Александр Кенин

Практическое руководство системного администратора

Санкт-Петербург

«БХВ-Петербург»

2010

УДК 681.3.06
ББК 32.973.26-018.2
К35

Кенин А. М.

К35 Практическое руководство системного администратора. — СПб.: БХВ-Петербург, 2010. — 464 с.: ил. — (Системный администратор)

ISBN 978-5-9775-0435-5

Практическое руководство к действию для системных администраторов, создающих и эксплуатирующих информационные системы офиса. Наряду с описанием коммерческих продуктов, рассматриваются решения на основе открытых кодов, не требующих приобретения лицензий. Автор обобщил собственный богатый практический опыт и интернет-ресурсы по теме в единое целое и представил рекомендации по установке, настройке и оптимизации основных служб офиса.

Рассмотрены особенности разворачивания операционных систем Windows и Linux (Ubuntu), программ корпоративной работы, мониторинга состояния серверов. Даны конкретные рекомендации по настройке основных сетевых служб, оптимизации почтового сервера, обеспечению безопасности при распределенной работе в Интернете. Описана технология разрешения проблем в работе операционной системы и прикладных программ, приведены многочисленные советы по их тонкой настройке. Подробно изложен процесс создания собственной бесплатной IP-телефонии офиса.

Для системных администраторов

УДК 681.3.06
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Григорий Добин*
Редактор	*Леонид Кочин*
Компьютерная верстка	*Натальи Караваевой*
Корректор	*Виктория Пиотровская*
Дизайн серии	*Инны Тачиной*
Оформление обложки	*Елены Беляевой*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 30.10.09.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 37,41.
Тираж 2000 экз. Заказ №
"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Санитарно-эпидемиологическое заключение на продукцию
№ 77.99.60.953.Д.005770.05.09 от 26.05.2009 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

ISBN 978-5-9775-0435-5

© Кенин А. М., 2009
© Оформление, издательство "БХВ-Петербург", 2009

Оглавление

Введение **1**

От автора 1
Открытое программное обеспечение 2
Открытые стандарты и проприетарные решения 7
Windows и Linux 8

Глава 1. Сетевая инфраструктура **9**

Строение сети передачи данных 9
Размеры сегментов сети 9
Выбор типа коммутаторов 10
Топология сети передачи данных 11
Ищем точку подключения компьютера 12
Контроль подключения к СКС 15
Предварительные настройки для использования протокола 802.1*x* 17
Настройка политики доступа на основе протокола 802.1*x* 18
Настройка коммутатора для работы с протоколом 802.1*x* 21
Обеспечение отказоустойчивой работы сетевой инфраструктуры 22
Отказоустойчивая топология сети передачи данных 22
Построение отказоустойчивой сети на основе протоколов второго уровня 23
Построение отказоустойчивой сети на основе протоколов третьего уровня 25
Время восстановления структуры сети 27
Настройка протокола IP 28
Протоколы UPD, TCP, ICMP 29
IPv6 29
Параметры TCP/IP-протокола 29
IP-адрес 29
Групповые адреса 30
Распределение IP-адресов сети малого офиса 31

Маска адреса ... 31
Шлюз (Gateway, default gateway) ... 33
Таблицы маршрутизации ... 33
Назначение адресов при совместном использовании подключения к Интернету ... 34
Порт ... 35
Имена компьютеров в сети TCP/IP ... 37
Проверка каналов связи ... 37
Диагностика линий связи ... 38
Диагностика IP-протокола ... 39

Глава 2. Сетевые службы ... 47

Служба автоматического назначения параметров IP-адреса ... 47
Адресация APIPA ... 47
Серверы DHCP ... 48
Настройка серверов DHCP в Windows ... 48
Установка и настройка сервера DHCP в Ubuntu ... 50
Обслуживание DHCP-сервером других сегментов сети ... 51
Отказоустойчивая конфигурация DHCP-сервера ... 52
Статическое разрешение имен ... 53
Серверы DNS ... 54
Основные понятия DNS ... 54
Основные типы записей DNS ... 57
Разделение DNS ... 58
Одинаковые имена локального домена и домена Интернета ... 58
Различные имена локального домена и домена Интернета ... 60
Установка сервера DNS ... 60
Установка DNS в Windows Server ... 61
Установка и настройка сервера DNS в Ubuntu ... 62
Динамическое обновление DNS ... 65
Обслуживание и диагностика неисправностей DNS-сервера ... 68

Глава 3. Обеспечение доступа в Интернет ... 73

Подключение к Интернету с использованием аппаратного маршрутизатора ... 73
NAT ... 75
Подключение к Интернету с использованием службы маршрутизации и удаленного доступа серверов Windows ... 76
Совместное использование интернет-подключения ... 77
Публикация компьютеров в Интернете при совместном использовании подключения ... 78
Ограничения совместного использования подключения к Интернету ... 79

Подключение к Интернету с помощью Microsoft ISA Server ... 79
Настройка прокси-сервера ... 81
Анализаторы логов ... 81
Поиск причин запрета трафика ... 82
Подключение к Интернету с использованием серверов Ubuntu ... 82
Настройка ufw ... 83
Межсетевой экран iptables ... 84
Последовательность обработки пакета (таблицы) ... 84
Использование iptables в Ubuntu ... 85
Правила iptables ... 86
Команды ... 87
Параметры ... 87
Опции ... 88
Настройка NAT ... 89
Очистка всех правил iptables ... 90
Назначение политик по умолчанию ... 91
Пример настройки iptables ... 91
Пользовательские цепочки команд ... 92
Некоторые полезные функции iptables ... 93
Отладка iptables ... 94
Настройка VPN-подключения к интернет-провайдеру ... 95
Прокси-сервер ... 98
Автообнаружение прокси-серверов ... 99
Установка и настройка прокси-сервера ... 101
Дополнительные настройки прокси-сервера ... 102
Как создавать собственные настройки ... 103
Настройка использования полосы пропускания ... 104
Блокировка рекламы, порносайтов и т. п. ... 106
Улучшение эффективности использования кэша прокси-сервера ... 107
Аутентификация доступа в Интернет ... 108
"Прозрачный" прокси-сервер ... 110
Анализ журналов работы прокси-сервера ... 110
Антивирусная проверка HTTP-трафика ... 113

Глава 4. Готовим новый компьютер к эксплуатации ... 117

Паспорт компьютера ... 117
Установка системных обновлений ... 118
Варианты установки программного обеспечения нового компьютера ... 118
Индивидуальная настройка серверов ... 119
Установка обновлений безопасности ... 120
Когда устанавливать обновления ... 120

Настройка обновлений с сервера интрасети ... 122
Нужно ли устанавливать все обновления? ... 124
Клонирование систем ... 125
WAIK ... 125
Дублирование жесткого диска ... 125
Подготовка к клонированию: утилита sysprep ... 126
Восстановление системы ... 128
Подготовка образа диска к восстановлению на отличающемся оборудовании ... 129
Клонирование компьютеров-членов домена ... 130
Сброс пароля администратора Windows ... 130

Глава 5. Доменная организация информационной системы ... 135

Структура домена Windows ... 135
Хозяева операций ... 137
Сервер глобального каталога (GC) ... 138
Создание нового домена ... 139
Создание домена на серверах Windows ... 139
Настройка Ubuntu в качестве контроллера домена ... 140
Серверы Linux в качестве контроллеров домена ... 140
Настройка контроллера домена на сервере корпоративной почты Zimbra ... 141
Настройка параметров аутентификации ... 146
Добавление новых членов домена ... 149
Добавление Windows-систем ... 149
Модификация настроек Windows-систем при добавлении их в домен ... 151
Добавление Linux-систем в домен Windows ... 152
Диагностика службы каталогов ... 153
Обнаружение неисправностей AD ... 154
Средства тестирования AD ... 154
Проверка разрешения имен ... 158

Глава 6. Настройка почтовой системы предприятия ... 161

Варианты почтового обслуживания пользователей ... 161
Протоколы для работы с почтовыми ящиками ... 162
Создание простого POP3-сервера ... 163
Почтовый сервер Microsoft Exchange ... 166
Выбор компьютера для установки Microsoft Exchange ... 167
Установка Exchange Server ... 168
Настройка Exchange Server после установки ... 169
Настройка почтовых доменов ... 170

Настройка кодировки электронных сообщений 170
Настройка отправки автоматических сообщений 171
Настройка протоколирования сообщений 172
Настройка встроенной антиспам-защиты 174
Опциональные настройки 178
Настройка фильтрации вирусов 183
Контроль за работой сервера Exchange 185
Резервное копирование сервера Exchange 188
Обслуживание почтовых баз 189
Использование базы восстановления 193
Трассировка пользовательских сообщений в Exchange 195
Zimbra Collaboration Suite 195
Возможности совместной работы в ZCS 196
Установка Zimbra 197
Администрирование ZCS 199
Особенности пользовательских почтовых ящиков Zimbra 203
Почтовый клиент Zimbra 204
Интеграция с Microsoft Outlook 205
Особенности настройки фильтрации спама в ZCS 205
Резервное копирование Zimbra 206
Трассировка сообщений в Zimbra 207
Поиск неисправностей ZCS 208

Глава 7. Организация корпоративных ресурсов 209

Использование распределенной файловой системы 210
Создание DFS в Windows-системах 210
Репликация DFS в домене Windows 212
Репликация папок в рабочих группах 214
Настройка DFS в Ubuntu 215
Лимитирование предоставляемых файловых ресурсов 215
Настройка квотирования в Ubuntu 215
Настройка квотирования в Windows 218
Квотирование на уровне файловой системы 218
Квотирование общих папок 219
Блокировка записи в папки по типам файлов в Windows 221
Запрет записи на сетевые ресурсы Ubuntu по типам файлов 223
Корпоративные порталы 223
Установка Liferay на сервере Ubuntu 224
Установка eGroupware 226
Настройка диаграммы Ганта 229

Установка служб Windows SharePoint Services 230
Установка дополнительных шаблонов SharePoint 233
Настройка страниц узла 235
Используйте возможности штатных элементов SharePoint 236
Установка поискового сервера по общим ресурсам 237
Настройка автоматических оповещений об изменениях документов на чужих серверах 239

Глава 8. Обеспечение удаленной работы пользователей 241

Терминальный доступ 241
Терминальные серверы от Microsoft 242
Особенности установки ПО на сервере терминалов 243
Безопасность при работе с терминальным сервером 244
Удаленные приложения 245
Web-доступ к терминальному серверу. Шлюз терминалов 247
Некоторые особенности работы в режиме терминального доступа 248
Подключение к консоли 249
Командная строка управления терминальными сессиями 249
Терминальные серверы в Linux 250
Технологии доставки виртуального рабочего стола 250
Удаленное подключение пользователей к внутренней сети предприятия 251
Создание входящего VPN-подключения на рабочих станциях Windows 252
Создание входящих VPN-подключений на серверах Windows 253
Безопасное объединение локальных сетей офисов 253
Подключение офисов по VLAN 254
Подключение удаленных офисов с использованием VPN-серверов Windows 255
Фильтрация VPN-трафика 256
В случае разрыва канала при доменной организации офиса... 257
Read-only domain controllers 258
Подключение удаленных офисов с использованием ПО Microsoft ISA Server 262
Подключение удаленных офисов с помощью VPN-серверов Ubuntu 262
Подключение "офис - офис" на основе технологии SSH 265
Применение Ubuntu для маршрутизации в сети филиалов 270
Управление оборудованием по сети Интернет 270
Intelligent Platform Management Interface 271
Управление оборудованием по сети IP 273
Утилиты удаленного управления Windows 274

Глава 9. Мониторинг информационной системы 275

Зачем нужен мониторинг 275
Системы мониторинга 276
Принципы мониторинга систем 277
Контроль журналов Windows 277
Operation Manager 2007 281
Установка сервера Operation Manager 2007 282
Необходимые операции по настройке сервера после установки 284
Импорт пакетов мониторинга 284
Добавление контролируемых систем 285
Настройка оповещений SCOM 287
Немного о структуре объектов SCOM 288
Установка Nagios 289
Первичное подключение к Nagios 292
Немного о логике работы Nagios 293
Структура конфигурационных файлов Nagios 296
Описание команд Nagios 296
Описание шаблонов служб 297
Описания служб Nagios 298
Описание контролируемых систем в Nagios 299
Описание временных параметров 301
Использование встроенных в Nagios команд контроля 302
Настройка мониторинга серверов Windows 306
Настройка мониторинга серверов Linux 313
Установка плагина NRPE из исходных кодов 313
Установка NRPE из подготовленных пакетов для контроля Linux-системы 314
Установка дополнительных плагинов 315
Использование прокси-NRPE 315
Мониторинг журналов событий Windows 315
Мониторинг систем с использованием протокола SNMP 317
Мониторинг Windows-систем на основе WMI 322
Мониторинг коммутационного оборудования 326
Использование собственных программ мониторинга 330
Отображение собранных данных на графиках 331
Как это работает 332
Установка Nagiosgraph 332
Редактирование интерфейса Nagios 335
Завершение установки 337
Создание графиков новых служб 337
Автоматическое реагирование на сбои в работе контролируемых систем 337

Глава 10. Поиск и устранение неисправностей 341

Где найти помощь 341
Что может отказать 343
Неисправности кабельной подсистемы 344
Неисправности активного (коммутационного) оборудования 346
Неисправности аппаратной части компьютеров 346
Резервирование узлов компьютера 347
Контроль теплового режима работы системы 348
Ошибки программного обеспечения 349
Выяснение причин катастрофических ошибок в программном обеспечении 349
Восстановление "упавших" систем 352
Загрузка в безопасном режиме 352
Загрузка последней удачной конфигурации 353
Консоль восстановления 353
Режим восстановления в Windows XP SP2/Windows 2003 Server 354
Варианты восстановления Windows Vista/Windows Server 2008 355
Восстановление реестра из файлов точек восстановления системы 356
Использование программ типа ERD Commander 358
Восстановление удаленных данных 358
Корзины 359
Восстановление из теневых копий 359
Восстановление данных с жестких дисков 361
Анализ производительности 362
Счетчики состояния системы 364
Оценка производительности процессора 365
Оценка использования оперативной памяти 367
Оценка дисковой подсистемы 367
Оценка работы сетевого адаптера 369
Счетчики прикладных программ 369
Server Performance Advisor 369
Диагностика доступа к ресурсам компьютера 371

Глава 11. Организация IP-телефонии офиса 373

Программная АТС 373
Подключение IP АТС к телефонным станциям общего пользования 374
IP-телефоны: выбор и необходимые настройки сети 375
Установка Asterisk 378
Локализация Asterisk 380
Первоначальная проверка Asterisk 380

Настройка АТС ... 383
Диагностика АТС ... 383
Настройка конфигурации SIP-телефонов ... 384
Настройка плана звонков ... 385
Синтаксис шаблонов номеров телефонных линий ... 389
Настройка плана звонков на разные периоды времени ... 390
Создание голосового меню ... 392
Настройка голосовой почты ... 393
Настройка групп вызова и перехвата звонка ... 394
Запись звукового сообщения ... 395
Телефонная книга ... 399
Конференции ... 400
Некоторые дополнительные возможности Asterisk ... 401
Функции и приложения в Asterisk ... 402

Приложение. Базовые правила работы с Ubuntu ... 403

Помощь ... 403
Установка Ubuntu ... 403
Настройка локализованной консоли ... 404
Настройка сетевых параметров ... 405
Настройка синхронизации времени ... 407
Установка программ ... 408
Установка последних обновлений ... 408
Обновление версии сервера ... 409
Установка и удаление программ ... 409
Переконвертация пакетов ... 412
Настройка параметров прокси-сервера для команды обновлений ... 412
Установка программ из исходных кодов ... 413
Изоляция приложений ... 416
Основные правила работы в Ubuntu ... 418
Графический интерфейс ... 418
Вход и выход пользователя, завершение работы ... 420
Работа в консоли ... 420
Работа в нескольких консолях ... 420
Путь к исполняемому файлу ... 421
Исполняемые файлы ... 421
Регистрозависимость ... 421
Автозаполнение ... 421
Фоновое выполнение команд ... 422
Перенаправление потоков ... 422
Подсказка по командам ... 424

Ссылки ... 424
Alias ... 424
Добавление пользователей ... 425
Права суперпользователя ... 426
Кто работает на компьютере ... 427
Несколько полезных команд ... 428
Права доступа ... 429
Принципы размещения данных в Ubuntu ... 430
Текстовый редактор VI ... 431
Команды для работы с файлами и дисками ... 433
Просмотр существующих дисков ... 433
Размеры папок и файлов ... 435
Подключение ISO-образа в Ubuntu ... 436
Подключение CD-ROM ... 437
Подключение flash-карт ... 437
Команды работы с файлами и папками ... 437
Поиск файлов ... 439
Создание шифрованного диска ... 440
Работа в Ubuntu с компьютеров под управлением Windows ... 441
Подключение Windows-сетевых дисков ... 444
Выполнение команд на удаленном компьютере ... 446
Создание и удаление демонов ... 447
Выполнение заданий по расписанию ... 447
Сброс пароля администратора ... 449

Предметный указатель ... 451

Введение

От автора

В каждой информационной системе есть компоненты, работа которых обеспечивает стабильность всех приложений. Администратору важно правильно настроить и сопровождать функционирование базовых служб. В этой книге мы рассмотрим вопросы, связанные с установкой, настройкой и обслуживанием системы передачи данных, базовых сетевых сервисов (DHCP, DNS и др.), систем обеспечения совместной работы пользователей (электронная почта, порталы) и контроля состояния информационной системы. Все то, с чем каждодневно приходится сталкиваться администратору.

В силу ограниченности ресурсов сопровождением информационных систем в малых и средних организациях часто занимаются специалисты, вынужденные одновременно работать в нескольких структурах. Часто им просто не хватает времени, чтобы изучить функции того или иного продукта, иногда внедрение и поддержка нового функционала просто расценивается как излишняя, неоплачиваемая нагрузка. Поэтому я постарался показать, как те или иные возможности современного программного обеспечения позволяют обеспечить более комфортную работу.

Настоящая книга предназначена в помощь тем системным администраторам, которые хотят наиболее эффективно задействовать возможности современных технологий. В ней я постарался изложить практические рекомендации по администрированию информационных систем, уделяя основное внимание конкретным советам по настройке применяемых продуктов. Те, кому важнее описание технологий и принципов, реализованных в информационных системах, могут обратиться, например, к моей книге "Самоучитель системного администратора. 2-е издание", БХВ-Петербург, 2008.

Учитывая, что в состав современных информационных систем входят как Windows-, так и Linux-компьютеры, рекомендации даны для обеих ОС.

В силу ограниченности объема издания я не смог уделить здесь достаточно внимания проблемам устранения неисправностей. При этом я постарался, по возможности, указать основные источники, к которым можно обратиться за получением подробной подсказки. Много практических рекомендаций по тюнингу операционных систем на основе Windows приведено в моей книге "Windows Vista: Народные советы", БХВ-Петербург, 2008.

В информационных технологиях очень важен показатель удовлетворенности клиента. Также и автору хотелось бы получить ваши отзывы, замечания, предложения, которые могли бы улучшить эту книгу, сделать ее более полезной на практике. Их можно отправить на адрес издательства или мне по электронной почте на **kenin@hotbox.ru**.

Открытое программное обеспечение

Базовые службы, которые рассматриваются в настоящей книге, давно уже основываются на открытых стандартах и не являются собственностью какой-либо компании. Эти решения могут быть реализованы как на коммерческом программном обеспечении, так и — при той же функциональности — на бесплатных программах. Зачастую мы платим существенные суммы за проекты, которые можно реализовать совершенно бесплатно, только потому, что лица, принимающие решения, заинтересованы в продаже и покупке дорогих продуктов.

> ***Замечание***
>
> Мы говорим не только об откатах, которые стали "притчей во языцех" всей системы поставок в информационных технологиях. Проценты, которые получают фирмы-продавцы совершенно официально от вендоров за продажу программного обеспечения, являются основой существования таких организаций. И опрометчиво думать, что представители коммерческих структур будут рубить сук, на котором сами сидят.

Конечно, существует привыкание к продукту. Если вы изучили одну программу, то переход к другой неизбежно вызовет дискомфорт. Но это временное явление. Опасения, что системы на основе Linux требуют специальной подготовки специалистов, беспочвенны, ведь хорошим администратором систем Windows тоже невозможно стать, имея только домашний опыт работы в Интернете и практику ремонта компьютеров друзей и знакомых.

Каждый программный продукт уникален. Но проанализируйте, какие операции вы *реально* выполняете с его помощью? В подавляющем большинстве случаев окажется, что все это можно сделать на бесплатном программном обеспечении. Зачем платить деньги за тот функционал, который не будет

востребован? Будем надеяться, что текущее состояние экономики заставит, наконец, считать деньги и оценивать эффективность выбора тех или иных продуктов.

Да, смена программы вызовет некоторое неудобство в начале работы. Я помню тот момент, когда мне в первый раз пришлось менять рабочий инструмент — вместо Microsoft Internet Explorer установил Firefox, поскольку более уже не мог мириться с медленной работой в Интернете из-за недостаточной мощности компьютера. Первые два дня я постоянно пересиливал себя в желании оставить все как есть, поскольку привык к какому-то сочетанию управляющих клавиш и т. п. Сейчас я открываю Internet Explorer только вынужденно, например, при обращении к Microsoft CRM, программе, которая работает только в окне своего обозревателя. А переход на OpenOffice вообще прошел незаметно: сначала я использовал OpenOffice в тех случаях, когда уставал искать нужное мне меню в ленте Microsoft Office 2007, а потом даже и не заметил, как полностью переключился на работу в бесплатном продукте, несмотря на наличие лицензии на коммерческое ПО.

Для большинства задач вполне реально найти бесплатный продукт, с помощью которого можно выполнить необходимые операции. Приведу небольшой перечень ссылок на программное обеспечение, с которым мне довелось работать (табл. 1).

Таблица 1. *Некоторые ссылки на бесплатные программные продукты*

Название программы	**Ссылки**	**Примечания**
OpenOffice	**http://www.openoffice.org/**	Пакет офисных программ, включает текстовый процессор, программы для работы с электронными таблицами, базами данных, презентациями. Форматы документов совместимы с продуктами Microsoft Office. Если загружать с сайта разработчика, то дополнительно необходимо устанавливать расширения для русского языка (проверка орфографии, переносы). Поэтому лучше воспользоваться специальной сборкой, полностью подготовленной для работы с русским языком с сайта компании "Инфра-Ресурс" — **http://i-rs.ru/Produkty/OpenOffice.org** Интерфейс русский

Таблица 1 *(продолжение)*

Название программы	Ссылки	Примечания
Firefox	**http://www.firefox.com/**	Обозреватель Интернета. Особенность этой программы в том, что для нее созданы тысячи различных дополнений, расширяющих функциональность обозревателя: различные записные книжки, блокировщики рекламы, переводчики и т. п. Поэтому не ограничивайтесь загрузкой самой программы, а обязательно расширьте ее возможности установкой дополнений. Интерфейс русский
GIMP	**http://www.gimp.org/**	Графический редактор — в некотором смысле аналог Adobe Photoshop. Работает со слоями, содержит множество инструментов и фильтров для обработки изображений, различные кисти и т. п. Интерфейс русский
InfraRecorder	**http://infrarecorder.org/**	Программа для записи, копирования CD- и DVD-дисков. Работает с аудио-, видеодисками, дисками с данными и с их образами. Интерфейс русский
FreeCommander	**http://www.freecommander.com/**	Файловый менеджер. Для тех, кто привык работать с панелями Norton'a. Интерфейс русский
7Zip	**http://www.7-zip.org/**	Архиватор. Может распаковать архивы форматов ARJ, CAB, CHM, CPIO, DEB, DMG, HFS, ISO, LZH, LZMA, MSI, NSIS, RAR, RPM, UDF, WIM, XAR и Z. Есть русскоязычный интерфейс

Таблица 1 *(продолжение)*

Название программы	**Ссылки**	**Примечания**
CCleaner	**http://www.ccleaner.com/**	Мощная программа для чистки реестра системы. Интерфейс англоязычный
Avast! AVG Avira PCTools Antivirus	**http://www.avast.com/** **http://free.avg.com/** **http://www.free-av.com/** **http://www.pctools.com/free-antivirus/**	Некоторые антивирусные программы, лицензия которых предусматривает бесплатное применение в некоммерческих целях. В коммерческих целях можно использовать ClamWin (**http://www.clamwin.com/**), но он не содержит антивирусного монитора в реальном режиме времени (позволяет сканировать файлы). В то же время на его основе созданы антивирусные серверы, сканирующие весь входящий трафик организации (как почтовый — см. раздел "*Zimbra Collaboration Suite*", так и трафик Интернета (см. раздел *"Антивирусная проверка HTTP-трафика"*)
Microsoft Security Essentials	**http://www.microsoft.com/security_essentials/**	Бесплатная антивирусная программа от Microsoft для защиты домашних компьютеров. Механизм сканирования и обнаружения вирусов практически не уступает лидерам. Полное сканирование системы производится в моменты неактивности. Работает в Windows XP с пакетами обновлений SP2 или SP3, Windows Vista и Windows 7 (в том числе для режима Windows XP) на 32-битовых и 64-битовых платформах. На момент подготовки книги русскоязычная версия продукта отсутствовала
ZoneAlarm	**http://www.zonealarm.com/**	Персональный межсетевой экран

Таблица 1 *(продолжение)*

Название программы	**Ссылки**	**Примечания**
COMODO Internet Security	**http://www.personalfirewall.comodo.com/**	Система персональной защиты, включающая межсетевой экран и антивирусную проверку
PC Tools Firewall Plus	**http://www.pctools.com/firewall/**	Межсетевой экран для Windows Vista 32-bit, XP, 2000 и Windows Server 2003
Ad-Aware Free	**http://lavasoft.element5.com/**	Программа для защиты от вредоносных кодов (SpyWare, mailware и т. д.)
PDF creator PDF converter	**http://sourceforge.net/projects/pdfcreator/** **http://www.dopdf.com//**	Утилиты устанавливают в системе PDF-принтер: печать на этот принтер создает документы в формате PDF (исключается необходимость в программе Adobe Acrobat)
Foxit Reader	**http://www.foxitsoftware.com/**	Легкая альтернатива Acrobat Reader (тоже бесплатной программы)
StarDict	**http://stardict.sourceforge.net/**	Программа-переводчик
Inkscape	**http://www.inkscape.org/**	Редактор векторной графики, сходный по возможностям с Illustrator, Freehand, CorelDraw
Фабрика форматов	**http://www.formatoz.com/**	Программа для преобразования форматов аудио- и видеофайлов. Интерфейс русский
Cuneiform	**http://www.cuneiform.ru/**	Программа оптического распознавания символов
Codendi Collabtive dotProject eGroupWare KForge OpenGoo Project.net ProjectPier Redmine Trac JotBug	**http://www.codendi.com** **http://collabtive.o-dyn.de** **http://www.dotproject.net** **http://www.egroupware.org** **http://www.kforgeproject.com/** **http://www.opengoo.org** **http://www.project.net** **http://www.projectpier.org** **http://www.redmine.org** **http://trac.edgewall.org** **http://www.jotbug.org**	Программное обеспечение управления проектами, основанное на Web-интерфейсе. Поддерживает обычно управление ресурсами, контакты, систему обмена сообщения, отслеживания событий, управления документами и т. д. Сравнительную характеристику продуктов можно уточнить на странице **http://en.wikipedia.org/wiki/List_of_project_management_software**

Таблица 1 *(окончание)*

Название программы	Ссылки	Примечания
SugarCRM	**http://www.sugarcrm.com/crm/community/sugarcrm-community.html**	Бесплатная версия коммерческого пакета управления отношениями с клиентами (CRM)
Alfresco	**http://www.alfresco.com/**	Система управления документами (Enterprise Content Management)

Отметим еще страницу **http://www.manageengine.com/free-softwares-download.html**, где представлен список утилит для администрирования системы, которые можно бесплатно загрузить и использовать в своей работе. Многие некоммерческие продукты можно загрузить с сайта Snapfiles (**http://www.snapfiles.com/**), специализирующегося на бесплатных или условно-бесплатных продуктах.

Это далеко не полный список доступных программ, но уже и он дает представление, насколько широко распространено программное обеспечение, с которым вы можете работать на законных основаниях.

Не следует также забывать, что многие коммерческие продукты имеют специальные выпуски, например, у всех коммерческих серверов баз данных есть "младшие" бесплатные "братья". Так, у Microsoft SQL Server 2008 существует бесплатная версия Microsoft SQL Server Express Edition. Эти редакции программ при определенных ограничениях функциональности (например, в случае Microsoft SQL Server Express Edition максимальный размер базы данных ограничен величиной 2–4 Гбайт в зависимости от версии, графическую оболочку управления нужно загружать отдельно и т. п.) позволяют использовать продукт бесплатно. Как правило, о наличии таких редакций продавцы ПО и разработчики проектов часто "забывают".

Открытые стандарты и проприетарные решения

Любая реклама назойливо предлагает внедрить "самое-самое" решение какой-либо фирмы. Конечно, применяя уникальную технологию, вы можете получить более высокую производительность, чем в типовом решении, но при этом оказываетесь привязанными к конкретному вендору. И не всегда такой выбор окажется оправданным в перспективе.

Поэтому я бы советовал ориентироваться на решения, описанные в открытых стандартах. И только в случае невозможности такого выбора — применять проприетарные технологии.

Системные администраторы могут оказать серьезное влияние на выбор продукта через выдвижение технических требований. И если в меньшей степени заботиться "о выплате ипотеки", то даже конкурс можно организовать и провести так, чтобы он привел к покупке оптимального варианта.

Windows и Linux

В реальности очень сложно предположить, какие программные продукты будут востребованы. Зависит это от множества факторов, как объективных (качество продукта в той или иной версии, стоимость владения и т. п.), так и субъективных (привычки, опасения выбора неизвестного продукта...). Однако можно уверенно сказать, что большинство информационных систем сегодня включают в себя как продукты на основе Windows, так и Linux-системы. Администратору важно уметь работать со всеми этими линейками. Именно поэтому в данной книге параллельно описаны реализации решений как на серверах Windows, так и на сервере Ubuntu — представителе многочисленной линейки Linux-операционных систем.

Почему для описания в книге выбрана именно операционная система Ubuntu? Это не жесткая рекомендация. Просто эта операционная система бесплатна, поддерживается крупнейшими вендорами оборудования, а для серверных редакций гарантируется длительная поддержка (пять лет с момента выпуска). Причем для обеспечения этой поддержки созданы специализированные фонды, в которые уже перечислены существенные финансовые средства.

> ***Совет***
>
> При выборе версий серверов Ubuntu обращайте внимание на параметр поддержки: наличие в обозначении символов LTS (Long Term Support) свидетельствует о таком длительном сроке.

Для тех, кто не знаком с основами Linux, в *приложении* даны краткие рекомендации по установке, обслуживанию и работе в операционной системе Ubuntu.

В своей организации вы вольны устанавливать любые версии программного обеспечения. Естественно, что в этом случае синтаксис некоторых команд будет отличаться от тех примеров, которые описаны в настоящей книге и базируются на реальных настройках серверов, выполненных автором в различных эксплуатируемых системах.



Глава 1

Сетевая инфраструктура

Как театр начинается с вешалки, так и любая информационная система — с ее инфраструктуры. Недостаточное внимание к качеству сети передачи данных может привести к постоянным проблемам при эксплуатации информационной системы.

Строение сети передачи данных

Практически все сети предприятий сегодня базируются на технологии Ethernet и протоколе TCP/IP. Наличие других протоколов, как правило, наследовано исторически и обусловлено эксплуатируемым оборудованием.

Рассмотрим, что необходимо знать системному администратору при работе и модернизации таких сетей.

Размеры сегментов сети

Длина медного кабеля от одного элемента активного оборудования до другого, например, от компьютера до коммутатора, в сети Ethernet не должна превышать 100 м. Обычно стандартами предусмотрена максимальная длина самого кабеля 90 м, а 10 м отводится на соединительные кабели.

> ***Замечание***
>
> На практике длина патч-кордов обычно составляет 1 м и более. Обратите внимание, что не имеет смысла применять самодельные короткие патч-корды, например, для подключения сервера к патч-панели, если оба этих элемента расположены рядом ("фирменные" кабели не могут быть короче ~ 60 см). При малой длине кабеля увеличивается уровень помех, возникающих при отражении высокочастотных сигналов от точки соединения кабеля и розетки. Это может привести к увеличению числа ошибок в линии.

В реальных сетях еще сохранились концентраторы (*хабы*). Для локальной 10-мегабитной сети, построенной на *концентраторах*, существует правило "5/4" — между любыми двумя сетевыми устройствами должно быть не более пяти сегментов сети с четырьмя концентраторами. При этом размер сети, построенной на витой паре, ограничен величиной 500 м. Ограничение на длину обусловлено самой природой Ethernet, принципами, на которых строится такая сеть, и не зависит от совершенствования элементной базы.

Хотя в 100-мегабитной сети обычно используются только коммутаторы, на практике в ряде организаций эксплуатируются и концентраторы. Стандартом предусмотрено в этом случае наличие не более *двух* концентраторов с расстоянием между ними не более 5 м.

При необходимости соединения устройств, отстоящих друг от друга на расстояние свыше 100 м, целесообразны волоконно-оптические линии связи. На небольших расстояниях (порядка 100–300 м) применяются *многомодовые* оптические кабели. Длины сегментов определяются параметрами оптических приемников и передатчиков. (Эти значения отличаются от вендора к вендору и не всегда соответствуют параметрам стандартов.) Стоимость прокладки и эксплуатации такой линии практически соизмерима со стоимостью линии на витой паре. Для длинных соединений предназначен *одномодовый* оптический кабель. Соответствующее оборудование для одномодового кабеля (приемники и передатчики оптического сигнала) в несколько раз дороже, чем модели для многомодовой технологии.

Поскольку на практике эксплуатируются различные технологии, при проектировании расширения сети следует обращать внимание на совместимость использованных решений. Так, например, необходимо учитывать типы оптических разъемов, которые могут отличаться на оборудовании различных вендоров. Нужно принимать во внимание тип оптического кабеля (выпускаются более чем по пяти стандартам), длину волны и т. п.

Выбор типа коммутаторов

В небольших сетях (и в больших на уровне доступа) традиционно задействуют коммутаторы второго уровня по модели OSI. Коммутаторов данного класса обычно достаточно для организации сети с не очень большим числом компьютеров — в одну-две сотни. Точно назвать границу, когда необходимо уже применять коммутаторы третьего уровня, сложно. Это зависит от специфики организации (имеющихся сетевых сервисов, реальной загрузки сети, наличии трафика реального времени — IP-телефонии и видеоконференций и т. д.). Коммутаторы третьего уровня нужны для того, чтобы разделить сеть на несколько независимых друг от друга сегментов. При этом передача информа-

ции из одного сегмента в другой осуществляется путем маршрутизации на коммутаторе третьего уровня.

Примечание

Для обеспечения надежности необходимо строить сеть с ядром на двух коммутаторах третьего уровня, работающих совместно (как отказоустойчивый стек и т. п.).

Коммутаторы лучше приобретать управляемые. Это обеспечит гибкость в настройке сети. Если в сети предполагается использование сервисов реального времени, то коммутаторы должны поддерживать режимы управления качеством передачи (QoS) и, по возможности, реализовывать режим гарантированного предоставления полосы пропускания.

Топология сети передачи данных

На практике компьютерную сеть пытаются сначала строить по какому-нибудь проекту, а потом, по мере развития организации, подключают новые коммутаторы и структура принимает достаточно хаотичный вид. На рис. 1.1 показан пример топологии реальной сети, построенный бесплатной программой 3Com Network Supervisor. Если администратор не контролирует развитие сети, часто формируются каскады из четырех-пяти последовательно включенных коммутаторов, что неизбежно ухудшает качество системы передачи данных.

Администратору нельзя выпускать развитие сетей передачи данных из-под своего контроля: в любой момент он должен знать, как соединены между собой коммутаторы, и быть уверенным, что ни к одному порту не подключено неизвестное ему оборудование.

При построении сети внутри здания обычно придерживаются иерархии связей "здание – этаж – рабочее место": на этажах устанавливают коммутаторы уровня доступа, к которым подключают рабочие места пользователей, после чего эти коммутаторы соединяют каналами связи с коммутатором (*-ами*) на каком-либо этаже, который выполняет в этом случае роль *ядра* сети.

Традиционной проблемой большинства организаций является документирование своей кабельной подсистемы. Специализированные программные продукты, позволяющие поддерживать схемы сети и оперативно учитывать вносимые в нее изменения, стоят весьма дорого, а исходная документация быстро становится неактуальной после нескольких перемещений сотрудников и прокладки дополнительных каналов связи.

Существует много программ, которые позволяют автоматически воспроизвести структуру сети. Окно одной из таких программ — 3Com Network Supervisor — представлено на рис. 1.1. С помощью данных, собираемых про-

граммой, легко находить точки подключения компьютеров к коммутаторам, обнаруживать те или иные неисправности конкретной конфигурации.

> ***Совет***
>
> Найти и загрузить подобную программу из Интернета достаточно легко, если выполнить поиск по ключевым словам *network monitoring tool*.

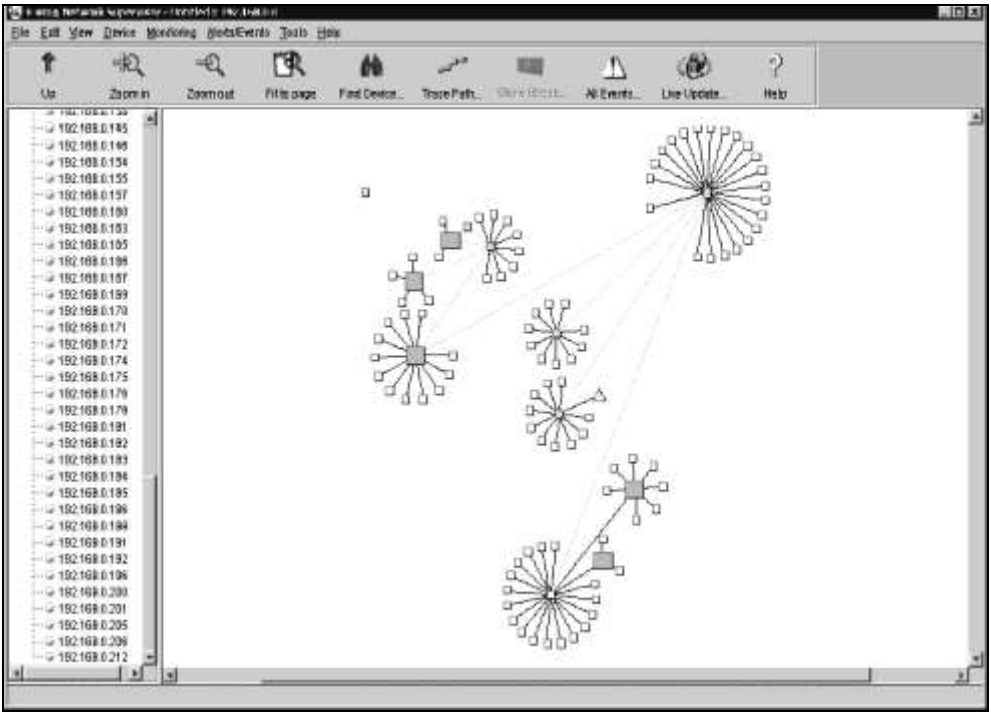


Рис. 1.1. Пример топологии реальной сети, построенной программой 3Com Network Supervisor

Естественно, что получаемая диаграмма тем точнее, чем более интеллектуальные активные устройства используются в сети. При эксплуатации неуправляемых устройств возможностей у администратора существенно меньше.

Ищем точку подключения компьютера

Точку подключения компьютера к порту коммутатора можно определить только в пределах текущего сегмента сети (одной VLAN). За пределами данного сегмента вам будет доступна информация только о том, в какой сети (за каким маршрутизатором) находится этот компьютер.

На практике в небольших организациях часто, несмотря на все рекомендации, отсутствует актуальная схема сети, поэтому поиск точки подключения устройства требует много усилий. Чтобы найти, к какому коммутатору подключен компьютер, следует искать устройство, в таблице MAC-адресов которого зарегистрирована сетевая плата соответствующего компьютера. Такая информация доступна только с управляемых коммутаторов.

> ***Замечание***
>
> Существуют программы, позволяющие найти маршрут подключения искомого устройства через все коммутаторы сети. Но они эксплуатируются преимущественно в крупных организациях с разветвленной сетью.

Последовательность действий такова. Сначала определите MAC-адрес устройства, точку подключения которого вы хотите найти. Это значение становится известным для локальной системы после того, как с ним происходили какие-либо сетевые операции. Быстрее всего выполнить команду `ping` на IP-адрес компьютера. После получения ответа посмотрите таблицу arp-кэша локальной системы, в ней должна содержаться запись об удаленном MAC-адресе (листинг 1.1).

Листинг 1.1

```
>arp -a
Интерфейс: 192.168.29.100 --- 0x4
  Адрес IP             Физический адрес      Тип
  192.168.29.1         00-1e-58-81-a0-89     динамический
```

MAC-адрес устройства отображен в столбце `Физический адрес`.

Точно такие же команды следует выполнить и на компьютерах Ubuntu, только вывод на экран результатов будет представлен немного по-иному. Хотя лучше вызвать команду `arp` без параметров (листинг 1.2).

Листинг 1.2

```
# arp
Address              HWtype   HWaddress           Flags Mask        Iface
192.168.32.120       ether    00:C0:9F:3F:D8:13   C                 eth0
192.168.177.85       ether    00:0D:28:F9:5D:80   C                 eth1
```

В этом листинге MAC-адрес устройства показан в столбце `HWaddress`.

После того как вы узнали MAC-адрес устройства, нужно найти его в таблице MAC-адресов на коммутаторе. Для этого необходимо подключиться к коммутатору одной из программ управления и выполнить поиск по этому значению (рис. 1.2).

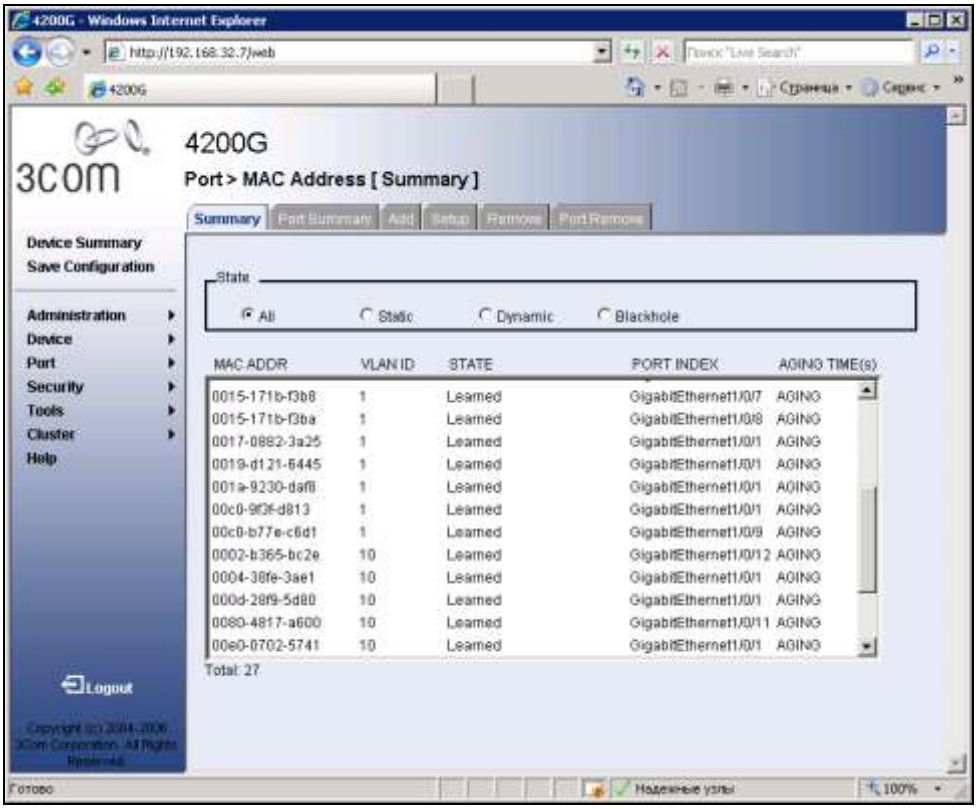


Рис. 1.2. Окно списка найденных на порту коммутатора MAC-адресов систем

На рис. 1.2 представлен графический интерфейс управления коммутатором 3Com4200G с отображением таблицы зарегистрированных MAC-адресов. Видно, что на некоторых портах имеются записи по нескольким MAC-адресам (например, на первом гигабитном порту). Это говорит о том, что данный порт является магистральным: через него коммутатор подключен к другому коммутатору и устройство нужно искать на удаленной системе.

Если на том порту коммутатора, на котором вы найдете зарегистрированным искомый MAC-адрес, есть еще MAC-адреса, значит, к данному порту подключен другой коммутатор. В этом случае нужно будет подключиться к сле-

дующему коммутатору и так по цепочке найти устройство, к которому подключена искомая система.

Контроль подключения к СКС

Администратор обычно не контролирует порты сети передачи данных постоянно. А если к вашей сети злоумышленник сможет подключить свой компьютер, то это существенно облегчит ему последующие операции по доступу к коммерческой информации организации.

Существует два метода контроля подключаемых устройств. Первый, который поддерживается всеми управляемыми коммутаторами, заключается в контроле MAC-адреса устройства на данном порту. После подключения к порту любого оборудования, коммутатор запоминает его MAC-адрес, и каждая последующая попытка другого компьютера (точнее, устройства с другим MAC-адресом) работать через этот порт приведет к блокировке порта. Эта функциональность имеет различные названия среди вендоров активного оборудования, чтобы ее задействовать, достаточно активировать соответствующую функцию для порта.

Недостатки такого решения состоят, во-первых, в том, что сегодня существует много программных способов смены MAC-адреса компьютера, например, достаточно указать значение соответствующей опции (параметра *Locally Administered Address*) в настройках сетевого адаптера в Windows (рис. 1.3).

Во-вторых, блокировка порта резко увеличивает нагрузку на администраторов, поскольку предполагает необходимость ручных операций для возобновления работы в случае замены оборудования и в других штатных ситуациях.

В настоящее время для контроля доступа к локальной сети наиболее распространены решения на основе протокола 802.1*x*. Упрощенно схему проверки оборудования с использованием данного протокола можно представить следующим образом (рис. 1.4):

- При подключении устройства порт коммутатора не пропускает никаких данных в локальную сеть, кроме специальных пакетов аутентификации на заданный в его настройках сервер RADIUS.
- Сервер Radius, получив от устройства необходимые аутентификационные данные, проверяет соответствие их неким параметрам. Обычно используются сертификаты безопасности, выданные контроллерами домена. В этом случае, информация проверяется во взаимодействии с сервером сертификатов и сервером службы каталогов.
- В зависимости от результатов проверки сервер RADIUS дает коммутатору разрешение на открытие порта.

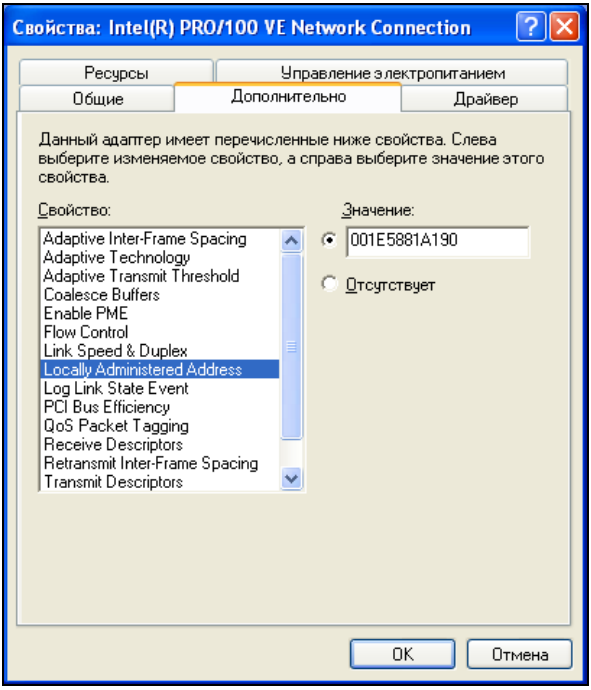


Рис. 1.3. Программная смена MAC-адреса компьютера

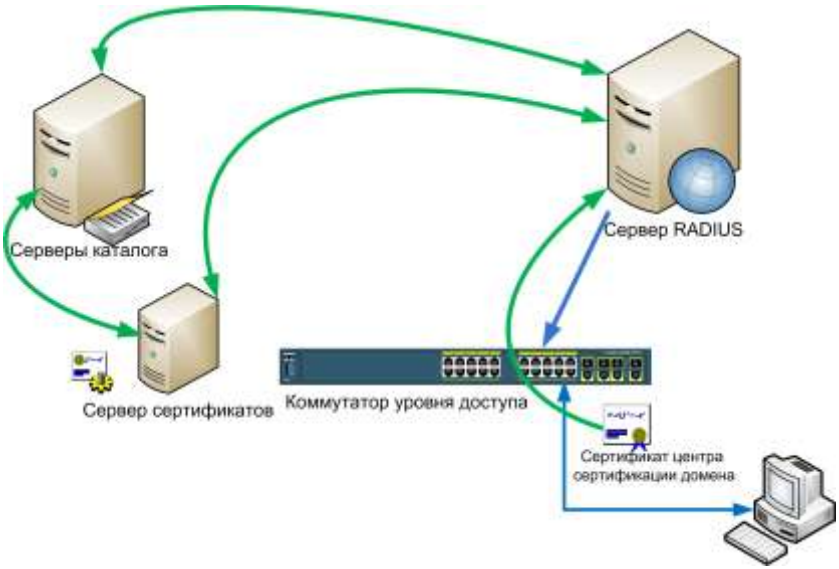


Рис. 1.4. Принципиальная схема взаимодействия компьютера, коммутатора и серверов системы при использовании протокола 802.1*x*

- Коммутатор, получив разрешение, открывает доступ устройству в локальную сеть. Далее, в зависимости от настроек коммутатора, такая проверка может осуществляться периодически через некоторое время, порт может открываться для любых MAC-адресов и т. д.

Сервер RADIUS может не только давать разрешение на открытие порта, но и сообщать коммутатору некоторые данные настройки, например, номер виртуальной сети, в которую должен быть помещен порт этого устройства. Данную функциональность поддерживают не все коммутаторы.

Самая строгая проверка компьютера будет осуществляться по протоколу 802.1*x* с учетом сертификатов, выданных удостоверяющим центром (например, внутренним центром сертификации). Опишем пример настройки коммутатора для такого случая.

Предварительные настройки для использования протокола 802.1*x*

Контроль подключения по протоколу 802.1.*x* с использованием сертификатов требует развернутой системы PKI в организации: установленного центра сертификации, наличие процедур выдачи/отзыва сертификатов и т. п. Обычно это реализуется только в достаточно крупных фирмах, тем более что, например, идентификация сервера RADIUS предполагает получение им самим сертификата, который может быть выдан только сервером сертификации на основе Windows Server Enterprise Edition.

Поэтому в малых организациях можно ограничиться аутентификацией по MD5-откликам. Процедура настройки практически не отличается от описанной далее, за исключением того, что вместо сертификатов нужно выбрать опцию **MD5-отклик** в мастере настройки политик подключения.

Настройка компьютера. Аутентификация на базе протокола 802.1*x* осуществляется службой *Беспроводная настройка*. По умолчанию ее запуск на рабочих станциях установлен в режим *ручной*. Смените ее на автоматический режим. Далее, с помощью сертификатов можно аутентифицировать как *компьютер,* так и *пользователя*. По умолчанию операционная система Windows аутентифицирует пользователя. То есть до локального входа пользователя на компьютер, работа в сети будет невозможна. Если вы хотите аутентифицировать компьютер, то необходимо в его реестр с помощью команды `regedit` добавить параметр HKLM\Software\Microsoft\EAPOL\Parameters\General\Global\AuthMode со значением 2 и типом DWORD.

> ***Замечание***
>
> Эти настройки можно определить централизованно с использованием групповой политики домена.

Настройка домена Windows. Учетные записи, которые будут аутентифицироваться по протоколу 802.1*x*, должны иметь разрешение на входящий звонок в свойствах учетной записи. Обратите внимание, что это касается и учетных записей *компьютеров*, если вы предполагаете авторизовать их сертификаты. Если вы планируете назначать компьютеры в отдельные VLAN в зависимости от членства в группах безопасности, то в этом случае необходимо создать столько групп безопасности, сколько различных настроек должно передаваться на коммутатор, и включить в эти группы соответствующие учетные записи. Для упрощения администрирования желательно создать групповую политику, предполагающую автоматическую выдачу сертификатов для компьютеров, входящих в домен. Это устранит операции ручного получения сертификатов для учетных записей компьютеров.

Настройка сервера RADIUS. Серверы RADIUS в операционных системах Microsoft носят название *Служба проверки подлинности в Интернете* (входит в состав *Сетевые службы* при выборе опции установки компонентов Windows). Для единообразия в этой книге мы будем называть эту службу как сервер RADIUS. Установите RADIUS-сервер на какой-либо системе Windows и зарегистрируйте его в службе каталогов (операция входит в меню свойств сервера IAS). Проверьте, что компьютер с сервером RADIUS включен в состав группы безопасности RAS and IAS Servers. Установите на сервер сертификат авторизации, предназначенный для серверов RAS и IAS (при ручном запросе сертификата необходимо выбрать соответствующий шаблон в мастере операций).

> ***ЗАМЕЧАНИЕ***
>
> В Windows 2008 сервер RADIUS включен в состав службы контроля доступа к сети (Network Access Protection, NAP). Для его установки достаточно добавить роль *Службы политики сети и доступа* в **Диспетчере сервера**. Сама настройка протокола 802.1*x* для доступа в локальную сеть принципиально не отличается от описанного далее примера для случая Windows 2003 Server.

Добавьте в качестве клиентов сервера RADIUS каждый коммутатор, на котором будет осуществляться авторизация на основе протокола 802.1*x*. При этой операции необходимо указать адрес коммутатора и пароль, который потребуется при связи с ним. Желательно указывать достаточно длинный пароль, не менее 23 символов, как рекомендуют разработчики. Для ключей целесообразно задать различные значения для каждого коммутатора.

Настройка политики доступа на основе протокола 802.1*x*

После предварительных настроек можно приступить непосредственно к созданию правил доступа в локальную сеть на основе протокола 802.1*x*. Эти настройки носят названия *политик RADIUS-сервера*.

Замечание

Обычно в RADIUS-сервере присутствует несколько политик, например, политика по назначению клиента в VLAN1, политика по назначению клиента в VLAN2 и т. д. В этом случае при попытке подключения клиента сервер будет последовательно проверять соответствие параметров клиента значениям политик до первого совпадения, после чего выполнит подключение в соответствии с определенными в ней значениями.

Создавать новую политику желательно с помощью мастера операций. На первом шаге вы определяете название политики, оно может быть любым. На втором — необходимо выбрать тип *Доступ по Ethernet* (рис. 1.5). Следующим шагом следует указать группы безопасности, в которые должен входить подключающийся клиент: достаточно просто добавить их названия с помощью соответствующей кнопки.

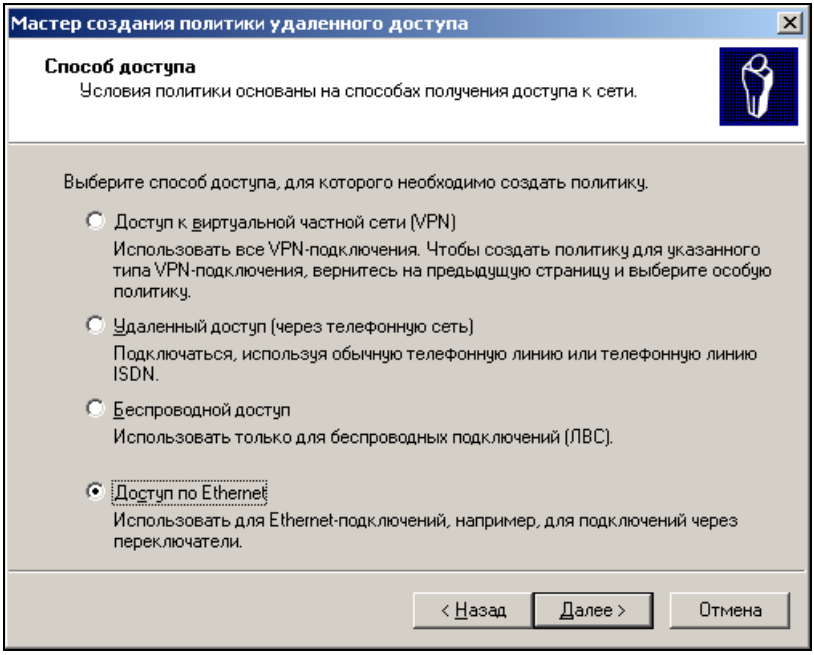


Рис. 1.5. Выбор способа доступа клиентов при создании политики сервера RADIUS

После выбора групп на следующем шаге работы мастера нужно определить тип аутентификации. Предлагаемое мастером операций значение необходимо сменить на Smart card or other certificate. При этом мастер подставит в качестве параметров центра сертификации данные своего сертификата, полученного от доменного центра сертификации.

В результате этих шагов мы получили политику, открывающую порт для компьютера, входящего в указанную группу безопасности домена. Но можно назначить и дополнительные параметры в политике доступа, которые позволят нам автоматически назначить порту подключения определенный номер VLAN.

> ***Замечание***
>
> Реализация данной возможности зависит от модели коммутатора. Некоторые модели позволяют только открывать порт, некоторые — назначать при этом номер VLAN, другие — кроме номера VLAN для успешно открытого порта могут иметь настройки, предусматривающие подключение порта в случае неудачной аутентификации к другой VLAN.

Для настройки дополнительных параметров, откройте соответствующую политику доступа и нажмите клавишу **Изменить профиль**.

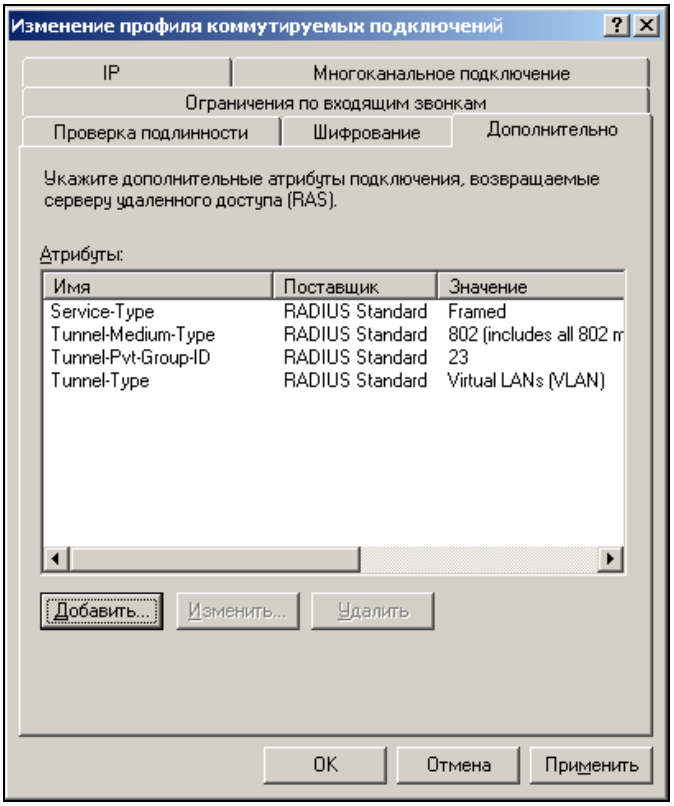


Рис. 1.6. Окно настройки дополнительных атрибутов подключения для сервера RADIUS

Для того чтобы RADIUS правильно сообщил коммутатору параметры VLAN, нужно добавить три атрибута (на вкладке **Дополнительно**):

- Tunnel-Medium-Type со значением 802 (includes all 802 media plus Ethernet canonical format);
- Tunnel-Pvt-Group-ID со значением номера VLAN, в которую должен быть помещен порт при удачной аутентификации;
- Tunnel-Type со значением Virtual LANs.

Для этого необходимо трижды выбрать операцию **Добавить**, указать в списке желаемый атрибут и настроить его значение. В результате вы должны увидеть приблизительно такие же параметры, как и на рис. 1.6 (атрибут Tunnel-Pvt-Group-ID определяет номер VLAN, в которую будет помещен порт коммутатора при прохождении проверки).

Настройка коммутатора для работы с протоколом 802.1*x*

В качестве примера мы рассмотрим настройку коммутатора Cisco. Команды будут отличаться для оборудования других вендоров, но правильно написать их не составит труда при понимании необходимых шагов.

> ***Замечание***
>
> Коммутаторы Cisco позволяют определить VLAN, в которую будут помещены порты в случае неудачной аутентификации (auth-fail vlan) или если клиент не поддерживает 802.1*x* (guest vlan).

Сначала в конфигурации коммутатора необходимо указать создание новой модели аутентификации с использованием сервера RADIUS (мы предполагаем, что консоль управления коммутатором открыта с необходимыми правами для выполнения описываемых операций) (листинг 1.3).

Листинг 1.3

```
aaa new-model
aaa authentication login default group radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
```

Далее, необходимо включить режим использования протокола 802.1*x* и определить параметры RADIUS-сервера (его адрес и ключ аутентификации):

```
dot1x system-auth-control
radius-server host <IP-адрес> key xxxxxxxxxxxx
```

(В этой строке следует указать тот ключ, который определен в установках сервера RADIUS для данного коммутатора.)

Теперь нужно настроить протокол 802.1*x* для каждого порта коммутатора. В листинге 1.4 мы приводим команды, настраивающие порт с номером 11.

