Резервное копирование и восстановление в WSS

Поскольку работа пользователей в вашей организации может зависеть от данных, хранящихся на серверах SharePoint, важно обеспечить защиту содержимого и конфигурации. Основная цель выполнения резервного копирования состоит в предотвращении потери данных в результате сбоев оборудования, ненамеренных модификаций или других проблем. В этом разделе мы рассмотрим способы резервного копирования и восстановления данных SharePoint.

Создание резервных копий SharePoint

Веб-сайт Центр администрирования SharePoint (SharePoint Central Administration) содержит функции для создания резервных копий. Для запуска процесса на вкладке Операции (Operations) щелкните ссылку Выполнение резервного копирования (Perform A Backup). На первом шаге процесса требуется выбрать информацию для сохранения в резервных копиях, как показано на рис. 9-17.

В WSS содержится много компонентов, каждый из которых можно включить в резервную копию. Если вы резервируете относительно небольшое развертывание WSS или хотите обеспечить защиту всех пользовательских данных и параметров конфигурации, установите флажок напротив элемента Ферма (Farm).

Все остальные компоненты будут выбраны автоматически. В других ситуациях может потребоваться создавать резервные копии лишь конкретного сайта или набора параметров. Для этого устанавливайте флажки только напротив соответствующих элементов. Чтобы указать остальные параметры, щелкните ссылку Параметры резервного копирования (Continue To Backup Options).

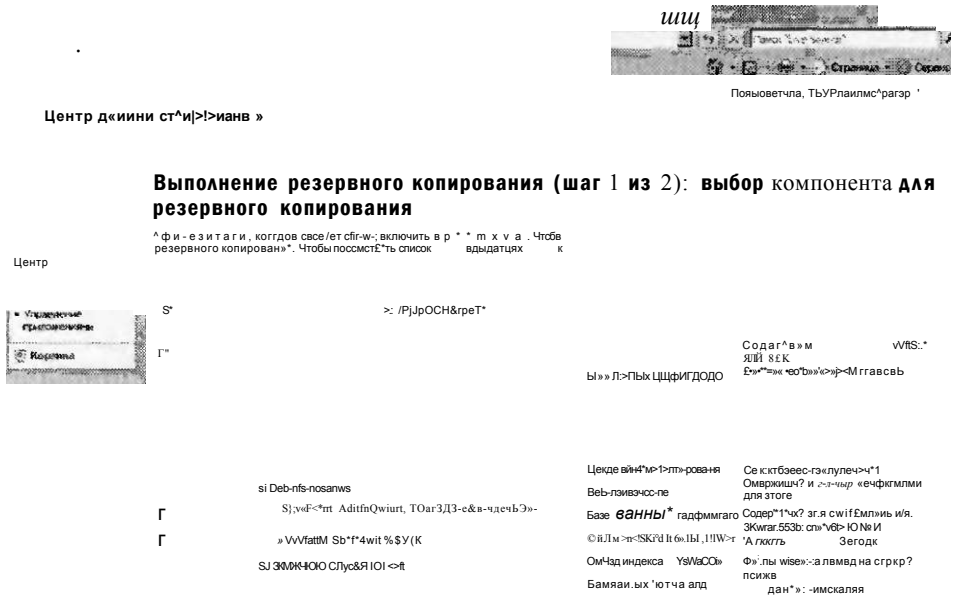


Рис. 9-17. Выбор компонентов, включаемых в резервную копию

На странице Запуск резервного копирования (Start Backup), показанной на рис. 9-18, представлены опции хранения содержимого резервных копий. В разделе Тип резервного копирования (Type Of Backup) есть две опции. Полное резервное копирование включает копии последних версий данных для всех выбранных компонентов. Размер резервной копии зависит от объема содержимого сайта SharePoint. (Приблизительная оценка необходимого места на диске представлена внизу страницы.)

С помощью второй опции в разделе Тип резервного копирования (Type Of Backup) можно создать разностную резервную копию, в которой будут сохраняться лишь те данные, которые были изменены со времени создания последней полной резервной копии. Хотя для разностного резервного копирования требуется меньше дискового пространства и ресурсов, для полного восстановления системы WSS потребуется доступ к полной и r-разностной резервным копиям.

С помощью последнего параметра можно указать размещение резервной копии. В поле Местоположение резервной копии (Backup Location) можно указать путь в локальной файловой системе или сетевую папку. Для обеспечения защиты от перманентной потери данных в результате сбоев оборудования

хранилища файлы резервных копий следует хранить еще на одном компьютере в рабочей среде.

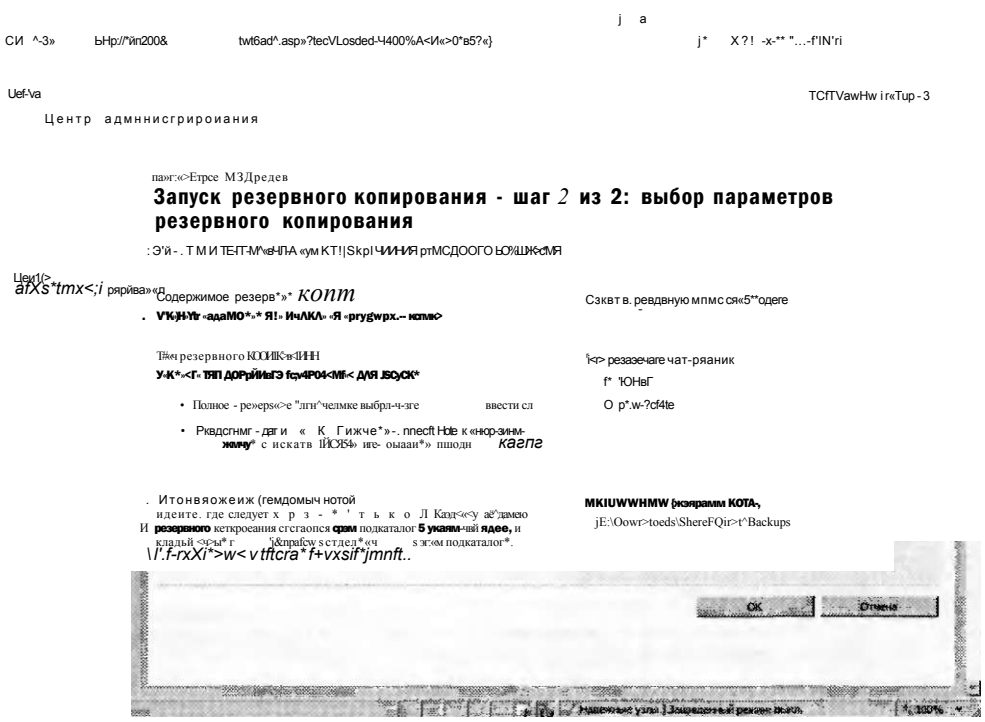


Рис. 9-18. Опции резервного копирования в центре администрирования WSS

После выбора соответствующих опций можете щелкнуть OK, чтобы составить расписание процесса резервного копирования. Для скорейшего запуска процесса задание будет использовать встроенный таймер WSS. Резервное копирование выполняется без нарушений режима работы сайта, хотя пользователи могут заметить снижение производительности системы SharePoint. На странице Состояние резервного копирования и восстановления (Backup And Restore Status) будет отображаться состояние выполнения задания с различными дополнительными деталями. Во время выполнения задания страница будет периодически обновляться.

Восстановление Windows SharePoint Services

Существует несколько причин, по которым может потребоваться восстановить данные SharePoint. В некоторых случаях сбой оборудования или повреждение файловой системы может привести к выходу сайта из строя, а также к удалению либо случайной модификации важных документов или другого содержимого. Для запуска процесса восстановления на вкладке Операции (Operations) щелкните ссылку Восстановление из резервной копии (Restore From Backup). Процесс восстановления выполняется в четыре шага.

- **Шаг 1. Выбор местоположения резервных копий (Select Backup Location)** В это поле можно ввести локальный или сетевой путь к местополо-

жению резервной копим. По умолчанию в нем указан путь, используемый для последней операции резервного копирования.

Шаг 2. Выбор резервной копии для восстановления (Select Backup To Restore) В зависимости от пути, введенного на шаге **1,** система WSS выполнит поиск резервных копий, которые хранятся в указанной папке. Затем вы можете выбрать найденную резервную копию и щелкнуть ссылку Продолжить восстановление (Continue Restore Process). В противном случае вы можете щелкнуть ссылку Сменить каталог (Change Directory) и указать другое местоположение.

Шаг 3. Выбор компонента для восстановления (Select Component To Restore) На этой странице можно выбрать один или несколько компонентов для восстановления на сервере WSS. В списке представлены компоненты, включенные в исходную резервную копию, как показано на рис. 9-19. Выберите соответствующие элементы и щелкните ссылку Продолжить восстановление (Continue Restore Process).

Шаг 4. **Выбор параметров восстановления (Select Restore Options)** На этой странице можно указать тип операции восстановления.

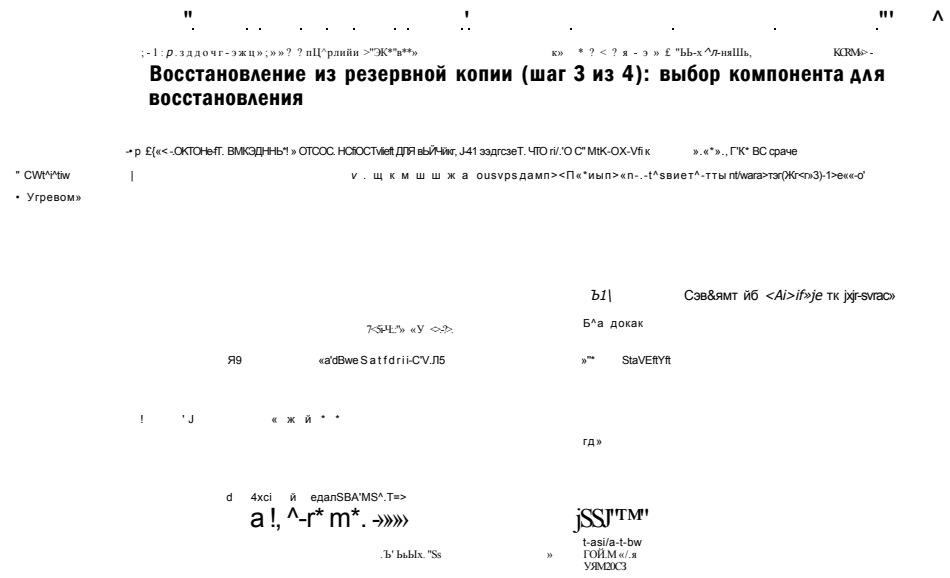


Рис. 9-19. Выбор компонентов для восстановления

Существует две опции для восстановления. Опцию Та же самая конфигурация (Same Configuration) удобно использовать для замены всех текущих компонентов с помощью резервной копии. Отметим, что при выборе этой опции будут потеряны все изменения, внесенные в выбранные компоненты со времени создания резервной копии.

Вторая опция, Новая конфигурация (New Configuration), позволяет указать альтернативную конфигурацию для восстановления данных. Эту опцию удобно применять для создания новой копии сайта из резервной копии. Ее использование также более безопасно, поскольку она не влияет на текущий сайт SharePoint. Доступные опции в значительной степени зависят от параметров, используемых при создании резервной копии, включая URL и имя веб-приложения для сайта SharePoint. Помимо имени и местоположения вы также можете выбрать сервер баз данных (или внутреннюю базу данных Windows, если она установлена). Для запуска операции восстановления щелкните ОК.

Журнал резервного копирования и восстановления

Для проверки выполнения резервного копирования щелкните ссылку Журнал резервного копирования и восстановления (Backup And Restore History) на вкладке Операции (Operations). На открывшейся странице (рис. 9-20) указаны дата и время начала и завершения задания, содержимое резервных копий, тип резервного копирования и местоположение файлов резервных копий. Процесс восстановления можно также запустить, выбрав резервную копию и щелкнув ссылку Продолжить восстановление (Continue Restore Process).

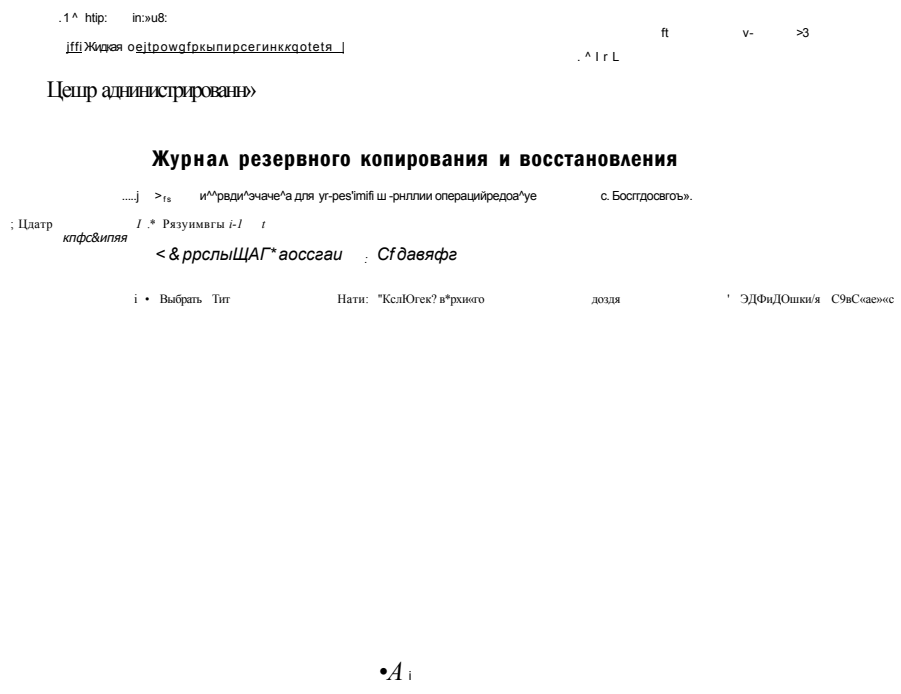


Рис. 9-20. Журнал резервного копирования и восстановления

Развертывание и конфигурирование сайтов SharePoint

Поскольку WSS позволяет создавать на одном сервере множество сайтов SharePoint, важно определить метод разделения содержимого и пользователей. В общем следует пытаться ограничить полномочия и количество пользователей для

каждого типа сайта. При использовании одного сайта для многочисленных типов деятельности пользователям становится довольно сложно быстро находить нужное содержимое. В дальнейшем организация содержимого может превратиться в непростое и утомительное занятие. В этом разделе мы рассмотрим способы создания сайтов и управления ими.

Реальный мир

Анил Десаи

Довольно часто IT-профессионалы больше внимания уделяют технологии, а не обеспечению преимуществ ее применения для пользователей. При развертывании такого продукта, как Windows SharePoint Services, важно вначале определить принципы его использования в корпоративной среде. Процесс создания нового сайта SharePoint довольно простой, однако определение оптимального метода реализации может отнимать много времени и сил. В некоторых случаях имеет смысл просто развернуть новый сайт, разрешить пользователям доступ к сайту и посмотреть, как будут развиваться события. Тем не менее в большинстве случаев для успешного развертывания следует выполнить некоторое планирование и проявить предусмотрительность.

Важным аспектом успешного развертывания приложений и служб является вовлечение пользователей в процесс принятия решения. Вы должны понимать реальные задачи сотрудников организации. В WSS содержится много возможностей, позволяющих совместно работать с документами. Однако пользователи не всегда просят сделать то, что им нужно на самом деле. Отдельные лица могут попросить создать сайт SharePoint, хотя аналогичный сайт уже существует, или пытаться использовать один сайт для выполнения множества функций. Кроме того, следует учитывать требования безопасности, количество активных пользователей сайта и объем данных, которыми нужно управлять. Эту информацию можно комбинировать для определения оптимального способа обеспечения доступа к WSS для пользователей. Четкое определение требований также поможет гарантировать успешное развертывание.

Уделите внимание определению потребностей и ожидаемых преимуществ SharePoint (или любой иной применяемой технологии) для пользователей. Более подробные сведения и примеры можно найти на странице Planning Worksheets for Windows SharePoint Services 3.0 веб-сайта Microsoft TechNet по адресу *http://technet.microsoft.com.*

Подузлы и семейства узлов

Семейство узлов представляет собой набор связанных сайтов SharePoint, совместно использующих множество параметров. Например, все сайты в семействе узлов совместно используют одни и те же панели навигации. Таким образом, пользователям проще получать доступ к сайтам в семействе без необходимости перехода на другой URL. Кроме того, все сайты в семействе используют идентичные типы содержимого, функции поиска и группы безопасности.

Существует два основных способа создания дополнительных сайтов в WSS. Лучше всего добавить множество сайтов со связанным содержимым и идентичными техническими требованиями в одно семейство. Второй способ состоит в создании нового сайта SharePoint верхнего уровня в новом семействе узлов. Этот способ лучше всего использовать в тех случаях, когда параметры нового сайта значительно отличаются от параметров существующих семейств узлов. Сайты в разных семействах узлов могут использовать для разрешений безопасности различные параметры конфигурации. Другими параметрами различных семейств узлов, такими как область поиска и квоты, можно управлять независимо. В крупных организациях с помощью семейств узлов можно разделять обязанности системных администраторов для WSS. Кроме того, эти сайты можно резервировать и восстанавливать по отдельности, что обеспечивает большую степень контроля над резервным копированием.

Создание семейства узлов

Для управления семействами узлов, веб-сайтами и другими связанными параметрами можно использовать веб-сайт Центр администрирования SharePoint (SharePoint Central Administration). В разделе Управление узлами SharePoint (SharePoint Site Management) можно создавать и удалять семейства узлов. Щелчком ссылки Создание семейства веб-узлов (Create Site Collection) на вкладке Управление приложениями (Application Management) открывается страница, показанная на рис. 9-21.

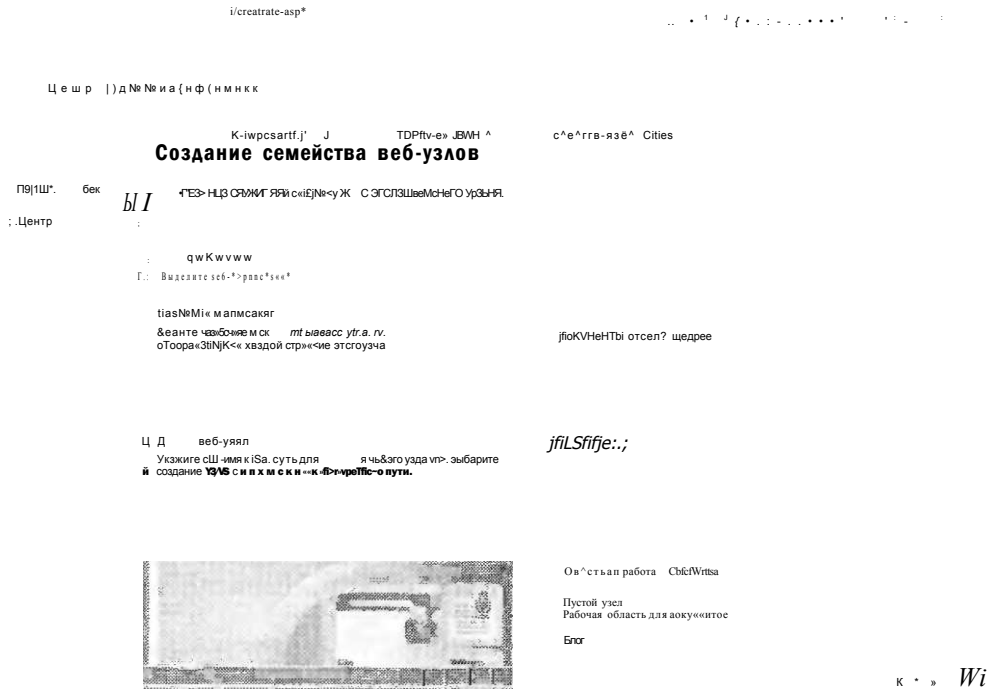


Рис. 9-21. Создание нового семейства узлов в центре администрирования SharePoint

Для создания семейства узлов нужно указать следующую информацию.

- **Веб-приложение (Web Application)** Этот раскрывающийся список содержит все веб-приложения, созданные в среде SharePoint. Если вы еще не создавали дополнительные веб-приложения, в списке будет представлен лишь URL сервера по умолчанию.
- **Название и описание (Title and Description)** Эта информация используется для идентификации семейства узлов. Название будет отображаться для пользователей и администраторов, а описание должно включать сведения о назначении и использовании семейства узлов. В некоторых случаях семейства узлов можно основать для подразделений организации, например отдела маркетинга или отдела кадров.
- **Адрес веб-узла (Web Site Address)** Каждый веб-сайт, создаваемый в WSS, должен иметь уникальный URL. По умолчанию доступен URL-адрес /sites. В этом поле можно указать ссылку браузера, которая будет использоваться для получения доступа к сайту. Поскольку пользователям потребуется вводить этот адрес, рекомендуется использовать аббревиатуру имени сайта и не применять такие символы, как пробелы и знаки препинания.
- **Выбор шаблона (Template Selection)** Для каждого нового семейства узлов SharePoint можно выбрать конкретный шаблон. По умолчанию шаблоны организованы в двух категориях: Совместная работа (Collaboration) и Собрания (Meetings). Позже в этом занятии вы узнаете, как добавлять на сервер новые шаблоны.
- **Главный администратор семейства веб-узлов (Primary Site Collection Administrator) и Дополнительный администратор семейства веб-узлов (Secondary Site Collection Administrator)** В относительно небольших средах SharePoint один системный администратор может отвечать за управление множеством сайтов и семейств узлов. В этих разделах можно указать пользователей, располагающих разрешениями управлять семейством узлов. Для просмотра списка учетных записей на локальном компьютере или в домене (если компьютер является членом домена) можно щелкнуть кнопку Обзор (Browse).
- **Шаблон квот (Quota Template)** В этом разделе можно выбрать шаблон квот для ограничения ресурсов, используемых семейством узлов. Более подробно мы рассмотрим шаблоны квот далее в этом занятии.

Содержимое и схема сайта будут зависеть от выбранного шаблона приложения. На рис. 9-22 показан пример использования шаблона Базовая рабочая область для собраний (Basic Meeting Workspace) для создания семейства узлов. Когда вы щелкнете OK, WSS создаст новое семейство узлов. В итоговом сообщении будет отображаться URL нового сайта верхнего уровня. Для проверки параметров созданного сайта щелкните ссылку или скопируйте ее и вставьте в новое окно браузера.

Для просмотра списка всех семейств узлов на сервере WSS щелкните ссылку Список семейств узлов (Site Collection) на вкладке Управление приложениями (Application Management). В сведениях будет указан администратор (администраторы) сайта, а также название и описание этого сайта.

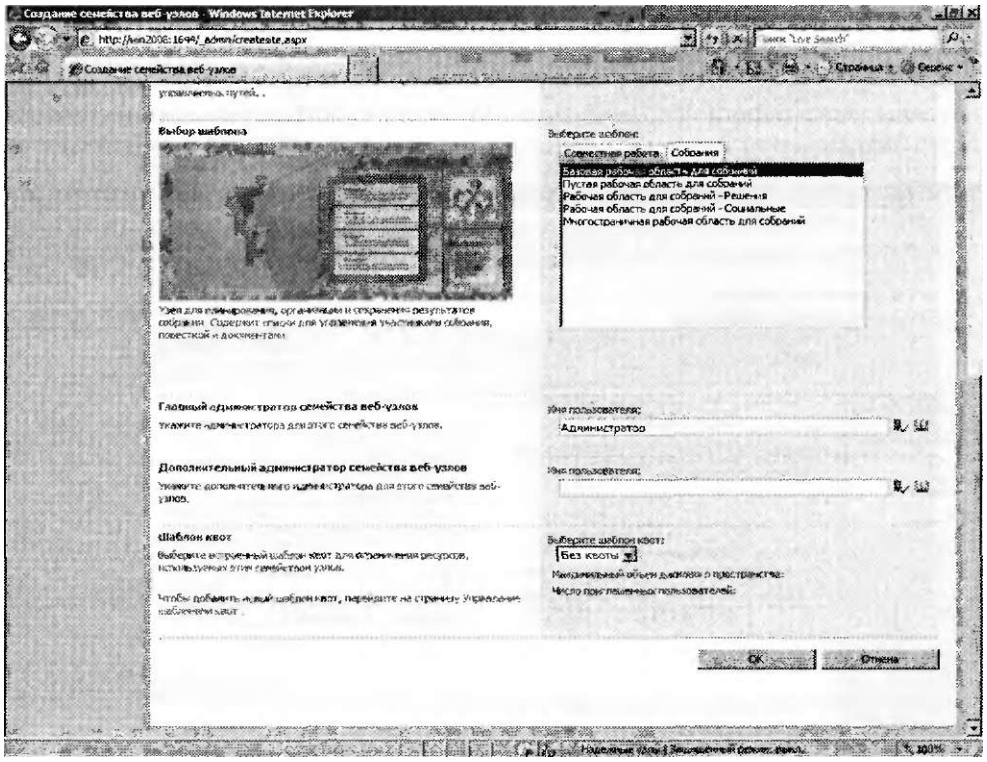


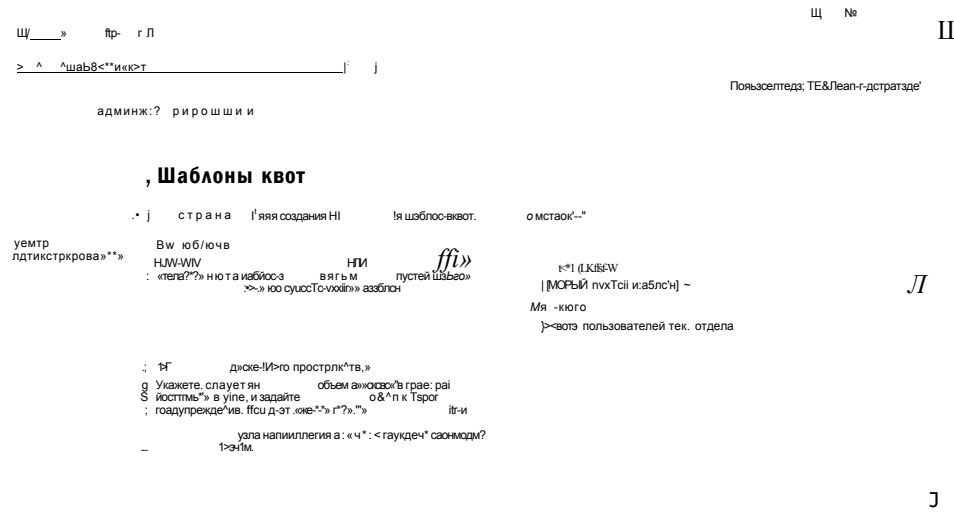
Рис. 9-22. Просмотр параметров нового семейства узлов, созданного с помощью шаблона Базовая рабочая область для собраний (Basic Meeting Workspace)

Определение шаблонов квот

Если вы осуществляете управление хранилищем данных, например с содержимым файлового сервера или Microsoft Exchange Server, то наверняка знаете, что пользователи могут очень быстро захватить большое дисковое пространство. Службы WSS также не являются исключением, поскольку пользователи часто выгружают на свои сайты много больших документов. Для управления использованием ресурсов можно создавать шаблоны квот. Эти шаблоны затем можно назначать для конкретных семейств узлов SharePoint. По умолчанию в конфигурацию WSS не включены шаблоны квот. Для того чтобы создать новый шаблон квот, на вкладке Управление приложениями (Application Management) щелкните ссылку Шаблоны квот (Quota Templates). На рис. 9-23 показаны все доступные опции.

В поле Имя нового шаблона (New Template Name) нужно ввести имя шаблона. Вы можете изменить параметры любого существующего шаблона квот или указать имя для нового шаблона. Имя должно описывать назначение шаблона. В разделе Ограничения дискового пространства (Storage Limit Values) откоп-фигурируйте два ограничения. В поле Максимальный объем дискового пространства, используемого узлом (Limit Site Storage To A Maximum Of) можно

указать максимальный объем дискового пространства, выделяемого для сайта (в мегабайтах). По достижении этого объема пользователи не смогут добавлять новое содержимое. При использовании второй опции в случае достижения определенного порога использования дискового пространства администратору сайта отправляется предупреждение по электронной почте.



*ƒНй«5ЯЗК)1уу)Л»}ЗйЩЩИ1И»Й ptmifK M*ш:*

Рис. 9-23. Определение нового шаблона квот в центре администрирования SharePoint

Чтобы прикрепить к сайту шаблон квот, на вкладке Управление приложениями (Application Management) необходимо щелкнуть ссылку Квоты и блокировки семейства узлов (Site Collection Quotas And Locks). На открывшейся странице, показанной на рис. 9-24, можно выбрать семейство узлов и указать опции хранения содержимого.

В разделе Сведения о блокировке узла (Site Lock Information) можно указать ограничения использования дискового пространства сайтом. Доступны следующие опции:

- Нет блокировки (Not Locked);
- Добавление содержимого запрещено (Adding Content Prevented);
- Только чтение (блокировка добавления, обновления и удаления) (Read-only (Blocks Additions, Updates, And Deletions);
- Нет доступа (No Access).

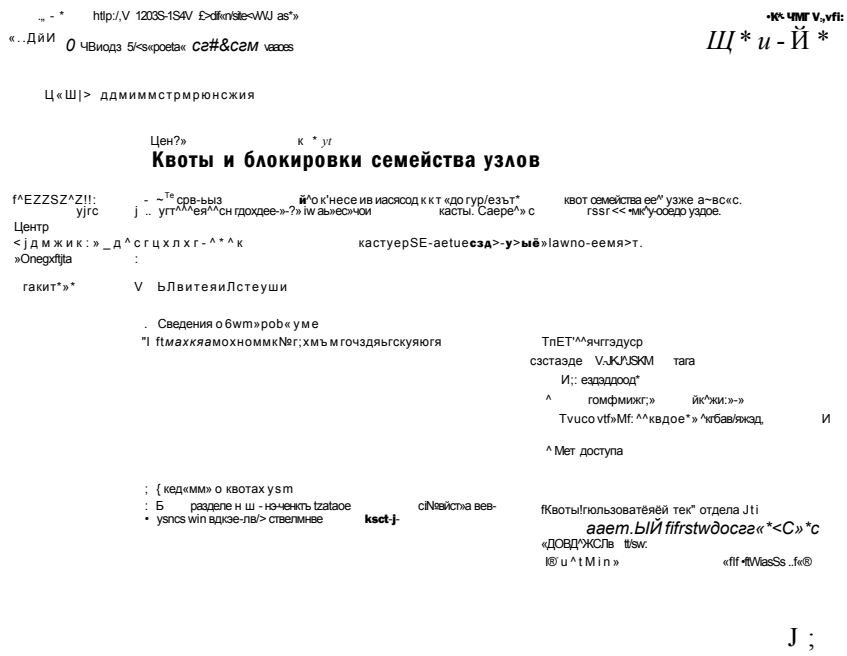


Рис. 9-24. Конфигурирование квот *и* блокировок семейства узлов

Эти опции удобно использовать в случаях, когда требуется запретить пользователям модификацию содержимого сайта SharePoint, однако разрешить просмотр существующих данных. В разделе Сведения о квотах узла (Site Quota Information) можно выбрать конкретные параметры для данного семейства узлов или использовать опцию Индивидуальная квота (Individual Quota) в раскрывающемся списке для назначения параметров. Основное преимущество использования шаблонов квот состоит в том, что эти ограничения дискового пространства можно централизованно модифицировать для многочисленных семейств узлов без необходимости редактировать параметры каждого сайта.

Настройка параметров сайта

Помимо основных параметров, которые можно указать при создании нового сайта или семейства узлов SharePoint, вы также можете управлять многочисленными параметрами содержимого самого сайта. Чтобы открыть эти параметры, вначале перейдите на сайт, который вы хотите администрировать. Все сайты в верхней правой области имеют раскрывающийся список Действия узла (Site Actions). Выбрав команду Параметры узла (Site Settings), вы сможете просмотреть большое количество опций (рис. 9-25).

Параметры распределены по следующим группам:

- Пользователи и разрешения (Users And Permissions);
- Внешний вид и функции (Look And Feel);
- Коллекции (Galleries);

- Администрирование узла (Site Administration);
- Администрирование семейства веб-узлов (Site Collection Administration).

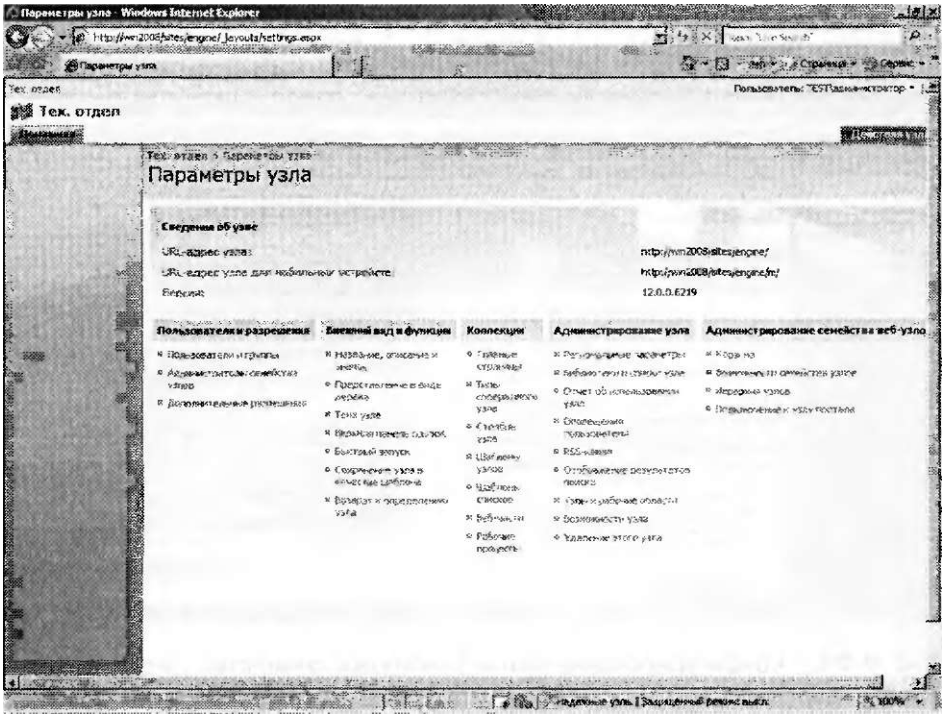


Рис. 9-25. Список параметров сайта

В некоторых случаях управление сайтом и внесение изменений входит в функции системных администраторов. Однако пользователи, имеющие базовый опыт работы с SharePoint и необходимые разрешения, также могут выполнять администрирование на основе требований организации.

Управление веб-приложениями

Веб-приложения используются для управления клиентскими сайтами SharePoint, к которым могут подключаться пользователи. По умолчанию роль сервера Windows SharePoint Services включает два встроенных веб-приложенпя: сайт SharePoint - 80 и сайт SharePoint Central Administration v3. Новые веб-приложения можно создавать с помощью команды Создание или расширение веб-приложения (Create Or Extend Web Application) на вкладке Управление приложениями (Application Management) веб-сайта Центр администрирования SharePoint (SharePoint Central Administration). На странице Создание веб-приложения (Create A New Web Application) можно указать параметры для нового веб-сайта и новой базы данных, как показано на рис. 9-26.

Вы также можете расширить существующее веб-приложение в другие веб-сайты IIS, например в конфигурации экстрасети. При этом один URL используется для внутренних пользователей компании и еще один — для пользователей,

получающих доступ к сай гу в Интернете. Хотя содержимое будет отображаться одинаково, системные администраторы могут применять для общедоступного веб-сайта другие параметры конфигурации. Например, сайт может запускаться на другом порте, а управление параметрами безопасности доступа к сайту может осуществляться отдельно.