Листинг 1.4

```
interface GigabitEthernet0/11
switchport mode access
dot1x port-control auto
dot1x guest-vlan номер
dot1x auth-fail vlan номер
```

На этом настройка в системе протокола 802.1*x* завершена, и вы можете проверить ее работу, подключая к порту коммутатора компьютер.

В случае каких-либо проблем, можно включить протоколирование работы RADIUS-сервера и исследовать причины возникающих неполадок на основе полученной информации.

Обеспечение отказоустойчивой работы сетевой инфраструктуры

Необходимое условие надежной работы информационной системы — безотказное функционирование каналов связи. Данная задача решается путем *дублирования* как собственно каналов связи, так и активного оборудования (коммутаторов).

Отказоустойчивая топология сети передачи данных

Для обеспечения отказоустойчивости сети передачи данных необходимо наличие резервных линий, причем пути их прокладки не должны совпадать с основными кабелями (чтобы случайное повреждение группы кабелей, например, в результате земляных работ, не привело к разрыву как основного, так и дублирующего кабеля). Понятно, что на практике отказоустойчивая конфигурация сети создается только в тех случаях, когда простои в работе информационной системы недопустимы и могут привести к существенным экономическим потерям.

Простое соединение двух коммутаторов двумя кабелями создаст кольцо, которое недопустимо в сети Ethernet. Результатом станет широковещательный шторм и практическая неработоспособность сегмента сети. Поэтому созда-

ние отказоустойчивых решений требует первоначальной настройки активного оборудования.

> ***Замечание***
>
> В коммутаторах, предназначенных для работы на уровне доступа, обычно по умолчанию включены протоколы, которые "разорвут" такое кольцо. Коммутаторы уровня ядра не имеют таких настроек, поэтому возникновение кольца быстро приведет к падению сегмента сети.

Существует два варианта построения сети, в которой присутствуют резервирующие каналы связи. Первый использует протоколы, работающие на втором уровне модели OSI. Второй основан на протоколах маршрутизации (третий уровень модели OSI).

Построение отказоустойчивой сети на основе протоколов второго уровня

Отказоустойчивая конфигурация на протоколах второго уровня обеспечивает самое быстрое восстановление в случае аварии. Сеть может восстановиться за 1–3 с или даже еще быстрее в случае проприетарных протоколов.

Использование протоколов остовного дерева

Протоколы остовного дерева — Spanning Tree Protocol (STP, стандарт 802.1d) и Rapid Spanning Tree (RSTP, стандарт 802.1w) — служат для автоматического построения связей сетевой структуры. Коммутаторы пытаются по определенным алгоритмам вычислить оптимальные маршруты между всеми устройствами и автоматически блокируют (отключают) порты при обнаружении петель. Для определения маршрутов и контроля соединений по специальным алгоритмам постоянно рассылаются служебные пакеты (BPDU — Bridge Protocol Data Units). В случае изменения структуры сети производится ее переконфигурирование. Этот процесс занимает от 30 секунд до нескольких минут в зависимости от размера сети для протокола STP. При использовании RSTP (усовершенствованной версии STP) время перестройки уменьшается до нескольких секунд.

Протоколы могут обеспечить связность сети без каких-либо ручных настроек. Для построения структуры алгоритмы учитывают скорость соединения и количество коммутаторов между точками. Администратору нужно только включить на портах данные протоколы (часто это настройка по умолчанию для коммутаторов уровня доступа). На основании анализа рассылки пакетов BPDU коммутатор определяет существующие связи и автоматически отключает порты, к которым подключены вторые, резервные каналы.

Для оптимизации дерева связей целесообразно *вручную* назначить приоритеты коммутаторам: устройство в центре сети должно иметь самый малый "вес" (Bridge ID или Bridge Priority), чем дальше от логического центра, тем большие веса нужно назначать коммутаторам. Кроме того, в случае применения протокола RSTP желательно настроить опцию быстрого старта порта (Fast Start) для тех портов, к которым подключены конечные устройства. Это исключит такие порты из процедуры определения маршрутов и ускорит сходимость.

> ***Замечание***
>
> Алгоритм выбора приоритета коммутатора основан на MAC-адресе устройства. Поэтому более *старое* устройство, как имеющее меньший номер MAC, получит приоритет в процедуре выбора корневого коммутатора. На практике обычно происходит с точностью "до наоборот". В центр сети размещают самое новое устройство, как самое производительное.

Протоколы STP/RSTP поддерживаются всеми современными коммутаторами. Однако их серьезный недостаток — *отключение* резервных связей. Резервные связи не задействуются для передачи данных и включаются только при повреждении основного канала.

> ***Примечание***
>
> Поддержку протокола RSTP (STP) следует включать и не только при наличии избыточных каналов связи. Включение этой функции позволит сохранить функционирование сети в случае случайного или умышленного создания петель, которые без данных протоколов приведут к широковещательному шторму и практическому прекращению функционирования сегмента. Для создания петли достаточно воткнуть один патч-корд в два порта коммутатора (например, пользователь увидел свободный конец патч-корда, не проверил, что другой конец его включен в розетку, и подключил разъем в соседнюю свободную розетку). Обычно протоколы STP/RSTP включаются по умолчанию на коммутаторах уровня доступа.

Использование стандарта MSTP

Стандарт MSTP (Multi Spanning Tree Protocol, описан в 802.1s) является расширением стандарта RSTP на сеть с VLAN (точнее, протокол RSTP стал частью протокола MSTP).

В отличие от RSTP, MSTP для каждой виртуальной сети строит свое дерево связей. Поэтому предупреждение петель происходит не путем отключения порта коммутатора, а через отключение передачи данных *только* для определенной VLAN. Иными словами, можно настроить MSTP так, чтобы для части VLAN было заблокировано одно соединение из дублированных линков, а для других VLAN — второе. Для этого в настройках протокола администратору

вручную нужно назначить каналам различные веса: в одном случае основным будет первый канал, а второй — резервным. Во втором — наоборот. Таким образом, все соединения будут передавать данные. При повреждении канала связи MSTP обнаружит это событие и автоматически перестроит структуру.

Таким образом, MSTP позволяет осуществить ***балансировку трафика*** по основному и резервному каналам связи.

Главный недостаток решения на протоколе MSTP заключается в сложности настройки такой структуры. Администратор должен четко представлять разбиение системы на VLAN, оценить потоки данных в каждом сегменте и путем ручной настройки добиться примерно равномерной загрузки всех каналов связи.

Также следует учитывать, что во многих моделях коммутаторов (особенно бюджетного ряда) поддержка протокола MSTP не реализована.

Построение отказоустойчивой сети на основе протоколов третьего уровня

Основной практический вариант создания отказоустойчивой конфигурации сети на сегодня — решения, основанные на применении протоколов автоматической маршрутизации. Хотя протоколы маршрутизации имеют несколько худшие показатели времени перестроения сети (например, OSPF может перестроить сеть приблизительно за 3 с), однако трудоемкость настройки структуры сети существенно ниже, чем при использовании, например, протокола второго уровня MSTP.

С точки зрения протоколов маршрутизации сеть с резервными каналами связи представляет собой отдельные подсети с несколькими возможными путями передачи данных из одной подсети в другую. В большинстве случаев администратору достаточно только включить протоколы автоматической маршрутизации, чтобы сеть "заработала". Причем переключение на другие пути передачи данных в случае повреждения каналов связи будет происходить за счет изменения таблиц маршрутизации.

VRRP

При маршрутизации между несколькими VLAN в качестве шлюза по умолчанию для рабочих станций назначен адрес интерфейса коммутатора. Это является узким местом такого решения, поскольку при выходе из строя коммутатора со шлюзом компьютеры потеряют связь с другими сетями.

Для предупреждения подобных ситуаций необходимо задействовать протокол VRRP (Virtual Routing Redundancy Protocol), который позволяет настроить

два коммутатора как *один* шлюз. Естественно, что от клиента в таком случае необходимо иметь две линии подключения. Поэтому такой вариант обычно применяется для резервированного подключения коммутаторов уровня доступа к коммутаторам распределения или ядра сети.

Примечание

Этот протокол реализован далеко не на всех моделях коммутаторов. Как правило, модели, приобретаемые в малых организациях, не имеют поддержки данного протокола VRRP.

Идея создания отказоустойчивого шлюза на базе протокола VRRP состоит в следующем. В сети устанавливают два коммутатора с поддержкой данного протокола. На каждом из них настраивают сетевые интерфейсы и включают протокол VRRP. После чего настраивают интерфейс с одним и тем же IP-адресом на *обоих* коммутаторах, причем один коммутатор определяется главным, а второй — ведомым. В нормальных условиях работы коммутаторы постоянно обмениваются между собой служебной информацией. Если оба они нормально работают, то по настроенному адресу шлюза "отвечает" только главный коммутатор. Если он выходит из строя, то второй коммутатор начинает принимать данные по адресу шлюза и передавать их в другие сети в соответствии с настройками.

Таким образом обеспечивается отказоустойчивая работа шлюза независимо от состояния отдельного коммутатора или целостности связей.

Протокол VRRP является стандартом. В то же время существуют отдельные модификации его реализации на коммутаторах различных вендоров. Так, из описанного принципа работы VRRP следует, что в "нормальных условиях" передачу данных в другую сеть обеспечивает только главный коммутатор. Хотя физические связи — в целях отказоустойчивости — имеют оба устройства. Поэтому, например, в коммутаторах Nortel реализовано расширение функциональности протокола VRRP. Оба коммутатора будут работать в качестве шлюза и передавать данные в другие сети. Только при выходе из строя одного из них, трафик будет перенаправлен в другой коммутатор. Этим достигается балансировка нагрузки на различные каналы связи и увеличение пропускной способности сети.

Замечание

Мы не будем останавливаться подробно на реализации такой технологии. При ее реализации к одному IP-адресу шлюза привязываются два MAC-адреса: один для клиентов первого коммутатора, другой — для второго. В результате пакеты, переданные на один шлюз (один IP-адрес), достигают различных устройств.

Время восстановления структуры сети

Добиться малого времени восстановления передачи данных после единичной аварии очень сложно. На основе использования открытых стандартов реально достичь восстановления обслуживания за период не более 3–5 с.

Проприетарные технологии принципиально способны несколько уменьшить данный период (до величин, менее одной секунды). Однако следует крайне осторожно подходить к подобным прогнозам. Очень часто даже крупные вендоры в маркетинговых целях презентуют крайне низкие значения периода восстановления (например, 20 мс), не особо привлекая внимания к тем условиям, при которых получен такой показатель. Если отказ внутри шассийного коммутатора может быть устранен за данное время, то на восстановление после другой неисправности требуется несколько секунд, и сеть в целом будет характеризоваться именно наихудшим показателем.

Что можно посоветовать администраторам? В первую очередь, больше проверять, чем доверять маркетинговым предложениям. Изучать базовые документы по существующим технологиям, читать технические описания оборудования, обращая внимания на любые оговариваемые особенности. Во-вторых, стараться быть в курсе тестов, проводимых независимыми лабораториями, например, Tolly Group (**http://www.tolly.com/**). Хотя и учитывать условия проведения теста.

В-третьих, просчитывать параметры именно для вариантов конфигурации вашей сети. Каждая конфигурация индивидуальна. И не факт, что лучшее решение для идеальной лаборатории окажется таковым в реальной ситуации.

Увеличение пропускной способности линий связи

Стандарт 802.3ad описывает агрегированные каналы, которые позволяют объединять несколько линий связи между коммутаторами в один общий канал передачи данных. Соответственно, агрегированный канал имеет пропускную способность, равную сумме пропускных способностей объединенных каналов. При передаче данных задействованы оба канала, причем в случае отказа одного из соединений все данные начинают передаваться через оставшийся канал. Агрегированный канал может настраиваться как вручную (явным указанием объединяемых портов), так и автоматически на основе специального протокола LACP — Link Aggregation Control Protocol. Соответствующие настройки выполняются в программе конфигурирования коммутаторов.

ЗАМЕЧАНИЕ

Данные по отдельным каналам распределяются на основе подсчета хэш-функции от MAC-адресов источника и назначения. В результате каналы загружаются примерно равномерно, но передача данных между компьютером А и компьютером Б *всегда* происходит только по одному каналу. Поэтому макси-

мальная скорость передачи данных между двумя устройствами всегда определяется только *одним* каналом передачи данных. Увеличение пропускной способности происходит в целом среднестатистически. Повысить пропускную способность между двумя системами таким способом невозможно: данные всегда пойдут только по одному из агрегированных каналов.

К сожалению, стандарт не описывает многоточечное подключение, т. е. соединение должно быть осуществлено *только* между двумя устройствами.

На практике многие вендоры создали решения, позволяющие "обойти" данное ограничение. Были разработаны технологии, в которых агрегированный канал создается из двух и более линков, соединяющих *различные* коммутаторы, объединенные в один стек. При этом настройка такой системы выполняется аналогично созданию агрегированного канала в пределах одного коммутатора.

Подобные решения требуют специальной организации стека коммутаторов, существуют у различных вендоров (3Com, Nortel, Cisco и т. п.), но могут в каждом случае иметь уникальные названия. При этом конкретные реализации могут быть совместимы между оборудованием различных вендоров (например, MLT от Nortel идентичен технологии EtherChannel от Cisco и т. п.). Самым главным для администраторов сетей является тот факт, что два канала подключения от любого его устройства к различным коммутаторам можно объединить в один агрегированный канал на основе открытого стандарта — 802.3ad. Как будто подключение осуществляется к одному коммутатору. Например, так можно осуществить отказоустойчивое подключение сервера к ферме коммутаторов, достаточно, чтобы программное обеспечение было настроено на поддержку протокола 802.13d.

Для того чтобы такое решение было полностью отказоустойчивым, коммутаторы должны быть объединены в *отказоустойчивый* стек. При создании отказоустойчивого стека все коммутаторы объединяются в кольцо, последний коммутатор объединяется возвратным стековым кабелем с первым коммутатором. В результате отказ любого устройства стека сохранит возможность передачи данных на верхний уровень сети. Такая конфигурация стека возможна не во всех моделях оборудования, поэтому выбор моделей коммутаторов должен учитывать требования к системе передачи данных и позволять создать необходимые конфигурации.

Настройка протокола IP

Сетевой протокол — это набор программно реализованных правил общения компьютеров в сети. Практически, это "язык", на котором компьютеры разговаривают друг с другом. В настоящее время стандартом стало использование *только* протокола TCP/IP. В отличие от других протоколов TCP/IP требует ряда предварительных настроек.

Протоколы UPD, TCP, ICMP

Для передачи данных служат протоколы TCP (Transmission Control Protocol, протокол управления передачей данных) и UDP (User Datagram Protocol, протокол пользовательских дейтаграмм). UDP применяется в тех случаях, когда не требуется подтверждения приема (например, DNS-запросы, IP-телефония). Передача данных по протоколу TCP предусматривает наличие подтверждений получения информации. Если передающая сторона не получит в установленные сроки необходимого подтверждения, то данные будут переданы повторно. Поэтому протокол TCP относят к протоколам, предусматривающим соединение (connection oriented), а UDP — нет (connection less).

Протокол Internet Control Message Protocol (ICMP, протокол управляющих сообщений Интернета) предназначен для передачи данных о параметрах сети. Он включает такие типы пакетов, как ping, destination unreachable, TTL exceeded и т. д.

IPv6

Бурное развитие Интернета привело к тому, что параметры, первоначально заложенные при создании протоколов IP, стали сдерживать дальнейшее развитие глобальной сети. Прежде всего, это банальная нехватка адресов для выделения компьютерам. Решить многие такие проблемы призван протокол IP версии 6.

Поддержка протокола IPv6 заложена в операционные системы Windows, начиная с Windows XP. Чтобы ее включить в Windows XP, необходимо выполнить команду `ipv6 install`. В операционных системах Vista, Windows 7 и Ubuntu протокол IPv6 включен по умолчанию, хотя в подавляющем большинстве локальных сетей он не используется.

> ***Примечание***
>
> Поэтому в целях предупреждения использования возможных уязвимостей этого протокола для атак на компьютеры целесообразно его отключить.

Параметры TCP/IP-протокола

Для работы с протоколом TCP/IP клиенту необходим ряд параметров. Прежде всего, это IP-адрес, маска и шлюз.

IP-адрес

Каждый компьютер, работающий по протоколу TCP/IP, обязательно имеет *IP-адрес* — 32-битовое число, предназначенное для идентификации узла

(компьютера) в сети. Адрес принято записывать десятичными значениями каждого октета этого числа с разделением полученных значений точками, например: 192.168.101.36.

IP-адреса в сети Интернет уникальны. Это значит, что каждый компьютер имеет свое сочетание цифр, и в сети не может быть двух компьютеров с одинаковыми адресами.

Для построения *локальных сетей* организаций выделены специальные диапазоны адресов: 10.*x.x.x*, 192.168.*x.x*, 10.*x.x.x*, с 172.16.*x.x* по 172.31.*x.x*, 169.254.*x.x* (под *x* подразумевается любое число от 0 до 254). Пакеты, передаваемые с указанных адресов, *не маршрутизируются* (иными словами, не пересылаются) в Интернете. Поэтому в различных локальных сетях компьютеры могут иметь совпадающие адреса из указанных диапазонов. Для пересылки информации с таких компьютеров в Интернет и обратно предусмотрены специальные программы, "на лету" заменяющие локальные адреса реальными при работе с Интернетом. Иными словами, данные в Сеть пересылаются от реального IP-адреса. Этот процесс происходит "незаметно" для пользователя. Такая технология называется *трансляцией адресов* (см. *главу 6*).

Групповые адреса

Если данные должны быть переданы на несколько устройств (например, просмотр видео с одной Web-камеры на различных компьютерах или одновременное разворачивание образа операционной системы на несколько систем), то уменьшить нагрузку на сеть можно с помощью *групповых рассылок*.

Для этого соответствующая программа динамически присваивает компьютеру еще один IP-адрес из специального диапазона: с 224.0.0.0 по 239.255.255.255. Причем диапазоны 224.0.0.0–224.0.0.255 и 239.0.0.0–239.255.255.255 не могут быть задействованы в приложениях и предназначены для протоколов маршрутизации (например, адрес 224.0.0.1 принадлежит всем системам сегмента сети; адрес 224.0.0.2 — всем маршрутизаторам сегмента и т. д.). Адреса групповой рассылки назначает соответствующее программное обеспечение.

Если коммутатор имеет функции работы с групповыми рассылками (поддержка IGMP snoophing, PIM DM/PIM SM), то передаваемые на адреса групповой рассылки данные будут рассылаться только на те порты, к которым подключены устройства, подписавшиеся на соответствующие рассылки. В результате сетевой трафик можно существенно снизить по сравнению с вариантом передачи таких данных независимо каждому устройству сети.

Распределение IP-адресов сети малого офиса

В сетях предприятий обычно задействованы диапазоны IP-адресов, выделенные для локального использования. Часть адресов закрепляется статически, часть — раздается динамически с помощью DHCP (Dynamic Host Configuration Protocol, динамический протокол конфигурации сервера).

Статические адреса закрепляются:

- За шлюзом, которому обычно назначают адрес xxx.xxx.xxx.1, но это традиция, а не правило.
- За серверами DNS, DHCP, WINS.
- За контроллерами домена; серверами (например, централизованные файловые ресурсы, почтовый сервер и т. п.).
- За станциями печати, имеющими непосредственное подключение к сети.
- За управляемыми сетевыми устройствами (например, сетевыми переключателями, SNMP-управляемыми источниками аварийного питания и т. п.).

Рабочие станции традиционно имеют *динамические адреса*. При этом часть динамических адресов выдается для локального использования, а часть предназначается для внешних клиентов, "гостей" сети.

Для упрощения администрирования сети рекомендуется выработать план распределения диапазона адресов и предусмотреть в нем некоторый запас для будущего развития информационной системы.

Маска адреса

Чтобы можно было выделить часть IP-адресов одной организации, часть другой и т. д., введено понятие *подсети*. Подсеть представляет собой диапазон IP-адресов, которые считаются принадлежащими одной локальной сети. При работе в локальной сети информация пересылается непосредственно получателю. Если данные предназначены компьютеру с IP-адресом, не принадлежащим локальной сети, то они пересылаются на другие компьютеры в соответствии с *таблицей маршрутизации*. Поэтому при использовании протокола TCP/IP важно знать, к какой сети принадлежит получатель информации: к локальной или удаленной.

Маска — это параметр, который "сообщает" программному обеспечению о том, сколько компьютеров объединено в данную группу ("подсеть"). Маска адреса имеет такую же структуру, как и сам IP-адрес: это набор из четырех групп чисел, каждое из которых может быть в диапазоне от 0 до 255. Чем меньше значение маски, тем больше компьютеров объединено в данную подсеть. Для сетей небольших предприятий маска обычно имеет вид 255.255.255.*x*

(например, 255.255.255.224). Маска сети присваивается компьютеру одновременно с IP-адресом.

Так, сеть 192.168.0.0 с маской 255.255.255.0 (иначе можно записать 192.168.0.0/24) может содержать хосты с адресами от 192.168.0.1 до 192.168.0.254.

> ***Замечание***
>
> Здесь число 24 соответствует длине маски, используемой для адресации подсетей. Если записать маску 255.255.255.0 в двоичном виде, то получится последовательность из 24 единиц и 8 нулей. Маска 255.255.255.128 будет представлять собой последовательность из 25 единиц и 7 нулей. Поэтому ее записывают также в виде /25 и т. д.

Адрес 192.168.0.255 — это адрес широковещательной рассылки для данной сети.
А сеть 192.168.0.0 с маской 255.255.255.128 (192.168.0.0/25) допускает адреса от 192.168.0.1 до 192.168.0.127 (адрес 192.168.0.128 служит при этом в качестве широковещательного).

Хотя многие сертификационные экзамены содержат вопросы, так или иначе связанные с разбиением на подсети (правильный подсчет маски сети, числа адресов и т. п.), на практике проводить ручной подсчет вряд ли придется. Существует много онлайновых ресурсов, которые предлагают различные варианты калькуляторов сетевых адресов (Network Calculator), например **http://www.globalstrata.com/services/network/bscnetcalc.asp**.

Тем не менее, при необходимости, определить диапазон адресов сети, в которую входит данный IP-адрес, можно очень простым способом. Запишите маску адреса не в восьмеричном, а в двоичном виде. Так, если последний октет маски равен 240, то это соответствует в двоичной записи 11110000. Первая единица справа будет соответствовать количеству адресов в подсети, в данном случае это 16. Теперь отсчитывайте от начального адреса сети (он всегда равен 0) по этому количеству адресов, пока не дойдете до диапазона, который включает ваш адрес. Например, если нужно узнать, к какому диапазону принадлежит адрес 10.10.10.50 с маской 255.255.255.240, то последовательно добавляя по 16 адресов к адресу 10.10.10.0, мы дойдем до диапазона 10.10.10.49–10.10.10.64, внутри которого находится наш адрес.

На практике сети с небольшим возможным числом хостов применяются интернет-провайдерами (с целью экономии IP-адресов). Например, клиенту может быть назначен адрес с маской 255.255.255.252. Такая подсеть содержит только два хоста. При разбиении сети организации используют диапазоны локальных адресов сетей класса C. Сеть класса C имеет маску адреса 255.255.255.0 и может содержать до 254 хостов. Выбор сетей класса C при

разбиении на VLAN в условиях предприятия связан с тем, что протоколы автоматической маршрутизации предназначены именно для таких подсетей.

При создании подсетей в организации рекомендуется придерживаться правила, что подсети, относящиеся к определенному узлу распределения, должны входить в одну сеть. Это упрощает таблицы маршрутизации и экономит ресурсы коммутаторов. Например, если к данному коммутатору подключены подсети 192.168.0.0/255.255.255.0, 192.168.1.0/255.255.255.0, 192.168.3.0/255.255.255.0, то другому коммутатору достаточно знать, что в этом направлении следует пересылать пакеты для сети 192.168.0.0/255.255.252.0.

Шлюз (Gateway, default gateway)

После того как компьютер получил IP-адрес и ему стало "известно" значение маски подсети, программа может начать работу в данной локальной подсети. Чтобы обмениваться информацией с другими компьютерами в сети, необходимо знать правила, куда пересылать информацию за пределы локальной сети. Для этого служит такая характеристика IP-протокола, как адрес шлюза.

Шлюз (gateway) — это устройство (компьютер), которое обеспечивает пересылку информации между различными IP-подсетями. Если программа определяет (по IP-адресу и маске), что адрес назначения *не входит* в состав локальной подсети, то она отправляет эти данные на устройство, выполняющее функции шлюза. В настройках протокола указывают IP-адрес такого устройства.

Для работы *только* в локальной сети шлюз может не назначаться. Если доступ в Интернет осуществляется через прокси-сервер, то компьютерам локальной сети также может не назначаться адрес шлюза (т. к. они взаимодействуют только с прокси-сервером, который находится внутри локальной сети).

Для индивидуальных пользователей, подключающихся к Интернету, или для небольших предприятий, имеющих единственный канал подключения, в системе назначается только один адрес шлюза — адрес того устройства, которое имеет подключение к Сети. При наличии нескольких маршрутов (путей пересылки данных в другие сети) будет существовать несколько шлюзов. В этом случае для определения пути передачи данных потребуется *таблица маршрутизации*.

Таблицы маршрутизации

Организация может иметь несколько точек подключения к Интернету (например, с целью резервирования или уменьшения стоимости каналов передачи данных и т. п.), а также содержать в своей структуре несколько IP-сетей. В этом случае, чтобы система "знала", каким путем (через какой шлюз)

посылать ту или иную информацию, создают *таблицы маршрутизации* (routing), где для каждого шлюза указывают те подсети Интернета, для которых через этот шлюз должна передаваться информация. При этом для нескольких шлюзов можно задать одинаковые диапазоны назначения, но с разной стоимостью передачи данных: информация будет отсылаться по каналу, имеющему самую низкую стоимость, а при его выходе из строя автоматически будет использоваться следующее наиболее "дешевое" подсоединение.

Таблицы маршрутизации имеются на каждом устройстве, работающем по протоколу IP. Администраторы в основном имеют дело с таблицами маршрутизации коммутирующего оборудования. Настройка таблиц маршрутизации компьютеров целесообразна только при наличии нескольких сетевых адаптеров, подключенных к различным сегментам сети. Если у компьютера есть лишь одна сетевая карта (одно подключение к Интернету), таблица маршрутизации имеет наиболее простой вид: в ней записано, что все сигналы должны отправляться на шлюз, назначенный *по умолчанию* (default gateway).

Другой пример — при создании VPN-подключений к компьютеру добавляется сетевой интерфейс. В этом случае с помощью таблиц маршрутизации также можно регулировать (перераспределять) трафик через VLAN и сетевую карту компьютера.

Посмотреть таблицу маршрутизации протокола TCP/IP в Windows можно по команде `route print`, а в Ubuntu — `route` или `netstat -r`. Команда `route` позволяет также добавить новый статический маршрут (`route add`). Чтобы этот маршрут сохранился после перезагрузки компьютера, в Windows команду необходимо выполнить с ключом `-p` (`route add -p`), а в Ubuntu команду добавления маршрута следует включить в сценарий, исполняемый при подключении соответствующего интерфейса (*см. разд. "Подключение к Интернету с использованием серверов Ubuntu"*).

> ***Примечание***
>
> Возможностей настройки таблиц маршрутизации в Linux несравнимо больше, чем в Windows. Так можно настроить несколько таблиц маршрутизации, которые будут применяться выборочно к пакетам на основе анализа каких-либо их признаков. Иными словами, в одном случае пакет из пункта А в пункт Б можно отправить по одному маршруту, а в другом — по совершенно иному. Для этого существует специальный набор утилит iproute2, который по умолчанию уже установлен в Ubuntu. Если подобная настройка необходима, то ознакомиться с правилами ее конфигурирования можно, выполнив команду `man ip`.

Назначение адресов при совместном использовании подключения к Интернету

Особая ситуация возникает при настройке совместного подключения к Интернету. В этом случае тот компьютер, на котором создается данное подклю-

чение, начинает выполнять функцию сервера DHCP с единственным ограничением, что его адрес *жестко фиксирован* — 192.168.0.1. Клиенты, которые получают от данного сервера адреса из подсети 192.168.0.0/24, автоматически настраиваются на использование его в качестве шлюза по умолчанию и сервера имен.

Поскольку вариант совместного подключения присутствует как на серверных системах, так и на рабочих станциях, то такое решение наиболее оптимально для небольших организаций.

Порт

При передаче данных кроме IP-адресов отправителя и получателя пакет информации содержит в себе номера *портов*. Порт — это некое число, которое необходимо при приеме и передаче данных для идентификации процесса (программы), который должен обработать данные. Так, если пакет послан на 80-й порт, то это свидетельствует, что информация предназначена серверу HTTP.

Номера портов с 1-го по 1023-й закреплены за конкретными программами (так называемые *well-known-порты*). Порты с номерами 1024–65 535 можно использовать в программах собственной разработки. При этом возможные конфликты должны разрешаться самими программами путем выбора свободного порта. Иными словами, порты будут распределяться динамически: возможно, что при следующем старте программа выберет иное значение порта.

Знание того, какие порты задействуют те или иные прикладные программы, важно при настройке брандмауэров. Часть настроек в таких программах для наиболее популярных протоколов предопределена, и вам достаточно только разрешить/запретить протоколы, руководствуясь их названиями. А в некоторых случаях придется обращаться к технической документации, чтобы определить, какие порты необходимо "открыть", чтобы обеспечить прохождение пакетов данной программы.

> ***Примечание***
>
> При настройке брандмауэра следует учитывать, что многие программы при подключении к Интернету открывают не один порт, возможно, даже некоторый диапазон значений. Один из распространенных вариантов настройки брандмауэров для недокументированных программ — это анализ реального их трафика с помощью какой-либо программы перехвата передаваемых по сети пакетов.

Часто возникает необходимость увидеть, какие порты могут принимать трафик или уже имеют соединение с каким-либо компьютером (если порт может принимать трафик, то его состояние отображается как *LISTENING*). Как в Windows, так и в Ubuntu для этого применяется команда `netstat`.

В зависимости от версий операционной системы данная команда имеет различный набор ключей, позволяющий детализировать отчет (например, указать программы или процессы, использующие конкретные порты). В общем случае достаточно запустить команду с ключом `-a` (листинг 1.5).

Листинг 1.5

```
>netstat -a
Активные подключения
  Имя    Локальный адрес      Внешний адрес          Состояние
  TCP    sasha:http           sasha.ask.ru:0         LISTENING
  TCP    sasha:epmap          sasha.ask.ru:0         LISTENING
  TCP    sasha:https          sasha.ask.ru:0         LISTENING
  TCP    sasha:microsoft-ds   sasha.ask.ru:0         LISTENING
  TCP    sasha:1025           sasha.ask.ru:0         LISTENING
  TCP    sasha:1033           sasha.ask.ru:0         LISTENING
  TCP    sasha:1064           ack-isa2.ask.ru:8080   CLOSE_WAIT
  TCP    sasha:1067           ack-exchange.ask.ru:2703  ESTABLISHED
  TCP    sasha:1070           ack-exchange.ask.ru:1025  ESTABLISHED
  TCP    sasha:1078           ack-frw.ask.ru:8080    CLOSE_WAIT
  UDP    sasha:microsoft-ds   *:*
  UDP    sasha:isakmp         *:*
  UDP    sasha:1041           *:*
  UDP    sasha:1053           *:*
```

В данном примере на компьютере готовы к подключению несколько портов (состояние `LISTENING`, это порты http, epmap и т. д. — номера портов можно отобразить, если добавить ключ `-n`), порты 1067 и 1079 подключены (`ESTABILISHED`, программа показывает, с какой системой идет обмен данными), передача информации с портов 1064 и 1078 завершена и система находится в состоянии закрытия соединения (`CLOSE_WAIT`) и т. д.

Получить информацию по удаленному компьютеру позволяют специальные программы *сканирования портов*. Данные по отдельному порту (открыт/не открыт) можно получить штатными средствами системы (например, с помощью команды `telnet` или утилиты PortQry из состава Support Tools); для контроля диапазона портов обычно используют утилиту nmap. Она есть как в варианте запуска под Linux, так и под Windows. Загрузить ее можно с **http://nmap.org/download.html**.

Имена компьютеров в сети TCP/IP

Человеку удобнее работать с именем компьютера, чем запоминать цифры, составляющие его IP-адрес. В сети на основе протокола TCP/IP компьютерам присваивают имена *хоста (hostname)*.

> ***Примечание***
>
> В сетях Windows компьютеры могут иметь еще одно имя. Это NetBIOS-имя компьютера, используемое в составе рабочих групп. В общем случае необходимо стремиться к тому, чтобы NetBIOS-имя соответствовало имени хоста.

Полное имя хоста, которое называют также FDQN (сокращение от *Fully Qualified Domain Name*), составляется из нескольких имен, разделяемых при написании точкой, например, так: **www.ask.ru**. Первая слева группа символов (до точки), в данном примере это **www**, является собственным именем компьютера. Следующая группа символов — от точки до точки — это имя группы компьютеров (*домена*), которой принадлежит данная система. Следующая группа символов — имя группы компьютеров, которой в свою очередь принадлежат группы компьютеров, имена которых находятся левее. Данную цепочку можно продолжать сколь угодно долго. Для удобства обычно ограничиваются тремя-четырьмя группами символов. Написание полного имени принято завершать символом точки, чтобы отличать полное имя хоста от имени того или иного домена.

В зависимости от того, сколько групп символов входит в доменное имя, различают домены первого, второго, третьего и так далее уровней. На практике под *именем домена* понимают всю группу символов в полном имени справа от имени компьютера. Самая правая группа символов имени (до первой точки) называется *доменом первого уровня*, вторая справа — *доменом второго уровня*, затем следует *домен третьего уровня* и т. д.

> ***Примечание***
>
> При создании нового домена Windows не следует давать ему имя домена первого уровня. В этом случае действуют некоторые ограничения, с которыми можно ознакомиться в базе данных Microsoft. Целесообразно домену Windows дать имя по принципу ***<название_организации>*.local**.

Имена хостов внутри локального сегмента сети (домена Windows) должны быть уникальными. Имена хостов в разных доменах могут совпадать (в этом случае будут различными *полные* имена — FQDN).

Проверка каналов связи

Любая информационная система нуждается в надежно работающих каналах связи. Опишем некоторые способы, которые помогут проверить работу транспортной подсистемы в условиях обычного офиса.

Диагностика линий связи

Для проверки линий связи на физическом уровне необходимо специальное оборудование, например, *кабель-тестеры*. Как правило, эти устройства есть только в специализированных организациях, занимающихся прокладкой и тестированием линий связи. В лучшем случае у администратора может иметься простейший индикатор, отображающий наличие соединения или его обрыв.

Косвенно судить о качестве линии связи можно по числу ошибок в ней, которое отображается управляемым коммутатором (рис. 1.7). Подобная статистика свидетельствует о необходимости принятия незамедлительных мер по устранению причин некачественной работы канала связи.

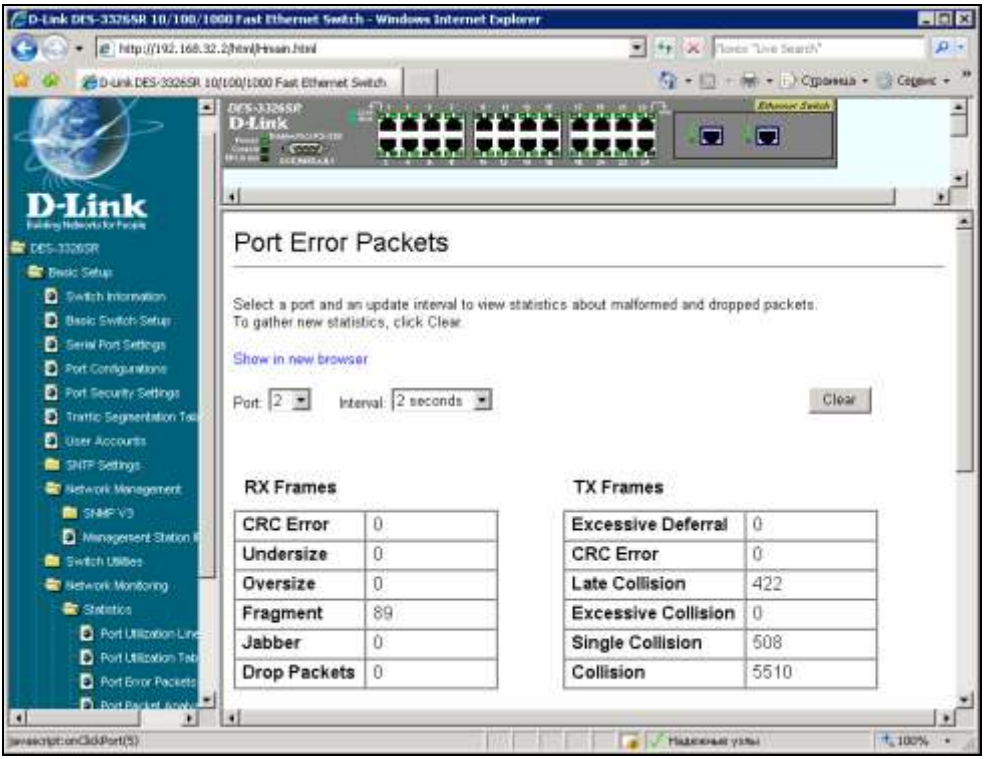


Рис. 1.7. Интерфейс отображения статистики ошибок на порту коммутатора

Поиск причин неудовлетворительного качества линии связи обычно следует начинать с проверки тех элементов, которые проще заменить:

- патч-корды (самодельные патч-корды часто через год-два эксплуатации становятся причинами ошибок);

- разъемы (наличие защелок, отсутствие пыли на оптических коннекторах и т. п.);
- качество расшивки в кроссе или кабельной розетке (потребуется вскрытие розетки, визуальная проверка и, возможно, повторная расшивка специальным инструментом).

Если самостоятельно устранить неполадки не удастся, то придется обратиться в специализированную организацию, которая проведет проверку и сможет указать на причину плохих показателей — например, на повреждение кабеля на расстоянии примерно 26 м от точки замера).

Диагностика IP-протокола

После проверки качества связи на транспортном уровне можно приступать к диагностике TCP/IP-протокола. Обычно это следует делать в таком порядке:

- проверить параметры настройки IP-протокола;
- определить достижимость ближайших компьютеров сети;
- проверить функционирование серверов имен;
- оценить качество канала связи глобальной сети (Интернета).

> ***Примечание***
>
> В Windows существует специальный мастер диагностики сетевого подключения, который выполняет аналогичные операции и выдает результаты соответствующих тестов. Эта программа вызывается из меню утилиты **Сведения о системе** (**Пуск | Все программы | Стандартные | Служебные | Сведения о системе | Сервис | Диагностика сети**).

Проверка параметров настройки IP-протокола

Для отображения параметров IP-протокола предусмотрены утилиты ifconfig (Ubuntu), `ipconfig` (Windows NT/200*x*/XP/Vista) и `winipcfg` (Windows 9*x*/ME). Утилиты ifconfig и `ipconfig` выполняются в режиме командной строки. Утилита `winipcfg` имеет графический интерфейс.

Утилиты выводят на экран параметры настройки протокола TCP/IP: значения адреса, маски, шлюза. При запуске `ipconfig` с ключом `/all` на экран будут выведены все действующие параметры протокола. Отмечу также ключ `/renew`, который позволяет обновить автоматически полученные параметры IP-протокола, и ключ `/registerdns`, с помощью которого можно обновить запись на DNS-сервере данного компьютера (используется в Windows 200*x*/XP/Vista).

Если утилита покажет, что сетевому адаптеру присвоен адрес 169.254.134.123 (или аналогичный — *см. разд. "Адресация APIPA"*), то можно сделать заключение, что в сети недоступен сервер, автоматически присваивающий

параметры IP-протокола. Часто причиной подобной ошибки (если ранее компьютер нормально работал в сети) является нарушение контакта в подсоединении сетевого кабеля.

Проверка достижимости ближайших компьютеров сети

Проверить достижимость компьютеров в сети TCP/IP позволяет команда `ping`, которая посылает на заданный компьютер последовательность символов определенной длины и выводит на экран информацию о времени ответа удаленной системы. Ключами команды можно регулировать количество отсылаемых символов и время ожидания ответа (через этот период выводится сообщение о превышении периода ожидания; если ответ придет позже, то он не будет показан программой).

При тестировании подключения рекомендуется применять такую последовательность операций.

1. Сначала проверяют работоспособность протокола TCP/IP путем "пингования" адреса 127.0.0.1:

   ```
   ping 127.0.0.1
   ```

   Адрес 127.0.0.1 — это "личный" адрес любого компьютера. Таким образом, эта команда проверяет прохождение сигнала "на самого себя". Ее можно выполнить без наличия какого-либо сетевого подключения. Вы должны увидеть приблизительно следующие строки (листинг 1.6).

Листинг 1.6

```
ping 127.0.0.1
Обмен пакетами с 127.0.0.1 по 32 байт:

Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
Статистика Ping для 127.0.0.1:
Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
Минимальное = 0 мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Если будет показано сообщение о недостижимости адресата, то это означает ошибку установки протокола IP. В этом случае целесообразно уда-

лить протокол из системы, перезагрузить компьютер и вновь установить поддержку протокола TCP/IP.

> ***Замечание***
>
> По умолчанию команда `ping` посылает пакет в 32 байта. Размер пакета можно увеличить (добавлением соответствующего ключа команды) до 65 Кбайт. Таким образом, можно обнаружить случаи ошибок пересылки пакетов большого размера. За размером тестового пакета отображается время отклика удаленной системы (в нашем случае — меньше 1 мс). Потом показывается еще один параметр протокола — значение TTL (*время жизни пакета*; практически это число маршрутизаторов, через которые может пройти пакет — каждый маршрутизатор уменьшает значение TTL на единицу).

2. На следующем шаге необходимо проверить ответ локального компьютера по присвоенному ему IP-адресу. Для этого следует выполнить команду:

   ```
   ping <адрес>
   ```

   Результат, который должен быть выведен на экран в случае нормальной работы, практически аналогичен предыдущему примеру.

3. Следующая проверка — это выполнение команды `ping` с указанием IP-адреса любого ближайшего компьютера. Можно указать любой адрес, относительно которого вы уверены, что он достижим в локальной сети на момент проверки, например, IP-адрес шлюза или адрес DNS-сервера.

   Наличие отклика свидетельствует, что канал связи установлен и работает. Отсутствие ответа обычно говорит либо о повреждении кабельной сети (например, нет контакта в разъеме), либо о неверно установленных параметрах статического адреса (если адрес получается автоматически, то следует обратиться в службу технической поддержки).

Проверка состояния порта TCP/IP удаленного компьютера

В случае применения брандмауэров для защиты подключения компьютера к Интернету наличие ответа от удаленной системы на команду `ping` совсем не означает, что пакеты, предназначенные другим портам, будут пропущены.

Существуют две возможности удостовериться в правильной настройке брандмауэра. Во-первых, в Support Tools от Windows 2003 присутствует утилита portqry.exe, которая позволяет увидеть ответ удаленной системы на запрос по конкретному порту. Так, для проверки достижимости FTP-сервера можно выполнить следующую команду:

```
portqry -n kenin -e 21
```

Возможный результат иллюстрирует листинг 1.7.

Листинг 1.7

```
Querying target system called:
kenin
Attempting to resolve name to IP address...
Name resolved to 192.168.0.29
TCP port 21 (ftp service): LISTENING
Data returned from port:
220 kenin.ask.ru X2 WS_FTP Server 5.0.0 (1845270209)
331 Password required
```

Утилита сообщила, что порт 21 открыт, и отобразила информацию, которую выдает FTP-сервер, работающий на этом компьютере (имя компьютера `kenin`).

Второй способ состоит в применении утилиты `telnet`. Запуская эту утилиту с параметрами в виде имени удаленной системы и номером порта, вы осуществляете попытку подключения к соответствующему порту.

> ***Примечание***
>
> Утилита Telnet по умолчанию недоступна в Vista, этот компонент следует добавить при необходимости.

Если вы не можете подключиться к удаленной системе, то необходимо найти компьютер, на котором происходит фильтрация пакетов. Для этого следует проверить путь прохождения информации с помощью команды `tracert`, после чего протестировать возможность подключения к соответствующему порту каждого компьютера этой цепочки (листинг 1.8).

Листинг 1.8

```
tracert www.ack.ru

Tracing route to ack.ru [212.107.195.12]
over a maximum of 30 hops:

 1   120 ms   111 ms   112 ms  ask_pdc.ask.ru [192.168.0.67]
 2   117 ms   113 ms   111 ms  frw.ask.ru [192.168.0.2]
 3   121 ms   113 ms   116 ms  cisco.ask.ru [195.161.192.254]
 4  1011 ms   346 ms   136 ms  aa-s0-6-r2.ekaterinburg.rostelecom.ru
[195.161.94.137]
 5   387 ms   181 ms   397 ms  aa-fe0-2-sw1.ekaterinburg.rostelecom.ru
[195.161.94.5]
```

```
 6   504 ms   461 ms   134 ms  tschelkun-bbn0-po1-5.rt-comm.ru
[217.106.6.149]
 7   751 ms  1146 ms  1712 ms  kochenevo-bbn0-po2-0.rt-comm.ru
[217.106.6.130]
 8  1855 ms  1796 ms     *     trs20-dsr0-po8-0-0.rt-comm.ru
[217.106.6.138]
 9  1221 ms  1313 ms  1212 ms  vlad-dsr0-po6-0.rt-comm.ru [217.106.6.158]
10  1223 ms  1212 ms  1212 ms  vmts.vladivostok.rostelecom.ru
[195.161.4.94]
11     *        *        *     Request timed out.
12     *        *        *     Request timed out.
13  1727 ms  1871 ms  1703 ms  ack.ru [212.107.195.12]
Trace complete.
```

По результату выполнения данной команды можно оценить, что наибольшая задержка в прохождении сигнала возникает на каналах связи с узлами, стоящими в строках 7 и 8. Одиночные звездочки свидетельствуют, что ответ от этого узла не получен в заданный диапазон времени. Если в строке стоят все звездочки, то это может обозначать, что администраторы соответствующих хостов не разрешили прохождение ICMP-пакетов (пакеты, которые используются в том числе и командами `ping` и `tracert`).

> ***Замечание***
>
> В Ubuntu утилита tracert должна быть доустановлена с использованием пакета traceroute (`apt-get install traceroute`). Кроме того, желательно запускать трассировку с ключом `-w` <*время*>, предписывающим ожидать ответа установленное время. В противном случае со значениями по умолчанию утилита для большинства узлов может вывести ответ только в виде звездочек.

Проверка функционирования серверов имен

Для проверки работоспособности сервера имен Интернета следует выполнить команду `ping`, указав в качестве параметра не IP-адрес, а доменное имя какого-либо компьютера, например, имя WWW-сервера вашего провайдера:

```
ping <имя>
```

Если команда сможет "разрешить" IP-адрес хоста и покажет отклик, то это означает работоспособность системы распознавания имен. Практически это говорит о правильной настройке протокола TCP/IP и работоспособности канала связи. Если не будет ответа на ввод команды с именем существующего хоста, то это может свидетельствовать либо об ошибке в задании DNS-серверов, либо об их неработоспособности.

Проверка качества канала связи

При работе в Интернете одни информационные серверы открываются быстрее, другие медленнее, бывают случаи недостижимости желаемого хоста. Часто причиной этого бывает недостаточное качество канала связи: большое время ожидания данных или существенный процент потерь пакетов, что обычно приводит к повторам передачи.

С помощью утилиты `pathping` в Windows можно оценить качество канала связи по всей цепочке до желаемого источника. Эта утилита посылает на каждый промежуточный хост серию пакетов и выводит информацию о количестве откликов и среднем времени ответа (листинг 1.9).

Листинг 1.9

```
C:\pathping www.microsoft.com
Tracing route to www.microsoft.akadns.net [207.46.230.219]
over a maximum of 30 hops:
0 ask-2002.ack.ru [192.168.0.52]
1 frw.ack.ru [192.168.0.12]
2 cisco.ack.ru [195.161.193.254]
3 aa-s0.ekaterinburg.rostelecom.ru [195.161.94.137]
4 aa-sw1.ekaterinburg.rostelecom.ru [195.161.94.5]
5 tschelkun.rt-comm.ru [217.106.6.149]
6 aksai.rt-comm.ru [217.106.6.97]
7 msk.rt-comm.ru [217.106.6.81]
8 ..spb.rt-comm.ru [217.106.6.70]
9 213.190.162.5
10 alv2-ge3-0.datanet.tele.fi [192.130.130.61]
11 208.51.142.197
12 ..pos8-0-2488M.cr1.CPH1.gblx.net [62.12.32.73]
13 pos1-0-2488M.cr2.SEA1.gblx.net [64.214.65.242]
14 so1-0-0-2488M.br2.SEA1.gblx.net [64.213.83.182]
Computing statistics for 375 seconds...
Source to Here This Node/Link
Hop RTT Lost/Sent = Pct Lost/Sent = Pct Address
0 ask-2002.ack.ru [192.168.0.52] 0/ 100 = 0% |
1 0ms 0/ 100 = 0% 0/ 100 = 0% frw.ack.ru [192.168.0.12] 0/ 100 = 0% |
2 1ms 0/ 100 = 0% 0/ 100 = 0% cisco.ack.ru [195.161.192.254] 2/ 100 = 2% |
3 637ms 2/ 100 = 2% 0/ 100 = 0% aa-s0.ekaterinburg.rostelecom.ru
[195.161.94.137] 0/ 100 = 0% |
4 613ms 4/ 100 = 4% 2/ 100 = 2% aa-sw1.ekaterinburg.rostelecom.ru
[195.161.94.5] 0/ 100 = 0% |
5 562ms 5/ 100 = 5% 3/ 100 = 3% tschelkun.rt-comm.ru [217.106.6.149] 0/
```

```
100 = 0% |
6 605ms 4/ 100 = 4% 2/ 100 = 2% aksai.rt-comm.ru [217.106.6.97] 0/ 100 = 0% |
7 623ms 4/ 100 = 4% 2/ 100 = 2% msk.rt-comm.ru [217.106.6.81] 0/ 100 = 0% |
8 725ms 5/ 100 = 5% 3/ 100 = 3% spb.rt-comm.ru [217.106.6.70] 0/ 100 = 0% |
9 864ms 2/ 100 = 2% 0/ 100 = 0% 213.190.162.5 0/ 100 = 0% |
10 942ms 2/ 100 = 2% 0/ 100 = 0% alv2-ge3-0.datanet.tele.fi
[192.130.130.61] 1/ 100 = 1% |
11 868ms 3/ 100 = 3% 0/ 100 = 0% 208.51.142.197 0/ 100 = 0% |
12 927ms 3/ 100 = 3% 0/ 100 = 0% pos8-0-2488M.cr1.CPH1.gblx.net
[62.12.32.73] 1/ 100 = 1% |
13 1040ms 4/ 100 = 4% 0/ 100 = 0% pos1-0-2488M.cr2.SEA1.gblx.net
[64.214.65.242] 0/ 100 = 0% |
14 1059ms 4/ 100 = 4% 0/ 100 = 0% so1-0-0-2488M.br2.SEA1.gblx.net
[64.213.83.182] 96/ 100 = 96% |

Trace complete.
```

После опубликования цепочки хостов, через которые проходит сигнал на пути к заданному серверу, программа `pathping` выводит статистические данные о достижимости каждого промежуточного хоста. Причем время усреднения выбирается исходя из конкретной ситуации (в примере подсчет проводился за период в 375 с). Первый параметр — время доступа к данному хосту, затем показано число посланных на него пакетов и число неполученных ответов (с процентом успеха). После чего отображаются аналогичные значения для достижимости конечного хоста при расчете прохождения пакетов от данной промежуточной точки. Так, в 14-й строке цифры "говорят", что время доступа к хосту составляет 1059 мс, что при посылке на него 100 пакетов на четыре отсутствовал ответ. А если бы сигнал на конечный хост передавался с позиции номер 14, то при посылке 100 пакетов на все был бы получен ответ. И в завершение после имени данного промежуточного хоста утилита сообщила, что число успешных пакетов составило 96%.

Переустановка протокола TCP/IP в Windows XP

Иногда "последним" средством восстановления работоспособности становится переустановка протокола TCP/IP. Поскольку в Windows XP данный протокол является практически основным компонентом, то пользователь не может удалить обычными операциями удаления/добавления компонентов.

Чтобы восстановить параметры протокола в первоначальное состояние, следует воспользоваться командой `netsh`. Команда

```
netsh interface ip reset
```

восстановит настройки протокола TCP/IP в значения по умолчанию.



Глава 2

Сетевые службы

Для функционирования любой информационной системы требуется наличие ряда сетевых служб. Прежде всего, это службы назначения параметров IP-адреса, службы разрешения имен. Рассмотрим реализацию этих служб как средствами Windows, так и операционной системы Ubuntu.

Служба автоматического назначения параметров IP-адреса

Параметры IP-протокола индивидуальны для каждого компьютера. Чтобы облегчить пользователям их назначение, были разработаны специальные механизмы, позволяющие автоматизировать данный процесс.

Адресация APIPA

Для облегчения построения небольших сетей разработчики Microsoft включили в Windows возможность самостоятельного назначения адресов. Если в сети не настроена служба выдачи параметров IP-адреса, то при автоматическом присвоении параметров Windows назначит сетевой плате адрес из диапазона от 169.254.0.1 по 169.254.255.254 (маска подсети 255.255.0.0), предварительно проверив, не занят ли уже такой адрес в сети.

Естественно, что никаких дополнительных параметров операционная система в этом случае не получает. Например, она не будет знать, куда посылать запросы, чтобы получить данные с серверов Интернета, и работа возможна только в пределах локальной сети.

Поэтому наличие адреса из указанного диапазона на рабочей станции обычно свидетельствует либо о проблеме со службой автоматического присвоения адреса в сети, либо о повреждении физической линии (например, обрыв кабеля).

Серверы DHCP

Для автоматической раздачи параметров IP-протокола в локальных сетях устанавливают так называемый сервер DHCP (Dynamic Host Configuration Protocol, динамический протокол конфигурации сервера). Сервер DHCP автоматически сообщает компьютерам, начинающим работу в составе сети, параметры настройки протокола TCP/IP: в первую очередь это IP-адрес, маска адреса, шлюз. Кроме того, сервер DHCP может предоставлять параметры серверов времени, указывать расположение данных автоматической настройки прокси-клиентов, данные для конфигурации IP-телефонов и т. п.

Обычно IP-адрес от сервера DHCP выделяется компьютеру на определенный срок, заданный в настройках сервера (поэтому его называют также *динамическим IP-адресом*). Если компьютер не будет продолжать работу в данной сети, то этот адрес может быть переназначен другому устройству.

Чтобы сервер начал раздавать адреса, вы должны задать диапазон этих адресов и определить необходимые параметры протокола. Делается это путем создания новой области (*scope*).

Для области необходимо определить, как минимум, диапазон распределяемых адресов, маску сети, указать срок аренды IP-адреса. Внутри диапазона адресов можно исключать некоторые адреса (например, если вы предполагаете задать их статически). Срок аренды выбирают исходя из особенностей вашей сети. При малом числе компьютеров его можно существенно увеличить по сравнению со значением по умолчанию в 8 суток (вплоть до неограниченного значения).

Для полноценной работы в составе компьютерной сети получения только IP-адреса и маски сети обычно недостаточно. Так, клиентам минимально необходимы адреса DNS-серверов и адрес шлюза. Кроме того, могут понадобиться DNS-суффикс существующей сети, адрес автоматической конфигурации прокси-сервера и т. п. Все эти параметры может сообщать DHCP-сервер.

Настройка серверов DHCP в Windows

Для установки службы DHCP в Windows достаточно отметить ее в перечне параметров Windows Server и затем авторизовать в службе каталогов. Чтобы авторизовать сервер (этот шаг необходим, если создан домен Windows), пользователю с правами администратора предприятия необходимо в меню консоли управления DHCP-сервером выбрать пункт **Авторизовать сервер.**

> ***Замечание***
>
> Индикатор, свидетельствующий об авторизации сервера, выдает статус с некоторой (обычно до 5 мин) задержкой. Поэтому после авторизации сервера следует выдержать незначительный промежуток времени и открыть консоль управления снова, чтобы убедиться в полной работоспособности сервера.

Параметры, сообщаемые пользовательской системе, определяются *опциями* DHCP. Глобальные опции определяются для всего сервера; они доступны в каждой области. Кроме того, можно определять опции в самой области: в случае, если для параметра назначены и глобальные значения, то будут применены параметры области.

В Windows операция добавления опций производится с использованием графического интерфейса. Достаточно открыть динамическое меню, найти нужную опцию, включить ее и назначить значение. Итоговый перечень опций доступен в окне оснастки управления (рис. 2.1).

Кроме перечисленных в оснастке, администратор легко может создать новые опции, руководствуясь описаниями прикладной программы. Две нижние опции в перечне соответствуют глобальным значениям всего сервера, остальные — определены для данной области.

DHCP-сервер можно настроить так, чтобы он выдавал клиентам не случайный, а заранее определенный адрес. Чтобы настроить резервирование адреса, необходимо *знать MAC-адрес сетевого адаптера* соответствующего клиента. Этот адрес легко определить в свойствах соответствующего подключения как для Windows-систем (ipconfig /all), так и Linux (ifconfig, значение HWaddr). Сам процесс резервирования не представляет сложности, достаточно (в Windows) в оснастке управления DHCP-сервером ввести в окне операции резервирования имя клиента и его MAC-адрес или, в случае Ubuntu, создать по образцу блок описания резервированного адреса и перезагрузить службу.

ЗАМЕЧАНИЕ

Для новых сетевых адаптеров MAC-адрес можно определить по их упаковке (вторая часть адреса — это серийный номер адаптера).

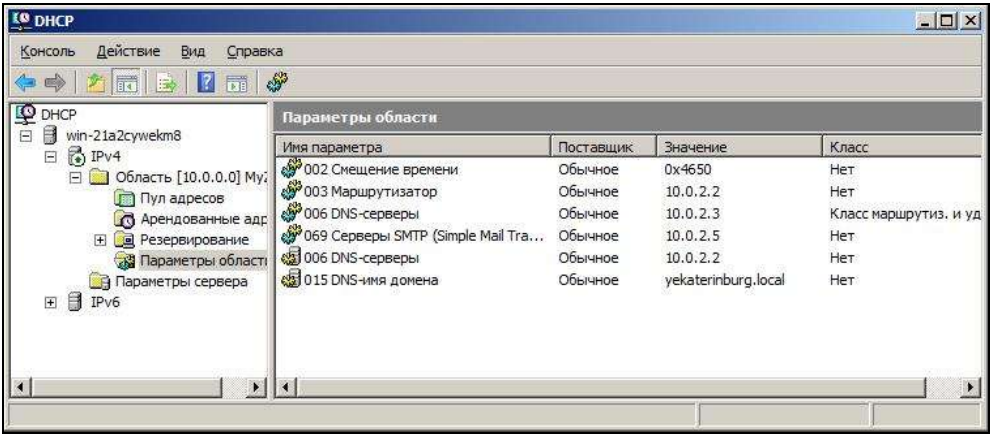


Рис. 2.1. Оснастка управления DHCP-сервером Windows 2008

Установка и настройка сервера DHCP в Ubuntu

В Ubuntu сервер DHCP устанавливается командой

```
sudo apt-get install dhcp3-server
```

> ***Примечание***
>
> Поскольку часто DHCP-сервер в небольших организациях устанавливают на компьютер, являющийся шлюзом Интернета, следует ограничить его работу только внутренним интерфейсом. Для этого укажите название интерфейса в параметре INTERFACES в файле /etc/default/dhcp3-server.

После установки сервера DHCP необходимо выполнить *настройку зоны*. В Ubuntu все параметры зоны настраиваются в файле /etc/dhcp3/dhcpd.cond. В файле подробно описаны все параметры с многочисленными примерами, так что определить по этим образцам свои зоны не представит никакого труда. Достаточно просто скопировать нужный блок и заменить образцы реальными значениями. В листинге 2.1 приведен образец конфигурации сервера DCHP в Ubuntu.

Листинг 2.1

```
ddns-update-style interim;
include "/etc/bind/rndc.key";
ddns-domainname "test.ru";

option domain-name "test.ru";
option domain-name-servers aster.test.ru;
option option-176 code 176 = string;
option netbios-name-servers 192.168.31.1;
option netbios-node-type 8;

default-lease-time 600;
max-lease-time 7200;

authoritative;

log-facility local7;

subnet 192.168.31.0 netmask 255.255.255.0 {
       range 192.168.31.100 192.168.31.200;
       option routers 192.168.31.10;
       option domain-name "test.ru";
       option broadcast-address 192.168.31.255;
```

```
        option option-176 "MCIPADD=192.168.31.10,TFTPSRVR=192.168.31.10";

        zone 31.168.192.in-addr.arpa. {
        primary 127.0.0.1;
        key "rndc-key";
        }

        zone test.ru. {
        primary 127.0.0.1;
        key "rndc-key";
        }
}
```

В листинге 2.1 показана конфигурация DHCP сервера, достаточная для обслуживания клиентов. Сервер дополнительно настроен на выдачу параметров опции с номером 176, которая необходима для работы IP-телефонов. Конфигурация также предполагает обновление сервера DNS (прямой зоны test.ru и обратной — 31.168.192.in-addr.arpa) в случае получения клиентом DHCP IP-адреса. Подробно эти настройки описаны далее.

При изменении настроек сервера DHCP в Ubuntu необходимо перезагрузить его конфигурацию:

```
sudo  /etc/init.d/dhcp3-server restart
```

Обслуживание DHCP-сервером других сегментов сети

С помощью одного DHCP-сервера администраторы могут раздавать IP-адреса различным сегментам своей сети. Для этого необходимо на DHCP-сервере создать области с диапазонами адресов, соответствующими этим сегментам, и обеспечить получение DHCP-сервером запросов из другого сегмента сети.

Создание областей с различными диапазонами IP-адресов выполняется стандартно: вы создаете область и определяете для нее любой желаемый диапазон адресов. Но чтобы сервер DHCP выдал адрес из этого диапазона, он должен получить запрос из другого сегмента сети.

В большинстве случаев для формирования запросов на получение IP-адреса используются возможности современных коммутаторов. Для этого достаточно выполнить настройку опции DHCP Relay (названия могут несколько отличаться) — рис. 2.2.

> ***ЗАМЕЧАНИЕ***
>
> Агенты ретрансляции DHCP-запросов могут быть и программными, например, такой агент входит в состав сервера маршрутизации и удаленного доступа Windows (Routing and Remote Access Server, RRAS).

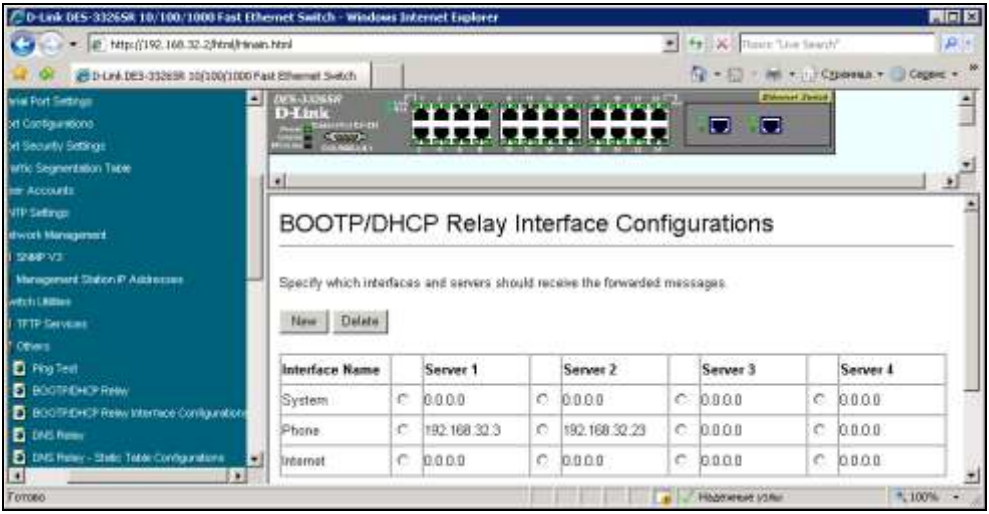


Рис. 2.2. Настройка функции DHCP Relay на коммутационном оборудовании

Для настройки пересылки запросов DHCP достаточно в интерфейсе управления коммутатором указать IP-адрес сервера DHCP. Как правило, настройки коммутаторов позволяют определять основной и резервный серверы DHCP. Такие настройки должны быть указаны для каждого IP-интерфейса, созданного на коммутаторе третьего уровня.

Принцип работы агента ретрансляции DHCP весьма прост. Агент прослушивает сеть на наличие пакетов запроса аренды адреса. Если такой пакет получен, то агент ретранслирует запрос на адрес, указанный в настройках опции. Сервер DHCP получает данный запрос и, поскольку он отправлен с адреса другого сегмента сети, предоставляет в аренду адрес именно того диапазона, из которого пришел запрос.

Отказоустойчивая конфигурация DHCP-сервера

При построении отказоустойчивых информационных систем важно обеспечить стабильную работу сетевых служб, в том числе сохранить функционирование службы автоматического присвоения параметров IP-адреса в случае выхода сервера DHCP из строя.

Реализация DHCP на основе сервера Microsoft имеет серьезный недостаток, связанный с тем, что невозможно создать горячий резерв данной службы для одного диапазона IP-адресов.

Документы Microsoft предлагают для повышения отказоустойчивости два варианта. Первый — это размещение службы DHCP на серверном кластере.

В этом случае база адресов будет храниться на общем диске, а при выходе из строя одного сервера его работу "подхватит" второй сервер кластера. К сожалению, такое решение часто не доступно (по стоимости реализации отказоустойчивого кластера) малым и средним организациям.

Второй вариант решения проблемы отказоустойчивости службы DHCP заключается в настройке для организации *двух* серверов DHCP с *различными* (неперекрывающимися) частями выделенного диапазона адресов организации. В этом случае клиент будет получать параметры адреса от любого сервера (реально от того, кто раньше ответит), а при выходе из строя одного из серверов, второй продолжит обслуживание организации.

В Ubuntu можно организовать совместную работу нескольких серверов DHCP так, чтобы они обеспечивали не только отказоустойчивость данной службы, но и балансировку нагрузки. Для этого достаточно описать в файле настроек группу DHCP-серверов и сослаться на нее в параметрах зон. Соответствующие настройки несложно найти в Сети.

Статическое разрешение имен

В небольшой локальной сети для задания соответствия "IP-адрес — сетевое имя" можно вручную сформировать статические записи. Это позволяет обеспечить функционирование локальной сети без серверов DNS, DHCP и т. п.

Если Windows не может динамически определить имена (IP-адреса) хостов, то система использует содержимое файлов hosts, networks и lmhosts. Первые два файла представляют обычный список соотношений "IP-адрес — имя" в прямом и обратном порядке (листинг 2.2).

Листинг 2.2

```
Файл hosts:
...
195.12.156.31      ads.adximize.com
63.120.34.76       c3.xxxcouter.it
...
Файл networks:
...
ads.adximize.com  195.12.156.31
c3.xxxcouter.it    63.120.34.76
...
```

Файл lmhosts совместим с Microsoft LAN Manager 2.*x* и предназначен для загрузки специальных NetBIOS-имен (указания сервера домена, серверов приложений и т. п.). Файлы находятся в папке %systemroot%/system32/drivers/etc (для Windows 9*x* — в папке Windows). При установке системы обычно создаются примеры (имеют расширение sam), по образцу которых и следует редактировать необходимые файлы.

В Ubuntu для статического разрешения имен предусмотрены файлы hosts (полный путь /etc/hosts) и resolv.conf (полный путь /etc/resolf.conf, в этом файле хранятся записи о серверах разрешения имен). Синтаксис записей об именах в этих файлах аналогичен описанному ранее.

Изменять файлы можно в обычном текстовом редакторе (необходимы права администратора/суперпользователя). Запись должна начинаться с первой позиции строки, а столбцы можно отделять любым числом пробелов.

Серверы DNS

Для снижения количества ручных операций в целях разрешения имен существуют специальные серверы — DNS-серверы (Domain Name System). Серверы DNS обеспечивают получение доменного имени по запросу на основе IP-адреса, и наоборот. Поэтому указание адреса сервера DNS — это одна из основных настроек протокола TCP/IP, необходимых для работы в Интернете.

> ***Замечание***
>
> Если в настройках не указан IP-адрес сервера DNS, то пользователь не будет полноценно работать в Интернете, поскольку не сможет переходить по ссылкам, в которых присутствует доменное имя. А это практически все ссылки на информационных серверах.

Адрес сервера DNS обычно назначается автоматически при инициализации протокола IP. Имена серверов DNS сообщаются DHCP-серверами. Обычно указывается несколько DNS-серверов, чтобы система могла использовать второй сервер при временной недоступности первичного DNS.

Основные понятия DNS

DNS (Domain Name System, система доменных имен) — это служба разрешения имен в сетях на основе протокола TCP/IP. Для уверенной работы с DNS необходимо четко представлять себе, что означают те или иные термины.

- **Зоны DNS.**

  Зона DNS — это часть пространства имен, для которого DNS-сервер может выполнять операции разрешения имен. Существуют зоны прямого

и обратного просмотра, которые на практике для удобства называют *прямыми* и *обратными* зонами.

Прямая зона позволяет по имени системы получать ее IP-адрес, *обратная* — по IP-адресу "выдает" информацию об имени хоста. Поэтому если нужно по имени компьютера узнать его адрес, то говорят о *прямом разрешении имени*. Если по IP-адресу хотят получить имя компьютера, то в этом случае происходит *обратное разрешение имени*. Строго говоря, если в DNS зарегистрировано прямое разрешение имени, то должно быть и обратное.

> ***ПРИМЕЧАНИЕ***
>
> Если ваша организация зарегистрировала на свое имя домен, то для нормальной работы почтового сервера необходимо зарегистрировать обратное разрешение имени. Проверьте (по протоколу telnet) ответ почтового сервера на обращение "Hello" и зарегистрируйте это имя в обратной зоне. Владельцами обратных зон являются, обычно, провайдеры. Поэтому именно к ним и нужно обращаться с подобной просьбой.

Для разрешения обратных имен в домене самого верхнего уровня создана зона `in-addr.arpa`. Названия зон обратного просмотра формируются с указанием этого имени и добавлением к нему слева имени трех октетов адреса сети в обратном порядке. Например, для сети 195.161.192.0/24 имя обратной зоны будет `192.161.195.in-addr.arpa`.

- **Первичная и вторичная зоны.**

У создаваемых записей DNS должен быть один "хозяин". Чтобы все записи были корректны, их необходимо вносить на одном DNS-сервере. В этом случае говорят, что на таком DNS-сервере расположена *первичная* зона. Для отказоустойчивости на других серверах можно создать копии этой зоны. Такие зоны будут называться *вторичными*. Вторичная зона содержит те же записи, что и первичная, но в нее нельзя вносить изменения или добавлять новые записи. Эти операции можно делать только для первичной зоны.

> ***ЗАМЕЧАНИЕ***
>
> В случае домена Windows 200*x* и использования зоны DNS, интегрированной со службой каталогов, изменения можно вносить на любом DNS-сервере такой зоны.

- **Серверы имен зоны.**

Для каждой первичной зоны можно создать сколько угодно копий на других серверах. Принято определять серверы имен, информация которых "официальна". Такие серверы называют NS-записями соответствующего

домена. Обычно для каждого домена создается два или три NS-сервера. Если ответ на запрос разрешения имени получен от NS-сервера, то он считается авторизованным, другие серверы возвращают неавторизованные ответы (принципиально возможна ситуация, что информация с таких серверов уже устарела).

Примечание

Для обновления записей DNS на клиентских компьютерах следует очистить кэш DNS-записей (`ipconfig /flushdns`).

- **Передача зон.**

  Так называется специальная операция копирования всех записей данной зоны с одного DNS-сервера на другой. По соображениям безопасности часто передача зон разрешается только на заранее определенный администратором системы список IP-адресов DNS-серверов.

- **Делегирование зон.**

  Если на DSN-сервере создана, например, прямая зона для домена `test.local`, то запись о домене третьего уровня `level3.test.local` должна содержаться на этом же сервере. Если географически домен `level3.test.local` удален от основного домена, то поддержание записей в его зоне на DNS-сервере становится не очень удобным. Проще поручить администратору этого домена вносить изменения в DNS-записи самостоятельно с помощью делегирования зоны. При делегировании DNS-сервер создает у себя запись, указывающую, что запросы разрешения имени для этой зоны должны перенаправляться на другой DNS-сервер, на который произведено *делегирование зоны*.

- **Stub-зоны (зона-заглушка).**

  При делегировании зоны на исходном сервере сохраняется информация о NS-сервере делегированной зоны. Поскольку администратор делегированной зоны может изменять ее DNS-записи, то он может и сменить записи NS-сервера. Если соответствующее изменение не будет внесено на сервер, который осуществляет делегирование, то процесс разрешения имен нарушится (основной сервер по-прежнему будет отправлять запросы на несуществующий уже адрес, в результате будет формироваться неверный ответ).

  Для исправления подобной ситуации введено понятие *stub-зоны*. При создании stub-зоны в ней определяются NS-записи делегированной зоны. Причем если администратор делегированной зоны меняет эти записи, то соответствующие изменения вносятся и в записи stub-зоны. В результате гарантируется целостность процесса разрешения имен.

- **Зона "точка".**

  Домен самого верхнего уровня, как уже писалось, принято называть именем "точка". Если в DNS создать зону "точка", то это будет фактически означать, что данный сервер является корневым в структуре DNS, т. е. он должен разрешать самостоятельно любые запросы имен. Если этот DNS-сервер не может разрешить имя, то его ответ будет гласить, что такого хоста не существует.

Основные типы записей DNS

При создании первичной зоны для своего домена следует обратить внимание на создание некоторых специальных записей ресурсов (resource records), которые полезны для получения информации общего типа.

- **SOA (Start of Authority).**

  Серийный номер зоны. В DNS автоматически увеличивается при любом изменении записей зоны. Используется в операциях переноса зон (если номер изменился, то происходит обновление записей вторичной зоны). На практике принято этот номер формировать на основе даты последнего изменения: год-месяц-день-(время), например, так: 20090810.

- **NS (Name Server).**

  Адреса "официальных" серверов имен данной зоны. Эти серверы возвращают *авторизованные* ответы.

- **RP (Responsible Person).**

  Адрес электронной почты лица, ответственного за внесение изменений в записи зоны. Наличие записи и поддержание ее актуальности желательно, чтобы при возникновении каких-либо вопросов по домену организации, у специалистов были реальные контактные данные. Обратите внимание, что символ `@` адреса электронной почты заменяется на точку.

- **A (Host Address).**

  Эта запись содержит информацию об имени системы и ее IP-адресе. Именно этот тип записи добавляется в DNS- сервер при регистрации хостов.

- **PTR (Pointer, указатель).**

  Так называется запись в обратной зоне. Настройками DNS локальных доменов обычно предусматривается автоматическое создание (изменение) PTR-записи при добавлении A-записи в прямую зону.

- **CNAME (Canonical NAME).**

  Записи псевдонима. Используются, если хосту необходимо дать второе DNS-имя.

- **MX (Mail eXchanger).**

  Запись хранит IP-адрес сервера электронной почты (SMTP-сервера), который обслуживает данный домен. Чтобы на данный домен можно было отправлять электронную почту, в DNS для домена должна быть обязательно создана MX-запись. Для целей резервирования может быть создано несколько MX-записей. Чтобы различать их, каждой записи соответствует определенный *вес*. По умолчанию почта отправляется на адрес, содержащийся в MX-записи с наименьшим весом. Если этот сервер не отвечает, то делаются попытки отправить почту на адреса, соответствующие MX-записям с последующими весами.

- **SRV (Запись службы).**

  Специальный тип записи для обнаружения служб в домене (например, службы IP-телефонии и т. п.). Записи о системных службах Windows автоматически создаются службой каталогов. Вручную записи добавляют при настройке дополнительных продуктов в соответствии с прилагаемой технической документацией.

Разделение DNS

Все большее число сотрудников начинают использовать мобильные компьютеры для доступа к ресурсам организации как изнутри локальной сети, так и из Интернета. Для сокращения затрат на изменение конфигураций персональных компьютеров следует выполнять настройки программного обеспечения так, чтобы доступ к сетевым ресурсам локальной сети осуществлялся *единообразно*, независимо от того, выполняется подключение из локальной или глобальной сети. Реализуется такое требование *разделением DNS* (DNS split).

Технология разделения DNS подразумевает, что разрешение имен локальной сети и Интернета для *одного доменного имени* настраивается на *различные DNS-серверы*. Суть решения будет понятна из рассмотрения двух возможных ситуаций.

Одинаковые имена локального домена и домена Интернета

Если имя домена Windows совпадает с именем домена Интернета, то единственная необходимая операция — это правильная настройка публикации внутренних ресурсов в глобальной сети. Когда клиент локальной сети пытается получить доступ к каким-либо ресурсам, он запрашивает их месторасположение у *локального, внутреннего* сервера DNS. Этот сервер возвращает клиенту внутренний адрес ресурса, к которому и осуществляется подключение (рис. 2.3).

Примечание

Ресурсом, для которого наиболее часто приходится реализовывать подключение пользователей как изнутри организации, так и снаружи, является почтовая система. Например, если в организации установлен MS Exchange Server и клиенты применяют MS Outlook (полной версии), то для локального подключения к почтовой системе по умолчанию применяется протокол RPC. Подключение по этому протоколу подразумевает динамическое открытие портов на сервере, что вызывает серьезные сложности в настройке брандмауэра при подключении клиента Outlook из глобальной сети. В результате на практике такое подключение из Интернета фактически не использовалось. Начиная с Windows Server 2003, для реализации всей функциональности полной версии Outlook предназначена специальная технология создания RPC Proxy, которая подробно описана в документах базы данных Microsoft (см. документ "Exchange Server 2003 RPC over HTTP Deployment Scenarios" или KB 833401). Обратите внимание, что одновременно следует настроить и клиента Outlook так, чтобы по умолчанию для подключения к почтовому серверу Exchange применялся вариант RPC over HTTP (статья "Configuring Outlook 2003 for RPC over HTTP").

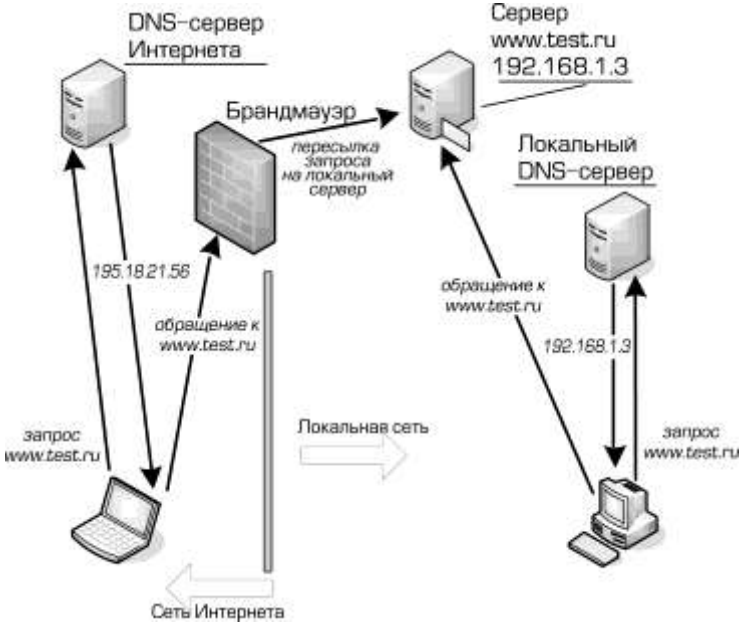


Рис. 2.3. Разделение DNS

На сервере DNS, обслуживающем домен Интернета этой же организации, необходимо настроить A-запись соответствующего ресурса на *внешний адрес* брандмауэра данной организации. А на брандмауэре настроить публикацию внутреннего ресурса таким образом, чтобы запрос, приходящий на брандмауэр и адресованный на данное имя, перенаправлялся на локальный адрес ресурса.

В результате, независимо от точки подключения, запрос клиента всегда будет доставлен на один и тот же локальный ресурс системы.

При реализации технологии разделения DNS клиент локальной сети и компьютер Интернета при разрешении одного и того же имени будут обращаться к различным DNS-серверам. Локальный клиент в результате будет обращаться по локальному адресу, а клиент Интернета перешлет запрос на брандмауэр организации, который и переправит его на локальный адрес запрашиваемого ресурса. В результате никакой перестройки прикладных программ на клиенте осуществлять не придется.

Различные имена локального домена и домена Интернета

Если "внутреннее" и "внешнее" имена домена организации не совпадают, то на внутреннем сервере DNS необходимо создать первичную зону для домена с "внешним" именем. В эту зону внести записи, соответствующие именам систем, предоставляющих необходимые службы (естественно, изменять записи этой зоны придется вручную). Причем в качестве IP-адресов этих записей следует указать *локальные* IP-адреса систем. Таким образом, на внутренних DNS-серверах будет по две зоны: зона, соответствующая "внутреннему" домену (реальные внутренние названия компьютеров локальной сети), и зона с "внешним" именем (содержит фактически синонимы, вторые имена только для компьютеров, публикующих ресурсы в глобальной сети). Так же как и в предыдущем примере, следует настроить публикацию внутренних ресурсов на брандмауэре организации.

Клиентов необходимо настроить (в том числе и в локальной сети) на подключение к ресурсам по *внешним именам*. Если клиент обратится к почтовому серверу *изнутри* организации, то он запросит *внутренний* сервер DNS об адресе, соответствующем внешнему имени почтовой системы. Поскольку на внутреннем сервере DNS существует одноименная первичная зона, то сервер будет считаться авторизованным для ответов и сообщит клиенту *внутренний адрес* почтовой системы. Произойдет подключение по локальному адресу системы.

А если, например, клиенту необходимо обратиться к этому же почтовому серверу из Интернета, то он запросит внешний сервер DNS, получит от него адрес брандмауэра и отправит запрос на него. Брандмауэр, получив запрос, проанализирует его и перешлет на локальный адрес почтовой системы.

Установка сервера DNS

Сервер DNS можно установить только на компьютер со статическим IP-адресом. При этом обратите внимание, чтобы сервер DNS, который предполагается для обслуживания организации, смог правильно разрешать *неполные* имена. Следовательно, он должен сообщить правильный адрес как на запрос

для `test.mydomain.local`, так и для запроса на имя `test`. Для этого необходимо, чтобы основной DNS-суффикс компьютера, на котором устанавливается сервер DNS, *совпадал* с суффиксом имени домена организации. Соответствующие настройки выполняются в параметрах TCP/IP протокола, устанавливаемых по статике для сетевого адаптера сервера DNS. В Ubuntu в этих целях необходимо правильно отредактировать файл /etc/resolf.conf (параметр *search*).

Установка DNS в Windows Server

Службу DNS устанавливают, добавляя соответствующую роль в оснастке **Диспетчера сервера**. Дальнейшие операции проходят под руководством мастера операций и не представляют особых сложностей.

Создание новой зоны также происходит под руководством мастера. Не забудьте только в свойствах созданной зоны определить параметры RP, перечислить серверы, которым вы разрешаете получить полный список зоны, и установить необходимый режим обновлений зоны. Если сервер функционирует, в том числе, в режиме кэширования (т. е. за реальными именами Интернета клиенты обращаются на этот же сервер), то необходимо указать адреса DNS-серверов провайдера в свойствах сервера. Для этого откройте свойства DNS-сервера (именно всего сервера, а не зоны) и на вкладке **Пересылка** укажите полученные от провайдера значения.

Управление сервером DNS осуществляется с помощью оснастки **Диспетчер DNS,** в которой представлены все операции, необходимые для управления сервером DNS от Microsoft (рис. 2.4). Текущие операции ограничиваются, как правило, только ручным добавлением необходимых записей.

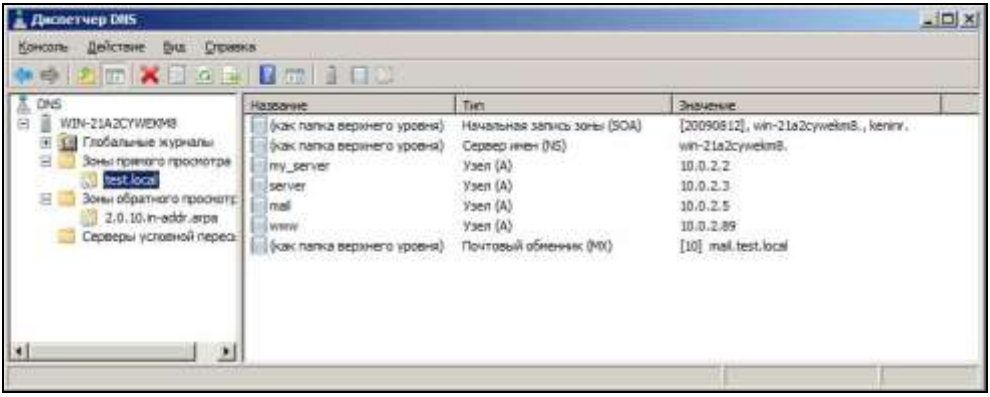


Рис. 2.4. Оснастка **Диспетчер DNS**

Новые зоны на сервер DNS добавляют с помощью мастера операций. Следует учесть, что если сервер предназначен для разрешения имен домена Windows и является контроллером домена, то оптимальным решением будет создание зоны, *интегрированной со службой каталогов*. Такой вариант позволит использовать службы Windows для репликации данных между серверами DNS. При этом зона DNS на *каждом* сервере будет фактически являться первичной (допускать внесение изменений), а сами данные — безопасными (при работе с зоной будет задействована встроенная в Windows система безопасности).

Интегрированная в службу каталогов система имен реплицируется по всем контроллерам домена. Начиная с Windows Server 2003, добавлена возможность размещения зоны DNS в *собственных разделах каталога*. Это позволяет реплицировать интегрированные в службу каталогов зоны *только* на серверы DNS либо домена, либо леса, в зависимости от того, какой раздел вы создаете, исходя из структуры организации. Данная операция выполняется из оснастки управления сервером DNS (соответствующая команда меню сервера).

Для зон, обслуживающих домен Windows, обязательно должна быть включена опция динамического обновления. В целях безопасности следует выбрать вариант безопасных динамических обновлений записей. При этом рекомендуется, чтобы служба DHCP была настроена на запуск не от системной учетной записи, а от имени специально созданного для такой цели пользователя.

Если вы не хотите регистрировать всех клиентов в DNS, то можно настроить сервер DNS так, чтобы он перенаправлял неразрешенные запросы имени на WINS-сервер. Для этого в настройках DNS-сервера в свойствах зоны на вкладке **WINS** следует включить опцию пересылки запросов на WINS-сервер и указать соответствующие IP-адреса. Обычно такая настройка необходима для сетей, в которых есть клиенты Windows 9*x*.

После установки и настройки основных параметров DNS-сервера необходимо выполнить его первичное тестирование. В свойствах сервера на вкладке мониторинга следует включить опции проверки как работы самого сервера, так и правильности перенаправления запросов и провести тест.

Установка и настройка сервера DNS в Ubuntu

Наиболее популярный сервер DNS в Linux — Bind — устанавливается командой

```
sudo apt-get install bind9
```

Конфигурация DNS-сервера представлена несколькими файлами в папке /etc/bind9. Это файл named.conf, в который включаются параметры из файлов named.conf.local и named.conf.options. Файл named.conf следует оставить без изменений, а все пользовательские настройки внести в оставшиеся два файла.

Конфигурация DNS-сервера допускает указание многих дополнительных параметров, но в условиях обслуживания внутренней сети обычно нет необходимости, например, скрывать номер версии программного обеспечения или определять, какой диапазон адресов сети будет обслуживаться сервером. Поэтому мы рассмотрим только основные настройки.

Параметры DNS-серверов провайдера (которые вы получили при подключении к Интернету) следует указать в файле named.conf.options, сняв комментарии в строках блока forwardes и заменив 0.0.0.0 на реальные IP-адреса серверов.

Обратите внимание, что для вступления в силу измененных настроек конфигурации сервера, его необходимо перезагрузить командой

```
sudo /etc/init.d/bind9 restart
```

Для создания собственной зоны ее следует определить в файле named.conf.local. В нем вы указываете название зоны и имя файла с ее записями, например, как показано в листинге 2.3.

Листинг 2.3

```
zone "имя.ru" {
    type master;
    file "db.имя.ru";
};

zone "31.168.192.in-addr.arpa" {
    type master;
    file "db.31";
};
```

После чего необходимо создать файлы зон с описаниями параметров систем. Если путь к файлам зон явно не указан в named.conf.local, то их необходимо создать в папке /var/cache/bind (это определено в файле named.conf.optios).

В Интернете можно найти много рекомендаций по созданию файлов зон. Листинг 2.4 иллюстрирует пример конфигураций для зон прямого и обратного разрешений.

Листинг 2.4

/var/cache/db.имя.ru

```
$TTL 604800     ; 1 week
@                 IN SOA  localhost. admin.имя.ru. (
```

```
                                20090118         ; serial
                                604800     ; refresh (1 week)
                                86400      ; retry (1 day)
                                2419200    ; expire (4 weeks)
                                604800     ; minimum (1 week)
                                )
имя.ru          IN          NS      localhost.
имя.ru          IN          MX   10   mail.имя.ru
имя.ru          IN          A       192.168.31.10
www             IN          A       192.168.31.20
mail            IN          A       192.168.31.15
```

/var/cache/db.31

```
$TTL 604800     ; 1 week
31.168.192.in-addr.arpa IN SOA  ns.имя.ru. admin.имя.ru. (
                                20090118        ; serial
                                604800     ; refresh (1 week)
                                86400      ; retry (1 day)
                                2419200    ; expire (4 weeks)
                                604800     ; minimum (1 week)
                                )
                           NS      localhost.
15                          PTR     mail.имя.ru.
20                         PTR     www.имя.ru.
```

Структура файла достаточно ясна из листинга 2.4 Отметим только, что в строке с SOA сначала указывается имя зоны (вместо явного указания имени зоны допустим символ `@`, как в третьей строке), после SOA следует полное имя первичного сервера имен (заканчивается точкой), потом владелец зоны. В качестве серийного номера на практике принято указывать дату внесения изменений. А в строках определения почтового сервера и сервера имен название домена можно опустить. Обратите внимание, что в строке адреса почтового сервера обязательно должен присутствовать номер ("вес" почтового сервера).

Для файлов зон следует установить полные права для учетной записи, от имени которой запускается сервер DNS (bind):

```
chown bind. /var/cache/bind/*
```

После этого нужно перезагрузить зоны. Сделать это можно либо командой

```
sudo /etc/init.d/bind9 reload
```

либо

```
sudo rndc reload
```

ЗАМЕЧАНИЕ

Утилита rndc, предназначенная для управления сервером DNS, устанавливается в систему по умолчанию с пакетом bind9.

Обязательно проверьте сообщения в журнале системы после перезагрузки зон:

```
tail /var/log/syslog
```

В этом журнале не должно быть сообщений об ошибках и о незагрузке той или иной зоны. Кроме того, проверьте ответы DNS-сервера (то, насколько вы правильно создали записи зон) следующей командой:

```
dig any имя_зоны
```

Динамическое обновление DNS

Поскольку IP-адреса раздаются динамически, то целесообразно настроить обновление DNS-зон на основе выданных параметров DHCP-сервера.

Современные Windows-клиенты реализуют обновление Windows-DNS-сервера при получении IP-адреса. Для предыдущих версий целесообразно включить в настройках DHCP-сервера Windows опцию обновления DNS-сервера (рис. 2.5).

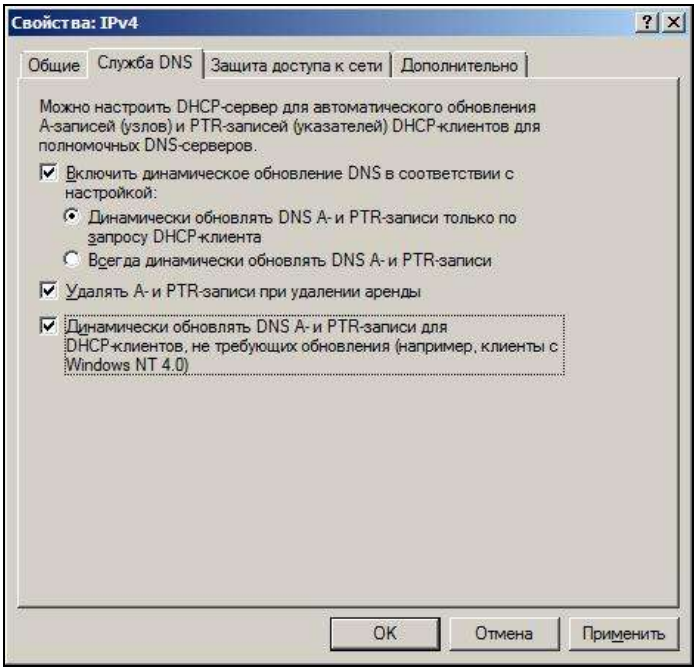


Рис. 2.5. Настройка параметров автоматического обновления DNS-сервера на платформе Windows 2008

Включение опции динамического обновления записей DNS-сервера для всех клиентов производится из меню свойств сервера DHCP. При наличии в сети клиентов предыдущих версий необходимо настроить сам сервер на обновление DNS после обработки от них DHCP-запроса.

При использовании служб сервера Ubuntu необходимо выполнить несколько больше операций, отредактировав как файлы настроек DHCP-сервера (указать, записи в каких зонах должны обновлять какие DNS-серверы), так и DNS-сервера (в первую очередь, настроив параметры для безопасного доступа к обновлениям).

Отредактируйте следующим образом настройки DNS-сервера. Во-первых, в файле named.conf.options раскомментируйте параметр `query-source` и укажите его так:

```
query-source address * ;
```

Во-вторых, в файле named.conf.local добавьте в начало следующие строки:

```
include "/etc/bind/rndc.key";
controls {
inet 127.0.0.1 allow { localhost; } keys { "rndc-key"; };
};
```

Это сообщает серверу параметры секретного ключа для осуществления безопасного обмена. Предоставьте право чтения файла /etc/bind/rndc.key всем учетным записям.

Далее, в описание каждой зоны, которая должна автоматически обновляться, добавьте строку

```
allow-update { key "rndc-key"; };
```

Замечания

Мы описываем конфигурацию, когда и сервер DHCP, и сервер DNS расположены на одном компьютере. Если они разнесены, то данный файл необходимо скопировать вручную.

Если сервер DNS обслуживает внутреннюю зону, то кроме ее обновления нужно не забыть настроить параметры обновления зоны обратного разрешения имен.

В результате описание зоны в файле named.conf.local должно выглядеть примерно так, как в листинге 2.5.

Листинг 2.5

```
zone "имя.ru" {
    type master;
    file "db.имя.ru";
    allow-update { key "rndc-key"; };
};
```

ЗАМЕЧАНИЕ

Обратите внимание, что по умолчанию в Ubuntu пакет AppArmor (см. раздел *"Изоляция приложений"*) запрещает запись в папку /etc/bind. Поэтому файлы для динамически изменяемых зон DNS следует размещать в папке /var/lib/bind.

В файл конфигурации DHCP-сервера (/etc/dhcp3/dhcpd.conf) внесите следующие строки:

```
ddns-update-style interim;
include "/etc/bind/rndc.key";
ddns-domainname "имя.ru";
```

Добавьте *вовнутрь* описания параметров зоны DHCP указания на те зоны DNS, которые должны обновляться при выдаче IP-адреса этого блока. Описание зоны DHCP при этом будет выглядеть примерно так, как в листинге 2.6.

Листинг 2.6

```
subnet 192.168.31.0 netmask 255.255.0.0 {
range 192.168.31.100 192.168.31.200;
# Далее указание на DNS-зоны, которые нужно обновлять
zone 31.168.192.in-addr.arpa. {
primary 192.168.31.1;
key "rndc-key";
}

zone имя.ru. {
primary 192.168.31.1;
key "rndc-key";
}
}
```

После внесения указанных изменений перестартуйте серверы DHCP и DNS. Обязательно проверьте по журналам системы отсутствие ошибок при их загрузке.

При первом запуске этих серверов после настройки динамического обновления будут созданы файлы журналов, в которые будут вноситься оперативные данные о выданных IP-адресах. Через некоторый промежуток времени изменения из файлов журналов будут автоматически переноситься в файлы зон DNS-сервера.

Обслуживание и диагностика неисправностей DNS-сервера

Самый простой способ проверить работоспособность сервера DNS на платформе Windows — включить опции мониторинга на соответствующей вкладке консоли управления. Вы должны получить положительную диагностику при тестировании самого сервера и ответа от сервера, на который настроена пересылка запросов. Для серверов на операционных системах Linux нужно проконтролировать удачный перезапуск демона (должны увидеть сообщение **OK** в строке запуска) и просмотреть журналы системы.

В любом случае журнал сервера DNS является основным источником информации по работоспособности службы. В Ubuntu обычно не нужно включать мониторинг каких-либо дополнительных событий — информации системного журнала вполне достаточно для анализа состояния службы. Протоколирование в Windows службы DNS можно расширить, если установить опции *ведения журнала отладки* на соответствующей вкладке консоли управления сервером DNS. Но пользоваться этой возможностью следует *только* в период отладки. В журнал по умолчанию заносится вся информация (подробно — все данные пакетов), что негативно сказывается на производительности сервера.

Универсальная утилита для получения данных с любого DNS-сервера (и, соответственно, проверки его работоспособности), — это `nslookup`. Она по умолчанию присутствует среди утилит в системах с установленным протоколом TCP/IP.

`nslookup` позволяет вручную получить от сервера DNS такую же информацию, какую системы получают в автоматическом режиме при разрешении имен. Поэтому она часто применяется при диагностике систем.

После запуска утилиты осуществляется подключение к серверу DNS, указанному в настройках сетевого адаптера по умолчанию. Далее в режиме командной строки можно получить ответ на запрос к любому DNS-серверу.

Рассмотрим пример диалога программы nslookup (строки, вводимые пользователем, отмечены знаком > в начале строки). Листинги 2.7–2.9 иллюстрируют работу с программой.

Листинг 2.7

```
>nslookup
Default Server: ack
Address: 192.168.0.10

>server ns.unets.ru
Default Server: ns.unets.ru
Address: 195.161.15.19
```

После запуска программа выдала сообщение, что подключена к DNS-серверу `ack` с IP-адресом 192.168.0.10.

В окне программы `nslookup` была введена команда подключения к DNS-серверу **ns.unets.ru**. В ответ программа сообщила, что подключилась к этому серверу и сообщила его IP-адрес.

Листинг 2.8

```
>uzvt.ru
Server: ns.unets.ru
Address: 195.161.15.19

Non-authoritative answer:
uzvt.ru nameserver = ns.isp.ru
uzvt.ru nameserver = ns.e-burg.ru
ns.e-burg.ru internet address = 195.12.66.65
```

Пользователь ввел запрос на разрешение имени **uzvt.ru**. Утилита сообщила, что сервер **ns.unets.ru** предоставил неавторизованную информацию (Non-authoritative answer) об этом имени. Из того что сервер "вернул" данные NS-записей, следует, что **uzvt.ru** — это домен Интернета, что его серверы имен — **ns.e-burg.ru** и **ns.isp.ru**.

Листинг 2.9

```
>set type=mx
>uzvt.ru
Server: ns.unets.ru
Address: 195.161.15.19

Non-authoritative answer:
uzvt.ru MX preference = 50, mail exchanger =
relay.utnet.ru
uzvt.ru MX preference = 10, mail exchanger = mail.uzvt.ru

uzvt.ru nameserver = ns.isp.ru
uzvt.ru nameserver = ns.e-burg.ru
mail.uzvt.ru internet address = 195.12.67.218
relay.utnet.ru internet address = 195.209.191.2
ns.e-burg.ru internet address = 195.12.66.65
```

Следующими командами пользователь определил, что ему нужна информация о почтовых серверах (`set type=mx`), и вновь указал в запросе тот же домен (**uzvt.ru**). Утилита вернула от сервера DNS ответ, что для домена зарегистрированы два почтовых сервера с разными приоритетами (**mail.uzvt.ru,** приоритет 10 и **relay.utnet.ru**, приоритет 50), и сообщила их адреса. Поскольку **mail.uzvt.ru** имеет меньший приоритет, то именно по этому адресу и будет направляться электронная почта для домена **uzvt.ru**.

> ***Примечание***
>
> Для проверки разрешения имен DNS почтового сервера MS Exchange предназначена специальная утилита, которую необходимо загрузить с сайта Microsoft — `dnsdiag`. Эта программа должна быть запущена на компьютере почтового сервера из папки информационного сервера (IIS). Выходная информация программы полностью соответствует тем данным, которые получает почтовый сервер в процессе разрешения имен. Эта информация может помочь в диагностике проблемных ситуаций, поскольку почтовый сервер Exchange использует собственные настройки для получения данных DNS, а не те, которые используются для сетевого интерфейса системы.

Листинг 2.10 иллюстрирует вывод этой утилиты.

Листинг 2.10

```
c:\WINNT\system32\inetsrv>dnsdiag mail.ru -v 1

mail.ru is an external server (not in the Exchange Org).
```

```
No external DNS servers on VSI. Using global DNS servers.
Created Async Query:
------------
QNAME = mail.ru
Type = MX (0xf)
Flags =  UDP default, TCP on truncation (0x0)
Protocol = UDP
DNS Servers: (DNS cache will not be used)
192.168.0.32
192.168.0.10

Connected to DNS 192.168.0.32 over UDP/IP.
Received DNS Response:
------------
Error: 0
Description: Success
These records were received:
mail.ru    MX    10    mxs.mail.ru
mxs.mail.ru    A    194.67.23.20

Processing MX/A records in reply.
Sorting MX records by priority.

Target hostnames and IP addresses
------------
HostName: "mxs.mail.ru"
194.67.23.20
```

Утилита сообщила параметры MX-записи для домена **mail.ru** и необходимую дополнительную информацию. В примере вызова утилиты после параметра `v` стоит цифра `1`. Это номер виртуального сервера, соответствующего почтовому серверу (может быть иным в зависимости от конфигурации системы).



Глава 3

Обеспечение доступа в Интернет

Современная работа любой организации не представляется возможной без подключения к глобальной сети — Интернету. В подавляющем большинстве случаев провайдеры обеспечивают выделенный канал передачи данных, а подключаемой организации выделяется Ethernet-порт и сообщаются параметры для настройки сетевого интерфейса.

В этом случае в организации необходимо решить две задачи: обеспечить защиту внутренней сети и организовать работу всех компьютеров в Интернете при наличии только одного IP-адреса. Первая задача решается настройкой *межсетевого экрана (брандмауэра)*, вторая обеспечивается за счет технологии NAT. Комплексно решить проблему подключения небольших организаций можно с помощью аппаратного маршрутизатора на основе Linux.

Подключение к Интернету с использованием аппаратного маршрутизатора

Сегодня в продаже доступны различные модели маршрутизаторов, предназначенные для подключения к Интернету небольшой локальной сети. Обычно такие устройства включают в себя:

- один WAN-порт для подключения к Интернету;
- несколько LAN-портов (обычно 4) для подключения локальных компьютеров;
- межсетевой экран с возможностями управления через обозреватель Интернета (по Web-интерфейсу);
- маршрутизатор с возможностями NAT, DHCP-сервера и т. п.

Иными словами, после первоначальной настройки такое устройство будет обеспечивать в локальной сети автоматическое предоставление адресов, предохранять сеть от доступа снаружи, работать в качестве коммутатора.

Существуют модели со встроенной точкой беспроводного доступа, что позволит организовать у себя беспроводное подключение таких устройств, как ноутбуки, медиапроигрыватели с беспроводным доступом и т. п. На рис. 3.1 представлен интерфейс управления одной из моделей маршрутизаторов. Интерфейс локализован, каждая операция снабжена интерактивной справкой, поясняющей возможные параметры настройки. В результате устройство может подготовить к эксплуатации практически любой пользователь.

Как правило, в таких маршрутизаторах встроены простейшие средства фильтрации трафика (например, можно заблокировать сайты по списку), публикации внутренних ресурсов (можно опубликовать в Интернете, например, почтовый сервер организации или FTP-сервер) и т. д.

Примечание

Если планируется ADSL-подключение, то можно сразу приобрести модели модемов, дополнительно включающие в себя как маршрутизатор, так и коммутатор на несколько портов, межсетевой экран и т. п.

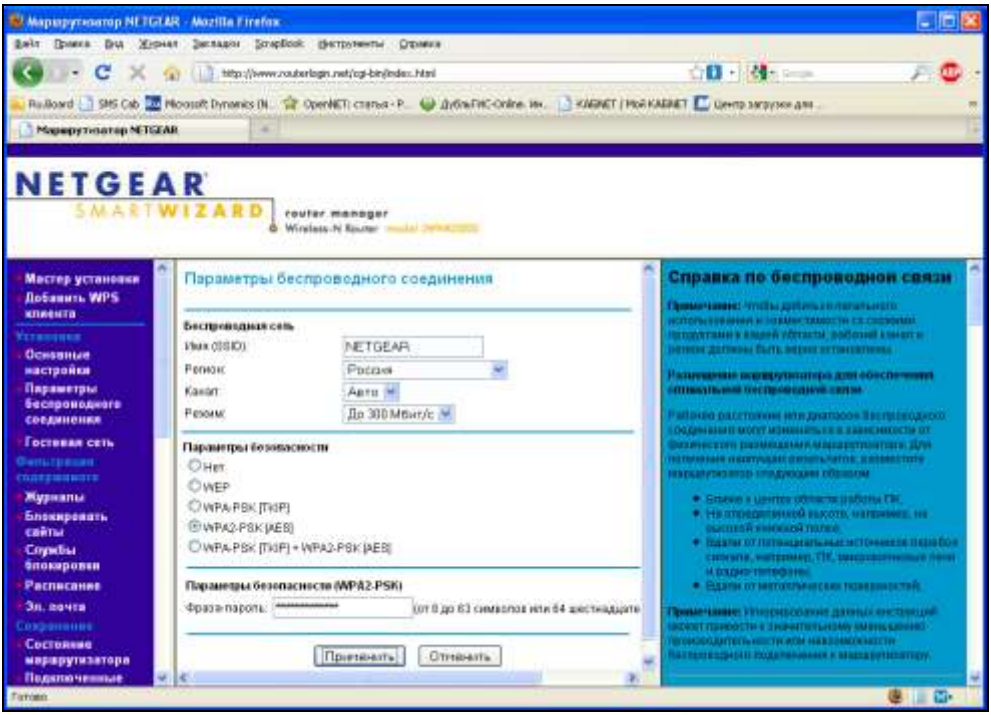


Рис. 3.1. Интерфейс управления маршрутизатором

Такие устройства просты в управлении, весьма надежны (как правило, они реализованы на Linux-платформах) и очень дешевы. В то же время у них есть ряд особенностей, которые не позволяют применять их в более крупных организациях. Отметим некоторые из них:

- маршрутизатор не имеет возможностей контролировать трафик по пользователям и формировать журналы (за длительный период) использования канала Интернета;
- в устройствах нет возможности регулировать полосу пропускания в зависимости от типа трафика и других параметров, что может привести к неудобствам работы в Сети нескольких пользователей (один пользователь может монополизировать канал при определенных условиях);
- отсутствует возможность проксирования трафика, что могло бы как ускорить работу в Интернете, так и сэкономить средства при тарификации по объему;
- дешевые модели маршрутизаторов не имеют средств для создания VPN-подключений между офисами. А модели, в которые такая функциональность включена, по стоимости уже сравнимы с программными решениями на основе простейших компьютеров;
- количество правил (публикации, запрета доступа и т. д.) обычно небольшое, этого достаточно для малых организаций или индивидуальных пользователей, но не перекрывает потребности более крупных организаций.

NAT

Технология трансляции адресов (Network Address Translator, NAT) позволяет осуществить подключение к Интернету практически любого числа компьютеров, задействовав при этом всего лишь один или несколько реальных адресов глобальной сети. Фактически NAT — это IP-маршрутизатор, который способен преобразовывать (транслировать) адреса и номера портов TCP/UDP-пакетов в процессе их пересылки.

Логика работы NAT достаточно проста. При получении от локального компьютера пакета, предназначенного для внешней сети, маршрутизатор пересылает пакет, заменив в нем частный IP-адрес на реальный IP-адрес, выделенный провайдером Интернета, и TCP-порт (или UDP-порт) источника на другой, *перенумерованный* порт. Информация об этом преобразовании сохраняется программой. После получения ответа NAT ищет "в своих записях", для какого локального запроса был выделен соответствующий порт. Если такая информация обнаружена, то NAT пересылает пакет

локальному компьютеру, заменяя в пакете перенумерованный порт на исходный. Если NAT не находит "у себя" записи о перенумерованном порте, то пакет отбрасывается. Таким образом, NAT одновременно является и межсетевым экраном, предотвращающим доступ из внешней сети к внутренним ресурсам.

Сервер NAT заменяет в пакетах адреса источника (назначения), номера портов и пересчитывает контрольную сумму пакета. Для большинства приложений такие изменения не вызывают каких-либо осложнений. Однако некоторые протоколы, например FTP, передают информацию о IP-адресах в своих данных. Поэтому для корректной работы таких протоколов NAT модифицирует и сами TCP-последовательности. Так, в Windows встроены редакторы для протоколов FTP, ICMP, PPTP, NetBIOS поверх TCP/IP. Если в организации на каком-либо компьютере применяется протокол, для которого необходимо внести аналогичные изменения в сам пакет, а соответствующего редактора не предусмотрено в операционной системе, то работа через NAT будет невозможна без использования для такой системы реального адреса. Например, сложности могут возникнуть при работе IP-телефонов по протоколу H323 (внутри пакетов пересылаются адреса устройств). В таком случае либо следует искать специализированное программное обеспечение, либо заказывать дополнительный реальный IP-адрес и транслировать его на внутреннее устройство.

Подключение к Интернету с использованием службы маршрутизации и удаленного доступа серверов Windows

NAT в серверах Windows реализован в службе маршрутизации и удаленного доступа.

Для настройки NAT после установки данной службы в оснастке управления следует добавить интерфейсы подключения к Интернету и локальной сети к протоколу маршрутизации NAT, для чего на вкладке **Общие** свойств интернет-интерфейса установить переключатель **Общий интерфейс подключен к Интернету** (Public Interface connected to the Internet), а для интерфейса локальной сети — **Частный интерфейс подключен к частной сети** (Private interface connected to private network). При наличии одного адреса подключения к Интернету нужно установить переключатель **Преобразовать TCP/UDP-заголовки** (Translate TCP/UDP headers) для свойств интернет-интерфейса.

Если необходимо опубликовать некоторые ресурсы локальной сети в Интернете, то следует создать соответствующие правила в оснастке NAT, которые определят, на какой частный адрес пересылать заданные протоколы.

NAT вместе со встроенным межсетевым экраном сервера является вполне надежным и функциональным вариантом подключения организации к Интернету.

Такой алгоритм работы достаточно эффективен и подходит в большинстве случаев. Однако он может приводить к неработоспособности отдельных функций программ, если они активизируются внешними запросами. Например, почтовый клиент MS Outlook при работе с сервером MS Exchange использует протокол RPC. Пройдя регистрацию на почтовом сервере, клиент находится в состоянии ожидания сигнала о приходе новой почты. Поскольку инициатором такого сигнала является не клиент, а внешняя система, то эти пакеты будут отброшены. Поэтому в данном примере клиент не будет получать автоматические сообщения о приходе новой почты, хотя сможет принимать и отправлять сообщения по команде пользователя.

Совместное использование интернет-подключения

Самый простой способ подключения к Интернету локальной сети организации на основе Windows, который не требует установки и настройки никаких дополнительных программ, — это использование *совместного подключения к сети Интернета*. Такая возможность предусмотрена уже с Windows 2000 Professional (операционной системы для рабочих станций).

Организовать совместное подключение к Интернету можно для любого варианта подключения к Сети (через модем или локальную сеть). Соответствующую настройку легко выполнить аналогично описываемому далее примеру подключения к Интернету с помощью модема.

Если компьютер имеет настроенное подключение к Интернету, то в папке задач **Сетевые подключения** есть значок, соответствующий данному подключению. Щелкните по нему правой кнопкой мыши и выберите команду **Свойства**. На вкладке **Дополнительно** в опции включения совместного использования доступа в Интернет поставьте соответствующий флажок.

При выборе совместного подключения IP-адрес сетевой карты компьютера автоматически изменяется на 192.168.0.1. Компьютер становится для других членов локальной сети сервером DHCP (диапазон 192.168.0.*x*) и сервером DNS. Поэтому на остальных компьютерах протокол TCP/IP нужно настроить с параметрами по умолчанию, которые предполагают автоматическое получение всех необходимых данных.

Публикация компьютеров в Интернете при совместном использовании подключения

Для публикации внутренних ресурсов в Интернете при совместном подключении достаточно создать соответствующее правило.

Покажем на примере, как выполнить в данном случае публикацию внутреннего FTP-сервера в сети Интернет.

- Откройте свойства соединения с Интернетом, для которого организовано совместное использование. Перейдите на вкладку **Дополнительно**. Нажмите кнопку **Настройки**. Появится окно с перечнем типовых сервисов Интернета, доступ к которым во внутреннюю сеть можно осуществить через данное подключение.
- Выберите нужный сервис и отметьте флажок, разрешающий его публикацию в Интернете. Появится окно, в котором нужно указать компьютер, где в локальной сети работает данный сервис. Обратите внимание, что можно указать как имя, так и IP-адрес компьютера. Если отдается предпочтение IP-адресу, то целесообразно прописать его на соответствующем компьютере статически, чтобы он не поменялся впоследствии (поскольку стандартно при совместном использовании подключения к Интернету адреса компьютерам выдаются динамически и могут изменяться). После завершения операций закройте все окна настройки, нажимая кнопку **OK**.

В результате данных настроек на FTP-запрос, поступающий из внешней сети на компьютер, непосредственно подключенный к Интернету, будет "отвечать" не этот компьютер, а указанный вами в описанных ранее операциях.

Таким способом можно настроить публикацию в Интернете любых сервисов, которые реализуются на локальных компьютерах сети. Если нужного сервиса нет в стандартном списке, вы можете его добавить, воспользовавшись соответствующей опцией. При введении нового сервиса необходимо указать тип протокола и номера портов.

Главная проблема, которая будет подстерегать вас при подобном решении, — это возможное отсутствие статического IP-адреса компьютера, подключенного к Интернету. Иными словами, если вы имеете в локальной сети информационный сервер и реализуете сеансовое подключение к Интернету, то его реальный адрес подключения будет меняться при каждом сеансе связи с провайдером, что, естественно, не позволит кому-либо обратиться к опубликованным ресурсам. В таком случае вам необходимо воспользоваться возможностями динамического DNS (динамические имена доступны на серверах **http://www.dyndns.com/**, **http://www.dtdns.com/** и др.; достаточно выполнить свободную регистрацию по правилам соответствующей службы).

Ограничения совместного использования подключения к Интернету

Из технических особенностей реализации совместного подключения к Интернету вытекают ограничения его применения.

В сети организации часто необходимо вести контроль доступа к ресурсам Интернета, иметь возможность выборочно предоставлять доступ одним сотрудникам и запрещать другим, создавать списки запрещенных сайтов и т. п. Эти настройки не выполнить при данном способе подключения к Интернету.

Кроме того, в локальной сети допустим только диапазон адресов 192.168.0.0/24, причем адрес 192.168.0.1 может быть только у компьютера, обеспечивающего совместное подключение к Интернету. Данное ограничение также осложняет задачу настройки безопасного соединения между несколькими площадками организации (или настройку VPN-подключения пользователя к ресурсам другой организации в случае совпадающих диапазонов адресов локальных сетей).

Подключение к Интернету с помощью Microsoft ISA Server

В составе семейства серверных решений от Microsoft есть специализированный сервер для обеспечения безопасного подключения организации к Интернету — Microsoft Internet Security and Acceleration Server.

Сервер включает в себя как межсетевой экран с большим количеством настроек, так и прокси-сервер для кэширования трафика. В выпуске Enterprise серверы ISA могут работать в составе массива с распределением трафика на несколько каналов доступа, с хранением конфигурации на выделенной системе, с балансировкой нагрузки и т. д. Более дешевый, стандартный выпуск, представляет собой вариант одиночного межсетевого экрана и прокси.

Настройка Microsoft ISA Server не представляет особых сложностей. Все операции выполняются с помощью мастеров в графическом режиме в оснастке управления (рис. 3.2). А правила ничем не отличаются от традиционных для межсетевых экранов: нужно указать, какой протокол с каких компьютеров, кому, куда и по какому расписанию необходимо разрешить или запретить.

Опишем основные моменты, которые администраторы, начинающие работу с ISA-сервером, не всегда принимают во внимание.

- Понятие *все* протоколы или *весь* трафик в ISA-сервере описывают только те протоколы, которые явно определены в параметрах сервера. Иными словами, если протокол не описан, то он и не будет пропущен, если вы включите разрешение для всех протоколов.

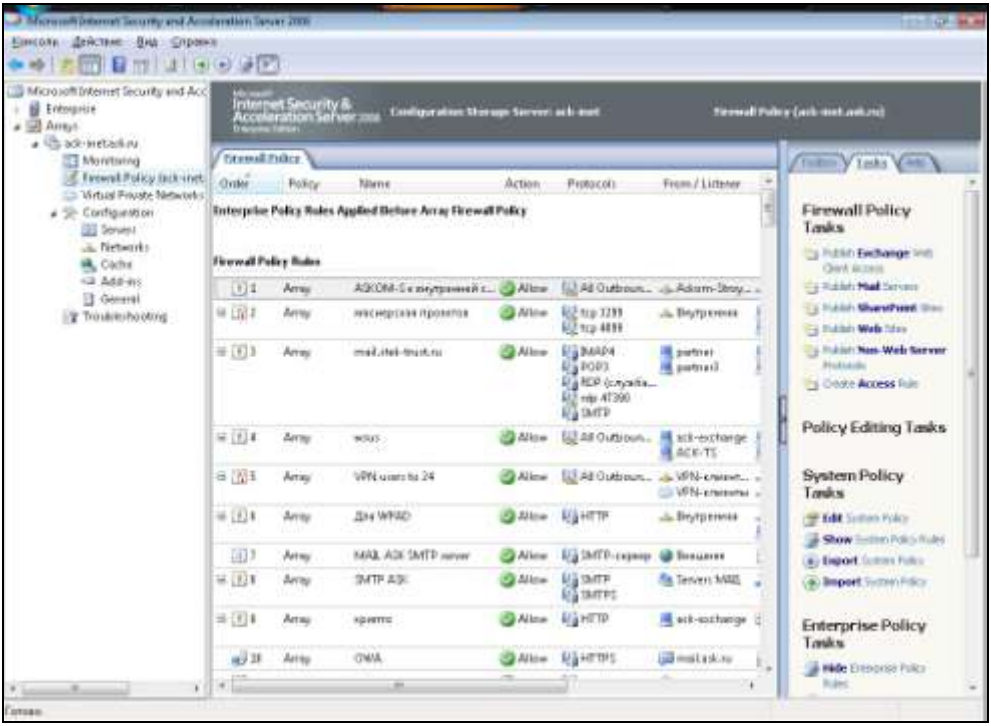


Рис. 3.2. Оснастка управления сервером Microsoft ISA

- Правила в ISA-сервере проверяются последовательно так, как они записаны. Поэтому, если вы хотите что-либо запретить всем, а разрешить конкретным пользователям, то более "верхним" должно быть правило разрешения, а за ним следовать правило запрета. Другой момент, который не всегда учитывается. Правила, в которых действие разрешено для всех пользователей, должно быть расположено выше правила, в котором этот протокол разрешается или запрещается конкретному пользователю. В противном случае сервер будет сначала запрашивать аутентификационные данные для проверки пользователей, что сделает невозможным анонимный пропуск протокола.
- Обратите внимание на наличие системных правил в сервере. Например, этими правилами разрешен неконтролируемый обмен с серверами Microsoft. Конечно, такая настройка помогает службам обновления, но часто наличие подобной "бреши" упускается из виду администраторами.
- Сервер Microsoft ISA рекомендуется в тех случаях, когда необходим контроль работы пользователей на основе их членства в группах безопасно-

сти домена. В то же время, не все приложения корректно могут передавать аутентификационные данные на сервер. Конкретные советы зависят от установленных приложений. Часто проблемы можно решить, разрешив стандартный вариант аутентификации (по умолчанию включен только интегрированный; настройка производится на вкладке **Web Proxy** окна свойств внутренней сети). В крайнем случае вам придется разрешить анонимную работу для соответствующих протоколов.

- На рабочих местах необходимо устанавливать клиент Microsoft ISA Server. Его версию лучше загрузить с сайта Microsoft. Но некоторые приложения не работают при наличии такого клиента. Например, автор встречался с подобной ситуацией при настройке программного IP-телефона и клиентских программ работы со счетами в банке. В этом случае либо необходимо деинсталлировать клиента, либо в его дополнительных настройках отключить клиента для конкретного приложения.
- Еще один класс приложений, для которых лучше отказаться от данного сервера — это задачи IP-телефонии и IP-видео. Часто для этих приложений необходим специальный редактор для пакетов при использовании NAT, которым сервер ISA не обладает.

Настройка прокси-сервера

В Microsoft ISA Server практически отсутствуют возможности настройки параметров кэширования трафика. Единственный доступный параметр — это объем дискового пространства, отводимого для хранения кэша.

Анализаторы логов

Microsoft ISA Server позволяет протоколировать работу в различных форматах: от SQL-сервера до записей в текстовый файл. Эту возможность следует включить в настройках сервера при необходимости. По умолчанию выполняется запись в базу SQL Server Express, причем журнал каждого дня сохраняется в отдельной базе. Штатные средства анализа журналов Microsoft ISA Server позволяют увидеть только общие параметры: суммарный трафик, самых потребляющих пользователей, распределение нагрузки в течение суток и т. п. При необходимости специального анализа следует либо найти соответствующие программы в Сети (в Интернете представлено много продуктов для анализа журналов таких серверов), либо просто собственными силами написать сценарии обработки исходных журналов.

Поиск причин запрета трафика

В Microsoft ISA Server имеется удобный механизм онлайнового контроля работы сервера — журнал реального времени (рис. 3.3).

Достаточно выбрать необходимые фильтры (при работе организации вычленить проблему без фильтров практически невозможно) и включить просмотр. На экране вы увидите пакеты, которые удовлетворяют заданным условиям фильтрации, и причины, по которым пакет пропущен или нет. Обычно следует обращать внимание на название правила, которое не пропустило пакет, и на тип отношения сетей (при наличии нескольких настроенных групп сетей в Microsoft ISA Server). После того как причины будут найдены, устранить их останется только делом администратора.

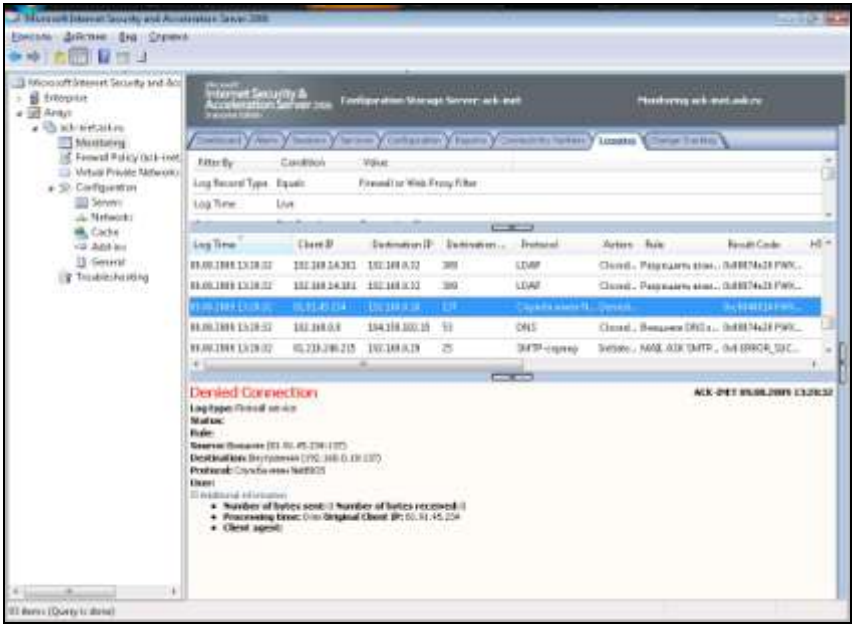


Рис. 3.3. Мониторинг работы Microsoft ISA Server в реальном режиме времени

Подключение к Интернету с использованием серверов Ubuntu

Возможностей настройки межсетевого экрана и прокси-сервера на Linux-компьютерах несравнимо больше, чем на Windows-системах. В Linux для подключения к Интернету обычно реализуют посредством межсетевого экрана iptables. Функционал NAT встроен в этот пакет.

Настройка iptables несколько неудобна для обычного пользователя из-за большой функциональности, поэтому в Ubuntu для управления параметрами межсетевого экрана применяется программа ufw, имеющая упрощенный интерфейс настройки и вполне достаточная для защиты конкретного хоста (компьютера). Если же вы настраиваете доступ в Интернет для офиса, то необходимо задействовать возможности iptables, которые также будут описаны в этой главе.

Настройка ufw

После установки системы межсетевой экран в Ubuntu отключен. Включить его можно командой

```
sudo ufw enable
```

Состояние межсетевого экрана (включен или выключен) можно увидеть, выполнив команду `sudo ufw status`.

Если вы управляете сервером удаленно, то активизация межсетевого экрана приведет к потере с ним связи. Поэтому необходимо включить межсетевой экран, предварительно создав правило, разрешающее удаленное управление. Если у вас подключение по ssh, то для включения межсетевого экрана выполните команду `sudo ufw allow proto tcp from any to any port 22` перед командой `sudo ufw enable`.

"Хорошим вкусом" для системных администраторов является первоначальный запрет на все подключения с последующим открытием нужных протоколов. Для этого служит команда выбора правил по умолчанию:

```
sudo ufw default deny
```

Правила доступа в ufw создать достаточно легко. Следует указать только нужное действие (разрешение или запрет: allow/deny) и параметры протокола. Например, команда `sudo ufw allow 53` разрешит доступ к компьютеру по портам 53 (используется при работе DNS). Вместо указания портов можно писать имена служб (система использует параметры служб, перечисленные в файле /etc/services, просмотрев его, вы можете уточнить допустимые названия), например, `sudo ufw allow smtp`.

При необходимости максимально точно указать параметры фильтрации нужно применять следующий синтаксис:

```
sudo ufw allow|deny proto <протокол> from <источник> port <порт> to
<назначение> port <порт>
```

В качестве протоколов обычно выбирают либо `tcp`, либо `udp`; в качестве источника/назначения можно указывать конкретные IP-адреса, подсети (например, 192.168.0.0/24) или `any` для любого назначения.

Межсетевой экран iptables

Команды настройки iptables потребуются в тех случаях, когда вы предполагаете задействовать межсетевой экран данного сервера для обеспечения работы с Интернетом всего офиса или же включить какие-либо специальные возможности, не реализуемые программой ufw.

Последовательность обработки пакета (таблицы)

Самое сложное при работе с iptables заключается в том, чтобы точно уяснить правила обработки пакетов этой программой. Любой пакет на каждом сетевом интерфейсе компьютера несколько раз анализируется на соответствие некоторым условиям. При удовлетворении условиям к пакету применяется соответствующее правило, и дальнейший анализ на данном этапе не производится. Если ни одно из правил не содержит условий, соответствующих пакету, к нему применяются правила по умолчанию. Подобные наборы правил носят названия *таблиц*.

Существует три таблицы правил: *filter* — основная таблица, *nat* — для пакетов, создающих новое подключение (можно менять адреса источника и назначения пакета), и *mangle* — для пакетов специального типа.

Межсетевой экран может анализировать один и тот же пакет несколько раз на различных этапах его обработки. Так, у таблицы filter можно создавать правила, применяемые при *приеме* пакетов данным интерфейсом (INPUT), при *передаче* пакета через этот же интерфейс (через который он принят) — OUTPUT и при *пересылке* пакетов на другой сетевой интерфейс (FORWARD). Для таблицы nat предусмотрены варианты PREROUTING (при приеме пакета данным интерфейсом), OUTPUT (применяется к пакетам *перед* маршрутизацией через данный интерфейс) и POSTROUTING (правило применяется перед тем, как пакет будет передан с данного интерфейса). Таблица mangle имеет только два варианта — PREROUTING и OUTPUT. Их смысл аналогичен одноименным цепочкам таблицы nat.

На рис. 3.4 показана последовательность применения таблиц обработки для пакетов, как поступающих на компьютер из сети, так и отсылаемых из компьютера во внешнюю сеть.

Для большей наглядности при составлении правил можно создавать собственные (пользовательские) цепочки. Смысл пользовательских цепочек состоит в том, что определенный блок анализа и обработки пакетов оформляется отдельной частью правил. После чего в заданном месте обработки управление передается на такую пользовательскую цепочку, а потом возвращается назад. Таким способом проще анализировать большой объем правил.

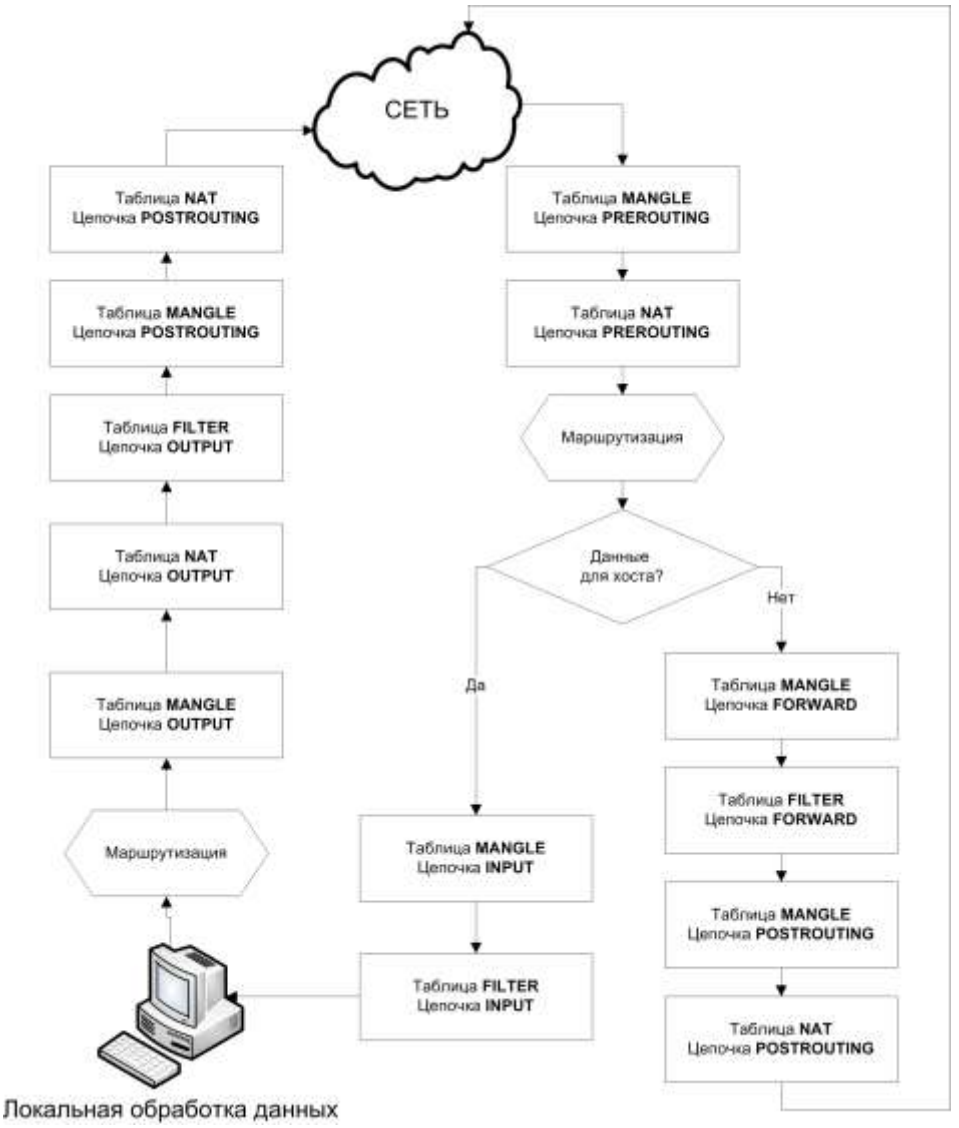


Рис. 3.4. Последовательность применения правил обработки пакета в iptables

Использование iptables в Ubuntu

Примечание

Для использования iptables демон ufw не должен быть запущен (sudo ufw disable). Иначе разобраться в совместном действии правил, которые подгружаются ufw и создаются явно командами iptables, будет практически невозможно.

Ubuntu не содержит сценарий автозапуска iptables, поэтому в системе отсутствуют соответствующие файлы настроек и, например, выполнить команду сохранения конфигурации межсетевого экрана (как это делается в других версиях Linux) не получится. Чтобы применить заданные настройки межсетевого экрана iptables при каждом запуске системы, вам следует:

- создать необходимые правила фильтрации трафика с использованием команды iptables;
- экспортировать настройки в какой-либо файл командой iptables-save;
- настроить автоматическую загрузку настроек из этого файла при каждом запуске Ubuntu.

Автоматическую загрузку проще всего сделать через возможности настройки конфигурации сетевого интерфейса путем добавления строк, описывающих действия, которые следует выполнить *перед* включением сетевого интерфейса и при его *отключении*. Для этого достаточно настроить и сохранить действующие на данный момент правила (например, командой `sudo bash -c "iptables-save > /etc/iptables.rules"`), после чего открыть для редактирования файл /etc/network/interfaces и добавить в конец блока настроек, описывающих сетевой интерфейс, следующие строки (вторая строка обеспечивает автоматическое сохранение настроек конфигурации при выключении системы):

```
pre-up iptables-restore < /etc/iptables.rules
post-down iptables-save -c > /etc/iptables.rules
```

Обратите внимание, чтобы файл /etc/iptables.rules существовал перед перезагрузкой системы, в противном случае сетевой интерфейс не будет включен.

Правила iptables

К пакетам, которые будут удовлетворять условиям фильтров, можно применить несколько действий. Они могут быть пропущены (вариант ACCEPT), удалены с сообщением источнику об ошибке передачи данных (REJECT), просто уничтожены без оповещения (DROP). Существует также возможность настройки и применения пользовательского варианта обработки (QUEUE).

Обратите внимание, что правила исполняются последовательно; если пакет удовлетворяет условиям, то к нему применяются правила, заданные в этой строке, и цепочка дальше не обрабатывается. Поэтому порядок правил очень важен. Обратите особое внимание, куда вы добавляете новое правило: в начало списка (параметр `-I`) или в его конец (параметр `-A`).

В общем виде команда редактирования правил межсетевого экрана выглядит следующим образом:

```
iptables [-t table-name ] command chain-name parameter-1   option-1
parameter-n option-n
```

Параметр `table-name` позволяет выбрать используемую таблицу. `Command` определяет выполняемое действие: добавление или исключение правила. `Chain-name` — это название соответствующего правила. Далее следует набор пар `parameter-n option-n`, которые, собственно говоря, и определяют конкретные действия программы.

Если в команде опущено название таблицы, то правила добавляются в таблицу *filter*.

Команды

В табл. 3.1 приведем часть команд (полный перечень можно отобразить в справке iptables).

Таблица 3.1. *Команды iptables*

Команда	Действие
`-L`	Выводит список действующих правил (для отображения подробного списка используйте параметр `-v`)
`-F`	Удаляет цепочку, имя которой приведено далее в качестве параметра. Если имя не указано, то *удаляет все правила* межсетевого экрана
`-A`	Добавляет новое правило в *конец* списка
`-D`	Удаляет правило в соответствии с указываемым далее номером
`-I`	Добавляет правило и размещает его по списку с указанным номером. Если номер правила не указан, то оно размещается *первым*
`-P`	Определяет правило по умолчанию для соответствующей цепочки

Примечание

Вместо параметров `-A`, `-D`, `-I`, `-R`, `-L`, `-F` при написании команд можно указывать, соответственно, `--append`, `--delete`, `--insert`, `--replace`, `--list`, `--flush` (обратите внимание на то, что указывается два тире).

Параметры

В табл. 3.2 укажем наиболее часто используемые параметры (полный перечень отображается в справке команды).

Таблица 3.2. *Параметры команд iptables*

Параметр	Назначение
`-d`	Назначение пакета. Можно указывать имя хоста, IP-адрес или подсеть (либо как 192.168.0.0/255.255.255.0, либо как 192.168.0.0/24)

Таблица 3.2 *(окончание)*

Параметр	Назначение
`-s`	Источник пакета. Синтаксис аналогичен параметру `-d`. Заметим, что символы `0/0` определяют *все сети*
`-f`	Правило будет применено только к фрагментированным пакетам (символ `!` после данного параметра определяет область применения для нефрагментированных пакетов)
`-i`	Интерфейс (eth0, ppp0 и т. п.). Если параметр опущен, то правило будет применяться ко всем интерфейсам. Знак `+` используется в качестве маски: `eth+` обозначает *все* интерфейсы Ethernet
`-o`	Выходной интерфейс (в правилах с OUTPUT и FORWARD)
`-j`	Определяет правило (ACCEPT, DROP, QUEUE, …). Применение без указания опции используется в правилах с подсчетом пакетов (каждый пакет увеличивает значение счетчика на единицу)
`-p`	Протокол IP: обычно указывают icmp, tcp, udp или all (для обозначения любого протокола). Перечень протоколов можно уточнить по содержимому файла /etc/protocols

Опции

В табл. 3.3 приведены наиболее распространенные опции (полный перечень отображается в справке команды).

Таблица 3.3. *Опции команд iptables*

Опция	Назначение
`--dport`	Порт назначения. Можно указывать диапазон (по принципу `--dport 3000:3200`) и применять символ `!` для указания исключения (*кроме указанных портов*). Допустимый диапазон значений 0–65535
`--sport`	Порт источника. Синтаксис аналогичен `--dport`
`--syn`	Тип пакетов — SYN. Можно использовать символ `!` для указания всех остальных пакетов
`--tcp-flags`	Определяет пакеты со специальными флагами: ACK, FIN, PSH, RST, SYN и URG. Допускаются обозначения ALL и NONE
`--tcp-option`	Определяет дополнительные опции пакетов протокола IP
`--icmp-type`	Имя или номер протокола ICMP. Допустимые имена можно вывести на экран командой `iptables -p icmp -h`

Некоторые опции могут присутствовать при указании в командной строке iptables дополнительно загружаемых модулей. Так, при загрузке модуля limit (`-m n limit`) можно указывать максимальное число пакетов за единицу времени (например, `--limit 5/hour` определяет максимально 5 пакетов данного типа в час). Модуль state позволяет использовать в правилах состояние соединения: `--state ESTABLISHED`, `--state INVALID`, `--state NEW`, `--state RELATED`. Модуль mac позволяет включить в правила проверку MAC-адресов (опция `--mac-source`). Полный список дополнительных модулей доступен в справочной подсистеме.

> ***Замечание***
>
> В правиле, которое служит для лимитирования числа пакетов, должно присутствовать два параметра: `--limit`, определяющий, как быстро будет уменьшаться счетчик максимально допустимого числа пакетов, и `--limit-burst`, который указывает на максимальное значение пакетов, для которого это правило будет выполняться. Иными словами, правило будет выполняться, пока число пакетов в счетчике будет меньше значения `limit-burst`, которое автоматически уменьшается со скоростью `limit`. Если параметр `limit-burst` не указан, то применяется значение по умолчанию, равное 5. Правила лимитирования необходимо применять парой: первое правило будет пропускать пакеты, пока счетчик не превысил заданного значения, а второе — уничтожать пакеты, скорость поступления которых привела к превышению показателя лимита.

Настройка NAT

Для работы NAT необходимо включить маршрутизацию в ядре Linux. Делается это командой

```
sudo bash -c "echo 1 > /proc/sys/net/ipv4/ip_forward"
```

Однако эта операция не сохранит настройки *после перезагрузки* сервера. Поэтому, если вы собираетесь включить маршрутизацию постоянно, отредактируйте файл /etc/sysctl.conf. Найдите в нем строчку net.ipv4.ip_forward=1 и удалите в ней комментарий (символ `#` в начале строки). Чтобы эта настройка вступила в силу, нужно перезагрузить систему (или до перезагрузки включите маршрутизацию согласно предыдущему варианту).

В iptables существует два варианта правил настроек при использовании NAT: для исходящего трафика (SNAT) и входящего (DNAT, иными словами, это публикация внутренних ресурсов сети наружу).

Существует упрощенный вариант правил, предназначенный специально для работы с динамическим внешним адресом (частый случай при dial-up-подключении к Интернету). При этом для включения NAT достаточно добавить следующее правило:

```
iptables --table nat --append POSTROUTING --out-interface eth0
-j MASQUERADE
```

Замечания

Кроме этого правила, если по умолчанию вы запретили пересылку, следует разрешить получение пакетов из локальной сети по внутреннему интерфейсу, например, командой `iptables --append FORWARD --in-interface eth1 -j ACCEPT`.

В этом примере и последующих предполагается, что `eth0` — это интерфейс Интернета, `eth1` — интерфейс, смотрящий в локальную сеть.

Обратите внимание, что настройки POSTROUTING не отражаются в консоли при исполнении команды `sudo iptables -L` без указания таблицы. Вы увидите по этой команде только правила, включенные в таблицу *filter*. Для того чтобы увидеть настройки работы в NAT, необходимо не забыть указать имя таблицы:

```
sudo iptables -L -t nat
```

Указанный вариант настройки NAT не рекомендуется для серверов, у которых точно известна настройка внешнего интерфейса. Хороший стиль настройки iptables — указание максимально точных параметров, чтобы исключить любые неконтролируемые пути доступа в систему. Поэтому для настройки NAT целесообразно воспользоваться следующим синтаксисом:

```
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 1.2.3.4
```

В этом примере `1.2.3.4` — условно принят как внешний IP-адрес сервера.

Чтобы обеспечить пересылку пакетов, поступающих на внешний IP-адрес сервера, на какой-либо адрес из внутренней сети, можно задать команду:

```
iptables -t nat -A PREROUTING -d 1.2.3.4 -p tcp --dport 80 -j DNAT
--to 192.168.1.1
```

В команде можно указывать протоколы, порты и т. п. Например, следующая команда обеспечит публикацию во внешней сети внутреннего почтового сервера:

```
iptables -t nat -A PREROUTING -p tcp -i eth0 --destination-port 25
-j DNAT --to-destination 192.168.1.10
```

Кроме этого, существует возможность преобразования (перенаправления) пакетов с одного порта на другой, например, такой командой:

```
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT
--to-port 3128
```

Эта команда отсылает пакеты, предназначенные для адреса 80 (WWW-сервер), на порт 3128. Такая настройка часто встречается при использовании "прозрачного" прокси.

Очистка всех правил iptables

Перед началом настройки межсетевого экрана целесообразно очистить все ранее созданные правила. Следующие команды удаляют все правила межсе-

тевого экрана (первая команда — в цепочке *filter*, следующие — в явно указанных цепочках):

```
iptables -F
iptables -t nat -F
iptables -t mangle -F
```

Эти команды удаляют пользовательские правила в соответствующих цепочках.

```
iptables -X
iptables -t nat -X
iptables -t mangle -X
```

Назначение политик по умолчанию

В большинстве случаев политики по умолчанию настраивают как запрет для входящего трафика и как разрешение для исходящего:

```
iptables -P OUTPUT ACCEPT
iptables -P INPUT DROP
iptables -P FORWARD ACCEPT
```

Конечно, для более точной настройки следует установить все политики по умолчанию в DROP. Однако такая настройка более трудоемка и предполагает знание администратором параметров служб системы для создания к ним соответствующих правил доступа. Первоначально вполне достаточно конфигурации, описанной в следующем примере. В дальнейшем, по мере приобретения опыта, администратор сможет создавать все более "жесткие" правила доступа, настраивая не один, а несколько рубежей сетевой защиты сервера.

Пример настройки iptables

Чтобы сервер мог выполнять функции межсетевого экрана, необходимо добавить несколько команд:

- разрешение приема трафика по интерфейсу локальной сети;
- разрешение приема трафика локальным интерфейсом (для обеспечения работы сетевых служб сервера);
- разрешение приема из внешней сети ответов на исходящий трафик (состояние пакетов ESTABLISHED и RELATED);
- команду включения NAT (если внутренняя сеть использует механизм трансляции адресов).

Такой настройке соответствует цепочка команд, приведенная в листинге 3.1.

Листинг 3.1

```
iptables -P OUTPUT ACCEPT
iptables -P INPUT DROP
iptables -P FORWARD ACCEPT
iptables -A INPUT -i eth0 -p ALL -m state --state ESTABLISHED,
RELATED -j ACCEPT
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -i eth1 -j ACCEPT
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

В результате мы получили простейшую рабочую конфигурацию iptables. На практике правила iptables необходимо составлять более конкретно, чтобы заблокировать потенциально нежелательный трафик. Например, вместо разрешения приема пактов из любых сетей на внутренний интерфейс сервера доступ можно ограничить только конкретным диапазоном:

```
iptables -A INPUT -s 192.168.10.0/255.255.255.0 -i eth1 -j ACCEPT
```

Опытные администраторы составляют еще более конкретные правила, явно описывая в правилах весь разрешенный трафик (например, почтовые протоколы, протоколы просмотра Web, работы в ICQ и т. д.).

Пользовательские цепочки команд

Пользовательские цепочки служат для большей удобочитаемости правил фильтрации пакетов (листинг 3.2).

В этом примере сначала создается пользовательская цепочка, в которой планируется выполнить ряд обработок. Это протоколирование пакетов из сети 192.168.1.0/24 с последующим их уничтожением. В этой цепочке присутствуют только две команды фильтрации, а третья команда фактически возвращает управление в исходную точку.

Команды фильтрации на межсетевом экране будут исполняться в такой последовательности. Сначала команда цепочки `INPUT` (`iptables -A INPUT -p ALL -i eth0 -m state...`), после выполнения первой команды пакеты передадутся в цепочку `my_packets`, после выполнения трех команд этой цепочки следующей командой будет правило уничтожения всех широковещательных пакетов (последнее правило данного примера).

Листинг 3.2

```
iptables -N my_packets
iptables -A my_packets -p ALL -i eth0 -s 192.168.1.0/24 -j LOG
--log-prefix "bad_network "
iptables -A my_packets -p ALL -i eth0 -s 192.168.1.0/24 -j DROP
iptables -A my_packets -p ALL -j RETURN
iptables -A INPUT -p ALL -i eth0 -m state --state ESTABLISHED,
RELATED -j ACCEPT
iptables -A INPUT -p ALL -i eth0 -j my_packets
iptables -A INPUT -m pkttype --pkt-type broadcast -j DROP
...
```

Некоторые полезные функции iptables

Ловушки

У специалистов информационной безопасности существует такой метод противодействия атакам, как создание ловушек. Ловушка — это порт, с которым можно установить соединение, но закрыть его не получится. В результате соединение будет завершено только по тайм-ауту (обычно этот период составляет более 10 мин), атакующая система все это время будет ожидать ответов и расходовать ресурсы на поддержание соединения.

Например, таким образом можно ввести злоумышленника в заблуждение, если поставить ловушки на порты NetBIOS:

```
iptables -A INPUT -p tcp -m tcp -m mport --dports 135,139 -j TARPIT
```

Фильтрация по содержимому пакета

В правилах можно задать критерий нахождения заданной последовательности символов в передаваемой информации. Причем вы можете анализировать как служебные данные пакетов, так и передаваемые в нем данные. Подобным способом можно, например, запретить передачу определенного типа файлов, если указать в критерии характерные для них последовательности символов. Многие форматы можно однозначно определить по служебным заголовкам, содержащимся в файлах. Такие последовательности несложно найти в Интернете.

Предупреждение атак

Некоторые сетевые атаки, основанные на отказе в обслуживании, можно пресечь, если на межсетевом экране включить лимитирование пропуска опреде-

ленных пакетов. Следующие команды вводят ограничение "один пакет в секунду" (предупреждают атаку "Syn-flood") и запрещают атаку "Ping of death":

```
iptables -A FORWARD -p tcp --syn -m limit --limit 1/s -j ACCEPT
iptables -A FORWARD -p icmp --icmp-type echo-request -m limit
--limit 1/s -j ACCEPT
```

Часто осуществляют фильтрацию пакетов с "плохим" состоянием:

```
iptables -A INPUT -p ALL -m state --state INVALID -j DROP
```

или новых пакетов, но без установленного признака `syn`:

```
iptables -A INPUT -p TCP ! --syn -m state --state NEW -j DROP
```

Открытие портов по специальным запросам

Iptables позволяет выполнить такие специфические настройки, как открытие порта после принятия определенной последовательности пакетов.

Идея заключается в том, что в настройках межсетевого экрана разрешаются установленные соединения, а они открываются только после получения определенной последовательности входных пакетов. Таким способом легко маскируется доступ к серверу Интернета: злоумышленник не сможет никак даже начать подключение, если не знает определенного алгоритма входа. В следующих ссылках вы найдете некоторые варианты реализации такой технологии:

http://www.opennet.ru/base/sec/port_knocking.txt.html,

http://gentoo-wiki.com/HOWTO_Port_Knocking

и т. п.

Отладка iptables

Для настройки межсетевого экрана используют протоколирование iptables. Для этого достаточно создать правило, описывающее необходимые фильтры, и применить к нему действие `LOG` (`-LOG`). Информация о пакетах, которые будут удовлетворять такому правилу, запишется в системный журнал. Например, если последним правилом в iptables поставить протоколирование всех пакетов:

```
iptables -A INPUT -j LOG
```

то в системном журнале появятся сообщения обо всех пакетах, которые достигли этого этапа и впоследствии уничтожены, так как политика по умолчанию для таблицы INPUT установлена в DROP.

Существует несколько параметров, которые пригодны в режиме отладки. Наибольший практический интерес представляет ключ `--log-prefix "метка"`, добавляющий к описаниям пакетов символы `метка`. Это позволяет легко

отфильтровать сообщения от iptables в системном журнале, который на рабочих серверах пополняется с достаточно высокой скоростью:

```
tail –f /var/log/syslog | grep метка
```

Задавая различные метки, команды протоколирования можно поместить в различные цепочки iptables и быстро найти ошибки настройки, наблюдая за журналом одновременно в нескольких консолях системы.

Настройка VPN-подключения к интернет-провайдеру

Интернет-провайдеру важно быть уверенным, что он предоставляет доступ именно тем пользователям (организации), с которыми заключен договор. Если в одном здании расположено несколько организаций, подключенных к единой физической сети, то для авторизации доступа в Интернет в таких случаях активно используется технология VPN. Канал Интернета будет открыт только в том случае, если на сервере провайдера успешно завершится аутентификация пользователя.

> ***Примечание***
>
> Описанным далее способом можно осуществлять не только подключение к Интернету, но и к сети удаленного офиса. Следует только настроить правильные таблицы маршрутизации, чтобы сервер знал, какие пакеты отправлять по такому соединению. Единственное отличие состоит в том, что провайдеры не шифруют трафик, а при подключении к удаленному офису эта опция должна быть настроена обязательно.

Настройка такого типа подключения может быть выполнена и средствами Microsoft, но в этом случае — по опыту автора — возможны проблемы с маршрутизацией трафика между сетями офисов. Более рационально настроить такие подключения с использованием возможностей Linux-систем. Рассмотрим необходимые настройки для подключения сервера Ubuntu к Интернет-провайдеру, открывающему доступ в Сеть только после успешной авторизации.

Установите VPN-клиента командой

```
sudo apt-get install pptp-linux
```

После завершения установки система полностью готова к соединению с VPN-сервером, имеющим настройки по умолчанию. Необходимо только создать соответствующие конфигурации для подключения.

Откройте файл /etc/ppp/chap-secrets (в целях безопасности права доступа на этой файл по умолчанию установлены только для администратора системы.

Не следует их менять). Добавьте в него строку с параметрами учетной записи, которая будет использоваться для подключения к VPN-серверу:

```
DOMAIN\\USERNAME PPTP PASSWORD *
```

В случае локальной учетной записи опустите название домена и обратные слеши. Если пароль содержит специальные символы, то его следует взять в кавычки.

В папке /etc/ppp/peers создайте файл с именем, которое будет использоваться для подключения, например, my_vpn. Добавьте в него строки листинга 3.3.

Листинг 3.3

```
pty "pptp имя_сервера_провайдера --nolaunchpppd"
name DOMAIN\\USERNAME
remotename PPTP
file /etc/ppp/options.pptp
persist
maxfail 0
ipparam my_vpn
```

В качестве `имя_сервера_провайдера` укажите доменное имя или IP-адрес VPN-сервера провайдера. Параметр `DOMAIN\\USERNAME` должен совпадать с именем, указанным в файле /etc/ppp/chap-secrets. Параметр `persist` указывает, что это соединение должно оставаться постоянным, иными словами, система будет пытаться установить его при обрыве вновь и вновь (число попыток не ограничено — параметр `maxfail 0`).

Внесите в файл /etc/resolf.conf параметры DNS-серверов, которые сообщили вам при заключении договора.

Теперь для установления VPN-подключения достаточно, имея права суперпользователя, выполнить команду (в качестве параметра указано имя подключения — `my_vpn`)

```
pon my_vpn
```

А для отключения — `poff my_vpn`.

> ***Примечание***
>
> Для диагностики процесса подключения можно выполнить команду pon со следующими параметрами `debug dump logfd 2 nodetach`.

Если необходимо, чтобы подключение к Интернету восстанавливалось автоматически при каждой перезагрузке сервера, то добавьте в файл /etc/network/interfaces следующие строки:

```
auto tunnel
iface tunnel inet ppp
        provider my_vpn
```

Обычно интернет-провайдеры отключают требование шифрования трафика для таких подключений. Настройка шифрования включена в файле /etc/ppp/options.pptp, опции которого импортируются в файл конфигурации конкретного VPN-подключения. Если шифровать трафик не нужно, то в файле /etc/ppp/options.pptp необходимо закомментировать строку `require-mppe-128`. А для того, чтобы подключаться к VPN-серверам, использующим шифрование, эту строку нужно включить в файлы индивидуальных настроек туннелей.

После установления VPN-соединения вы увидите среди сетевых интерфейсов новый с именем `ppp0` (листинг 3.4).

Листинг 3.4

```
$ ifconfig -a
….....часть листинга, соответствующая интерфейсам eth0 и lo, опущена
ppp0      Link encap:Point-to-Point Protocol
          inet addr:192.168.32.208  P-t-P:192.168.32.201
Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1396  Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:486 (486.0 B)  TX bytes:500 (500.0 B)
```

При создании VPN-подключения в системе меняется шлюз по умолчанию. Все пакеты за пределы локальной сети будут направляться в интерфейс ppp0. Такая настройка может привести к проблемам установления подключения к Интернету для провайдеров, которые предоставляют клиентам локальные адреса из сети, не совпадающей с сетью, в которой расположен VPN-сервер. Например, если вам предоставлен локальный адрес 10.0.48.13/24, а адрес VPN-сервера провайдера — 10.0.0.1, то это как раз такой случай.

В этой ситуации связь с провайдером будет устанавливаться, рваться, снова устанавливаться и т. д. Причина в том, что пакеты до VPN-сервера в подобной конфигурации система будет пытаться направить через интерфейс ppp0,

через который он недостижим. Чтобы исправить это, необходимо добавить статический маршрут до сервера провайдера, минуя ppp0-интерфейс:

```
route add -net 10.0.0.0 netmask 255.0.0.0 dev eth0
```

Замечание

В примере считается, что eth0 соответствует интерфейсу, подключенному к сети провайдера.

Для того чтобы разрешить доступ NAT-клиентов через установленное VPN-соединение, не забудьте добавить правило `iptables`:

```
iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

Примечание

Некоторые провайдеры сохраняют аутентификацию на основе MAC-адреса. Чтобы не утруждать себя лишними операциями по смене данных у провайдера, включите в файл /etc/networks/interfaces строку hwaddress со значением зарегистрированного MAC-адреса для соответствующего интерфейса (в примере — eth0) по следующему образцу:

```
auto eth0
iface eth0 inet dhcp
hwaddress ether 01:02:03:04:05:06
```

Таким способом можно назначить желаемый MAC-адрес сетевому интерфейсу.

Прокси-сервер

Практика показывает, что некоторая информация пользуется особой популярностью: ее запрашивают многие пользователи, иногда даже не по одному разу в день. Чтобы снизить нагрузку на сети, стали устанавливать так называемые прокси-серверы. На прокси-сервере автоматически сохраняется на некоторый срок вся проходящая через него информация. Если прокси-сервер обнаружит запрос данных, уже находящихся в копии на нем, то именно эта копия и будет направлена пользователю.

Кроме того, включение прокси-сервера в настройки обозревателя Интернета позволяет повысить скорость просмотра сети. Это связано с тем, что многие файлы уже не приходится получать из Сети: скорость загрузки файлов с прокси-сервера, располагающегося обычно "вблизи" пользовательского компьютера, выше скорости получения данных с удаленных хостов.

Прокси-сервер позволяет как сэкономить объем входящего трафика, что важно при оплате Интернета "по факту", так и повысить скорость работы с Web-серверами, если в организации применяется безлимитная схема оплаты (поскольку в этом случае ширина канала доступа в Интернет достаточно

серьезно ограничена средствами провайдера). Конечно, реальная эффективность использования прокси-сервера зависит от особенностей работы пользователей. Если данный сайт уже кем-то посещался, то доступ к нему другого пользователя будет более быстрым. Для среднестатистических организаций (по опыту автора) внедрение прокси-сервера позволяет снизить объем входящего трафика примерно на 20%.

> ***Примечание***
>
> Для того чтобы повысить эффективность работы через прокси-сервер, следует предусмотреть достаточный объем жесткого диска для хранения данных, получаемых из Интернета. Обычно при оценке размеров кэша стоит ориентироваться на объем месячного трафика организации, обслуживаемой таким сервером.

Автообнаружение прокси-серверов

Рабочие станции можно настраивать на автоматическое обнаружение и использование прокси-сервера. Существуют различные механизмы, при помощи которых клиенты локальной сети могут получать необходимые настройки для автоматического конфигурирования работы через прокси-сервер.

Для автоматической конфигурации параметров прокси-сервера предназначен специальный сценарий. По умолчанию такой сценарий должен иметь имя `wpad.dat` и публиковаться по протоколу HTTP на сервере с доменным именем WPAD.

Сценарий автообнаружения прокси-серверов написан на языке макропрограммирования. При необходимости его можно откорректировать. Например, при наличии двух точек доступа к Интернету сценарий может содержать функции случайного выбора того или иного канала с заранее определенным весовым коэффициентом (при работе с массивом прокси-серверов). Если необходимо работать с некоторыми серверами Интернета только через один канал, то такую возможность можно реализовать именно через модификацию данного сценария.

Если вы имеете подобный сценарий, то необходимо создать на DNS-сервере запись, которая указывала бы на данный хост (например, можно создать запись-синоним — CNAME). Параметры сценария может сообщать также и сервер DHCP. Для этого нужно добавить новый стандартный параметр (в меню **Predefined Options** оснастки управления сервером DHCP) с номером 252 (этому параметру можно дать любое название, например, Proxy Autodiscovery Option или просто wpad) и установить его значение равным URL сценария автонастройки, например:

```
http://wpad.<имя_домена>:8080/wpad.dat
```

Замечания

Для Windows-клиентов необходимо записывать URL только строчными символами. Поскольку, например, наличие прописной буквы может привести к ошибке автообнаружения прокси при использовании ISA-сервера (см. KB307502).

В параметрах DHCP можно указывать и номер порта, на котором публикуется сценарий. Для DNS-записей публикация допустима только по стандартному порту HTTP — 80.

Прокси-сервер может автоматически создавать файл сценария (например, при установке Microsoft ISA Server — рис. 3.5).

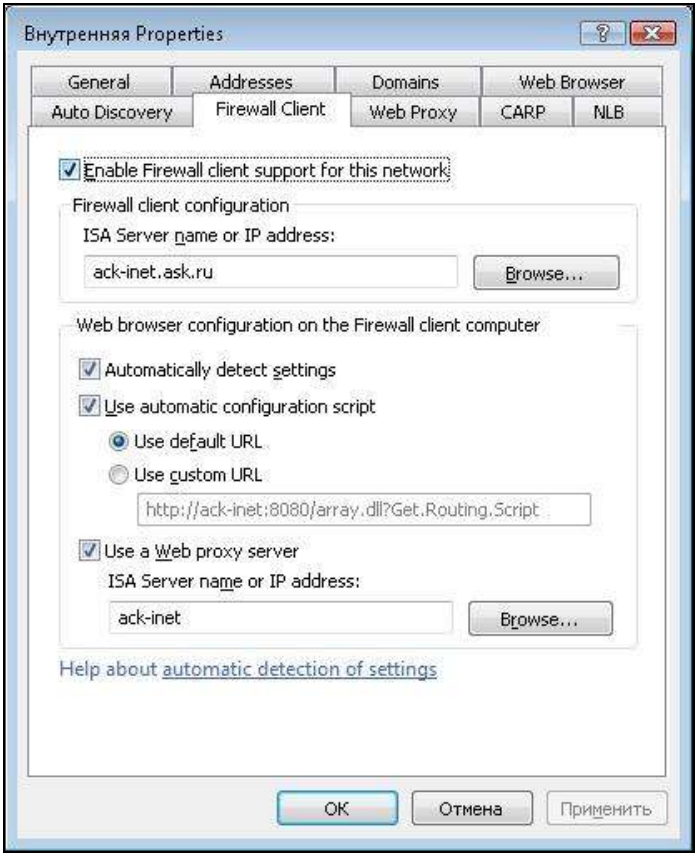


Рис. 3.5. Настройка параметров автообнаружения прокси-сервера для клиентов Microsoft ISA Server

Для серверов на основе Linux образец такого файла легко найти в Интернете (можно искать также по названию файла *proxy.pac*). При наличии только

одного прокси-сервера (одного канала доступа в Интернет) файл настроек будет всегда возвращать адрес того же самого прокси-сервера. В листинге 3.5 приведен пример такого файла.

Листинг 3.5

```
function FindProxyForURL(url, host)
{
 if (isInNet(myIpAddress(), "192.168.3.0", "255.255.255.0"))
  return "PROXY 192.168.3.10:3128";
 else
  return "DIRECT";
}
```

Установка и настройка прокси-сервера

Стандартный прокси-сервер Интернета — Squid.

> ***Примечание***
>
> В составе пакетов прокси-сервера, доступных для установки, есть стабильные версии Squid 2.6 и 3. Установка Squid версии 3 осуществляется командой `sudo apt-get install squid3`. При этом параметры настройки прокси-сервера останутся теми же, что и описаны далее в данной книге (с учетом небольших изменений в названии программы и папки — *squid* нужно будет заменить на *squid3*). Однако многие пакеты программ-анализаторов лога по умолчанию включают настройки для Squid версии 2. При установке Squid 3 вам необходимо будет самостоятельно подкорректировать соответствующие файлы конфигурации. Поскольку форматы журналов обеих версий идентичны, можно создать ссылку командой `ln -s /var/log/squid3 /var/log/squid`, которая обеспечит доступ к журналам по "старому" пути.

Для установки Squid в Ubuntu достаточно выполнить команду

```
sudo apt-get install squid
```

После загрузки и установки пакета Squid практически сразу готов к работе. Единственное, что нужно изменить в его конфигурации, — это добавить разрешение на доступ в Интернет, поскольку по умолчанию предполагается запрет доступа для всех пользователей.

Конфигурация Squid хранится в файле /etc/squid/squid.config. Это очень большой файл, содержащий подробное описание настроек множества параметров. Большинство этих настроек вам не придется менять, если Squid обслуживает в одиночку сеть небольшого офиса. Необходимо только сменить

правило по умолчанию, запрещающее доступ в Интернет через Squid, на разрешающее для компьютеров вашей сети.

> ***Замечание***
>
> Например, очень много параметров описывают условия пересылки данных между несколькими кэширующими прокси-серверами, при каких условиях пересылать пакеты одним серверам, когда это нужно делать напрямую и т. п.

Чтобы разрешить работу через Squid со всех компьютеров локальной сети, нужно: а) откорректировать правило, описывающее диапазон адресов локальной сети и б) включить правила разрешения доступа.

Найдите в конфигурации блок, описывающий создание правил доступа (его заголовок ACCESS CONTROLS). В нем присутствует закомментированная строка, описывающая локальную сеть:

```
#acl our_networks src 192.168.1.0/24 192.168.2.0/24
```

> ***Замечание***
>
> Если вы пользуетесь редактором VI, то нажмите (в командном режиме) клавишу </>, наберите `our_networks` (ввод будет отображаться в нижней части экрана) и нажмите <Enter>. Вы сразу перейдете на нужную строку.

Снимите комментарий (удалите `#` в первой позиции строки) и замените приведенные диапазоны на те, которые используются в вашей локальной сети. Раскомментируйте также и следующую строку (`#http_access allow our_networks`). Сохраните настройки и перезагрузите конфигурацию Squid командой

```
sudo /etc/init.d/squid reload
```

> ***Замечание***
>
> В конфигурации Squid содержится также пожелание раскомментировать строку `#http_access deny to_localhost`, если на компьютере со Squid установлено то или иное Web-приложение.

Теперь нужно только настроить обозреватели Интернета на компьютерах локальной сети, указав параметры прокси-сервера: адрес сервера Squid и номер порта 3128 (это порт, используемый Squid по умолчанию; обычно нет необходимости изменять этот номер).

Дополнительные настройки прокси-сервера

Понятно, что настройка только из разрешения ходить в Интернет с любого компьютера локальной сети всем пользователям может применяться лишь в небольших организациях. Какие настройки обычно следует добавить?

Как правило, это управление полосой пропускания канала, фильтрация трафика и настройка авторизации или режима "прозрачного" прокси-сервера.

Как создавать собственные настройки

Любые настройки Squid выполняются на основе единого подхода. Сначала описываются в конфигурации объекты, к которым правило будет применено. Затем создается само правило. При этом очень важна последовательность, в которой правила встречаются в файле конфигурации: Squid просматривает правила от начала перечня к концу и, если найдет правило, применимое к данному пакету, то использует его и прекратит дальнейший просмотр списка. Поэтому если нужно разрешить кому-то иметь доступ к конкретному сайту, а всем остальным — запретить, то сначала должно быть определено правило разрешения конкретному пользователю, а после него добавлено правило запрета для всех.

Объекты, к которым предполагается применить правила, описываются с помощью так называемых *списков доступа* (Access Control List, ACL). Списки доступа могут определять:

- адреса источника и назначения (как конкретный IP-адрес, так и подсети);
- домены источника и назначения;
- время (часы и дни недели);
- порты источника и назначения, MAC-адреса источника;
- URL-строки запросов обозревателя, в том числе, и поиск по подстроке запроса с учетом регулярных выражений;
- протоколы, типы обозревателя, методы запроса (POST, GET), параметры заголовков и т. п.

Для создания списка доступа достаточно включить в файл конфигурации строку

```
acl имя_списка тип_списка перечень_объектов
```

Параметр `тип_списка` в этой строке должен соответствовать одному из вариантов, приведенному в комментариях в файле конфигурации. Перечислять, какие объекты попадут под определение данного списка, можно как в одной строке (например, указать несколько IP-адресов источников через пробел), так и в нескольких строках (при этом необходимо повторить `имя_списка`). Но, чтобы не затруднять работу с файлом конфигурации, особенно при большом перечне объектов, удобнее вынести сам перечень в отдельный файл (в каждой строке этого файла должно быть указание только на один объект), а в строке определения списка доступа указать имя этого файла, взятое в двойные кавычки. Например, так:

```
acl porno dstdomain "/etc/squid/blacklists/porn/domains"
```

После того как списки доступа созданы, можно использовать их имена в правилах обработки запросов прокси-сервером.

Примечание

После изменения правил необходимо перезагрузить конфигурацию Squid командой `/etc/init.d/squid reload`.

Настройка использования полосы пропускания

Squid позволяет регулировать полосу пропускания при работе пользователей в Интернете. Это полезно в организациях, выбравших безлимитные тарифы, которые обычно предполагают искусственное ограничение полосы пропускания. Поэтому, чтобы один пользователь, поставивший на загрузку файл большого размера, не парализовал работу всех других сотрудников, ищущих на сайтах необходимую для текущей деятельности информацию, следует ввести лимиты на использование канала.

Squid предоставляет несколько возможностей управления. Во-первых, можно ограничить полосу пропускания для каждого сотрудника: фактически разделить весь канал между всеми. Как правило, такие настройки применяют только для отдельных "наказанных" сотрудников, поскольку если в Интернете в текущий момент работает только несколько сотрудников с ограничением полосы пропускания, то бóльшая часть канала будет простаивать.

Более удобен второй вариант, при котором первая часть файла загружается на максимально настроенной скорости, а для последующей вступают в силу ограничения. Так можно обеспечить всем сотрудникам максимально быструю работу с сайтами (поскольку оформление WWW-страниц обычно не занимает большого объема), но ограничить выделение канала для загрузки файлов большого размера.

Чтобы включить управление полосой пропускания, нужно настроить *пулы задержек*, создать списки доступа, определяющие пользователей или компьютеры, для которых будут вводиться ограничения, и настроить правила.

Фактически, пул задержек — это набор параметров, определяющих использование канала доступа в Интернет. Каждый пул задержек может быть одного из трех *классов*. Первый класс позволяет ограничивать полосу индивидуально, второй — устанавливать лимиты для подсети в целом и, кроме того, лимиты для каждого пользователя. Третий класс устанавливать лимиты для сетей, подсетей и индивидуально. Если представить IP-адрес как a.b.c.d., то первый класс может быть применен только индивидуально, это разные значения d. Класс 2 учитывает параметры с для групповых ограничений, а класс 3 учитывает для первого лимита значения b, для второго — c и потом устанавливает индивидуальные ограничения.

По умолчанию число пулов задержки равно нулю. В конфигурации Squid нужно сначала определить число создаваемых пулов, а потом указать, какой пул к какому классу относится (листинг 3.6).

Листинг 3.6

```
delay_pools 4 # Будет создано 4 пуля задержек
delay_class 1 1 # Первый пул относится к классу 1
delay_class 2 2 # Второй пул относится к классу 2
delay_class 3 2 # Третий пул относится к классу 2
delay_class 4 3 # Четвертый пул относится к классу 3
```

Параметры лимитирования полосы пропускания определяются командой delay_parameters, ее параметрами должны быть номер пула задержки и лимиты. Лимит для класса 1 всегда общий, для параметров классов 2 и 3 — сначала указывается лимит для сети (или для сетей в случае класса 3), потом — индивидуальное значение, при этом цифры указывают значения в *байтах*.

> ***Замечание***
>
> В договоре с интернет-провайдером обычно указывается предоставляемая полоса пропускания в битах в секунду. Это следует учитывать при установке ограничений.

Обозначение лимита 600/8000 устанавливает максимальную скорость в 600 байт/с или 4800 бит/с после загрузки первой части файла размером 8 Кбайт. Обозначение -1/-1 применяется при отсутствии лимитирования. Посмотрите пример конфигурации настроек, предполагая, что пул с номером 2 относится к третьему классу:

```
delay_parameters 2 32000/32000 8000/8000 600/8000
```

Включать использование пулов задержек следует командой `delay_access`, в качестве ее параметров должны быть указаны номер пула, правило и команда (`allow` или `deny`). Причем команды должны быть написаны в сортированном порядке: сначала команды для пулов класса 1, потом для пулов класса 2, потом — для класса 3. При этом последней командой для каждого пула должен быть включен запрет для всех, чтобы программа вышла из анализа по данному классу (листинг 3.7).

Листинг 3.7

```
delay_access 1 allow users1
delay_access 1 deny all
delay_access 2 allow users2
```

```
delay_access 2 deny all
delay_access 3 allow users3
delay_access 3 allow users4
delay_access 3 deny all
delay_access 4 allow users5
delay_access 4 deny all
```

Блокировка рекламы, порносайтов и т. п.

С помощью прокси-сервера можно ограничить доступ пользователей к сайтам определенной направленности. Для этого нужно создать соответствующие списки доступа и применить к ним правило запрета.

> ***Примечание***
>
> Не стоит обольщаться, что такие списки "закроют", например, все порносайты. Число порносайтов превышает по разным оценкам несколько миллионов, и блокировать их тем или иным списком доступа нереально. Следует также учитывать, что увеличение числа правил обработки запросов снижает производительность прокси-сервера. Поэтому не стоит особенно увлекаться числом заблокированных доменов, следите за производительностью сервера и находите разумный баланс ограничений и скорости работы прокси. С точки зрения влияния на производительность прокси-сервера, предпочтительнее ограничения по доменам назначения, чем сложные регулярные выражения. При этом обычно несколько тысяч строк с именами блокированных доменов не очень существенно сказываются на производительности сервера.

Основу таких списков блокировки лучше всего найти в Интернете по ключевому термину "blacklist". Так, можно использовать перечни с сайта **http://urlblacklist.com/** (сайт представляет коммерческую службу, поддерживающую актуальность таких списков. Но условия его лицензии позволяют однократно загрузить эти списки. Объем загрузки составляет около 18 Мбайт архивированных файлов.), списки, используемые в дополнениях к Firefox, — см. **http://adblockplus.org/en/subscriptions** или любые другие.

Загрузите их из Интернета, сохраните, например, в папке /etc/squid/blacklists по соответствующим разделам и создайте определения списков доступа. Если файл списка содержит имена доменов, то укажите строку (в примерах указаны названия файлов списка с сайта Urlblacklist.com).

```
acl porno dstdomain "/etc/squid/blacklists/porn/domains"
```

Если в файле списка даны регулярные выражения, то нужно определять правило следующим образом:

```
acl banners url_regex "/etc/squid/blacklists/porn/expressions"
```

Для списков по URL потребуются типы `acl url_regex`, `urlpath_regex`, `dstdom_regex` — в зависимости от того, какой вариант вы имеете.

Затем включите в файл конфигурации правила, блокирующие запросы на сайты, включенные в такие списки:

```
http_access deny porno
```

После перезагрузки конфигурации прокси-сервера администратору нужно некоторое время анализировать результаты фильтрации. Как правило, в списках, полученных из Интернета, попадаются ресурсы, случайно попавшие в такой перечень и нужные для текущей работы. Кроме того, некоторая часть, например, рекламы не будет отфильтрована. Такие случаи нужно отследить по файлам журнала работы Squid и добавить новые условия фильтрации.

Улучшение эффективности использования кэша прокси-сервера

Чтобы увеличить процент объектов, которые будут загружаться из кэша, можно несколько подкорректировать конфигурацию Squid. Для этого нужно увеличить размер дискового пространства, выделенного для размещения кэша, и предписать Squid хранить в кэше объекты более длительный период, чем предусмотрено его настройками по умолчанию или параметрами открываемых Web-страниц.

> ***Примечание***
>
> При наличии возможности кэш прокси-сервера лучше разместить на нескольких дисках. Это повысит производительность системы. Для такой конфигурации достаточно добавить только одну директиву `cache_dir`, указывающую на точку монтирования другого диска. После чего остановить Squid и запустить его командой `squid -z`.

Для увеличения размера кэша найдите в файле конфигурации строку `#cache_dir ufs /var/spool/squid 100 16 256`, раскомментируйте ее. Замените 100 на величину ожидаемого месячного трафика в мегабайтах, хотя обычно вполне достаточно установить ее значение равным нескольким гигабайтам, например, так:

```
cache_dir ufs /var/spool/squid 4096 16 256
```

Теперь можно предписать Squid хранить в кэше объекты более длительный срок, чем предусмотрено настройками. Обычно на страницах Web-серверов самые неизменяемые элементы — это графика. Поэтому добавим в файл конфигурации в блок OPTIONS FOR TUNING THE CACHE параметры, которые заставят программу хранить такие файлы длительный период (в примере значение выбрано равным одному месяцу или 43 200 мин), не учитывать пользовательские настройки периода их хранения и не обновлять эти файлы во время операции ручного обновления страницы. Листинг 3.8 иллюстрирует пример такой настройки для графических файлов форматов gif, jpg, pdf.

Листинг 3.8

```
refresh_pattern \.gif$ 43200 100% 43200 override-lastmod override-expire
ignore-reload ignore-no-cache

refresh_pattern \.jpg$ 43200 100% 43200 override-lastmod override-expire
ignore-reload ignore-no-cache

refresh_pattern \.pdf$ 43200 100% 43200 override-lastmod override-expire
ignore-reload ignore-no-cache
```

По этому образцу вы легко сможете увеличить число подобных настроек, например, включив в них и другие допустимые для Интернета расширения имен графических файлов, добавив расширения exe, cab, mp3 и т. д. Кроме того, если объем диска позволяет, можно увеличить максимальный размер файла, помещаемого в кэш. По умолчанию это значение равно 4 Мбайт, его можно увеличить, настроив параметр `maximum_object_size`.

> ***Примечание***
>
> После директивы `refresh_pattern` указано регулярное выражение, определяющее URL-адреса объектов, которые будут помещаться в кэш. Описание синтаксиса таких выражений легко найти в Интернете, отметим только, что символы `\` указывают на любое начало такой строки, а символ `$` соответствует окончанию строки. Таким образом, приведенные в примере выражения определяют любые URL-строки, которые заканчиваются на gif, jpg и pdf соответственно.

Аутентификация доступа в Интернет

При использовании списков доступа на основе IP-адресов или MAC-адресов компьютеров у злоумышленников остается возможность присвоения себе чужих параметров для обхода такой защиты. Выходом в такой ситуации является аутентификация *любой* попытки доступа в Интернет.

Squid позволяет реализовать несколько вариантов аутентификации пользователей. В файле конфигурации Squid есть минимальный набор параметров для включения аутентификации пользователей по той или иной схеме (закомментированные строки, начинающиеся с `auth_param`). Необходимо раскомментировать все параметры, соответствующие желаемой схеме (например, *basic* или *ntlm*), при этом следует указать программу, которая будет осуществлять аутентификацию. В комментариях в файле конфигурации приведены указания по наиболее распространенным вариантам. Поскольку на практике наиболее часто применяется аутентификация пользователей по внутренней базе

сервера или по базе пользователей домена Windows, мы приведем образцы первых строк параметров для таких случаев.

- Аутентификация по внутренней базе пользователей сервера Ubuntu.

  Нужно раскомментировать блок для схемы basic и указать для программы следующую настройку:

  ```
  auth_param basic program /usr/lib/squid/pam_auth -n passwd
  ```

- Аутентификация с использованием протокола NTLM в домене Windows.

  Для NTLM-аутентификации необходимо включить сервер в состав домена Windows. Как это сделать, описано в *главе 5*. В этом примере мы считаем, что все необходимые операции выполнены и работоспособность в домене протестирована.

  Для осуществления аутентификации в домене Windows необходимо раскомментировать блоки параметров для схем basic и ntlm (чтобы сохранить возможность получения от пользователя имени и пароля в ответ на запрос системы) и указать (см. **http://wiki.squid-cache.org/ConfigExamples/WindowsAuthenticationNTLM**) для схемы basic:

  ```
  auth_param basic program /usr/lib/squid/ntlm_auth
  --helper-protocol=squid-2.5-basic
  ```

  для схемы ntlm:

  ```
  auth_param ntlm program /usr/lib/squid/ntlm_auth
  --helper-protocol=squid-2.5-ntlmssp
  ```

  Примечание

  Можно добавить в строку параметр `require-membership-of=DOMAIN\\InternetUsers`. В этом случае правило будет считать аутентификацию успешной только для членов группы DOMAIN\\InternetUsers.

Остальные строки можно оставить в значениях по умолчанию.

После включения схем аутентификации необходимо создать список доступа, описывающий аутентифицированных пользователей:

```
acl auth proxy_auth REQUIRED
```

А потом включить правило, запрещающее доступ в Интернет всем неаутентифицированным пользователям:

```
http_access deny !auth
```

Для того чтобы изменения аутентификации вступили в силу, необходимо перестартовать Squid (перезагрузки конфигурации при изменении схемы недостаточно).

"Прозрачный" прокси-сервер

Прокси-сервер можно настроить так, что клиентам, выходящим в Интернет, не придется никоим образом настраивать свои обозреватели. Такой режим работы прокси-сервера называется *прозрачным прокси* (transparent proxy).

Использование режима прозрачного прокси связано с некоторыми ограничениями. Во-первых, прокси-сервер должен быть шлюзом по умолчанию для компьютеров локальной сети. Во-вторых, в этом режиме прокси-сервер не может использовать никакую аутентификацию пользователей для доступа в Интернет (доступ будет разрешен всем анонимным пользователям).

> ***ЗАМЕЧАНИЕ***
>
> Можно, конечно, перенаправить http-запросы со шлюза на прокси-сервер, но более логичен выход в Интернет с компьютера со Squid.

Для перевода Squid в такой режим достаточно выполнить две настройки. Первая — это добавить параметр `transparent` в строку `http_port`, например, так:

```
http_port 3128 transparent
```

Вторая настройка перенаправляет HTTP-пакеты из локальной сети на порт Squid. Выполняется она с помощью команды iptables:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT
--to-port 3128
```

Эти две настройки обеспечат "невидимую" для пользователей работу прокси-сервера.

> ***ЗАМЕЧАНИЕ***
>
> Предполагается, что `eth0` — это интерфейс локальной сети. Обратите внимание, что если вы разрешаете работу пользователям по другим протоколам в Интернете, то приведенная строка должна стоять *до* строки, настраивающей такой доступ для локальных клиентов.

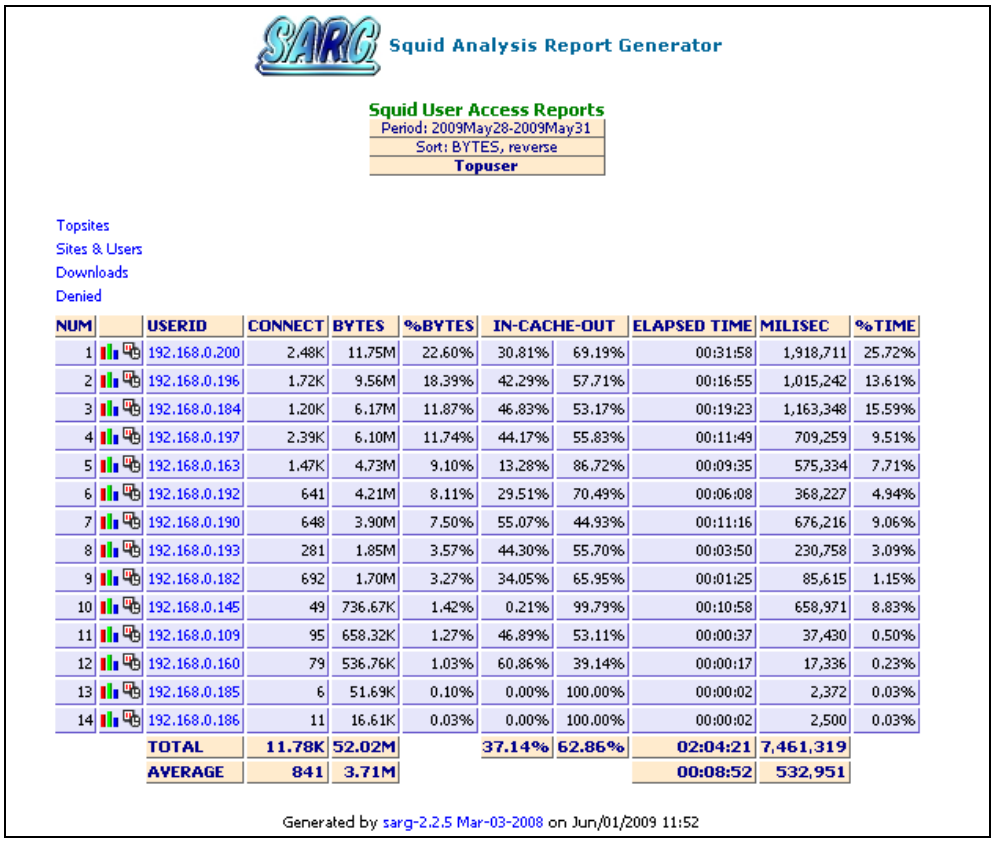
Анализ журналов работы прокси-сервера

Squid записывает протоколы своей работы по умолчанию в папку /var/log/squid. Файлы cache.log и store.log представляют интерес для оценки работы самой программы. А в файл access.log записываются данные о результатах доступа в Интернет пользователей. Этот файл целесообразно непрерывно анализировать, чтобы, с одной стороны, постоянно уточнять политики доступа в Интернет, с другой стороны, в нем содержатся данные, полезные для оценки работы пользователей (трафик, посещаемые сайты и т. п.).

Для анализа журналов имеется много программ. Часть из них приведена на странице **http://www.squid-cache.org/Scripts/**. Этот список далеко не исчерпывающий. Вы можете найти и другие решения, более точно приспособленные к конкретным целям анализа (например, программа Free-sa для анализа файлов журналов большого объема, см. **http://sourceforge.net/projects/free-sa**). При желании можно формировать несколько вариантов отчета различными утилитами, достаточно только указать параметры их запуска в файле ротации (см. далее).

На рис. 3.6 представлен вариант отчета использования прокси-сервера Squid.