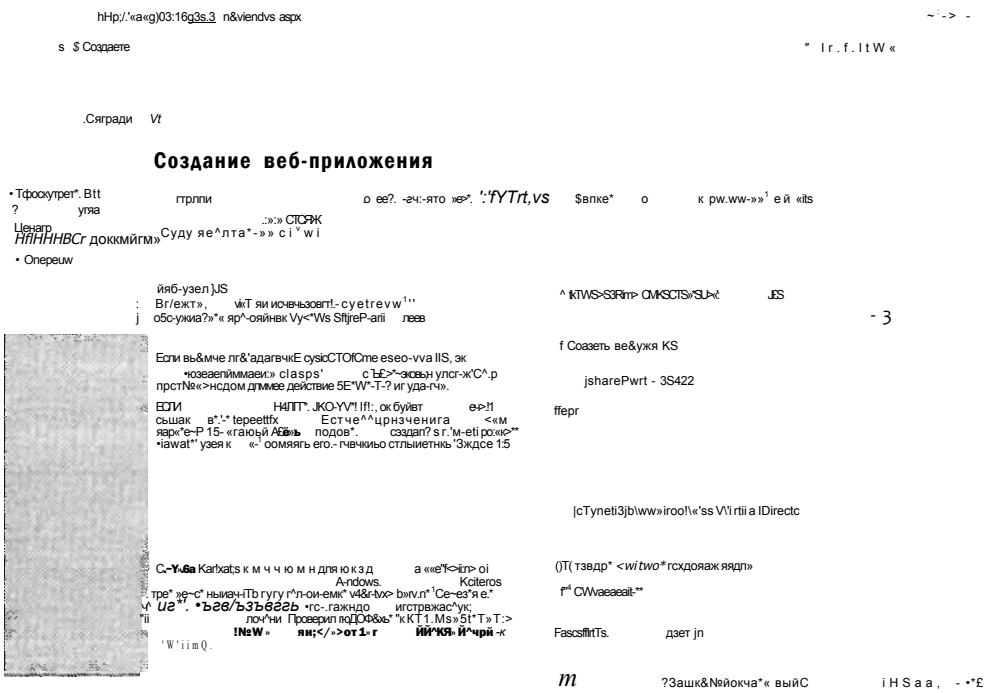


Рис. 9-26. Создание нового веб-прияожения

Щелкнув ссылку Список веб-приложений (Web Application List) на вкладке Управление приложениями (Application Management), вы откроете список существующих веб-приложений, определенных для WSS. Ссылка Удаление веб-приложения (Delete Web Application) используется для удаления веб-приложения из конфигурации WSS. Вы можете удалить базы данных содержимого веб-приложения, связанный веб-сайт либо и то, и другое.

Если вам требуется удалить лишь один веб-сайт, используйте ссылку Удаление SharePoint с веб-узла IIS (Remove SharePoint From IIS Web Site). На открывшейся странице можно удалить веб-нрпложение из конфигурации WSS, а также связанный веб-сайт IIS.

Настройка общих параметров веб-приложений

Системные администраторы могут конфигурировать многие параметры для каждого веб-приложения. Доступные опции открываются с помощью ссылки Общие параметры веб-ириложенй (Web Application General Settings). После выбора веб-приложения для модификации доступны такие опции (рис. 9-27):

- Часовой пояс по умолчанию (Default Time Zone);

Шаблон квот по умолчанию (Default Quota Template);

Параметры смарт-тега имени пользователя и сведений о присутствии (Person Name Smart Tag And Presence Settings);

Максимальный объем отправляемых данных (Maximum Upload Size);

Оповещения (Alerts);

Параметры RSS-каналов (RSS Settings);

Параметры API-интерфейса блогов (Blog API Settings);

Проверка безопасности веб-страницы (Web Page Security Validation);

Отправка имени и пароля пользователя по электронной почте (Send User Name And Password In E-Mail);

Обработчики событий с обратной совместимостью (Backward-Compatible Event Handlers);

Журнал изменений (Change Log);

Корзина (Recycle Bin).

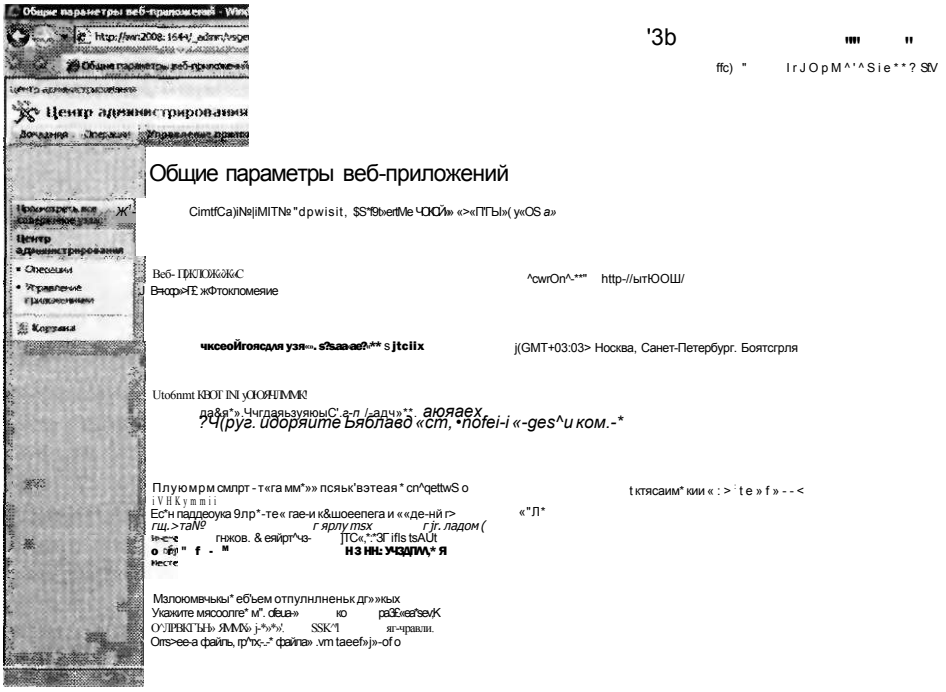


Рис. 9-27. Общие параметры веб-приложений

Одни исходные параметры зависят от параметров конфигурации на уровне сервера, а другие используют опции по умолчанию новых веб-приложений WSS. Поэтому вам следует проверять эти опции для каждого нового веб-приложения. Такие детали, как часовой пояс для веб-приложения, могут варьироваться, особенно в географически распределенных организациях или, скажем, для сайтов групп.

Определение управляемых путей

Ранее в этом занятии были описаны принципы определения сайтов и семейств узлов. Управляемые пути позволяют указать реагирование WSS на определенные веб-запросы. Для получения доступа к этим параметрам на вкладке Управление приложениями (Application Management) щелкните ссылку Определение управляемых путей (Define Managed Paths), чтобы открыть страницу, показанную на рис. 9-28.

По умолчанию в WSS включено два управляемых пути. Корневой путь (root) доступен по умолчанию для пользователя, который подключается к веб-сайту по умолчанию на порте 80. Путь sites включает URL, в котором может быть указано множество дополнительных сайтов и веб-приложений. Новый путь можно добавить с целью создания именного пространства URL для коллекции новых веб-приложений. Этот путь удобно использовать в случае работы с большим количеством веб-приложений или для упрощения URL-адресов, с помощью которых пользователи могут получать доступ к веб-приложениям.

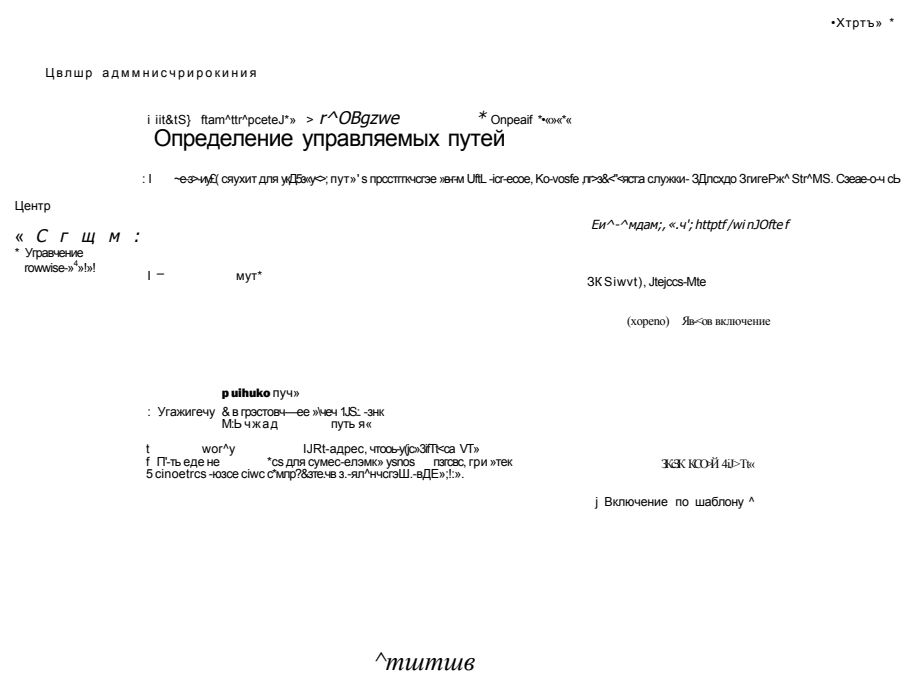


Рис. 9-28. Определение управляемых путей для веб-приложений

Настройка разрешений веб-приложений

Поскольку организации часто хранят на веб-сайтах SharePoint уязвимые данные, управление параметрами безопасности играет очень важную роль. Администраторы могут ограничивать доступ к сайту и управлять разрешениями для него различными способами. Доступ к страницам конфигурации можно получить

в разделе Безопасность приложений (Application Security) на вкладке Управление приложениями (Application Management).

Страница Разрешения пользователя для веб-приложения (User Permissions For Web Application), показанная на рис. 9-29, содержит много опций. Разрешения не назначаются конкретным пользователям.

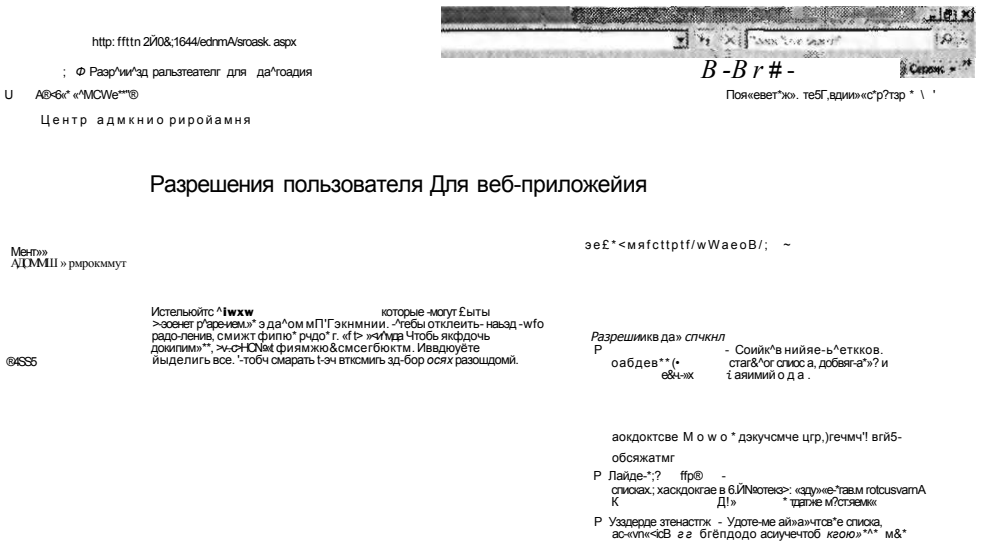


РИС. 9-29. Настройка пользовательских разрешений для веб-приложений

Список разрешений разбит на три группы.

- **Разрешения для списка (List Permissions)** Эти разрешения применяются к элементам управления SharePoint, которые используются для добавления и удаления данных. В качестве примеров можно привести компоненты Извещения (Announcements) и Обсуждение (Discussion). В список доступных разрешений включены операции добавления, изменения, удаления и просмотра элементов.
- **Разрешения для узла (Site Permissions)** Эти разрешения используются для определения функций и операций, которые могут выполнять администраторы веб-приложения SharePoint, в частности управление разрешениями для других пользователей, добавление и настройка страниц, а также просмотр данных статистики использования сайта.
- **Личные разрешения (Personal Permissions)** Пользователи веб-сайтов SharePoint могут создавать собственные настраиваемые представления Веб-частей (Web Parts). Пользователи могут добавлять, удалять и менять расположения этих веб-частей на основе личных предпочтений. Эти разрешения

определяют возможности пользователем создавать личные представления и управлять ими.

Управление параметрами проверки подлинности

Критически важным аспектом общей безопасности SharePoint является обеспечение гарантии получения доступа к конкретным сайтам лишь для авторизованных пользователей. Страница Изменение параметров проверки подлинности (Edit Authentication), которую можно открыть, щелкнув ссылку Поставщики проверки подлинности (Authentication Providers) на вкладке Управление приложениями (Application Management) и выбрав поставщика, содержит параметры выполнения проверки подлинности (рис. 9-30). Параметры безопасности можно определять отдельно для каждого веб-приложения WSS.

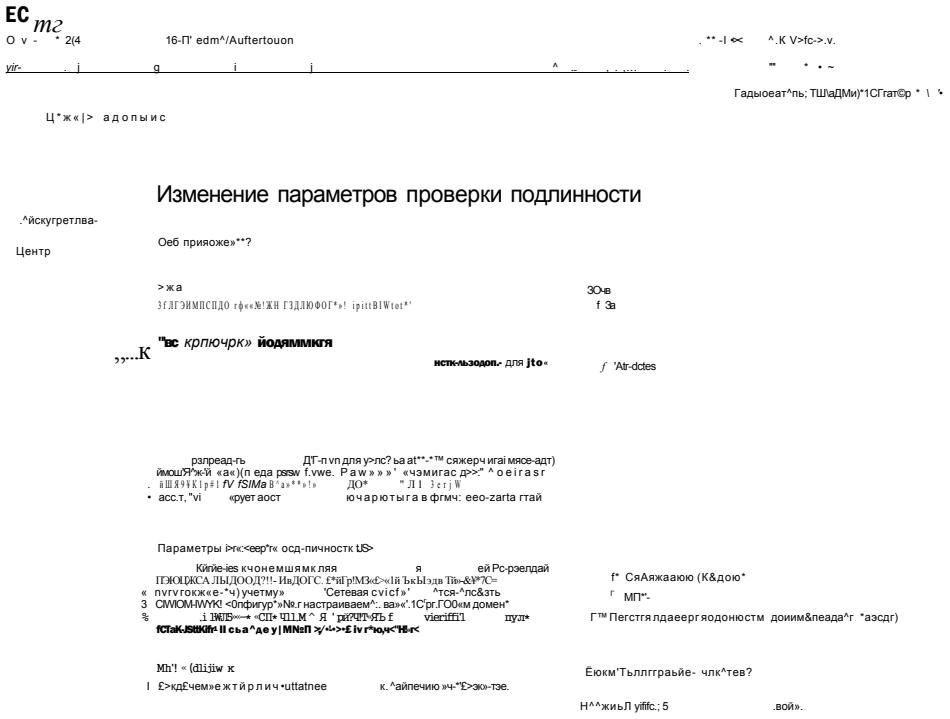


Рис. 9-30. Параметры проверки подлинности в центре администрирования SharePoint

В разделе Тип проверки подлинности (Authentication Type) представлены три опции.

- **Windows** Используется стандартный метод проверки подлинности Windows. Эту опцию лучше всего использовать в случае, если основные пользователи сайта являются сотрудниками, имеющими учетные записи на локальном компьютере или в домене Active Directory. За исключением применения строгих протоколов безопасности (таких как Kerberos) пользователям, прошедшим проверку подлинности, может не требоваться вводить имя и пароль для получения доступа к сайту.

- Формы (Forms) При прохождении проверки подлинности с помощью форм пользователи должны указывать действительное пользовательское имя и пароль. Эту опцию удобно использовать в случаях, когда нет возможности применить проверку подлинности Windows. Например, формы можно применять для внешних бизнес-партнеров или пользователей Интернета, которым нужен доступ к сайту SharePoint.
- Единый вход (Web Single Sign-On) Стандарт Web Single Sign-On (SSO) используется при проверке подлинности пользователя для веб-службы. Его удобно использовать в случае, если нет возможности применить проверку подлинности Windows. Этот стандарт предоставляет упрощенный метод доступа для пользователей, которым часто нужен доступ к многочисленным веб-системам и приложениям. Для обеспечения услуг SSO в Windows Server 2008 можно использовать Службы федерации Active Directory (Active Directory Federation Services, ADFS).

Вы можете указать дополнительные детали, включая разрешение анонимного доступа к сайту SharePoint. Эту опцию удобно использовать для сайтов, содержащих информацию, которая должна быть доступна для всех пользователей в организации или Интернете. В целом возможность выбора нескольких опций проверки подлинности сервера поможет администраторам гарантировать безопасность сайтов SharePoint, обеспечивая при этом поддержку пользователей вне организации.

Управление средствами самостоятельного создания сайтов

В небольших и малодинамичных средах на системных администраторов целесообразно возложить ответственность за создание новых сайтов. В более крупных средах следует разрешить пользователям создавать собственные сайты. Страница параметров Управление средствами самостоятельного создания сайтов (Self-Service Site Management), ссылка на которую представлена на вкладке Управление приложениями (Application Management), содержит опции разрешений для создания пользователями собственных сайтов SharePoint. По умолчанию эти средства отключены для новых веб-приложений.

Установка шаблонов приложений

Хотя сайт, созданный по умолчанию, обеспечивает большую часть полезной функциональности, существует множество способов улучшения возможностей архитектуры SharePoint в соответствии с конкретными требованиями. Для содействия организациям в достижении поставленных целей корпорация Microsoft разработала набор бесплатных шаблонов приложений для WSS. Далее приведен список примеров таких шаблонов:

- Discussion Database;
- Classroom Management;
- Employee Training Scheduling and Materials;
- Request for Proposal;
- Call Center;
- Event Planning;

- Help Desk;
- IT Team Workspace;
- Sales Lead Pipeline.

Доступны два основных типа шаблонов. Пользователи с необходимыми разрешениями могут установить шаблоны Site Admin Templates в архитектуре сайта SharePoint. Шаблоны Server Admin Templates устанавливаются на уровне сервера. Доступ к ним в веб-приложениях и на сайтах должны обеспечить системные администраторы. Шаблоны для загрузки и более подробные сведения о них можно найти на веб-сайте Microsoft SharePoint Products and Technologies Template по адресу *http://www.microsoft.com/sharepoint/templates.mspx.* Пакет загрузки включает инструкции по установке шаблонов на сервере WSS.

Проверьте себя

1. Какую опцию следует выбрать для создания нового сайта SharePoint, который будет использовать параметры навигации и безопасности существующего сайта?
2. Как ограничить объем дискового пространства для нескольких сайтов SharePoint?

Ответы

1. Нужно создать сайт в семействе исходного узла. Таким образом, новый сайт автоматически будет использовать параметры навигации и безопасности существующего сайта.
2. Самый простой метод ограничения дискового пространства для хранения данных состоит в создании шаблона квот и его применении к семейству узлов. Для каждого семейства узлов можно назначить отдельные параметры квот.

Практикум. Настройка и управление службами Windows SharePoint Services

В предложенных далее упражнениях вы настроите параметры WSS и используете функции резервного копирования и восстановления центра администрирования SharePoint. Предполагается, что вы уже установили роль сервера Windows SharePoint Services и все необходимые зависимости в автономной конфигурации сервера на локальном компьютере. Поскольку в упражнениях требуется вносить изменения в конфигурацию, их следует выполнять на тестовом компьютере.

Упражнение 1. Настройка сайтов и семейств узлов WSS

В этом упражнении вы создадите новый сайт SharePoint Services. Затем вы проверите работу сайта в Internet Explorer.

1. Войдите на сервер Server2 в качестве пользователя с привилегиями администратора.

2. Откройте веб-сайт Центр администрирования SharePoint (SharePoint Central Administration Web-site), щелкнув значок Центр администрирования SharePoint 3.0 (SharePoint 3.0 Central Administration) в группе программ Администрирование (Administrative Tools).
3. Введите учетные данные, которые вы использовали для входа на сервер на шаге 1. В Internet Explorer откроется веб-сайт Центр администрирования SharePoint (SharePoint Central Administration).
4. На вкладке Домашняя (Home) просмотрите рекомендуемые задачи администратора. Позже вы сможете вернуться к этой странице для настройки параметров конфигурации, не описанных в данном упражнении.
5. В верхней части страницы щелкните вкладку Управление приложениями (Application Management). В разделе Управление веб-приложениями SharePoint (SharePoint Web Application Management) щелкните ссылку Создание или расширение веб-приложения (Create Or Extend Web Application).
6. На странице Создание или расширение веб-приложения (Create Or Extend Web Application) выберите опцию Создать веб-приложение (Create A New Web Application).
7. На странице Создание веб-приложення (Create New Web Application) выберите в разделе Веб-узел IIS (IIS Web Site) параметры по умолчанию. Отметим, что Центр администрирования SharePoint автоматически создает описание и номер порта, а также выбирает параметр Путь (Path) на основе местоположения существующего веб-содержимого.
8. В разделе Пул приложений (Application Pool) выберите опцию Создать пул приложений (Create A New Application Pool). Выберите опцию учетной записи безопасности Встроенная (Predefined) и укажите учетную запись Сетевая служба (Network Service).
9. Просмотрите другие доступные опции, включая параметры разделов Настройка безопасности (Security Configuration) и Имя базы данных и режим проверки подлинности (Database Name And Authentication). В этом упражнении вы используете значения по умолчанию для этих опций.
10. В разделе Сервер поиска (Search Server) выберите Server2. Чтобы начать процесс создания сайта, щелкните кнопку ОК. Процесс может выполняться несколько минут — в зависимости от производительности и выполнения других действий на сервере.
11. После завершения процесса вы увидите страницу Приложение создано (Application Created). Щелкните ссылку Создание семейства веб-узлов (Create Site Collection), чтобы начать процесс создания семейства узлов.
12. На странице Создание семейства вёб-узлов (Create Site Collection) введите в поле Название (Title) имя *Contoso Meetings*.
13. В разделе Выбор шаблона (Template Selection) выберите вкладку Собрания (Meetings), а затем в списке выберите элемент Рабочая область для собраний — Решения (Decision Meeting Workspace).
14. В разделе Главный администратор семейства веб-узлов (Primary Site Collection Administration) введите в поле Имя пользователя (User Name) имя, которое вы использовали для входа на сервер на шаге 1.

15. Чтобы начать процесс создания семейства узлов, щелкните OK.
16. На странице Узел верхнего уровня успешно создан (Top-Level Site Successfully Created) будет указан URL, который можно использовать для получения доступа к новому сайту. Щелкните эту ссылку и укажите свои учетные данные.
17. Теперь вы можете получить доступ к новому сайту SharePoint с именем Contoso Meetings. По умолчанию сайт включает множество элементов, в том числе: Повестка (Agenda), Задачи (Objectives) и Библиотека документов (Document Library). При желании вы можете создать новые элементы и выгрузить файлы на сайт. Кроме того, запомните URL для нового сайта, если вы планируете посетить его позже.
18. Закройте Internet Explorer и выйдите с сервера Server2.

Упражнение 2. Резервное копирование и восстановление сайта Windows SharePoint

В этом упражнении вы создадите на локальном компьютере резервную копию конфигурации сайта WSS. Затем вы восстановите сайт Contoso Meetings, который создали в упражнении 1 (предполагается, что вы выполнили предыдущее упражнение). Поскольку содержимое и параметры конфигурации будут переписаны в процессе восстановления, рекомендуется выполнять это упражнение на тестовом компьютере.

1. Войдите на сервер Server2 в качестве пользователя с привилегиями администратора.
2. С помощью Проводника Windows (Windows Explorer) создайте новую папку для хранения резервной копии. Папку можно разместить в любом томе сервера. Запомните полный путь к папке, поскольку он вам потребуется в дальнейшем.
3. Откройте веб-сайт Центр администрирования SharePoint (SharePoint Central Administration Web-site), щелкнув значок Центр администрирования SharePoint 3.0 (SharePoint 3.0 Central Administration) в группе программ Администрирование (Administrative Tools).
4. Введите учетные данные, которые вы использовали для входа на сервер на шаге 1. В Internet Explorer откроется веб-сайт Центр администрирования SharePoint (SharePoint Central Administration).
5. Перейдите на вкладку Операции (Operations). В разделе Резервное копирование и восстановление (Backup And Restore) щелкните ссылку Выполнение резервного копирования (Perform A Backup).
6. На странице Выбор компонента для резервного копирования (Select Component To Backup) выберите компонент верхнего уровня Ферма (Farm). При этом будет автоматически выбрано все содержимое сервера, включая все сайты SharePoint. Щелкните Параметры резервного копирования (Continue To Backup Options).
7. На странице Выбор параметров резервного копирования (Select Backup Options) оставьте параметры по умолчанию в разделах Содержимое резервной копии (Backup Content) и Тип резервного копирования (Type Of Backup).

В разделе Местоположение резервных копий (Backup File Location) введите полный путь к папке, созданной на шаге 2. Обратите внимание на оценку объема требуемого дискового пространства в нижней части страницы. Щелкните ОК.

8. Процесс резервного копирования начнется автоматически. Для просмотра состояния выполнения процесса щелкайте ссылку Обновить (Refresh). Страница автоматически обновляется каждые несколько секунд. Дождитесь завершения процесса резервного копирования.
9. Чтобы начать процесс восстановления сайта SharePoint, в Центре администрирования SharePoint щелкните вкладку Операции (Operations). В разделе Резервное копирование и восстановление (Backup And Restore) щелкните ссылку Восстановление из резервной копии (Restore From Backup).
10. В поле Местоположение резервной копии (Backup File Location) должен автоматически быть указан путь к папке, созданной на шаге 2. Если он не указан, введите путь вручную. Щелкните кнопку ОК.
11. На странице Выбор резервной копии для восстановления (Select Backup To Restore) выберите созданную резервную копию. Если в списке представлено множество копий, вы можете определить нужную копию на основе данных Время начала (Start Time) и Дата завершения (Finish Time). Щелкните ссылку Продолжить восстановление (Continue Restore Process).
12. На странице Выбор компонента для восстановления (Select Component To Restore) выберите новый сайт SharePoint, созданный в упражнении 1. Вы можете идентифицировать его по имени и номеру порта. Отметим, что элемент База данных содержимого (Content Database) для сайта будет выбран автоматически. Щелкните ссылку Продолжить восстановление (Continue Restore Process).
13. На странице Выбор параметров восстановления (Select Restore Options) выберите в разделе Параметры восстановления (Restore Options) опцию Та же самая конфигурация (Same Configuration). В окне появившегося предупреждения о перезаписи существующего сайта щелкните ОК. Отметим, что вы также можете восстановить сайт в другой базе данных, чтобы создать копию без перезаписи текущей версии. Щелкните ОК.
14. Процесс восстановления начнется автоматически. Для просмотра состояния выполнения процесса можно щелкать кнопку Обновить (Refresh). После завершения процесса на сервере должно быть восстановлено все содержимое сайта SharePoint. При желании вы можете проверить доступ к сайту, открыв Internet Explorer и указав URL сайта.
15. Закройте все открытые окна браузера и выйдите с сервера Server2.

Резюме

- Службы WSS можно использовать в автономной конфигурации или ферме серверов.
- Веб-сайт Центр администрирования SharePoint (SharePoint Central Administration) обеспечивает возможности управления сайтами, семействами узлов и связанными параметрами конфигурации.

- После установки WSS следует проверить или обновить параметры электронной почты, ведения журналов и сбора данных статистики использования.
- Утилиту командной строки Stsadm.exe можно применять для выполнения распространенных административных задач без использования Центра администрирования SharePoint.
- Для разделения содержимого на основе потребностей пользователей можно создавать множество подузлов и семейств веб-узлов.
- С помощью шаблонов квот можно указать максимальный объем дискового пространства, используемый семейством узлов.
- В архитектуре SharePoint можно использовать несколько методов проверки подлинности.
- Чтобы получить возможность добавлять новые операционные компоненты в сайты и веб-приложения SharePoint, нужно установить шаблоны приложений.

Закрепление материала

Приведенные ниже вопросы можно использовать для проверки знаний, полученных в ходе занятия 1. Эти вопросы представлены также в электронном виде на прилагаемом к книге компакт-диске.

ПРИМЕЧАНИЕ Ответы
Ответы и пояснения к каждому их варианту размещены в разделе «Ответы» в конце книги.

1. Будучи системным администратором, вы добавляете на компьютер Windows Server 2008 роль сервера Windows SharePoint Services (WSS). Исходная установка сервера выполнена, но никакие роли и компоненты еще не добавлены. Исходя из технических требований, вы решили установить WSS в конфигурации фермы серверов. Какая из следующих зависимостей не имеет отношения к роли сервера WSS? (Укажите все варианты.)
   А. Служба ролей Внутренняя база данных Windows (Windows Internal Database).
   Б. Служба активации Windows (Windows Process Activation Service).
   В. Microsoft .NET Framework 3.0.
   Г. Веб-сервер (IIS) (Web Server (IIS)).
   Д. Файловый сервер (File Server).
2. Вы являетесь системным администратором и отвечаете за развертывание Windows SharePoint Services (WSS) с целью обеспечения доступа пользователей внешнего бизнес-партнера. Вы установили соответствующую роль сервера и проверили загрузку веб-сайта SharePoint с локального сервера. При установке использовались опции по умолчанию. Внешние пользователи жалуются, что не могут войти на сайт. Какие из следующих изменений помогут решить проблему?
   А. Создание для внешних пользователей нового сайта в существующем семействе узлов.
   Б. Создание для внешних пользователей нового семейства узлов.

В. Назначение для веб-приложения режима проверки подлинности Формы (Forms).

Г. Модификация параметров Разрешения пользователя для веб-приложения (User Permissions For Web Applications).

Д. Модификация для созданного по умолчанию веб-приложения параметров Шаблон квот (Quota Template).

Закрепление материала главы

Для того чтобы попрактиковаться и закрепить знания, приобретенные в ходе изучения представленного в данной главе материала, вам необходимо:

- ознакомиться с резюме главы;
- повторить используемые в главе основные термины;
- выполнить задания лабораторной работы, которые моделируют реальные ситуации, требующие применения полученных знаний;
- выполнить рекомендуемые упражнения;
- сдать пробный экзамен с помощью тестов.

Резюме главы

- Службы Windows SharePoint Services включают веб-сайт по умолчанию и веб-сайт Центр администрирования SharePoint (SharePoint Central Administration Web-site).
- Службы Windows SharePoint Services можно развернуть в автономной конфигурации одного сервера или в конфигурации серверов фермы.
- Администраторы могут создавать сайты, семейства узлов и веб-приложений, а также управлять ими с помощью Центра администрирования SharePoint (SharePoint Central Administration).
- Веб-приложения могут использовать собственные параметры безопасности и проверки подлинности в соответствии с требованиями организации.

Основные термины

Проверьте, знаете ли вы. что означают перечисленные ниже термины (свои ответы можно сверить с определениями, содержащимися в конце книги):

- шаблоны приложений;
- шаблоны квот;
- ферма серверов;
- Центр администрирования SharePoint;
- семейство узлов;
- автономная конфигурация сервера;
- stsadm;
- веб-приложение;
- Внутренняя база Windows;
- Службы Windows SharePoint Services (WSS).

Лабораторная работа

В следующих заданиях вы примените знания, полученные в этой главе. Ответы находятся в разделе «Ответы» в конце книги.

Задание 1. Развертывание Windows SharePoint Services

Вы являетесь системным администратором и отвечаете за работу Windows SharePoint Services на семи компьютерах Windows Server 2008. Для хранения данных конфигурации и содержимого сайтов ваша организация планирует использовать единую серверную базу данных. На шести серверах требуется создать несколько семейств узлов и веб-приложений.

1. Какую опцию развертывания следует использовать при установке Windows SharePoint Services на компьютерах?
2. Как автоматизировать процесс создания семейств узлов и веб-приложений?

Задание 2. Управление Windows SharePoint Services

Вы являетесь системным администратором и отвечаете за управление существующим сервером Windows SharePoint Services (WSS). На сервере отконфигурировано несколько сайтов и семейств узлов. Сервер WSS входит в домен Active Directory, где все пользователи располагают индивидуальными учетными записями. Пользователи несколько месяцев могли получать доступ к сайту, однако начали жаловаться на неполадки. Пользователи некоторых веб-приложений SharePoint сообщили, что при подключении к определенным сайтам им всегда приходится указывать пользовательское имя и пароль. Кроме того, раньше сервер WSS становился недоступным в случае нехватки свободного дискового пространства. И наконец, некоторые пользователи хотели бы иметь возможность создавать собственные сайты, не обращаясь в отдел IT.

1. Как нужно отконфигурировать параметры проверки подлинности в соответствии с пользовательскими требованиями?
2. Как на сервере WSS предотвратить возникновение проблем, связанных с нехваткой дискового пространства?
3. Какой из самых простых методов нужно применить, чтобы разрешить пользователям создавать собственные сайты SharePoint?

Рекомендуемые упражнения

Чтобы успешно справиться с экзаменационными заданиями, выполните следующие упражнения.

Реализация служб Windows SharePoint Services и управление ими

В следующих упражнениях вы попрактикуетесь в настройке служб WSS и управлении ими.

- **Упражнение 1** В Центре администрирования SharePoint создайте новое семейство узлов. Выберите один из встроенных шаблонов приложений, чтобы настроить содержимое по умолчанию. Добавьте второй сайт в то же семейство

и обратите внимание на изменения в панели навигации. Загрузите и установите новые шаблоны приложений Microsoft. Создайте новый сайт, использующий один из шаблонов, и с помощью веб-браузера протестируйте включенную функциональность.

- **Упражнение 2** На тестовом сервере WSS попрактикуйтесь в резервном копировании и восстановлении данных конфигурации. Вначале восстановите параметры конфигурации существующего сайта и проверьте, восстановлена ли ранняя версия содержимого. Затем с помощью процесса резервного копирования и восстановления создайте вторую копию семейства узлов SharePoint, восстановив ее с использованием параметров другого сайта.
- **Упражнение** 3 Найдите дополнительные сведения на прилагаемом CD или по указанным ниже URL-адресам.

  Windows SharePoint Services TechCenter: *http://technet.microsoft.com/ru-ru/windowsserver/sharepoint/default.aspx.*

  Microsoft TechNet Virtual Labs: SharePoint Products and Technologies: *http://technet.microsoft.com/ru-ru/bb512933.aspx.*

  Домашняя страница Microsoft Office Windows SharePoint Services: *http://office.microsoft.com/ru-ru/sharepointtechnology/default.aspx.*

Пробный экзамен

На прилагаемом к книге компакт-диске представлено несколько вариантов тренировочных тестов. Проверка знаний выполняется только по одной или же по всем экзаменационным темам сертификационного экзамена 70-643. Тестирование можно организовать таким образом, чтобы оно проводилось как экзамен, или же настроить его на изучение — в этом случае вы сможете после каждого своего ответа на вопрос просматривать правильные ответы и объяснения.

ПРИМЕЧАНИЕ Пробный экзамен

Подробнее о пробном экзамене рассказано во введении к данной книге.

ПРИЛОЖЕНИЕ

Развертывание Windows Server 2008

Ниже представлены дополнительные сведения о развертывании Windows Server 2008. Хотя данное приложение создавалось с целью содействия в проведении реального развертывания, излагаемую информацию можно использовать для подготовки к сдаче сертификационного экзамена 70-643.

Существуют различные технологии развертывания Windows Server 2008, начиная с ручной установки продукта с DVD-диска и заканчивая автоматизированным развертыванием с помощью пакета Windows Automated Installation Kit (Windows AIK), инструментария Microsoft Windows Deployment Services (WDS) и Microsoft System Center Configuration Manager 2007. Выбор технологии зависит от размеров организации и ее потребностей в автоматизации процесса развертывания.

Технологии развертывания Windows

Прежде чем приступать к выбору средства или платформы для развертывания серверов, нужно ответить на ряд ключевых вопросов.