Элементы окна обозревателя на рис. 3.6 не показаны. Видно, что прокси-сервер позволил сэкономить 37% трафика Интернета. Другие формы отчета дают возможность проанализировать частоту посещений сайтов, наиболее существенные загрузки, активность пользователей организации и т. п.



NUM		USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILISEC	%TIME
1		192.168.0.200	2.48K	11.75M	22.60%	30.81%	69.19%	00:31:58	1,918,711	25.72%
2		192.168.0.196	1.72K	9.56M	18.39%	42.29%	57.71%	00:16:55	1,015,242	13.61%
3		192.168.0.184	1.20K	6.17M	11.87%	46.83%	53.17%	00:19:23	1,163,348	15.59%
4		192.168.0.197	2.39K	6.10M	11.74%	44.17%	55.83%	00:11:49	709,259	9.51%
5		192.168.0.163	1.47K	4.73M	9.10%	13.28%	86.72%	00:09:35	575,334	7.71%
6		192.168.0.192	641	4.21M	8.11%	29.51%	70.49%	00:06:08	368,227	4.94%
7		192.168.0.190	648	3.90M	7.50%	55.07%	44.93%	00:11:16	676,216	9.06%
8		192.168.0.193	281	1.85M	3.57%	44.30%	55.70%	00:03:50	230,758	3.09%
9		192.168.0.182	692	1.70M	3.27%	34.05%	65.95%	00:01:25	85,615	1.15%
10		192.168.0.145	49	736.67K	1.42%	0.21%	99.79%	00:10:58	658,971	8.83%
11		192.168.0.109	95	658.32K	1.27%	46.89%	53.11%	00:00:37	37,430	0.50%
12		192.168.0.160	79	536.76K	1.03%	60.86%	39.14%	00:00:17	17,336	0.23%
13		192.168.0.185	6	51.69K	0.10%	0.00%	100.00%	00:00:02	2,372	0.03%
14		192.168.0.186	11	16.61K	0.03%	0.00%	100.00%	00:00:02	2,500	0.03%
		TOTAL	11.78K	52.02M		37.14%	62.86%	02:04:21	7,461,319	
		AVERAGE	841	3.71M				00:08:52	532,951	

Generated by sarg-2.2.5 Mar-03-2008 on Jun/01/2009 11:52

Рис. 3.6. Отчет об эффективности работы прокси-сервера Squid

Анализаторы журналов подготавливают свои отчеты для публикации на Web-сервере. Поэтому, если вы собираетесь установить такую программу, сначала следует настроить Web-сервер. Для установки Web-сервера Apache выполните команду:

```
sudo apt-get install apache2
```

После установки сервер Apache с параметрами конфигурации по умолчанию сразу начинает работать, при этом корневой каталог его расположен в папке /var/www.

В качестве программы анализа журналов работы установим популярную утилиту sarg:

```
sudo apt-get install sarg
```

Файлы конфигурации sarg содержат настройки, соответствующие настройкам Squid и Apache по умолчанию. И, если вы не меняли пути к файлам журналов и папкам Web-сервера, то в консоли можно просто набрать

```
sarg
```

После чего в папке /var/www/squid-reports появится отчет, сформированный по данным текущего журнала Squid. Просмотреть его можно, открыв страницу **http://адрес_squid/squid-reports**.

Файл access.log очень быстро увеличивается в объеме. По умолчанию предусмотрена его *ротация*: через определенный промежуток времени (неделю, если вы не меняли это значение) создается новый файл журнала, старый файл переименовывается и несколько таких копий сохраняется на диске. После того, как число копий достигнет заданной величины (2), самая старая копия удаляется.

Эти операции выполняются в Ubuntu утилитой logrotate. Файлы настроек опций ротации журналов расположены в папке /etc/logrorate.d. Необходимо исправить небольшую неточность параметров запуска программы sarg.

Откройте в этой папке файл squid. Найдите в нем строку `prerotate`. Она начинает блок команд, которые выполняются *перед* началом ротации файлов журналов. В этом блоке нужно подправить название утилиты. Строка должна иметь следующий вид:

```
test ! -x /usr/bin/sarg || /usr/bin/sarg
```

(Сценарий проверяет существование исполняемого файла по заданному пути и, в случае успеха, запускает его на выполнение.) Эта строка обеспечит вам регулярное обновление отчетов, составляемых программой sarg на основе журнала Squid.

Не забывайте периодически удалять старые отчеты программы sarg. Ключей запуска, предусматривающих штатное удаление старых отчетов, в программе не предусмотрено. Вы можете просто удалить файл index.html и все папки, имена которых соответствуют датам отчетов. При последующем запуске утилиты необходимые файлы и папки будут созданы вновь.

Антивирусная проверка HTTP-трафика

Современное программное обеспечение позволяет выполнить антивирусную проверку всего трафика, проходящего через шлюз Интернета. Подобные разработки от Microsoft являются коммерческими. Для шлюзов на основе Linux-операционных систем есть абсолютно бесплатные решения.

Для проверки интернет-трафика на Linux-системах достаточно направить трафик прокси-сервера через программу, выполняющую антивирусную проверку файлов. Наиболее просто это осуществить с помощью еще одного прокси-сервера со встроенной антивирусной проверкой. Используем для этого пакеты *havp* и *ClamAV*.

Если вы организуете проверку всего трафика, то будьте готовы выделить на это соответствующие аппаратные ресурсы. Даже в условиях небольшого офиса при числе пользователей около 20 человек и ширине канала 1 Мбит/с проверка всех файлов в HTTP-запросах на наличие вирусов может потребовать несколько сотен мегабайт оперативной памяти и существенную часть процессорного времени (порядка 10–20%).

Прокси-сервер havp (**http://www.server-side.de**) и антивирусная программа ClamAV устанавливаются командой

```
sudo apt-get install havp clamav
```

> ***ЗАМЕЧАНИЕ***
>
> Часто при одновременной установке возникают ошибки настройки, которые можно исправить повторным запуском `sudo apt-get -f install havp`.

После установки этих программ требуется лишь минимальное вмешательство администратора. Во-первых, в файле конфигурации havp (/etc/havp/havp.config) нужно указать на использование русских шаблонов страниц-сообщений. Для этого необходимо найти строку `# TEMPLATEPATH /etc/havp/templates/en` и заменить ее на

```
TEMPLATEPATH /etc/havp/templates/ru
```

Во-вторых, целесообразно в самих шаблонах заменить фразу *"Здесь должно быть название Вашей компании"* на более подходящий текст.

Учтите, что по умолчанию программа обновления антивирусных баз пытается выполнить обновления каждый час. Если вы не согласны с такой периодичностью, то измените величину `Checks` в файле `/etc/clamav/freshclam.conf` на желаемое значение.

Проверьте работу havp попыткой загрузки тестового вируса со страницы **www.eicar.org/anti_virus_test_file.htm**. Havp по умолчанию задействует порт 8080, поэтому для проверки на данном шаге настройки в параметрах обозревателя следует установить это значение порта прокси-сервера.

После проверки следующим шагом должна быть настройка Squid на работу с вновь установленным прокси-сервером в качестве *родительского прокси*. Для этого укажите в файле конфигурации Squid параметры данного сервера:

```
cache_peer 127.0.0.1 parent 8080 0 no-query no-digest
no-netdb-exchange default
cache_peer_access 127.0.0.1 allow all
```

Далее следует указать, какой трафик запрашивать через havp. Для этого нужно создать соответствующий список доступа и правило направления запросов через этот прокси. Можно реализовать два варианта настроек. Самый простой — направить через прокси-сервер havp весь http-трафик. Сделать это можно настройкой конфигурации Squid:

```
acl av_scan proto HTTP
never_direct allow av_scan
```

Первая строка определяет список доступа — весь HTTP-трафик. Вторая указывает, что его необходимо всегда запрашивать через родительский прокси-сервер.

Другой подход предполагает более точное указание тех объектов, которые необходимо проверять на вирусы. Это более трудоемкий способ, но он позволяет снизить нагрузку на сервер. Для этого необходимо создать дополнительные списки доступа, которые будут описывать пропускаемые в антивирусной проверке файлы, например, так:

```
acl no_avir urlpath_regex -i \.avi$ \.jpg$ \.gif$ \.mp3$
always_direct allow no_avir
```

Естественно, что такой список можно делать как более развернутым, снижая нагрузку на процессор и память, так и более узким, проверяя большую часть файлов. Какой уровень проверки выбрать, решит сам администратор.

После того как все настройки будут выполнены, перезапустите havp и Squid (restart) и проверьте работу системы загрузкой тестового вируса (рис. 3.7).

Видно, что антивирусная программа заблокировала попытку загрузки тестового вируса. Такая проверка осуществляется на сервере, еще до попадания данных на пользовательский компьютер.

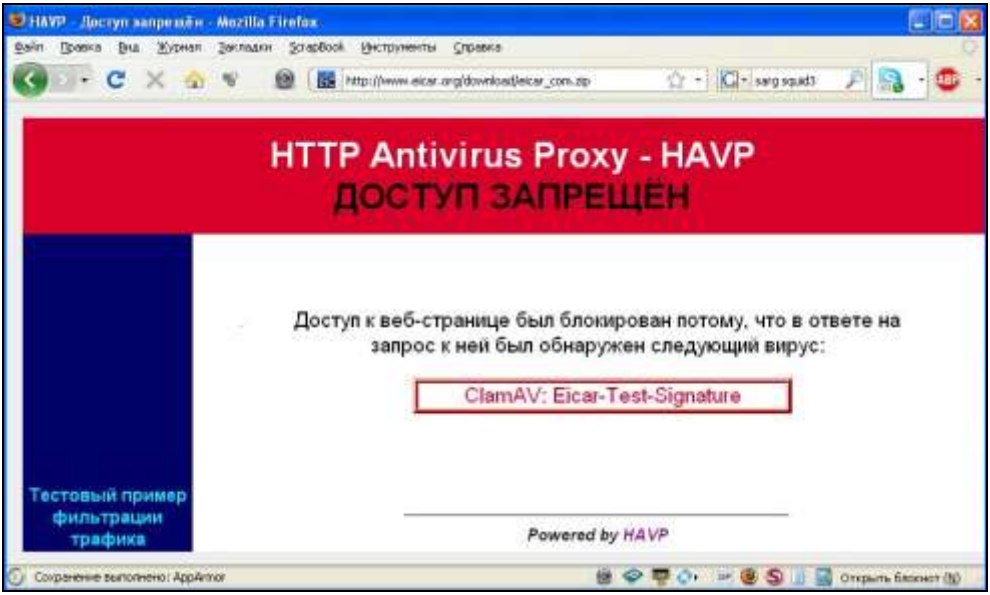


Рис. 3.7. Проверка работы антивирусной фильтрации трафика



Глава 4

Готовим новый компьютер к эксплуатации

После появления нового компьютера перед системным администратором встает задача ввода его в эксплуатацию. В зависимости от целей приобретения системы — под новую задачу, в качестве дополнительного типового рабочего места или взамен вышедшей из строя системы, возможны различные варианты подготовки компьютера. Это может быть как полная установка системы с нуля, так и дублирование жесткого диска или восстановление из резервной копии.

Паспорт компьютера

Одно из главных требований при вводе в эксплуатацию новой системы — наличие на нее паспорта. Неважно, в какой форме будут храниться данные, в электронном ли виде или на бумаге, на форме или просто написанные от руки. Главное, чтобы конфигурация компьютера была описана, чтобы вы и последующие администраторы знали, каковы параметры настройки компонент системы, какие версии драйверов установлены.

Если вы настроили оборудование с установками по умолчанию, то и просто отметьте этот факт. Чтобы специалист, которому, например, через два года придется восстанавливать вышедший из строя RAID-массив, знал, что был выбран тип 5 с размером сектора в 64 Кбайт, а не какая-либо иная конфигурация. Поверьте, подобная информация очень дорого стоит для обслуживающего персонала.

Обратите внимание на функционирование системы именно в первые месяцы после ее запуска. Может быть, какие-либо версии драйверов приводят к нестабильной работе. И вы нашли причину и заменили версии программ. Все это следует описать и сохранить.

Установка системных обновлений

Начинать ввод в эксплуатацию нового компьютера всегда нужно с обновления программных компонентов оборудования.

Ряд элементов системного блока компьютера имеет обновляемое ПО, которое часто называют прошивками. Это могут быть и новые версии BIOS, и программное обеспечение, контролирующее работу узлов серверной платы (BMC — Baseboard Management Controller), различные обновления firmware и т. п. Качество данного ПО существенно влияет на стабильность работы прикладного программного обеспечения. Поэтому крайне важно установить последнюю версию таких прошивок до передачи системы в эксплуатацию.

За время, пока новый системный блок попадает к конечному пользователю (а это обычно не менее полугода), производитель успевает выпустить не одно обновление. В комплекте с системным блоком приходит программное обеспечение, актуальное на момент выпуска оборудования. Чтобы получить новые версии, необходимо посетить сайт изготовителя. При этом нужно быть особо внимательным к описаниям, сопровождающим различные версии ПО. Часто установка того или иного обновления допустима только на определенные серийные номера оборудования.

Процедура установки системных обновлений подробно описана в инструкциях. Нужно только загрузить с сайта производителя необходимые версии ПО и тщательно выполнить все рекомендации.

Варианты установки программного обеспечения нового компьютера

После того как на компьютер установлены последние обновления системного ПО, приступают к установке операционной системы и прикладных программ. Обычно придерживаются данной последовательности:

- ❒ установка операционной системы;
- ❒ установка драйверов изготовителя (для видеоадаптера, системы ввода-вывода и т. п.);
- ❒ установка обновлений операционной системы;
- ❒ установка прикладных программ;
- ❒ установка обновлений прикладных программ;
- ❒ настройка параметров безопасности сервера (рабочей станции).

Иногда установку обновлений безопасности операционной системы переносят в конец операций, вместе с обновлением прикладных программ. Но это не меняет существенно время для подготовки компьютера: все эти операции требуют участия системного администратора от полутора часов (в лучшем случае) и более. В условиях, когда администратору приходится сопровождать несколько фирм, чтобы получить достойную оплату, тратить столько времени на подобные операции нерационально.

Обычно это время можно сократить за счет процессов *клонирования* системы. Для чего сначала следует подготовить образцовую установку операционной системы, установить на нее программное обеспечение, настроить и, затем, выполнить сам процесс клонирования. Мы опустим описания собственно установки операционных систем и прикладных программ, поскольку соответствующие операции подробно описаны во многих источниках. Рассмотрим более внимательно те моменты, на которые иногда не обращают достаточного внимания.

Индивидуальная настройка серверов

Типовая конфигурация операционной системы (после стандартной установки "из коробки") предназначена для обеспечения универсальной работоспособности компьютера, чтобы установленная система сразу была пригодна для производственной деятельности.

Поэтому в подавляющем большинстве случаев система содержит *излишние функции*, которые целесообразно отключить в целях повышения безопасности (каждая такая функция — это избыточный код с потенциальными ошибками, увеличивающими риск несанкционированного проникновения в систему). Как правило, следует отключить запуск излишних служб системы (неиспользуемых в конкретной конфигурации) и настроить параметры безопасности (например, применяемые протоколы аутентификации, уровень предоставления информации анонимному пользователю и т. п.) по максимально возможному уровню с учетом специфики информационной системы. Такие настройки во многом индивидуальны для каждого компьютера, поэтому привести универсальные рекомендации в данной книге не представляется возможным.

Отмечу только, что администратору системы следует оптимизировать *каждый* сервер под те задачи, которые он решает. Необходимые рекомендации легко можно найти на сайтах разработчиков программного обеспечения по ключевым словам *"hardening"* или *"security guide"*. В подобных документах обычно достаточно подробно описываются параметры, влияющие на уровень безопасности системы, и возможные последствия в функционировании информа-

ционной структуры при их изменении. Администратору следует внимательно проанализировать каждый параметр и оценить целесообразность предполагаемых изменений.

Установка обновлений безопасности

Установку обновлений безопасности необходимо обеспечивать в течение всего периода эксплуатации сервера или рабочей станции. Если в системе будет сохраняться уязвимость, то это означает, что злоумышленник в любой момент может получить управление над нею. Строгая настройка межсетевого экрана снижает риск атаки, но оставляет "двери" в систему в виде портов, открытых для каких-либо приложений.

Если говорить об обновлениях для операционных систем Windows, то они выпускаются регулярно, обычно раз в месяц. Естественно, что при обнаружении критической уязвимости соответствующая заплатка выпускается вне графика. Для того чтобы быть в курсе выпускаемых обновлений безопасности, следует подписаться на соответствующие рассылки вендоров. На странице **http://technet.microsoft.com/ru-ru/security/dd252948.aspx** можно подписаться на наиболее удобный для вас вид оповещений о выпуске обновлений безопасности для систем Windows (возможны варианты по электронной почте, по каналам RSS, Windows Live Alert и т. д.). Для операционной системы Ubuntu получение оповещений доступно на основе RSS-подписки (**http://www.ubuntu.com/usn/rss.xml**), а перечень выпущенных обновлений публикуется на странице **http://www.ubuntu.com/usn**.

Когда устанавливать обновления

Установка обновлений безопасности — это модификация операционной системы. В общем случае, перед установкой каждое обновление нужно протестировать в условиях, приближенных к реальной эксплуатации в данной организации. Было много случаев, когда установка вроде безобидного патча приводила, например, к ошибкам печати на сетевой принтер или отказу какого-либо эксплуатируемого приложения и т. п. Конечно, в средних и небольших организациях такие проверки выполнить очень сложно. Поэтому отключите автоматическое обновление, по крайней мере, серверов и настройте график установки заплаток так, чтобы в эти моменты вы могли быстро вмешаться и восстановить работу информационной системы.

> ***Совет***
>
> Автор советовал бы до установки обновлений изучить их описания, для чего они предназначены и т. п. Часто установка обновлений на конкретную систему нецелесообразна в силу специфики данного конкретного рабочего места.

Кроме того, нелишне убедиться, что до начала установки обновлений у вас есть актуальная копия данных, которая позволит восстановить работу при катастрофическом отказе системы в результате процесса обновления.

Для большинства пользовательских компьютеров обычно не критично, если они будут выведены из строя на достаточно существенный промежуток времени. Поэтому на таких рабочих местах можно включить режим автоматической загрузки и установки обновлений.

В Windows XP/2003 режим установки обновлений настраивался через вызов свойств задачи Мой компьютер, в Windows Vista/2008 необходимые параметры назначают в задаче **Панель управления | Центр обновлений | Изменить параметры**. Обратите внимание, что в этом окне (рис. 4.1) можно включить поиск и установку обновлений не только для самой операционной системы, но и для тех приложений Microsoft, которые обслуживаются Windows Update (программы Microsoft Office, SQL Server и т. п.). Для этого необходимо включить опцию использования Windows Update.

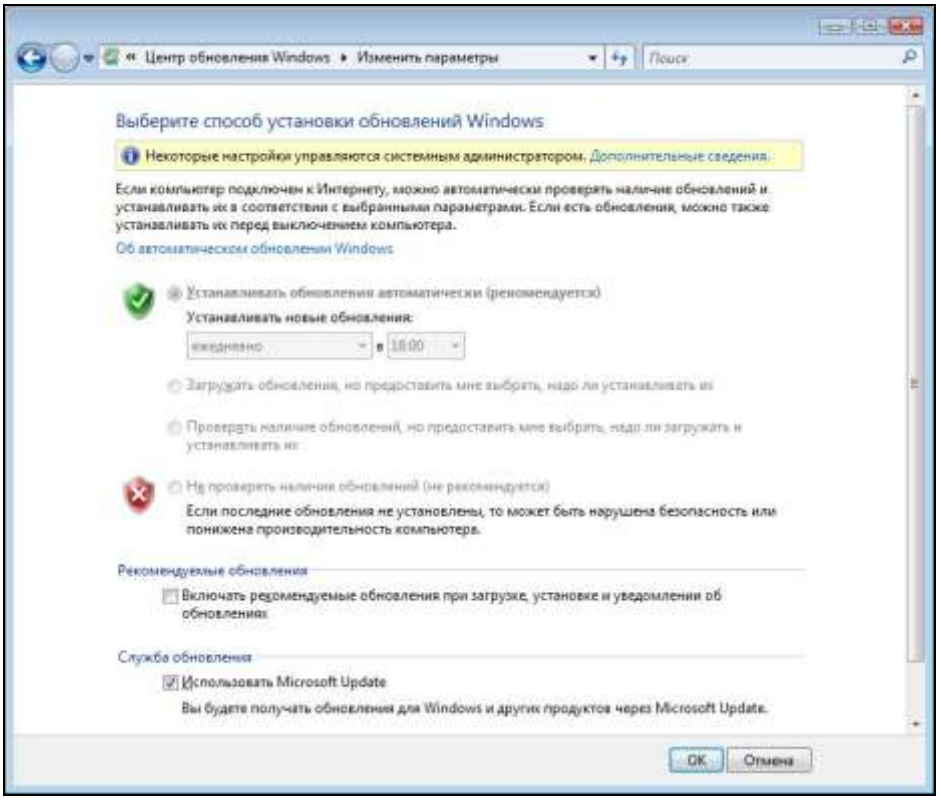


Рис. 4.1. Настройка режима обновления операционной системы Windows

Настройка обновлений с сервера интрасети

Microsoft выпустил бесплатный пакет установки сервера обновлений — WSUS, позволяющий создать у себя в сети сервер обновлений. Этот сервер фактически является прокси-сервером для обновлений с сайта Microsoft.

> ***Примечание***
>
> Не забудьте, что на системы Windows 2000 и Windows XP без пакетов обновлений необходимо предварительно установить пакет автоматического обновления, который нужно загрузить с сайта Microsoft.

Устанавливать WSUS в небольшой сети не имеет смысла, поскольку экономия на трафике будет не столь существенной, по сравнению с затратами на поддержание сервера в работоспособном состоянии и периодический контроль результатов операций для локальных систем. Однако серверы WSUS часто устанавливают интернет-провайдеры и разрешают использование их для обновлений систем из обслуживаемых диапазонов. При этом трафик с такого сервера, как правило, тарифицируется как бесплатный.

Для реализации локального сервера обновлений необходимо выполнить настройку систем. Сделать это предпочтительно через настройку групповой политики (запустить оснастку следует командой `gpedit.msc` — рис. 4.2).

Параметры настройки сервера обновления расположены по пути **Конфигурация компьютера | Административные шаблоны | Компоненты Windows | Центр обновления Windows**. Минимально необходимо определить адрес сервера, другие параметры (время обновления и т. п.) уточняются при необходимости.

Другой способ заключается в непосредственном указании в реестре систем адреса сервера обновлений:

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
        WUServer=http://адрес
        WUStatusServer=http://адрес
```

Системы с Vista несмотря на подобные установки иногда обращаются за обновлениями на сайт Microsoft. Если вы не хотите платить за данный трафик, то ограничьте доступ только к локальному серверу обновления средствами межсетевого экрана.

Локальные системы загружают обновления с помощью службы HTTP, которая не применяет настройки доступа в Интернет из обозревателя. Это может осложнить процесс обновлений при наличии в локальной сети прокси-сервера. В этом случае необходимо воспользоваться утилитой proxycfg, включенной

в состав Windows XP начиная со второго обновления. Ключи утилиты описаны в библиотеке Microsoft (**http://msdn.microsoft.com/en-us/library/aa384069%28VS.85%29.aspx**), обычно достаточно выполнить команду

```
proxycfg -p адрес:порт
```

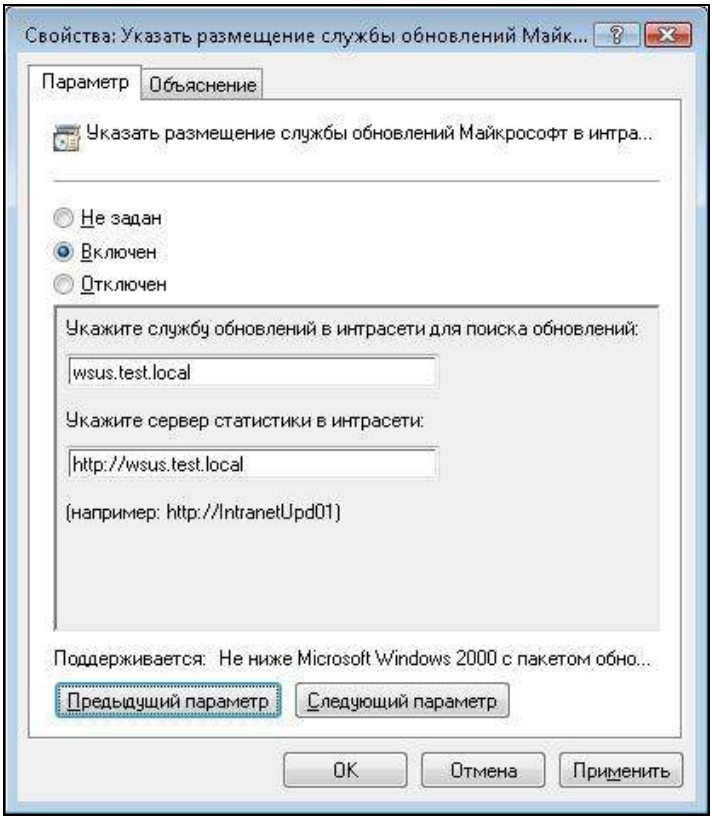


Рис. 4.2. Настройка параметров сервера обновления

Замечания

Для предыдущих версий, в том числе и для систем с Windows 2000, можно воспользоваться данной утилитой, просто скопировав ее с Windows XP Sp2.

Клонированные системы не могут использовать сервер обновлений до тех пор, пока вручную не будет выполнен ряд настроек. Подробности операций описаны на странице **http://support.microsoft.com/Default.aspx?id=903262**. Это не касается систем с Windows Vista.

Нужно ли устанавливать все обновления?

Обновления принято подразделять на критические, рекомендуемые и обновления драйверов (программного обеспечения видеоадаптеров, материнских плат и т. п.). Общая рекомендация заключается в обязательной установке всех критических и рекомендуемых обновлений. Однако если вы обладаете некоторым опытом администрирования систем, то можете сделать осознанный выбор. Например, стоит или нет устанавливать обновление безопасности, основная цель которого — исключить возможность пиратской активации Vista. Или обновить медиапроигрыватель, которым вы точно не будете пользоваться. Понятно, что реальной безопасности эти обновления не прибавят, а потенциально нарушить работу системы смогут.

Каждое обновление сопровождается соответствующим бюллетенем безопасности, в котором описаны устраняемые уязвимости. Достаточно внимательно прочитать этот документ, чтобы принять верное решение. Для отключения установки обновления в Windows при использовании технологии Windows Update достаточно просто скрыть его, для установки скрытого обновления — отобразить список скрытых обновлений и подтвердить необходимость установки (рис. 4.3).

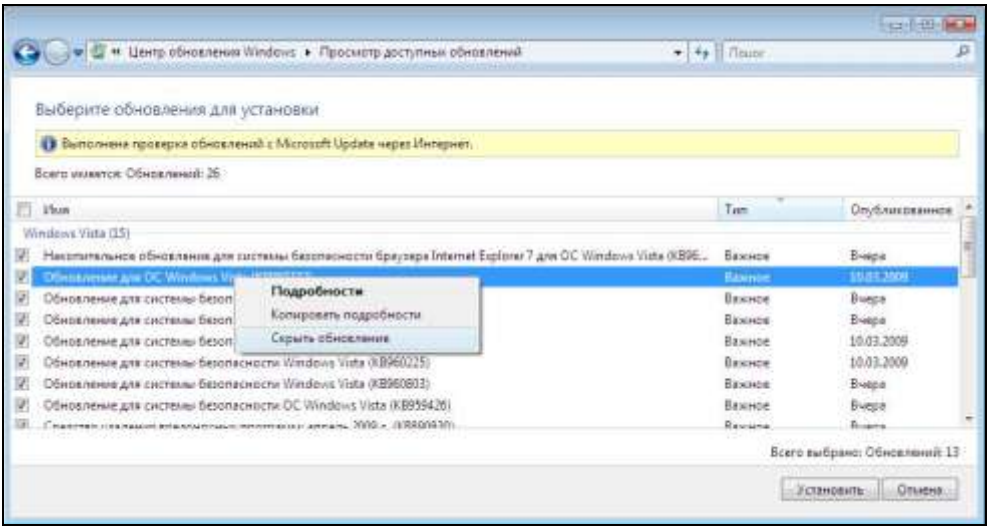


Рис. 4.3. Скрытие и отображение обновлений Windows

Клонирование систем

Сэкономить свое время при вводе новой системы можно, если выполнить *клонирование* жесткого диска.

Клонирование представляет собой процесс воспроизведения данной системы на другом рабочем месте. Клонированная станция будет иметь аналогичную версию операционной системы, те же установленные (и соответствующим образом настроенные) прикладные программы пользователей и т. п. К клонированию обычно прибегают при обновлении аппаратной части рабочего места (новый системный блок), при восстановлении "упавшего" компьютера, при создании типовых рабочих мест и т. д.

Существуют различные способы клонирования. Это и простое дублирование структуры жесткого диска, и тот или иной вариант удаленной установки, входящей в состав Windows, и перенос настроек с одного компьютера на другой. Администратор выбирает тот вариант, который оптимальным образом подходит для его системы.

WAIK

Система автоматизации установки Windows — Windows Automation Installation Pack — позволяет установить ОС и прикладные программы на новый системный блок при загрузке его из сети и наличии необходимых установленных служб.

К сожалению, WAIK, заменивший службы удаленной установки (Remote Installation Service), достаточно трудоемок в настройке и требует специальных усилий администратора для подготовки восстановления операционных систем предыдущих выпусков (до Windows Vista 7).

Поэтому на практике более распространен вариант клонирования систем через дублирование жесткого диска с использованием продуктов третьих фирм.

Дублирование жесткого диска

Наиболее простой вариант создания копии системы заключается в дублировании жесткого диска. Существует несколько программ, с помощью которых можно выполнить подобную операцию. Наиболее популярна программа GHost от Symantec, часто применяют утилиты от Acronis (**http://www.acronis.ru/**).

Структуру жесткого диска можно копировать непосредственно с диска на диск как на одном компьютере, так и на различных системах при подключении через COM-, LPT-, USB-порты или сеть. Можно сохранить образ диска в виде

файла и на его основе создать последующие копии дисков. Последний вариант наиболее удобен в практике администрирования, поскольку подготовить инфраструктуру для восстановления в такой конфигурации не представляет особого труда.

> ***Примечание***
>
> Поскольку при шифровании данных применяется уникальный идентификатор безопасности, который заменяется программами дублирования диска, то для сохранности информации *все зашифрованные файлы необходимо расшифровать перед клонированием*.

Для систем на базе ядра Windows NT простая перестановка жесткого диска с одной системы на другую обычно заканчивается "голубым экраном смерти" (BSOD). Происходит это, в основном, по причине отличающихся драйверов доступа к жестким дискам и из-за различия библиотек доступа к оборудованию компьютера — HAL (Hardware Abstraction Layer). Поэтому жесткий диск перед переносом на другой системный блок (или перед операцией клонирования) необходимо специальным образом подготовить.

> ***Замечание***
>
> Различают три основных типа компьютеров, которым требуются отличающиеся HAL. Это Standart PC, ACPI PC, ACPI Uniprocessor PC. Кроме того, HAL отличаются для одно- и многопроцессорных систем. Компьютерные бренды могут иметь собственные коды, поставляемые производителями.

В состав операционной системы входит специальная программа, подготавливающая диск с ОС Windows к переносу на другую систему — утилита sysprep.

Подготовка к клонированию: утилита sysprep

Утилита `sysprep` входит в состав дистрибутива системы. Утилита находится в папке Support\Tools\ установочного компакт-диска системы в архиве deploy.cab.

> ***Замечание***
>
> Версии утилиты отличаются для различных операционных систем. При возможности следует всегда отдавать предпочтение наиболее свежим версиям. Например, с версии 1.1 добавлена возможность обнаружения при завершении установки новых драйверов IDE-дисков. Проверить наличие новых версий необходимо на сайте изготовителя.

`Sysprep` "возвращает" ОС в процесс установки, к моменту определения состава оборудования. Причем все прикладные программы, которые установлены на исходной системе, останутся работоспособными после переноса на новый компьютер.

Иными словами, после того, как будет включен компьютер с диском, подготовленным утилитой sysprep, пользователь увидит завершающие шаги процесса установки операционной системы.

Для ускорения завершения установки можно создать файл ответов. В результате, например, не придется вводить серийный номер системы или указывать часовой пояс. А для того, чтобы диск мог быть использован на другом системном блоке, можно добавить в установочные файлы драйверы устройств, которые отсутствуют в исходном дистрибутиве ОС.

Чтобы подготовить эталонный образ жесткого диска, нужно выполнить следующие шаги:

1. Установите на типовой компьютер нужную версию операционной системы, последние обновления безопасности, все прикладное программное обеспечение (программы офиса, антивирусное ПО, обозреватели Интернета третьих фирм и т. п.).
2. Создайте на диске (в корне) папку SYSPREP, запишите в нее утилиты Sysprep.exe и Setupcl.exe (эта папка после установки системы будет автоматически удалена).
3. Чтобы исключить запросы дополнительной информации после переноса диска на новый компьютер (например, запроса серийного номера Windows), создайте в папке SYSPREP файл ответов. Проще всего воспользоваться программой диспетчера установки (Setupmgr.exe). После генерации файла ответов желательно просмотреть его и включить дополнительные параметры, если это необходимо.
4. После сохранения файла ответов запустите программу `sysprep`. По завершении ее работы исходный компьютер нужно выключить.

> ***Замечание***
>
> Если предполагается наличие не PnP-устройств, то при запуске укажите ключ `-pnp`. Это позволит обнаружить такие устройства на новом компьютере, но может существенно (до 20 мин) увеличить процесс установки.

Теперь с такого эталонного жесткого диска можно получить файл образа, который пригоден для клонирования исходного компьютера. Для этого достаточно воспользоваться загрузкой с компакт-диска, на котором записана программа и имеются средства сетевой работы. Подобный диск достаточно легко найти в Интернете, если создание его собственными силами вызывает сложности.

Восстановление системы

Процесс восстановления весьма прост. Следует загрузиться на новой системе с компакт-диска, на котором присутствует программа клонирования жесткого диска и имеются средства сетевой работы. После чего запустить эту программу и восстановить жесткий диск из образа, хранящегося в сети организации. На рис. 4.4 представлен один из шагов восстановления жесткого диска из файла образа. Для примера выбрана программа от Acronis, но администратор легко может найти и другие продукты. Восстанавливать диск можно из файла, который хранится либо на сетевых ресурсах локальной сети, либо в специальных разделах серверов восстановления (для коммерческих продуктов).

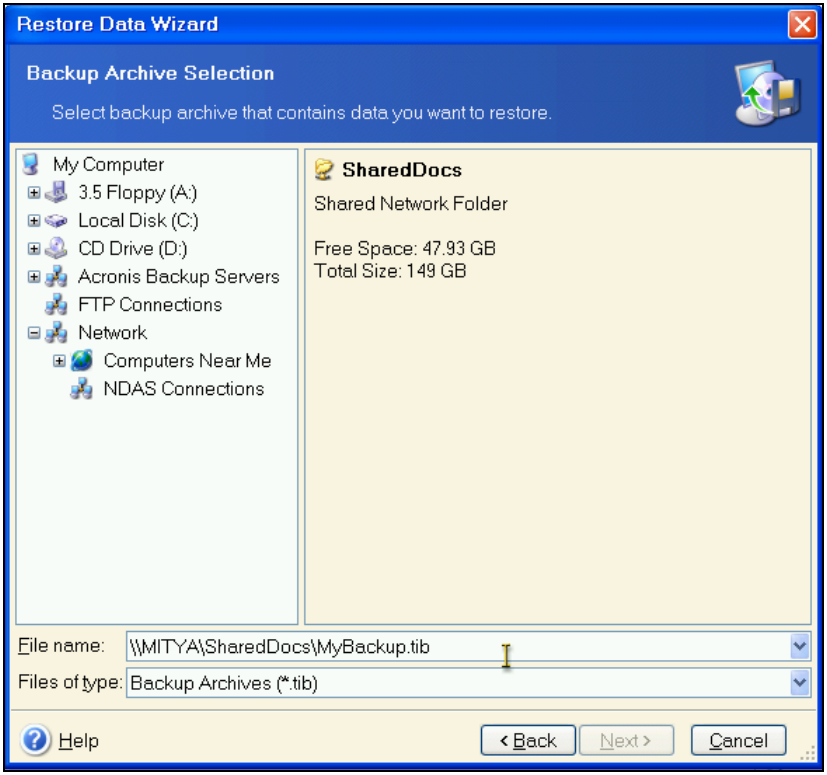


Рис. 4.4. Процесс восстановления жесткого диска из файла образа

После завершения восстановления образа следует перезагрузить систему с жесткого диска. Начнется финальный этап установки операционной системы. Обычно через несколько минут система завершит процесс установки

и будет полностью работоспособна. Как правило, основное время восстановления затрачивается на копирование файла образа диска по сети.

Подготовка образа диска к восстановлению на отличающемся оборудовании

Описанные действия создают образ системы, который можно развернуть на *аналогичные* конфигурации компьютеров. Однако в организации комплектации рабочих станций часто существенно отличаются друг от друга, а драйверы используемых в них устройств часто *не входят* в состав дистрибутива операционной системы.

> ***Замечание***
>
> Конечно, можно воспользоваться утилитами редактирования файла образа диска, добавить в него необходимые папки и изменить соответствующим образом файлы настроек. Но это требует наличия специальных программ (коммерческих) и некоторого опыта работы с ними.

Чтобы `sysprep` "заставила" программу установки протестировать на новой системе все типы жестких дисков, следует включить в файл ответов такие строки:

```
[Sysprep]
BuildMassStorageSection = Yes
[SysprepMassStorage]
```

Чтобы добавить новые драйверы устройств, которые отсутствуют в дистрибутиве Windows, внутри папки SYSPREP создайте папку с названием, например, Drivers. Для удобства можно сделать структуру папки разветвленной, например, создать папки Drivers\Video, Drivers\Net и т. п. Скопируйте в эти папки OEM-драйверы устройств компьютеров вашей сети.

> ***Примечания***
>
> Можно разместить драйверы и в другом месте, например, в корневой папке жесткого диска, соответственно подправив путь к ним в файле ответов. Причина размещения драйверов именно в папке SYSPREP — это автоматическое ее удаление после завершения установки системы.
>
> По умолчанию драйверы должны содержать цифровую подпись изготовителя. В противном случае их установка будет отложена до первого входа администратора в систему. Если необходимо разрешить установку драйверов без цифровой подписи, то следует включить в секцию `[Unattended]` файла ответов строку `DriverSigningPolicy = Ignore`.

После чего дополните файл ответов Sysprep.inf в разделе `[Unattended]` ссылками на папку с драйверами по следующему образцу:

```
OemPnPDriversPath = <путь_к_папке_драйверов>;<путь_к_папке_драйверов>
```

Желательно включить в образ максимальное число драйверов, чтобы обеспечить его универсальность. Добавленные вами папки должны быть перечислены через точку с запятой. Например:

```
OemPnPDriversPath = "sysprep\Drivers\net; sysprep\Drivers\Video"
```

После завершения этих операций запустите утилиту `sysprep` для подготовки диска к переносу.

Клонирование компьютеров-членов домена

В домен Windows входят не только пользователи, но и компьютеры. Поэтому дублирование дисков не может проводиться для создания копий рабочих станций и серверов, являющихся *членами домена*, т. к. в домене не может быть двух идентичных учетных записей (за исключением контроллеров домена, которые имеют одинаковый идентификатор SID). Необходимо сначала перевести компьютер в рабочую группу, после чего клонировать диски и добавить новые станции в домен.

> ***Примечание***
>
> Обратите внимание, что коммерческие программы дублирования дисков, например, уминавшаяся ранее программа Symantec GHost CE, имеют специальные функции для клонирования станций-членов домена. При установке такой программы учетная запись, от имени которой она будет запускаться, наделяется правом добавления рабочих станций в домен. В результате появляется возможность клонирования диска и последующего автоматического добавления системы в домен за одну операцию. Для пользователя это воспринимается как клонирование станции-члена домена.

Сброс пароля администратора Windows

Для Windows существует несколько утилит, позволяющих заменить пароль администратора (в том числе и администратора домена). Среди коммерческих вариантов едва ли не самая популярная — это программа ERD Commander (**http://www.winternals.com/**). Программа создает загрузочный компакт-диск, который позволяет не только заменить пароль администратора, но и отредактировать настройки реестра системы, использовать сетевой доступ для копирования файлов (после загрузки система "видит" сеть) и выполнить другие операции конфигурирования систем на основе Windows.

Среди бесплатно распространяемых программ можно отметить Offline NT Password Editor (**http://home.eunet.no/~pnordahl/ntpasswd/**), которая неоднократно успешно применялась автором для восстановления паролей на Windows NT 4.0, серверах и рабочих станциях Windows 2000, Windows XP. С этого сайта вы можете скопировать себе образ загрузочного диска (если

компьютер оборудован дисководом гибких дисков, то образы для диска есть, в общем случае придется закачивать образ загрузочного компакт-диска, но все равно объем закачки составит порядка 3 Мбайт).

После загрузки образа, его необходимо "прожечь" на матрицу компакт-диска. Стартовав с такого компакт-диска, вы получаете доступ к реестру системы и можете заменить любой пароль. По умолчанию опции программы предполагают смену пароля локального администратора. Так что вам достаточно только соглашаться с предложениями программы на каждом ее шаге.

Учитывая, что не все читатели свободно владеют английским языком, на котором выводятся сообщения этой программы, опишем действия, которые нужно выполнить пользователю для смены пароля.

После того как в BIOS компьютера вы установите порядок загрузки, начинающийся с CD-ROM, вставьте записанный диск в привод и загрузите с него компьютер. Первый раз программа приостановится, спрашивая вас, не нужно ли выбрать какой-либо особый вариант загрузки, например, отключить USB-устройства. Как правило, следует продолжить работу с параметрами по умолчанию, нажав <Enter>.

Первый шаг в операциях по смене пароля — выбор раздела жесткого диска, на котором установлена операционная система Windows. Программа просматривает структуру диска и самостоятельно предлагает номер раздела (список найденных разделов выше выбора, предлагаемого программой) (листинг 4.1).

Листинг 4.1

```
================================================================================
Step ONE:  Select  disk  where  the  Uindous  installation  is
================================================================================
Disks:
Disk /dev/sda:   21.4  GB, 21474836480 bytes
Candidate Windows partitions found:
 1   : /dev/sda   20465 MB BOOT
Please select partition by number or
 q = quit
 d = automatically start disk drivers
 m = manually select disk drives to load
 a = fetch additional   drivers from floppy / usb
 l = show probable Windows (NTFS) partitions only
Select: [1]
```

Программа нашла раздел, содержащий установку Windows, и предлагает выбрать его для дальнейших операций. Вам достаточно просто нажать <Enter>. Раздел будет подключен, о чем на экран будет выведено сообщение, приведенное в листинге 4.2 (обратите внимание на сообщение об удачном подключении — *Success!*).

Листинг 4.2

```
Selected 1
Mounting from /dev/sda1, whith assumed filesystem type NTFS
So, let's really check if it is NTFS?
Yes, pead-write seems OK
Mounting   it.   This  may   take up to a few minutes:
Success!
```

На втором шаге необходимо указать путь хранения файлов реестра. Здесь также вы должны просто согласиться и нажать <Enter> (листинг 4.3).

Листинг 4.3

```
================================================================
Step TWO: Select PATH and registry files
================================================================
What is the path to the registry directory? (relative to windows disk)
[WINDONS/system32/config]    :
```

Следующим шагом нужно выбрать операцию. Поскольку мы запустили программу для смены пароля, то согласимся с предложениям сброса пароля, нажав Enter (листинг 4.4).

Листинг 4.4

```
Select which part of registry to load, use predefined choices
or list the files with space as delimiter
1 — Password  reset   [sam  system  security]
2 — RecoveryConsole parameters     [software]
q — quit — return to previous
[1] :
```

На экран будет выведена информация по файлам реестра (листинг 4.5). Обратите внимание на последние строки, которые описывают действующую политику паролей.

Листинг 4.5

```
* SAM policy limits:
Failed logins before lockout is:  0
Minimum password length        :  0
Password  history  count       :  0
<>========<>  chntpw  Main  Interactive  Menu  <>========<>
Loaded  hives:  <SAM>  <system>  <SECURITY>
 1 — Edit  user  data  and  passwords
 2 — Syskey  status  &  change
 3 — RecoveryConsole  settings
     - - -
 9 — Registry  editor,  now  with  full  write  support!
 q — Quit  (you  will  be  asked  if  there  is  sonething  to  save)
What  to  do?  [1]  ->
```

Если вы захотите сменить пароль, то необходимо соблюсти эти требования (например, минимальную длину пароля). В качестве следующего шага выбираем опцию редактирования пароля (значение по умолчанию, просто нажимаем <Enter>).

Теперь программа выведет на экран перечень учетных записей системы. Если они русскоязычные, то вы увидите "бессмысленный" набор символов (листинг 4.6). Но программа по умолчанию выбирает для редактирования учетную запись администратора, так что вы также можете просто согласиться с предложенным вариантом (нажать <Enter>).

Листинг 4.6

```
====  chntpw  Edit  User  Info  &  Passwords  ====
| RID  -|----------Username-----------|  Admin?  |-  Lock?  —|
| 01f4  |  Administrator              |  ADMIN   |
| 01f5  |  Guest                      |          |  dis/lock  |
Select: q - quit, . - list users, 0x<RID> - User with RID (hex)
or  simply  enter the username  to change:  [Administrator] _
```

А вот на следующем шаге необходимо явно указать, что вы собираетесь сделать. Я рекомендую сбрасывать пароль до пустого значения, т. к. эта опера-

ция срабатывает во всех случаях (вам не придется разбираться с ограничениями политики паролей и т. д.). Поэтому нажмите клавишу <1>, когда увидите на экране строки, аналогичные приведенным в листинге 4.7.

Листинг 4.7

```
- - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Edit (set new) user password (careful with this on XP or Vista)
 3 - Promote user (make user an administrator)
(4 - Unlock and enable user account) [seems unlocked already]
 q - Quit editing user, back to user select
Select: [q] >
```

Пароль сброшен, и теперь нужно выйти из программы с сохранением результатов (иначе изменения внесены не будут). Для этого нажмите несколько раз клавишу <q> для выхода из режима редактирования.

Последним шагом необходимо указать, что изменения должны быть записаны (нажать клавишу <y>) и перезагрузить после этого компьютер в обычном варианте (листинг 4.8).

Листинг 4.8

```
================================================================================
Step FOUR: Writing back changes
================================================================================
About to write file(s) back! Do it? [n] :
```

После того как вы сбросили таким способом пароль администратора, можно войти в систему и получить *полный* контроль над компьютером.

> ***Примечание***
>
> При смене пароля в Windows следует учитывать, что если на компьютере имелись файлы или папки, зашифрованные с использованием свойств файловой системы (EFS), то они после смены пароля станут недоступными. Принципиально можно попытаться подобрать к ним пароль, применяя одну из утилит восстановления пароля к EFS, но такая попытка будет удачна только в том случае, если пароль был выбран недостаточно сложным (хотя к таковым, по практике автора, относится подавляющее число паролей пользователей). При наличии зашифрованных файлов можно также попытаться подобрать пароль пользователя, воспользовавшись одной из доступных утилит, например, Cain&Abel (**http://www.oxid.it/cain.html**).



Глава 5

Доменная организация информационной системы

Для упрощения управления компьютерами можно создать систему централизованного управления. В случае Windows это означает создание *домена*.

В доменах Windows каждый компьютер "теряет" свою автономность, он подчиняется общим правилам (*политикам*), а администратор домена получает полные права на каждой системе, включенной в домен. Локальный администратор может осуществлять свои функции в некоторых пределах, пока они не противоречат настройкам, заданным администратором домена.

Домены Windows могут быть реализованы и средствами Linux. Так, за создание и работу домена Windows "отвечает" пакет Samba, так же, как и в Windows, данные домена могут храниться в службе каталогов (пакет OpenLDAP), аутентификация происходить с использованием Kerberos (точнее, в Windows реализован открытый протокол Kerberos, применяемый в Unix-системах) и т. п.

Указать некое число компьютеров, когда более выгодно централизованное управление, достаточно сложно. Все зависит от конкретной практики администрирования. Обычно при наличии 20–30 компьютеров уже имеет смысл настроить централизованное управление.

Структура домена Windows

В настоящее время домены Windows хранят информацию о своей структуре с помощью *службы каталогов* (Active Directory). Взаимодействие со службой каталогов происходит по протоколу LDAP (Lightweight Directory Access Protocol, протокол облегченного доступа к каталогам). Этот протокол является открытым стандартом, что позволяет осуществлять взаимодействие со службой каталогов различным приложениям.

Примечание

Поэтому утилитами, использующими протокол LDAP, из состава Windows можно работать с серверами LDAP из состава Linux и наоборот. Конечно, существуют некоторые ограничения и особенности реализации, в том числе и каталогов различных вендоров, например, IBM, Novell и т. д., но мы не будем их касаться в данной книге.

В терминах службы каталогов мы в домене работаем с *объектами.* Пользователи, компьютеры, подразделения, территории, предприятия и т. п., — все это объекты службы каталогов. Каждый объект описывается различными характеристиками — *свойствами*. Например, у пользователя это имя, фамилия, группа, в которую он входит, время действия учетной записи, допустимые часы работы в компьютерной сети, адрес электронной почты и т. п.

Работа со всеми объектами службы каталогов производится с учетом прав доступа (кто может создать нового пользователя, кому разрешено перевести его в другую штатную структуру и т. п.), сами операции специфичны для каждого объекта. Набор объектов, их атрибутов (свойств) и методов (допустимых операций) принято называть *схемой каталога*.

Служба каталогов Windows имеет следующую организационную структуру:

- лес;
- дерево;
- домен;
- организационное подразделение (OU);
- сайты.

Основная структурная единица домена, с которой придется работать администратору, это *подразделение*. Подразделение (Organization Unit, OU) OU — это своеобразный контейнер, в который можно помещать как компьютеры, так и пользователей (естественно, что речь идет о соответствующих логических объектах). Основная причина создания OU для администраторов системы — возможность применения к объектам OU *групповых политик*.

Каждое OU может, в свою очередь, содержать внутри себя любое количество вложенных OU, учетные записи компьютеров и пользователей, группы (пользователей).

Если на одном предприятии существуют несколько доменов с различными пространствами имен (например, **testorg.ru** и **testorg.cs**), то, представленная графически, такая структура будет напоминать *лес*. Лес — это коллекция (одного или более) доменов Windows, объединенных общей схемой, конфигурацией и двусторонними транзитивными доверительными отношениями.

Если домены и OU описывают логическую организацию, то *сайты* (Sites) предназначены для описания *территориальных делений*. Считается, что *внутри одного сайта* присутствуют скоростные каналы связи (обычно компьютеры сайта находятся в одном сегменте локальной сети). А различные сайты связаны друг с другом относительно медленными каналами связи. Поэтому между ними создаются специальные механизмы репликации данных. Например, можно задать график репликации (использовать периоды наименьшей загрузки каналов связи), выбрать определенный протокол (IP или путем приема/передачи сообщений по протоколу SMTP) и т. п.

Соотношение территориальной и логической структуры выбирают исходя из конкретной конфигурации предприятия. Например, можно создать несколько сайтов в одном домене или сформировать в каждом сайте свой домен и т. п.

Для небольшого предприятия обычно создают структуру "один лес — один домен — несколько подразделений — один сайт".

Хозяева операций

В домене Windows 200*x* все контроллеры *равнозначны*. Однако для обеспечения правильной синхронизации данных между различными контроллерами некоторые функции зафиксированы только за одной системой. Такие функции носят название Flexible Single Master Operation role (FSMO). В доменах Windows 200*x* их пять:

- Schema master (один на лес).
- Domain naming master (один на лес).
- RID master (один на домен).
- PDC emulator (один на домен).
- Infrastructure master (один на домен).

При первоначальной установке домена все пять ролей зафиксированы за первым контроллером. Впоследствии их можно переносить на другие контроллеры, учитывая специфику структуры организации. Важно только, чтобы при исключении контроллера домена администратор был уверен, что все эти пять операций не потеряли хозяина.

Три роли (PDC, RID, Infrastructure) легко переносятся с помощью оснастки **AD Пользователи и компьютеры**. Необходимо просто открыть оснастку, подключиться к тому контроллеру домена, на который планируется перенести соответствующую роль, и выполнить соответствующую команду в меню.

Все операции по переносу ролей можно выполнить в командной строке. Для этого служит утилита `ntdsutil`. Главное, что эта утилита пригодна не только

для переноса ролей при *работающих* контроллерах, но и для *назначения* нового владельца роли в случае аварийного выхода из строя прежнего хозяина.

> ***Примечание***
>
> Роли следует назначать с осторожностью, при полной уверенности в том, что прежний хозяин не будет вновь доступен в сети. Появление двух хозяев одной роли может привести к неработоспособности всего домена.

Опишем кратко последовательность операций, которые необходимо выполнить для назначения контроллеру домена новой роли.

Открыть утилиту и набрать команду `ROLES`.

1. Указать, к каким контроллерам необходимо подключиться, для чего набрать команду `CONNECTIONS` и ввести команду подключения к необходимому контроллеру. После чего закрыть опцию `CONNECTIONS`, набрав `QUIT`.
2. Выбрать нужную команду `SEIZE ...`, чтобы переписать соответствующую роль.

Утилита сначала попытается корректно перенести выбранную роль и лишь при недоступности соответствующего контроллера будет выполнена операция перезаписи.

Сервер глобального каталога (GC)

Контроллеры домена хранят информацию об объектах *текущего* (собственного) домена. Поскольку в логической структуре предприятия может существовать несколько доменов, то для выполнения операций, затрагивающих объекты разных доменов, необходим доступ к соответствующим контроллерам. Для ускорения операций в системе существуют специальные контроллеры, которые в режиме только для чтения хранят *все объекты леса*, но не с полным, а с частичным набором атрибутов. Такие контроллеры называются *серверами глобального каталога* (Global catalog, GC).

В качестве GC может быть назначен любой контроллер домена. Назначение контроллера домена сервером глобального каталога производится через оснастку **AD – Сайты и Службы**. Раскрыв узел, соответствующий нужному контроллеру, в свойствах **NTDS Settings** необходимо включить параметр использования контроллера в качестве GC.

Серверы GC хранят наиболее часто используемые атрибуты объектов. Условно можно считать, что объем хранимых на GC данных снижается примерно в два раза по сравнению с "полным" вариантом описания объекта. Но если конкретным приложениям необходим частый доступ к нереплици-

руемым атрибутам, то администратор может внести изменения в параметры GC, откорректировав *схему организации*. Для этого достаточно в консоли управления оснасткой **AD Schema** (по умолчанию этой оснастки нет в списке меню, ее следует добавить в консоль управления) включить репликацию в свойствах соответствующих атрибутов.

Создание нового домена

Создание домена на серверах Windows

Для создания нового домена необходимо запустить утилиту `dcpromo` (ее можно стартовать также из задачи управления сервером, выбрав в меню пункт создания контроллера домена). В зависимости от ответов на вопросы мастера операции, вы сможете добавить новый контроллер в существующем домене либо создать новый домен. Можно создать новый домен внутри уже существующего, либо создать новое дерево доменов, дав домену уникальное имя. Все операции достаточно просты и обычно выполняются в течение нескольких минут. После чего, перезагрузив компьютер, вы получаете новый контроллер домена.

Перед началом операции следует тщательно обдумать то доменное имя, которое вы дадите вновь создаваемому домену. Если ваша организация имеет уже зарегистрированное в Интернете доменное имя, то имя домена Windows может быть основано на нем. Ничто не запрещает вам избрать для внутреннего домена имя, которое не соответствует реальным доменам Интернета, например, дать название **myorg.local**.

> ***Замечания***
>
> Можно присвоить внутреннему домену реальное имя Интернета, а можно дать только локальное название. В любом случае по соображениям безопасности данные структуры домена Windows (DNS-сервера) *не публикуются* в Глобальной сети.
>
> Обратите внимание, чтобы полное доменное имя *не являлось именем первого уровня*, а обязательно состояло из двух частей. В противном случае необходимо выполнить ряд дополнительных настроек, которые следует уточнить по документации с сайта разработчика.

Создание домена обязательно требует наличия сервера DNS. По умолчанию (если сервер DNS не настроен) программа установки предлагает создать и настроить локально сервер DNS. В общем случае служба каталогов не требует обязательного DNS-сервера разработки Microsoft. AD может быть установлена, например, на сервер BIND. При этом следует учесть, что BIND

версии 4.9.7 и старше поддерживает возможность создания SRV-записей, которые необходимы для работы службы каталогов. А начиная с версии 8.2.2 поддерживаются и динамические обновления записей данного типа.

Настройка Ubuntu в качестве контроллера домена

Серверы Linux в качестве контроллеров домена

На сегодня Linux-системы не могут выступать в качестве контроллеров домена, аналогичных контроллерам службы каталогов Windows. Эта функциональность планируется в следующей версии пакета Samba. Но Linux-системы можно настроить как контроллеры домена, идентичные доменам Windows NT 4.0. При такой конфигурации контроллеры домена будут обеспечивать централизованную аутентификацию пользователей и компьютеров.

> ***Примечание***
>
> В настоящее время идет разработка версии 4 пакета Samba, которая реализует функциональность серверов Windows 2008. Сроки выхода стабильных релизов пакета пока не называются.

Настройка Linux-системы для использования в качестве контроллера домена широко описана в Интернете. Для этих целей предназначен пакет Samba, воспользоваться для настройки можно, например, статьей с сайта Ubuntu по адресу **https://help.ubuntu.com/8.10/serverguide/C/samba-dc.html** или любыми другими материалами. Найти информацию по настройкам и устранению возможных проблем достаточно легко.

Традиционные конфигурации предполагают хранение паролей пользователей в файлах на контроллерах домена. Сегодня существует более прогрессивная технология — хранение идентификационных данных в службах каталогов (серверах LDAP). Преимущества таких решений, во-первых, в универсальности: многие прикладные программы сегодня используют службы каталогов. Во-вторых, базы служб каталогов хорошо реплицируются между серверами, что позволяет создать отказоустойчивую структуру.

Настройка Samba+LDAP несколько более трудоемка. Она предполагает установку пакетов, настройку LDAP на функционирование по схеме Samba (иными словами, добавление в базу службы каталогов новых параметров для работы в домене), настройку Samba на аутентификацию в LDAP. Эти процедуры весьма подробно описаны и рекомендации широко представлены в Сети (достаточно выполнить поиск на ключевые слова sabma, OpenLDAP|LDAP, ubuntu; например, **https://help.ubuntu.com/8.04/serverguide/C/openldap-server.html**). Мы же опишем более подробно настройку сервера

Ubuntu в качестве контроллера домена при наличии пакета OpenLDAP из состава Zimbra — программы коллективной работы, которая описана в настоящей книге в *главе 6*.

Настройка контроллера домена на сервере корпоративной почты Zimbra

> ***Примечание***
>
> В приведенном далее описании мы предполагаем, что используется пакет Zimbra версии 5 и он уже установлен в соответствии с рекомендациями *главы 6* на данном сервере. Мы не описываем настройку репликации OpenLDAP из состава Zimbra между основным и ведомым серверами. Эти операции необходимы при создании отказоустойчивых конфигураций. Описание настроек можно уточнить по документации Zimbra в случае необходимости.

В описании настроек данной конфигурации мы использовали рекомендации, содержащиеся на странице **http://wiki.zimbra.com/index.php?title=UNIX_and_Windows_Accounts_in_Zimbra_LDAP_and_Zimbra_Admin_UI** с небольшими изменениями, вызванными особенностями операционной системы. В частности, существенно упрощены советы по настройке аутентификации по LDAP по сравнению с рекомендациями на указанной страницей в связи с тем, что в Ubuntu имеются специальные сценарии, автоматически конфигурирующие соответствующие компоненты.

Для настройки домена на основе службы LDAP из состава Zimbra необходимо:

- установить расширения для управления учетными записями служб Postfix и Samba из административной консоли Zimbra;
- установить службу Samba в Ubuntu и настроить ее для LDAP-аутентификации;
- настроить LDAP из состава Zimbra для работы с Samba;
- настроить аутентификацию в Ubuntu на использование сервера LDAP.

Обратите также внимание, что время на рабочих станциях и контроллере домена должно быть синхронизировано. Отличия в текущем времени являются типовыми причинами ошибок добавления рабочих станций в домен.

Установка расширений Zimbra для управления служебными учетными записями

Чтобы управлять служебными учетными записями в административной консоли Zimbra, необходимо установить расширения zimbraSamba и ZimbraPosixAccount.

Расширения zimbraSamba и ZimbraPosixAccount входят в состав установочного комплекта Zimbra, но их необходимо перед установкой отредактировать, указав параметры вашего домена. После установки Zimbra их файлы находятся в папке /opt/zimbra/zimlets-admin-extra.

В обоих архивах необходимо отредактировать содержимое `config_template.xml`, для этого нужно извлечь этот файл, внести в него описанные далее изменения, сохранить их и этим файлом заменить исходный файл в архиве. Эти операции можно выполнить и за один шаг, если, например, воспользоваться возможностями пакета Midnight Commander по редактированию файлов внутри архива.

В файле `config_template.xml` необходимо установить реальное значение для параметра `ldapSuffix`. Его значение должно указывать на ваш домен. Например, если домен имеет имя example.com, то `ldapSuffix` следует заменить на `dc=example,dc=com`. Если у вас домен третьего уровня, то значение `ldapSuffix` может выглядеть примерно так: `dc=my_server,dc=example,dc=com`.

> ***Примечание***
>
> Можно также откорректировать параметры `uidBase` и `gidBase`. Они определяют начало нумерации идентификаторов при создании учетных записей пользователей и групп соответственно. По умолчанию они установлены в 10000, и если нет особых причин, то можно эту настройку сохранить.

После того как вы внесете необходимые изменения в оба архива, эти расширения нужно установить в Zimbra. Для чего достаточно зайти в административную консоль управления, слева в панели навигации выбрать **Конфигурация | Admin Extensions**, нажать на кнопку **Инсталляция** в правой части консоли и указать на отредактированные вами файлы архивов. Если администрирование ведется с удаленной системы, то эти файлы нужно предварительно на нее скопировать (выбор файлов возможен только с локальных дисков).

> ***Совет***
>
> Автор советует устанавливать расширения последовательно и после каждого шага перезагружать административную консоль (закрыть и снова открыть).

Установка Samba и сопутствующих пакетов

Для настройки сервера Ubuntu в качестве контроллера домена необходим пакет Samba. Кроме того, следует установить пакет samba-doc, в составе которого находится образец схемы, которую необходимо подключить к LDAP.