- Какими будут масштабы развертывания? Необходимо развернуть много серверов или можно обойтись несколькими? Использование технологий крупномасштабного развертывания для установки множества серверов означает, что вам придется потратить много времени на изучение этих технологий и на работу с ними. К тому же технологии крупномасштабного развертывания могут очень дорого обходиться, особенно с учетом лицензирования. Применение же технологий мелкомасштабного развертывания для установки тысяч серверов может отнять еще больше времени, поскольку требует многократного выполнения операций установки на множестве компьютеров; при этом существует большая вероятность допущения различного рода ошибок.
- Насколько критично для организации время развертывания? Если времени хватает, установку десятков серверов можете выполнить вручную или делегировать эту задачу местным администраторам. Если же время развертывания ограничено, то лучше воспользоваться файлами ответов, позволяющими выполнять установку без участия пользователя.
- Каким образом должны настраиваться развертываемые серверы? Если все серверы будут развернуты на идентичном оборудовании с одинаковыми

ролями, то выполнение развертывания на основе образа без участия пользователя может сэкономить много времени и усилий. Однако если все серверы развертываются на уникальном оборудовании с различными наборами ролей, то имеет смысл комбинировать установку вручную и установку без участия пользователя.

Отвечая на эти вопросы и учитывая условия среды, вы должны выбрать наиболее подходящий инструмент для развертывания Windows Server 2008. Такие мощные и сложные платформы, как System Center Configuration Manager, •лучше всего использовать в крупных организациях, располагающих временем, средствами и персоналом для надлежащего применения возможностей платформы. Поэтому при выборе оптимальной технологии развертывания, вы должны определить, которая из них более всего соответствует потребностям и возможностям организации.

Далее мы рассмотрим различные технологии и платформы, используемые для развертывания Windows Server 2008.

Установка сервера вручную

Чтобы установить систему Windows Server 2008 вручную, вставьте DVD-диск продукта в DVD-привод компьютера, скопируйте содержимое DVD в общий сетевой ресурс и после загрузки предыдущей операционной системы на компьютере удаленно запустите файл Setup.exe. Вы также можете загрузить предустановочную среду Windows Preinstallation Environment (Windows PE) с DVD-диска.

Пакет Windows AIK

Пакет Windows AIK содержит набор средств и документацию, с помощью которых администраторы и независимые производители оборудования OEM (Original Equipment Manufacturer) могут выполнять автоматизированную установку Windows Server 2008, Windows Vista и некоторых предшествующих им версий, включая Microsoft Windows Server 2003 и Windows XP.

ВНИМАНИЕ Версии Windows AIK

Для развертывания Windows Server 2008 необходимо использовать самую последнюю версию Windows AIK. На время написания данной книги использовалась версия Windows AIK 1.1, с помощью которой можно развертывать Windows Server 2008 и Windows Vista с пакетом обновлений Service Pack 1.

Инструментарий Windows Deployment Services

Инструментарий WDS содержит набор компонентов, заменяющих процедуры Remote Installation Services (RIS) — технологии развертывания, которая была включена в Windows 2000 Server. Версия Windows Server 2008 включает роль сервера Службы развертывания Windows (Windows Deployment Services), которую можно добавить с помощью диспетчера сервера. Инструментарий WDS обеспечивает возможность использования технологии развертывания серверов на основе образов, которая предназначена для организаций средних размеров и позволяет автоматизировать развертывание рабочих станций и серверов.

Инструментарий Microsoft Deployment

Инструментарий Microsoft Deployment предоставляет в ваше распоряжение самую последнюю версию Microsoft Solution Accelerator для пакета Business Desktop Deployment (BDD).

Решения Microsoft Solution Accelerator обеспечивают эффективное планирование, построение, тестирование и развертывание платформ и продуктов Microsoft. Набор средств Microsoft Deployment позволяет оптимальным образом выполнять развертывание серверов Windows, клиентов Windows, а также пакета Microsoft Office 2007.

Отметим, что инструментарий Microsoft Deployment предназначен в первую очередь для небольших и средних организаций и содержит инструменты, сценарии, шаблоны, документацию, позволяющие администраторам планировать развертывание системы, обеспечивать и тестировать совместимость приложений, настраивать и паковать приложения для развертывания, а также автоматизировать развертывание настольных систем на основе образов. Все эти задачи набор средств Microsoft Deployment позволяет выполнять в централизованном автоматизированном приложении, в которое интегрированы следующие инструменты:

- Windows AIK;
- Application Compatibility Toolkit;
- User State Migration Tool:
- WDS.

В Microsoft Deployment также поддерживается интеграция с Microsoft System Center Configuration Manager 2007 и обеспечивается возможность определения автоматизированной роли сервера с использованием диспетчера сервера Windows Server 2008.

Microsoft System Center Configuration Manager 2007

Программный пакет Microsoft System Center Configuration Manager 2007 является последней версией Microsoft Systems Management Server (SMS) и использует автоматизацию на основе политик для управления полными жизненными циклами развертывания, обновления и расширения серверов, клиентов и мобильных устройств в физических, виртуальных, распределенных и мобильных системах. Платформа Configuration Manager уровня Enterprise Class входит в семейство продуктов Microsoft System Center, включающих Microsoft System Center Operations Manager 2007, Microsoft System Center Data Protection Manager 2007 (DPM), Microsoft System Center Virtual Machine Manager 2007 и некоторые другие продукты, позволяющие корпоративным подразделениям управлять ресурсами и жизненными 1Т-циклами.

К СВЕДЕНИЮ System Center Configuration Manager 2007

В данной книге не описывается развертывание Windows Server 2008 с использованием System Center Configuration Manager 2007. Более подробные сведения о семействе продуктов Configuration Manager и System Center можно найти по адресу *http://www.microsorft.com/systemcenter/*.

Проверьте себя

- Какая технология развертывания интегрирует инструменты, шаблоны, сценарии и документацию для развертывания настольных и серверных версий Windows в небольших и средних организациях?

Ответ

- Инструментарий Microsoft Deployment.

Использование Windows AIK

Как мы уже говорили ранее, пакет Windows AIK содержит набор инструментов для развёртывания последней версии Windows. В Windows AIK включены следующие средства.

- **Windows System Image Manager (Windows SIM)** Позволяет создавать файлы ответов (unattend.xml) и дистрибутивные общие ресурсы для выполнения автоматизированной установки Windows.
- **Windows Preinstallation Environment (Windows PE)** Дает возможность загружать системы Bare-Metal (системы, запускающиеся на голой конфигурации оборудования) и в них развертывать Windows.
- **ImageX** Позволяет захватывать, модифицировать и применять файловые образы для быстрого развертывания.

Помимо этих инструментов установка Windows AIK также обеспечивает возможность пользоваться следующими средствами.

- Средства Windows Recovery Environment (Windows RE), предназначенные для построения решений диагностики и восстановления на основе среды Windows PE.
- Дополнительные инструменты командной строки, включая Pkgmgr.exe, PEImg.exe и другие. Эти инструменты описаны далее.
- Документация в виде файлов справки Windows (.chm).

К СВЕДЕНИЮ Встроенные средства

В процессе развертывания можно также использовать встроенные инструменты операционной системы, включая средства DiskPart, BCDEdit и некоторые другие. Эти инструменты описаны в следующем разделе и в разделе Line Tools Technical Reference руководства User's Guide пакета Windows Automated Installation Kit (Windows AIK).

Тем не менее для реализации реального развертывания перечисленных здесь инструментов Windows AIK недостаточно. Этим инструментам требуется взаимодействовать с другими технологиями и компонентами Windows, включая следующие.

- **Windows Setup** Программа, которая устанавливает Windows в системе Bare-Metal (запускается на голой конфигурации оборудования) или при обновлении предыдущей версии Windows до новой версии.

- **Файл образа Windows Image (.wim)** Единый сжатый файл, используемый для дублирования пакета установки Windows в томе диска.
- **Службы развертывания Windows (Windows Deployment Services, Windows DS, WDS)** Этот опциональный компонент используется для установки Windows Server 2008 и Windows Vista или удаленной установки Windows Server 2008 без необходимости в физическом взаимодействии с каждым конечным компьютером.

Архитектура платформ развертывания Windows Server 2008 и Windows Vista показана на рис. П-1.

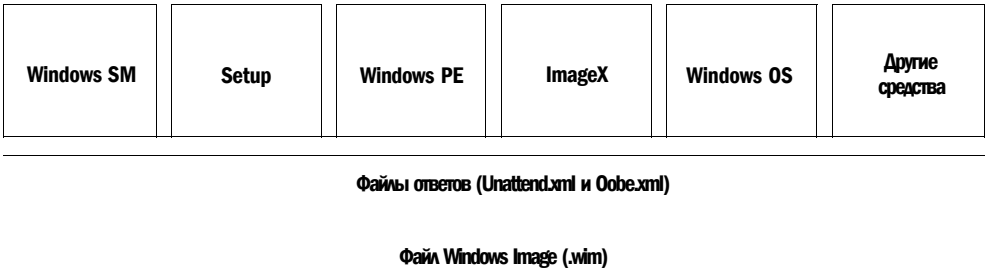


Рис. П-1. Архитектура платформ развертывания Windows Server 2008 и Windows Vista

ПРИМЕЧАНИЕ Поддерживаемые версии Windows
Большая часть информации, касающейся развертывания Windows Server 2008, также может использоваться при развертывании настольных систем Windows Vista, поскольку с помощью версии Windows AIK 1.1 можно устанавливать обе системы, Windows Server 2008 и Windows Vista. Все ссылки по установке Windows Server 2008 также могут быть применимы к установке Windows Vista, за исключением оговоренных случаев. Тем не менее следует помнить, что настоящее приложение посвящено развертыванию Windows Server 2008, а не Windows Vista.

Средства развертывания для различных версий Windows

В табл. П-1 характеристики различных инструментов и технологий, используемых для развертывания Windows Server 2008 и Windows Vista, даются в сравнении с характеристиками средств развертывания Windows Server 2003 и Windows XP Professional.

Если вы знакомы с основными средствами развертывания Windows Server 2003 и Windows XP, то с помощью этой таблицы сможете быстро обновить навыки развертывания и применить их по отношению к Windows Server 2008 и Windows Vista. Дополнительную информацию об этих инструментах можно найти и в руководстве User's Guide пакета Windows Automated Installation Kit (Windows AIK).

Табл. П-1. Средства и технологии, используемые при развертывании Microsoft Windows и Windows Server последних и предшествующих им версий

Windows Server 2003 и Windows XP	Windows Server 2008 и Windows Vista
Файлы ответов и средства для их создания	
Setup Manager	Windows SIM
Текстовые файлы ответов	Файлы ответов XML
Множество файлов ответов Unattent.txt Winnt.sif Winborn.ini Oobeinfo.ini Sysprep.inf	Два файла ответов Unattend.xml (или Autounattend.xml) Oobe.xml (используется в основном для Windows Vista)
Cmdlines.txt	RunSynchronous
Раздел [GUIRunOnce]	First LogonCommands
Папки OEM	Образ данных (хотя папки OEM все еще поддерживаются с использованием наборов конфигурации)
Версии Windows PE	
Windows PE 1.0	Windows PE 2.0
Инструменты для создания образов дисков	
Должны использоваться сторонние средства	ImageX
Windows Setup	
Winnt.exe и Winnt32.exe	Setup.exe
Добавление драйверов устройств	
OEMPnPDriverPath	Package Manager
Добавление языковой поддержки	
Файлы MUI	Языковые пакеты

В следующем разделе детально описаны различные инструменты Windows AIK и улучшения этих средств, появившиеся в версии Windows AIK 1.1.

Диспетчер Windows SIM и файлы ответов

С помощью диспетчера Windows System Image Manager (SIM) можно не только создавать файлы ответов, используемые для выполнения автоматизированной установки Windows, но и управлять таковыми. Диспетчер Windows SIM обеспечивает графический пользовательский интерфейс (рис. П-2), в котором можно создавать новые файлы ответов и настраивать параметры установки Windows.

Консоль Windows SIM содержит пять панелей.

- **Distribution Share (Дистрибутивный общий ресурс)** Отображает каталог текущего открытого дистрибутивного общего ресурса и его папки. В этой

панели можно выбирать, создавать, развертывать и закрывать каталоги дистрибутивных общих ресурсов, а также добавлять элементы из открытого дистрибутивного общего ресурса в файл ответов. Дистрибутивные общие ресурсы обсуждаются далее в этом разделе.

Windows Image (Образ Windows) Содержит текущий открытый файл Windows Image (.wim), а также компоненты и пакеты этого файла, доступные для установки. Обычно файл .wim открывают перед созданием файла ответов для выполнения автоматизированной установки Windows. Далее в этом разделе мы поговорим о файлах .wim более подробно.

Answer File (Файл ответов) Отображает фазы установки, выполняемые программой Windows Setup, а также все параметры файла ответов, добавленные для обработки в каждой фазе.

Properties (Свойства) Сохраняет свойства параметров файла ответов, которые можно конфигурировать в панели Answer File.

Messages (Сообщения) Служит для отображения информационных сообщений о корректности синтаксиса XML-файла ответов, его параметров для устанавливаемой версии Windows, а также сообщений других типов.

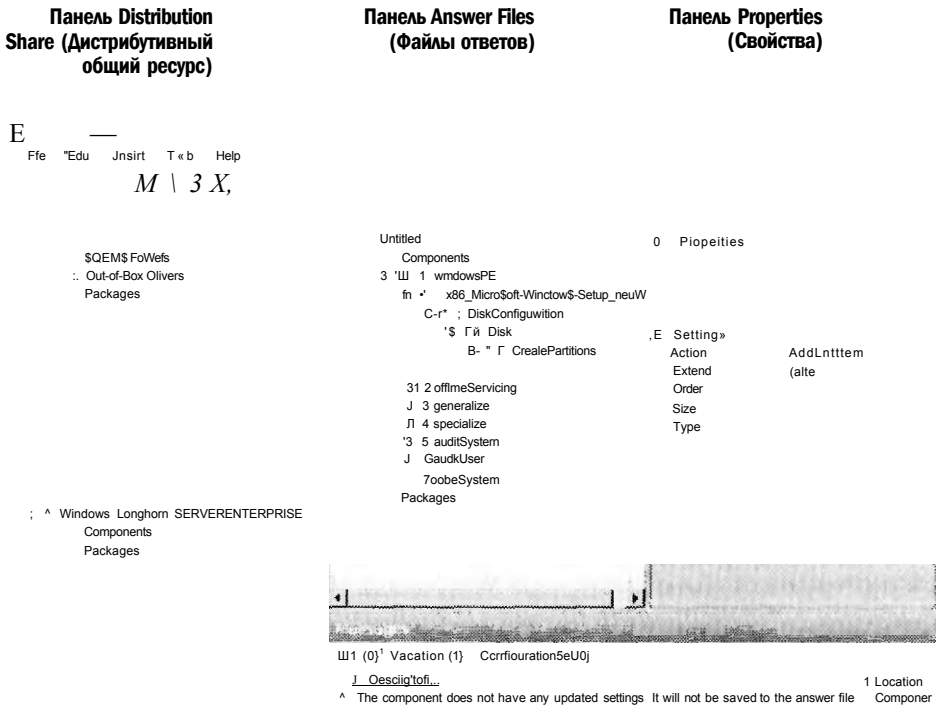


Рис. П-2. Интерфейс Windows SIM

Вот какие операции можно выполнить с помощью Windows SIM:

- создать новый файл ответов, отконфигурировать параметры компонентов и пакетов, чтобы эти параметры были обработаны в отдельной фазе конфигурации;
- модифицировать параметры существующего файла ответов;
- добавить в файл ответов драйверы сторонних производителей, приложения и другие пакеты;
- подтвердить корректность синтаксиса и приемлемость параметров файла ответов для развертываемой версии Windows;
- создать дистрибутивный общий ресурс для выполнения автоматизированной установки Windows в сети;
- создать конфигурационный набор для выполнения автоматизированной установки Windows в случае недоступности сети.

Согласно терминологии Windows, *компонент* — это часть операционной системы Windows с файлами, ресурсами и параметрами для конкретного набора функций Windows. Многие компоненты содержат параметры автоматизированной установки, которые можно использовать для их настройки во время установки Windows. *Пакетом* называют группу файлов, которую можно использовать для модификации некоторого компонента Windows. В качестве примеров пакетов можно привести пакеты обновлений (Service Pack), обновления системы безопасности, языковые пакеты и пакеты исправления ошибок. Пакеты также могут содержать параметры автоматизированной установки, которые можно использовать для их настройки во время установки Windows.

При настройке параметра автоматизированной установки для компонента или пакета нужно также выбрать этап настройки, на котором будет выполняться обработка этого параметра. Под *этапом настройки* подразумевается стадия установки Windows. В программу Setup версии Windows Server 2008 включено семь этапов настройки, которые можно использовать во время установки. На различных этапах настройки устанавливаются разные элементы операционной системы Windows, причем обработку параметра автоматизированной установки можно при необходимости назначить на нескольких этапах настройки.

Дистрибутивный общий ресурс — это набор папок для хранения драйверов сторонних производителей, приложений и таких пакетов Microsoft, как обновления программного обеспечения и пакеты обновлений Service Pack. Дистрибутивные общие ресурсы являются опциональными. Их можно создавать на компьютере с помощью диспетчера Windows SIM, а также вручную. *Конфигурационным набором* принято называть автономный файл вместе со структурой папок, содержащий лишь те файлы, которые нужны для управления процессом установки. По сути, конфигурационный набор представляет собой уменьшенную версию дистрибутивного общего ресурса. Его можно хранить в общем сетевом ресурсе или копировать на переносной накопитель для установки Windows на компьютере, не подключенном к сети. Файлы конфигурационного набора содержат информацию, аналогичную данным в дистрибутивном общем ресурсе, однако хранятся в двоичном формате.

Дистрибутивные общие ресурсы и конфигурационные наборы можно использовать вместе с файлами ответов для выполнения автоматизированной установки Windows в системах Bare-Metal (компьютеры с без какого-либо про-

граммного обеспечения) через сеть. Структура папок дистрибутивного общего ресурса, созданная с помощью Windows SIM, показана на рис. П-3.

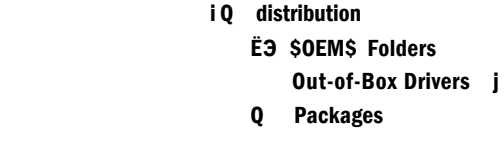


Рис. П-3. Структура папок дистрибутивного общего ресурса

Далее приведен перечень папок каталога дистрибутивного общего ресурса с кратким описанием их содержимого.

- **Папка OEM** Содержит файлы, используемые для отображения торговой марки настраиваемых приложений и их добавления в установку Windows. Эта старая технология развертывания все еще поддерживается в Windows Server 2008, однако новые файлы и ресурсы удобней добавлять в установку Windows с помощью образов данных. *Образ данных* — это дополнительный файл .wim, содержащий приложения, файлы и другие вспомогательные ресурсы главного файла .wim, используемого для установки самой системы Windows. Чуть позже мы поговорим о файлах .wim более подробно.
- **Папка Out-of-Box Drivers** Содержит дополнительные драйверы устройств, которые будут установлены программой Windows Setup.
- **Папка Packages** Содержит обновления программного обеспечения Windows — пакеты обновлений Service Pack, языковые пакеты, обновления системы безопасности и т. д. Пакеты в эту папку нужно импортировать с помощью Windows SIM. После импорта с использованием Windows SIM пакет можно добавить в установку и отконфигурировать все его параметры.

Программа Windows Setup и драйверы устройств

Иногда для успешной установки Windows требуются дополнительные драйверы устройств. Очень важно понимать разницу между типами драйверов устройств и знать, как они добавляются в установку Windows.

- **Встроенные драйверы (In-box)** Обычно это драйверы с файловым расширением .inf, включенные в саму систему Windows. Еще один тип встроенных драйверов устанавливается с помощью MSI-файла установщика Windows. Этот тип драйверов добавляется методом, который используется для добавления приложений в установку.
- **Дополнительные драйверы (Out-of-box)** Дополнительные драйверы .inf, добавляемые в Windows Setup с помощью Windows SIM. Драйверы Out-of-box должны содержаться в папке Out-of-Box Drivers дистрибутивного общего ресурса. Как правило, их обработка выполняется на фазе конфигурации auditSystem процесса Setup. Еслн драйверы Out-of-box играют критически важную роль при загрузке, как, скажем, драйверы, требуемые для успешной загрузки самой системы, их нужно добавить в фазу конфигурации windowsPE, а не конфигурировать в компоненте Windows-PnpCustomizationsWinPE с помощью Windows SIM.

С помощью Windows SIM создаются файлы ответов XML, содержащие определения и значения различных параметров, конфигурирование которых осуществляется в автоматизированной установке Windows. Далее описаны файлы ответов.

- **Unattend.xml** Файл ответов, используемый в большинстве типов автоматизированной установки Windows Server 2008. Единый файл ответов Unattend.xml управляет практически всеми фазами процесса автоматизированной установки. В предыдущих версиях Windows, в частности в Windows Server 2003 и Windows XP Professional, для управления различными фазами процесса установки использовалось множество типов файлов ответов.
- **Autounattend.xml** Файл ответов, используемый для автоматизированной установки Windows путем загрузки с DVD-диска. Чтобы загрузиться с DVD-диска Windows Server 2008 и выполнить автоматизированную установку, файл ответов Autounattended.xml копируется в корневой каталог дискеты или флэш-памяти USB. Этот процесс похож (но не идентичен) на метод использования файла Winnt.sif для установки предыдущих версий Windows путем загрузки с CD-диска.

Чтобы увидеть, на что похож файл ответов XML, просмотрите различные секции файла autounattend_sample.xml в папке %ProgramFiles%\Windows AIK\Samples:

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
   <settings pass="Windows PE">
      <component name="Microsoft-Windows-Setup" processorArchitecture="x86"
publicKeyToken="31bf3856ad364e35" landuade="neutral" versionScope="nonSxS"
xmlns:wcm=http://schemas.microsoft.com/WMIConfig/2002/State
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance>
```

После этой заголовочной информации, определяющей параметры и фазу конфигурации, в которой будет выполняться их обработка (Windows PE), а также архитектуру системы развертывания Windows (x86), следует описание схемы разбиения и форматирования дисков:

```
<DiskConfiguration>
   <Disk>
      <CreatePartitions>
         <CreatePartition wcm:action="add">
            <0rder>1</0rder>
            <Size>20000</Size>
            <Type>Primary</Type>
         </CreatePartition>
      </CreatePartitions>
      <ModifyPartitions>
         <ModifyPartition wcm:action="add">
            <Active>true</Active>
            <Extend>false</Extend>
            <Format>NTFS</Format>
            <Label>OS_Install</Label>
            <Letter>C</Letter>
```

```
            <0rder>1</0rder>
            <PartitionID>1</PartitionID>
         </ModifyPartition>
      </ModifyPa rtitions>
      <DiskID>0</DiskID>
      <WillWipeDisk>true</WillWipeDisk>
   </Disk>
   <WillShowUI>OnError</WillShowllI>
</DiskConfiguration>
```

Затем, в следующей секции, указан ключ продукта, который будет использоваться для установки и принятия условий лицензионного соглашения EULA (End-User Licensing Agreement).

```
<UserData>
   <ProductKey>
      <Key>&lt;productkey&gt;</Key>
      <WillShowUI>OnError</WillShowllI>
   </ProductKey>
   <AcceptEula>frue</AcceptEula>
</UserData>
```

Далее программе Setup дается указание установить Windows в ранее созданном разделе.

```
   <lmagelnstall>
      <0SImage>
         <InstallTo>
            <DiskID>0</DiskID>
            <PartitionID>1</PartitionID>
         </InstallTo>
         <WillShowUI>OnErro.r</WillShowllI>
      </0SImage>
   </ImageInstall>
</component>
```

После этого следуют параметры для еще одного компонента, указывающие, что во время установки будет использоваться язык U.S English.

```
              <component  name="Microsoft-Windows-International-Core-WinPE"
processorArchitecture="x86"  publicKeyToken="31bf3856ad364t35"
language="neutral"  versionScope="nonSxS"
xmlns:wcm=http://schemas.mic rosoft.com/WMIConfig/2002/State
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance>
                     <SetupUILanguage>
                              <UILanguage>en-us</UILanguage>
                     </SetupUILanguage>
                     <InputLocale>0409:0DD00409</InputLocale>
                     <SystemLocale>en-us</SystemLocale>
                     <UILanguage>en-us</UILanguage>
                     <UserLocale>en-US</UserLocale>
              </component>
         </settings>
```

Следующая секция содержит параметры, обработка которых будет выполняться в фазе конфигурации oobeSystem. Эти параметры будут применены во время первой загрузки. В секции указано, что Sysprep следует запустить в режиме аудита для вторичного уплотнения системы перед передачей управления пользователю:

```
   <settings pass="oobeSystem">
      <component name="Microsoft-Windows-Deployment"
processorArchitecture="x86" publicKeyToken="3"1bf3856ad364t35"
language="neutral" versionScope="nonSxS"
xmlns:wcm=http://schemas.microsoft.com/WMIConfig/2002/State
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance>
            <Reseal>
                  <Mode>Audit</Mode>
            </Reseal>
      </component>
   </settings>
```

Последняя секция содержит параметры, обработка которых будет выполняться в фазе конфигурации specialize, где применяются машинные данные для образа. Изготовитель оборудования OEM может указать в этой секции модель системы и предоставить для конечных пользователей телефон поддержки. Корпоративные пользователи могут указать в этой секции контактную информацию для руководителей подразделений или URL-адреса веб-сайтов поддержки в интрасети корпорации.

```
      <setting pass="specialize'^
         <component name="Microsoft-Windows-Shell-Setup"
processorArchitecture="x86" publicKeyToken="31bf3856ad364t35"
language="neutral" versionScope="nonSxS"
xmlns:wcm=http://schemas.microsoft.com/WMIConfig/2002/State
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance>
            <OEMInformation>
               <Manufacturer>&lt;manufacturer&gt;</Manufacturer>
               <Model>&lt;model&gt:</Model>
               <SupportHours>&lt;support hours&gt;</SupportHours>
               <SupportPhone>&lt;support phone&gt;</SupportPhone>
            </OEMInformation>
         </component>
      </settings>
<cpi:offlinelmage cpi:source="catalog:c:/daninstall_windows vista
Ultimate.clg" xmlns:cpi="urn:schemas-microsoft-com:cpi" />
</unattend>
```

К СВЕДЕНИЮ Файлы ответов и Windows SIM

Дополнительную информацию о Windows SIM можно найти в разделе Deployment Tools Technical Reference справочного файла WAIK.chm пакета Windows AIK. Детальные сведения об отдельных параметрах файла ответов имеются в документации Unattended Windows Setup Reference пакета Windows AIK.

Проверьте себя

1. Чем файл Autounattend.xml похож на файл Winnt.sif?
2. Чем отличаются эти файлы?

Ответы

1. Оба файла являются текстовыми и их можно использовать для выполнения автоматизированной установки Windows с носителя.
2. Файл Winnt.sif использовался в старой технологии для установки Windows 2000, Windows XP и Windows Server 2003. Файл Autounattend.xml предназначен для установки Windows Vista и Windows Server 2008. Еще одно отличие состоит в том, что файл Autounattend.xml использует синтаксис XML, а файл Winnt.sif состоит из заголовков секций, параметров и значений для этих параметров.

Среда Windows PE

Предустановочная среда Windows Preinstallation Environment (Windows PE) представляет собой минимальную (неполную) версию Windows на основе ядра Windows Vista (идентичного ядру Windows Server 2008) и может использоваться для развертывания системы и устранения возникающих при этом неполадок. В частности, с помощью Windows PE можно выполнять следующие задачи.

- **Загрузка системы Bare-Metal для установки Windows** С применением Windows PE можно загрузить систему (рис. П-4), разбить и отформатировать жесткие диски и подключиться к дистрибутивному общему ресурсу в сети для копирования образов диска и установки Windows в автоматизированном или ручном режиме.

Рис. П-4. Командная оболочка Windows PE

- **Устранение неполадок уже установленной системы Windows** С помощью Windows PE можно запустить инструмент Windows RE и использовать встроенные средства диагностики и устранения неполадок. Windows PE также можно использовать для построения настраиваемого решения восстановления с целью автоматической переустановки или восстановления компьютеров Windows.

Среда Windows PE также запускается при каждой установке Windows Server 2008. Графические инструменты, отображаемые во время установки, на самом деле запускаются в среде Windows PE.

Как показано на рис. **П-4,** среда Windows PE предоставляет интерфейс командной строки, из которого можно запускать различные встроенные средства для выполнения установки и устранения неполадок. Далее описаны инструменты, которые можно запускать из командной строки Windows PE.

ПРИМЕЧАНИЕ Что такое диск X
Диск X в среде Windows PE — это диск RAM (записываемый том в памяти), который используется при загрузке Windows PE с CD, DVD, USB или образа WDS. По умолчанию Windows PE выделяет для этого RAM-диска 32 Мбайта памяти, однако размер RAM-диска можно настроить с помощью утилиты PEImg.exe. В разделе «Улучшения Windows AIK 1.1» представлена более подробная информация по этой теме.

- **Boot Configuration Data** Инструмент, предназначенный для редактирования хранилища данных конфигурации загрузки (BCD), которые описывают приложения загрузки и их параметры. В Windows Vista и Windows Server 2008 хранилище BCD заменило файл Boot.ini, использовавшийся в предыдущих версиях Windows.
- **Bootsect** Средство для восстановления загрузочного сектора на компьютере путем обновления главной загрузочной записи для разделов жесткого диска с целью выбора между файлами BOOTMGR и NTLDR. Оно заменило инструменты FixFAT и FixNTFS, использовавшиеся в предыдущих версиях Windows.
- **DiskPart** Этот инструмент можно использовать для управления дисками, разделами и томами с командной строки или в автоматизированном режиме с помощью сценариев.
- **Drvload** С помощью этого средства в загружаемый образ Windows PE можно добавлять дополнительные драйверы (Out-of-box), используя в качестве входных параметров один или несколько файлов .inf.
- **Oscdimg.exe** Используется для создания файла образа (.iso) настраиваемой 32- или 64-разрядной версии Windows PE, которую можно затем записать на CD с целью создания загружаемого носителя Windows PE.
- **PEImg.exe** С помощью этого средства можно создавать или модифицировать образ Windows PE, например, импортировав пакет, установив драйвер и т.д.
- **Winpeshl.ini** Используется для настройки оболочки Windows PE по умолчанию и позволяет запускать собственное приложение оболочки вместо командной строки Windows PE по умолчанию.
- **Wpenit.exe** Используется для инициализации Windows PE при каждой загрузке Windows PE.

К СВЕДЕНИЮ Инструменты Windows PE
Более подробные сведения об инструментах командной строки Windows PE представлены в разделе Windows PE Tools Technical Reference руководства Windows Preinstallation Environment (Windows PE) User's Guide программного пакета Windows AIK.

Изначально Windows PE предназначалась для инициализации Windows Setup в системах Bare-Metal без использования сетевых загрузочных дискет MS-DOS. Первая версия Windows PE была построена на ядре Windows XP и получила название Windows PW 1.0. Параллельно с выпуском Windows Vista была также выпущена новая версия Windows PE 2.0 на основе ядра Windows Vista.

ПРИМЕЧАНИЕ Ограничения Windows PE
В среде Windows PE существует много ограничений, а следовательно, эта среда не предназначена для ежедневного использования в качестве операционной системы. Например, Windows PE автоматически прекращает работать через 72 ч и перезагружается, причем это ограничение отменить невозможно. Кроме того, все изменения, внесенные в реестр Windows PE, теряются при перезагрузке. Помимо всего прочего Windows PE не поддерживает .NET Framework, общеязыковую среду выполнения CLR (Common Language Runtime), а также приложения, упакованные в файлы установщика Windows (.msi). И наконец, Windows PE поддерживает лишь поднабор API-интерфейсов Win32, ограничивающий запуск приложений в этой среде.

Ограничения загрузочных дискет MS-DOS

В течение долгих лет администраторы использовали загрузочные дискеты MS-DOS для загрузки «голого» оборудования и выполнения автоматизированной установки операционных систем Windows по сети. Существует множество причин, по которым пришло время отказаться от подобной практики. Например, MS-DOS обладает следующими недостатками:

- минимальная сетевая поддержка;
- отсутствие поддержки файловой системы NTFS;
- отсутствие поддержки драйверов устройств для 32- и 64-разрядных версий Windows.

Вследствие этих ограничений, а также из-за утраты популярности дискет MS-DOS корпорация Microsoft разработала Windows PE как новое средство для загрузки компьютеров без установленной операционной системы. В сравнении с загрузочными дискетами MS-DOS среда Windows PE обеспечивает следующие преимущества:

- поддержка NTFS 5.x, включая поддержку возможности создания динамических томов и управления ими;
- сетевая поддержка TCP/IP, включая клиента общего доступа к файлам;
- поддержка 32- и 64-разрядных драйверов устройств в зависимости от используемой версии Windows PE;
- возможность загрузки с CD и DVD, флеш-устройств USB и удаленных образов WDS.

В Windows PE для создания и преобразования среды построения Windows PE в файл .iso, содержащий готовую к запуску операционную систему Windows, как правило, используются инструменты, включенные в Windows AIK. При необходимости в среду построения Windows PE добавляются дополнительные инструменты. Файл .iso можно записать на CD-диск с помощью программного обеспечения стороннего производителя, после чего этот загружаемый диск можно будет применить для установки операционной системы на «голом» оборудовании Bare-Metal.

ImageX и файловый формат .wim

Инструмент командной строки Image.exe позволяет управлять файлами образов Windows (.wim) при выполнении развертывания операционной системы на «голом» оборудовании. Многие системные администраторы развертывали предыдущие версии Windows с помощью программного обеспечения сторонних производителей, предназначенного для создания образов дисков. Такое программное обеспечение обычно создавало образы на основе секторов для копирования или посекторного клонирования установочных дисков Windows в новые отформатированные тома дисков конечных систем. Инструмент ImageX обеспечивает значительно большую гибкость, чем метод создания образов по секторам, начиная от ускорения развертывания за счет снижения размера образа и заканчивая автономным обслуживанием образов путем добавления, перемещения и удаления файлов из образа.

Инструмент ImageX способен работать и с другими технологиями создания образов Windows (рис. П-5).

- **Файлы образов Windows Imaging (.wim)** Коллекции файлов образов, содержащие одну или несколько операционных систем с компонентами и добавленными пакетами. Сжатый файловый формат образа диска был введен в Windows Vista.
- **Фильтр файловой системы WIM** Позволяет просматривать и редактировать содержимое файла .wim для выполнения автономного обслуживания после прикрепления файла к диску.
- **Набор API-интерфейсов WIM** Эти API-интерфейсы обеспечивают поддержку драйвера WIM FS Filter и команды ImageX. На их основе сторонние независимые поставщики программного обеспечения (ISV) могут разрабатывать инструменты развертывания, совместимые с WIM.

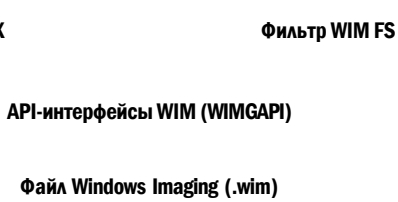


Рис. П-5. Архитектура ImageX

При использовании ImageX обычно вводится команда с одной командной опцией и дополнительной информацией. Например, команда *imagex/capture*

image_path image_file "name" **захватит на диске образ тома imagepath в файл image_file.wim с именем name.**

Далее приведены описания всех командных опций ImageX (чтобы получить подробный синтаксис любой из них, на компьютере с установленным пакетом Windows AIK необходимо ввести в командную строку Windows PE Tools Command Prompt команду *image /?).*

- */append* **Прикрепляет образ тома к существующему файлу .wim.**
- */apply* **Применяет образ тома к указанному диску.**
- */capture* **Захватывает образ тома с диска в новый файл .wim.**
- */delete* **Удаляет указанный образ тома из файла .wim, содержащего множество образов томов.**
- */dir* **Отображает список файлов и папок в указанном образе тома.**
- */export* **Экспортирует копию указанного файла .wim в еще один файл .wim.**
- */info* **Возвращает полный размер файла, индекс образа, число каталогов и файлов, описание и хранимые процедуры XML для указанного файла .wim.**
- */split* **Разбивает существующий файл .wim на множество файлов .wim, предназначенных только для чтения.**
- */mount* **Монтирует файл .wim с правом чтения в указанном каталоге, позволяя просматривать всю информацию в каталоге без права модификации.**
- */mountrw* **Монтирует файл .wim с правом чтения и записи в указанном каталоге, позволяя просматривать и модифицировать всю информацию в каталоге.**
- */unmount* **Открепляет смонтированный образ от указанного каталога.**

Инструмент Sysprep

Инструмент развертывания Sysprep.exe позволяет выполнить такие задачи:

- **удалить всю системную информацию из установки Windows для захвата ее образа с помощью ImageX и развертывания образа в других системах;**
- **конфигурировать установку Windows для загрузки в режиме Audit, чтобы установить сторонние драйверы устройств и приложения и протестировать функциональность системы перед захватом ее образа;**
- **конфигурировать установку Windows для загрузки приветствия Windows при следующем запуске компьютера (как правило, эта задача выполняется перед передачей компьютера конечному пользователю или потребителю);**
- **трижды сбрасывать активацию продукта Windows.**

ВНИМАНИЕ! Использование Sysprep

Средство Sysprep нужно использовать только в установке Windows с нуля. Инструмент Sysprep не следует использовать в существующих установках Windows. Кроме того, его нельзя использовать при обновлении существующих операционных систем до новой версии.

Команды Sysprep имеют следующий синтаксис:

```
Sysprep.exe [/oobe | /audit/] [/generalize] [/reboot | /shutdown | /quit]
[/quiet] [/unattend:answerfile]
```

Далее описаны командные опции Sysprep.

- */audit* **Перезапускает компьютер в режиме аудита, чтобы в Windows можно было добавить дополнительные драйверы и приложения и протестировать установку перед доставкой пользователю.**
- */generalize* **Подготовка установки Windows к созданию образа путем удаления всех уникальных системных данных, то есть сброс идентификаторов безопасности SID, удаление точек восстановления системы и журналов событий. Затем, при следующей загрузке системы, запускается фаза конфигурации specialize, в которой создаются новые идентификаторы SID и сбрасывается время активации Windows (если оно уже не было трижды сброшено перед этим).**
- **/ооЬе Перезапускает компьютер Windows в режиме приветствия (Windows Welcome), чтобы пользователи могли создать учетные записи, назначить имя компьютеру и выполнить другие задачи. Все параметры файлов ответов, указанные в фазе конфигурации oobeSystem, незамедлительно обрабатываются перед запуском Windows Welcome.**
- */reboot* **Перезагружает компьютер. Эта опция используется при выполнении аудита компьютера и проверки корректности работы настроек OOBE.**
- */shutdown* **Выключает компьютер после завершения работы Sysprep.**
- */quiet* **Запускает Sysprep без отображения экранных подтверждений. Эту опцию удобно использовать для автоматизации Sysprep.**
- */quit* **Закрывает Sysprep после запуска указанных команд.**
- */unattend:answerfile* **Применяет параметры в указанном файле ответов во время автоматизированной установки Windows.**

Наряду с запуском Sysprep с командной строки или с помощью сценариев определенные опции Sysprep также можно указывать в пользовательском интерфейсе. Для этого нужно ввести команду *%systemroot%\system32\sysprep\sysprep* **без параметров, после чего откроется диалоговое окно, показанное на рис. П-6.**

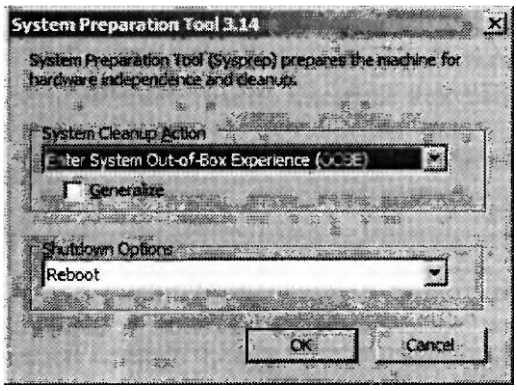


Рис. П-6. Диалоговое окно Sysprep Preparation

Хотя Sysprep обычно используется для подготовки установки Windows к захвату образа, в случае с Windows Server 2008 для этого инструмента существуют некоторые ограничения. В частности, перечисленные далее установленные

роли нельзя вновь внедрить с помощью команды *sysprep /generalize* для подготовки к захвату в образ:

- **все роли сервера Active Directory, включая AD CS, AD DS, AD FS, AD LDS и AD RMS;**
- **DNS-сервер (DNS-Server);**
- **Факс-сервер (Fax Server);**
- **Файловые службы (File Services);**
- **Службы политики сети и доступа (Network Policy and Access Services);**
- **Службы печати (Print Services);**
- **Роль Службы UDDI (UDDI Services);**
- **Службы развертывания Windows (Windows Deployment Services);**
- **Windows SharePoint Services.**

Каждую из этих ролей нужно установить после инсталляции системы. Кроме того, при использовании Sysprep существуют следующие ограничения ролей:

- **роль Веб-сервер (IIS) (Web Server (IIS)) не поддерживает Sysprep с помощью зашифрованных реквизитов в файле конфигурации applicationhost.config;**
- **роль Службы терминалов (Terminal Services) не поддерживает Sysprep в случае присоединения образа Windows к домену.**

Улучшения Windows AIK 1.1

В Windows AIK 1.1 включено множество улучшений, касающихся выполнения развертывания образов поверх исходной версии Windows AIK 1.0, выпущенной вместе с Windows Vista. Назовем некоторые из этих улучшений.

- **Возможность развертывания Windows Vista, Windows Vista Services Pack 1 и Windows Server 2008.**
- **Возможность автоматизации процесса добавления ролей сервера и компонентов на финальных стадиях Windows Setup.**
- **Возможность развертывания 64-разрядных версий Windows из 32-разрядной среды.**
- **Возможность применения образов Windows для компьютеров Unified Extended Firmware Interface (UEFI).**
- **Поддержка Extensive Firmware Interface (EFI) для 64-разрядных версий и установка на диски iSCSI с переносных носителей.**
- **Поддержка 1A64 для Windows SIM с целью обеспечения возможности монтировать файл .wim с носителя IA64.**
- **Дополнительные параметры файлов ответов, поддерживаемые лишь в Windows Server 2008 и не поддерживаемые в Windows Vista. Эти параметры позволяют указать тип установки (Windows Server 2008 или ядро сервера Windows Server 2008), отключить усиленную безопасность Internet Explorer (IE-ESC, Internet Explorer Enhanced Security), указать административный пароль, включить автоматический вход в систему с использованием административной учетной записи, отключить запуск окна Задачи начальной настройки (Initial Configuration Tasks), а также отключить Диспетчер сервера (Server Manager) и запуск других серверных параметров.**

- **Улучшения Windows PE, включая возможность конфигурирования размера RAM-диска (диск X:) с помощью команды *PEImg/scratchspace size,* позволяющей указать размер 32, 64, 128, 256 или 512 Мбайт. Обновлена утилита Oscdimg.exe, включающая новые командные опции и поддержку больших образов. Кроме того, обеспечена поддержка прямой загрузки с жесткого диска вместо RAM-диска, а также версия IA64 среды Windows PE.**
- **Поддержка виртуальных флоппи-дисков для установки Windows с помощью розничных копий.**
- **Новый инструмент PostReflect.exe, который можно использовать для отражения всех критически важных для загрузки драйверов вне хранилища драйверов в автономном образе Windows, что позволяет развертывать образ в различных типах конфигурации оборудования.**
- **Набор определений схемы, позволяющих добавлять задачи, ссылки и элементы торговых марок в приложение OOBE установки Windows.**

Терминология предустановки

Термин *предустановка* означает процесс планирования, подготовки, настройки, развертывания и поддержки образов операционной системы Windows. Образ Windows представляет собой единый сжатый файл, содержащий коллекцию файлов и папок, которые можно использовать для дублирования установки Windows в томе диска. При планировании и реализации предустановочного процесса используют следующую терминологию.

- **Технический компьютер Машина, на которой устанавливается Windows System Image Manager (Windows SIM) и обычно размещаются конфигурационные наборы и дистрибутивный общий ресурс.**
- **Мастер-установка Настраиваемая установка Windows, которую планируется дублировать на одном или нескольких конечных компьютерах.**
- **Основной образ Коллекция файлов и папок (иногда сжатая в один файл), захваченная из мастер-установки и содержащая базовую операционную систему с дополнительными параметрами конфигурации и файлами.**
- **Конечный компьютер Любой компьютер, на котором выполняется предустановка Windows — путем запуска программы Windows Setup или копирования мастер-установки.**

Предустановочный процесс

Жизненный цикл предустановочного процесса развертывания Windows Server 2008 и Windows Vista с использованием образов состоит из следующих шести фаз (рис. П-7).

1. **Планирование: выбираются метод развертывания и средства.**
2. **Установка среды: выполняется проектирование технического компьютера и установка на нем диспетчера Windows SIM. Кроме того, на данной фазе создается лабораторная среда, позволяющая тестировать установку перед развертыванием в корпоративной сети.**
3. **Настройка: создается файл ответов. В Windows SIM указанный файл можно использовать для настройки установки.**

4. Установка и тестирование: создается и тестируется мастер-установка.
5. Развертывание: осуществляется захват образа Windows из мастер-установки и развертывание образа на конечных компьютерах.
6. Поддержка: производится модификация захваченных образов с добавлением дополнительных драйверов устройств, обновлений программного обеспечения, пакетов обновлений и приложений сторонних производителей.

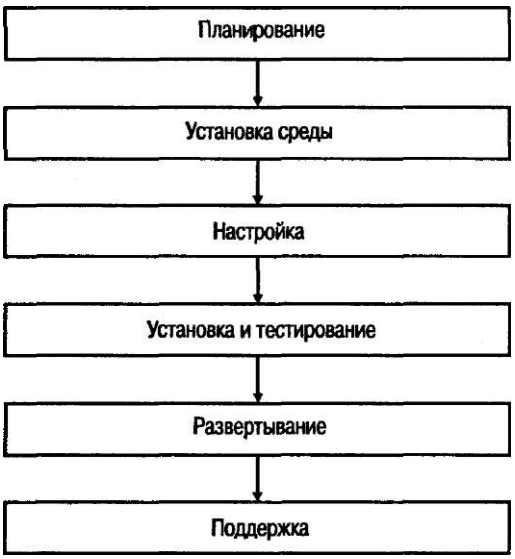


Рис. П-7.. Предустановочный процесс

Методы развертывания

Методы развертывания различаются масштабами развертывания: крупномасштабное, среднемасштабное и мелкомасштабное.

- Крупномасштабное развертывание Сценарий развертывания настольных систем на крупных предприятиях, где требуется быстро развернуть сотни или тысячи компьютеров Windows Vista. (Обычно развертывание большого количества компьютеров Windows Server 2008 производится для больших сред центров данных.) Как правило, при крупномасштабном развертывании используется методика установки из образа с созданием мастер-установки, захватом ее образа и его развертыванием из общего сетевого ресурса на конечных компьютерах.
- Среднемасштабное развертывание Сценарий развертывания настольных систем или серверов в небольших и средних средах, где требуется быстро развернуть несколько десятков компьютеров Windows Vista или несколько компьютеров Windows Server 2008, но без захвата и поддержки библиотеки образов Windows. Обычно для среднемасштабного развертывания используется методика установки из конфигурационных наборов, где конечные компьютеры загружаются с дискет или флэш-устройства USB, после чего из общего сетевого ресурса запускается программа Windows Setup.

- **Мелкомасштабное развертывание** Этот сценарий применяется в небольших офисных и домашних средах, где навыки администратора ограничены и требуется развернуть лишь несколько систем, а также в небольших и средних бизнес-средах с ограниченными административными ресурсами и необходимостью в развертывании лишь нескольких серверов. Для мелкомасштабного развертывания чаще всего используется методика установки с DVD-диска.

Сравнительные характеристики описанных методов развертывания приведены в табл. П-2.

Табл. П-2. Сравнительные характеристики методов развертывания

Метод	Объем	Скорость	Требование сетевой поддержки
Установка из образа	Большой	Быстро	Да
Установка из конфигурационного набора	Средний	Медленно	Опционально
Установка с DVD-диска	Небольшой	Медленно	Нет

В следующем разделе эти три метода развертывания описаны более подробно.

Установка с DVD-диска

На рис. П-8 проиллюстрирован метод установки с DVD для развертывания Windows, который, как правило, используется для проведения мелкомасштабного развертывания настольных систем или серверов в небольших офисных и домашних средах, а также развертывания серверов в небольших и средних средах с ограниченными административными ресурсами.

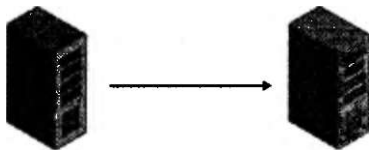


Рис. П-8. Метод развертывания Windows-путем установки с DVD

При использовании этого метода на техническом компьютере можно использовать диспетчер Windows SIM для создания файла ответов Autounattend.xml. Затем конечный компьютер загружается с DVD-диска продукта, используя файл ответов на дискете или флэш-устройстве USB.

С помощью данного метода можно также построить мастер-установку, а затем развернуть Windows путем установки из образа. Например, чтобы построить мастер-установку, в предыдущей схеме нужно вместо конечного компьютера указать мастер-компьютер.

Далее описаны шаги по развертыванию Windows путем установки с DVD-диска.

1. С помощью Windows SIM на конечном компьютере создайте и отконфигурируйте файл ответов и сохраните его под именем Autounattend.xml. Под-

твердите файл ответов, а затем скопируйте его на дискету, флэш-память USB или другой переносной носитель.

2. В DVD-привод конечного компьютера вставьте DVD продукта Windows. Кроме того, в дисковод конечного компьютера вставьте дискету или подключите флэш-память USB с файлом ответов. Убедитесь, что система BIOS конечного компьютера отконфигурирована для запуска с DVD.
3. Включите конечный компьютер. Программа Windows Setup выполнит поиск файла ответов Autounattend.xml. Если программа найдет его, во время установки будут использованы настройки, указанные в этом файле.
4. После завершения установки и перезагрузки конечный компьютер можно сразу развернуть в сети или применить дополнительные настройки путем запуска команды *sysprep /generalize /shutdown* и развертывания компьютера в сети в соответствии с требованиями.

Установка из конфигурационного набора

На рис. П-9 продемонстрирован метод развертывания Windows путем установки из конфигурационного набора, который обычно используется для среднемасштабного развертывания настольных систем или серверов в небольших и средних организациях.

Рис. П-9. Развертывание Windows путем установки из конфигурационного набора

В случае использования данного метода на техническом компьютере с помощью Windows SIM создается файл ответов с конфигурационным набором. Затем конфигурационный набор копируется в общий сетевой ресурс (или на переносной носитель). И наконец, с помощью Windows PE загружается конечный компьютер, который затем подключается к общему сетевому ресурсу для установки Windows из конфигурационного набора.

Какие именно шаги нужно выполнить для развертывания Windows путем установки из конфигурационного набора, зависит от места хранения конфигурационного набора (в сетевом общем ресурсе или на переносном накопителе).

Установка из конфигурационного набора с помощью переносного носителя

Для того чтобы развернуть Windows путем установки из конфигурационного набора, который хранится на переносном накопителе, выполните следующие действия.

1. С помощью Windows SIM на техническом компьютер создайте и отконфигурируйте файл ответов и сохраните его под именем Autounattend.xml.

2. Затем с помощью Windows SIM создайте на техническом компьютере папку дистрибутивного общего ресурса. При необходимости добавьте в дистрибутивный общий ресурс дополнительные драйверы устройств и приложения сторонних производителей, соответствующим образом настройте файл ответов. Подтвердите файл ответов.
3. Вновь воспользовавшись Windows SIM, создайте конфигурационный набор со всеми файлами ресурсов, указанными в файле ответов.
4. Скопируйте конфигурационный набор на переносной накопитель (например, флэш-память USB).
5. В DVD-привод конечного компьютера вставьте DVD с продуктом Windows. Кроме того, подключите к конечному компьютеру переносной накопитель или укажите общий сетевой ресурс, содержащий конфигурационный набор. Убедитесь в том, что система BIOS конечного компьютера отконфигурирована для загрузки с DVD.
6. Включите конечный компьютер. Программа Windows Setup выполнит поиск файла ответов Autounattend.xml. Если программа найдет его, во время установки будут использованы настройки, указанные в этом файле.
7. После завершения установки и перезагрузки сразу же разверните конечный компьютер в сети или же примените дополнительные настройки путем запуска команды *sysprep /generalize /shutdown* и развертывания компьютера в сети в соответствии с требованиями.

Установка из конфигурационного набора с помощью общего сетевого ресурса

Если же потребуется развернуть Windows путем установки из конфигурационного набора, который хранится в общем сетевом ресурсе, ваши действия должны быть следующими.

1. С помощью Windows SIM на техническом компьютер создайте и отконфигурируйте файл ответов и сохраните его под именем Autounattend.xml.
2. Затем с помощью Windows SIM создайте на техническом компьютере папку дисfрибутивного общего ресурса. При необходимости добавьте в дистрибутивный общий ресурс дополнительные драйверы устройств и приложения сторонних производителей, соответствующим образом настройте файл ответов. Подтвердите файл ответов.
3. Опять-таки с помощью Windows SIM создайте конфигурационный набор со всеми файлами ресурсов, указанными в файле ответов.
4. В сети создайте общий ресурс, а в нем две папки: одну для исходных файлов Windows, другую —для конфигурационного набора. В частности, вы можете создать такую структуру папок:

```
\\sharename\source
\\sharename\confsets
```

5. Скопируйте файлы установки Windows из папки \source на DVD-диске продукта в папку \source общего сетевого ресурса.
6. Файлы конфигурационного набора скопируйте в папку \confsets общего сетевого ресурса.

7. **С помощью загружаемого носителя Windows PE загрузите конечный компьютер. Когда на экран будет выведено окно командной строки Windows PE, подключитесь к общему сетевому ресурсу с помощью команды**

   ```
   net use y: \\sharename
   ```

   Для подключения, возможно, понадобится указать детальные сведения. Введите эти реквизиты в формате *имя_компьютера\имя_пользователя.*
8. **После подключения к общему сетевому ресурсу запустите Windows Setup и сошлитесь на файл ответов в конфигурационном наборе с помощью следующей команды:**

   ```
   y:\sou rce\setup.exe /unattend:y:\confsets\autounattend.xml
   ```

9. **Завершив установку и перезагрузку, сразу же разверните конечный компьютер в сети или же примените дополнительные настройки путем запуска команды** *sysprep /generalize /shutdown* **и развертывания компьютера в сети в соответствии с требованиями.**

Проверьте себя

- **В каких случаях следует использовать метод развертывания Windows из конфигурационного набора вместо простой установки с DVD-диска для инсталляции Windows Server 2008 без сетевой поддержки?**

Ответ

- **Для установки без поддержки сети метод развертывания Windows из конфигурационного набора используется для добавления дополнительных драйверов устройств и приложений сторонних производителей.**

Метод установки из образа

На рис. П-10 проиллюстрировано развертывание Windows методом установки из образа, который используется в процессе крупномасштабного развертывания настольных компьютеров в корпоративных средах и серверов в центрах данных.

Рис. П-10. Развертывание Windows путем установки из образа

В соответствии с этим методом на техническом компьютере с помощью Windows SIM создается файл ответов и при необходимости дистрибутивный набор. Затем на мастер-компьютере выполняется построение мастер-установки, после чего с помощью инструмента Sysprep осуществляется подготовка этого компьютера к созданию образа. Потом в среде Windows PE используется инструмент

ImageX для захвата образа мастер-компьютера и его выгрузки в сетевой дистрибутивный общий ресурс. И наконец, на конечном компьютере загружается Windows PE, с помощью инструмента Diskpart.exe форматируется жесткий диск и компьютер подключается к дистрибутивному общему ресурсу для применения образа.

Как именно производится развертывание Windows путем установки из образа, зависит от способа применения захваченного образа мастер-установки на конечном компьютере (с помощью ImageX или Windows Setup).

Установка из образа с помощью ImageX

Чтобы развернуть Windows из образа с помощью инструмента ImageX, выполните действия, перечисленные далее.

1. Создайте мастер-установку Windows путем установки с DVD-диска или из конфигурационного набора. При необходимости выполните настройку установки и тщательно протестируйте ее.
2. Подготовьте мастер-установку, используя для удаления машинных данных (SID и прочее) команду *sysprep /generalize /shutdown.*
3. Загрузите мастер-компьютер с помощью загружаемого носителя Windows PE. Убедитесь, что носитель с Windows PE включает утилиту ImageX.
4. В командной строке Windows PE, воспользовавшись командой *imagex /capture,* захватите образ Windows мастер-установки.
5. С помощью команды *net use* назначьте диск для подключения к сетевому ресурсу. (Для этого, возможно, потребуется предоставить учетные данные.) С помощью команды copy скопируйте захваченный файл .wim в общий сетевой ресурс.
6. Воспользовавшись загружаемым носителем Windows PE, загрузите конечный компьютер.
7. С помощью команды *diskpart* командной строки Windows PE разбейте и отформатируйте жесткий диск конечного компьютера. Заметим, что этот шаг можно автоматизировать с помощью сценариев с командой *diskpart.*
8. Затем с помощью команды *net use* назначьте диск для подключения к общему сетевому ресурсу, где хранится мастер-установка.
9. Наконец, используя команду *imagex /apply* командной строки Windows PE, примените образ мастер-установки в разделе жесткого диска конечного компьютера.

Установка из образа с помощью Windows Setup

Перечислим действия, которые необходимо выполнить для того, чтобы развернуть Windows путем установки из образа с помощью программы Windows Setup.

1. Создайте мастер-установку Windows путем установки с DVD-диска или из конфигурационного набора. При необходимости произведите настройку установки и тщательно протестируйте ее.
2. Подготовьте мастер-установку, используя для удаления машинных данных (SID и прочее) команду *sysprep /generalize /shutdown.*

3. **Загрузите мастер-компьютер с помощью загружаемого носителя Windows PE. Убедитесь в том, что носитель с Windows PE включает утилиту ImageX.**
4. **Используя команду *imagex/capture* командной строки Windows PE, захватите образ Windows мастер-установки. Чтобы метод работал, захваченному образу нужно присвоить имя Install.wim.**
5. **С помощью команды *net use* назначьте диск для подключения к сетевому ресурсу. (Для этого, возможно, понадобится предоставить учетные данные.) Применив команду copy, скопируйте захваченный файл .wim в общий сетевой ресурс.**
6. **На конечном компьютере с помощью Windows SIM откройте файл .wim, захваченный из мастер-установки. Создайте и отконфигурируйте файл ответов и сохраните его под именем Unattend.xml. Подтвердите файл ответов, а затем скопируйте его в общий сетевой ресурс, где хранится захваченный образ Install.wim.**
7. **Воспользовавшись загружаемым носителем Windows PE, загрузите конечный компьютер.**
8. **С помощью команды *net use* командной строки Windows PE назначьте диск, который будет подключен к общему сетевому ресурсу, где хранятся захваченный образ мастер-установки и файл ответов Unattend.xml.**
9. **Запустите программу Windows Setup и сошлитесь на файл ответов, который хранится вместе с захваченным образом мастер-установки, например с помощью команды:**