```
apt-get install samba samba-doc
```

После установки пакетов можно приступать к редактированию настроек Samba (/etc/samba/smb.conf). Основные параметры конфигурации должны соответствовать указанным в листинге 5.1.

Листинг 5.1

```
[global]

workgroup = EXAMPLE
netbios name =  my_server
os level = 33
preferred master = yes
enable privileges = yes
wins support =yes
dns proxy = no
name resolve order = wins bcast hosts
security = user
encrypt passwords = true
ldap passwd sync = yes
passdb backend = ldapsam:ldap://my_server.example.com/
ldap admin dn = cn=config
ldap suffix = dc=my_server,dc=example,dc=com
ldap group suffix = ou=groups
ldap user suffix = ou=people
ldap machine suffix = ou=machines
obey pam restrictions = no
passwd program = /usr/bin/passwd %u
passwd chat = *Enter\snew\spassword:* %n\n *Retype\snew\spassword:* %n\n
*password\supdated\ssuccessfully* .
domain logons = yes
logon path =
logon home =
logon script = logon.cmd
add user script = /usr/sbin/adduser --quiet --disabled-password --gecos
"" %u
add machine script = /usr/sbin/adduser --shell /bin/false --disabled-
password --quiet --gecos "machine account" --force-badname %u
socket options = TCP_NODELAY
domain master = yes
local master = yes

[homes]
comment = Home Directories
browseable =yes
read only = No
valid users = %S

[netlogon]
```

```
comment = Network Logon Service
path = /var/lib/samba/netlogon
guest ok = yes
locking = no

[profiles]
comment = Users profiles
path = /var/lib/samba/profiles
read only = No
```

В листинге 5.1 представлена только часть параметров, которые относятся к настройке LDAP-конфигурации Samba. Естественно, что имена из примера необходимо заменить на реальные названия серверов. Хотя код взят со страницы **http://wiki.zimbra.com/index.php?title=UNIX_and_Windows_Accounts_in_Zimbra_LDAP_and_Zimbra_Admin_UI**, основан он на примере конфигурации Samba из поставки пакета.

Дадим некоторые пояснения к примененным параметрам.

- `passdb backend` — в качестве его значения нужно указать имя вашего сервера LDAP (сервера Zimbra).
- `ldap admin dn` — параметр подключения к LDAP для Zimbra версии 5.
- `ldap suffix` — имя домена. Мы его указывали при редактировании файлов config_template.xml (параметр `ldapSuffix`).
- `ldap group suffix`, `ldap machine suffix` и `ldap user suffix` — определены в файле config_template.xml. Указанные значения — это их величины при установке Zimbra по умолчанию.

Сохранив настройки конфигурации, проверьте конфигурацию на отсутствие ошибок (командой `testparm`) и перестартуйте сервер Samba. Далее, в Samba необходимо назначить пароль для доступа к LDAP в Zimbra. Этот пароль сгенерирован Zimbra автоматически, его можно узнать или заменить. Чтобы его получить, следует перейти в режим суперпользователя (`sudo -s`), потом переключиться в учетную запись zimbra (`su - zimbra`) и выполнить команду от имени пользователя zimbra

```
zmlocalconfig -s ldap_root_password
```

После чего назначьте пароль, используемый Samba для доступа к LDAP, в соответствии с полученным значением:

```
smbpasswd -w пароль
```

Для настройки LDAP необходимо "представить" схему, используемую пакетом Samba, которая зависит от версии Samba и включена в состав пакета

samba-doc. Установите этот пакет и скопируйте схему (файл samba.schema, находится в архивированном виде как /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz, для распаковки введите команду `gunzip имя_архива`) в папку /opt/zimbra/openldap/etc/openldap/schema/.

Теперь необходимо указать серверу LDAP на использование схемы Samba и nis (схема nis входит в состав Zimbra, но не подключена к LDAP). Для этого откройте в текстовом редакторе файл /opt/zimbra/conf/slapd.conf.in и добавьте в него следующие строки после последней директивы `include`:

```
include "/opt/zimbra/openldap/etc/openldap/schema/nis.schema"
include "/opt/zimbra/openldap/etc/openldap/schema/samba.schema"
```

Желательно также назначить индексы и права доступа к разделам LDAP, добавив в конец этого же файла строки листинга 5.2.

Листинг 5.2

```
index uidNumber   eq
index gidNumber   eq
index memberUID   eq
index sambaSID          eq
index sambaPrimaryGroupSID eq
index sambaDomainName   eq
access to dn.subtree="ou=people,dc=my_server,dc=example,dc=com"
        by dn.children="cn=admins,cn=zimbra" write
        by * read

access to dn.subtree="ou=groups, dc=my_server,dc=example,dc=com"
        by dn.children="cn=admins,cn=zimbra" write
        by * read
```

ЗАМЕЧАНИЕ

Эти рекомендации есть в файле slapd.conf, который включен в состав примеров расширения ZimbraSamba.

После всех этих изменений следует перестартовать службы Zimbra (`zmcontrol stop & zmcontrol start`) и от имени пользователя zimbra выполнить следующие команды:

```
zmprov mcf +zimbraAccountExtraObjectClass posixAccount
zmprov mcf +zimbraAccountExtraObjectClass sambaSamAccount
```

Настройка параметров аутентификации

Для LDAP-аутентификации нужно добавить в систему пакеты pam_ldap и nss_ldap:

```
apt-get install libpam-ldap libnss-ldap nss-updatedb libnss-db
```

В процессе установки необходимо определить ряд параметров настройки, ответив на вопросы мастера операций. При настройке имени сервера следует указать ldap://*имя_сервера_Zimbra*. Параметр *Distinguished name of search base* определить в соответствии с именем домена — точно таким же, как и значение `ldapSuffix`, которое вы настроили в файлах zimbraSamba и ZimbraPosixAccount: `dc=example,dc=com` или `dc=my_server,dc=example,dc=com`.

Далее нужно задать версию LDAP равной 3, локального суперпользователя не следует определять администратором LDAP, но укажите, что сервер LDAP требует параметров учетной записи для подключения. Эта учетная запись должна быть введена как `cn=config`, на следующем шаге нужно указать пароль этой записи (мы его узнали чуть ранее, когда настраивали параметры доступа для службы Samba).

После завершения установки пакетов необходимо вручную внести некоторые дополнительные изменения. Во-первых, проверьте содержимое файла /etc/ldap.conf, чтобы в нем присутствовали строки по образцу, приведенному в листинге 5.3.

Листинг 5.3

```
host my_server.example.com
uri ldap://my_server.example.com
base dc=example,dc=com
binddn cn=config
bindpw пароль
rootbinddn uid=zimbra,cn=admins,cn=zimbra
port 389
nss_base_passwd ou=people,dc=my_server,dc=example,dc=com?one
nss_base_shadow ou=people,dc=my_server,dc=example,dc=com?one
nss_base_group ou=groups,dc=my_server,dc=example,dc=com?one
nss_base_hosts ou=machines,dc=my_server,dc=example,dc=com?one
bind_policy soft
nss_reconnect_tries 2
```

Замечания

Указанные строки находятся в разных частях файла и обычно закомментированы. Вам необходимо снять комментарий и отредактировать содержимое строк по фактическим именам сервера и домена.

В строке `bindpw`, строго говоря, указывается пароль для другой учетной записи. Но при установке по умолчанию этот пароль совпадает с полученным нами ранее значением. Проверить пароль можно командой `zmlocalconfig -s zimbra_ldap_password`.

Теперь необходимо изменить содержимое ряда файлов, отвечающих за аутентификацию пользователей. В качестве образца подходят рекомендации, содержащиеся в файле /etc/auth-client-config/profile.d/ldap-auth-config. Далее мы просто приведем названия файлов, которые следует отредактировать, и их новое содержимое (листинг 5.4).

Листинг 5.4

```
/etc/pam.d/common-auth
       auth       sufficient   pam_ldap.so
       auth       required     pam_unix.so nullok_secure use_first_pass

/etc/pam.d/common-account
       account    sufficient   pam_ldap.so
       account    required     pam_unix.so

/etc/pam.d/common-password=
       password   sufficient   pam_ldap.so
       password   required     pam_unix.so nullok obscure min=4 max=8 md5

pam_session=
       session    required     pam_unix.so
       session    required     pam_mkhomedir.so skel=/etc/skel/
       session    optional     pam_ldap.so
```

Следующим шагом отредактируйте файл /etc/nsswitch.conf (по умолчанию он настроен на хранение паролей в файлах). Замените строки, начинающиеся так же, как и в последующем примере, на такие значения:

```
passwd: files ldap
group: files ldap
shadow: files ldap
```

Перезагрузите сервер Ubuntu, чтобы изменения вступили в силу.

Замечание

Следует быть внимательным при редактировании перечисленных файлов. Перед изменением сохраните оригинальные версии файлов в виде копий. В случае ошибки может возникнуть ситуация, когда вы даже не сможете войти в систему, указывая верные параметры учетной записи. Тогда необходимо при старте Ubuntu выбрать вариант безопасной загрузки, зайти в систему в однопользовательском режиме (пароль не будет запрошен) и исправить файлы конфигурации.

После этих операций пользователей и группы Linux можно создавать в административной консоли Zimbra (рис. 5.1).

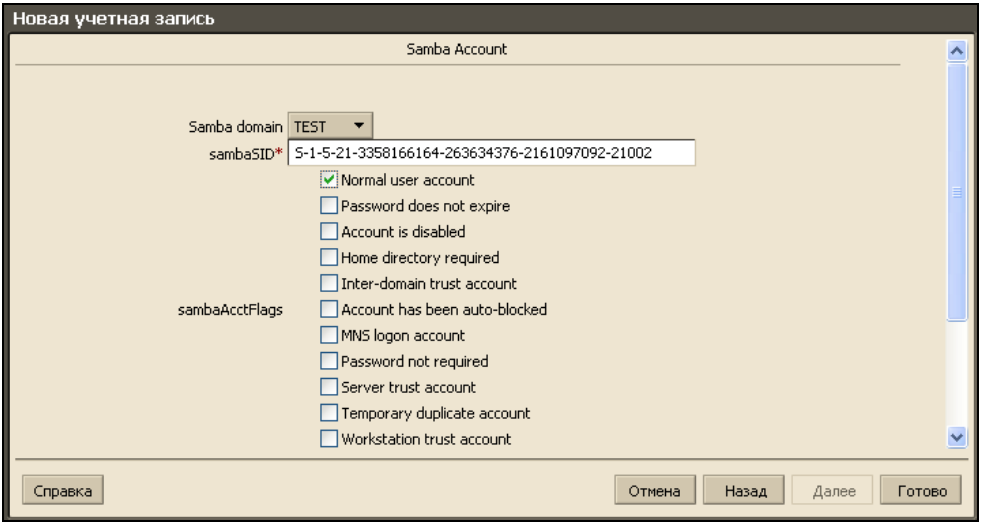


Рис. 5.1. Этап создания новой учетной записи ZCS в домене

После настройки на LDAP-аутентификацию при создании учетных записей в административной консоли Zimbra добавляются новые интерфейсы мастера операций. Необходимо указать параметры Postfix-учетной записи (обычно не требуется вносить какие-то пользовательские параметры, в качестве номера группы достаточно указать 2 — стандартное значение) и параметры в домене. Кроме того, следует определить ряд параметров настройки учетной записи в домене Samba.

Обязательно проверьте, что службе Samba доступны учетные записи, созданные в административной консоли Zimbra. Чтобы проверить индивидуальные учетные записи, нужно ввести команду `getent passwd`, которая должна показать как локальные учетные записи Ubuntu, так и учетные записи, хранящиеся на сервере LDAP Zimbra. Для проверки списка групп используйте команду `getent group`.

При возникновении ошибок в настройке следует проанализировать файлы журналов (журнала Samba, авторизации — auth.log и др.). Как правило, причины ошибок видны по соответствующим записям (например, отсутствие контакта с сервером LDAP из-за неверно назначенного пароля или невозможность завершения авторизации пользователя домена в силу необходимости смены пароля при первом подключении и т. п.).

Создание специальных групп

Для работы в качестве домена Windows должны быть созданы специальные группы. Для этого в консоли управления Zimbra необходимо создать группы Domain Admins и Domain Users (следует указать вариант создания специальных групп и просто выбрать эти группы из предлагаемого списка). Другие специальные группы, соответствующие стандартным группам домена Windows, можете создавать или не создавать по своему усмотрению.

Группе Domain Admins необходимо назначить специальные привилегии, с помощью которых будут реализовываться права администраторов домена. Для этого в командной строке выполните:

```
net rpc rights grant "EXAMPLE\Domain Admins" SeAddUsersPrivilege
SeMachineAccountPrivilege SePrintOperatorPrivilege
```

Этими шагами можно ограничиться в настройке сервера Ubuntu в качестве контроллера домена. Пользователи, интересующиеся тонкой настройкой системы в качестве контроллера домена Windows, могут ознакомиться с официальными рекомендациями разработчиков Samba на странице **http://us3.samba.org/samba/docs/man/Samba-HOWTO-Collection/**. Те, кто хочет проверить работу четвертой версии Samba, совместимой с Windows 2008, могут воспользоваться рекомендациями сайта **http://wiki.samba.org/index.php/Samba4/Debian**.

> ***Замечание***
>
> В то время, когда издание уже было подготовлено к печати, появилась новая версия пакета Zimbra — шестая. В этой версии несколько модифицирована работа с OpenLDAP, например, изменились названия служебных учетных записей подключения к LDAP. Поэтому при наличии у вас этой версии уточните параметры настройки по онлайновой документации (**http://wiki.zimbra.com/index.php?title=UNIX_and_Windows_Accounts_in_Zimbra_LDAP_and_Zimbra_Admin_UI_6.0**).

Добавление новых членов домена

Добавление Windows-систем

Для того чтобы Windows-систему включить в состав домена, достаточно в свойствах компьютера на вкладке **Имя компьютера** выбрать вариант изменения его членства в рабочей группе или домене. Такую операцию может

провести пользователь, обладающий административными правами над локальной системой и имеющий право добавления рабочей станции в домен.

По умолчанию каждый пользователь домена может включить в состав домена до 10 рабочих станций. Это значение определяется в атрибуте **ms-DS-MachineAccountQuota** объекта "домен" службы каталогов. Изменить данное значение можно с помощью программы ADSI Edit из состава Resource Kit. Установка в 0 разрешает создание любого числа рабочих станций.

Более управляемым вариантом является предварительное создание администратором в службе каталогов объекта типа *компьютер* и предоставление права конкретным пользователям на его управление и включение в домен (рис. 5.2).

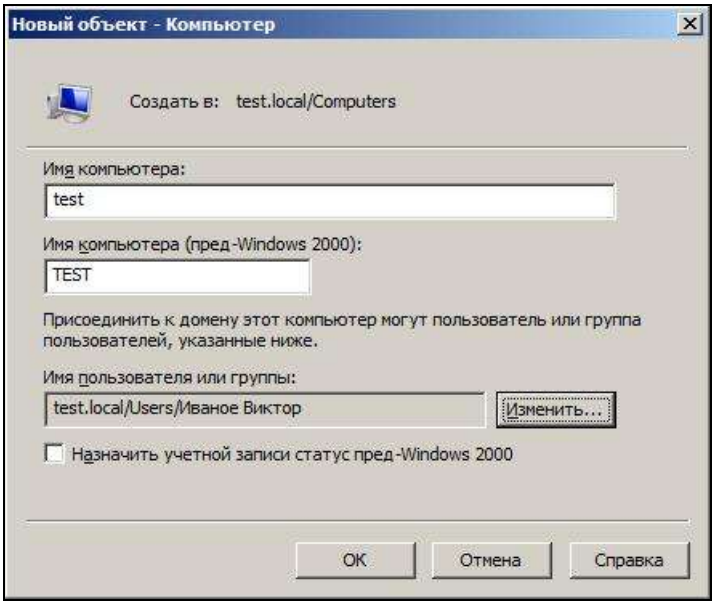


Рис. 5.2. Создание нового объекта службы каталогов — *компьютера*

При создании нового компьютера можно сразу назначить пользователя (или группу), которому будет предоставлено право добавления этой системы в домен. Этот вариант предпочтителен, если вы предполагаете выполнение операции добавления нового компьютера в домен силами обычного пользователя.

Примечание

Рабочую станцию можно добавить в домен удаленно командой `net computer /add` (см. онлайновую справку команды). Но это возможно только в том случае, если добавляемая система уже была ранее в составе какого-либо домена.

Но обычно операцию включения в домен администратор проводит непосредственно на этом компьютере. При этом администраторы указывают свой пароль во время операции. Причем на этом этапе невозможно вместо пароля предоставить параметры аппаратной аутентификации, например, смарт-карты администратора. Такая ситуация не является вполне безопасной, поскольку на компьютере могут быть установлены различные перехватчики клавиатуры. Лучше создать специальную учетную запись с минимальными правами в домене, которую и использовать только для операций добавления рабочих станций.

Модификация настроек Windows-систем при добавлении их в домен

При включении компьютера в домен в локальную группу безопасности **Администраторы** добавляется группа администраторов домена, а в группу локальных пользователей — группа пользователей домена. Именно потому, что администратор предприятия состоит в группе локальных администраторов, он и получает право управления этим компьютером. А пользователи домена могут работать в системе, поскольку они состоят в группе пользователей домена, входящей в группу пользователей этого компьютера.

Кроме того, назначаются новые ресурсы для совместного использования: корневые каталоги всех локальных дисков (под именами C$, D$ и т. д.), каталог установки системы (ADMIN$), создается совместный ресурс IPC$ (для установки соединений *named pipes*), PRINT$ (для управления принтерами) и FAX$ (при наличии факса с совместным доступом). Эти ресурсы носят название *административных*, поскольку они предназначены для управления системами.

Данные ресурсы *невидимы* при просмотре сети (как и все другие совместные ресурсы, имя которых заканчивается знаком $). Если вы попытаетесь удалить их, то после перезагрузки системы они вновь восстановятся (настройкой реестра системы эти ресурсы можно отключить). За счет наличия этих ресурсов можно осуществлять копирование необходимых файлов на локальную систему (установку приложений), подключаться к принтерам и т. д.

Кроме того, при входе в систему может быть назначен сценарий, который может включать необходимые для работы в домене настройки. Но основной объем модификаций локальной системы производится при помощи *групповых политик*, которые описаны далее в этой главе.

Добавление Linux-систем в домен Windows

Примечание

Если в вашей информационной системе контроллерами домена являются серверы Windows 2008, то по умолчанию включен параметр использования строгих алгоритмов шифрования, которые несовместимы как с предыдущими версиями Windows, так и с клиентами Samba. Для разрешения такой ситуации необходимо выполнить рекомендации, изложенные в статье базы знаний KB942564. Открыть для редактирования групповую политику контроллеров домена (**Администрирование** | **Управление групповой политикой** в панели навигации в левой части перейти **Лес** | **Домены** | ***имя_домена*** | **Domain Controller**, щелкнуть правой кнопкой мыши по вкладке **Default Domain Controllers Policy** и открыть пункт меню **Изменить**), найти вкладку **Конфигурация компьютера** | **Политики** | **Административные шаблоны** | **Система** | **Сетевой вход в систему**, в правой части окна найти параметр **Разрешить алгоритмы шифрования, совместимые с Windows NT 4.0** и установить его в значение **Включен**.

Если в вашей организации существует домен, который поддерживается сервером Windows, то в него можно добавить в качестве члена компьютер с операционной системой Ubuntu. Это позволит использовать единые учетные записи домена для доступа к ресурсам Ubuntu. Одновременно можно будет предоставить ресурсы Ubuntu для совместного доступа с правами доступа доменных учетных записей.

Существуют различные варианты включения Linux-системы в домен Windows. Поскольку наиболее современный способ аутентификации — использование Kerberos, а домены Windows работают со службой каталогов, то мы и опишем процедуры подключения в такой конфигурации.

Для Ubuntu разработаны специализированные пакеты, которые предназначены для подключения к домену на основе службы каталогов. Установите пакет *likewise-open* командой

```
apt-get install likewise-open
```

Для подключения к домену Windows на Ubuntu нужно правильно настроить параметры DNS-серверов. Проверьте, что вы можете разрешать доменные ресурсы по их полному имени (с помощью команды `nslookup`).

Подключение к домену производится командой `domainjoin-cli` с указанием полного имени домена (не NetBIOS-имени, а именно FDQN — Fully Qualified Domain Name):

```
domainjoin-cli join example.local имя_пользователя
```

При вводе данной команды система запросит пароль учетной записи *имя_пользователя*, которая должна иметь право подключения компьютеров в домен. Результатом работы команды должно быть сообщение:

```
SUCCESS
```

Процедура произведет все необходимые настройки файлов конфигурации, так что после получения этого сообщения вы можете заходить на сервер Ubuntu, используя доменные учетные записи.

> ***Примечание***
>
> Доменные учетные записи будут иметь права обычных пользователей Ubuntu. При необходимости иного варианта соответствия групп пользователей домена и Ubuntu требуемые корректировки следует выполнить вручную. Например, чтобы предоставить администраторам домена права суперпользователя Ubuntu, следует отредактировать конфигурацию sudo (командой *visudo*), добавив следующую строку: `%YOURDOMAINNAME\\domain^admins ALL=(ALL) ALL`.

Командой `domainjoin-cli` можно отключиться от домена, выполнить подключение к заданному подразделению (в этом случае компьютер будет помещен в соответствующую группу службы каталогов) и т. д. Подробности следует изучить по справке команды (`man domainjoin-cli`).

Есть еще несколько полезных утилит, которые устанавливаются вместе с пакетом Likewise. Это `lwinet` — возвращает информацию о домене и сетевом окружении и `lwiinfo` — показывает информацию о различных параметрах домена. Например, команда

```
lwiinfo --dsgetdcname=ask.ru
```

отобразит имя системы, несущей роль первичного контроллера домена ask.ru.

Диагностика службы каталогов

Следствием неисправностей функционирования службы каталогов (Active Directory, AD) неизбежно являются отказы информационной системы. Поэтому в задачи системного администратора входит предупреждение отказов, своевременное их обнаружение и устранение в сжатые сроки.

Описываемые далее методы диагностики относятся, в первую очередь, к станциям на основе операционных систем Windows. Хотя утилиты, входящие в состав Windows Server, пригодны и для работы с соответствующими службами Linux-систем.

На работоспособность AD оказывают влияние как "собственные" службы, так и подсистемы, обеспечивающие функционирование сетевой инфраструктуры: службы динамического назначения параметров протокола и разрешения имен (DHCP, DNS, WINS), службы аутентификации пользователей (Net Logon, Kerberos), репликации данных (FRS), синхронизации времени, собственные службы AD: KDC (Key Distribution Center), KCC (Knowledge Consistency Checker), ISTG (Intersite Topology Generator), TRS (Time Reference Server) и т. д.

Поэтому работы по поиску неисправностей должны включать анализ всех компонентов системы, начиная от проверки кабельной структуры.

Обнаружение неисправностей AD

Системный администратор должен принять максимум усилий, чтобы обнаружить и правильно интерпретировать первые предвестники неисправности AD. В первую очередь, этому поможет анализ файлов протоколов систем. Особое внимание необходимо уделить событиям, перечисленным в табл. 5.1.

Таблица 5.1. *Перечень событий журнала, подлежащих анализу*

Источник	Номер события
FRS	13508, 13509, 13512, 13522, 13567, 13568
Netlogon	5774, 5775, 5781, 5783, 5805
NTDS	1083, 1265, 1388, 1645
UserEnv	1085
W32Time	13, 14, 52-56, 60-64

Примечание

К сожалению, появление записей об ошибках в протоколах событий, как правило, уже свидетельствует о наличии проблем. Конечно, можно включить расширенные возможности аудита, но в нормальных условиях эта настройка обычно не используется, поскольку снижает полезную производительность системы. Если администратор хочет своевременно обнаруживать проблемы функционирования AD и ликвидировать их еще до того момента, как они приведут к сбоям служб бизнес-структуры, следует задействовать любую систему мониторинга реального времени.

Следует также внимательно относиться ко всей информации, получаемой от пользователей. Например, известие о том, что система второй раз запросила смену пароля пользователя, может косвенно свидетельствовать о проблемах репликации двух контроллеров AD.

Средства тестирования AD

Для проверки функционирования службы каталогов подходят любые утилиты, которые взаимодействуют с AD.

В первую очередь это три стандартные консоли управления AD: пользователи и компьютеры, доверительные отношения и домены, сайты. В состав

Resource Kit входит ряд утилит, которыми можно воспользоваться для диагностирования проблемы. Это `dcdiag`, специально предназначенная для тестирования AD. Кроме того, для тестирования инфраструктуры можно воспользоваться утилитами, перечисленными в табл. 5.2.

Таблица 5.2. *Утилиты для тестирования инфраструктуры*

Утилита	Назначение
netdiag	Проверка сетевой инфраструктуры
netdom	Проверка и управление доверительными отношениями
nltest	Проверка состояния secure channel
ntfrsutl	Управление службой репликации файлов
dcdiag	Диагностика контроллера домена
dsastat	Анализ состояний AD на различных контроллерах
repadmin	Проверка репликации данных AD, возможность инициировать частичную или полную репликацию заданного контекста
replmon	Контроль репликации данных и запуск ручной репликации (графическая утилита)

Совет

Утилиты имеют много ключей для точной настройки проверки. Обязательно ознакомьтесь с их справочной документацией!

Порядок работы с утилитами достаточно прост. Необходимо выполнить ее и просмотреть отображаемые результаты. Если есть предупреждения (или ошибки), то следует поочередно устранить их и добиться отсутствия предупреждений при тестировании (листинг 5.5).

Листинг 5.5

```
>dcdiag

Диагностика сервера каталогов

Выполнение начальной настройки:
   Выполняется попытка поиска основного сервера...
   Основной сервер = WIN-21A2CYWEKM8
   * Идентифицирован лес AD.
   Сбор начальных данных завершен.
```

```
Выполнение обязательных начальных проверок

   Сервер проверки: Default-First-Site-Name\WIN-21A2CYWEKM8
      Запуск проверки: Connectivity
          WIN-21A2CYWEKM8 - пройдена проверка Connectivity

Выполнение основных проверок

   Сервер проверки: Default-First-Site-Name\WIN-21A2CYWEKM8
      Запуск проверки: Advertising
      WIN-21A2CYWEKM8 - пройдена проверка Advertising
      Запуск проверки: DFSREvent
      За последние 24 часа после предоставления SYSVOL в общий доступ
      зафиксированы предупреждения или сообщения  об ошибках.  Сбои при
      репликации SYSVOL могут стать причиной проблем групповой политики.
         WIN-21A2CYWEKM8 - не пройдена проверка
         DFSREvent
         Запуск проверки: SysVolCheck
         WIN-21A2CYWEKM8 - пройдена проверка          SysVolCheck

<...блок сообщений удален..>

   Выполнение проверок разделов на: test
      Запуск проверки: CheckSDRefDom
         ..................... test - пройдена проверка CheckSDRefDom
      Запуск проверки: CrossRefValidation
                  ........... test - пройдена проверка CrossRefValidation