```
y:\setup.exe /unattend:unattend.xml
```

Другие типы развертывания с помощью образов

Помимо развертывания захваченного образа мастер-установки с помощью команды *imagex /apply* или Setup.exe существуют еще два метода развертывания Windows с использованием образов.

- **Используя роль Службы развертывания Windows (Windows Deployment Services, WDS), Windows PE можно запустить удаленно, что избавит от необходимости садиться за конечные компьютеры, вручную форматировать их диски и запускать процесс установки.**
- **Технология сервера Preboot Execution Environment (PXE) от стороннего производителя позволяет скопировать на PXE-сервер исходные файлы Windows PE и настроить конфигурацию загрузки PXE-сервера для использования данной ОС.**

Более подробные сведения о втором методе можно найти в руководстве Windows Automated Installation Kit (Windows AIK) User's Guide программного пакета Windows AIK.

Программа Windows Setup

Перед тем как создавать реальные файлы ответов и использовать их для автоматизированного развертывания Windows с помощью ранее описанных методов,

следует разобраться в принципе работы программы Windows Setup. Данная программа является ключевой в процессе развертывания как в случае полной установки с нуля, так и при обновлении существующей версии системы. Программа Windows Setup (Setup.exe) запускает установку, собирает информацию, необходимую для выполнения установки (запрашивая данные у пользователя или считывая параметры в файле ответов), устанавливает и конфигурирует Windows, при необходимости перезагружает компьютер и выводит окно Out Of Box Experience (OOBE) или Приветствие Windows (Windows Welcome). В случае полной установки Windows с нуля выполнение программы Setup.exe начинается с загрузки Windows PE с целью настройки жесткого диска и копирования на него образа Windows.

Windows Setup выполняется в несколько этапов настройки. Этап настройки — это фаза выполнения программы Windows Setup, когда для автоматизированной установки Windows применяются параметры, указанные в файле ответов. Существует семь этапов настройки программы Windows Setup, однако не все они используются в стандартной установке Windows.

В следующих семи разделах описаны различные этапы настройки, а также принципы их применения при типичном методе развертывании Windows — путем установки из образа. Порядок описания этапов настройки соответствует их порядку в файле ответов (рис. П-11).

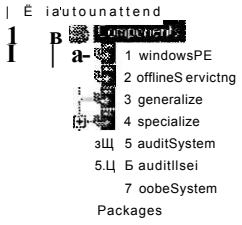


Рис. П-11. Этапы настройки Windows Setup в файле ответов

Этап настройки windowsPE

Этап настройки windowsPE используется для конфигурирования параметров Windows PE, таких как местоположение файлов журнала, разрешение экрана для Windows PE и т. д.

Этап windowsPE также используется для конфигурирования параметров установки. Приведем примеры таких параметров:

- параметры разбиения и форматирования жесткого диска;
- устанавливаемый образ Windows (например, Enterprise Edition или Standard Edition, полный или только ядро сервера);
- ключ продукта, применяемый при установке;
- языковые и региональные параметры, используемые для установки.

Этап настройки offlineServicing

Этап настройки offlineServicing используется для применения параметров файла ответов к автономному образу Windows. В автономный образ можно добавлять, в частности, файлы таких типов:

- **языковые пакеты;**
- **обновления программного обеспечения;**
- **дополнительные пакеты драйверов;**
- **пакеты обновлений (Service Pack).**

Этап настройки generalize

В отличие от этапов windowsPE и offlineServicing этап настройки generalize никогда не запускается при стандартном процессе выполнения Windows Setup. Он запускается только в случае использования команды *sysprep /generalize* **для повторной очистки установки Windows путем удаления всех машинных данных, в том числе идентификаторов SID, файлов журналов и т. д. Сразу же после завершения этапа generalize система выключается, после чего ее образ можно захватить и развернуть на других компьютерах. В случае выполнения этапа generalize при следующем запуске системы немедленно запустится этап specialize.**

Этап настройки specialize

На этапе настройки specialize производится конфигурирование машинных данных в установке, таких как:

- **временной пояс;**
- **региональные и языковые параметры;**
- **сетевые параметры;**
- **доменные данные;**
- **URL домашней страницы подразделения.**

Этап specialize всегда сопровождает этап generalize и никогда не запускается при стандартном методе выполнении программы Windows Setup. После очистки машинных данных системы с помощью команды *sysprep /generalize* **этап настройки specialize сразу же запустится при следующем запуске системы. Другими словами, на этапе specialize восстанавливаются параметры, сброшенные на этапе generalize.**

Этап настройки auditSystem

Этап настройки auditSystem запускается в контексте режима аудита, причем для включения этого режима в системе должна быть запущена команда *sysprep /audit.* **Этап auditSystem, как правило, используется для установки дополнительных драйверов устройств и обновлений программного обеспечения в образ, содержащий минимальный набор драйверов устройств. После запуска данного этапа в системе запускается этап настройки auditUser. Оба этапа настройки никогда не запускаются в стандартном режиме выполнения программы Windows Setup.**

Этап настройки auditUser

Сразу же после запуска этапа auditSystem (для этого нужно использовать команду *sysprep /audit)* запускается этап настройки auditUser. Обычно на данном этапе выполняются дополнительные команды, необходимые для запуска в системе сценариев или приложений. Эти команды можно запускать с помощью параметров RunSynchronous и RunAsynchronous файла ответов.

Этап настройки oobeSystem

Наконец, этап настройки oobeSystem конфигурирует параметры, применяемые во время открытия окон Out Of Box Experience (OOBE) программы Windows Setup. Для компьютеров Windows Vista на этапе oobeSystem настраивается приветствие Windows.

Этапы настройки в развертывании путем установки из образа

Далее речь пойдет о применении описанных этапов настройки при типичном методе развертывания — путем установки из образа, в частности с использованием инструмента ImageX для захвата образа мастер-компьютера и его применением на конечном компьютере. В табл. П-3 описаны шаги, выполняемые при таком типе развертывания, и указаны этапы настройки, используемые на каждом шаге.

Табл. П-3. Этапы настройки, выполняемые при развертывании путем установки образа с использованием ImageX

Этапы развертывания	Этапы настройки
Создание мастер-установки путем инсталляции с DVD-диска с применением файла ответов Autounattend.xml	windowsPE offlineServicing oobeSystem
Запуск команды *sysprep /geneialize* для очистки мастер-установки от машинных данных и подготовки к созданию образа	generalize
Запуск мастер-компьютера с загружаемого носителя Windows PE и захват образа Windows с компьютера с помощью инструмента ImageX	windowsPE
Запуск конечного компьютера с загружаемого носителя Windows PE и применение ранее захваченного образа	windowsPE
Перезагрузка конечного компьютера с установленного образа	specialize oobeSystem

Обновление текущей операционной системы до Windows Server 2008

В этом разделе вы ознакомитесь с процессом обновления предыдущих версий операционной системы Windows Server до Windows Server 2008. Здесь приведены соображения относительно выбора между обновлением текущей системы и установкой с нуля, а также описаны подготовительные действия, которые

следует выполнить перед обновлением. Кроме того, в настоящем разделе описаны пути обновления и системные требования для Windows Server 2008. И наконец, здесь рассказывается, как использовать различные журналы установки для устранения неполадок в случае возникновения ошибок, связанных с установкой или обновлением.

Процесс обновления системы Windows Server 2003 до Windows Server 2008 очень отличается от установки системы с нуля на «голом» оборудовании (Bare-Metal System), без установленной операционной системы. Отметим, что процесс установки с нуля можно автоматизировать с помощью Windows AIK и других технологий развертывания. Существует и альтернативный метод обновления, требующий тщательного планирования и выполнения операции вручную.

Перед обновлением существующих серверов Windows Server 2003 до Windows Server 2008 нужно ответить на ряд вопросов.

- **Совместимы ли текущие рабочие приложения на сервере с новой версией Windows? Вряд ли вы захотите обновлять свои серверы лишь затем, дабы убедиться, что приложения сторонних производителей (и даже программы Microsoft) больше не работают должным образом и не могут поддерживать операционные требования организации. Чтобы гарантировать совместимость текущих приложений с Windows Server 2008, загрузите последнюю версию средства Application Compatibility Toolkit (ACT) в центре загрузок Microsoft по адресу** *http://www.microsoft.com/downloads* **и тщательно протестируйте совместимость приложений с новой платформой.**
- **Способно ли оборудование ваших текущих серверов поддерживать Windows Server 2008? Просмотрите требования к оборудованию для Windows Server 2008 в табл. П-4 и выясните, имеет ли смысл обновлять текущие серверы или же целесообразнее приобрести новое оборудование и выполнить установку с нуля. Кроме того, вам нужно проверить доступность драйверов устройств Windows Server 2008 в хранилищах драйверов существующих систем серверов, поскольку в противном случае вы не сможете их обновить. В каталоге Windows Server Catalog, расположенном по адресу** *http://www.windows-servercatalog.com,* **представлен список устройств, поддерживающих новую операционную систему. Помимо всего прочего следует знать, что Windows Server 2008 поддерживает лишь те системы, которые соответствуют требованиям Windows Server 2008 ACPI, причем при установке Windows Server 2008 невозможно указать настраиваемый файл уровня абстрагирования оборудования (HAL).**
- **Было ли выполнено резервное копирование серверов? Прежде чем переходить на новую версию Windows, следует создать резервные копии конфигурации серверов и всех хранящихся на них данных. Кроме того, нужно выполнить резервное копирование всех служб ролей серверов, например создать резервную копию базы данных DHCP серверов DHCP.**
- **Поддерживают ли текущие установленные на серверах роли обновление до Windows Server 2008? Не все роли поддерживают обновление, а некоторые из них обновляются намного сложнее других. Самые последние сведения относительно обновления различных ролей сервера можно найти на сайте Windows Server 2008 TechCenter по адресу** *http://technet.microsoft.com/en-us/windowsserver2008/.*

Помимо следования общим соображениям относительно обновления, перед выполнением обновления Windows Server 2003 до Windows Server 2008 нужно выполнить ряд дополнительных задач.

- **Запустите диагностику памяти и жестких дисков сервера, чтобы во время установки не возникли аппаратные ошибки.**
- **Отключите все антивирусное программное обеспечение на сервере, поскольку иногда эти продукты могут конфликтовать с процессом установки.**
- **Отключите от сервера все устройства UPS, поскольку они иногда создают проблемы при обнаружении оборудования программы Windows Setup.**

К тому же вам потребуется определить поддерживаемые пути обновления предыдущих версий операционной системы Windows Server до Windows Server 2008. Эту тему мы обсудим позже, в разделе «Поддерживаемые пути обновления до Windows Server 2008».

Параллельное обновление

Один из способов обеспечить для существующего оборудования сервера возможность выполнять обновление даже в случае сбоя состоит в так называемом параллельном обновлении (side-by-side). В соответствии со сценарием Windows Server 2008 устанавливается в отдельный раздел, а не в раздел с Windows Server 2003. Например, если версия Windows Server 2003 установлена на жестком диске C, вы можете создать второй раздел D и запустить программу Windows Setup в Windows Server 2003 для установки Windows Server 2008 в раздел D.

Хотя параллельное обновление по сути представляет собой установку с нуля, а не реальное обновление, такой метод позволяет в случае возникновения ошибок в процессе обновления обеспечить доступ к предыдущей версии Windows. Кроме того, такой метод можно использовать для постепенной миграции с Windows Server 2003 до версии Windows Server 2008 на одном компьютере.

Системные требования Windows Server 2008

Перед обновлением существующих серверов до Windows Server 2008 проверьте, выполняются ли системные требования, указанные в табл. П-4.

Табл. П-4. Системные требования Windows Server 2008

Компонент	Требование
Процессор	Минимальные: 1 ГГц (процессор x86) или 1,4 ГГц (процессор x64)
	Рекомендуемые: не менее 2 ГГц
	Примечание: для систем Itanium требуется процессор Intel Itanium 2
Память	Минимальные: 512 Мбайт
	Рекомендуемые: не менее 2 Гбайт
	Максимальные (32-разрядные системы): 4 Гбайт (Standard Edition) или 64 Гбайт (Enterprise Edition и Datacenter Edition)
	Максимальные (64-разрядные системы): 32 Гбайт (Standard Edition) или 2 Тбайт (Enterprise Edition и системы Itanium)

Компонент	Требование
Доступное дисковое пространство	Минимальные: 10 Гбайт Рекомендуемые: не менее 40 Гбайт Примечание: на компьютерах с объемом оперативной памяти свыше 16 Гбайт потребуется больше дискового пространства для файла подкачки, гибернации и файлов дампа
Диск	Привод DVD-ROM
Дисплей и периферия	Super VGA (8004600) или монитор с более высоким разрешением Клавиатура Мышь Microsoft или совместимое указывающее устройство

Поддерживаемые пути обновления до Windows Server 2008

Перед обновлением системы с предыдущих версий Windows до Windows Server 2008 также нужно определить поддерживаемые пути обновления (табл. П-5).

Табл. П-5. Поддерживаемые пути обновления для Windows Server 2008

Текущая операционная система	Обновление до следующей системы
Microsoft Windows Server 2003 R2 Standard Edition Операционные системы Microsoft Windows Server 2003 с Service Pack 1 (SP1) Standard Edition Операционные системы Microsoft Windows Server 2003 с Service Pack 2 (SP2) Standard Edition	Полная установка Windows Server 2008 Standard Edition
Microsoft Windows Server 2003 R2 Enterprise Edition Операционные системы Microsoft Windows Server 2003 с Service Pack 1 (SP1) Enterprise Edition Операционные системы Microsoft Windows Server 2003 с Service Pack 2 (SP2) Enterprise Edition	Полная установка Windows Server 2008 Enterprise Edition
Microsoft Windows Server 2003 R2 Datacenter Edition Windows Server 2003 с Service Pack 1 (SP1) Datacenter Edition Microsoft Windows Server 2003 с Service Pack 2 (SP2) Datacenter Edition	Полная установка Windows Server 2008 Datacenter Edition

Далее приведены ограничения, касающиеся обновления систем до Windows Server 2008.

- **Windows Server 2000 нельзя обновить до Windows Server 2008.**
- **Windows NT 4.0 Server нельзя обновить до Windows Server 2008.**
- **Выполнять обновление архитектуры нельзя. Например, 32-разрядную версию Windows Server 2003 невозможно обновить до 64-разрядной версии Windows Server 2008, а 64-разрядную версию Windows Server 2003 нельзя обновить до 32-разрядной версии Windows Server 2008.**
- **Windows Server 2003 Web Edition нельзя обновить до Windows Server 2008.**
- **Выпуск Windows Server 2003 Itanium (IA64) нельзя обновить до Windows Server 2008.**

- **Выпуск RTM любой версии Windows Server 2003 нельзя обновить до Windows Server 2008. Другими словами, к версии Windows Server 2003 нужно применить как минимум Service Pack 1, чтобы обновить ее до Windows Server 2008.**
- **Windows Server 2003 нельзя обновить до установки ядра сервера Windows Server 2008. Другими словами, можно выполнить лишь обновление до полной установки Windows Server 2008. Установка ядра сервера должна производиться с нуля.**

Проверьте себя

1. **Почему перед обновлением системы от сервера нужно отключать все устройства UPS?**
2. **Как проверить, поддерживает ли устройство хранения возможность обновления до Windows Server 2008?**

Ответы

1. **Устройство UPS может конфликтовать с процессом обнаружения оборудования, выполняемым во время установки.**
2. **Посетить сайт Windows Server Catalog, расположенный по адресу** *http://www.windowsservercatalog.com,* **и проверить, поддерживает ли устройство систему Windows Server 2008.**

Устранение неполадок

В процессе выполнения полной установки Windows Server 2008 и во время обновления с Windows Server 2003 могут возникать различные ошибки. Важно знать, какие действия по устранению неполадок нужно выполнять в подобных ситуациях. Далее приведены некоторые соображения и рекомендации.

Файлы журнала установки

В случае ошибки установки по неизвестной причине, следует начать с просмотра журналов установки. В частности, для устранения неполадок такого рода используются два файла журналов.

- **setupact.log Этот файл журнала содержит информацию о действиях установки, выполняемых в процессе инсталляции.**
- **setuperr.log Содержит информацию об ошибках установки, возникших в процессе инсталляции.**

Расположение этих файлов журналов зависит от того, на каком этапе настройки процесса установки они генерировались. Как правило, они содержатся в одной из следующих папок.

- **C:\$WINDOWS.~BT\Sources\Panther Файлы журналов установки хранятся в этой папке во время выполнения этапа настройки windowsPE программы Windows Setup, однако они могут также храниться и в папке X:\$WINDOWS.~BT\Sources\Panther на RAM-диске Windows PE, то есть в памяти.**

- C:\Windows\Panther Этап настройки online является первой загрузочной фазой Windows Setup и начинается с сообщения Please wait a moment while Windows prepares to start for this time. На этапе настройки online устанавливается базовая поддержка оборудования, а также (в случае обновления предыдущей версии системы) выполняется миграция данных и программ. Файлы журналов хранятся в этой папке на этапе настройки oobeSystem.

Отметим, что в приведенных примерах диском C является раздел, в котором выполняется установка Windows Server 2008, или раздел, содержащий предыдущую операционную систему (в случае обновления). Если используется архитектура оборудования Itanium (IA64), то файлы журналов могут храниться на еще одном жестком диске — это зависит от объема дискового пространства, доступного во время установки.

Проблемы драйверов

Довольно часто невозможность установки объясняется существованием проблем с драйверами устройств. Далее перечислено несколько проблем, возникающих при установке и связанных с драйверами.

- Установка неподписанного драйвера устройства во время инсталляции системы может привести к тому, что установка Windows Server 2008 в архитектуре x64 будет незагружаемой. Чтобы решить эту проблему, во время загрузки можно нажать клавишу F8 и выбрать опцию Отключить требование цифровой подписи драйверов (Disable Driver Signature Enforcement) в меню Дополнительные варианты загрузки (Advanced Boot Options). Однако лучше всего получить версию проблемного драйвера с цифровой подписью.
- Если при обновлении предыдущей версии программа установки не может обнаружить переносное загрузочное устройство, то после первого перезапуска может появиться синий экран. В том случае если во время установки требуется загрузить драйвер загрузочного устройства, сохраните драйвер на дискете, флэш-устройстве USB, CD или DVD. Драйвер должен быть размещен либо в корневом каталоге носителя, либо в одной из следующих подпапок:
  - \Sources для систем x86;
  - \AMD64 для систем x64;
  - \IA64 для систем Itanium.

Установка ядра сервера

Новая опция Установка ядра сервера Windows (Windows Server Core) системы Windows Server 2008 позволяет установить урезанную версию Windows Server 2008, которая по сравнению с полной установкой предъявляет более низкие требования к оборудованию, обеспечивает более высокий уровень безопасности и проще в поддержке. Администраторы IT могут использовать ядро сервера как новую платформу для запуска критически важных сетевых служб, в частности DHCP и DNS.

Хотя для развертывания ядра сервера используются те же инструменты, что и для развертывания полной версии Windows Server 2008, существуют некоторые отличия в принципах применения этих средств, в частности для автоматизации

послеустановочных задач, например создания начальной конфигурации сервера, а также для добавления ролей сервера и компонентов.

Ядро сервера Windows

В предыдущих версиях операционных систем сервера Windows, скажем, в Windows Server 2003, при установке операционной системы устанавливались и двоичные файлы для компонентов, редко используемых в сетевом окружении. Например, серверу, который не используется как сервер приложений, не нужны компоненты .NET Framework и CLR. Аналогично удаленно управляемому серверу без клавиатуры, мыши и монитора (headless server) не нужна оболочка рабочего стола Проводник Windows (Windows Explorer) и такие элементы GUI, как темы или окно поиска. Проблема установки исполняемых двоичных файлов для таких компонентов состоит в том, что они могут потребовать дополнительной поддержки на сервере. Например, если на сервере установлена структура .NET Framework, то к нему должны применяться все обновления программного обеспечения Microsoft для этого компонента, даже если данный компонент не используется. В противном случае, если вы не установите обновления неиспользуемых компонентов, сервер может остаться незащищенным. Еще одна проблема, связанная с установкой ненужных компонентов на сервере, заключается в том, что каждый компонент предъявляет собственные требования к таким ресурсам, как память, процессор и диск.

По этим и некоторым другим причинам корпорация Microsoft создала две опции установки Windows Server 2008: полная установка и установка ядра сервера (Server Core). При выборе первой опции в системе выполняется установка двоичных исполняемых кодов для всех компонентов. При установке ядра сервера устанавливаются лишь те двоичные файлы, которые требуются для поддержки ограниченного набора ролей сервера, служб ролей и компонентов. Обеспечивая минимальную среду для запуска ограниченного набора ролей сервера и компонентов, новая опция установки ядра сервера позволяет снизить уровень требований к оборудованию и технической поддержке. В частности, установка ядра сервера обеспечивает следующие преимущества.

- **Более высокий уровень стабильности и производительности** Ядро сервера (Server Core) поддерживает лишь ограниченное количество ролей сервера, то есть на сервере запускается меньше служб. Чем меньше служб запущено на сервере, тем более высокий уровень стабильности и производительности будет обеспечен.
- **Уменьшенный фронт атак** Поскольку на компьютере с ядром сервера запускается меньше служб, также уменьшается фронт атак на сервер. Исключив из системы двоичные файлы для ненужных служб и уменьшив количество запущенных служб, ядро сервера (Server Core) может обеспечить более высокий уровень безопасности, чем полная установка сервера.
- **Снижение уровня требований к техническому обслуживанию** Если в ядре сервера недоступны роль или компонент, двоичные файлы для этой роли или компонента также будут отсутствовать в системе. Поэтому отпадает необходимость устанавливать в системе новые обновления для этой роли или компонента. Корпорация Microsoft подсчитала, что ядру сервера требу-

ется лишь около 40 % обновлений программного обеспечения от необходимых для предыдущих версий Windows Server.

- **Снижение уровня требований диска Поскольку многие двоичные файлы, включенные в полную установку, в инсталляции ядра сервера не нужны, для установки ядра требуется намного меньше дискового пространства (около 1,5 Гбайт по сравнению с 5,9 Гбайт при полной установке). Кроме того, ядро сервера может работать более эффективно, чем полная установка, в системах с ограниченным объемом оперативной памяти.**

Доступность и системные требования для ядра сервера

Ядро сервера (Server Core) можно установить в 32- и 64-разрядных версиях следующих SKU-идентификаторов выпусков Windows Server 2008:

- **Windows Server 2008 Standard Edition;**
- **Windows Server 2008 Enterprise Edition;**
- **Windows Server 2008 Datacenter Edition.**

В табл. П-6 приведены минимальные и рекомендуемые системные требования по установке ядра сервера Windows Server 2008.

Табл. П-6. Минимальные и рекомендуемые системные требования по установке ядра сервера Windows Server 2008

Компонент	Требования
Процессор	Минимальные: 1 ГГц Рекомендуемые: 2 ГГц Оптимальные: не ниже 3 ГГц Отметим, что для версии Windows Server 2008 Itanium требуется процессор Intel Itanium 2
Память	Минимальные: 512 Мбайт Рекомендуемые: 1 Гбайт Оптимальные: 1 Гбайт (ядро сервера) и выше Максимальные (32-разрядные системы): 4 Гбайт (Standard) или 64 Гбайт (Enterprise Edition и Datacenter Edition) Максимальные (64-разрядные системы): 32 Гбайт (Standard Edition) или 2 Тбайт (Enterprise Edition, Datacenter Edition и системы Itanium)
Жесткий диск	Минимальные: 8 Гбайт Рекомендуемые: 10 Гбайт (ядро сервера) Оптимальные: 40 Гбайт (ядро сервера) и выше Отметим, что компьютерам с объемом оперативной памяти 16 Гбайт требуется больше дискового пространства для файлов подкачки, гибернащш и дампов. Кроме того, хотя для установки ядра сервера требуется минимум 1,5 Гбайт, для включения обновлений, исправлений, временных файлов и других изменений рекомендуется зарезервировать хотя бы 10 Гбайт
Диск	Привод DVD-ROM
Дисплей	Монитор Super VGA (800x600) или с более высоким разрешением
Другое	Клавиатура и мышь от Microsoft или совместимые указывающие устройства

Содержимое ядра сервера

Ядро сервера предназначено для установки серверов, на которых будет запущена одна или несколько критически важных ролей. Например, ядро сервера можно использовать для запуска DHCP-сервера, DNS-сервера, контроллера домена и т. д. Поскольку назначение ядра сервера состоит в снижении системных требований и уменьшении фронта атак, в этой установке доступен лишь поднабор ролей сервера полной установки Windows Server 2008. В установке ядра сервера доступны только следующие роли:

- **Доменные службы Active Directory (Active Directory Domain Services, AD DS);**
- **Службы Active Directory облегченного доступа к каталогам (Active Directory Lightweight Directory Services, AD LDS);**
- **DHCP-сервер (DHCP Server);**
- **DNS-сервер (DNS Server);**
- **Файловые службы (File Services);**
- **Службы печати (Print Services);**
- **Веб-сервер (IIS) (Web Server (IIS));**
- **Средства Hyper-V (Hyper-V).**

В ядре сервера также можно установить роль Службы потокового мультимедиа (Streaming Media Services). Эта роль недоступна в Windows Server 2008, однако ее можно срочно загрузить (загрузка Out-Of-Band, OOB), щелкнув ссылку в статье 934518 базы знаний Microsoft (*http://support.microsoft.com/kb/934518).*

Отметим, что факт доступности роли сервера для ядра сервера не означает, что будут установлены все службы ролей, которые связаны с этой ролью. Например, хотя в ядре сервера можно установить IIS 7 (роль Веб-сервер (IIS)), структуру .NET Framework установить невозможно, в результате чего и компонент ASP.NET для IIS 7 нельзя установить. Более того, поскольку ядро сервера не располагает оболочкой GUI, на компьютере с ядром сервера невозможно установить средства управления IIS 7.

Ядро сервера поддерживает лишь поднабор компонентов полной установки Windows Server 2008. Напомним, что роль представляет собой конкретную функцию, выполняемую сервером в сети. Роли поддерживаются одной или несколькими службами ролей, которые обеспечивают для каждой из них различные типы функциональности. Опциональные компоненты можно устанавливать для обеспечения дополнительной функциональности на сервере. Иногда компоненты обеспечивают поддержку одной или нескольких ролей, а иногда обеспечивают автономную функциональность на сервере. На компьютере с ядром сервера можно установить лишь следующие компоненты:

- **Шифрование диска BitLocker (BitLocker Drive Encryption);**
- **Средство отказоустойчивости кластеров (Failover Clustering);**
- **Многопутевой ввод-вывод (Multipath Ю);**
- **Балансировка сетевой нагрузки (Network Load Balancing);**
- **Диспетчер съемных носителей (Removable Storage);**
- **Службы SNMP (Simple Network Management Protocol, SNMP);**
- **Подсистема для UNIX-приложений (Subsystem for UNIX-based applications);**

- **Клиент Telnet (Telnet client);**
- **WINS-сервер (Windows Internet Name Service, WINS);**
- **Возможности системы архивации данных Windows Server (Windows Server Backup).**

Отметим, что для обеспечения функциональности некоторых из этих компонентов требуется особое оборудование. Например, для компонента Шифрование диска BitLocker (BitLocker Drive Encryption) необходимо оборудование, поддерживающее доверенный платформенный модуль (Trusted Platform Module) версии не ниже TPM 1.2 с соответствующей интеграцией требований Trusted Computing Group (TCG) в BIOS. Для шифрования BitLocker также требуются два раздела диска NTFS: один нужен для системного тома, другой — для тома операционной системы. Кроме того, некоторые компоненты доступны не в каждом выпуске Windows Server 2008. Например, Средство отказоустойчивости кластеров (Failover Clustering) поддерживается лишь в выпусках Enterprise Edition и Datacenter Edition, но не поддерживается в выпуске Standard Edition.

Что же касается графических инструментов GUI, то в ядре сервера поддерживается лишь их ограниченный набор. В табл. П-7 эти доступные средства перечислены с коротким пояснением причин, по которым они включены в ядро сервера, то есть какие функции они там выполняют. Кроме того, отметим, что некоторые функции этих инструментов могут не работать. Например, если в меню программы Блокнот (Notepad) выбрать опцию Справка (Help), файл справки не откроется, поскольку движок справки, запускающий файлы .chm, в ядре сервера отсутствует.

Табл. П-7. Инструменты TGUI, доступные в ядре сервера

Средство	С какой целью используется
Командная строка cmd.exe (Command Prompt)	Для администрирования ядра сервера с локальной консоли
Блокнот (Notepad) (notepad.exe)	Для просмотра файлов журналов, модификации файлов конфигурации и т. д.
Редактор реестра (Registry Editor) (regedit.exe)	Для просмотра и модификации параметров реестра
Сведения о системе (System Information) (msinfo32.exe)	Для просмотра сведений о системе
Диспетчер задач (Task Manager)	Для управления процессами запуска новых окон командной строки
Установщик Windows (Windows Installer) (msiexec.exe)	Для интерпретации пакетов MSI установщика Windows и установки приложений
Средство диагностики технической поддержки Microsoft (Microsoft Support Diagnostic Tool) (msdt.exe)	Для сбора и отправки сведений о системе в службу технической поддержки продуктов Microsoft (Microsoft Product Support Services, PSS) с целью устранения неполадки

Чего нет в ядре сервера

В процессе планировании развертывания сервера нужно также знать, какие роли и компоненты недоступны в ядре сервера, чтобы не пришлось переустанавливать полную версию сервера.

На компьютере с ядром сервера недоступны следующие роли:

- Службы сертификации Active Directory (Active Directory Certificate Services, AD DS);
- Службы федерации Active Directory (Active Directory Federation Services, AD FS);
- Службы управления правами Active Directory (Active Directory Rights Management Services, AD RMS);
- Сервер приложений (Application Server);
- Факс-сервер (Fax Server);
- Службы политики сети и доступа (Network Policy And Access Services);
- Службы терминалов (Terminal Services);
- Службы UDDI (UDDI Services);
- Службы развертывания Windows (Windows Deployment Services);
- Службы Windows SharePoint (Windows SharePoint Services).

Например, компьютер с ядром сервера нельзя развернуть как корневой центр сертификации CA (Certificate Authority) в инфраструктуре открытых ключей (Public Key Infrastructure, PKI) организации. Вы также не сможете развернуть сервер терминалов на компьютере с ядром сервера, чтобы обеспечить пользователям возможность запускать централизованные службы приложений.

Если говорить в целом, ядро сервера не является платформой для запуска сетевых приложений. Например, в ядре сервера нельзя установить не только роль Службы терминалов (Terminal Services), но и такие приложения, как Microsoft Office System 2007 и Microsoft Visual Studio. Причина невозможности запуска этих программ состоит в том, что в ядро сервера не включено большинство функций GUI (с целью снижения системных требований и уменьшения фронта атак). Таким образом, Проводник Windows (Windows Explorer), а также диалоговые окна Открыть (Open) и Сохранить как (Save As) не будут доступны. Более того, поскольку приложения типа Office располагают множеством зависимостей с подобными диалоговыми окнами, обычно их невозможно установить в ядре сервера, а если это и можно сделать (с регулировкой совместимости приложений), то их функциональность ограничивается.

ПРИМЕЧАНИЕ Удаленный рабочий стол

Хотя роль Службы терминалов (Terminal Services) не поддерживается в установке ядра сервера (Server Core), ядро поддерживает подключения к удаленному рабочему столу с других компьютеров, обеспечивая удаленное управление компьютером с ядром сервера. (Отметим, что подключение к удаленному рабочему столу компьютера с ядром сервера не обеспечивает наличия доступных графических средств на удаленном сервере.)

Список компонентов, не поддерживаемых ядром сервера, намного обширней, чем список неподдерживаемых ролей:

- Серверные расширения BITS (BITS Server Extensions);
- Пакет администрирования диспетчера подключений (Connection Manager Administration Kit);

- **Возможности рабочего стола (Desktop Experience);**
- **Управление групповой политикой (Group Police Management);**
- **Клиент печати через Интернет (Internet Printing Client);**
- **Сервер службы имен хранилищ Интернета (Internet Storage Name Server);**
- **Монитор LPR-портов (LPR Port Monitor);**
- **Очередь сообщений (Message Queuing);**
- **Возможности .NET Framework 3.0 (Microsoft .NET Framework 3.0 Features);**
- **Протокол PNRP (Peer Name Resolution Protocol);**
- **Quality Windows Audio Experience;**
- **Удаленный помощник (Remote Assistance);**
- **Удаленное разностное сжатие (Remote Differential Compression);**
- **Средства удаленного администрирования сервера (Remote Server Administration Tools);**
- **RPC через HTTP-прокси (RPC Over HTTP Proxy);**
- **Средства служб для NFS (Services For NFS);**
- **Простые службы TCP/IP (Simple TCP/IP Services);**
- **Сервер SMTP (SMTP Server);**
- **Диспетчер хранилища для сетей SAN (Storage Manager for SANs);**
- **Сервер Telnet (Telnet Server);**
- **Клиент TFTP (TFTP Client);**
- **Внутренняя база данных Windows (Windows Internal Database);**
- **Windows PowerShell;**
- **Служба активации процессов Windows (Windows Process Activation Service);**
- **Диск восстановления Windows (Windows Recovery Disc);**
- **Диспетчер системных ресурсов (Windows System Resource Manager);**
- **Служба беспроводной локальной связи (Wireless LAN Service).**

Причины невозможности установить некоторые из этих компонентов на компьютере с ядром сервера вполне очевидны. Например, компонент Возможности рабочего стола (Desktop Experience) нельзя установить в ядре сервера потому, что ядро не располагает рабочим столом. Средства же удаленного администрирования сервера (Remote Server Administration Tools, RSAT) невозможно установить в ядре сервера из-за того, что эти консольные инструменты MMC (Microsoft Management Console) запускаются в окнах, а в случае отсутствия рабочего стола окон не существует. Возможно, вам непонятно, почему их нельзя установить в ядре сервера. Обычно причины кроются в скрытых зависимостях, не позволяющих компоненту работать на основе ограниченного набора двоичных файлов операционной системы, доступного в ядре сервера. Чтобы прояснить эти моменты, в следующем разделе мы рассмотрим архитектуру установки обоих типов: установки ядра сервера (Server Core) и полной установки Windows Server 2008.

И наконец, в то время как список графических инструментов, доступных в ядре сервера, довольно короток (см. табл. П-7), список графических средств, отсутствующих в ядре сервера, намного длиннее.

Далее приведен список инструментов GUI (правда, не полный), которые не доступны в ядре сервера:

- оболочка рабочего стола Windows (Explorer.exe);
- структура .NET Framework и CLR;
- консоль управления Microsoft Management Console (Mmc.exe) и ее многочисленные оснастки;
- большинство апплетов панели управления;
- Internet Explorer;
- проигрыватель Windows Media (Windows Media Player);
- почта Windows (Windows Mail).

Отсутствие многих из этих инструментов в ядре сервера является причиной определенных последствий, в том числе описанных далее.

- Отсутствие Internet Explorer означает отсутствие движка прорисовки HTML, то есть на компьютере с ядром сервера нельзя просмотреть справку HTML (HTML Help). Так что если вам в Windows Server 2008 требуется справка, придется выполнять полную установку продукта.
- Отсутствие консоли MMC и ее оснасток вызывает сложности с локальным администрированием компьютера с ядром сервера, поскольку придется обходиться лишь командной строкой. Это означает, что управление компьютером с помощью инструментов MMC можно осуществлять только удаленным образом, поскольку MMC нельзя запустить локально.
- Отсутствие оболочки рабочего стола указывает на отсутствие панели задач, области уведомлений и всплывающих сообщений. Таким образом, в случае отказа сетевых подключений на сервере ядра, истечения срока действия пароля или, скажем, при необходимости выполнить активацию приложения вы не увидите соответствующего всплывающего сообщения.
- Отсутствие .NET Framework свидетельствует о невозможность запуска на компьютере с ядром сервера управляемого кода. В частности, нельзя локально запускать сценарии Windows PowerShell. Однако сценарии PowerShell, в которых используется Инструментарий управления Windows (Windows Management Instrumentation, WMI), можно удаленно запускать на компьютерах с ядром сервера, поскольку ядро сервера включает в себя многих (но не всех) поставщиков WMI из набора полной установки сервера.
- Очень малое количество апплетов в панели управления (в ядро сервера включены лишь апплеты Язык и региональные стандарты (Regional and Language Options, Intl.cpl) и Дата и время (Date and Time, Timedate.cpl)) означает сложности конфигурирования компьютера с ядром сервера. Для автоматизации задач конфигурации на компьютерах с ядром сервера можно использовать сценарии или применить автоматизированную установку, в которой будут выполнены все необходимые послеустановочные задачи конфигурации.

ПРИМЕЧАНИЕ Файлы DLL-оболочки

Хотя ядро сервера не включает программу Explorer.exe, оно все же содержит файлы Shell32.dll и Shlwapi.dll.

Проверьте себя

1. Почему в ядро сервера включен Диспетчер задач (Task Manager)?
2. Почему в ядре сервера доступна программа Блокнот (Notepad)?

Ответы

1. В случае закрытия оболочки командной строки ядра сервера новое окно можно открыть, запустив в Диспетчере задач новый экземпляр cmd.exe.
2. Блокнот можно использовать для просмотра файлов журнала, написания сценариев и выполнения на компьютере с ядром сервера множества других действий.

Архитектура полной установки Windows Server 2008

На рис. П-12 показана архитектура полной установки Windows Server 2008. Такая архитектура включает компоненты для всех типов установки (полной и ядра сервера), а также компоненты, доступные лишь при полной установке.

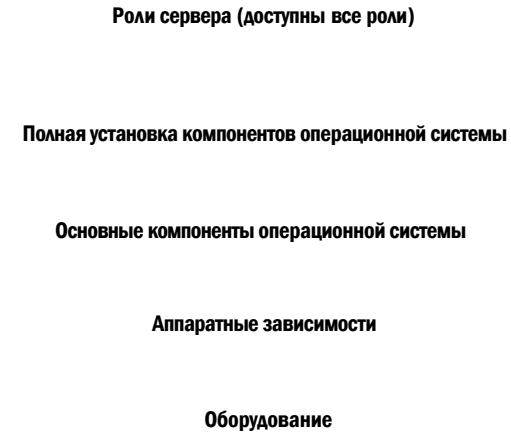


Рис. П-12. Архитектура полной установки Windows Server 2008

Компоненты операционной системы, доступные в установках обоих типов, включают функциональность вызовов удаленных процедур (RPC), сетевой стек, функции безопасности, компонентную модель CBS (Component-Based Servicing), Диспетчер пакетов Windows (Package Manager, Pkgmgr.exe), утилиту Установка необязательного компонента Windows (OCSetup.exe) и т. д. Полная установка Windows Server 2008 включает множество дополнительных компонентов, в том числе .NET Framework, CLR, оболочку рабочего стола Windows. Различные роли, которые можно запускать при полной установке, используют эти многочисленные компоненты операционной системы для своей работы.

Архитектура установки ядра сервера Windows Server 2008

На первый взгляд, архитектура ядра сервера практически аналогична архитектуре полной установки, в чем можно убедиться, взглянув на рис. П-13.

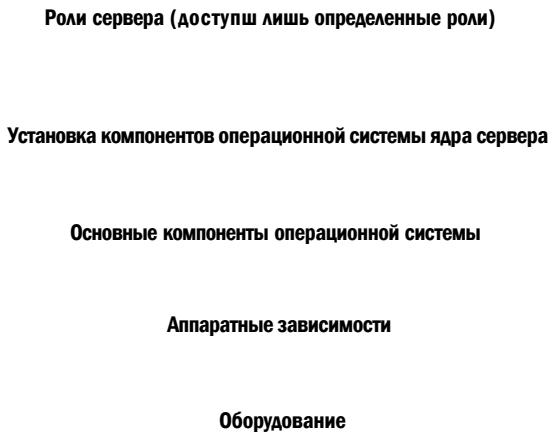


Рис. П-13. Архитектура установки ядра сервера Windows Server 2008

Ключевое отличие между ними состоит в том, что ядро сервера содержит компоненты операционной системы, отсутствующие в полной установке. Примерами таких эксклюзивных компонентов являются OCList.exe, SCRegEdit.wsf и некоторые другие. Сравнив эти две архитектуры, можно сделать следующие важные выводы.

- Архитектура Windows Server 2008 является модульной, то есть состоит из нескольких уровней функциональности, на самом нижнем из которых функционирует оборудование операционной системы, а на верхнем роли сервера обеспечивают работу важных для пользователей и компьютеров служб в сети.
- Оба типа установки (полная и ядра сервера) основаны на еще меньшем наборе компонентов ядра операционной системы. При выполнении каждого типа установки к этим компонентам ядра добавляется собственный уникальный набор дополнительных компонентов операционной системы с целью поддержки требований функциональности установки.

Сравнивая рис. П-12 и П-13, следует учитывать, что ядро сервера является не версией или выпуском Windows Server 2008, а лишь опцией установки. Это означает, что если отдельный двоичный файл существует в обоих типах установки, то это один и тот же двоичный файл. В обеих опциях установки используется одно и то же ядро.

Однако сказанное касается не всех выпусков. Ядро в выпуске Standard Edition не идентично ядру в выпусках Enterprise Edition и Datacenter Edition. Если бы в различных выпусках использовалось идентичное ядро, эти выпуски не смогли бы содержать разные уровни симметричного мультипроцессирования (Symmetric Multiprocessing, SMP).

Развертывание ядра сервера

Поскольку ядро сервера (Server Core) представляет один из вариантов установки Windows Server 2008, его можно развернуть любым из следующих методов:

- **установка с DVD-диска (ручная или автоматизированная);**
- **установка из конфигурационного набора на переносном носителе или в сетевом общем ресурсе;**
- **установка из образа с помощью инструмента ImageX или программы Windows Setup.**

Кроме того, ядро сервера можно развернуть с применением других технологий развертывания, в частности с помощью Службы развертывания Windows (WDS), средства Microsoft Deployment и программного пакета System Center Configuration Manager.

Невозможность обновления существующей системы

Ядро сервера можно установить лишь с использованием метода установки с нуля, то есть развернуть на «голом» оборудовании (Bare-Metal System). Ядро сервера также можно установить во второй раздел существующей системы Windows Server, хотя многовариантная загрузка в корпоративных средах не приветствуется. Другими словами, ядро сервера нельзя установить путем обновления существующей операционной системы. В частности:

- **предыдущие версии Windows Server невозможно обновить до ядра сервера Windows Server 2008;**
- **ядро сервера нельзя установить путем обновления полной установки Windows Server 2008;**
- **установку ядра сервера нельзя обновить до полной установки Windows Server 2008.**

Таким образом, возможна лишь полная установка ядра сервера, без вариантов обновления.

Ядро сервера и драйверы устройств

Следует учитывать, что развертывание ядра сервера обеспечивает более ограниченный набор встроенных драйверов (In-Box), чем полная установка. Цель ограничения количества встроенных драйверов заключается в уменьшении размера установки ядра сервера и снижении уровня требований жесткого диска. В частности, ядро сервера включает встроенные драйверы для устройств следующих классов:

- **устройств хранения;**
- **стандартных видеокарт VGA;**
- **сетевых адаптеров.**

Драйверы для устройств указанных классов, включенные в ядро сервера, идентичны драйверам для устройств этих классов в полной установке. Отметим, что ядро сервера также включает подсистему plug and play, которая присутствует и в полной установке Windows Server 2008. Эта подсистема позволяет ядру сервера устанавливать доступные встроенные драйверы (In-box) для оборудования, обнаруженного в процессе установки.

Упражнение. Анализ ядра сервера

В этом упражнении вы проанализируете установку ядра сервера (Server Core), в частности выясните, какие инструменты GUI для настройки установки ядра сервера доступны в окне командной строки.

Для выполнения упражнения можно использовать сервер Corel, установка которого описана во введении к данной книге. Однако вы также можете воспользоваться любой установкой ядра сервера. Прежде чем приступить к упражнению, войдите на сервер как администратор.

1. **В командную строку ядра сервера введите команду** *notepad,* **чтобы открыть программу Блокнот (Notepad).**
2. **В меню Файл (File) программы Блокнот (Notepad) примените команду Открыть (Open). Отметим, что программа Блокнот (Notepad) в ядре сервера использует старую версию Windows 3.1 диалогового окна Открыть (Open).**
3. **В меню Справка (Help) программы Блокнот (Notepad) выберите команду Вызов справки (View Help). Вы увидите, что ничего не произошло — ядро сервера не поддерживает Справку Windows (Windows Help) как приложение.**
4. **Закройте Блокнот (Notepad) и в командную строку ядра сервера введите команду** *regedit,* **чтобы открыть Редактор реестра (Registry Editor).**
5. **Закройте Редактор реестра (Registry Editor) и в командную строку введите команду** *control timedate.cpl.* **Откроется апплет панели управления Дата и время (Date And Time), с помощью которого можно отконфигурировать дату и время на сервере.**
6. **Закройте апплет Дата и время (Date And Time) и в командную строку введите команду** *control sysdm.cpl.* **Апплет Система (System) панели управления не откроется. Вместо него вы увидите сообщение об ошибке «Не удается найти "SystemPropertiesComputerName.exe". Проверьте, правильно ли указано имя, и повторите попытку» (Windows cannot find "SystemPropertiesComputerName.exe". Make sure you typed the name correctly, and then try again). Поэтому имя компьютера с ядром сервера и членство в домене придется конфигурировать с помощью других методов.**
7. **Щелкните ОК, чтобы закрыть окно с сообщением об ошибке, а затем введите следующие две команды:**

   ```
   net start > services.txt
   notepad services.txt
   ```

   Первая команда отображает список всех текущих служб Windows, которые запущены в системе, и сохраняет этот список в файл %USERPROFILE%\Services.txt. Вторая команда открывает файл Services.txt в программе Блокнот (Notepad).

   По умолчанию в ядре сервера запущено 40 служб без дополнительных ролей и компонентов.
8. **Закройте Блокнот (Notepad). Затем закройте окно командной строки ядра сервера, щелкнув в верхнем правом углу окна кнопку в виде красного крестика Закрыть (Close). Теперь экран должен быть абсолютно пустым. Окно командной строки можно вернуть, нажав клавиши Ctrl+Alt+Del и выбрав**

опцию Запустить диспетчер задач (Start Task Manager). В открывшемся Диспетчере задач (Task Manager) перейдите на вкладку Приложения (Applications) и шелкните кнопку Новая задача (New Task).

9. В диалоговом окне Создать новую задачу (Create New Task) введите *cmd.exe* и щелкните ОК. Откроется окно командной строки ядра сервера. После этого вы можете закрыть Диспетчер задач. Новая командная строка будет отличаться от старой: по умолчанию текущим каталогом командной строки ядра сервера является папка пользовательского профиля. Текущим каталогом новой командной строки, открытой с помощью диспетчера задач, является папка %WINDIR%\System32. Каталог пользовательского профиля можно вернуть с помощью команды *cd %userprofile%* в новой командной строке.
10. В командную строку введите команду *ipconfig.* Для ядра сервера DHCP-сервер в сети должен назначить динамический IP-адрес.
11. В командную строку введите команду *msinfo32.* Откроется окно инструмента Сведения о системе (System Information), где отобразится информация о программном обеспечении и оборудовании системы. Разверните узел Сведения о системе (System Summary) и элемент Программная среда (Software Environment), после чего выберите Задания для принтера (Print Jobs). В панели справа отобразится сообщение об ошибке «Нет доступа к средствам WMI. Файлы управления Windows были перемещены или удалены» (Cannot access the Windows Management Instrumentation software. Windows Management Instrumentation files may be moved or missing). Это сообщение указывает, что в установке ядра сервера недоступны некоторые поставщики WMI.
12. Чтобы завершить работу ядра сервера, в командную строку введите команду *shutdown /s /t 0.*

Выполнение задач по конфигурированию после развертывания

После установки ядра сервера (Server Core) или полной установки Windows Server 2008 в системе перед использованием сервера для целей производства потребуется выполнить множество задач, связанных с настройкой, начиная с назначения временного пояса и заканчивая установкой и конфигурированием ролей, служб ролей и компонентов. Многие из этих задач можно автоматизировать.

В данном разделе вы ознакомитесь с различными способами выполнения послеустановочных задач при развертывании системы Windows Server 2008, начиная с конфигурирования серверов вручную с помощью инструментов GUI и командной строки и заканчивая автоматизацией задач с использованием файлов ответов.

Послеустановочные задачи

После успешной установки Windows Server 2008 требуется отконфигурировать систему, а также установить роли и компоненты для функционирования сервера в сети.

Послеустановочные задачи в Windows Server 2008 можно выполнять различными способами, включая следующие:

- локальное использование доступных на сервере инструментов GUI для администрирования;
- локальная настройка с помощью командной строки (включая сценарии пакетной обработки);
- удаленное использование Средств удаленного администрирования сервера (Remote Server Administration Tools, RSAT), Служб терминалов (Terminal Services), сценариев WMI или PowerShell, а также оболочки Windows Remote Shell (WinRS).

Различные инструменты позволяют выполнять разные задачи по конфигурированию. Поэтому нужно знать, с помощью каких инструментов можно реализовать те или иные задачи. Кроме того, по причине ограниченного набора двоичных файлов некоторые задачи конфигурирования в ядре сервера выполняются не так, как в полной установке. Задача IT-администратора состоит в том, чтобы правильно выбирать средства, которые можно использовать для решения конкретных задач в установках сервера обоих типов.

Послеустановочные задачи можно разбить на две общие категории.

- Начальные задачи конфигурирования, например настройка сетевых параметров, выбор временного пояса, включение удаленного рабочего стола, активация установки и многие другие операции, которые нужно выполнять на всех серверах, развертываемых в сети.
- Добавление ролей и компонентов, позволяющих серверу выполнять специфические функции в сети и обеспечивать конкретный набор функций.

Далее мы рассмотрим некоторые способы выполнения послеустановочных задач конфигурирования на компьютерах с ядром сервера и полной установкой Windows Server 2008. Вначале будут описаны задачи по конфигурированию полной установки, чтобы позже показать, чем отличается выполнение этих задач в ядре сервера.

Выполнение начальных задач по конфигурированию в полной установке Windows Server 2008

Самый простой способ выполнения начальных задач по конфигурированию на компьютере с полной установкой Windows Server 2008 заключается в использовании опций диалогового окна Задачи начальной настройки (Initial Configuration Tasks), показанного на рис. П-14.

С помощью этого окна на всех серверах, развернутых в сети, можно выполнять следующие задачи:

- создание пароля для локальной учетной записи администратора;
- конфигурирование сетевых параметров TCP/1P-сервера;
- изменение имени компьютера;
- присоединение сервера к домену;
- включение автоматического обновления на серверах с помощью Центра обновления Windows (Windows Update);
- загрузка и установка всех доступных обновлений в центре обновления Windows;

- генерирование отчетов об ошибках Windows (Windows Error Reporting) для программы улучшения качества программного обеспечения (Customer Experience Improvement Program);
- включение удаленного рабочего стола (Remote Desktop) на сервере;
- включение брандмауэра Windows (Windows Firewall) на сервере.

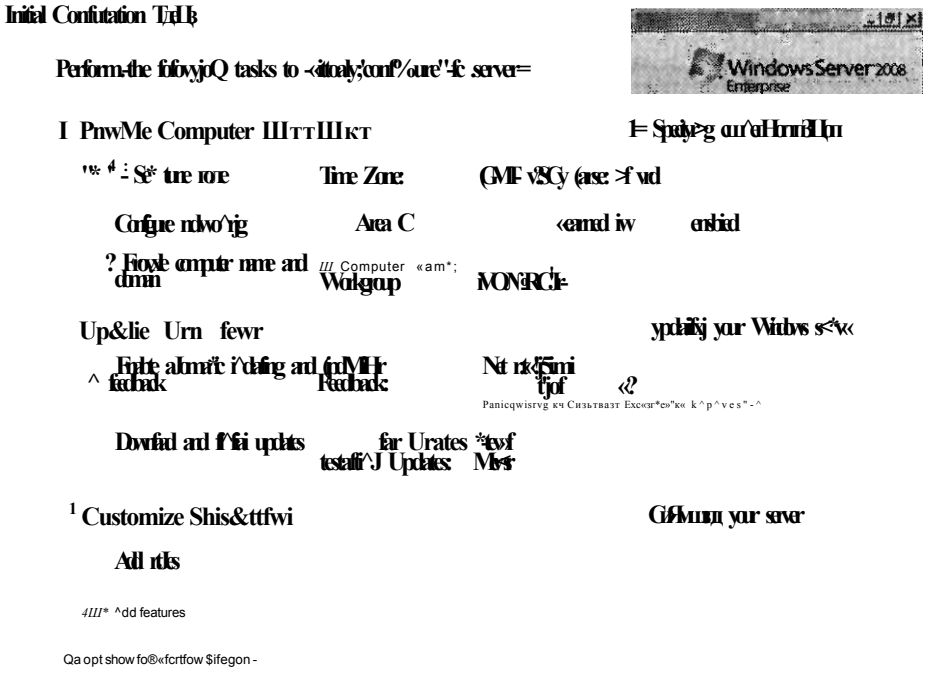


Рис. П-14. Задачи начальной настройки полной установки Windows Server 2008

ПРИМЕЧАНИЕ Открытие окна начальных задач по конфигурированию с помощью команды Oobe

Если в диалоговом окне Задачи начальной настройки (Initial Configuration Tasks) установлен флажок Не показывать это окно при входе в систему (Do Not Show This Window Again At Logon), данное окно можно открыть, задав команду *Oobe.exe* в окне Выполнить (Run), поле Начать поиск (Start Search) или в командной строке.

Помимо выполнения этих задач в окне Задачи начальной настройки (Initial Configuration Tasks) можно запустить Мастер добавления ролей (Add Roles Wizard) и Мастер добавления компонентов (Add Features Wizard), чтобы установить на сервер дополнительные роли и компоненты.

Проще всего эти задачи выполнить в полной установке Windows Server 2008, войдя локально на сервер после завершения программы Windows Setup. Каждая такая задача выполняется вручную, но некоторые из них можно автоматизировать в самом процессе установки. Например, пароль для локальной учетной

записи администратора можно назначить с помощью следующего параметра файла ответов:

```
Microsoft-Windows-Shell-Setup\UserAccounts\AdministratorPassword
```

Аналогичным образом во время установки можно определить временной пояс, отконфигурировав в файле ответов параметр Microsoft-Windows-Shell-Setup (рис. П-15).

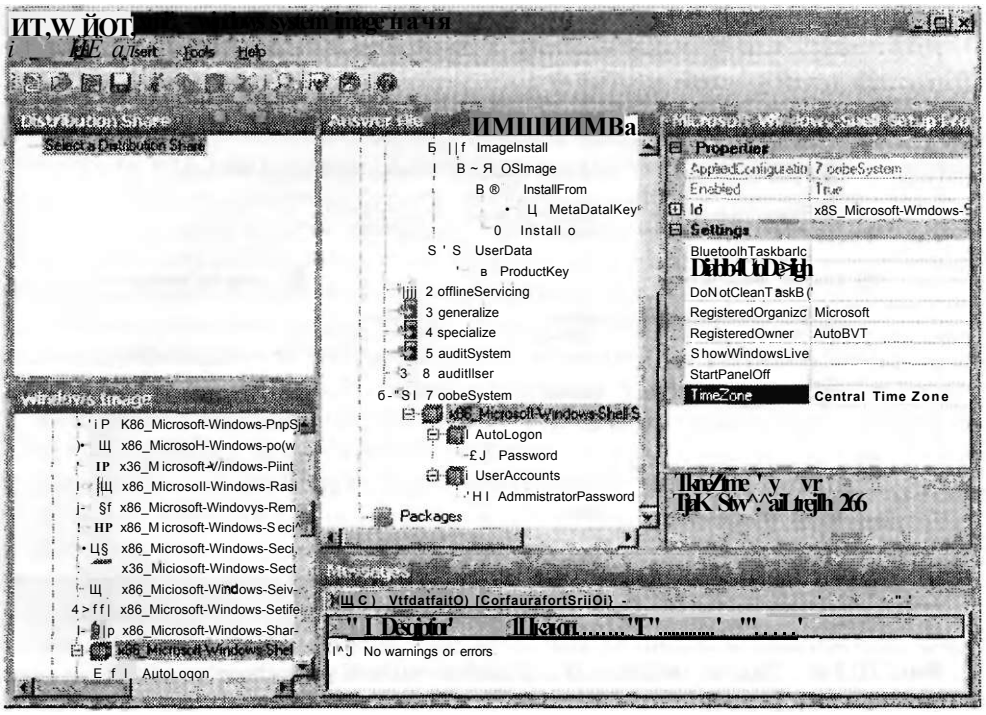


Рис. П-15. Назначение временного пояса в файле ответов

Чтобы во время установки включить на сервере удаленный рабочий стол (Remote Desktop), нужно настроить следующий параметр файла ответов:

```
Microsoft-Windows-TerminalServices-LocalSessionManager
```

Для этого добавьте указанный параметр в секцию этапа настройки offline-Servicing файла ответов, а затем с помощью Windows SIM назначьте параметру fDenyTSConnections булево значение False, как показано на рис. П-16.

После включения на сервере удаленного рабочего стола другие задачи начальной настройки можно выполнять удаленно посредством подключения к удаленному рабочему столу на еще одном компьютере и получения удаленного доступа к рабочему столу сервера. Отметим, что по умолчанию при включении удаленного рабочего стола с помощью параметра Microsoft-Windows-Terminal-Services-LocalSessionManager файла ответов проверка подлинности пользователей, удаленно подключающихся к серверу, будет выполняться согласно опции Разрешать подключения только от компьютеров с удаленным рабочим столом

с сетевой проверкой подлинности (Allow Connections Only From Computers Running Remote Desktop With Network Level Authentication).

Этот самый безопасный тип проверки подлинности подключений к удаленному рабочему столу разрешает подключения только от компьютеров Windows Vista или Windows Server 2008 (или же на компьютере Windows XP должно быть загружено и установлено программное обеспечение Remote Desktop Connection 6.1). Чтобы обеспечить большую гибкость, для удаленных подключений можно использовать опцию Разрешать подключения от компьютеров с любой версией удаленного рабочего стола (Allow Connections Only From Computers Running Any Version Of Remote Desktop).

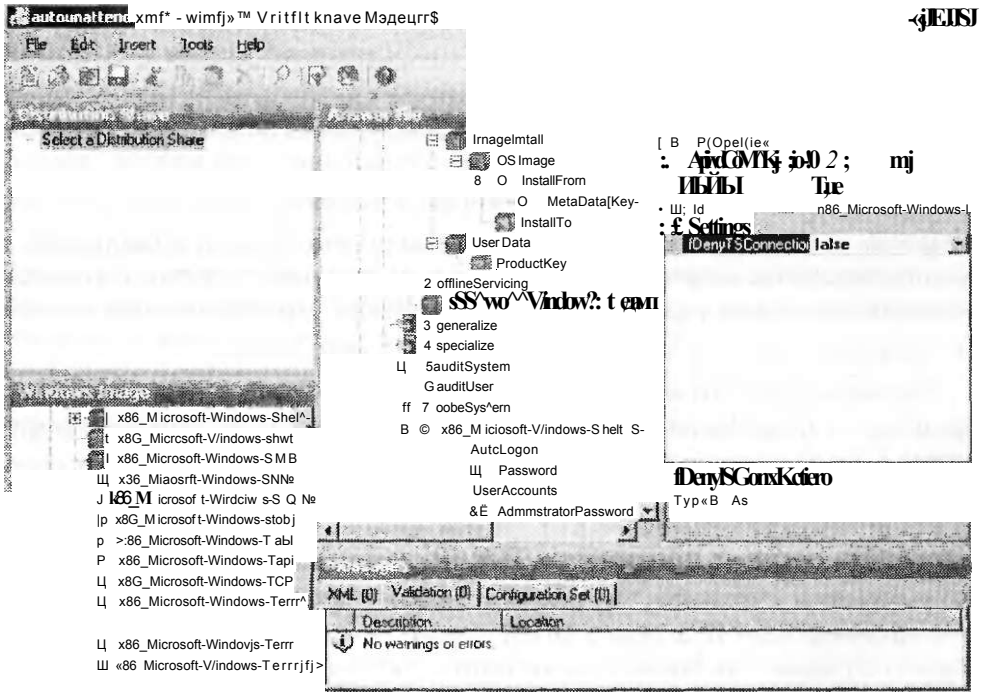


Рис. П-16. Включение удаленного рабочего стола с помощью файла ответов

При необходимости отконфигурировать этот тин проверки подлинности в файле ответов добавьте параметр Microsoft-Windows-TerminalServices-RDP-WinStationExtensions в секцию этапа настройки specialize файла ответов и в Windows SIM назначьте параметру UserAuthentication значение 0.

Задачи начальной настройки на компьютере с ядром сервера

Выполнение задач по начальной настройке на компьютере с установленным ядром сервера очень отличается от выполнения тех же задач на компьютере с полной установкой Windows Server 2008. Связано это с тем, что в ядре сервера

отсутствует рабочий стол и нельзя использовать такие инструменты, как окно Задачи начальной настройки (Initial Configuration Tasks). Все задачи начальной настройки, выполняемые в полной установке Windows Server 2008, также можно выполнять и в установке ядра сервера, однако для этого нужно хорошо знать соответствующие инструменты командной строки Windows и несколько сценариев. Далее мы опишем настройку новой установки ядра сервера с помощью оболочки командной строки.

Назначение пароля локального администратора

На компьютере с установленным ядром сервера пароль локального администратора можно назначить в командной строке с помощью следующей команды:

```
net user administrator *
```

Дважды введите новый пароль, после чего пароль этой учетной записи будет изменен. С помощью команд *net* на компьютере с ядром сервера можно выполнять и другие задачи. Например, задав команду, указанную ниже, пользователя можно добавить в локальную группу администраторов:

```
net localgroup Administrators /add домен/имя_пользователя
```

В этом примере следует указать домен и имя пользователя, добавляемого в группу локальных администраторов сервера. С помощью следующей команды пользователя можно удалить из группы локальных администраторов сервера:

```
net localgroup Administrators /remove домен/имя_пользователя
```

Указанные команды можно применять и по отношению к другим локальным группам. А с помощью этой команды во встроенной локальной группе Пользователи (Users) можно создать новую пользовательскую учетную запись:

net user *имя_пользователя* * **/add**

Настройка сетевых параметров TCP/IP

По умолчанию в установку ядра сервера включен протокол DHCP для получения динамического IP-адреса с DHCP-сервера в сети (если таковой имеется). Однако серверам, как правило, назначаются статические IP-адреса. Для конфигурирования параметров статического IP-адреса на компьютере с ядром сервера с помощью одной лишь командной строки можно использовать команду *Netsh.exe.*

Перед попыткой настроить статический адрес следует просмотреть список текущих адаптеров и подключений сервера. Для этого достаточно ввести команду:

```
netsh interface ipv4 show interfaces
```

Запомните номер сетевого интерфейса Подключение по локальной сети (Local Area Connection), отображаемого в результатах выполнения команды *netsh* **в столбце Инд (IDX). Этот номер понадобится для выполнения других команд *netsh*, описанных далее.**

Чтобы назначить интерфейсу IP-адрес, введите такую команду:

```
netsh interface ipv4 set address name=ID source=static IP SM DG
```

В этом примере параметром ID является номер (индекс) интерфейса, параметром IP — назначаемый IP-адрес, параметром SM — маска подсети, а параметром DG — основной шлюз.

Если вы назначаете серверу статический адрес, для него также нужно указать статический адрес DNS-сервера. Это можно сделать с помощью команды:

```
netsh interface ipv4 add dnsserver name=ID address=DNSIP index=1
```

В данном примере ID — это номер (индекс) интерфейса, а DNSIP — IP-адрес DNS-сервера. Указанную команду можно повторять для добавления резервных DNS-серверов, однако при этом следует учитывать приращение индекса.

Для включения DHCP на сервере предназначена команда:

```
netsh interface ipv4 set address name=I0 source dhcp
```

Изменение имени сервера

Если вам понадобится изменить имя компьютера с установленным ядром сервера перед присоединением к домену, в командную строку введите следующую команду Netdom.exe:

```
netdom renamecomputer %computername% /He\нN°me:H0B0E_ИМЯ
```

Для проверки имени в командную строку нужно ввести команду *hostname.* **В качестве альтернативы можно ввести команду** *set* **и проанализировать содержимое переменной среды** *% COMPUTERNAME%,* **либо для отображения имени компьютера ввести команду** *echo % COMPUTERNAME%.*

ПРИМЕЧАНИЕ Изменение имени компьютера

После изменения имени компьютера нужно перезагрузить сервер, чтобы изменение вступило в силу.

Если сервер уже присоединен к домену, то для изменения его имени нужно воспользоваться такой командой:

```
netdom renamecomputer %computername% /NewName:H0B0E_ИМЯ /userd:домен\имя_
пользователя /passwordd:*
```

Присоединение к домену

Инструмент Netdom.exe также можно использовать для присоединения или удаления сервера из домена. Чтобы присоединить сервер к домену, используйте следующую команду:

```
netdom join ИМЯ /domain-.ДОМЕН /userd-.ADMINUSER /passwordd:*
```

В этом примере *имя* **— это имя сервера,** *ДОМЕН* **— имя домена, к которому присоединяется сервер, а** *ADMINUSER* **— учетная запись администратора домена.**

При необходимости удалить сервер из домена введите команду:

```
netdom remove ИМЯ /domain-.ДОМЕН /userd-.ADMINUSER /passwordd:*
```

ПРИМЕЧАНИЕ Присоединение к домену и удаление из него

После присоединения сервера к домену или его удаления нужно перезагрузить компьютер, чтобы изменения вступили в силу.

Включение автоматического обновления

Сценарий Scregedit.wsf можно использовать для конфигурирования различных аспектов установки ядра сервера, включая следующие:

- включение автоматического обновления;
- разрешение клиентам удаленного рабочего стола предыдущих версий Windows подключаться к компьютеру с установленным ядром сервера;
- настройка веса и приоритета SRV-записи DNS;
- удаленное управление Монитором IP-безопасности (IPsec Monitor).

СОВЕТ Подготовка к экзамену

Ознакомьтесь с различными опциями командной строки сценария scregedit.wsf. Для просмотра списка доступных опций в командную строку ядра сервера введите команду *cscript %syspemroot% \system32\scregedit.wsf* /?. А для просмотра команд, с помощью которых можно конфигурировать установку ядра сервера, можно ввести команду *cscript %syspemroot%\system32\scregedit.wsf /sli.*

Для того чтобы с помощью сценария Scregedit.wsf включить автоматическое обновление установки ядра сервера, введите команду:

```
cscript %systemroot%\system32\scregedit.wsf /AU 4
```

Наконец, для отключения автоматического обновления предназначена команда:

```
cscript %systemroot%\system32\scregedit.wsf /AU 1
```

ПРИМЕЧАНИЕ Настройка автоматического обновления

Для настройки других параметров автоматического обновления лучше всего использовать групповую политику.

Включение удаленного рабочего стола

Сценарий Scregedit.wsf также используется для настройки удаленного рабочего стола на компьютере с установленным ядром сервера. Например, чтобы сервер принимал подключения к удаленному рабочему столу, введите следующую команду:

```
cscript %systemroot%\system32\scregedit.wsf /ar 0
```

А для того чтобы отключить удаленный рабочий стол на сервере, достаточно задать команду:

```
cscript %systemroot%\system32\scregedit.wsf /ar 1
```

Если вы хотите разрешить клиентам предыдущих версий удаленного рабочего стола подключаться к компьютеру с ядром сервера, нужно вначале отключить уровень усиленной безопасности, по умолчанию назначенный удаленному рабочему столу:

```
cscript %systemroot%\system32\scregedit.wsf /cs 0
```

И наконец, для просмотра текущей конфигурации удаленного рабочего стола на сервере введите команду:

```
cscript %systemroot%\system32\scregedit.wsf /ar /v
```

Включение отчетов об ошибках Windows

Для включения и отключения отчетов об ошибках Windows (Windows Error Reporting, WER) на сервере используется еще один инструмент командной строки — ServerWEROptin.exe. Синтаксис этого инструмента приведен ниже.

```
C:\Windows\System32>serverweroptin /?

ServerWerOption /h[elp] | /q[uery] | /sfummary] | /de[tailed] | /d[isable]

Описание:
Это средство позволяет включить отчеты об ошибках Windows,
чтобы автоматически отправлять описания неполадок
на сервере в корпорацию Майкрософт.
Дополнительные сведения об отчетах об ошибках Windows
см. в заявлении о конфиденциальности по адресу
http://до.microsoft.com/fwlink/?linkid=50163

Список параметров:
/query     Отображение состояния отправки отчетов
           об ошибках Windows,
/summary   Автоматически отправлять сводные отчеты
           с помощью отчетов об ошибках Windows,
/detailed  Автоматически отправлять подробные отчеты
           с помощью отчетов об ошибках Windows,
/disable   Отключить отчеты об ошибках Windows,
/help      Отображение параметров и синтаксиса команды.

Примеры:
ServerWerOptin /query
ServerWerOptin /summary
```

На основе этой информации можно, в частности, понять, что для автоматической отправки детальных отчетов WER в Microsoft нужно использовать следующую команду:

```
serverweroptin /detailed
```

Включение брандмауэра Windows

В командной строке на компьютере с ядром сервера брандмауэр Windows включить немного сложнее по причине использования контекста advfirewall команды *netsh,* для которого существует множество опций. Так что вместо отдельной настройки профилей и правил брандмауэра с помощью команд *netsh advfirewall* лучше просто включить удаленное управление брандмауэром для всех профилей с помощью такой команды:

```
netsh adbfirewall set allprofiles settings remotamanagement enable
```

После ее выполнения можно использовать компонент Управление групповой политикой (Group Policy Management) с административной рабочей станции Windows Vista или с сервера с полной установкой Windows Server 2008. Оснастка

Брандмауэр Windows в режиме повышенной безопасности (Windows Firewall With Advanced Security) обеспечит для Редактора объектов групповой политики (Group Policy Editor) простой способ удаленной настройки брандмауэра Windows на компьютерах Windows Vista и Windows Server 2008 (включая компьютеры с установленным ядром сервера).

Автоматизация задач начальной настройки

Для автоматизации некоторых задач, связанных с начальной настройкой на компьютере с установленным ядром сервера, можно использовать те же параметры файла ответов, которые применяются в полной установке системы Windows Server 2008. Как и в случае с полной установкой, на компьютере с ядром сервера можно автоматизировать лишь некоторые задачи по начальной настройке.

Добавление ролей и компонентов в полной установке Windows Server 2008

После выполнения задач начальной настройки на сервер можно установить роли и компоненты, чтобы включить в сети требуемую функциональность. Например, на сервере можно установить роль DHCP-сервер (DHCP Server) — в таком случае сервер будет назначать IP-адреса клиентским компьютерам.

Установка ролей и компонентов Windows Server 2008 выполняется различными способами, в том числе такими:

- с помощью инструмента командной строки ServerManagerCmd.exe;
- запуск Мастера добавления ролей (Add Roles Wizard) или Мастера добавления компонентов (Add Features Wizard) — щелчком соответствующей ссылки в окне Задачи начальной настройки (Initial Configuration Tasks);
- запуск Мастера добавления ролей (Add Roles Wizard) или Мастера добавления компонентов (Add Features Wizard) — щелчком правой кнопкой мыши соответствующего узла в Диспетчере сервера (Server Manager).

Все три способа можно применять для установки и удаления ролей и компонентов вручную.

Для автоматизации процесса установки ролей и компонентов утилиту ServerManagerCmd.exe нужно использовать вместе с файлом ответов, как будет продемонстрировано далее.

Ручная установка ролей и компонентов с помощью мастеров

Роли и компоненты можно добавлять вручную, с помощью соответственно Мастера добавления ролей (Add Roles Wizard) и Мастера добавления компонентов (Add Features Wizard).

Для того чтобы добавить на сервер, скажем, роль DHCP-сервер (DHCP Server), в области Настроить этот сервер (Customize This Server) окна Задачи начальной настройки (Initial Configuration Tasks) щелкните ссылку Добавить роли (Add Roles). В процессе работы мастера вам потребуется ввести дополнительную информацию, необходимую для конфигурирования устанавливаемой роли (рис. П-17).

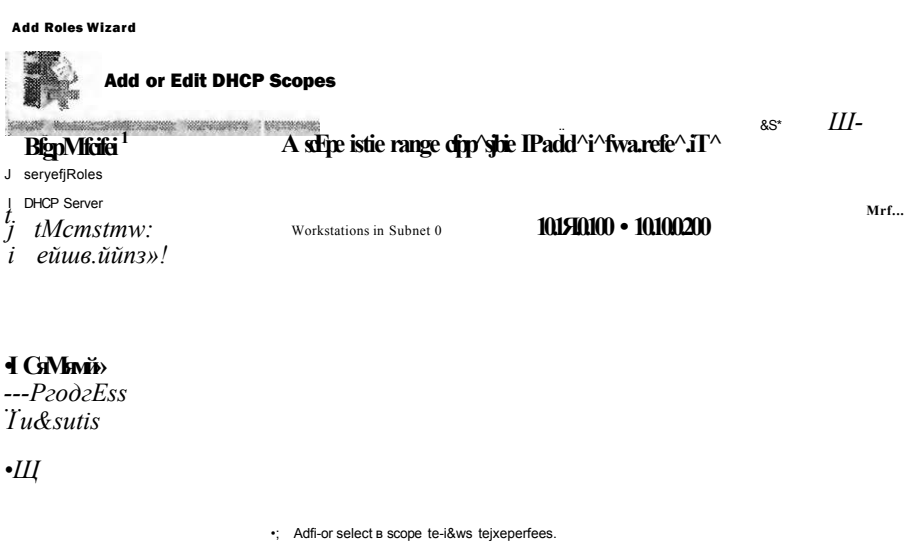


Рис. П-17. Установка роли DHCP-сервера с помощью мастера добавления ролей

Установка ролей и компонентов вручную с помощью утилиты ServerManagerCmd.exe

Роли и компоненты можно также добавлять вручную с помощью утилиты командной строки ServerManagerCmd.exe. Этот инструмент позволяет устанавливать и удалять роли и компоненты, а также предварительно просматривать компоненты, которые будут установлены в случае добавления на сервер отдельной роли или компонента. Далее описаны параметры, которые принимает инструмент ServerManager.exe.

- **-query [<query.xml>] Отображает список всех ролей, служб ролей и компонентов, установленных и доступных на сервере. Для того чтобы сохранить результаты запроса в XML-файле, вместо параметра query.xml укажите имя XML-файла.**
- **-inputPath <answer.xml> Устанавливает или удаляет роли, службы ролей икомпоненты, указанные в файле ответов XML, представленном параметром <answer.xml>.**
- **-install <name> Устанавливает роль, службу ролей или компонент, указанный параметром <name>.**
- **-remove <name> Удаляет роль, службу ролей или компонент, указанны!'] параметром <name>.**

Параметр <name> указывает роль или компонент, который требуется установить или удалить с помощью инструмента ServerManagerCmd.exe. Например, значением параметра <name> для роли DHCP-сервера является DHCP, а значением параметра <name> для роли Доменные службы Active Directore (Active Directory Domain Services, AD DS) — ADDS-Domain-Controller. Параметр <name> нечувствителен к регистру.

Далее следует несколько примеров использования утилиты ServerManager. Cmd.exe для выполнения задач, связанных с ролями и компонентами.

- **servermanagercmd -install Web-Server -whatif Определяет, какие роли, службы ролей и компоненты будут установлены вместе с ролью Веб-сервер (IIS). Эта команда сравнивает список ролей, служб ролей и компонентов роли Веб-сервер (IIS) со списком элементов, уже установленных на сервере. Будут идентифицированы лишь те роли, службы ролей и компоненты, которые еще не установлены на сервере. Параметр -whatif позволяет определить полный список действий, которые будут выполнены командой ServerManagerCmd.exe в случае установки указанной роли, службы или компонента.**
- **servermanagercmd -install Web-Server Выполняет те же действия, что и предыдущая команда с параметром -whatif, то есть устанавливает роль Веб-сервер (IIS).**
- **servermanagercmd -remove Web-Server Удаляет роль Веб-сервер (IIS). Все остальные роли и компоненты, зависящие от роли Веб-сервер (IIS), скажем, Windows SharePoint Services, также будут удалены.**
- **servermanagercmd -remove Web-Server -resultPath** *results.xm* **Выполняет те же действия, что и предыдущая команда, однако с использованием параметра -resultPath. Инструмент ServerManagerCmd.exe сохранит результаты операции удаления в XML-файле, который позже можно будет проанализировать.**
- **servermanagercmd -install Terminal-Services -restart Устанавливает на сервер роль Службы терминалов (Terminal Services). Поскольку при установке ролей требуется перезагрузка, с помощью параметра -restart можно автоматически перезагружать машину после установки роли. Если параметр -restart не используется, компьютер для завершения процесса установки роли потребуется перезагрузить вручную.**
- **servermanagercmd -inputPath** *input.xml* **Позволяет установить или удалить множество ролей, служб ролей и компонентов с помощью команды ServerManagerCmd.exe. Таким образом, вы можете установить или удалить сразу все роли, службы ролей и компоненты, не используя множество команд -** *install* **или** *-remove.* **В файле input.xml можно указать любое количество элементов. Далее приведен пример типичного файла input.xml.**

```
<?xml version="1.0" encoding="utf-8" ?>
<ServerManagerConfiguration Action="Install"
   xmlns="http://schemas.microsoft.com/sdm/Windows/ServerManager/
   Configuration/2007/1"
   xmlns:xs=http://www.w3.org/2001/XMLSchema>
      <Feature Id="NLB"                    InstallAllSubFeatures="true"/>
      <Feature Id="Desktop-Experience"     InstallAllSubFeatures="true"/>
      <Feature Id="NET-Framework"          InstallAllSubFeatures="true"/>
```

```
        <Feature Id= "WSRM"                    InstallAllSubFeatu res="  rue />
        <Feature ld= 'Wireless-Networking"     InstallAllSuDFeatures="  rue />
        <Feature ld= 'Backup"                  InstallAllSubFeatures="  rue />
        <Feature ld= 'WINS-Server"             InstallAllSubFeatu res="  rue />
        <Feature ld= 'Remote-Assistance"       InstallAllSubFeatures="  rue />
        <Feature Id= 'Simple-TCPIP"            InstallAllSubFeatures="  rue />
        <Feature Id= 'Telnet-Client"           InstallAllSubFeatures="  rue />
        <Feature Id= 'Telnet-Server"           InstallAllSubFeatures="  rue />
        <Feature Id= 'Subsystem-UNIX-Apps"     InstallAllSubFeatu res="  rue />
        <Feature Id= "RPC-over-HTTP-Proxy"     InstallAllSubFeatu res="  rue />
        <Feature Id= 'SMTP-Server"             InstallAllSubFeatures="  rue />
        <Feature ld= 'LPR-Port-Monitor"        InstallAllSubFeatures="  rue />
        <Feature ld= 'Storage-Mgr-SANs"        InstallAllSubFeatures="  rue />
        <Feature ld= 'BITS"                    InstallAllSubFeatu res="  rue />
        <Feature ld= 'MSMQ"                    InstallAllSubFeatures="  rue />
        <Feature Id= "MSMQ-Services"           InstallAllSubFeatures="  rue />
        <Feature ld= 'MSMQ-DCOM"               InstallAllSubFeatu res="  rue />
        <Feature ld= 'WPAS"                    InstallAllSubFeatu res="  rue />
        <Feature ld= 'Windows-Internal-DB"     InstallAllSubFeatu res="  rue />
        <Feature ld= 'BitLocker"               InstallAllSubFeatures="  rue />
        <Featи re ld= 'Multipath-IO"           InstallAllSubFeatu res="  rue />
        <Feature Id= "ISNS"                    InstallAllSubFeatu res="  rue />
        <Feature Id= ' Removable-Sto rage"     InstallAllSubFeatures="  rue />
        <Feature ld= "TFTP-Client"             InstallAllSubFeatures="  rue />
        <Feature ld= "SNMP-Service"            InstallAllSubFeatures="  rue />
        <Feature ld= 'Internet-Print-Client"   InstallAllSubFeatures="  rue />
        <Feature ld= •PNRP"                    InstallAllSubFeatures="  rue />
        <Feature ld= 'CMAK"                    InstallAllSubFeatures="  rue'/>
    </ServerManagerConfiguration>
```

ПРИМЕЧАНИЕ Справка ServerManagerCmd.exe
Для получения справки о синтаксисе ServerManagerCmd.exe в командную строку введите команду *ServerManagerCmd.exe -help.*

Автоматизация установки ролей и компонентов

Процесс установки ролей и компонентов на сервере можно автоматизировать с помощью инструмента ServerManagerCmd.exe и файла ответов Autounattend.xml или Unattend.xml. Для этого в секцию этапа настройки oobeSystem файла ответов нужно добавить компонент Microsoft-Windows-Shell-Setup\FirstLogonCommands, как показано на рис. П-18.

Параметр FirstLogonCommands определяет все команды, требуемые для запуска при первом входе пользователя в систему. Другими словами, команды FirstLogonCommands запускаются после входа пользователя в систему перед отображением рабочего стола. Эти команды запускаются один раз, а уровень их привилегий повышается в соответствии с административными правами вошедшего пользователя. (На компьютере с ядром сервера повышение привилегий

этих команд не требуется, поскольку опция установки ядра сервера не поддерживает контроль учетных записей пользователей (User Account Control).) Такое повышение привилегий необходимо, поскольку команды для конфигурирования сервера или добавления ролей и компонентов, как правило, редактируют реестр или запускают программу Windows Setup с параметрами FirstLogonCommands, указанными в файле ответов. Все команды FirstLogonCommands запускаются синхронно, то есть следующая команда запускается лишь после завершения работы предыдущей.

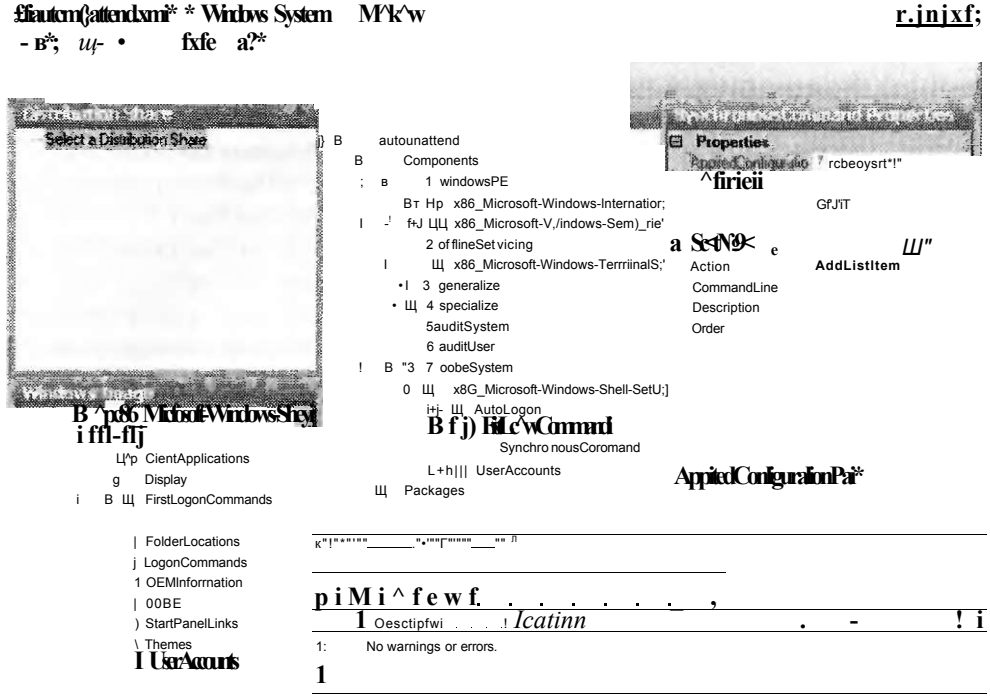


Рис. П-18. Конфигурирование секции Microsoft-Windows-Shell-Setup\ FirstLogonCommands этапа настройки oobeSystem файла ответов

Для того чтобы с помощью параметра FirstLogonCommands запустить команду на этапе настройки oobeSystem, для этой команды нужно отконфигурировать три значения:

- CommandLine — указывает путь выполнения команды;
- Description — описывает запускаемую команду;
- Order — определяет порядок запуска команд.

Если на этапе настройки oobeSystem нужно запустить несколько команд, добавьте в файл ответов секции FirstLogonCommands и укажите отдельный номер Order для каждой команды. В качестве примера на рис. П-19 показаны три команды, синхронно выполняющихся на этапе настройки oobeSystem, вторая из которых устанавливает роль DHCP-сервера с опциями по умолчанию.

Для того чтобы установка ролей и компонентов выполнялась в автоматизированном режиме, помимо команд FirstLogonCommands в файле ответов тре-

буется также использовать параметры Microsoft-Windows-Shel]-Setup\Autologon и Microsoft-Windows-Shell-Setup\Autologon\Password.

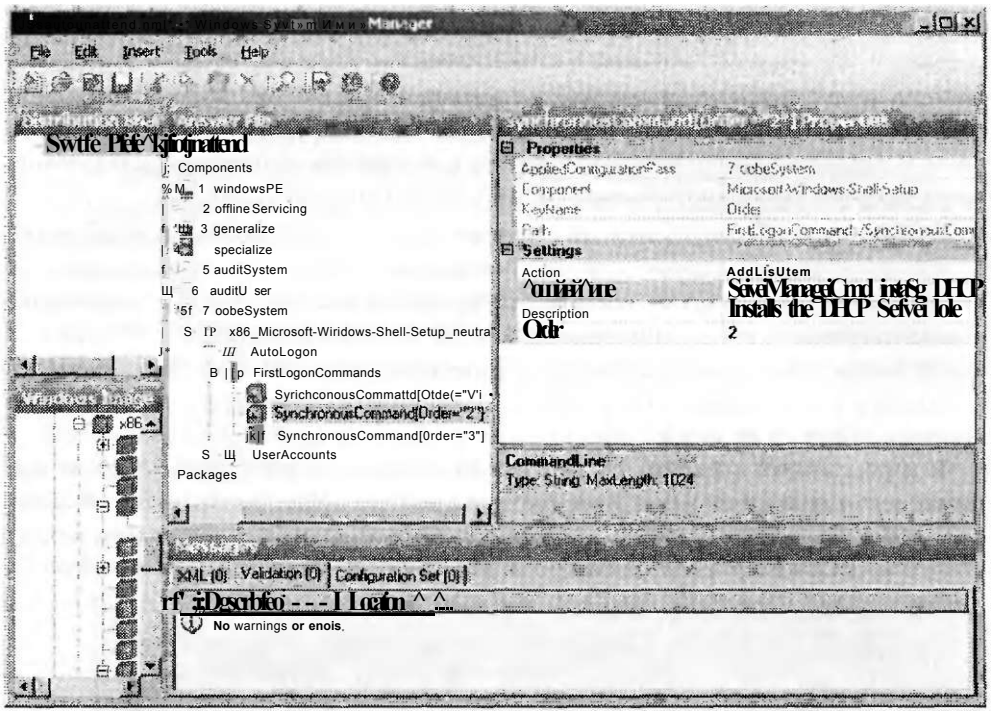


Рис. П-19. Запуск множества команд на этапе настройки oobeSystem установки сервера

ПРИМЕЧАНИЕ Параметр FirstLogonCommands и секция [GUIRunOnce]
Параметр FirstLogonCommands заменил секцию [GUIRunOnce], использовавшуюся в файлах ответов Unattend.txt предыдущих версий Windows.

Проверьте себя

1. **Почему в файле ответов нужно с помощью параметра FirstLogon-Commands конфигурировать параметры автоматического входа для автоматизации задач начальной настройки?**
2. **Как с помощью инструмента ServerManagerCmd.exe установить множество ролей и компонентов путем запуска одной команды?**

Ответы

1. **Если параметры автоматического входа не будут откопфикурированы, команды FisrtLogonCommands не будут запущены на этапе настройки oobeSystem.**
2. **Нужно задать команду** *servermanagercmd.exe -inputPath inpit.xrnl.*

Установка ролей и компонентов на компьютере с ядром сервера

Установка ролей и компонентов на компьютере с ядром сервера отличается от установки на машине с полной версией Windows Server 2008. Дело в том, что система ядра сервера не поддерживает мастеров добавления ролей и компонентов, а также инструмент ServerManager.exe. На компьютере с ядром сервера роли и компоненты можно устанавливать и удалять с помощью следующих инструментов командной строки ОС (Optional Component, ОС).

- **OCList.exe Используется для перечисления ролей сервера, служб ролей и компонентов, которые можно установить, а также для определения их состояния (установлены или нет). Эта утилита доступна только в установке ядра сервера и недоступна в полной установке Windows Server 2008.**
- **OCSetup.exe Используется для установки и удаления ролей сервера, служб ролей и компонентов. Эта утилита доступна в обоих типах установки Windows Server 2008.**

Если вы хотите на компьютере с ядром сервера начать установку роли или компонента, в командную строку введите команду *oclist.* Отобразится текущее состояние установки опциональных ролей и компонентов, а также имя пакета для установки каждой отдельной роли и каждого компонента (рис. П-20).

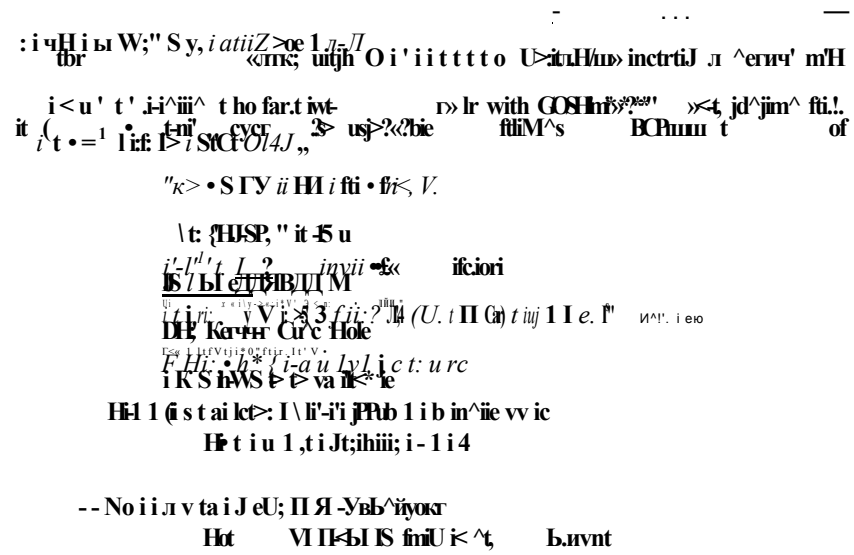


Рис. П-20. Результат запуска утилиты OCList.exe на компьютере с ядром сервера

Как показано на рисунке, именем пакета для роли DHCP-сервера является DHCPServerCore. Зная это, вы можете установить данную роль на сервере с помощью команды:

```
start /w ocsetup DHCPServerCore
```

Следует отметить два нюанса, связанных с использованием инструмента OCSetup.exe.

- **Синтаксис OCSetup.exe чувствителен к регистру, так что имя пакета нужно вводить точно в том виде, в каком оно отображается с помощью описанной ранее команды OCList.exe. В противном случае может возникнуть ошибка установки указанной роли или службы.**
- **Хотя фрагмент команды *start/w* не обязателен, ее все же рекомендуется использовать. Дело в том, что в зависимости от устанавливаемого компонента инструмент OCList.exe может неверно указать, что роль или компонент не устанавливается, поскольку выполняется установка компонента. Часть команды *start/w* исключает неверные отчеты. В частности, аргумент */w* (WAIT) используется вместе с командой *start* для запуска указанного приложения (то есть OCSetup.exe), в ожидании завершения приложения перед возвратом к командной строке.**

Инструмент OCSetup.exe обеспечивает упаковщик для интерфейса командной строки Диспетчера пакетов Windows (Package Manager, PkgMgr.exe). Этот инструмент Windows используется для установки и удаления пакетов, а также для включения и отключения компонентов. Диспетчер пакетов (PkgMgr.exe) вызывается инструментом OCSetup.exe. Во время стандартной установки Windows (вручную или в автоматизированном режиме) Диспетчер пакетов вызывается программой Windows Setup и прозрачным образом запускается в фоновом режиме.

Диспетчер пакетов также можно использовать для автоматизированной установки исправлений и других обновлений программного обеспечения, а также для включения и отключения компонентов Windows и работы с автономным образом Windows.

Инструмент OCSetup.exe может принимать следующие параметры командной строки.

- **,/log:file Определяет местоположение файла журнала.**
- **/norestart Указывает, что компьютер не должен перезагружаться, даже если это требуется после установки компонента.**
- **/passive Включает автоматизированный режим. Отображается лишь ход выполнения установки.**
- **/quiet Использует тихий режим (quiet mode). Взаимодействия с пользователем не отображаются.**
- **/unattendfile:0aiw Использует указанный файл, содержащий изменения или дополнения к параметрам конфигурации по умолчанию. (Подразумевается пассивный режим.)**
- **/uninstall Удаляет указанный компонент.**
- **/x:** *параметр* **Указывает дополнительные параметры конфигурации, которые будут применены при установке компонента.**

Для получения дополнительных сведений о синтаксисе OCSetup.exe в командную строку введите команду *ocsetup /help.*

ПРИМЕЧАНИЕ Использование диспетчера пакетов PkgMgr.exe вместо OCSetup.exe

Хотя для установки ролей и служб на компьютере с ядром сервера рекомендуется использовать инструмент OCSetup.exe, вы можете также применять для этого Диспетчер пакетов (Package Manager). Так, с помощью следующей команды на компьютере с ядром сервера Windows Server 2008 будут установлены все доступные компоненты IIS 7.