   Выполнение проверок предприятия на: test.local
      Запуск проверки: LocatorCheck
         ..................... test.local - пройдена проверка LocatorCheck
      Запуск проверки: Intersite
        ..................... test.local - пройдена проверка Intersite
```

В листинге 5.5 (часть сообщений опущена для краткости) присутствуют предупреждения (выделено полужирным). Администратор обязательно должен разобраться с причинами, их вызвавшими.

Можно также воспользоваться утилитами, позволяющими отображать необходимую структуру AD и менять параметры объектов (табл. 5.3).

Таблица 5.3. *Утилиты для отображения структуры AD и изменения параметров объектов*

Утилита	Можно использовать для
ADSI Edit	Просмотра и редактирования объектов AD, установки списков доступа (access control lists, ACLs)
ldp	Взаимодействия с AD по протоколу LDAP

Для проверки сетевых соединений и их качества пригодны любые утилиты из состава операционной системы (ping, nslookup, ipconfig и т. п.). Вы должны проверить доступность на контроллере домена портов 53 (служба DNS), 3268 и 3269 (службы глобального каталога), 88 (порт Kerberos), 389 (порт LDAP), 445 (порт службы Server Message Block).

Кроме того, при анализе и настройке AD придется использовать оснастки управления DNS, монитора производительности, утилиту редактирования реестра, утилиту управления AD с возможностью модификации ее метаданных — ntdsutil.exe и т. д.

Можно воспользоваться утилитами, которые подготавливают информацию для технических служб Microsoft при разборе различных инцидентов. Например,

Microsoft Premier Services Reporting Utility (**http://www.microsoft.com/downloads/details.aspx?familyid=00AD0EAC-720F-4441-9EF6-EA9F657B5C2F&displaylang=en**),

MPSRPT_DirSvc.EXE (**http://download.microsoft.com/download/b/b/1/bb139fcb-4aac-4fe5-a579-30b0bd915706/MPSRPT_DirSvc.exe**)

и др. Эти утилиты представляют собой набор сценариев, собирающих различную информацию из операционной системы. Вы можете запустить их и просмотреть собранные данные на предмет найденных ошибок. Возможно, что это поможет в устранении неисправностей.

Кроме того, существует много коммерческих утилит, предназначенных в помощь администраторам. Хочу посоветовать приобрести утилиту Insight for Active Directory (автономную или в составе Winternals Administrator's Pak 5.0 — **http://www.winternals.com/**), позволяющую наблюдать ответы службы каталогов в реальном времени (рис. 5.3). В окне утилиты показаны все запросы к службе каталогов, их содержимое, результаты операции и возвращаемые данные. Подобная информация существенно облегчает поиск неисправности, связанной со службой каталогов.



Рис. 5.3. Insight for Active Directory

Проверка разрешения имен

В оперативных случаях следует быть готовым выполнить простейшие проверки службы каталогов стандартными средствами операционной системы. Обычно достаточно проконтролировать возможность разрешения имен с помощью утилит `ping` и `nslookup`. Следует проверить достижимость контроллера домена по его краткому (без доменного суффикса) и полному имени. Желательно проверить разрешение адресов служб AD. Соответствующая структура DNS создается автоматически, и обычно достаточно проконтролировать ее наличие в оснастке управления сервером DNS. Если такая возможность отсутствует, то нужно вручную, с помощью `nslookup`, выполнить попытку разрешения имен, перечисленных в табл. 5.4.

Таблица 5.4. *Перечень имен, проверяемых в процессе теста*

Имя	Тип записи	Соответствие
_ldap._tcp.dc._msdcs.<*DNS_имя_домена*>	SRV	Контроллер домена
_ldap._tcp.pdc._msdcs.<*DNS_имя_домена*>	SRV	Эмулятор первичного контроллера
_ldap._tcp.gc._msdcs.<*DNS_имя_леса*>	SRV	Сервер глобального каталога
_kerberos._tcp.dc._msdcs.<*DNS_имя_домена*>	SRV	Расположение службы Kdc

Примечание

Для разрешения имен служб (записи типа SRV) следует в `nslookup` предварительно выполнить команду `set type=all` или `set type=srv`. Обратите также внимание, что в операции разрешения имени сервера глобального каталога указывается имя леса, а не домена. Обычно в малых организациях эти имена совпадают.

Обратите внимание на весьма простую операцию, удачное выполнение которой зависит от правильности настройки системы разрешения имен и от функционирования контроллера домена. Попробуйте открыть следующий сетевой ресурс \\<*DNS_имя_домена*>\SYSVOL. Если попытка неудачна, то либо в организации неверно настроено разрешение имен, либо контроллер домена неработоспособен.



Глава 6

Настройка почтовой системы предприятия

Варианты почтового обслуживания пользователей

Наличие почтового обслуживания стало сегодня обязательным атрибутом любой информационной системы. Существует несколько вариантов настройки электронной почты для малых и средних организаций.

- Размещение почтовых ящиков на бесплатных серверах Интернета.

  Как правило, у каждого пользователя создано не по одному ящику бесплатной электронной почты. Такие ящики пригодны как для обмена сообщениями внутри организации, так и для общения с внешним миром. Неоспоримый плюс такого решения — простота и достаточно высокая надежность при доступности информации с любой точки Интернета.

  Среди недостатков можно отметить не столь высокую скорость обмена сообщениями, как в локальной сети, необходимость дополнительных расходов в случае оплаты трафика по объему, неудобные адреса (из-за занятости коротких имен на наиболее популярных серверах), отсутствие средств групповой работы и т. д. Ну и, конечно, указание бесплатных адресов в контактах фирмы часто воспринимается как свидетельство не очень "серьезной" организации.

- Использование локальной почты.

  Сервер электронной почты легко можно развернуть в локальной сети. Существует множество решений как бесплатных, так и коммерческих, отличающихся наборами реализованных функций. Наиболее простой вариант — установка только службы электронной почты на основе протоколов POP3/SMTP. Это решение для систем на основе Windows мы опишем в *разд. "Создание простого POP3-сервера"*.

- Создание собственного почтового сервера с реальными адресами Интернета.

  При расширении организации возможностей, предоставляемых простыми почтовыми серверами, становится недостаточно. Во-первых, появляется необходимость работы с реальными адресами Интернета. Во-вторых, востребованными оказываются такое функции групповой работы, как назначение совещаний, отслеживание занятости, общие папки почты и т. п. В-третьих, крайне важной становится возможность удаленного доступа к почте, в том числе с клиентами в виде обычных обозревателей Интернета. Этот перечень требований легко продолжить.

Установка подобной службы групповой работы требует, во-первых, регистрации домена организации и, во-вторых, выбора и настройки соответствующего программного обеспечения. Кроме собственно настройки служб обмена сообщениями, администратору необходимо принять меры к защите от спама и для фильтрации почтового трафика от вирусов и иных зловредных вложений. Соответствующие рекомендации описаны далее в этой главе.

Протоколы для работы с почтовыми ящиками

Почтовые серверы обмениваются друг с другом сообщениями по протоколу SMTP (Simple Mail Transfer Protocol, простой протокол передачи почты). Существуют варианты безопасного протокола (с шифрованием), различные разработки дополнений, призванных так или иначе аутентифицировать серверы и т. п. Но реально большинство серверов работают в соответствии со стандартом SMTP. Протокол задействует для работы порт 25, который необходимо открыть на соответствующих межсетевых экранах.

Почтовые серверы могут предоставлять почтовые ящики пользователям по разным протоколам, серьезно отличающимся сервисными возможностями. Дадим им краткую оценку, чтобы вы могли осознанно выбирать опции конфигурации при настройке почтовых серверов.

- **POP3** (Post Office Protocol 3, протокол обслуживания почтового офиса) — наиболее распространенный протокол для чтения сообщений с почтовых серверов Интернета. Обычно используется пакетный прием сообщений: все письма копируются на компьютер пользователя и удаляются затем с сервера. Позволяет загружать письма *только* из папки **Входящие**. Существует вариант протокола с шифрованием трафика: POP3S.

  На корпоративных серверах данный протокол лучше отключать, чтобы почтовые сообщения не переносились автоматом на компьютеры пользо-

вателей (это обычно настройка по умолчанию для почтовых клиентов, работающих с протоколом POP3).

- **IMAP** (Internet Message Access Protocol, протокол доступа к сообщениям Интернета) — при подключении по этому протоколу пользователь может не только читать входящую почту, но и создавать дополнительные папки на почтовом сервере. Это более удобный вариант работы с почтой, поскольку дает возможность организовать структуру папок с сообщениями, "читать" папки специальной конфигурации — контакты и т. п., выбирать отображаемую на локальной машине структуру папок и т. д.
- **HTTP** (Hypertext Transfer Protocol, протокол передачи гипертекста) — возможность работы с почтовым ящиком через программу обозревателя Интернета (Mozilla's Firefox, Opera, MS Internet Explorer и т. п.).

  При работе по протоколу HTTP объем передаваемой и принимаемой информации существенно выше, чем при чтении почты с помощью POP3 или IMAP. Кроме того, каждое сообщение необходимо индивидуально загружать в окно программы для прочтения. Все это существенно снижает скорость работы с почтовым ящиком (по сравнению с традиционным почтовым клиентом). Но поскольку протокол открыт в программах межсетевых экранов, это позволяет получить доступ к почтовому ящику практически из любого места.

Также существует безопасный вариант с шифрованием трафика — HTTPS.

- **"Поддержка MS Exchange"** — работа с почтовым сервером Microsoft Exchange осуществляется на основе функций удаленного вызова процедур (RPC, Remote Procedure Call). Этот вариант обозначается в настройках Outlook как "поддержка MS Exchange". Протокол встречается практически только в локальных сетях, поскольку требует динамического открытия большого числа портов. Начиная с Windows 2003/Exchange 2003, предусмотрена возможность работы RPC поверх протокола HTTP. Это позволяет организовать доступ к корпоративной сети через Интернет на основе полнофункциональных версий программы Outlook. Такой вариант требует большого количества дополнительных настроек почтового сервера, прокси-сервера RPC и описан подробно в KB833401 и в специальном руководстве (**http://www.microsoft.com/downloads/details.aspx?FamilyId=EF58395D-3710-49CF-9698-938E2BEF39E8&displaylang=en**).

Создание простого POP3-сервера

В состав операционной системы Windows-сервера версии 2003 входит простой почтовый сервер, который пригоден как для обмена сообщениями внутри организации, так и для работы с адресатами Интернета. Этот сервер

позволяет принимать/отправлять почту по протоколу SMTP и предоставлять ее пользователям по протоколу POP3. Соответственно, установка его включает добавление двух компонент: службы SMTP и службы POP3.

> ***Замечание***
>
> В версии Windows Server 2008 компонент POP3-сервера исключен. Однако данная функция реализуется многими бесплатными программами, которые легко можно найти в Сети.

Установка данного сервера производится либо добавлением роли **Почтовый сервер** (рис. 6.1), либо включением указанных компонентов через функцию установки и удаления компонент Windows (**Компоненты Windows** | **Сервер приложений** | **Службы IIS** | нажать на клавишу **Состав** | **Добавить службу SMTP** для службы SMTP и **Компоненты Windows** | **Службы электронной почты** | *включить опцию* — для службы POP3).

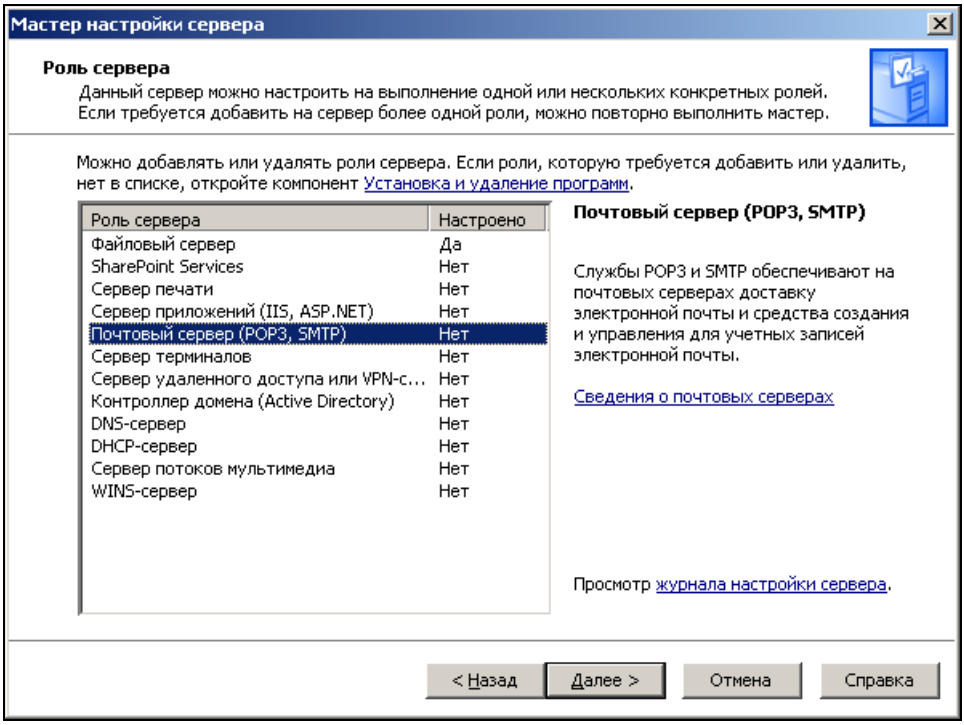


Рис. 6.1. Установка простого POP3-сервера организации

В качестве пользователей почты можно регистрировать как учетные записи домена, так и создавать записи только для доступа к почтовому ящику (в этом

случае почтовый сервер будет проводить аутентификацию по собственному файлу паролей). При этом сервер может обслуживать несколько почтовых доменов (можно создавать ящики в различных почтовых доменах).

Настройка сервера крайне проста. Сервер управляется из двух консолей: почтовые ящики настраиваются в консоли Служба POP3 (вызов через **Административные задачи**), а параметры пересылки сообщений — в консоли управления Web-сервером. Консоль **Служба POP3** позволяет создать почтовые домены и пользователей почты, назначить им пароль, просмотреть состояние почтовых ящиков и при необходимости заблокировать их (рис. 6.2).



Рис. 6.2. Консоль управления POP3-сервером

Замечание

Возможности управления почтовыми ящиками в данном сервере весьма ограничены: можно просмотреть объем ящика, сменить пароль. Никаких дополнительных возможностей простой почтовый сервер не предоставляет.

В консоли **Диспетчер служб IIS** можно настроить свойства SMTP-сервера: периоды попыток отправки сообщений, предельные размеры письма, разрешить ретрансляцию сообщений, ввести ограничения по IP-адресам и т. д. (рис. 6.3).

Сервер подходит и для работы с почтой Интернета, для чего необходимо обеспечить пересылку на него и получение с него пакетов по протоколу SMTP.

К недостаткам данного решения следует отнести отсутствие средств корпоративной работы (общие папки и т. п.), использование только протокола POP3 для работы с почтовым ящиком.

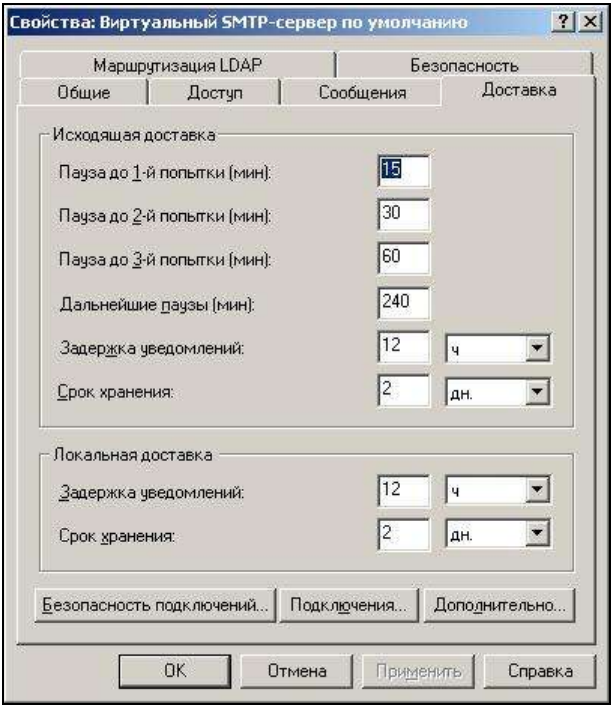


Рис. 6.3. Настройка параметров SMTP-сервера

Почтовый сервер Microsoft Exchange

Почтовый сервер от Microsoft для доменов Windows — Exchange. Наиболее распространенной его версией является выпуск 2003, который представлен только англоязычным вариантом управления, в том числе и в составе локализованной версии операционной системы Small Business Server 2003. Последняя версия сервера — Exchange Server 2007 — локализована. Она включает в себя ряд усовершенствований, но для применения в небольших организациях оба выпуска достаточно равноправны.

Учитывая распространенность выпусков, а также тот факт, что не во всех небольших организациях до сих пор есть в наличии 64-битовые серверы, в этом разделе мы остановимся подробно именно на описании особенностей установки и работы с Microsoft Exchange Server 2003.

Замечание

Exchange Server 2007 выпущен только для использования на 64-битовых ОС. Существует выпуск этого сервера под 32-битовые ОС, но он предназначен только для партнеров и тестирования.

Выбор компьютера для установки Microsoft Exchange

Сервер Exchange предназначен для почтового обслуживания только клиентов доменов Windows. Он может быть установлен на сервере-члене домена, в том числе и на контроллере домена.

> ***Замечание***
>
> Сервер Exchange 2007 устанавливается только на Windows Server 2008 directory server.

Поскольку Exchange постоянно интенсивно взаимодействует с сервером глобального каталога, необходимо обеспечить достаточно близкое их размещение. Для обслуживания одного домена можно применять несколько серверов в целях распределения и балансировки нагрузки, разделения ролей. Но по экономическим соображениям обычно устанавливают только один сервер: технически один сервер может поддерживать сотни и тысячи почтовых ящиков, а каждая дополнительная установка влечет новые расходы по оплате лицензий. Для операционной системы Small Business Server расположение Exchange четко оговорено условиями: только на контроллере домена.

Крайне не рекомендуемая операция — это установка Exchange сначала, например, на контроллере домена, а потом — перенос на рядовой сервер (и наоборот). Вообще, *первый* Exchange-сервер в домене имеет особое значение, поскольку при его установке вносится большое количество информации в службу каталогов домена. Перенос на другой сервер первой установки Exchange, смена его имени и т. п. — это особые случаи, которых следует избегать или же, при необходимости, тщательно планировать с учетом статей KB822931, KB152959, KB158559.

Сервер Exchange крайне требователен к ресурсам компьютера. Конечно, конкретная конфигурация зависит от числа пользователей, предполагаемых объемов хранения сообщений, интенсивности использования электронной почты. Но в любом случае желательно выделить для Exchange-сервера многопроцессорную платформу (или многоядерную) с объемом памяти не менее 2 Гбайт (точнее эта величина — стартовая для установки сервера Exchange). Особое внимание следует уделить дисковой подсистеме: во многом именно ее производительность определяет скорость работы сервера. Понятно, что в небольших организациях практически невозможно выполнить рекомендации относительно выделения отдельных RAID-массивов под хранение почтовых баз, журналов транзакций сервера. Но в любом случае постарайтесь собрать хотя бы минимальный массив.

Заранее следует продумать объем дисков. Для нормальной работы Exchange необходимо, чтобы свободное пространство на диске примерно в 1,1×1,2 раза превосходило суммарный объем почтовых сообщений пользователей. Причем при расчете следует учитывать объемы журналов транзакций, которые также находятся на диске до момента выполнения операции резервного копирования. Так, если вы примете политику ограничения максимальных размеров почтового ящика пользователя примерно в 2 Гбайта и журналы транзакций могут достигать в сумме порядка 5 Гбайт, то при числе пользователей в 30 человек дисковое пространство на сервере только для размещения почтовых должно иметь размер 30 × 1,2 + 3 + 5 = 71 Гбайт. Кроме этого, необходимо место для собственно операционной системы, папки установки программ (в том числе, и сервера Exchange) и общих папок Exchange. В результате, размер RAID-массива должен быть не менее чем на 100×150 Гбайт.

Замечание

Существуют разные подходы по данному вопросу. Некоторые руководители предпочитают, чтобы в почте сохранялась вся переписка. В этом случае объемы ящиков могут достигать, по моей практике, величины 6–8 Гбайт. В других организациях лимитируют ящики пользователя объемами 500–1000 Мбайт для того, чтобы сотрудники переносили свою почту на локальные диски и т. п.

Установка Exchange Server

Установка Exchange Server выполняется в соответствии с указаниями мастера операций и обычно не представляет никаких сложностей. Если в системе не установлены необходимые компоненты (например, Web-сервер или поддержка протокола SMTP), то мастер предложит установить их в систему.

Следует только учесть, что максимальные права управления почтовым сервером предоставляются той учетной записи, от имени которой был запущен процесс установки. Поэтому, если в дальнейшем требуется передать права на управление почтовым сервером другому администратору, то необходимо выполнить *делегирование прав* (рис. 6.4).

Делегирование прав вызывается из контекстного меню почтовой организации (поставить курсор на название организации и нажать правую кнопку мыши). Делегирование прав должен осуществлять администратор, выполнявший установку Exchange. Более точную настройку прав можно выполнить через индивидуальную конфигурацию параметров безопасности объектов Exchange (для этого при использовании оснастки MS Exchange необходимо включить в опциях отображение закладок безопасности).

После установки сервера Exchange при создании на этом компьютере пользовательской учетной записи будут выполнены и шаги настройки почтового

ящика. Чтобы иметь возможность автоматически создавать почтовые ящики для новых пользователей с любой системы, оснастку управления Microsoft Exchange следует установить на соответствующий компьютер. Для этого достаточно запустить инсталляцию почтового сервера и в параметрах установки сохранить только данный пункт. Обратите внимание, что оснастку управления сервером Exchange можно установить и на операционную систему рабочей станции.

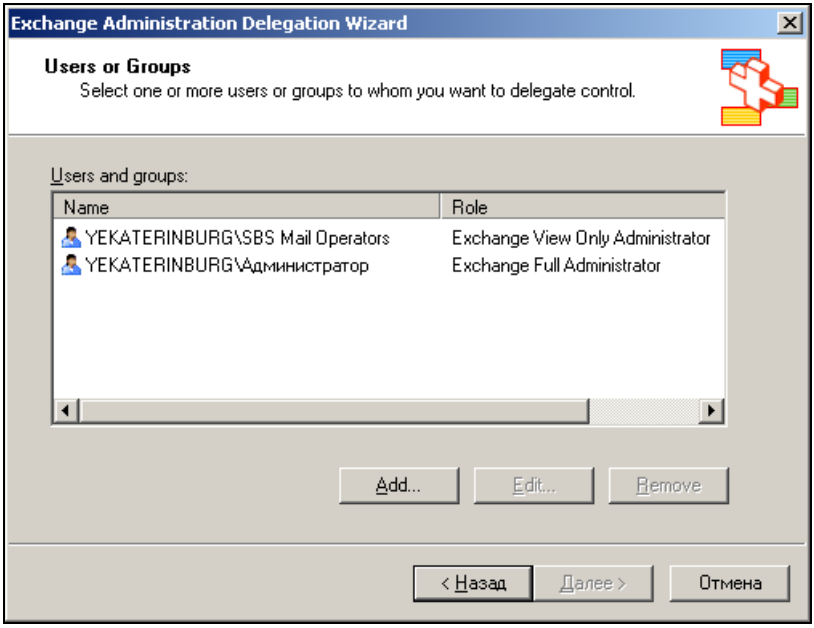


Рис. 6.4. Делегирование прав
на управление почтовым сервером Exchange

Примечание

Для пользователей, существовавших *до* установки Exchange, почтовый ящик создается из контекстного меню учетной записи в оснастке управления пользователями и компьютерами в домене.

Настройка Exchange Server после установки

Исходя из практики работы с Microsoft Exchange Server, я бы рекомендовал сразу после установки сменить некоторые параметры настройки.

Настройка почтовых доменов

Часто во внутренней сети употребляют одно название домена, а для работы в Интернете — другое. В этом случае настроить работу сервера с двумя доменами можно через редактирование политики адресов (**Организация** | **Recipients** | **Recipient Policies** открыть свойства **Default Policy** справа расположена вкладка **E-Mail Addresses (Policy)**). Достаточно добавить новый почтовый адрес с типом *SMTP Address* (рис. 6.5).

Сервер автоматически создаст новые дополнительные адреса у существующих пользователей. Если вы хотите, чтобы эта операция была выполнена максимально быстро, то инициируйте ее вручную через операции **Организация** | **Recipients** | **Recipient Update Services**.

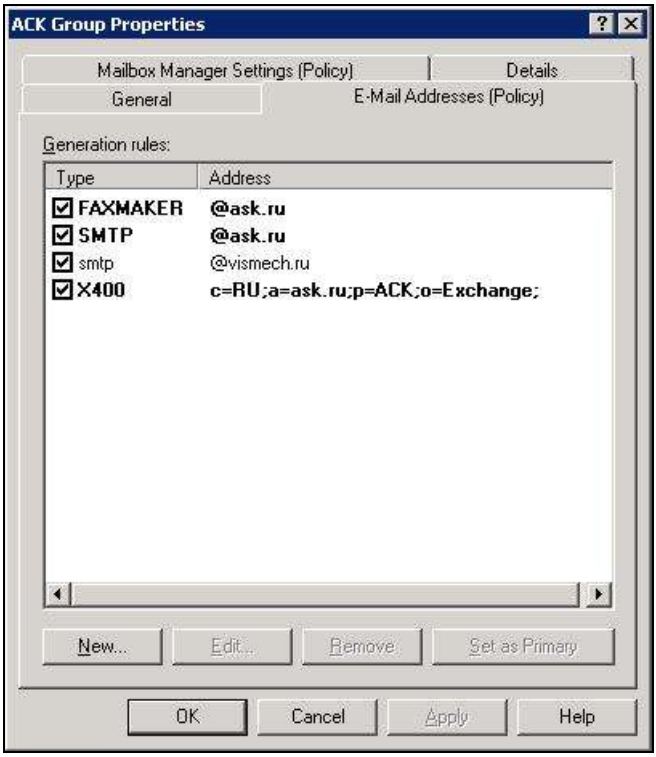


Рис. 6.5. Добавление нового почтового домена

Настройка кодировки электронных сообщений

В России в электронных письмах принята кодировка KOI-8R. Современные почтовые клиенты без труда смогут разобраться с любой кодировкой, однако

будем вежливы и исправим значения в окне **Организация** | **Global Settings** | **Internet Messages Format** открыть справа свойства **Default** и вкладку **Message Format** (рис. 6.6).

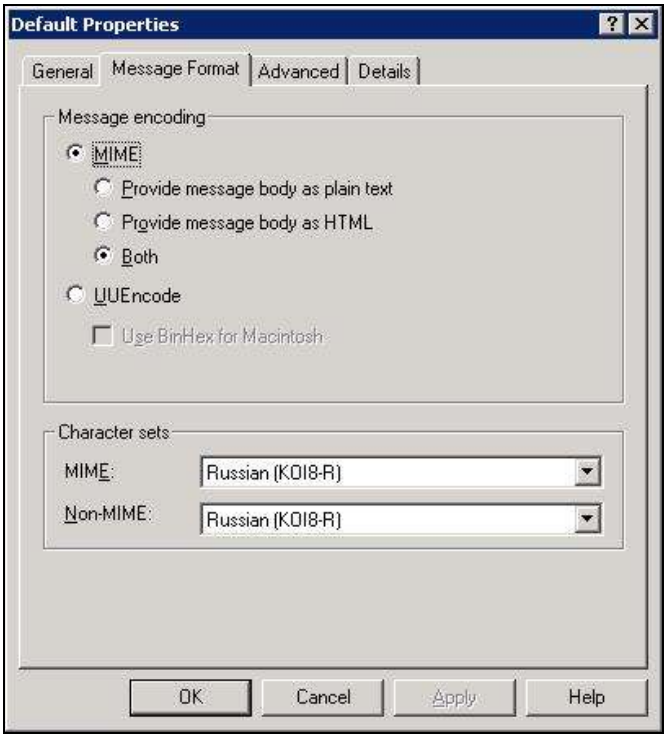


Рис. 6.6. Настройка кодировки сообщений по умолчанию

Настройка отправки автоматических сообщений

Почтовый сервер Exchange может автоматически отвечать на некоторые типы писем: сообщать об отсутствии на работе (если такая опция включена пользователем), подтверждать прием сообщения и т. п. Опция включается в свойствах **Internet Messages Format** на вкладке **Advanced**. Эти настройки не влияют на отправку соответствующих сообщений в локальной сети. Я думаю, что в большинстве случаев в целях предупреждения спама не следует выдавать такую информацию в Интернет. После установки по умолчанию на сервере включена отправка сообщений о доставке и о недостижимости. Эти опции желательно отключить (рис. 6.7).



Рис. 6.7. Настройка автоматических сообщений Exchange

Настройка протоколирования сообщений

Наиболее частые проблемы, с которыми пользователи обращаются к администратору по почтовому серверу, как правило, связаны с поиском сообщений (где сообщение, почему не дошло или почему я не получил ожидаемое письмо и т. п.). Чтобы уверенно отвечать на подобные вопросы, необходимо максимально задействовать протоколирование.

Дойдите слева в панели навигации до обозначения сервера (**Основная организация** | **Servers** | *<имя сервера>*) и откройте его свойства. На вкладке **General** включите все опции протоколирования и увеличьте срок хранения журналов, например, до месяца (периода в 7 дней, которые назначены по умолчанию, на практике обычно не хватает для обеспечения разбора инцидентов). Журналы позволят вам отслеживать сообщения с помощью средства Message Tracking Center из оснастки управления почтового сервера (рис. 6.8).

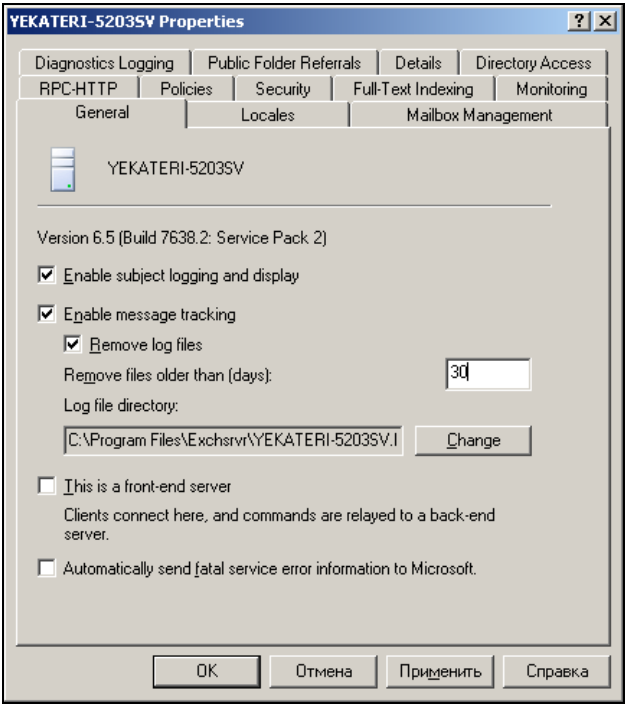


Рис. 6.8. Настройки протоколирования сервера Exchange

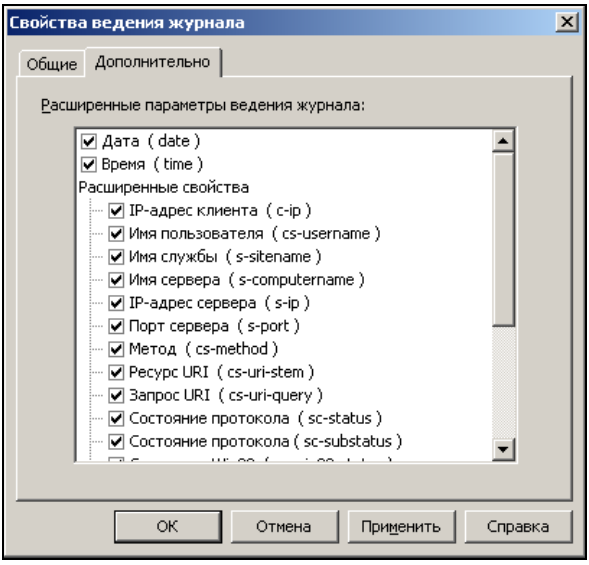


Рис. 6.9. Настройка параметров протоколирования протокола SMTP

Автор рекомендует также включить протоколирование службы SMTP. В некоторых ситуациях информация из этого журнала может помочь выяснить причины недоставки сообщений. Для этого перейдите к меню **Основная организация** | **Servers** | *<имя сервера>* **Protocols** | **SMTP** | **Default SMTP Virtual Server** и откройте меню его свойств. На вкладке **General** включите опцию **Enable Logging** и нажмите кнопку **Properties**, чтобы определить объем заносимых в журнал данных. В окне **Свойства ведения журнала** на вкладке **Дополнительно** включите те поля, значения которых будут заноситься в журнал. Обычно можно включить запись всех значений (рис. 6.9).

Настройка встроенной антиспам-защиты

В составе сервера Exchange есть несколько технологий, направленных на борьбу со спамом. Если судить по опыту автора, современные рассылки спама достаточно успешно преодолевают фильтры Exchange. Например, когда в той организации, где работает автор, возник некоторый перерыв использования антиспам-технологии от Symantec из-за вовремя не продленной лицензии, то количество ежедневных сообщений спама возросло с 3×4 до 50×80 — при включенной соответствующей опции сервера Exchange.

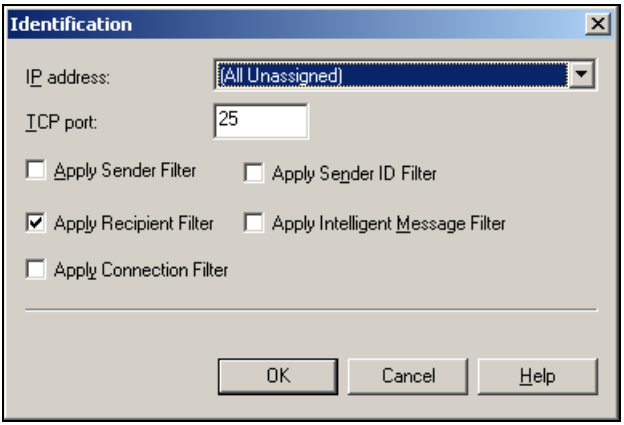


Рис. 6.10. Включение опций фильтрации в IP-интерфейсе SMTP-сервера

Тем не менее, некоторую фильтрацию эти решения обеспечивают, и их настройкой не следует пренебрегать.

Примечание

Чтобы фильтры действовали, необходимо включить опции фильтрации IP-интерфейса (рис. 6.10). Для этого откройте свойства объекта **Default SMTP Virtual**

Server (**Основная организация** | **Servers** | ***<имя сервера>*** | **Protocols** | **SMTP** | **Default SMTP Virtual Server |** открыть свойства), на вкладке **General** рядом с полем **IP address** нажмите на кнопку **Advanced**. В появившемся окне нажмите кнопку **Edit**. Включите опции для всех используемых фильтров.

Фильтры по адресам отправителя/получателя

Фильтр настраивается на вкладках Sender Filtering и Recipients Filtering (**Основная организация** | **Global Settings** | **Message Delivery** | открыть свойства). Для настройки необходимо указать адреса, прием (отправка) сообщений с которых (на которые) будет заблокирован.

Данные фильтры не имеют практического значения, поскольку сообщения спама повторно не используют одинаковые адреса отправителей.

Фильтрация подключений

Фильтр настраивается на вкладке Connection Filtering окна Message Delivery Properties (рис. 6.11) (**Основная организация** | **Global Settings** | **Message Delivery** | открыть свойства). Здесь можно указать службы, обеспечивающие предоставление "черных списков" (или *блок-листов*, Block lists), локальные исключения из этих списков (Exeption) и адреса почтовых серверов, с которых всегда разрешено (или запрещено) принимать почту (Accept/Deny).

Службы блок-листов — это серверы Интернета, на которых ведется учет адресов систем, замеченных в отправке спама. Такие списки составляются как автоматически (в результате автоматизированной проверки наличия опции пересылки сообщений почтовым сервером), так и по результатам обращений пользователей Сети. Почтовый сервер запрашивает в такой службе информацию по адресу системы, с которой осуществляется попытка передачи сообщения, и по ее результатам либо осуществляет прием сообщения, либо отказывает в нем.

Замечание

Сервер отправляет специально сформированный DNS-запрос на такую службу. Если адрес замечен в распространении спама, то получаемый ответ равен 127.0.0.1, 127.0.0.2 и т. д. (адрес возвращается в зависимости от типа списка).

Вы можете указать любое число таких служб, однако увлекаться не стоит, поскольку при этом будет увеличиваться время обработки сообщения и нагрузка на сервер. Обычно вполне достаточно указать две-три службы. Адреса некоторых служб приведены в табл. 6.1.

Параметры выбранных для использования блок-листов следует указать в соответствующих полях формы ввода (рис. 6.12).

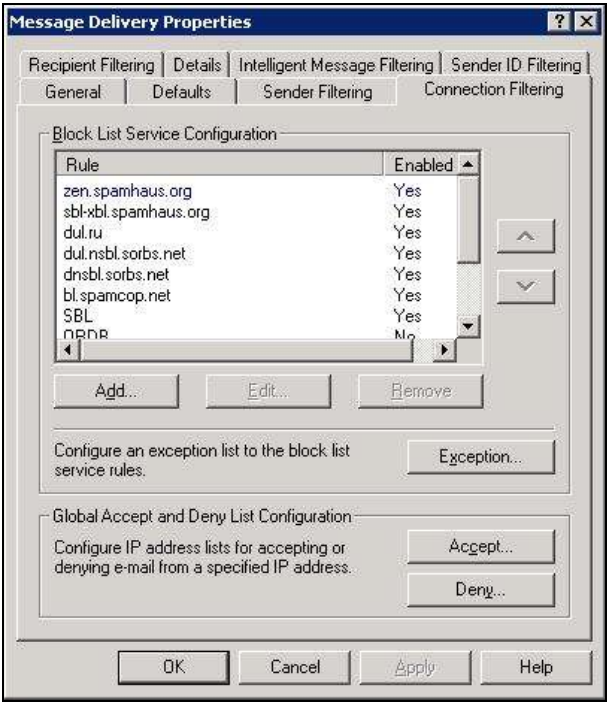


Рис. 6.11. Настройка фильтрации подключений



Рис. 6.12. Настройка параметров блок-листов

Таблица 6.1. *Адреса служб листов блокировки*

dialups.mail-abuse.org	zen.spamhaus.org
sbl-xbl.spamhaus.org	dul.ru
dul.nsbl.sorbs.net	dnsbl.sorbs.net
bl.spamcop.net	sbl.spamhaus.org
relays.ordb.org	relays.mail-abuse.org
cbl.abuseat.org	

В описаниях фильтра важно правильно указать адрес службы в строке DNS Suffix of Provider. Кроме того, обязательно укажите строку, которая будет сообщаться передающему почтовому серверу при отказе в приеме сообщения (коды отказа можно оставить по умолчанию). Желательно привести в ней имя службы, из-за блок-листа которой было отказано в приеме сообщения. Это позволит отправителю знать причину отказа и, если его сервер попал в черный список по ошибке, принять меры к исключению из такого списка.

Фильтр Intelligent Message Filtering

Этот фильтр по некоторым не вполне очевидным правилам вычисляет уровень "спамопасности" сообщения. Возможности как-то настроить данный фильтр у пользователя нет. Разработчики пишут, что фильтр самообучающийся: если пользователь вручную перемещает сообщения из папки *Входящие* в папку *Нежелательная почта* (или наоборот), то этот факт учитывается при "обучении" фильтра.

Реально можно только выбрать уровень спама, после которого сервер будет предпринимать некоторые действия и снабжать сообщение признаком для отправки его в папку *Нежелательная почта* локальным почтовым клиентам пользователя.

Действия сервера могут быть разными: от отсутствия операции до автоматического удаления сообщения. Автор советует не устанавливать опции автоматического удаления, а позволить сообщению достичь почтового ящика пользователя с установленным признаком (рис. 6.13). Порог, который следует выставить в данном фильтре, необходимо подобрать на практике с помощью нескольких итераций.

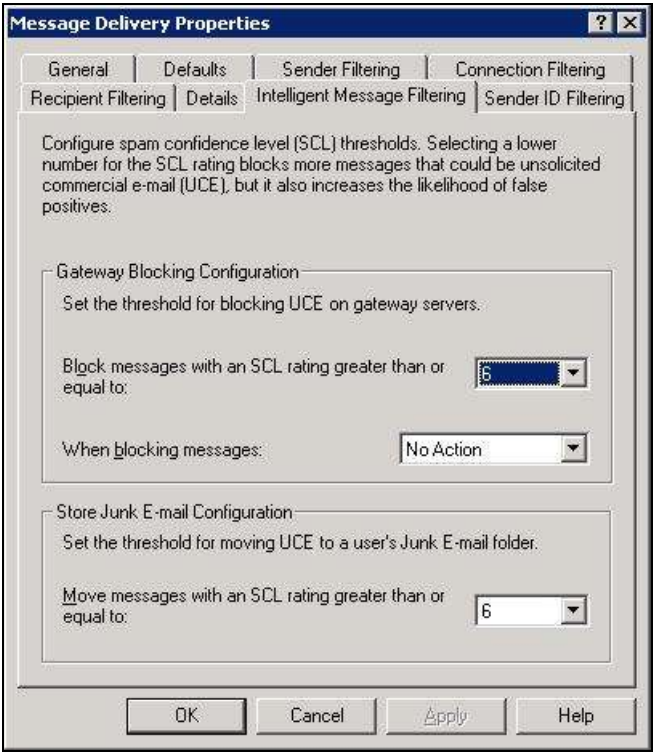


Рис. 6.13. Настройка Intelligent Message Filtering

Опциональные настройки

Перечисленные ранее настройки автор рекомендует выполнить. Кроме них можно отметить еще несколько позиций, которые помогут оптимизировать работу почтового сервера Exchange.

Настройка предельных размеров сообщений

В свойствах **Message Delivery** (на вкладке **Defaults**, рис. 6.14) можно установить максимальные размеры сообщений, которые сервер будет отправлять и принимать. Обратите внимание, что это размеры сообщений, рассылаемых *внутри* организации. При отправке (приеме) сообщений в Интернет действуют ограничения, устанавливаемые в свойствах виртуального сервера SMTP (объект находится внутри контейнера **Protocols** | **SMTP**) (рис. 6.15).

Обычно для отправки в Интернет желательно устанавливать порог порядка 1,5×2 Мбайт. Это гарантирует прием сообщения любым сервером Сети.

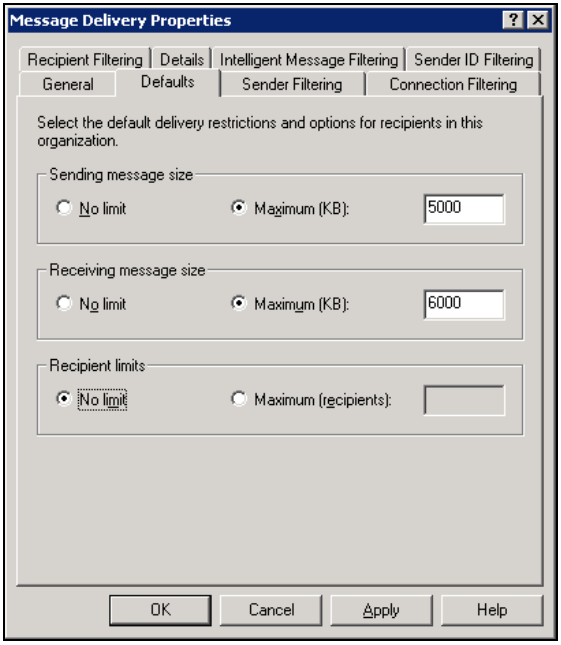


Рис. 6.14. Установка предельных размеров сообщений *внутри* организации

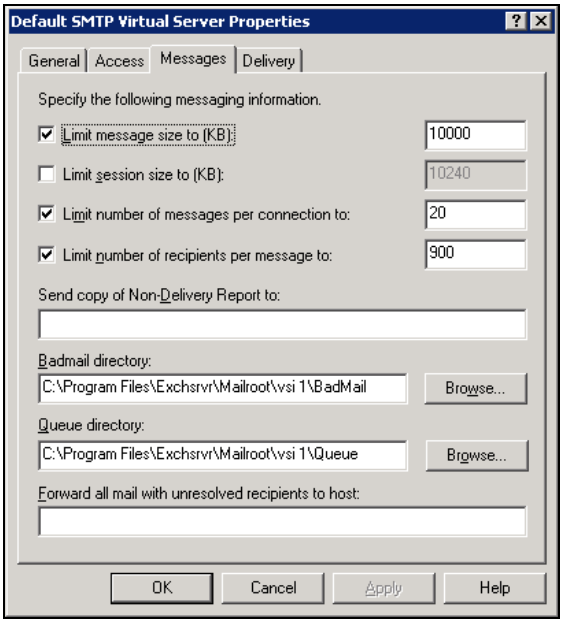


Рис. 6.15. Установка предельных размеров сообщений, обрабатываемых сервером SMTP

Настройка предельных размеров почтового ящика

На размер почтового ящика пользователя можно наложить ограничения по размеру. При достижении некоторого лимита можно запретить отправку сообщений, а при последующем увеличении объема — запретить и прием сообщений.

Значения пределов объемов ящика задаются по умолчанию для свойств базы сообщений (рис. 6.16). Их можно установить как непосредственно на базу, так и создать политику и назначить ее соответствующей базе.

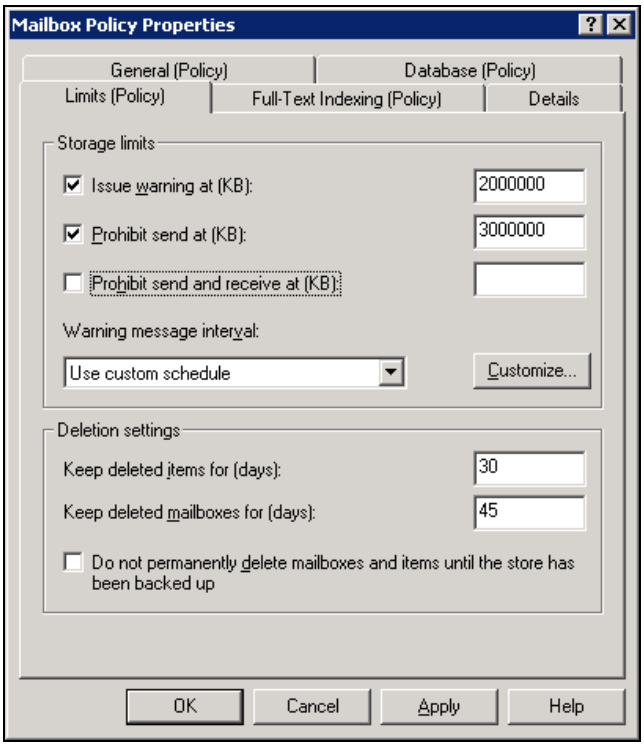


Рис. 6.16. Установка предельных размеров почтового ящика пользователей

Настройка периода хранения удаленной информации

На той же вкладке, что упомянута ранее, настраивают сроки хранения удаленных данных. Если пользователь удалил, например, сообщение или встречу в *Корзину*, то оно будет храниться там сколь угодно долго. После очистки *Корзины* элементы будут сохранены на сервере в срок, указанный в параметрах этой вкладки.

Восстановить удаленные сообщения может сам пользователь при помощи команды **Восстановить удаленные элементы** в программе Microsoft Outlook. Если же нужно восстановить *весь* ящик, то эту операцию проводят в оснастке управления сервером Exchange. Нужно открыть объект **Mailboxes** соответствующей почтовой базы, найти в правой части окна удаленные ящики (отмечены красной пиктограммой на рис. 6.17) и применить к ним операцию **Reconnect**, которая подключает данный почтовой ящик к существующей учетной записи.

Примечание

Если ящик удален, но отображается в оснастке в нормальном состоянии, то необходимо запустить Cleanup Agent из меню операций для объекта **Mailboxes**. Через некоторое время состояние почтового ящика будет соответствовать реальному.

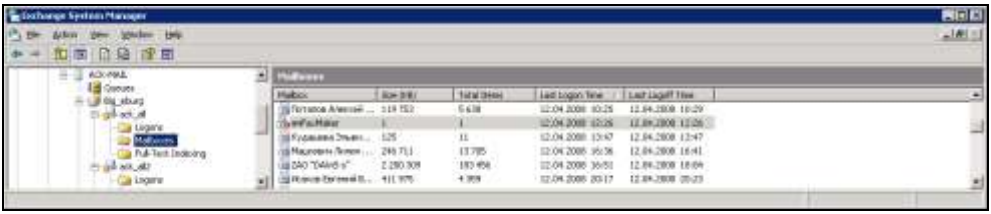


Рис. 6.17. Восстановление удаленных почтовых ящиков

Принципиально можно восстанавливать и элементы, удаленные *помимо* корзины (например, нажатием комбинации клавиш <Shift>+<Del>). Но предварительно следует отредактировать реестр локальной системы (см. статью **http://support.microsoft.com/?id=246153**).

Настройка оповещений о размерах ящика или о его автоматической очистке

Призывы удалять старые ненужные сообщения не действуют на большинство пользователей. Exchange Server позволяет проверять размеры почтовых ящиков и либо отправлять пользователю соответствующее предупреждение, либо даже автоматически удалять сообщения. Политику мониторинга почтового ящика настраивают на вкладке **Mailbox Manager Settings** в меню **Основная организация** | **Recipients** | **Recipient Policies** | *свойства соответствующей политики* (рис. 6.18).

Вы можете установить раздельные показатели для каждой типовой папки почтового ящика и выбрать вариант операций (отправка сообщения, удаление и т. п.). При необходимости также редактируется текст оповещения, отсылаемого автоматически системой пользователю при достижении указанного лимита.

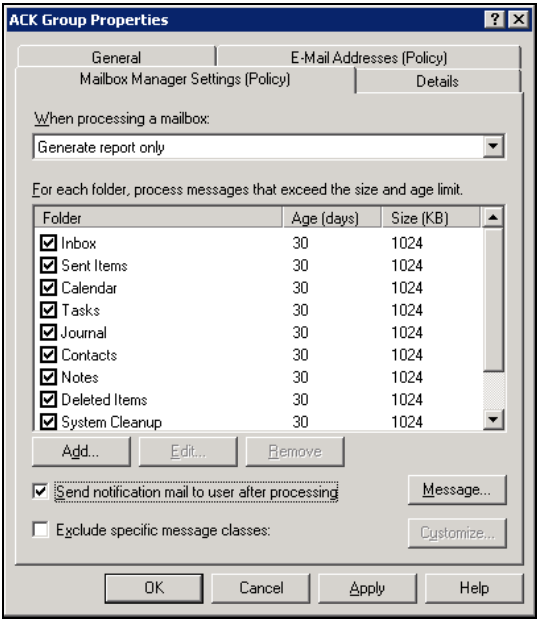


Рис. 6.18. Настройка параметров политики мониторинга почтового ящика

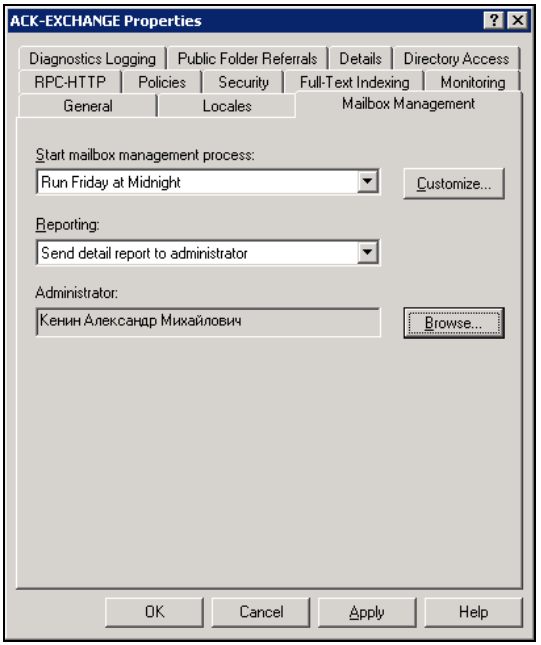


Рис. 6.19. Настройка расписания автоматической проверки почтовых ящиков

Время для проведения анализа почтовых ящиков устанавливается в свойствах сервера на вкладке **Mailbox Management** (рис. 6.19). При необходимости процесс проверки можно запустить вручную из динамического меню свойств сервера (**Start Mailbox Management Process**).

Настройка особого графика отправки сообщений

При недостаточном качестве средств доступа в Интернет иногда имеет смысл отправлять большие сообщения по специальному графику, чтобы не занимать весь канал. Делается это путем создания нового *SMTP-коннектора* (объект находится в **Routing Groups** | **Connectors**). После этого необходимо определить расписание, когда этот коннектор будет работать, типы сообщения, которые он будет отправлять и т. д. При этом нужно не забыть внести согласованные изменения в другие коннекторы, если вы их создали ранее.

> ***Примечание***
>
> Кстати, настраивая права доступа к коннектору, которым почта отправляется в Интернет, можно ограничить, например, для некоторых пользователей пересылку их сообщений только внутри организации. При этом, однако, необходимо внести небольшую правку в реестр системы (см. **http://technet.microsoft.com/en-us/library/aa998486.aspx**).

Включение поискового индекса

Для каждой почтовой базы можно создать *поисковый индекс*. Эту операцию выполняют в свойствах базы на соответствующей вкладке, где вы должны указать путь создания индекса, график его обновления и т. д. Создание индекса уменьшает время поиска по сообщениям почты на клиентских компьютерах, но приводит к существенной дополнительной нагрузке на процессор и дисковую подсистему. Поэтому необходимость включения этой опции администратор определяет в каждом конкретном случае.

> ***Примечание***
>
> Обратите внимание, что новые почтовые сообщения не попадут у пользователя в результаты поиска, пока на сервере не будет обновлен поисковый индекс.

Настройка фильтрации вирусов

Через почту в локальную сеть поступает основная часть вирусов. Учитывая, что обычной практикой стало предоставление удаленного доступа к почтовому ящику, при котором вы не можете проконтролировать наличие на клиентском компьютере антивирусного программного обеспечения, на сервере крайне желательно установить программу для проверки почтового трафика.

Примечание

В этом разделе мы приведем примеры коммерческого программного обеспечения.

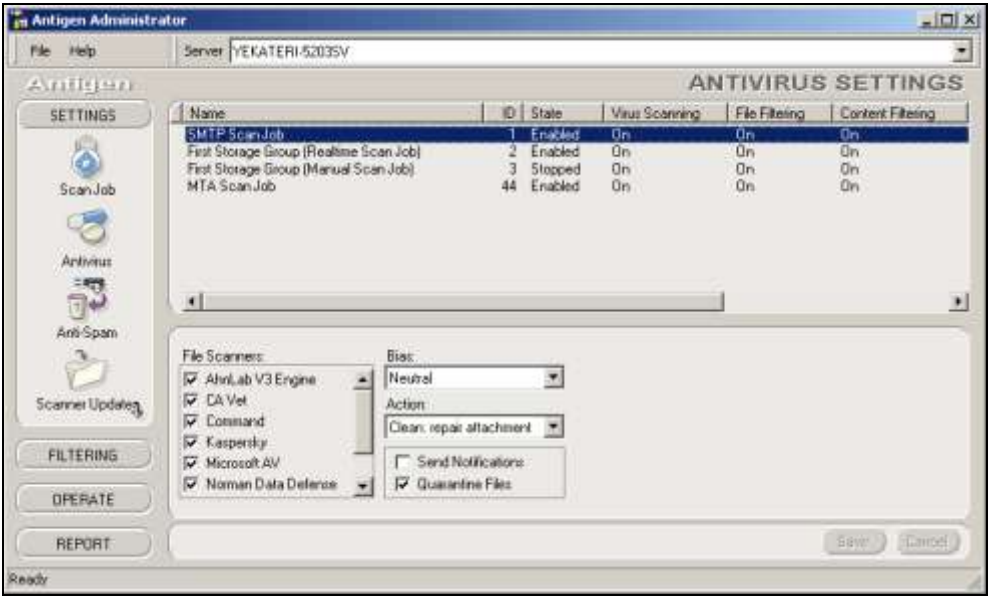


Рис. 6.20. Антивирусная программа для Exchange от Microsoft

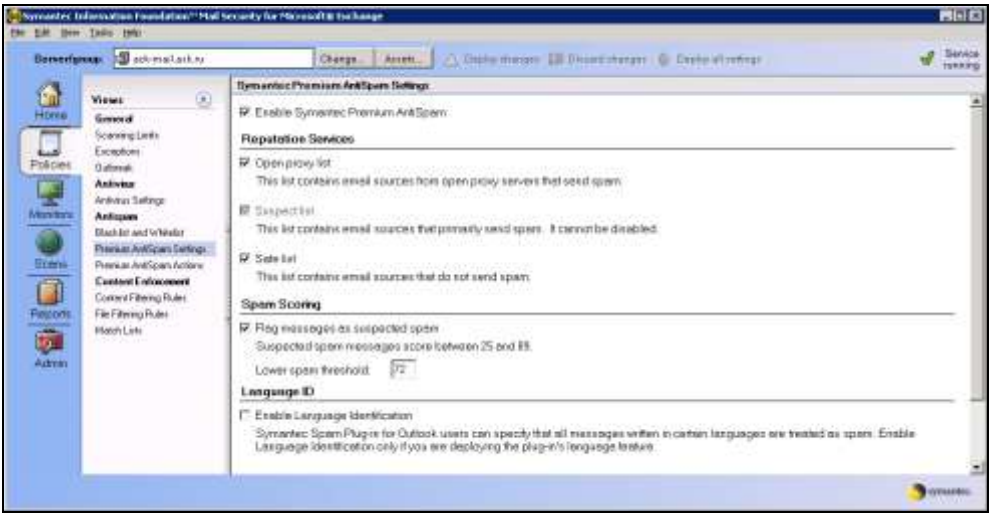


Рис. 6.21. Программа обеспечения безопасности сервера Exchange от Symantec

Существуют различные версии таких программ. Конкретный выбор зачастую определяется многими субъективными причинами. В то же время продукты ведущих антивирусных вендоров имеют практически одинаковую функциональность и надежность. Следует только убедиться, что эти пакеты программ разработаны специально для Microsoft Exchange Server. Для этого лучше всего проверить наличие соответствующего сертификата.

Современное антивирусное ПО для почтового сервера, кроме проверки на вирусы, обычно обеспечивает и фильтрацию спама по различным критериям. На рис. 6.20 представлен интерфейс антивирусной программы с функциями спам-фильтрации от разработчика Exchange — Microsoft Antigen for Exchange. На рис. 6.21 — оснастка управления от Symantec Mail Security for Exchange.

Примечание

Часто администраторы используют почтовый сервер и для предоставления в общий доступ других ресурсов, например, в качестве файлового сервера. В этом случае возникает необходимость установки на почтовый сервер и обычной антивирусной защиты. Следует учесть, что для предотвращения сбоев в работе почтового сервера в настройках файловой антивирусной программы следует исключить из контроля папки, в которые Exchange-сервер записывает текущую информацию. Чтобы не запоминать конкретные пути расположения папок, проще всего отключить сканирование папки установки почтового сервера и папок с базами данных и журналами (обычно они находятся в папке установки Exchange, но их часто переносят в другое место).

Контроль за работой сервера Exchange

Правильно настроенный почтовый сервер практически не нуждается в особом контроле. Основная проблема, с которой приходится сталкиваться администратору, — это постоянная необходимость отслеживать наличие свободного места. Свободное пространство на диске имеет свойство катастрофически быстро уменьшаться, а сервер Exchange останавливает работу, если на диске остается его меньше 2 Мбайт.

Если возникают какие-либо проблемы, то сначала необходимо получить по ним максимум информации. Для этого нужно включить дополнительные опции протоколирования в свойствах почтового сервера (вкладка **Diagnostics Logging** на рис. 6.22). Следует выбрать те службы и тот уровень отображения данных, который требуется для решения возникшей проблемы. Информация по выбранным событиям будет заноситься в системные журналы и может помочь в выяснении причин нарушения работы сервера.

Примечание

Не забудьте по окончании настройки выключить протоколирование, чтобы не расходовать лишние ресурсы сервера.

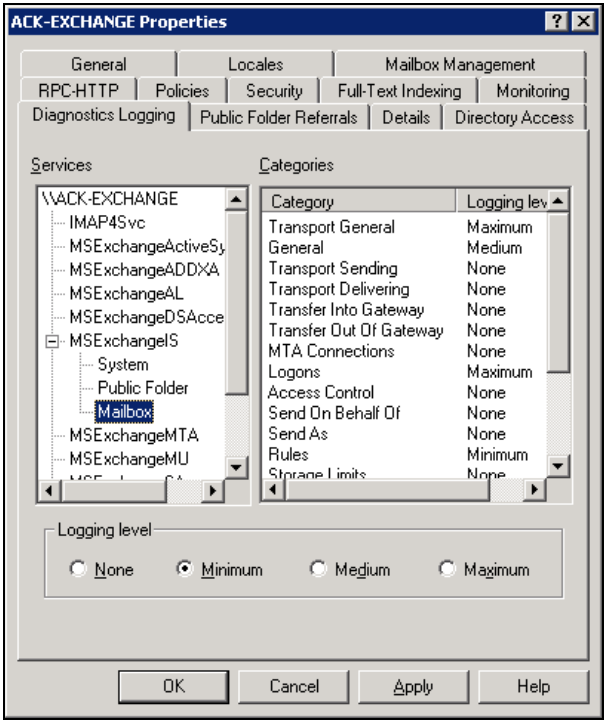


Рис. 6.22. Включение протоколирования служб Exchange

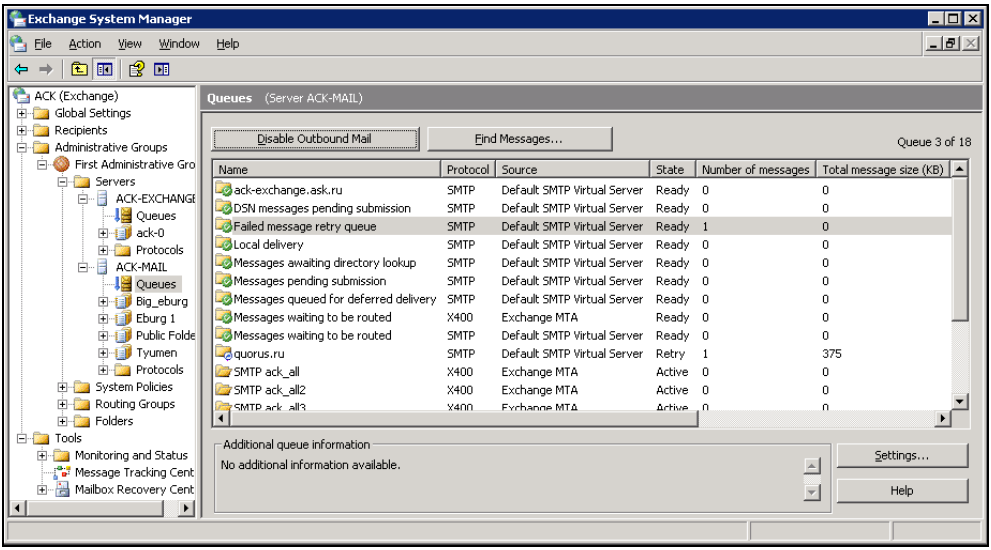


Рис. 6.23. Очереди сообщений почтового сервера Exchange

В качестве интегрального критерия нормального функционирования почтового сервера я бы отметил размеры очередей сообщений (рис. 6.23). В нормальной ситуации размер очередей не превышает нескольких сообщений. Накопление почты в очередях свидетельствует о возникновении неполадок в отправке сообщений и требует принятия соответствующих мер.

Размер очередей характеризует работоспособность соответствующего компонента. Вы можете просмотреть содержимое очереди и некоторую информацию по сообщениям, если выполнить поиск сообщений внутри очереди (из контекстного меню очереди) и выбрать свойства сообщения.

Microsoft разработала специальный пакет, который помогает администраторам оптимально настраивать как сам почтовый сервер Exchange, так и находить неверно назначенные параметры в домене. Этот продукт носит название Exchange Best Practices Analyzer и доступен к бесплатной загрузке с сайта Microsoft (рис. 6.24). Данное средство позволяет проверить почтовые серверы организации, выявить проблемы в их работе, показать настройки, внесенные администраторами. Программу можно запускать периодически для проверки состояния сервера и оптимизации его производительности.



Рис. 6.24. Отчет о проверке сервера средствами Exchange Best Practices Analyzer

Резервное копирование сервера Exchange

Для резервного копирования почтового сервера существует стандартная утилита из состава операционной системы — необходимый компонент добавляется в нее при установке Exchange.

Если вы хотите выполнять не только полные копии почтового сервера, то включите опцию Enable circular logging в свойствах соответствующей базы (рис. 6.25).

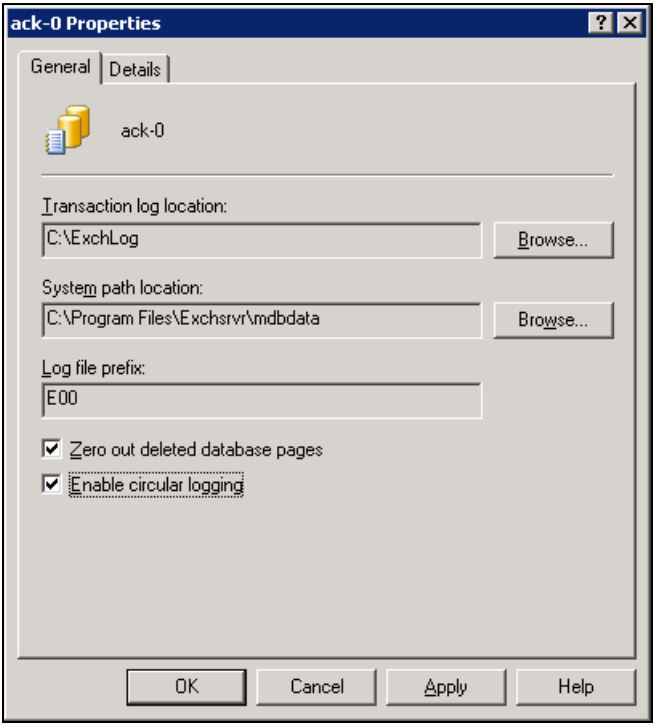


Рис. 6.25. Включение режима протоколирования circular

Резервное копирование Exchange следует планировать на периодической основе. Это нужно не только для того, чтобы иметь резервную копию данных, но и для очистки диска. Exchange создает журналы транзакций, каждый размером по 5 Мбайт. В журналах хранится весь объем почты после последнего резервного копирования. А удаляются журналы штатным образом именно по результатам создания резервной копии. Удалять их вручную не рекомендуется разработчиком в целях обеспечения нормальной работы сервера.

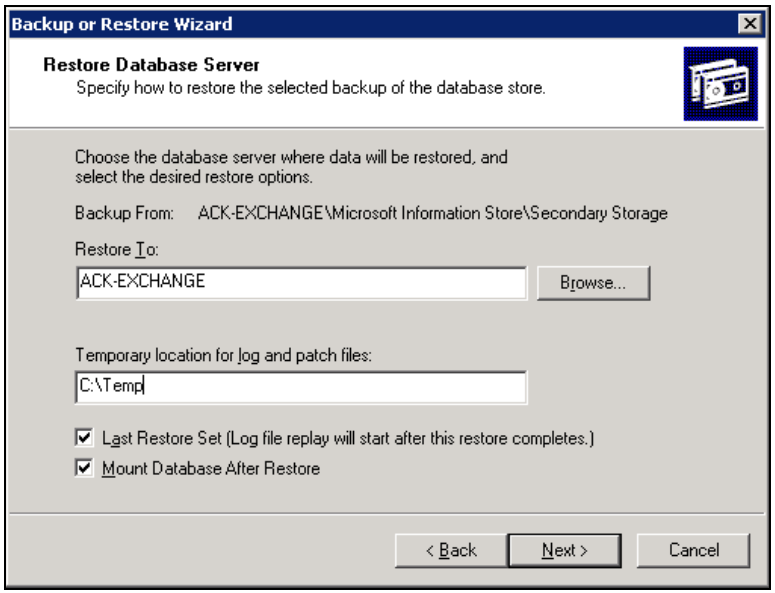


Рис. 6.26. Восстановление почтовой базы из резервной копии

Восстановление из резервной копии происходит как обычно. Не забудьте только при восстановлении последнего файла (если вы использовали промежуточные копии) установить опцию **Last Restore Set** (рис. 6.26). Иначе вы не сможете подключить базу после завершения операции.

В настройках операции вы указываете, что это последний файл из комплекта резервных копий, а также называете путь к папке, где программа создает временные файлы. Не удаляйте эту папку в случае неудачной операции. Информация, содержащаяся в ней, может быть использована при восстановлении баз утилитой `eseutil`.

К сожалению, автор несколько раз на практике сталкивался с ситуациями, когда база, восстановленная из резервной копии, не подключалась в почтовом сервере. Тогда приходится обращаться к утилите `eseutil`. Обычно в журнале сервера создается описание причины ошибки. По этой информации следует выполнить поиск в базе знаний Microsoft. Как правило, вы сможете найти подробные рекомендации по ручному восстановлению базы.

Обслуживание почтовых баз

В составе Exchange Server есть две утилиты, предназначенные для обслуживания почтовых баз. Это `isinteg` и `eseutil`. Обе программы находятся в папке установки сервера Program Files\Exchsrvr\Bin и должны вызываться в кон-

соли с явным указанием пути (папка их расположения не включена в переменную PATH).

Примечания

Для работы утилит требуется свободное место на диске, не менее чем на 10×20% превосходящее размер той базы, с которой будет работать программа.

Крайне рекомендуется *до* запуска утилит создать резервную копию почтовой базы.

Длительность работы утилит зависит от размера баз и обычно составляет от нескольких минут до нескольких часов. Поэтому их запуск следует планировать на ночное время или на выходные дни, чтобы не создавать помех работе пользователей с почтовым сервером.

Почтовые сообщения в Exchange хранятся в базе данных. Для проверки и восстановления собственно базы данных применяется утилита eseutil. Также эта утилита выполняет дефрагментацию базы в режиме off-line.

Замечание

Exchange Server каждую ночь (по умолчанию) проводит онлайновую дефрагментацию базы. Это нужно, например, если вы удалили много сообщений и хотите, чтобы размер файла базы на диске уменьшился (онлайновая дефрагментация не может уменьшить размер файла).

Утилита isinteg "работает" на более высоком уровне: она знает структуру базы и проверяет все взаимосвязи (например, может найти такую ошибку, как хранящееся вложение, у которого нет связанного с ним сообщения почты).

Работа обеих утилит возможна только при *отключенной* базе данных. Иными словами, сначала необходимо открыть оснастку управления сервером Exchange, отметить нужную базу и отключить ее (опция **Dismount Store**).

Запуск isinteg относительно прост. Достаточно открыть консоль, перейти в папку Program Files\Exchsrvr\Bin и запустить isinteg с ключом -s <*имя сервера Exchange*> -test <*тест*>. Перечень доступных тестов можно увидеть из онлайновой подсказки (isinteg -h). Добавление ключа -fix позволит утилите устранить найденные ошибки, а ключ -v приведет к выводу на экран максимально подробной информации о работе утилиты.

При работе утилита будет показывать ход выполнения и информацию по тесту. Вас больше всего будет интересовать заключительная информация о наличии ошибок в базе и результатах их исправления (листинг 6.1).

Листинг 6.1

```
C:\Program Files\Exchsrvr\bin>isinteg -s exchange -test allfoldertests
Databases for server exchange:
Only databases marked as Offline can be checked

Index  Status       Database-Name
Storage Group Name: base-0
  1    Offline      Archiv
  2    Online       Mailbox Store (EXCHANGE)
  3    Online       Public Folder Store (EXCHANGE)
Enter a number to select a database or press Return to exit.
1
You have selected base-0 / Archiv.
Continue?(Y/N)Y
Test reference table construction result: 0 error(s); 0 warning(s);
0 fix(es); 0  row(s); time: 0h:0m:1s
Test Folder result: 0 error(s); 0 warning(s); 0 fix(es); 1220 row(s);
time: 0h:40m:9s
Now in test   3(reference count verification) of total   3 tests;
100% complete.
```

После запуска утилиты необходимо указать номер базы, с которой она будет работать, и подтвердить операцию. Обратите внимание, что даже не для очень объемной базы утилита отработала более 40 мин.

Для запуска утилиты `eseutil` обычно требуется указать существенно больше ключей, особенно, если вы перемещали базы, журналы и т. п. средствами оснастки Exchange. Эти ключи отображаются на экране при вызове справки по утилите (`eseutil /?`) и последующем выборе одной из операций (дефрагментации, копирования, восстановления и т. д.).

Поясню некоторые ключи, поскольку по собственному опыту помню, как сложно было разобраться с их составлением. В табл. 6.2 указано, как можно определить значения для ключей утилиты `eseutil`.

> ***Примечание***
>
> Одноименные ключи имеют разный смысл в опциях утилиты. Это следует уточнить по описанию ключа в соответствующей подсказке команды.

Например, строка запуска утилиты для дефрагментации базы при использовании временной папки на другом диске могла бы выглядеть примерно так:

```
C:\Program Files\Exchsrvr\bin>eseutil.exe /d E:\Exch\Archiv.edb
/sE:\Exch\Archiv.stm /tC:\temp\temp.db /fC:\temp\temp.stm
```

Таблица 6.2. *Описание параметров утилиты eseutil*

Параметр (*описание в подсказке*)	**Значение**
`/l<path>` *location of log files*	Путь к папке с файлами журналов. Этот путь можно увидеть в окне свойств всего сервера на вкладке **General** в поле **Log file directory**
`/s<path>` *location of system files (eg. checkpoint file)*	Путь к файлу checkpoint. Его можно увидеть в окне свойств всего хранилища (*Store*, см. рис. 6.25)
`/d[path]` *location of database files*	Путь к файлу базы данных. Его можно увидеть в окне свойств соответствующей базы на вкладке **Database** (рис. 6.27) — поле **Exchange Database**
`/s<file>` *set streaming file name*	Путь к файлу с расширением .stm. Поле **Exchange streaming database** в окне свойств базы (рис. 6.27)
`/t<db>`	Путь к папке с временными файлами. Можно указать на другой диск, если на текущем не хватает места для проведения операции
`Restore.Env location`	Путь к папке, указанной в операции восстановления базы из резервной копии (см. рис. 6.26)

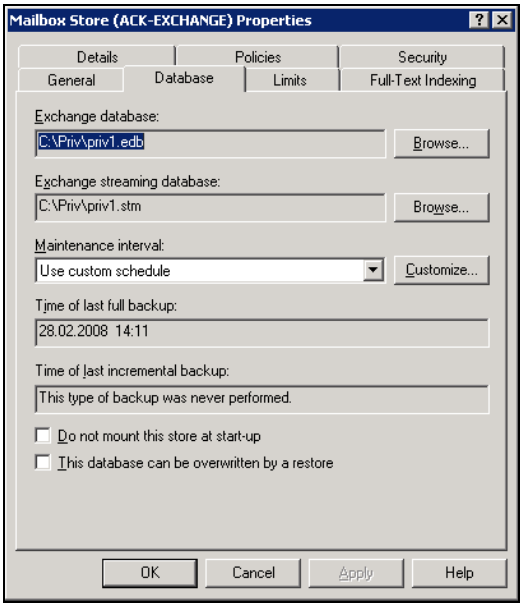


Рис. 6.27. Свойства почтовой базы

Замечание

Если в путях размещения файлов есть пробелы, то эти строки необходимо взять в кавычки.

Результат работы утилиты для данной строки вызова приведен на рис. 6.28. Обратите внимание на время выполнения операции. Дефрагментация базы (ее размер 11 Гбайт + 4 Гбайта файл stm) проходила почти 2,5 часа.

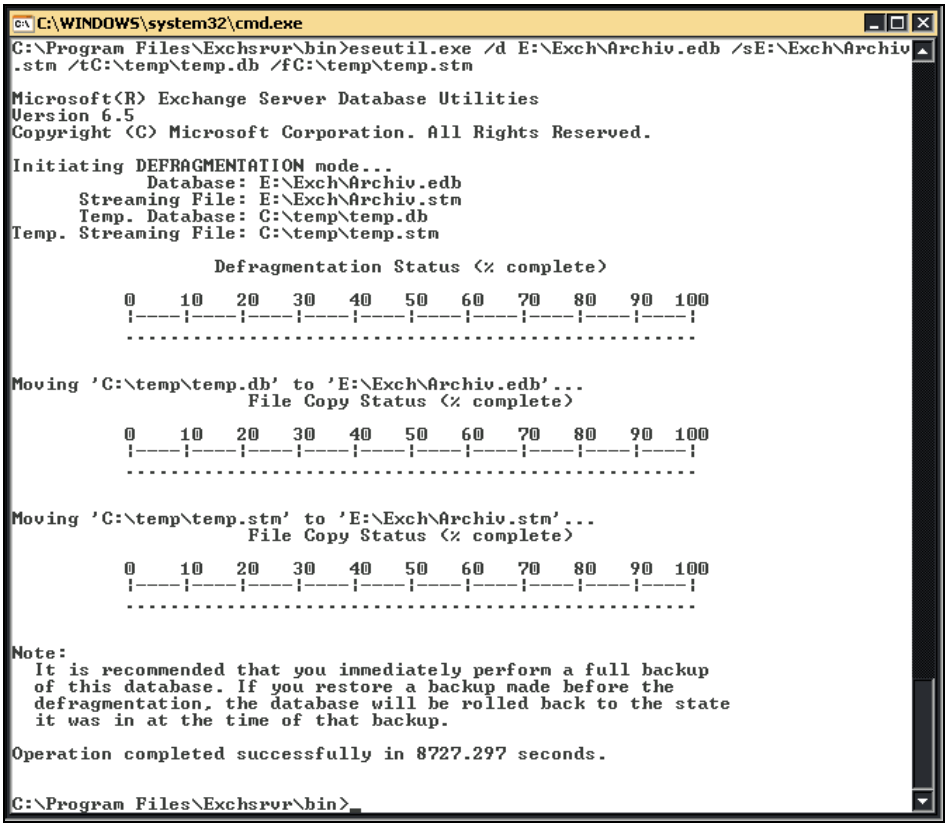


Рис. 6.28. Листинг утилиты `eseutil` при дефрагментации почтовой базы

Использование базы восстановления

При большом объеме почтовой базы ее восстановление из резервной копии может длиться часами. А если цель такой операции заключается только в восстановлении какого-либо сообщения, удаленного пользователем, то останавливать работу всех других сотрудников с почтой крайне нерационально.

Возможности восстановления отдельных ящиков или сообщений есть только в коммерческих программах резервного копирования для Exchange. Для того чтобы минимизировать потери в обслуживании при таких операциях, в Exchange предусмотрено создание базы восстановления.

База восстановления позволяет восстановить всю информацию из резервной копии, не прекращая работу сервера. После восстановления данных в эту базу можно либо переключить весь сервер на ее использование, либо экспортировать нужные сообщения с использованием утилит из состава Resource Kit для Exchange. Создается такая база опцией **Создать | Recovery Storage Group** в свойствах сервера. После создания **Recovery Storage Group** необходимо подключить в нее почтовую базу (рис. 6.29).

После выполнения этих настроек в случае операции восстановления из резервной копии (штатными средствами) данные станут копироваться именно в эту базу, а работа почтового сервера не будет приостанавливаться.

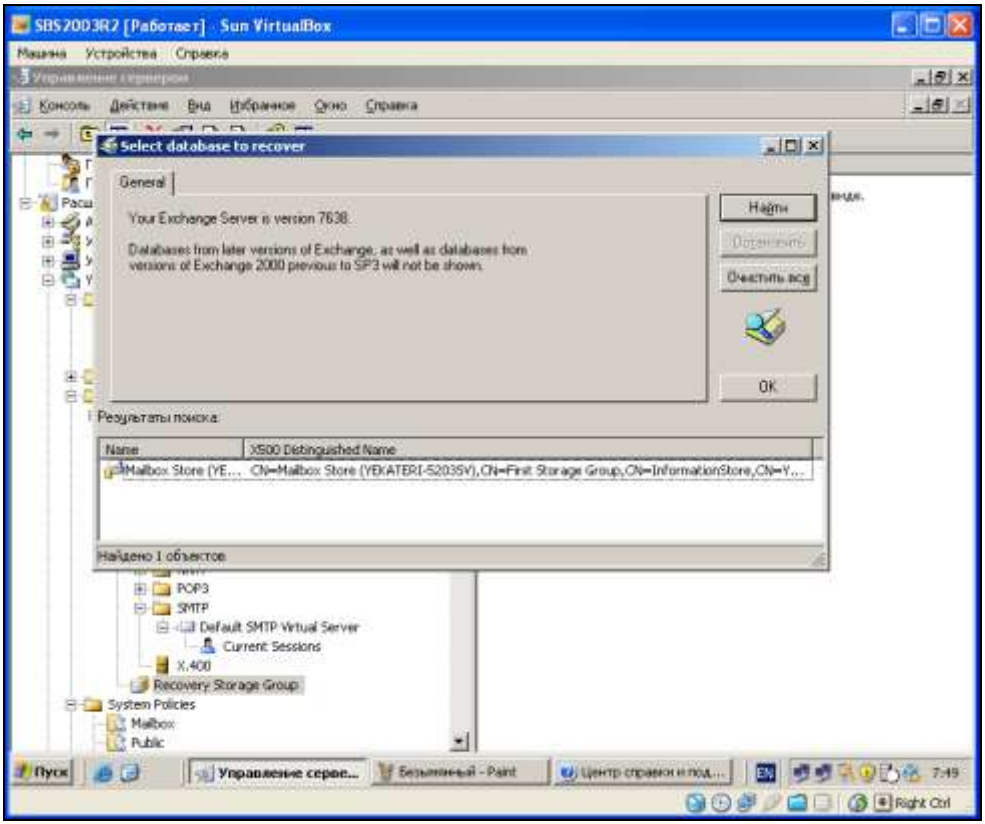


Рис. 6.29. Настройка базы восстановления почтового сервера Exchange

Трассировка пользовательских сообщений в Exchange

Наиболее частой задачей, с которой пользователи обращаются к администратору почтового сервера, является трассировка сообщения: получение информации о том, где находится отправленное письмо (или почему не получено). В Exchange в этих целях предусмотрен специальный инструмент — Message Tracking Center (находится в папке Tools панели навигации). Достаточно указать в полях значения, по которым производится поиск, и система отобразит необходимую информацию (рис. 6.30).

ЗАМЕЧАНИЕ

Дополнительную информацию по сообщению можно получить, если отметить его и в динамическом меню выбрать пункт **Track Message**.

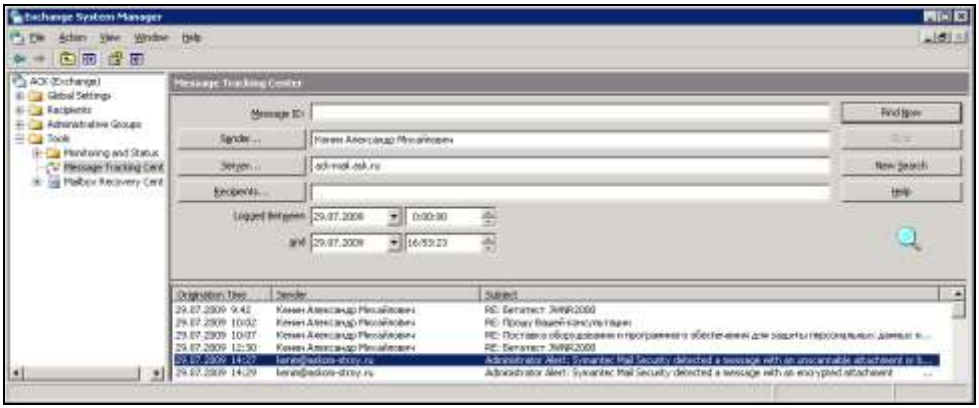


Рис. 6.30. Поиск сообщений отправленных или полученных пользователем

Для того чтобы эта утилита могла сообщить такую информацию, в настройках Exchange должны быть включены опции создания журналов (*см. разд. "Настройка протоколирования сообщений"* настоящей главы).

Сведений, получаемых от утилиты Message Tracking Center, не всегда бывает достаточно для получения полной информации. Например, в свое время автору часто приходилось анализировать журналы SMTP-сервера, чтобы выяснить причины отказа в приеме сообщений. Эти журналы хранятся в папке %SYSTEM32%/LogFiles/Smtpsvc1/.

Zimbra Collaboration Suite

Во многих организациях от "чисто почтовой" системы переходят к обеспечению корпоративной работы. Современные коммерческие программы электронной почты, такие как описанный сервер Microsoft Exchange, позволяют

организовывать совместную работу пользователей: назначать задания, планировать совещания с учетом занятости сотрудников и т. п.

Один из лидеров программного обеспечения корпоративной работы для серверов на основе Linux — Zimbra Collaboration Suite (ZCS). Этот продукт доступен как в коммерческом, так и в бесплатном варианте (в последнем случае отсутствует поддержка продукта со стороны фирм-изготовителей и возможности несколько ограничены). Пользователям доступны для установки системы как исходные коды программы, так и предварительно скомпилированные пакеты. Понятно, что подготовленные пакеты удобнее для обычных пользователей.

Основным вариантом работы с ZCS является обозреватель Интернета. Firefox предпочтительнее, поскольку Microsoft Internet Explorer весьма медленно работает с новыми технологиями, реализованными на Web-сервере ZCS. Имеется собственный бесплатный почтовый клиент (*см. разд. "Почтовый клиент Zimbra"* далее в этой главе). Кроме того, с системой могут работать любые клиенты, поддерживающие стандартные протоколы IMAP. POP и iCalendar.

Zimbra Collaboration Suite доступна к загрузке со страницы
http://www.zimbra.com/community/downloads.html.

Возможности совместной работы в ZCS

ZCS обеспечивает не только обмен почтовыми сообщениями. Кроме почты пользователям доступны групповое планирование, создание и управление заданиями, общие адресные книги. При этом почтовые сообщения проверяются на наличие вирусов и фильтруются по признакам спама. Пользователи имеют возможность использовать ZCS для хранения и совместного доступа к документам (общие папки).

Интерфейс ZCS полностью локализован. При наличии обозревателей, не вполне поддерживающих новые технологии Ajax, Java, или на медленных соединениях, можно переключиться на "классический" HTML. Имеется специальный интерфейс для подключения мобильных клиентов (КПК).

В состав ZCS входят многие открытые решения: Postfix в качестве агента передачи сообщений, OpenLDAP для аутентификации, MySQL как сервер базы данных, ClamAV и SpamAssassin для фильтрации почты, Jetty в качестве сервера Web-приложений и др. Консоль администрирования и пользовательская Web-консоль доступа к почте написаны на Java.

> ***Примечание***
>
> По опыту работы наилучшей производительностью при работе с Java-приложениями отличается Firefox. Страницы ZCS в Microsoft Internet Explorer открываются крайне медленно.

Установка Zimbra

Для установки ZCS подойдет любой компьютер с процессором частотой более 2 ГГц и оперативной памятью 2–4 Гбайта (для обслуживания нескольких сотен пользователей). Объем дискового пространства должен обеспечивать хранение почтовых ящиков пользователей. При этом нежелательно формировать RAID 5-го уровня из-за не очень высокой его производительности при числе пользователей более 100.

Стандартная поставка Zimbra включает установку LDAP, собственно почтового сервера, антивирусной защиты и программы фильтрации спама. Для начала операции нужно распаковать полученный дистрибутив Zimbra и запустить сценарий install.sh:

```
tar xzvf <имя_пакета_установки>.tgz
cd <имя_пакета_установки>
./install.sh
```

Программа установки проверит наличие необходимых компонентов и предложит установить их. Например, при установке на новую систему Ubuntu, потребовались пакеты libgmp3c2, libstdc++5, libltdl3. Обязательным условием установки является наличие MX-записей в зоне DNS для устанавливаемого почтового домена. Эти записи должны соответствовать адресу системы, на которую ставится ZCS.

В случае удовлетворении всем требованиям сценарий предложит подтвердить установку необходимых пакетов и модернизировать систему. Нужно согласиться (можно просто нажимать <Enter> до момента ответа на запрос *Continue*, когда нужно будет явно ввести <Y>).

Сценарий установки по умолчанию предлагает создать почтовый домен с именем, совпадающим с именем хоста, на котором производится разворачивание Zimbra. Если вы хотите создать почтовое обслуживание *домена* Windows или Linux, то введите его имя. В любом случае после установки Zimbra почтовые домены можно создать средствами административного управления.

После чего на экран будет выведено меню, в котором будут описаны все параметры установки (для раскрытия меню нажмите цифровую клавишу, соответствующую номеру пункта меню, а затем <Enter>). Те позиции, для которых необходимо указать параметры, будут отмечены звездочками. В листинге 6.2 в целях экономии приведена только часть меню настройки Zimbra.

Листинг 6.2

```
Main menu

   1) Common Configuration:
   2) zimbra-ldap:                          Enabled
   3) zimbra-store:                         Enabled
        +Create Admin User:                 yes
        +Admin user to create:              admin@ack.ack
******* +Admin Password                     UNSET
        +Enable automated spam training:    yes
….
```

Необходимо перейти в соответствующие пункты (переход нажатием на клавишу с номером меню; так для назначения пароля администратора нужно будет сначала ввести **3**, а потом, в новом меню, — **4**) и ввести нужные значения. Возврат в меню нажатием клавиши <r>. После редактирования следует сохранить изменения конфигурации (вводом команды **a** — *apply*) и дать согласие на изменение конфигурации системы.

Успешность установки можно проверить командой `zmcontrol status`. Все службы должны быть запущены (листинг 6.3).

Листинг 6.3

```
sudo -s
sudo – zimbra
cd /opt/zimbra/bin/
zmcontrol status
Host <имя_системы>
antispam Running
antivirus Running
ldap Running
logger Running
mailbox Running
mta Running
snmp Running
spell Running
stats Running
```

Если какая-либо служба не запущена, нужно стартовать ее (`zmcontrol start`). Обычно никаких проблем при установке не возникает, и сразу же можно переходить к административному интерфейсу Zimbra.

Примечание

Деинсталляция ZCS производится командой `./install.sh -u`. После ее выполнения следует вручную удалить папку установки ZCS.

Администрирование ZCS

Администрирование ZCS выполняется как из Web-интерфейса, так и из командной строки. Причем в первом режиме доступны не все опции настройки.

Примечание

Документация по ZCS доступна в Интернете, прежде всего, по адресу http://wiki.zimbra.com/.

После установки ZCS доступ к управлению осуществляется по адресу хоста и порту 7071 (рис. 6.31). При подключении к интерфейсу администрирования первоначально отображается состояние всех служб сервера. Для настройки параметров Zimbra достаточно выбрать соответствующую позицию в панели навигации слева.

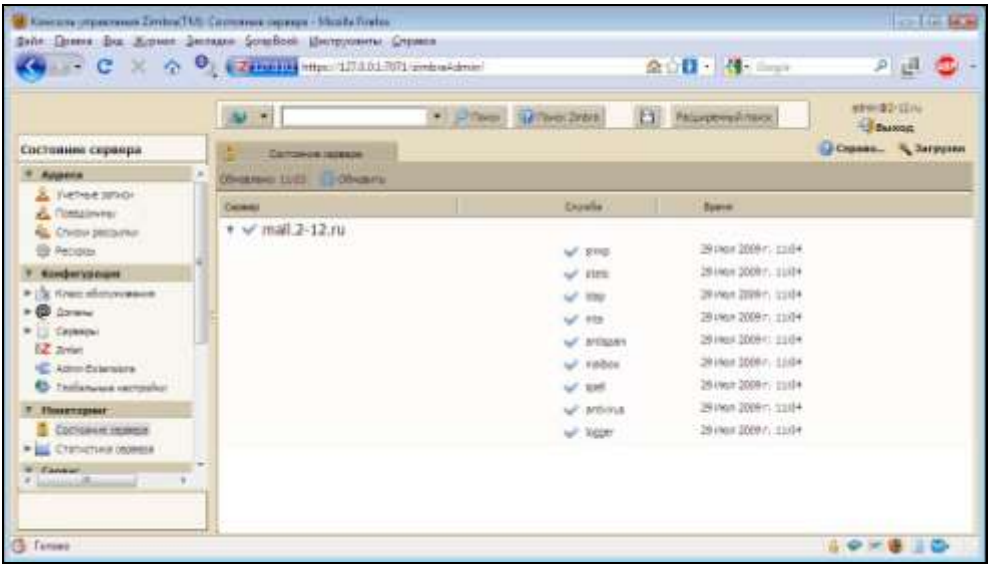


Рис. 6.31. Интерфейс администрирования Zimbra

Желательно проверить все настройки сервера, которые отображаются на страницах управления. Прежде всего, проконтролируйте часовой пояс и глобальные установки. Обратите внимание на перечень типов файлов, которые запрещены к пересылке, и, при необходимости, откорректируйте его. Установите максимальные размеры вложений в сообщения почты и максимальные объемы документов, которые можно сохранять на сервере Zimbra.

Убедитесь, что вас удовлетворяют настройки пользовательских учетных записей (лимиты почтовых ящиков, правила составления паролей, тайм-ауты работы с почтовым ящиком и т. п. — все это настраивается в параметрах класса обслуживания по умолчанию, рис. 6.32).

После настройки параметров сервера можно приступать к созданию учетных записей пользователей.

Примечание

Если Zimbra находится в составе домена, то она может использовать доменные учетные записи. Соответствующие настройки можно уточнить по документации пакета. Если сервер Zimbra сам является контроллером домена, то необходимые настройки описаны в *главе 5* настоящей книги.

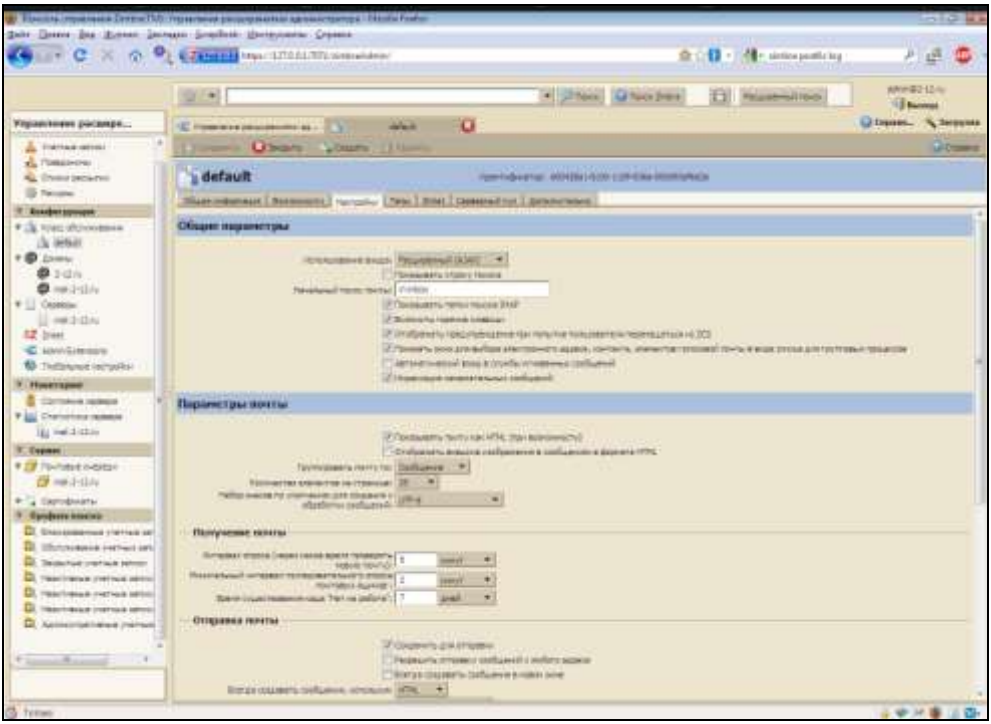


Рис. 6.32. Настройка параметров сервера Zimbra

Обратите внимание, что вы можете создать еще и *ресурсы*. Ресурсы необходимы при планировании совещаний, заданий и т. п.; их можно "бронировать" для проведения мероприятия, причем настройки допускают автоматическое закрепление ресурса при получении заявки пользователя.

В целом, Web-интерфейс администрирования Zimbra достаточно понятен, и настройки обычно не вызывают сложностей.

Класс обслуживания определяет настройки пользователей. При необходимости можно добавить новые классы обслуживания и назначить их соответствующим группам.

Кроме Web-интерфейса в Zimbra присутствует ряд команд управления, которые выполняются из консоли. Они находятся по умолчанию в папке /opt/zimbra/bin. Запускать эти команды необходимо от пользователя Zimbra. Листинг 6.4 иллюстрирует, как это можно сделать.

Листинг 6.4