```
start /w pkgmgr /iu:IIS-WebServerRole;IlS-WebServer;
IIS-CommonHttpFeatures; HS-StaticContent;IIS-DefaultDocument;
IIS-DirectoryBrowsing;IIS-HttpErrors;IIS-HttpRedirect;
IIS-ApplicationDevelopment;IIS-ASP;IIS-CGI;IIS-ISAPIExtensions;
IIS-ISAPIFilter; IlS-ServerSidelncludes;IIS-HealthAndDiagnostics;
IIS-HttpLogging;IIS-LoggingLibraries;IIS-RequestMonitor;
IIS-HttpTracing;IIS-CustomLogging;IIS-ODBCLogging;IlS-Security;
IIS-BasicAuthentication;IIS-WindowsAuthentication;
IIS-DigestAuthentication;IIS-ClientCertificateMappingAuthentication;
IIS-IISCertificateMappingAuthentication;IIS-URLAuthorization;
IIS-RequestFiltering;IlS-IPSecurity;IlS-Performance;
IIS-HttpCompressionStatic;IIS-HttpCompressionDynamic;
IIS-WebServerHanagementTools;IIS-ManagementScriptingTools;
IIS-IIS6ManagementCompatibility;IIS-Metabase;IIS-WMICompatibility;
IIS-LegacyScripts;IIS-FTPPublishingService;IIS-FTPServer;
WAS-WindowsActivationService;WAS-ProcessModel
```

Автоматизация процесса установки ролей и компонентов

Процесс установки ролей и компонентов на компьютере с ядром сервера можно автоматизировать, комбинируя использование инструмента OCSetup.exe и параметров FisrtLogonCommands в файле ответов. По сути этот процесс ничем не отличается от описанного ранее использования инструмента ServerManagementCmd.exe с параметрами FirstLogonCommands.

Ответы

Глава 1. Закрепление материала

Занятие 1

1. **Правильный ответ: В.**
   - **А. Неправильный** Windows PE используется для загрузки с CD-диска и для обслуживания жесткого диска.
   - **Б. Неправильный** Утилита ImageX захватывает, изменяет и применяет образы WIM.
   - **В. Правильный** Утилита Sysprep подготавливает установку Windows к записи в образ, при этом удаляется вся уникальная системная информация из этой установки, в частности, сбрасывается ключ безопасности (Security ID SID), удаляются точки восстановления и журналы событий.
   - **Г. Неправильный** Windows System Image Manager (SIM) — это утилита, которая используется с целью создания файла ответов для программы Windows Setup.

Занятие 2

1. **Правильный ответ: В.**
   - **А. Неправильный** Хранилище образов находится в папке Path\RemoteInstall на вашем WDS-сервере и используется для хранения загрузочных и установочных образов, которые предназначены для развертывания операционных систем, а также для управления этими образами.
   - **Б. Неправильный** WDS включает в себя TFTP-сервер, способный отвечать PXE-совместимым компьютерам клиентов, которые в дальнейшем могут загрузить WDS-клиент, отобразить загрузочное меню, а после этого начать установку.
   - **В. Правильный** Хотя SIM используется при создании файлов ответов для неконтролируемых установок с применением WDS, эта программа не является составляющей WDS — она входит в пакет Windows AIK.
   - **Г. Неправильный** WDS включает в себя PXE-сервер, который может отвечать на BOOTP-запросы PXE-совместимых компьютеров клиентов и предоставлять этим компьютерам информацию о местонахождении WDS-клиента, который нужен для запуска процесса установки.

2. Правильные ответы: А и В.
   А. Правильный Windows DS не поддерживает диски FAT32.
   Б. Неправильный Начальные параметры PXE-сервера наименее подходят для данного сценария. Фактически параметры, которые вы выбрали, являются наиболее неверными параметрами.
   В. Правильный Только файл Boot.wim, который вы можете найти на дисках с системами Windows Server 2008 и Windows Vista со встроенным Service Pack 1, предоставляют вам преимущества WDS-версии Windows Server 2008. Файл Boot.wim системы Windows Vista RTM поддерживает только раннюю версию Windows DS.
   Г. Неправильный Вы путаете загрузочный образ с установочным.

Занятие 3

1. Правильный ответ: Г.
   А. Неправильный Virtual Server и Windows Server Hyper-V поддерживают балансировку загрузки сети.
   Б. Неправильный Virtual Server и Windows Server Hyper-V предоставляют пользователям возможность назначать процессор хоста виртуальной машине.
   В. Неправильный Все три решения виртуализации корпорации Microsoft поддерживают 64-разрядные хосты.
   Г. Правильный Только Hyper-V поддерживает 64-разрядные гостевые операционные системы.
2. Правильный ответ: Г.
   А. Неправильный Миграция физического компьютера в виртуальный не является особенностью Virtual PC.
   Б. Неправильный Миграция физического компьютера в виртуальный не является особенностью Virtual Server.
   В. Неправильный Миграция физического компьютера в виртуальный не является особенностью Hyper-V.
   Г. Правильный Утилита Virtual Server Migration Toolkit предоставляется бесплатно (ее можно загрузить с официального веб-сайта корпорации Microsoft) и используется для упрощения процесса миграции P2V (Physical-to-Virtual).

Занятие 4

1. Правильный ответ: В.
   А. Неправильный 25 компьютеров нужно будет активировать до того, как будут активированы клиенты Windows Vista. Главный офис удовлетворяет этим требованиям, при этом удовлетворяются и требования активации Windows Server 2008.
   Б. Неправильный Пять компьютеров должны запросить активацию до того, как можно будет активировать систему Windows Server 2008 с помощью KMS-хоста. Главный офис удовлетворяет этому требованию, при этом удовлетворяются и требования активации Windows Server 2008.

В. Правильный KMS-лицензирование доступно для двух типов клиентов. Чтобы активировать клиентов Windows Vista, KMS-хост должен получить запрос на активацию от 25 компьютеров. Для активации Windows Server 2008 тот же KMS-хост должен получить запрос на активацию от пяти компьютеров. Главный офис удовлетворяет этим требованиям.

Г. Неправильный Главный офис удовлетворяет требованиям KMS-лицензирования для обеих операционных систем.

2. **Правильный ответ: Б.**

А. Неправильный В отсутствие доступа в Интернет независимая МАК-активация потребует активировать каждый компьютер по телефону. Эта процедура занимает много времени.

Б. Правильный Активация МАК-ргоху — наиболее эффективный способ активации компьютеров, на которых установлена операционная система Windows Vista и которые не подключены к сети Интернет, при условии, что количество таких компьютеров составляет менее 25. При этом используется XML-файл с идентификационными номерами клиентов. После пересылки подтвержденных идентификационных кодов от корпорации Microsoft на компьютер, который подключен к сети Интернет, эти коды распределяются между компьютерами клиентов и тем самым активируют их.

В. Неправильный Вы не можете применить в этом сценарии KMS-лицензирование либо активацию, поскольку в тестовой сети не хватает компьютеров для использования KMS-хоста.

Г. Неправильный Вы не можете выполнить активацию с помощью retail-ключа, так как условия сценария предполагают, что для 15 компьютеров была получена одна volume-лицензия.

Глава 1. Лабораторная работа

Задание 1

1. System Center Configuration Manager 2007.
2. Вы должны, используя виртуализацию (Virtual Server или Hyper-V), объединить серверы, которые работают под управлением операционных систем Windows NT и Linux. Таким образом можно уменьшить стоимость содержания серверов и количество серверов, которые вам нужно будет приобрести для системы Windows Server 2008.

Задание 2

1. На площадке главного офиса необходимо применить KMS-лицензирование и активацию для всех компьютеров, кроме тех, которые подключены к тестовой сети. Для изолированных компьютеров необходимо применить активацию МАК-ргоху.
2. На площадке в городе Бирмингеме нужно использовать KMS-лицензирование и локально установленный KMS-хост.
3. На площадке в городе Сиракузы нужно использовать МАК-лицензирование.

Глава 2. Закрепление материала

Занятие 1

1. **Правильный ответ: Б.**
   - **А. Неправильный** Если в аппаратном решении поставщика не будет задействован аппаратный провайдер VDS, то ни один из дисков не будет обнаружен в оснастке Управление дисками (Disk Management). Даже при наличии аппаратного провайдера VDS, диски будут обнаружены только после того, как будет создана и подключена к серверу сеть LAN.
   - **Б. Правильный** VDS представляет собой API-интерфейс, позволяющий управлять дисковыми подсистемами и аппаратными средствами SAN с помощью средств администрирования операционной системы Windows. В случае встроенных средств управления хранилищем, таких как Диспетчер хранилища для сетей SAN (Storage Manager for SANs, SMfS), чтобы иметь возможность подключаться к дисковым корпусам, изготовленным независимыми производителями, аппаратное обеспечение должно также содержать программный интерфейс для VDS.
   - **В. Неправильный** Соединение iSCSI с устройством будет сразу установлено, если программное обеспечение поставщика можно использовать для подключения к дисковой подсистеме. Кроме того, если аппаратное решение поставщика не будет включать аппаратный провайдер VDS, то Инициатор iSCSI (iSCSI Initiator) в операционной системе Windows не сможет обнаружить устройство.
   - **Г. Неправильный** Соединение с устройством будет сразу установлено, если программное обеспечение поставщика можно использовать для подключения к дисковой подсистеме. Настройка iSNS-сервера не даст возможности физически обнаружить устройство. Необходимо, чтобы аппаратное решение поставщика содержало аппаратный провайдер VDS.
2. **Правильный ответ: Г.**
   - **А. Неправильный** Простой том будет использовать пространство только одного из трех дисков и не обеспечит высокой производительности чтения или записи данных.
   - **Б. Неправильный** Составной том способен использовать максимальное пространство на всех трех дисках, но не обеспечивает высокой производительности чтения или записи данных.
   - **В. Неправильный** Зеркальный том будет использовать пространство, объем которого эквивалентен объему только одного диска. Кроме того, зеркальный том не обеспечит высокой производительности чтения или записи данных.
   - **Г. Правильный** Чередующийся том будет использовать все свободное пространство на всех трех дисках. Кроме того, он обеспечит наилучшую среди томов всех типов производительность чтения или записи данных.
   - **Д. Неправильный** Том RAID-5 будет использовать пространство, объем которого эквивалентен объему двух из трех дисков. И хотя том RAID-5 обеспечивает превосходную производительность чтения данных, производительность записи данных будет относительно низкой.

Занятие 2

1. **Правильный ответ: Б.**
   - **А. Неправильный** Более мощный сервер мог бы за короткое время обеспечить производительность, требуемую для веб-сайта, но поскольку в ближайшие несколько лет ожидается возрастание трафика, это решение не даст хорошего результата на длительный период времени.
   - **Б. Правильный** NLB-кластер (веб-ферма) даст возможность обеспечить требуемую производительность для веб-сайта и на короткий, и на длительный периоды времени. Поскольку трафик к веб-сайту будет возрастать, вам придется добавлять дополнительные серверы.
   - **В. Неправильный** Отказоустойчивый кластер не позволит веб-сайту поддерживать возрастание рабочей нагрузки. Он только может разрешить одному серверу взять на себя работу другого сервера в случае, если тот откажет.
   - **Г. Неправильный** Циклического распределения может быть достаточно для выполнения нескольких небольших развертываний, но это не лучшее решение на длительный период времени. Ведь никто не хочет, чтобы веб-клиенты в течение продолжительного времени направлялись на вышедшие из строя или загруженные веб-серверы; необходимо обеспечить лучший контроль за распределением рабочей нагрузки, чем это возможно при циклическом распределении.
2. **Правильный ответ: Б.**
   - **А. Неправильный** Выбирать конфигурацию кворума Большинство узлов (Node Majority) не стоит потому, что данный параметр лучше всего подходит для отказоустойчивых кластеров с нечетным количеством узлов.
   - **Б. Правильный** Конфигурация кворума Большинство узлов и дисков (Node and Disk Majority) является наиболее подходящей для отказоустойчивых кластеров с нечетным количеством узлов и множеством параметров совместно используемого хранилища.
   - **В. Неправильный** Конфигурация кворума Большинство узлов и общих файловых ресурсов (Node and File Share Majority) является наиболее подходящей для отказоустойчивого кластера с нечетным количеством узлов, но не имеющего доступа к совместно используемому тому, который может быть использован вместо диска-свидетеля.
   - **Г. Неправильный** Конфигурацию Кворум без большинства: только диск (No Majority: Disk Only), как правило, не рекомендуется использовать. Она может применяться при тестировании сред или в особых конфигурациях, когда не подходит никакая другая конфигурация кворума.

Глава 2. Лабораторная работа

Задание 1

1. **Вам следует выбрать сеть SAN на базе технологии iSCSI, поскольку она обеспечивает превосходную производительность записи данных, в то время как вы можете привлекать к выполнению данной задачи квалифицированных специалистов, занимающихся вопросами сетевых технологий.**

2. Вам следует искать такие аппаратные решения поставщиков, в которых предусматривалось бы применение аппаратных провайдеров VDS.

Задание 2

1. Вам следует настроить NLB-кластер, который будет исполнять роль ведущего узла для IIS и веб-приложения. Это позволит максимально увеличить производительность, балансируя нагрузку запросов клиентов среди серверов. Кроме того, NLB-кластер дает возможность минимизировать время простоя, перенаправляя запросы с бездействующих серверов.
2. Вам следует выбрать NLB-кластер, который будет исполнять роль ведущего узла для сервера базы данных. Поскольку данные всегда должны быть внутренне совместимы, необходимо, чтобы база данных постоянно хранилась на одном устройстве. Отказоустойчивый кластер также будет минимизировать время простоя, обеспечивая переход на другой ресурс при сбое сервера базы данных.

Глава 3. Закрепление материала

Занятие 1

1. Правильные ответы: А и В.
   - А. Правильный Эта команда конфигурирует компьютер с установленным ядром сервера Windows Server 2008 для приема подключений к удаленному рабочему столу.
   - Б. Неправильный Эта команда блокирует подключения к удаленному рабочему столу компьютера с установленным ядром сервера Windows Server 2008.
   - В. Правильный Эта команда настраивает компьютер с установленным ядром сервера Windows Server 2008 для приема подключений к удаленному рабочему столу от клиентов Windows XP и Windows более ранних версий.
   - Г. Неправильный Эта команда блокирует подключения к удаленному рабочему столу компьютера с установленным ядром сервера Windows Server 2008 от клиентов Windows XP и Windows более ранних версий.
2. Правильный ответ: Г.
   - А. Неправильный Удаленный стол для администрирования (RDA) является нелицензированной версией служб терминалов, которая разрешает провести лишь два одновременных сеанса рабочего стола. Однако двух сеансов недостаточно для поддержки 75 консультантов. Кроме того, в случае использования RDA не нужно приобретать никаких лицензий.
   - Б. Неправильный . Удаленный стол для администрирования (RDA) является нелицензированной версией служб терминалов, которая разрешает провести лишь два одновременных сеанса рабочего стола. Двух сеансов недостаточно для поддержки 75 консультантов.
   - В. Неправильный Службы терминалов нужно установить на сервере приложений, чтобы к нему одновременно могли подключаться более двух поль-

зователей. Однако целесообразнее использовать лицензии CAL на пользователя, поскольку количество устройств превышает количество пользователей.

Г. Правильный На сервер приложений нужно установить службы терминалов, чтобы к нему одновременно могли подключаться более двух пользователей. В то время как вам, возможно, потребуется приобрести лишь 75 лицензий CAL на пользователя, лицензий TS CAL на устройство понадобится приобрести намного больше, поскольку консультанты будут подключаться с большого количества компьютеров. Поэтому в данном случае лучше выбрать лицензирование CAL на пользователя.

Занятие 2

1. Правильный ответ: Б.

   А. Неправильный Посредник сеансов служб терминалов отслеживает пользовательские сеансы в ферме и отвечает за переподключение пользователей к отключенным сеансам RDP. Чтобы посредник сеансов служб терминалов отслеживал сеансы на каждом сервере фермы, все серверы фермы нужно добавить в локальную группу Компьютеры каталога сеансов (Session Directory Computers) на сервере с установленным посредником сеансов. В данном сценарии сервером посредника сеансов служб терминалов является машина TSLB1.

   Б. Правильный Чтобы пользователи могли переподключаться к отключенным сеансам RDP в ферме серверов служб терминалов, каждый член фермы следует добавить в локальную группу Компьютеры каталога сеансов (Session Directory Computers) на сервере с посредником сеансов служб терминалов. В данном сценарии сервером посредника сеансов служб терминалов является машина TSLB1.

   В. Неправильный При использовании этой опции лишь некоторые клиентские запросы TSFARM1 будут направляться на TSLB6. Данная опция не разрешает посреднику сеансов служб терминалов переподключаться к отключенным сеансам.

   Г. Неправильный При использовании этой опции пользователи смогут подключаться к TSLB6, лишь указав непосредственно имя сервера. Данная опция не позволяет пользователям, подключившимся с помощью имени фермы TSFARM1, переподключаться к отключенным сеансам RDP.

2. Правильный ответ: Г.

   А. Неправильный При использовании этой опции клиентам служб терминалов будет запрещено выводить печать на свои локальные принтеры. С помощью данной опции нельзя отконфигурировать резервный драйвер принтера для клиентов служб терминалов.

   Б. Неправильный При выборе этой опции принтер по умолчанию в сеансе служб терминалов будет заменен локальным принтером TS1. С помощью данной опции нельзя отконфигурировать резервный драйвер принтера для клиентов служб терминалов.

В. Неправильный Этот параметр политики обеспечивает согласованную печать для клиентов служб терминалов, однако с его помощью нельзя отконфигурировать резервный драйвер принтера для клиентов служб терминалов.

Г. Правильный Чтобы отконфигурировать резервный драйвер принтера, данный параметр политики следует настроить в групповой политике.

Глава 3. Лабораторная работа

Задание 1

1. **Да, нужно установить службы терминалов, поскольку вам потребуется поддерживать множество одновременных подключений. Следует использовать лицензирование CAL на пользователя, поскольку пользователей, подключающихся к TS1, меньше, чем устройств.**
2. **Нет, вам не нужно устанавливать службы терминалов на TS2, поскольку нет необходимости поддерживать больше двух одновременных сеансов рабочего стола. Вместо этого вы можете просто включить на сервере удаленный рабочий стол, для которого не нужно приобретать клиентские лицензии доступа.**

Задание 2

1. **На вкладке Общие (General) диалогового окна RDP-Tcp Свойства (RDP-Tcp Properties) сервера App3 сбросьте флажок разрешения подключений только от компьютеров с удаленным столом, где включена проверка подлинности на уровне сети.**
2. **На вкладке Сеансы (Sessions) диалогового окна RDP-Tcp Свойства (RDP-Tcp Properties) сервера Appl задайте для опции Завершение отключенного сеанса (End A Disconnected Session) параметр Никогда (Never).**

Глава 4. Закрепление материала

Занятие 1

1. **Правильный ответ: Б.**

   А. Неправильный Обязательные профили несовместимы с требованием обеспечить для пользователей возможность сохранять свои данных.

   Б. Правильный Реализовав дисковые квоты, вы сможете гарантировать, что пользовательские профили не захватят все доступное дисковое пространство.

   В. Неправильный Перемещаемые пользовательские профили сами по себе не решают проблему. Вам потребуется хранить профили в отдельном ресурсе, где достаточно места.

   Г. Неправильный Профили для пользователей служб терминалов хранятся на удаленном сервере терминалов, а не на локальном компьютере. Назначение дисковых квот для локальных дисков каждого пользователя не решит проблему.

2. **Правильный ответ: А.**
   - **А. Правильный** Для удаления пользовательского сеанса на сервере терминалов используйте команду *Rwinsta* или *Reset.* Удаление отключенных бездействующих сеансов позволит освободить ресурсы сервера для активных сеансов.
   - **Б. Неправильный** Команда *Tdiscon* отключает текущие пользовательские сеансы. Вам же нужно удалить отключенные сеансы, а не отключать активные.
   - **В. Неправильный** Команда *Tskill* завершает на сервере терминалов лишь отдельный процесс. Она не завершает полностью пользовательские сеансы.
   - **Г. Неправильный** Команда *Tscon* подключается к отключенному сеансу. Она не завершает пользовательские сеансы.

Занятие 2

1. **Правильный ответ: В.**
   - **А. Неправильный** TCP-порт 25 используется для SMTP-трафика. Этому порту не требуется обмениваться данными со шлюзом служб терминалов.
   - **Б. Неправильный** TCP-порт 3389 используется для прямых подключений RDP без использования шлюза служб терминалов, а для клиентов требуется обеспечить коммуникации через шлюз.
   - **В. Правильный** TCP-порт 443 используется для подключений SSL. Шлюз служб терминалов обменивается данными с клиентами через SSL.
   - **Г. Неправильный** TCP-порт 80 используется для HTTP-трафика. Этот порт нужно оставить открытым, чтобы клиенты могли связываться с веб-сервером, размещенным за пределами брандмауэра организации.
2. **Правильный ответ: Г.**
   - **А. Неправильный** Если включить мост HTTPS-HTTP, то ISA-сервер не будет использоваться как конечная точка SSL для подключений шлюза служб терминалов. Коммуникации со шлюзом служб терминалов будут осуществляться в незашифрованном виде через HTTP.
   - **Б. Неправильный** На сервере ISA необходимо открыть TCP-порт 443, чтобы к нему могли подключаться внешние клиенты. Однако открытие этого порта не гарантирует, что сервер ISA будет осуществлять коммуникации со шлюзом служб терминалов.
   - **В. Неправильный** SSL-сертификат ISA-сервера нужно экспортировать лишь на ISA-сервер.
   - **Г. Правильный** Если развернуть ISA-сервер между внешними клиентами и внутренним шлюзом служб терминалов, ISA-сервер будет выполнять роль клиента шлюза служб терминалов. По этой причине сертификат шлюза служб терминалов, используемый для SSL, должен быть установлен на компьютере с установленным ISA-сервером.

Занятие 3

1. **Правильный ответ: Б.**
   - **А. Неправильный** Эта команда используется для включения и отключения учетных данных в клиентских сеансах на сервере терминалов. Она не

гарантирует, что установленное приложение будет поддерживать множество пользователей.

Б. Правильный Перед установкой приложения используйте команду *chguser/install,* **чтобы создать для приложения в системном каталоге файлы .ini. Таким образом, пользователи, запускающие приложение, смогут сохранять для них личные параметры. После установки используйте команду** *chguser /execute.*

В. Неправильный Эта команда отображает список всех серверов терминалов в сети. Она не используется для обеспечения поддержки множества пользователей установленным приложением.

Г. Неправильный Эта команда запускает клиента служб терминалов Подключение к удаленному рабочему столу (Remote Desktop Connection) (Mstsc.exe). Она не предназначена для обеспечения установленным приложениям поддержки множества пользователей.

2. Правильные ответы А и Б.

А. Правильный Новый сайт Веб-доступ к службам терминалов (TS Web Access) назовет программу RemoteApp и укажет ее новое местоположение.

Б. Правильный После миграции программы RemoteApp старый RDP-файл использовать нельзя. Вам потребуется создать этот файл заново и распространить его среди пользователей.

В. Неправильный В RDP-файле можно модифицировать некоторые параметры, однако вы не сможете изменить размещение программы RemoteApp, на которое указывает файл. В случае перемещения приложения все связанные RDP-файлы потребуется создавать заново.

Г. Неправильный В параметрах сервера терминалов можно изменить имя сервера, однако это делается в тех случаях, когда локальный сервер принадлежит ферме серверов. Изменение имени сервера не обеспечит пользователям возможность подключаться к перемещенному приложению.

Глава 4. Лабораторная работа

Задание 1

1. Для поиска LD-сеанса можно использовать команду *Query.* **При необходимости завершить или удалить сеанс можно применить команду** *Rwinsta* **или** *Reset.*

2. С помощью компонента Удаленное управление (Remote Control) можно перехватить управление пользовательским сеансом и показать пользователю, как работать с приложением.

Задание 2

1. Для публикации программы RemoteApp на рабочих столах пользователей следует применить групповую политику. При этом можно использовать файл RDP или MSI.

2. Чтобы добавить Appl в список программ RemoteApp, а затем создать для приложения пакет установщика Windows, нужно использовать Диспетчер удаленных приложений RemoteApp служб терминалов (TS RemoteApp Manager). Откonфигурируйте MSI-файл для установки ярлыка программы RemoteApp в меню Пуск (Start) и запуска программы при открытии каждого сопоставленного с ней файла. Разверните MSI-файл с помощью групповой политики.
3. В сети по периметру разверните сервер шлюза служб терминалов. С помощью Диспетчера удаленных приложений RemoteApp служб терминалов (TS RemoteApp Manager) создайте для приложения Appl файл RDP, указывающий сервер шлюза служб терминалов. Распространите этот RDP-файл среди удаленных пользователей.

Глава 5. Закрепление материала

Занятие 1

1. Правильный ответ: Б.
   А. Неправильный Служба ролей Ошибки HTTP (HTTP Errors) используется для отправки пользователям настраиваемых страниц ошибок. Поскольку сервер не реагирует, вряд ли данная служба сможет помочь решить проблему.
   Б. Правильный Скорее всего, причина проблемы кроется в том, что остановлена Служба веб-публикаций (World Wide Web Publishing Service). Состояние этой службы можно проверить (и просмотреть все связанные события) с помощью Диспетчера сервера (Server Manager).
   В. Неправильный Поскольку неполадки доступа к сайту возникли у множества пользователей, вероятнее всего, что проблема возникла на стороне сервера.
   Г. Неправильный Служба ролей Ведение журнала HTTP (HTTP Logging) позволяет собирать информацию о запросах к веб-сайту. Однако по причине того, что веб-сервер не реагирует на запросы, добавление этой службы не поможет решить проблему.
   Д. Неправильный Служба администрирования IIS (IIS Admin Service) требуется для внесения изменений в конфигурацию веб-сервера. Даже если эта служба остановлена, веб-сервер все равно должен реагировать на пользовательские запросы.

Занятие 2

1. Правильные ответы: А и Г.
   А. Правильный Поскольку доступ к обоим приложения должен быть обеспечен на стандартном HTTP-порте, эти приложения должны располагаться внутри одного веб-сайта.
   Б. Неправильный В IIS множество веб-сайтов не могут совместно использовать одни параметры привязок. Поэтому вы не имеете возможности запустить множество веб-сайтов, привязанных к HTTP-порту 80.

В. Неправильный Назначение двум веб-приложениям одного пула приложений не поможет решить проблемы, связанной с влиянием одного веб-приложения на другое.

Г. Правильный При использовании отдельных пулов приложений каждое веб-приложение будет запускаться изолированно. Такая методика поможет устранить потенциальные проблемы производительности и стабильности.

2. **Правильный ответ: Г.**

А. Неправильный Процесс воссоздания веб-сайтов может отнимать много времени. К тому же в нем сложно гарантировать корректное восстановление всех параметров.

Б. Неправильный Добавление параметров в файл ApplicationHost.config вручную отнимает много времени и не исключает появления ошибок.

В. Неправильный Поскольку резервное копирование конфигурации IIS не выполнялось вручную, утилита AppCmd не в состоянии восстановить резервную копию.

Г. Правильный Поскольку каждый веб-сайт имеет многочисленные дополнительные параметры, а в конфигурацию сервера никакие дополнительные изменения не вносились, самый быстрый способ восстановления сайтов состоит в восстановлении конфигурации IIS из копии рабочего файла ApplicationHostxonfig.

Глава 5. Лабораторная работа

Задание 1

1. Элемент управления IIS Общая конфигурация (Shared Configuration) позволяет множеству веб-серверов использовать одни и те же файлы конфигурации. Для этого экспортируйте данные конфигурации с одного сервера и настройте все веб-серверы для использования одного файла параметров.
2. В процесс архивации следует включить папки содержимого всех веб-сайтов (в том числе их файлы Web.config). Резервная копия также должна содержать папку %SystemDrive%\Inetpub\History, поскольку в этой папке хранятся предыдущие версии файлов конфигурации.
3. Для создания и восстановления резервных копий данных конфигурации LIS вручную можно использовать утилиту AppCmd.exe. Резервные копии рекомендуется создавать вручную перед внесением изменений в конфигурацию сервера. При желании вы можете восстанавливать предыдущие версии файла ApplicationHost.config поверх рабочей версии, чтобы вернуться к предыдущей конфигурации сервера.

Задание 2

1. Если каждому веб-приложению назначить отдельный пул приложений, вероятность влияния ошибок одних веб-приложений на работу других веб-приложений на одном сервере будет сведена к минимуму.

2. Для каждого веб-сайта можно модифицировать привязки, чтобы включить отдельное имя узла. На основе этой информации пользователи будут автоматически перенаправляться на соответствующий сайт.
3. Если добавить службу ролей Совместимость управления IIS 6 (IIS 6 Management Compatibility), то можно будет обеспечить доступ к метабазе IIS 6.0 и к другим компонентам. Если приложению ASP.NET требуется доступ к классическому режиму конвейера, нужно назначить или изменить параметры его пула приложений.

Глава 6. Закрепление материала

Занятие 1

1. Правильный ответ: Б.
   - А. Неправильный Если добавить обработчик для всего веб-сайта, он станет доступен для всех веб-приложений, что потенциально снижает уровень безопасности.
   - Б. Правильный Для обработки запроса управляемый обработчик позволяет вызывать библиотеку .NET. Чтобы снизить фронт атак IIS, доступ к этому обработчику следует предоставить только тому веб-приложению, которому он требуется для работы.
   - В. Неправильный Сопоставления модуля не обеспечивают доступ к библиотекам .NET.
   - Г. Неправильный Сопоставления модуля не обеспечивают доступ к библиотекам .NET.
2. Правильный ответ: В.
   - А. Неправильный Диспетчер IIS (LIS Manager) позволяет конфигурировать пользовательские разрешения для веб-сайтов даже в случае остановки Службы управления (Management Service).
   - Б. Неправильный Разрешения файловой системы не влияют на возможность добавления в веб-сайт пользователей диспетчера IIS.
   - В. Правильный Для добавления в веб-сайт пользователей диспетчера IIS нужно отконфигурировать Службу управления (Management Service), чтобы она принимала реквизиты диспетчера IIS.
   - Г. Неправильный Параметры проверки подлинности применяются лишь по отношению к пользователям, получающим доступ к веб-содержимому с помощью веб-браузера или других приложений. Эти параметры не влияют на параметры подключения пользователей диспетчера IIS.

Занятие 2

1. Правильные ответы: А и В.
   - А. Правильный Проверка подлинности Windows позволяет пользователям с учетными записями домена Windows или локальными учетными записями проходить проверку подлинности на сервере.

Б. Неправильный Обычная проверка подлинности обеспечивает более низкий уровень безопасности, чем проверка подлинности Windows, поскольку все пользователи располагают учетными записями Windows.

В. Правильный Для того чтобы пользователям приходилось вводить учетные данные при получении доступа к сайту, нужно отключить анонимную проверку подлинности.

Г. Неправильный Если включить анонимную проверку подлинности, пользователи смогут получать доступ к сайту без ввода учетных данных.

2. Правильный ответ: В.

А. Неправильный Сайт принимает подключения по порту 443, поскольку пользователи получают предупреждение, а не ошибку.

Б. Неправильный Согласно требованиям, пользователи должны иметь возможность подключаться с помощью обоих протоколов, HTTP и HTTPS. Поэтому для получения доступа к сайту не следует требовать SSL.

В. Правильный Пользователи получают предупреждение по причине того, что сертификат сервера был издан не доверенным сторонним центром сертификации. Возможно, на сервере ранее был установлен самозаверяющийся сертификат. Для решения этой проблемы можно сгенерировать запрос сертификата в Интернете, получить сертификат и зарегистрировать его на сервере.

Г. Неправильный Поскольку сертификат сервера установлен должным образом, его экспорт и повторный импорт не поможет решить проблему.

Д Неправильный Поскольку при попытке подключиться к веб-сайту пользователи получают лишь предупреждение, брандмауэр не запрещает подключение.

Глава 6. Лабораторная работа

Задание 1

1. При наличии необходимых разрешений в Диспетчере IIS (IIS Manager) можно создать множество подключений (по одному для каждого сервера). При желании для каждого подключения можно назначить различные учетные данные.
2. Самый безопасный способ состоит во включении реквизитов диспетчера IIS для Службы управления (Management Service) и в создании новой учетной записи диспетчера IIS для администратора.
3. Параметры делегирования компонентов определяют, какие параметры диспетчера IIS могут просматривать или модифицировать администраторы. Чтобы запретить администраторам вносить изменения, установите для компонентов Документ по умолчанию (Default Document) и Просмотр каталога (Directory Browsing) параметр Только чтение (Read Only).

Задание 2

1. Поскольку веб-приложению требуется возможность подключаться к удаленному серверу баз данных, для указания уровня доверия .NET нужно выбрать

параметр High (файл Webhightrustxonfig). Этот параметр следует назначить на уровне веб-приложения.

2. Вначале используйте системные разрешения для разрешения доступа к содержимому лишь группе утвержденных пользователей. Затем, чтобы указать пользователей, которые могут получать доступ к содержимому, можно применить правила авторизации.
3. Вначале нужно получить и установить на веб-сервере Сертификат безопасности Интернета (Internet Security Certificate). Затем с помощью параметров привязок узлов можно включить подключения SSL. И наконец, чтобы включить шифрование, используйте компонент Параметры SSL (SSL Settings) для веб-приложения.

Глава 7. Закрепление материала

Занятие 1

1. Правильный ответ: В.
   - А. Неправильный Учетная запись IU*БК ИмяМашины* используется для подтверждения разрешений анонимных подключений к FTP-серверу. Поскольку пользователь применяет учетные записи и разрешения Windows, эти параметры не влияют на доступ к папке Drawings.
   - Б. Неправильный Ограничения по TCP/IP-адресам (TCP/IP Address Restrictions) используются для настройки доступа к FTP-серверу на основе IP-адресов или DNS-имен. Эти параметры не запрещают доступ к конкретным папкам.
   - В. Правильный Наиболее вероятная причина проблемы заключается в том, что все подключения рассматриваются как анонимные. Чтобы разрешить FTP-серверу проверять разрешения в соответствии с учетной записью пользователя Windows, отключите данную опцию.
   - Г. Неправильный Пользователи, добавленные в группу локальных администраторов, получат ненужные им разрешения на сервере.
2. Правильные ответы: Б и Г.
   - А. Неправильный Если разрешить подключения SSL, пользователям не потребуется включать шифрование. Поэтому эта опция не соответствует требованию шифрования учетных данных и команд.
   - Б. Правильный При отключении 128-разрядного шифрования FTP-сайт будет использовать 40-разрядное шифрование. Таким образом, производительность FTP-сервера повысится, а данные будут по-прежнему шифроваться.
   - В. Неправильный При использовании политики Require SSL Connections (Требовать SSL-подключения) шифруются все коммуникации между FTP-клиентом и FTP-сайтом.
   - Г. Правильный Собственная политика SSL (Custom SSL Policy) позволяет администраторам независимо назначать параметры управляющего канала (Control Channel) и канала данных (Data Channel).

Занятие 2

1. **Правильные ответы: А и В.**
   - **А. Правильный** В случае применения обычной проверки подлинности всем пользователям и приложениям придется предоставлять учетные данные для использования виртуального сервера SMTP.
   - **Б. Неправильный** При использовании промежуточного узла виртуальный сервер SMTP будет выполнять маршрутизацию всех новых сообщений электронной почты через указанный сервер. Промежуточный узел не обеспечивает запрет неавторизованного доступа к серверу.
   - **В. Правильный** Чтобы указать компьютеры или IP-адреса, которые могут получать доступ к виртуальному серверу SMTP, можно использовать правила управления подключениями.
   - **Г. Неправильный** Вкладка Безопасность (Security) используется для определения операторов сервера SMTP. В ней нельзя непосредственно запретить неавторизованным пользователям отправлять сообщения.
2. **Правильный ответ: Б.**
   - **А. Неправильный** Компонент Текущие сеансы (Current Sessions) отображает лишь пользователей и приложения, которые подключены к серверу в конкретное время. Он не обеспечивает надежный метод мониторинга производительности.
   - **Б. Правильный** Счетчики производительности SMTP-сервера могут предоставлять сведения о количестве отправленных и полученных сообщений. Вы также можете производить корреляцию этих данных статистики с помощью другой информации, например об использовании процессора, памяти и сети.
   - **В. Неправильный** Журналы событий Windows не содержат данных о производительности службы SMTP-сервер (SMTP Server).
   - **Г. Неправильный** Журналы событий Windows не содержат данных о производительности службы SMTP-сервер (SMTP Server).
   - **Д. Неправильный** В папке Badmail содержатся недоставленные сообщения, однако проблемы производительности не обязательно связаны с такими сообщениями.

Глава 7. Лабораторная работа

Задание 1

1. **Для поддержки требований безопасности и веб-интеграции загрузите и установите FTP 7.**
2. **Получите сертификат для FTP-сервера, а затем с помощью диспетчера IIS включите опцию FTP Over SSL (FTPS).**
3. **Чтобы добавить новую привязку FTP-узла для существующего веб-сайта, используйте Диспетчер IIS (IIS Manager). При этом для сайта будет автоматически отконфигурирован корневой каталог.**

Задание 2

1. С помощью параметров, представленных на вкладке Общие (General) виртуального сервера SMTP, можно указать IP-адреса и номера портов, на запросы которых будет реагировать сервер.
2. На вкладке Доступ (Access) диалогового окна свойств виртуального сервера SMTP нужно включить обычную проверку подлинности.
3. С помощью опции Ограничить размер сообщений (Limit Message Size) на вкладке Сообщения (Messages) можно указать максимальный размер отдельного сообщения SMTP.

Глава 8. Закрепление материала

Занятие 1

1. Правильные ответы: Б и В.
   - А. Неправильный Пользователи не смогут перематывать потоковое мультимедиа из широковещательного пункта публикации.
   - Б. Правильный Пользователи могут получить доступ к пункту публикации по запросу, выбрать видео для просмотра и управлять воспроизведением.
   - В. Правильный Модуль Проверка подлинности IP-адреса WMS (WMS IP Address Authorization) может разрешить подключение к серверу только компьютерам, размещенным в указанной сети LAN.
   - Г. Неправильный Модуль Проверка подлинности согласования WMS (WMS Negotiate Authentication) предназначен для проверки подлинности пользователей на основе учетных записей Windows и не запрещает клиентам за пределами сети LAN получать доступ к содержимому.
   - Д. Неправильный Модуль Проверка подлинности NTFS ACL WMS (WMS NTFS ACL Authentication) проверяет учетные записи пользователей Windows на право доступа к содержимому, однако он не ограничивает сетевые размещения, с которых можно получать доступ к потоковому мультимедиа.
2. Правильный ответ: Б.
   - А. Неправильный Мастер одноадресных объявлений (Unicast Announcement Wizard) не запрещает пользователям получать доступ к конкретному содержимому пункта публикации.
   - Б. Правильный С помощью разрешений NTFS можно определить содержимое, которое будет доступным при использовании данного пункта публикации. В модуле Проверка подлинности NTFS ACL WMS (WMS NTFS ACL Authentication) можно указать пользовательскую учетную запись, которую следует применять.
   - В. Неправильный При копировании обучающего видео уменьшится объем доступного дискового пространства, а требования могут быть и не выполнены.
   - Г. Неправильный При отключении проверки подлинности анонимного пользователя WMS (WMS Anonymous User Authentication) пользователям

для получения доступа к содержимому потребуется предоставлять учетные данные для проверки подлинности.

Д. Неправильный Доступ к списку воспроизведения сопровождения (Wrapper Playlist) не обеспечит пользователям возможность выбора видео для просмотра.

3. Правильный ответ: Б.

А. Неправильный Копирование обучающего видео усложнит процесс обновления и инвентаризации содержимого, а также снизит объем доступного дискового пространства на сервере.

Б. Правильный При кэшировании серверов с целью обеспечения потоков мультимедиа будут автоматически извлекаться и сохраняться копии содержимого видео с исходного сервера.

В. Неправильный Прокси-серверы используются для перенаправления клиентских запросов на другие серверы. При их использовании может повыситься производительность, но не обеспечиваются возможности расширяемости, как в случае с серверами кэширования.

Г. Неправильный Ограничение подключений исходящего распределения не обеспечивает расширяемость для поддержки клиентских подключений.

Глава 8. Лабораторная работа

Задание 1

1. Нужно создать отдельный пункт публикации, обеспечивающий доступ к видеофайлам по запросу. В таком случае пользователи смогут выбирать видео для просмотра и управлять воспроизведением его содержимого.
2. Поскольку пользователи применяют учетные записи Active Directory, следует включить модуль Проверка подлинности NTFS ACL WMS (WMS NTFS ACL Authentication). Чтобы упростить администрирование, студентов можно разбить на группы с учетом изучаемого ими материала. Затем с помощью разрешений файловой системы можно указать файлы, к которым пользователи будут получать доступ.
3. Для автоматического воспроизведения видео перед запуском конкретного клипа можно использовать рекламу сопровождений. Это самый простой метод, поскольку не требует вручную создавать списки воспроизведения.

Задание 2

1. Для событий в прямом эфире лучше всего использовать широковещательный пункт публикации, поскольку он может получать информацию непосредственно из прямого потока кодировщика служб Windows Media.
2. В сетях с возможностями поддержки многоадресная ретрансляция может значительно снизить требования относительно пропускной способности для исходного сервера. Поддержку пользователей, которые не могут получать доступ к многоадресному потоку, можно обеспечить с помощью одноадресных потоков.
3. Добавление серверов кэш/прокси Windows Media способно значительно повысить производительность, причем содержимое останется на исходном сервере.

Глава 9. Закрепление материала

Занятие 1

1. **Правильные ответы: А и Д.**
   - **А. Правильный** В отличие от автономной (из одного сервера) конфигурации WSS в конфигурации фермы серверов не требуется устанавливать службу ролей Внутренняя база данных Windows (Windows Internal Database). Все содержимое и данные конфигурации будут храниться в назначенной для этой цели базе данных SQL Server.
   - **Б. Неправильный** Служба ролей Служба активации Windows (Windows Process Activation Service) необходима для управления веб-сайтами SharePoint.
   - **В. Неправильный** Для работы WSS требуется Microsoft .NET Framework 3.0.
   - **Г. Неправильный** Роль Веб-сервер (IIS) требуется для управления пользовательскими и административными веб-сайтами SharePoint.
   - **Д. Правильный** Роль Файловый сервер (File Server) для работы сервера WSS не нужна.
2. **Правильный ответ: В.**
   - **А. Неправильный** Для обеспечения доступа к сайту SharePoint по умолчанию не нужно создавать новый сайт.
   - **Б. Неправильный** Для обеспечения доступа к сайту SharePoint, созданному по умолчанию, новое семейство узлов создавать не нужно.
   - **В. Правильный** Создаваемому по умолчанию сайту SharePoint назначается проверка подлинности Windows. Для подключения к сайту пользователям нужен доступ к учетным данным локального домена. Внешние пользователи, не располагающие учетными записями домена, не смогут получать доступ к сайту, если им не назначить режим проверки подлинности Формы (Forms).
   - **Г. Неправильный** Параметры пользовательских разрешений применяются только к операциям, выполняемым после подключения пользователя к сайту SharePoint. Они не запрещают пользователям подключаться к самому сайту.
   - **Д. Неправильный** Шаблоны квот лишь ограничивают максимальный объем дискового пространства для семейства узлов и не запрещают пользователям подключаться к сайту.

Глава 9. Лабораторная работа

Задание 1

1. **Поскольку сервер баз данных будет использоваться для хранения содержимого, серверы следует развернуть с применением конфигурации фермы серверов. Позже параметры доступа к базам данных можно будет настроить с помощью Мастера настройки продуктов и технологий SharePoint (SharePoint Products And Technologies Configuration Wizard).**

2. Утилиту командной строки Stsadm.exe можно использовать для выполнения таких задач, как создание новых сайтов, без запуска Центра администрирования SharePoint (Share Point Central Administration). Команды можно поместить в файл сценария.

Задание 2

1. Поскольку все пользователи сайта являются члеиами одного домена Active Directory, проверка подлинности Windows позволит им подключаться к WSS, не предоставляя дополнительных учетных данных.
2. Для конкретных семейств узлов можно создать и назначить шаблоны квот, чтобы ограничить объем дискового пространства, используемого каждым сайтом. Если конкретные пользователи устанавливают свои ограничения, можно также отконфигурировать предупреждения электронной почты.
3. Управление средствами самостоятельного создания сайтов (Self-Service Site Management) дает пользователям возможность создавать собственные сайты SharePoint. Эту опцию можно включить на вкладке Управление приложениями (Application Management) веб-сайта Центр администрирования SharePoint (Share Point Central Administration).

Словарь терминов

AppCmd.exe Утилита командной строки, используемая для управления параметрами конфигурации IIS 7.0 и выполнения таких задач, как резервное копирование и восстановление данных конфигурации.

ApplicationHost.config Хранит исходные данные конфигурации IIS на уровне сервера. Этот XML-файл можно модифицировать вручную.

ASP.NET Технология разработок веб-приложений на основе структуры Microsoft .NET Framework. Приложения ASP.NET поддерживаются в IIS.

DRM Технология Digital Right Management (Технические средства защиты авторских прав) позволяет разработчикам содержимого запрещать неавторизованное использование своей интеллектуальной собственности.

FTP (File Transfer Protocol) Стандартный протокол, используемый для передачи файлов.

FTP-клиент Программное обеспечение, позволяющее пользователям подключаться к FTP-серверу для выгрузки и загрузки файлов. В качестве примеров можно привести утилиту командной строки FTP в Windows и функции FTP в Internet Explorer.

FTP-сервер Компьютер, отконфигурированный для обеспечения возможностей доступа к файлам, их выгрузки и загрузки.

FTPS (FTP Over SSL) Безопасная реализация протокола FTP, используя которую администраторы могут требовать или разрешать шифрование данных и контролировать управляющие каналы.

HTTP (Hypertext Transfer Protocol) Основной протокол, используемый для коммуникаций между веб-браузерами и веб-серверами. По умолчанию протокол HTTP использует TCP-порт 80.

HTTPS (Hypertext Transfer Protocol Secure) Безопасная версия протокола HTTP, которая позволяет использовать Secure Sockets Layer (SSL) и сертификаты. По умолчанию протокол HTTPS функционирует на основе TCP-порта 443.

HTTP-Over-SSL Распространенный метод шифрования веб-трафика.

Internet Information Services (IIS) Платформа веб-сервера, включенная в Windows Server 2008. В IIS обеспечена поддержка HTTP. FTP. SMTP и других

коммуникационных протоколов. Она также поддерживает множество языков и платформ веб-разработок.

Multiple Access Key (MAK) Ключ лицензии Volume, который может быть активирован несколько раз.

RTSP (Real-Time Streaming Protocol) Протокол потокового мультимедиа, используемый службами Windows Media с совместимыми проигрывателями (например, проигрыватель Windows Media 9). Протокол TRSP может функционировать поверх протоколов UDP (RTSPU) и TCP (RTSPT).

Secure Sockets Layer (SSL) Протокол безопасности, обеспечивающий возможности шифрования и проверки подлинности для веб-серверов и веб-браузеров. Протокол SSL является предшественником протокола TLS (Transport Layer Security).

SMTP (Simple Mail Transfer Protocol) Стандарт, используемый в Интернете для отправки текстовых сообщений с помощью протокола TCP/IP.

Stsadm.exe Утилита командной строки, предназначенная для настройки Windows SharePoint Services и управления таковыми.

TLS (Transport Layer Security) Протокол безопасности, который обеспечивает возможности шифрования и проверки подлинности для сетевых подключений.

TS CAP Политика авторизации подключений служб терминалов (Terminal Services Connection Authorization Policy). Этот тип политики применяется к серверу шлюза служб терминалов и ограничивает клиентский доступ к шлюзу извне.

TS RemoteApp Удаленные приложения RemoteApp служб терминалов. Компонент служб терминалов в Windows Server 2008, который позволяет пользователю запускать установленные на удаленном сервере программы как локальные.

Web-config Файлы конфигурации, которые можно создавать в веб-приложениях IIS и на веб-сайтах. Эти файлы могут содержать параметры, заменяющие настройки, указанные в файле ApplicationHost.config.

Windows Media Load Simulator 9 Series Бесплатная утилита Microsoft, имитирующая клиентскую нагрузку и активность на серверах Windows Media.

Windows PowerShell Среда сценариев Microsoft и язык программирования. Оболочка Windows PowerShell предоставляет пользователям возможность создавать сценарии с использованием технологий объектно-ориентированного программирования.

Автономная конфигурация сервера (Windows SharePoint Services) Опция развертывания Windows SharePoint Services, при использовании которой все необходимые компоненты устанавливаются на один сервер.

Веб-доступ к службам терминалов Компонент служб терминалов, дающий возможность пользователям получать доступ к удаленным программам RemoteApp и удаленным рабочим столам с помощью веб-браузера.

Веб-приложение (Windows SharePoint Services) Веб-сайт SharePoint, обеспечивающий в организации функциональность для подразделения. Веб-приложения можно создавать для удовлетворения потребностей различных групп пользователей.

Виртуальный сервер SMTP Экземпляр сервера SMTP, реагирующий на запросы отдельного домена, IP-адреса и номера порта. Виртуальные серверы SMTP можно независимо запускать и останавливать.

Внутренняя база Windows Встроенное ядро базы данных, используемое Windows Server 2008 для хранения внутренней информации. Службы Windows SharePoint Services и другие компоненты операционной системы могут хранить в этой базе данных свою информацию.

Глубинная защита Методология безопасности с реализацией множества уровней безопасности, применяемая для защиты таких уязвимых данных, как содержимое веб-сервера.

Делегирование компонента (IIS) Метод ограничения параметров конфигурации, которые пользователи могут просматривать или изменять при подключении к веб-серверу с помощью диспетчера IIS.

Диспетчер системных ресурсов Windows (WSRM) Утилита Windows Server 2008, используемая для управления ресурсами. Администраторы могут определить приоритеты распределения ресурсов процессора и памяти среди приложений и служб, запущенных на их серверах.

Диспетчер служб IIS (IIS Manager) Основное графическое средство управ-
• ления IIS.

Домашняя папка Папка по умолчанию, в которой хранятся файлы пользователя.

Домен маскировки SMTP-опция доменного имени, которая переписывает информацию домена для всех сообщений, пересылаемых через виртуальный сервер SMTP.

Доменные ограничения (IIS) Метод, с помощью, которого системные администраторы могут ограничивать доступ пользователей к веб-серверу на основе доменного DNS-имени клиентского компьютера.

Загрузочный образ (Boot Image) Файл .wim, используемый для загрузки нового компьютера. Системы Windows Vista и Windows Server 2008 могут загружать компьютер с помощью нескольких загрузочных образов с именем Boot.wim.

Запрос сертификата Интернета (IIS) Запрос сертификата сервера, генерируемый на общедоступном веб-сервере. Запрос посылается в центр сертификации (CA), который затем генерирует сертификат сервера для установки на компьютер.

Захваченный образ (Captured Image) Специальный загрузочный образ, предназначенный для загрузки главного компьютера и последующей загрузки на него образа для WDS.

Изоляция пользователя FTP Параметры, определяющие папки по умолчанию, а также папки, к которым пользователи FTP будут получать доступ.

Клиентская лицензия доступа служб терминалов (TS CAL) Лицензии нужно приобретать для каждого пользователя или устройства, подключаемого к службам терминалов в Windows Server 2008. Без лицензий TS CAL службы терминалов перестанут функционировать через 120 дней.

Консольный сеанс Сеанс пользователя, локально вошедшего на сервер терминалов.

Кэш/прокси-сервер Windows Media Конфигурация сервера Windows Media, позволяющая серверам управлять клиентскими подключениями и сохранять копии потокового содержимого с целью повышения производительности и расширяемости.

Многоадресная передача сервера Windows Media Метод доставки потокового мультимедиа, в случае применения которого множество клиентов подключается к одному исходящему потоку служб Windows Media.

Модули (IIS) Код веб-сервера, обеспечивающий дополнительную функциональность и возможности для веб-служб. Модули можно добавлять, удалять и отключать с помощью диспетчера IIS.

Обзорный образ (Discover Image) Загрузочный образ, который вы можете использовать на всех новых компьютерах, кроме PXE-совместимых, для указания WDS-сервера, загрузки загрузочного меню и образа.

Обработчики запросов Программы, предназначенные для приема входящих запросов IIS и генерирования ответов. Обработчики запросов можно включать и отключать с учетом конкретных требований веб-приложений.

Ограничения по IP-адресам (IIS) Метод, с помощью которого системные администраторы могут ограничивать подключения пользователей к веб-серверу на основе IP-адресов.

Одноадресная передача сервера Windows Media Метод доставки потокового мультимедиа, при использовании которого между сервером Windows Media и клиентскими компьютерами устанавливаются подключения типа «точка-точка».

Олицетворение ASP.NET Метод безопасности IIS, позволяющий приложениям ASP.NET запускаться в конкретном контексте безопасности или в контексте безопасности пользователя, прошедшего проверку подлинности.

Перенаправление принтеров (Printer Redirection) Компонент, позволяющий клиенту служб терминалов выполнять в сеансе службы терминалов операции печати на локальных клиентских принтерах.

Подключаемые модули сервера Window Media Метод, с помощью которого Microsoft и независимые поставщики могут расширять функциональность сервера Windows Media. Подключаемые модули позволяют управлять проверкой подлинности, авторизацией и производительностью.

Подключение служб терминалов Открытое окно, отображающее окно входа в сеанс на компьютере с запущенными службами терминалов.

Пользовательский профиль Коллекция данных, составляющих личное окружение пользователя, включая личные файлы, параметры приложений и конфигурацию рабочего стола.

Правила авторизации URL Параметры сервера IIS, определяющие доступное для пользователей содержимое на основе URL-запроса.

Привязка узла Параметры, определяющие типы запросов, на которые должен реагировать веб-сайт IIS.

Проверка подлинности на уровне сети (NLA) Компонент RDP 6.0, позволяющий выполнять проверку подлинности пользователя перед установлением подключения к удаленному компьютеру.

Проверка подлинности с помощью сертификата клиента Метод, с помощью которого сертификаты безопасности устанавливаются на клиентских компьютерах и проверяются веб-сервером для подтверждения идентичности пользователя компьютера.

Промежуточная реклама Рекламные аудио- и видеоролики, предназначенные для воспроизведения через регулярные интервалы при получении пользователями доступа к содержимому.

Промежуточный узел Опция конфигурации виртуального сервера SMTP, с помощью которой все исходящие сообщения пересылаются через конкретный сервер SMTP, а не напрямую. Использование промежуточных узлов может содействовать повышению производительности и уровня безопасности.

Протокол удаленного рабочего стола RDP Протокол, позволяющий транспортировать сеанс рабочего стола с одного компьютера на другой при использовании компонентов Службы терминалов (Terminal Services) и Удаленный рабочий стол (Remote Desktop).

Публикация приложения Обеспечение удаленного доступа к приложению.

Пулы приложений (IIS) Метод, с помощью которого множество веб-приложений могут запускаться в IIS с использованием разных рабочих процессов. Пулы приложений сводят к минимуму влияние веб-сайтов и веб-приложений на другие сайты и приложения.

Пункты публикации Конечная точка сервера Windows Media, обеспечивающая доступ к содержимому широковещания или по запросу. Один сервер Windows Media может управлять множеством пунктов публикации.

Режим TS-Install Режим служб терминалов, используемый с целью установки приложений для множества пользователей.

Реквизиты диспетчера IIS Метод проверки подлинности, позволяющий администраторам веб-сервера определять пользовательские учетные записи и пароли, чтобы разрешать удаленным пользователям управлять IIS.

Рекламные объявления сервера Windows Media Метод, с помощью которого поставщики информации могут предоставлять ссылки на содержимое, доступное на их серверах. Опции данного метода позволяют создавать веб-страницы или специальные файлы рекламных объявлений, к которым пользователи обычно подключаются напрямую.

Рекламные объявления сопровождения списков воспроизведения Реклама, предназначенная для воспроизведения до или после запроса клиентом доступа к пункту публикации мультимедиа по запросу.

Роль сервера Веб-сервер (IIS) Роль сервера Windows Server 2008, обеспечивающая поддержку веб-сайтов и веб-приложений. Эта роль устанавливает версию IIS 7 и позволяет администраторам включать множество дополнительных служб ролей.

Самозаверяемый сертификат Сертификат безопасности, который сервер издает для себя в целях разработки или тестирования. Самозаверяемый сертификат не обеспечивает подтверждениея идентичности, однако может использоваться для шифрования. Для создания самозаверенных сертификатов не нужно обращаться в центр сертификации.

Сеанс служб терминалов Продолжительный период времени, в течение которого пользователь работает с компьютером, где запущены службы терминалов.

Семейство узлов (Windows SharePoint Services) Группа сайтов SharePoint, совместно использующих параметры навигации и конфигурации. Для обеспечения различных функций можно создать множество семейств узлов.

Сертификат (Certificate) Цифровой документ, который идентифицирует пользователя и ключ шифрования.

Сертификаты сервера Метод, с помощью которого веб-серверы могут обеспечивать свою идентичность для веб-пользователей. Сертификаты сервера публикуются центрами сертификации (CA).

Служба управления ключами (Key Management Service, KMS) Служба и опция volume-лицензирования, основанная на ключе KMS. При KMS-активации клиенты автоматически находят локальный KMS-хост И проходят процедуру активации без вмешательства пользователя.

Службы Windows Media Роль сервера, обеспечивающая доступ к содержимому аудио- и видеовещания, а также по запросу.

Службы Windows SharePoint Services (WSS) Роль сервера, предоставляющая пользователям возможность получать доступ к сайтам SharePoint с целью сотрудничества, совместного управления документами и создания коммуникаций. Службы WSS обеспечивают веб-интерфейс для получения доступа к содержимому и для администрирования.

Службы потокового мультимедиа Роль сервера, обеспечивающая доступ к содержимому аудио- и видеовещания, а также по запросу.

Службы управления IIS Служба ролей, обеспечивающая возможности удаленного управления IIS для пользователей роли Веб-сервер (IIS).

Службы управления правами Active Directory (AD RMS) Роль сервера Windows Server 2008, позволяющая компьютеру издавать сертификаты и разрешения на создание и редактирование содержимого документов и файлов мультимедиа.

Сопоставления обработчиков (IIS) Параметры конфигурации, которые определяют типы содержимого, и обработчики, которые выполняют обработку запросов содержимого.

Список воспроизведения сервера Windows Media Файл, содержащий список аудио- и видеофайлов, запланированных для воспроизведения.

Удаленный рабочий стол для администрирования (RDA) Режим служб терминалов, не требующий установки роли сервера Службы терминалов (Terminal Services) или приобретения сертификатов TS CAL. Этот компонент, который также носит имя Удаленный рабочий стол (Remote Desktop), разрешает выполнять лишь два одновременных сеанса рабочего стола на локальном сервере, включая консольный сеанс. По умолчанию данный компонент отключен.

Уровни доверия .NET Параметры конфигурации IIS, которые применяются к приложению .NET Framework и определяют правила доступа кода CAS (Code Access Security).

Установочный образ (Install Image) Образ установки системы Windows Vista или Windows Server 2008, который можно развернуть на компьютере.

Файл WIM (WIM File) Файл, в котором содержится один или несколько образов в формате Windows Imaging.

Ферма серверов Windows SharePoint Services Опция развертывания Windows SharePoint Services, позволяющая множеству веб-серверов на клиентской стороне получать доступ к серверам баз данных на серверной стороне с целью повышения производительности, расширяемости и стабильности.

Фермы веб-серверов Группы веб-серверов, совместная работа которых обеспечивает повышение их мощности, расширяемости, производительности и стабильности. Как правило, серверы в ферме совместно используют одно содержимое и те же параметры конфигурации.

Фронт атак Общая потенциальная уязвимость безопасности сервера или службы. Фронт атак, например, для веб-сервера можно уменьшить, отключив ненужные компоненты и службы.

Центр администрирования SharePoint Веб-сайт по умолчанию, предназначенный для управления Windows SharePoint Services. С его помощью можно выполнять операционные задачи и управлять приложениями.

Центр сертификации (CA) Организация или служба, генерирующая сертификаты серверов. Доверенные сторонние организации могут издавать сертификаты для веб-серверов в Интернете.

Шаблоны квот (Windows SharePoint Services) Параметры, управляющие максимальным объемом дискового пространства, которое используется семейством узлов. Создание шаблонов квот и управление ими осуществляется в центре администрирования SharePoint.

Шаблоны приложений (Windows SharePoint Services) Загружаемые шаблоны сайтов SharePoint, которые можно установить для использования в новых

сайтах. Как правило, шаблоны приложений создаются для конкретных задач или организаций.

Широковещание сервера Windows Media Метод отправки потокового аудио и видео множеству пользователей одновременно. Широковещание чаще всего используется для передачи событий в прямом эфире с помощью кодировщика потокового мультимедиа.

Шлюз служб терминалов Компонент Windows Server 2008, позволяющий авторизованным пользователям Интернета подключаться к серверу терминалов в частной сети.

Об авторах

Дж. К. Макин (J. C. Mackin)

Дж. К. Макин — писатель, редактор, консультант и инструктор, более десяти лет посвятивший работе с сетями Microsoft. Его перу принадлежат десятки книг (некоторые из них написаны в соавторстве с другими специалистами), включая столь известные, как MCSA/MCSE Self-Paced Training Kit (Exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure; MCITP Self-Paced Training Kit (Exam 70-443): Designing a Database Server Infrastructure Using Microsoft SQL Server 2005 и MCITP Self-Paced Training Kit (Exam 70-622): Supporting and Troubleshooting Applications on a Windows Vista Client for Enterprise Support Technicians. Дж. К. Макин является обладателем сертификатов MCITP, MCTS, MCSE, MCDST, MCT, имеет степень магистра в области управления телекоммуникациями и сетями. В свободное от основной работы время он занимается панорамными съемками средневековых поселений в Италии и Франции.

Анил Десаи (Anil Desai)

Анил Десаи, независимый консультант, основная сфера деятельности которого — оценка и реализация IT-решений, а также управление такими решениями, имеет более чем 12-летний опыт работы с серверными продуктами Microsoft и платформой разработок Microsoft .NET. Он автор многочисленных книг, посвященных сертификации Microsoft, платформе Windows Server, виртуализации, Active Directory, Microsoft SQL Server и IT-управлению, а также сотрудник нескольких известных электронных и печатных журналов. Многие свои презентации на конференциях Анил нередко превращал в события национального масштаба. Он является обладателем сертификатов MCITP, MCSE, MCSD, имеет звание Microsoft MVP (Windows Server — Management Infrastructure). Проживает Анил Десаи в г. Остин, штат Техас, любит музицировать на гитаре и барабанах, увлекается играми на ХЬохЗбО. Более подробные сведения об этом авторе можно найти по адресу *http://AnilDesai.net.*

Макин Дж. К., Десаи Анил

Развертывание и настройка Windows Server® 2008

Учебный курс Microsoft

Подготовлено к печати издательством «Русская Редакция»
123290, Москва, Шелепихинская наб., д. 32. Тел.: (495) 638-5-638, тел./факс: (495) 256-7145
e-mail: info@nisedit.com, http://www.rusedit.coni

1И.РУШП РЕДАКЦИЯ

Подписано в печать 05.08.2008 г.
Формат 70x100/16. Усл. физ. л. 40
Тираж 2500 экз. Заказ № 3414

Санитарно-эпидимиологическое заключение на продукцию
Ns 77.99.60.953.Д.003650.04.08 от 14.04.2008 г. выдано Федеральной службой
по надзору в сфере защиты прав потребителей и благополучия человека.
Отпечатано с готовых диапозитивов
в ГУП «Типография «Наука»
199034, Санкт-Петербург, 9 линия, 12

Учебный

> - v