```
sudo -s
sudo – zimbra
cd /opt/zimbra/bin/
zmprov gacf
```

Из особенностей работы с программой отметим, что написание команд чувствительно к регистру (нужно внимательно следить, где строчные, а где заглавные буквы). Также, если параметр команды должен включать пробелы, его следует заключить в кавычки.

Консольные команды управления целесообразны в тех случаях, когда необходимо:

- ❒ настроить учетные записи в пакетном режиме (например, создать несколько записей путем импорта списка);
- ❒ вручную остановить или запустить какую-либо службу;
- ❒ переместить почтовые ящики (в случае установки нескольких серверов Zimbra);
- ❒ осуществить поиск по нескольким почтовым ящикам сразу;
- ❒ установить сертификаты безопасности на сервер (требуются для создания защищенных каналов);
- ❒ изменить локальную конфигурацию сервера.

Список наиболее употребительных консольных команд Zimbra приведен в табл. 6.3.

Таблица 6.3. *Команды администрирования Zimbra*

Команда	Функция
`postconf`	Редактирование конфигурации `postfix` (отвечает за передачу сообщений)
`postfix`	Остановка/запуск/обновление `postfix`
`qshape`	Проверка очереди сообщений `postfix`
`zmantispamctl`	Остановка/запуск/состояние службы проверки спама
`zmantivirusctl`	Остановка/запуск/состояние службы антивирусной проверки
`zmcontrol`	Остановка/запуск/состояние сервера Zimbra
`zmhostname`	Отображает имя сервера Zimbra
`zmldappasswd`	Используется для смены пароля доступа к LDAP
`zmlmtpinject`	Утилита тестирования
`zmlocalconfig`	Отображает или настраивает локальную конфигурацию Zimbra
`zmmailboxctl`	Остановка/запуск/состояние компонент почтового ящика (Tomcat, MySQL, convert)
`zmmsgtrace`	Трассировка сообщений
`zmprov`	Осуществление любых операций в Zimbra LDAP, в том числе, создание учетных записей, доменов, списков рассылки и т. д. Например, команда `zmprov sm имя_ящика emptyFolder /contacts` очищает папку контактов для указанного пользователя
`zmtlsctl`	Настраивает Web-сервер на протокол HTTP, HTTPS или обоих протоколов сразу
`zmvolume`	Управление томами хранения данных почтового сервера

Команды могут использоваться для различных операций, поэтому, в целях экономии, мы отошлем читателя к онлайновой справке по этим утилитам (вызывается ключом `-h`).

Особенности пользовательских почтовых ящиков Zimbra

Пользовательский Web-интерфейс кажется достаточно понятным. В то же время для большинства пользователей необходимо дать некоторые разъяснения по его применению.

Web-интерфейс поддерживает операции drag-and-drop, например, при получении сообщения пользователь может перетащить его непосредственно в обозревателе на календарь, и программа автоматически предложит создать встречу на основе для этого сообщения в указанный день.

Zimbra позволяет легко создавать общие папки. При этом, в отличие от Microsoft Exchange, права доступа к папке определяет сам пользователь. Для этого достаточно выполнить операцию **Документы | Создать | Новый блокнот**, отметить пункт **Новый блокнот** и выполнить для него команду (из контекстного меню) **Общий доступ к блокноту**. После чего следует указать права доступа и отправить другим пользователям приглашение на подключение к данному хранилищу документов (рис. 6.33).

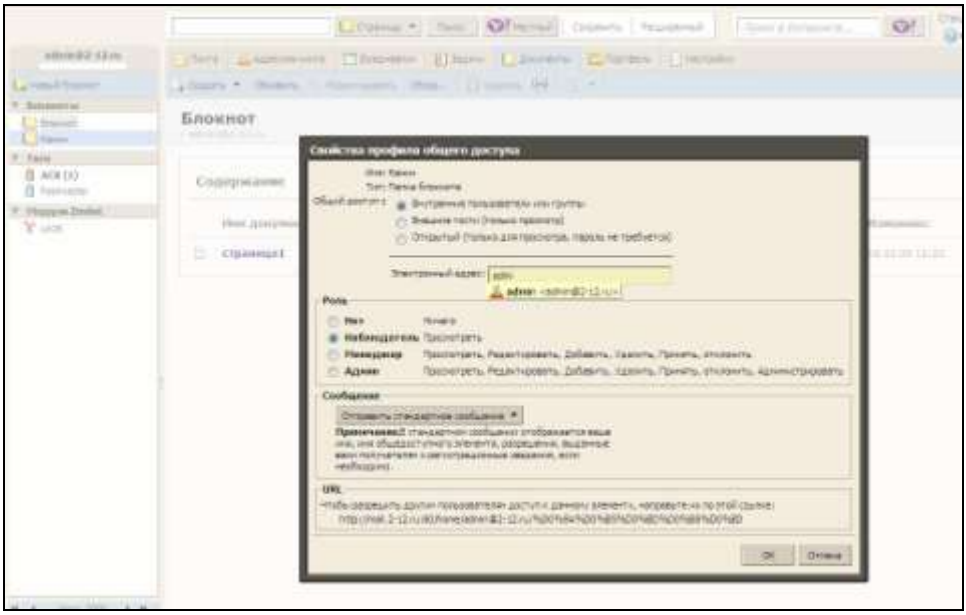


Рис. 6.33. Предоставление папки с документами в общий доступ

В общий доступ папка предоставляется из меню ее свойств. Вы должны указать права доступа и направить приглашения для подключения к папке дру-

гим пользователям. Поиск пользователей осуществляется по глобальной адресной книге, так что обычно достаточно набрать только первые символы адреса, чтобы система предложила найденную учетную запись.

Обратите также внимание пользователей на раздел **Настройки**, в котором содержатся операции настройки параметров учетной записи. В том числе, смена пароля пользователя, создание фильтров сортировка почты, настройка типа отображения сообщений (по теме или дате), параметры автоответов, создание оповещений о получении почты (удобно при настройке оповещений о получении почты через SMS на сотовый телефон и т. п.).

Пользователи могут создавать несколько календарей и использовать, например, напоминания о предстоящих событиях из нескольких источников.

Кроме того, пользователи должны знать, что спам-фильтрация в Zimbra является обучаемой: если сообщения перетаскивать из папки спама в папку *Входящие* или наоборот, то программа впоследствии будет допускать меньше ошибок классификации сообщений.

Почтовый клиент Zimbra

Для Zimbra разработан специальный почтовый клиент — Zimbra Desktop. Программа доступна к бесплатной загрузке с сайта Zimbra и предназначена для установки на операционные системы Windows XP и Windows Vista (рис. 6.34).

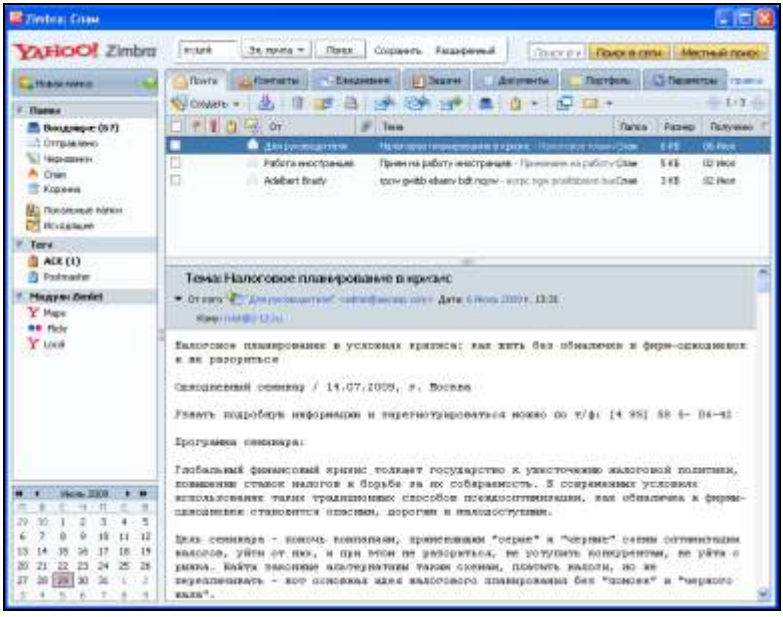


Рис. 6.34. Почтовый клиент Zimbra Desktop

Zimbra Desktop обеспечивает подключение не только к ящикам на серверах Zimbra, но и к Yahoo Mail, Gmail, Microsoft Live Hotmail, а также к любым другим серверам по протоколам IMAP и POP.

Конечно, вы можете выбрать и любые другие почтовые клиенты, поддерживающие стандартные протоколы, применяемые в ZCS.

Интеграция с Microsoft Outlook

В Zimbra присутствует программный коннектор, позволяющий работать в Microsoft Outlook с почтовыми ящиками на сервера ZCS. Этот коммерческий продукт, он доступен только обладателям платной версии Zimbra Network.

Особенности настройки фильтрации спама в ZCS

В ZCS каждое сообщение оценивается некоторой численной величиной, свидетельствующей о "спам-подозрительности". Делает это компонент SpamAssassin. В ZCS оценка от SpamAssassin используется для пропуска или удаления сообщений. Уровень в 20 единиц от SpamAssassin в ZCS принимается за 100%. При уровне от 33 до 75%, сообщение попадает в ящик нежелательной почты пользователя, а при бóльших значениях — удаляется по умолчанию. Эти уровни можно изменить в графическом интерфейсе управления.

В ZCS доступно обучение системы на спам. Для этого пользователь должен в Web-интерфейсе отметить нежелательные сообщения как спам, а случайно попавшие в ящик нежелательной почты — как благонадежные. Такие сообщения попадают в специальные почтовые ящики, обрабатываются сценарием и формируют базу нежелательной почты.

Кроме описанного способа оценки спама, в ZCS можно дополнительно включить стоп-листы реального времени (по умолчанию они отключены). Можно включить следующие стоп-листы:

- dnsbl.njabl.org
- cbl.abuseat.org
- bl.spamcop.net
- dnsbl.sorbs.net
- sbl.spamhaus.org
- relays.mail-abuse.org

Для этого необходимо добавить соответствующий стоп-лист с помощью команды `zmprov`. В параметрах команды следует указать все блокировки, при-

чем перечисленные стоп-листы должны быть указаны каждый по типу *zimbraMtaRestriction "reject_rbl_client стоп-лист"*. Таким образом, учитывая три включенных фильтра по умолчанию, строка команды будет выглядеть в максимальном случае так, как в листинге 6.5.

Листинг 6.5

```
zmprov mcf zimbraMtaRestriction reject_invalid_hostname
zimbraMtaRestriction
       reject_non-fqdn_hostname zimbraMtaRestriction
reject_non_fqdn_sender
       zimbraMtaRestriction "reject_rbl_client dnsbl.njabl.org"
zimbraMtaRestriction
       "reject_rbl_client cbl.abuseat.org" zimbraMtaRestriction
"reject_rbl_client
       bl.spamcop.net" zimbraMtaRestriction "reject_rbl_client
dnsbl.sorbs.net"
       zimbraMtaRestriction "reject_rbl_client sbl.spamhaus.org"
zimbraMtaRestriction
        "reject_rbl_client relays.mail-abuse.org"
```

Резервное копирование Zimbra

Бесплатная версия Zimbra не содержит настроек для выполнения операций резервного копирования. Поэтому вам следует воспользоваться рекомендациями со страницы **http://wiki.zimbra.com/index.php?title=Open_Source_Edition_Backup_Procedure**. Этот источник содержит несколько различных сценариев, выполняющих резервное копирование данных сервера.

Логика работы всех сценариев примерно одинаковая. Сначала производится пересылка в локальную папку резервного копирования незаблокированных данных (для минимизации времени остановки служб Zimbra), потом останавливаются процессы Zimbra (если процесс не останавливается за выделяемое в сценарии время, он удаляется) и проводится окончательная синхронизация с локальной копией. Затем службы Zimbra запускаются, а сценарий начинает передачу данных из локальной папки резервного копирования на удаленный сервер. После завершения сценарий фиксирует продолжительность всех операций.

Приведенные сценарии хорошо комментированы, так что установить их на сервер не составит особого труда.

Трассировка сообщений в Zimbra

Чтобы узнать состояние отправки или получения сообщения, в Zimbra необходимо выполнить команду `zmmsgtrace`. В качестве ее параметров (фильтров) можно указать идентификатор сообщения, адрес отправителя или получателя, IP-адрес почтового сервера и временной диапазон.

По умолчанию данные трассировки хранятся 30 дней.

Например, можно ввести команду, чтобы увидеть информацию по всем сообщениям, отправленным пользователем. Листинг 6.6 иллюстрирует результат.

Листинг 6.6

```
zmmsgtrace -s user@rrr.ru
Tracing messages
        from user@rrr.ru

Message ID '15614059.101246175945950.JavaMail.SYSTEM@desktop'
user@rrr.ru -->
                aaa.bbb@isory.ee
  Recipient aaa.bbb@isory.ee
  2009-06-28 13:59:29 - mail.rrr.ru (192.168.31.20) --> mail
  2009-06-28 13:59:34 - mail --> 127.0.0.1 (127.0.0.1]:10024) status sent

Message ID '30004518.21246795150656.JavaMail.SYSTEM@desktop'
user@rrr.ru -->
                sfn@list.ru
  Recipient sfn@list.ru
  2009-07-05 17:59:41 - mail.rrr.ru (192.168.31.20) --> mail
  2009-07-05 17:59:46 - mail --> 127.0.0.1 (127.0.0.1]:10024) status sent
…
26 messages found
```

По этой информации видно, что пользователь отправил 26 сообщений. Статус сообщений — *отправленные*.

Иногда такой информации недостаточно для выяснения причин недоставки сообщений. В таком случае придется обращаться к журналам отдельных компонентов почтового сервера. Так, журнал агента сообщений хранится

как /var/log/mail.log. В этом журнале можно узнать, например, на какой сервер было передано сообщение:

```
Jul 23 01:10:10 mail postfix/smtp[2652]: 3C9B252A002: to=<kenin@ask.ru>,
relay=mail2.ask.ru[81.91.63.38]:25, delay=2.3, delays=0.04/0.02/0
.04/2.2, dsn=2.6.0, status=sent (250 2.6.0
<698422244.8981248289804948.JavaMail.root@mail> Queued mail for delivery)
```

Приведенный отрывок журнала говорит, что сообщение было удачно (код 250) отправлено на почтовый сервер mail2.ask.ru с адресом 81.91.63.38 для пользователя kenin@ask.ru. Такие сведения позволят уже конкретно выяснить прохождение сообщения на другом сервере.

Если подобная подробная информация будет постоянно востребована, то необходимо изменить период хранения данных журналов. По умолчанию они архивируются ежедневно программой `logrotate`, и система хранит семь таких архивов (информация доступна только за прошедшую неделю).

Самый простой способ — изменить настройку числа хранимых копий в файле /etc/logrotate.d/zimbra. В строке, начинающейся со слова `rotate`, введите необходимое вам значение и сохраните изменения.

Поиск неисправностей ZCS

При возникновении проблем в работе служб ZCS следует увеличить объем протоколирования. По умолчанию уровень протоколирования настроен в режиме INFO. Для увеличения протоколирования следует добавить строку

```
log4j.logger.zimbra.soap=DEBUG
```

в файл /opt/zimbra/conf/log4j.properties.in и перезагрузить сервер. Чтобы режим протоколирования сменился без перезагрузки, можно выполнить команду `zmmtaconfig mailboxd`. В этом случае возможна небольшая пауза до того момента, когда изменения начнут действовать.

Протоколирование можно установить не в целом для всего сервера, а только для одного пользователя. Это более щадящий режим с точки зрения дополнительной нагрузки на сервер. Такая операция выполняется командой `zmprov` следующим образом:

```
zmprov addAccountLogger адрес_пользователя zimbra.soap debug
```

Подробности использования данной команды следует уточнить по онлайновой документации.

> ***Примечание***
>
> Режим отладки пользователя действует только до перезагрузки сервера.



Глава 7

Организация корпоративных ресурсов

Традиционно под общими ресурсами системы понимались предоставленные в общее пользование файлы на сервере (и рабочих станциях). На сегодня это наиболее быстрый и легко настраиваемый тип общего ресурса, но не самый удобный.

> ***Замечание***
>
> Мы не будем в этом разделе рассматривать совместное использование серверов печати.

Каких же возможностей не хватает для данных ресурсов? Во-первых, как правило, общие папки со временем превращаются в подобие "свалки", размер которой неконтролируемо увеличивается, а найти нужные данные становится очень сложно. Во-вторых, более удобно представление, когда вместо перечня имен файлов пользователь сможет увидеть какую-то информацию, иллюстрации, заметки и т. п. В-третьих, обычно для выполнения действий над каким-либо проектом необходима *рабочая область*. Тогда появляется возможность одним щелчком мыши позвонить автору документа, создать приглашение на обсуждение документа группе участников, видеть доступность других сотрудников и взаимодействовать с ними в службе мгновенных сообщений. Причем доступ к такой рабочей области пользователь хочет иметь как из внутренней сети, так и из дома, с рабочего компьютера или, при необходимости, с мобильного устройства. При обеспечении версионности документов, наличии удобного поиска данных одновременно по всем типам документов и т. п.

Подобную функциональность реализуют *портальные решения*. Существуют как коммерческие (IBM WebSphere, портал Oracle, Microsoft SharePoint Server и др.), так и бесплатные продукты, обеспечивающие не худшую функциональность и масштабируемость, чем платные программы (Liferay, eXo Platform, eGroupware, службы Windows SharePoint Services и др.).

Использование распределенной файловой системы

При создании общих файловых ресурсов целесообразно отказаться от предоставления ресурсов с конкретного сервера. В случае выхода из строя сервера или необходимости перемещения ресурса на другую систему (например, из-за нехватки дискового пространства) администратору придется менять точки подключения на всех компьютерах своей сети. Выходом из данной ситуации является создание *сетевой* файловой системы. Учитывая, что у большинства клиентов установлены рабочие станции Windows, мы опишем совместимые варианты настройки.

Распределенная файловая система (Distributed File System, DFS) представляет собой коллекцию ссылок на совместные ресурсы, находящиеся на различных компьютерах сети, доступ к которым производится через единую точку входа. Структура DFS напоминает дерево каталогов: на самом "верху" расположена одна точка входа, называемая *корнем DFS*, к которой подключены вложенные папки.

DFS в Windows может быть привязана к домену (имена ресурсов начинаются с имени всего домена) или к какому-либо серверу. DFS в Linux реализуется с привязкой корня (точки, в которой видна структура общих ресурсов данного DFS) к серверу.

> ***Примечание***
>
> Использование доменного корня DFS в системах Linux представляет определенные сложности, поскольку по умолчанию запрос доменного корня не возвращает имени сервера хранения. Поэтому для подключения к такому ресурсу системы Ubuntu необходимо указывать адрес ссылки DFS на конкретном сервере.

Если администратору по каким-либо причинам необходимо переместить ресурс в структуре DFS на другой сервер, достаточно просто скопировать файлы по новому пути и заменить ссылку со старой сетевой папки на новую. При этом все сетевые пути для клиентов (если, конечно, они указывали на структуру DFS) останутся неизменными.

Создание DFS в Windows-системах

Корень DFS можно создать на любом сервере Windows 200*x*. Причем на рядовых серверах возможно создание только одного корня DFS, в домене может поддерживаться *несколько корней DFS* (разными контроллерами).

В качестве корня DFS указывают любую совместно используемую папку (мастер создания DFS позволяет создать такую папку в процессе настройки). Рекомендуется не хранить в этой папке никаких файлов, а задействовать ее только для создания ссылок на сетевые ресурсы.

Создание корня DFS выполняется мастером операций (из меню **Администрирование | Управление DFS |** вызвать операцию **Новое пространство имен**) — рис. 7.1. Мастер позволяет настроить разрешения сетевого доступа для общей папки, в которой будет размещен корень DFS.

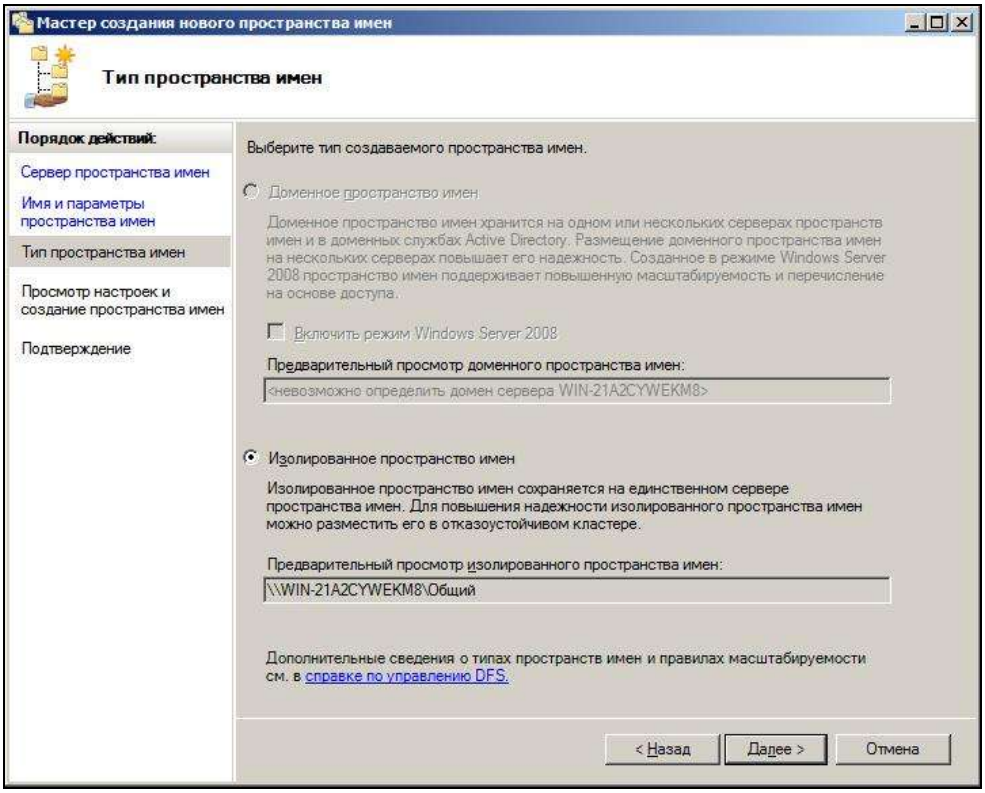


Рис. 7.1. Мастер создания нового пространства имен в Windows 2008

После создания корня DFS необходимо начать собирать структуру папок распределенной файловой системы. Для этого с помощью оснастки управления следует добавить папки, указав в их свойствах ссылки на уже существующие *совместно используемые ресурсы сети*. Причем можно указать несколько ссылок на аналогичные ресурсы на разных компьютерах. Операция обычно не представляет никакой сложности (рис. 7.2).

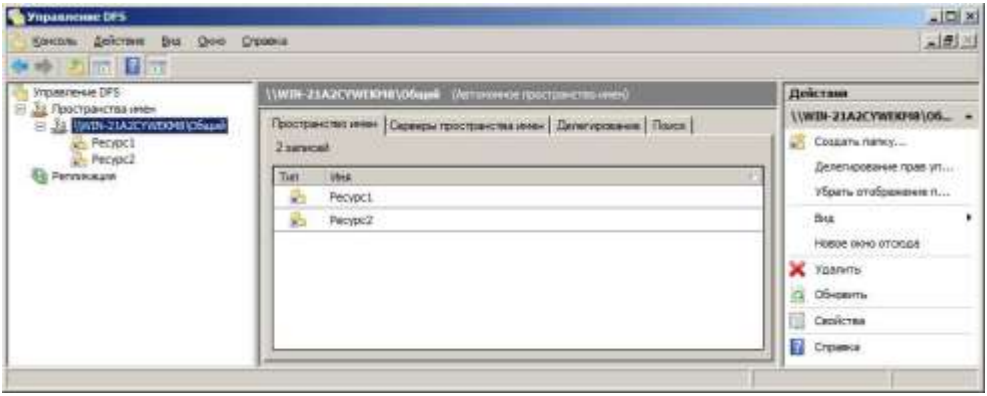


Рис. 7.2. Пространство имен с настроенными ссылками

В окне на рис. 7.2 вы можете видеть, какие совместно используемые папки подключены в это пространство имен, просмотреть серверы имен, найти объекты и т. д.

Репликация DFS в домене Windows

В домене Windows возможна настройка репликации DFS — автоматическое поддержание копий данных на нескольких компьютерах. Например, можно создать копию папки с файловыми ресурсами центрального офиса в удаленном филиале, и система самостоятельно будет синхронизировать изменения, независимо (в каждом офисе) вносимые пользователями. Причем пользователи будут автоматически подключаться к тому компьютеру, данные которого расположены "ближе" к пользователю.

Подобная структура DFS является *отказоустойчивой*. Каждую ссылку можно продублировать, создав вторую ссылку на аналогичный сетевой ресурс на другом компьютере. В результате при недостижимости одного ресурса клиенты будут перенаправлены к функционирующему компьютеру. Причем система может *автоматически синхронизировать* эти ресурсы. Если данные будут изменены в папке по одной ссылке, то в папке по другой ссылке они будут продублированы.

Реплицируемые ресурсы нужно располагать в папках с NTFS 5.0, поскольку в процессе задействована система протоколирования этой файловой структуры для отслеживания изменений.

По умолчанию репликация не включена. В Windows 2008 она создается операцией **Репликация | Новая группа репликации**. Откроется мастер операций, который выполнит последующие настройки в зависимости от ответов

администратора (рис. 7.3). Мастер настроит все параметры репликации в зависимости от ответов пользователя: подключит папки, настроит график репликации и ограничения по пропускной способности, если используются каналы Интернета, и т. п.

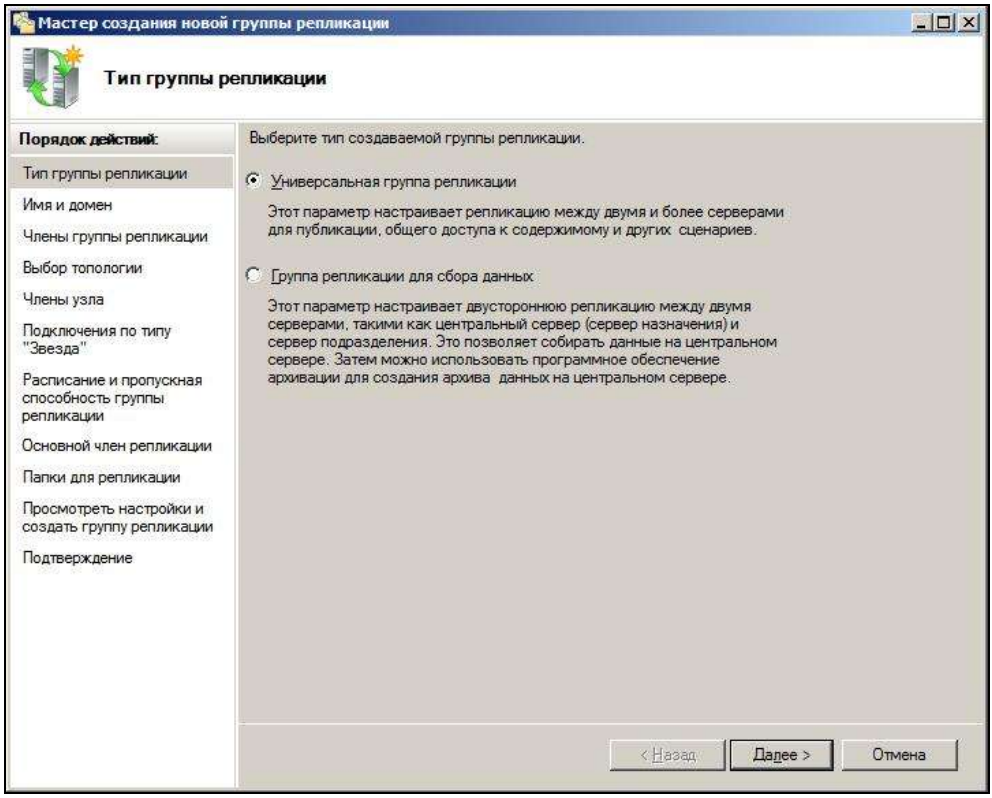


Рис. 7.3. Мастер настройки репликации в Windows 2008

Для серверов Windows 2003 необходимо выделить несколько ссылок на аналогичные ресурсы, выбрать команду **Синхронизовать,** указать основной ресурс (*мастер*, он будет считаться эталонным при начале репликации).

Автоматически синхронизируются не все файлы. Из репликации исключаются временные файлы (список расширений можно просмотреть в настройках). Сами файлы реплицируются только после того, как пользователь завершает работу с ними. Иными словами, если пользователь открыл файл и работает с ним в течение всего дня, то копия файла по реплицируемой ссылке изменится только *после завершения работы — вечером*.

Если два пользователя одновременно работают с одним и тем же файлом в различных репликах, то система разрешит такой конфликт путем сохранения тех изменений, которые были внесены в файл, сохраненный позже.

Настройка графиков репликации в серверах 2003 находится в задаче AD **Пользователи и компьютеры**. Открыв оснастку, следует включить отображение дополнительных функций (**Вид | Дополнительные функции**) и найти необходимый корень DFS. Открыв его свойства на вкладке **Набор репликации**, нужно нажать кнопку **Изменить расписание** и отредактировать график (рис. 7.4).

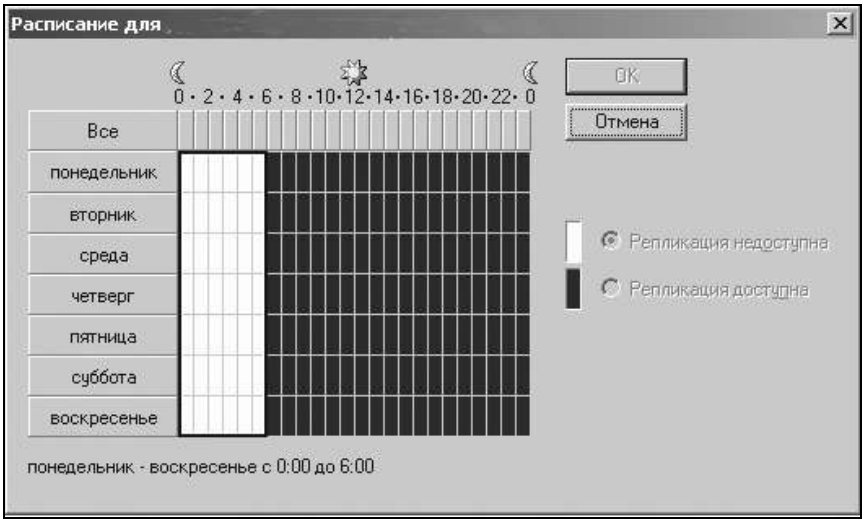


Рис. 7.4. Настройка графика репликаций DFS

Репликация папок в рабочих группах

Описанная автоматическая репликация работает только в условиях домена Windows. Если у вас рабочая группа или необходимо синхронизировать данные между двумя компьютерами через сеть Интернета, то можно воспользоваться одной из бесплатных программ, которые легко найти в Сети (см., например, **http://www.softsoft.ru/search/freeware/8021/index.htm**). Каждая программа имеет несущественные отличия.

Основные "минусы" таких бесплатных программ по сравнению с коммерческими версиями — это выполнение заданий периодически, по некоторому графику (до начала очередного периода синхронизации данные в папках могут

отличаться) и отсутствие поддержки режима копирования только измененных данных внутри файла (поддерживается современными версиями Windows; это позволяет снизить объем данных, передаваемых по каналам связи). В подавляющем большинстве случаев эти характеристики несущественны. Так, автор эксплуатирует без нареканий одну из таких программ синхронизации папок уже более полутора лет.

Настройка DFS в Ubuntu

Настройка распределенной файловой системы в Ubuntu не представляет особой сложности и работает со всеми версиями Windows. Требуется лишь добавить несколько опций в файл конфигурации Samba.

Для включения DFS необходимо в файле конфигурации Samba в секции `global` добавить строку `host msdfs = yes`:

```
[global]
...
host msdfs = yes
...
```

А в описание для папки, которая должна быть корнем DFS, — строку `msdfs root = yes`:

```
[dfs]
path = /<путь к папке>
msdfs root = yes
```

Чтобы в совместно используемой папке появились сетевые папки, необходимо создать в ней символические ссылки на эти ресурсы по следующему образцу:

```
ln -s msdfs:serverA\\shareA linka
ln -s msdfs:serverB\\share,serverC\\share linkb
```

В первом примере в папке создана ссылка с названием `linka`, указывающая на общую папку `shareA` на сервере `serverA`, во втором — ссылке `linkb` сопоставлено два сетевых ресурса.

Лимитирование предоставляемых файловых ресурсов

Настройка квотирования в Ubuntu

В Ubuntu можно настроить квоты на дисковое пространство для пользователей и для групп. Между этими квотами установлена следующая связь: если

лимит для группы исчерпан, то всем пользователям, входящим в эту группу, запись на диск будет запрещена. Несмотря даже на то, что по их индивидуальным квотам они могли бы еще дозаписывать данные.

По умолчанию программы квоты в Ubuntu не установлены, необходимо добавить как собственно программу квотирования, так и комплект утилит управления квотами:

```
apt-get install quota quotatool
```

Следующим шагом необходимо включить возможность квотирования для дисков. Для этого нужно открыть в текстовом редакторе (также с правами суперпользователя) файл /etc/fstab и найти строки, монтирующие ваши диски. В листинге 7.1 приведен пример реального файла fstab и соответствующая строка, которая монтирует диск в качестве корневой файловой системы (/), выделена полужирным шрифтом.

> ***Замечание***
>
> Для удобства чтения значение UUID диска укорочено.

Листинг 7.1

```
# /etc/fstab: static file system information.
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
proc            /proc           proc    defaults        0       0
# /dev/sda1
UUID=a116dc47-   /          ext3    relatime, errors=remount-ro 0      1
# /dev/sda5
UUID=75aa5a1d-...   none            swap    sw              0           0
/dev/scd0      /media/cdrom0   udf,iso9660 user,noauto,exec,utf8 0      0
/dev/fd0        /media/floppy0  auto    rw,user,noauto,exec,utf8 0      0
```

Добавьте в выделенной строке в блок опций (через запятую) ключевое слово `usrquota` для включения квот для пользователей, `grpquota` — для включения квот для групп, или оба (включаются все квоты):

```
UUID=a116dc47-... /    ext3    relatime,errors=remount-ro,
usrquota,grpquota 0       1
```

Теперь необходимо указать системе, в каком файле хранятся значения квот. Сделать это можно было и в файле fstab (указать как `usrquota=...`), но удобнее создать отдельный файл quota.user для квот пользователей и quota.group для квот групп. Эти файлы должны быть на каждом диске, на котором вы

включаете квоты, и находиться всегда в корне диска. Создадим пустые файлы в корне диска и запретим другим пользователям доступ к этим файлам, установив разрешение с маской 600:

```
touch /quota.user /quota.group
chmod 600 /quota.*
```

Квотирование включается после перемонтирования тома. Это можно сделать после перезагрузки системы либо в процессе работы:

```
mount -o remount /
```

Теперь необходимо пересчитать реальные значения квот:

```
quotacheck -avugm
```

Не обращайте внимания на предупреждения программы, они вызваны тем, что файлы `quota.user` и `quota.group` были созданы вручную. И последняя операция по установки программы квотирования — включение квот:

```
quotaon -avug
```

После установки программы необходимо при помощи команды `edquota` настроить квоты для пользователей и групп (с ключом `-g` команда будет редактировать квоты групп):

```
edquota -u имя_пользователя
```

Эта команда открывает в текстовом редакторе файл настроек. При создании квоты на экране вы увидите примерно такое содержимое:

```
Disk quotas for user kenin (uid 1000):
  Filesystem           blocks       soft       hard     inodes     soft
hard
  /dev/sda1             25256          0          0         11        0
0
```

Параметры `block` и `inodes` показывают, сколько блоков (размером по 1 Кбайт) и дескрипторов файлов в настоящее время используется этим пользователем. Для определения квоты необходимо установить желаемое значение в блоки `soft` и `hard`. Soft — это "мягкое" ограничение, пользователь получит предупреждение, но дальнейшая запись будет возможна в течение некоторого периода времени. По умолчанию этот период установлен равным семи дням, его можно настроить командой

```
edquota -t
```

`Hard` — жесткое ограничение, при достижении этого значения последующая запись будет невозможна. Чтобы отключить квоту, просто установите в 0 значение соответствующего блока.

Ускорить редактирование можно, записав квоту какого-либо пользователя в качестве шаблона. Следующая команда создаст записи квот для всех поль-

зователей (*, можно указать имена явно) по шаблону пользователя `kenin`: `edquota -p kenin -u *`

> ***Примечание***
>
> При некорректных выключениях сервера информация о реальном использовании дискового пространства может исказиться. Поэтому существует рекомендация о периодическом выполнении команды `repquota -avugm` с помощью `cron`. Например, раз в месяц.

Еще несколько полезных команд: `quota` — отображает на экране параметры квоты для пользователя/группы, `repquota` — формирует отчет по реально установленным объемам и квотам для дисков.

Настройка квотирования в Windows

В Windows возможно применение различных вариантов квотирования. На уровне файловой системе можно включить ограничения по объему для каждой учетной записи. А для сервера версии R2 можно устанавливать ограничения на объем папки и на типы файлов, которые можно размещать в ней.

Квотирование на уровне файловой системы

Квотирование диска возможно для компьютеров на дисках с файловыми системами NTFS. Чтобы включить квоту, следует открыть свойства жесткого диска, перейти на вкладку **Квота** и настроить опции (рис. 7.5).

В параметрах настройки можно запретить запись на диск при превышении квоты, а также настроить квоты, которые будут назначаться для вновь создаваемых пользователей. При включении опции **Регистрация...** в журнал системы будут записываться сообщения о превышении заданных лимитов. Кнопка **Записи квот...** позволяет увидеть реальные значения квот на жестком диске.

После того как первоначальные квоты были созданы, изменить их можно в списке **Записи квот**. Достаточно отметить необходимую строчку, через меню свойств открыть свойства соответствующей записи и назначить новые параметры.

Квотирование на уровне файловой системы Windows неудобно тем, что не позволяет устанавливать квоты на группы. Так, если на сервере будут храниться какие-либо общие документы, то их объем будет включаться в квоту того пользователя, который их создал. Это не всегда удобно. В таких случаях администратору можно стать владельцем подобных файлов (для файла или папки выполните последовательность команд: **Свойства** | **Безопасность** | **Дополнительно** | **Владелец** | **Изменить**). Поскольку квоты считаются по

владельцам файлов, то такая операция перенесет квоты с пользователя на администратора, который может для себя отключить контроль квот.

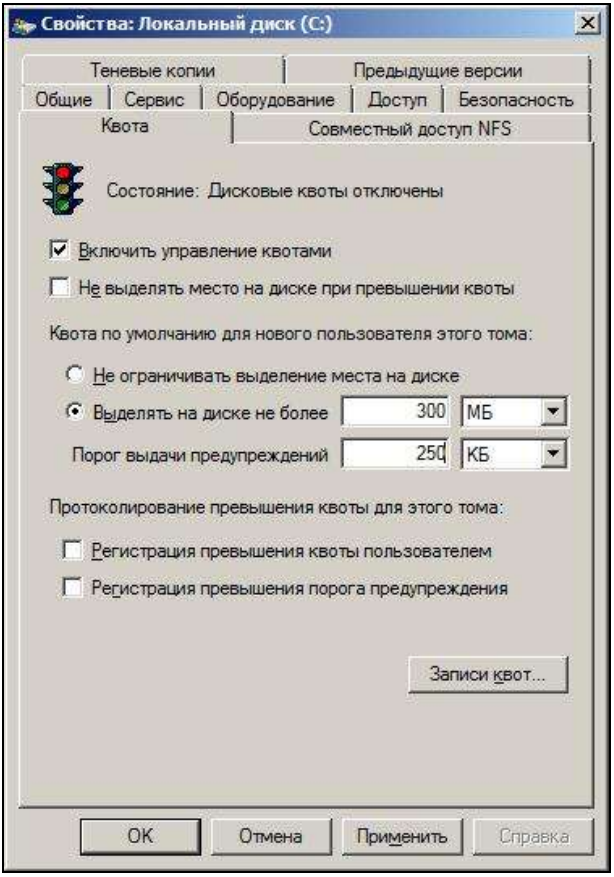


Рис. 7.5. Настройка квот на диске Windows

Квотирование общих папок

В составе выпуска R2 присутствуют компоненты, позволяющие реализовать политику ограничений для совместно используемых ресурсов. В частности, можно установить лимиты на объемы папок и запретить размещение в них определенных типов файлов. По умолчанию, после установки Windows Server 2003 R2 (выпуск Windows 2008 R2 на момент подготовки книги был еще не доступен) эти компоненты не устанавливаются в систему. Их необходимо добавить как роль **Файлового сервера**.

Замечание

Компоненты можно установить и через программу **Установка/Удаление программ** (компоненты **Управление файловым сервером** и **Диспетчер ресурсов файлового сервера**), но они требуют предварительной установки .NET, поэтому удобнее выполнить операцию через добавление роли.

После установки компонентов (и перезагрузки системы, если это были первые компоненты R2), для доступа к необходимым нам настройкам следует открыть меню **Администрирование | Управление файловым сервером**. В открывшейся оснастке в панели навигации нас будет интересовать только первый блок — **Диспетчер ресурсов файлового сервера** (рис. 7.6). По умолчанию в системе представлено несколько шаблонов политик ограничения доступа, по образцу которых можно создать собственные правила.

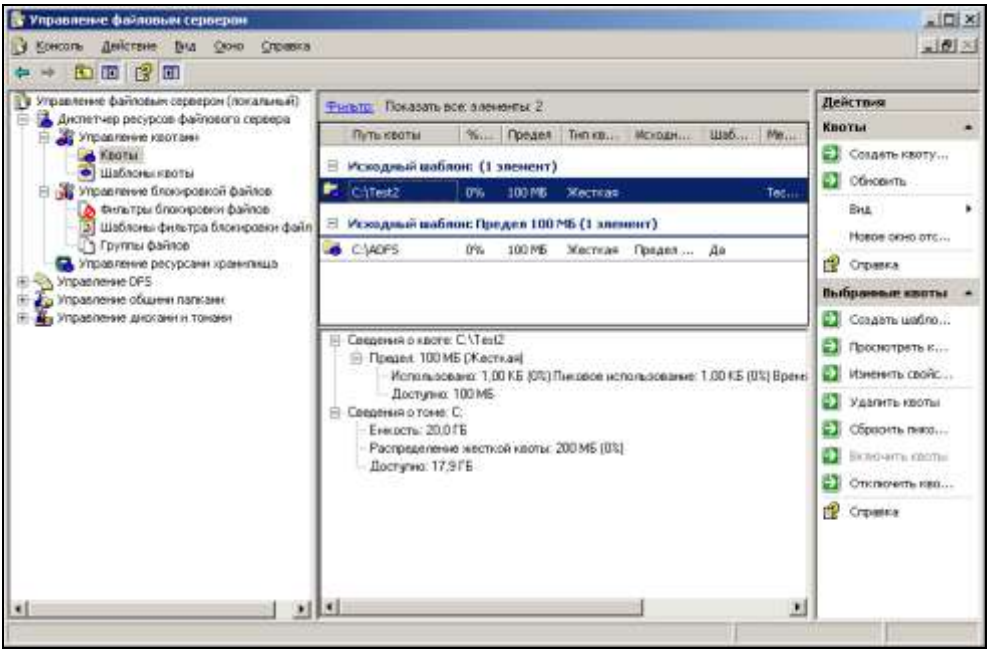


Рис. 7.6. Управление квотами. Программа управления файловыми ресурсами сервера R2

Методика использования квот проста. Вы создаете новую квоту, указывая, к какой папке она будет применена. В квоте вы определяете максимальный объем данной папки, тип ограничения (в случае жесткого ограничения превысить указанный в квоте порог невозможно). Кроме того, для каждой квоты можно задать несколько действий, которые будут выполняться при достижении некоторого объема: например, можно указать, что при достижении 80%

от предельного значения объема папки будет направлено сообщение пользователю по электронной почте, а при достижении 90% аналогичное сообщение уйдет администратору (рис. 7.7). Возможными действиями системы может быть отсылка сообщений электронной почты (текст сообщения доступен для редактирования), запись в журнал событий, выполнение любой команды операционной системы.

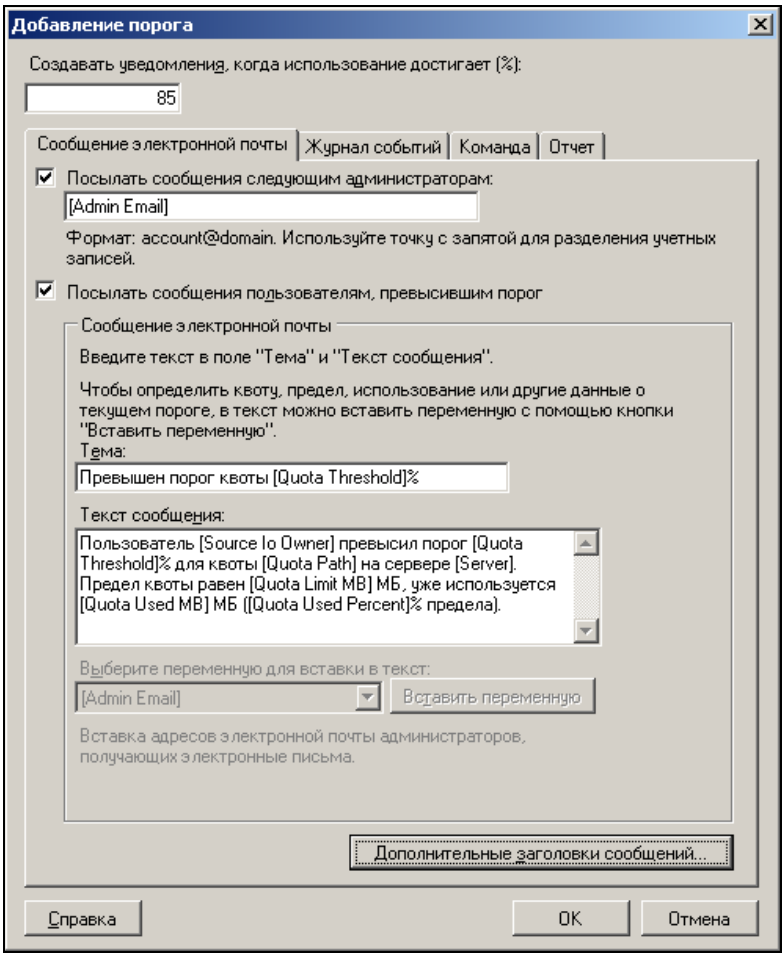


Рис. 7.7. Редактирование правил квоты на папку

Блокировка записи в папки по типам файлов в Windows

Вторая возможность, предоставляемая консолью **Управление файловым сервером**, — это блокировка записи в папку определенных типов файлов.

Такая настройка позволяет запретить запись в папку файлов по заданному шаблону имени. Как правило, устанавливаются ограничения по типу файлов (по расширениям имени файла), но можно задавать и маски на само имя. В системе существует несколько заранее подготовленных шаблонов (аудио- и видеофайлы, файлы программ офиса и т. п.), легко можно добавить и свои настройки (рис. 7.8).

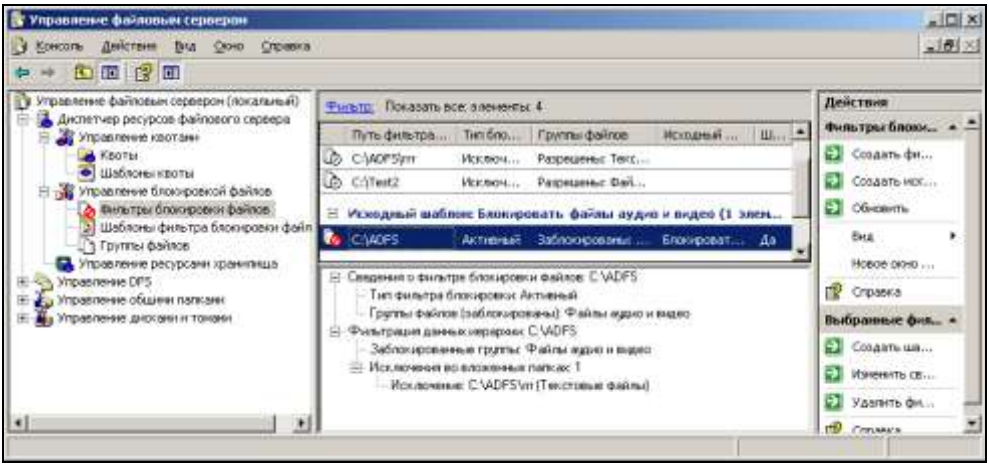


Рис. 7.8. Интерфейс операции блокировки файлов

Ограничения как по объему, так и по типу файлов можно наложить на саму папку и отдельно на вложенные каталоги. Таким способом можно достаточно точно настроить политики хранения информации.

Замечание

Обратите внимание, что при задании шаблона блокировки имеется возможность явно указать разрешенные файлы. Например, можно заблокировать все видеофайлы, но разрешить те, названия которых начинаются с символов "мои" и т. п.

Задача **Управление ресурсами хранилища** позволяет выполнять на периодической основе отчеты по использованию назначенных ограничений и направлять их на просмотр ответственным специалистам.

Примечание

Блокировка по типу файлов привносит только некоторые неудобства в работу пользователей. Программа не проверяет тип содержимого сохраняемой информации, поэтому пользователи могут либо сохранять файлы в архивах, либо просто давать им другие расширения. При этом, настроив у себя новые ассоциации для типов файлов, пользователи смогут легко открывать такие файлы в программах для работы.

Запрет записи на сетевые ресурсы Ubuntu по типам файлов

Скрыть файлы в папке при просмотре пользователем, в Ubuntu позволяет директива Samba `veto files`. Перечисленные в такой строке файлы не будут видны пользователю и, соответственно, не смогут быть им созданы. По правилам синтаксиса строка параметров в `veto files` должна начинаться и заканчиваться слешем, все перечисляемые в ней элементы также должны разделяться слешами:

```
veto files = /*.dll/
veto files = /*.dll/*.exe/
```

> ***Примечание***
>
> Если в предоставленной в общее пользование папке существуют файлы, подпадающие под описание параметра `veto files`, и пользователям предоставлено право удаления папки, то такая папка будет удалена только в том случае, если для нее включено следующее описание: `delete veto files = yes`.

Корпоративные порталы

Корпоративные порталы обеспечивают возможность безопасного и удобного доступа пользователей к разнородной информации, позволяют интегрировать данные различных приложений, позволяют применять регламенты публикации данных (функции документооборота) и т. д.

Один из наиболее перспективных решений открытых кодов — портал LifeRay (**http://www.liferay.com/**), в нашей стране распространены также решения на основе eGroupware (**http://www.egroupware.org/**) во многом благодаря наличию русскоязычного интерфейса. Эти два решения занимают по разным оценкам порядка 2/3 эксплуатируемых порталов на основе открытого кода. Из коммерческих решений, на взгляд автора, лидирует IBM WebSphere. В последнее время разработчики предпринимают активные действия по распространению решения Microsoft SharePoint Server.

Следует обратить особое внимание, что сам портал — это платформа для реализации тех или иных *решений* в информационной системе конкретного предприятия. Поэтому, даже покупка коробочной коммерческой версии не позволит быстро создать *корпоративный* портал. Скорее всего, вы будете иметь набор разрозненных базовых функций. Внедрение корпоративного портала — достаточно сложный процесс, зависящий от состояния информационной системы предприятия, ожиданий заказчика и опытности команды внедрения. Поэтому в данной книге мы опишем только базовые моменты

инсталляции бесплатных портальных решений, которые помогут вам установить портал и получить первый опыт работы с ним. После некоторого периода опытной эксплуатации вы сможете уже более обоснованно подойти к выбору программного решения и его наполнению.

Установка Liferay на сервере Ubuntu

Liferay является, по сути, профессиональным порталом, позволяющим реализовать практически любые функции на основе стандартов, принятых для построения порталов. Прежде чем начать настраивать и эксплуатировать его, обязательно следует изучить сопроводительную документацию.

Для Liferay доступны для загрузки как собственно портал, так и готовые его сборки с различными серверами приложений, которые доступны с сайта **http://www.liferay.com/**. Мы опишем запуск бесплатного варианта портала, который на момент подготовки книги имел версию 5.2.3.

Загрузка портала Liferay (страница загрузки **http://www.liferay.com/Web/guest/downloads/portal**) представляет собой файл архива с подготовленным к запуску сервером Tomcat. Портал снабжен примером организации, который доступен после старта приложения. Все данные хранятся в этой конфигурации в собственной базе данных портала, что не является самым производительным решением. Если вы захотите использовать сервер баз данных, например, MySQL, то легко можно найти описания, как подключить портал к этому серверу и перенести на него данные.

Портал Liferay выполнен на Java, поэтому предварительно на сервер необходимо установить пакет Sun Java Development Kit. Он доступен через репозитории:

```
apt-get install sun-java6-jdk
```

Это достаточно большая загрузка (более 50 Мбайт). По умолчанию пакет устанавливается в папку /usr/lib/jvm, при этом в папке создается символическая ссылка java-6-sun на каталог с файлами установки (в нашем случае это была папка java-6-sun-1.6.0-14. После установки нужно вручную внести путь к папке в файл /etc/jvm, причем желательно поместить новую строчку первой (листинг 7.2, новая строка выделена полужирным).

Листинг 7.2

```
# This file defines the default system JVM search order. Each
# JVM should list their JAVA_HOME compatible directory in this file.
# The default system JVM is the first one available from top to
```

```
# bottom.

/usr/lib/jvm/java-6-sun
/usr/lib/jvm/java-gcj
/usr/lib/jvm/ia32-java-1.5.0-sun
/usr/lib/jvm/java-1.5.0-sun
/usr
```

Теперь можно разархивировать загруженный файл портала:

```
unzip liferay-portal-tomcat-6.0-5.2.3.zip
```

Примечания

Если программа *unzip* не установлена, то ее также следует загрузить командой `apt-get install unzip`.

Желательно поместить портал в папку, предназначенную для программных кодов, например, в /opt. Именно этот вариант и будет показан в примере (с учетом актуального на момент подготовки книги номера версии портала).



Рис. 7.9. Пример входной страницы портала Liferay тестовой организации

После разархивирования можно запускать портал командой:

```
/opt/liferay-portal-5.2.3/tomcat-6.0.18/bin/startup.sh
```

Портал может запускаться довольно долго (несколько минут). Чтобы войти в него, достаточно набрать в строке обозревателя адрес **http://<имя_сервера>:8080**. Вы должны увидеть в обозреватели страницы тестового портала — организации 7Cogs (рис. 7.9). Вы можете войти на портал как администратор организации (достаточно выбрать ссылку входа, пароль отсутствует) и попробовать различные варианты настройки портала организации.

Остановка портала осуществляется сценарием `shutdown.sh` (из той же папки), для автоматического запуска необходимо создать ссылку на этот файл в папках автозапуска (*см. разд. "Создание и удаление демонов" в приложении*).

Для создания собственного портала данные организации можно удалить. Подробности операций доступны в Сети.

Установка eGroupware

eGroupware — это портал, написанный на языке программирования Perl и работающий на Web-сервере Apache. Информацию портал хранит на сервере баз данных MySQL. Поэтому перед его установкой эти компоненты должны быть встроены в систему. На сайте разработчика загрузочные файлы портала представляют собой архив виртуального Web-сервера, который необходимо просто подключить к Apache. Но, поскольку большинство пользователей не имеет достаточного навыка работы с этим продуктом, мы предложим следующий простой способ установки.

Установите серверы Apache и MySQL:

```
apt-get install apache2 mysql-server
```

После этой операции будут установлены Web-сервер, сервер баз данных, все необходимые для их работы компоненты. Кроме того, в процессе установки вы назначите пароль для администратора сервера MySQL (в ответ на запрос мастера операций).

Теперь установите с репозиториев портал eGroupware:

```
apt-get install egroupware
```

Самое главное, что при этой установке в систему будут добавлены все необходимые компоненты для работы eGroupware и вам не придется делать это вручную. Скачайте с сайта eGroupware последнюю версию портала (эта версия существенно лучше локализована, чем та, которая находилась в репозиториях Ubuntu на момент подготовки книги), разархивируйте все полученные файлы и просто замените папку, установленную автоматически, на загруженный вами вариант (по умолчанию установка eGroupware командой `apt-get` производится в папку /usr/share/egroupware/).

Остается только добавить компоненты PHP, обеспечивающие взаимодействие с MySQL:

```
apt-get install php5-odbc php5-mysql
```

Перезапустите Apache, чтобы эти изменения были им приняты (/etc/init.d/apache2 restart).

Финальная настройка eGroupware осуществляется из обозревателя Интернета, для чего следует открыть страницу **http://имя_сервера/egroupware/setup**, где представлены рекомендации по необходимым действиям при наличии предупреждений и ошибок (рис. 7.10).

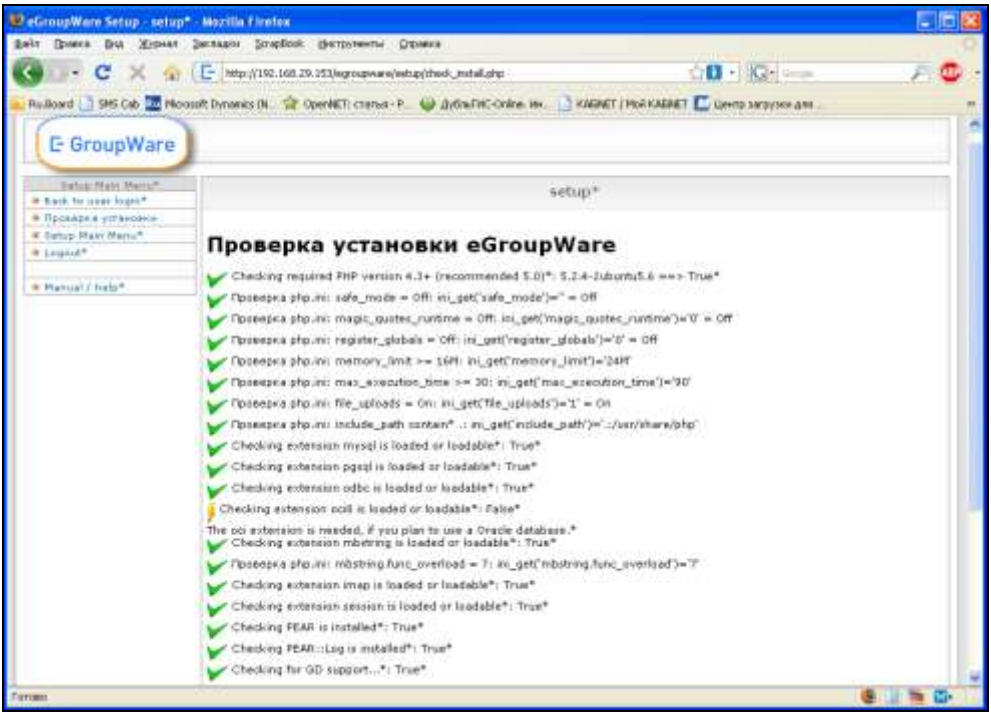


Рис. 7.10. Проверка условий установки компонент, необходимых для настройки eGroupware

Обычно необходима только корректировка содержимого настроек PHP. Здесь есть небольшая тонкость. Поскольку eGroupware — виртуальный каталог Web-сервера, то соответствующие настройки система может получать из нескольких мест, а не только из указанного на странице проверок. Можно, конечно, изменить параметры и оставить только один файл, но проще выполнить согласованные операции редактирования следующих файлов: /usr/share/egroupware/.htacess,

/etc/php5/cli/php.ini, /etc/php5/apache2/php.ini, /etc/egroupware/apache.conf. Еще необходимо загрузить дополнительные модули для php, эту операцию можно выполнить так, как указано в подсказке (*pear install Auth_SASL* и т. д.).

После проверки настроек перейдите в редактирование заголовка (выбрав соответствующую ссылку в интерфейсе управления). Заполните поля настройки. Обратите внимание, что эта форма предлагает новую учетную запись для редактирования портала — *changeme*. Именно с параметрами, определенными в этой форме, нужно будет заходить для дальнейшей установки портала.

После того как вы заполнили поля формы и сохранили настройки в файл, можно переходить к следующему этапу. Войдите в редактирование настроек и последовательно выполните все операции (рис. 7.11). Сначала необходимо создать базу на MySQL (достаточно указать пароль администратора MySQL и эта операция будет выполнена), потом проверить результат и установить приложения.

В заключение следует указать параметры портала и настроить учетную запись администратора. После всех этих операций вы можете начинать работу с порталом по адресу **http://*имя_сервера*/egroupware**.

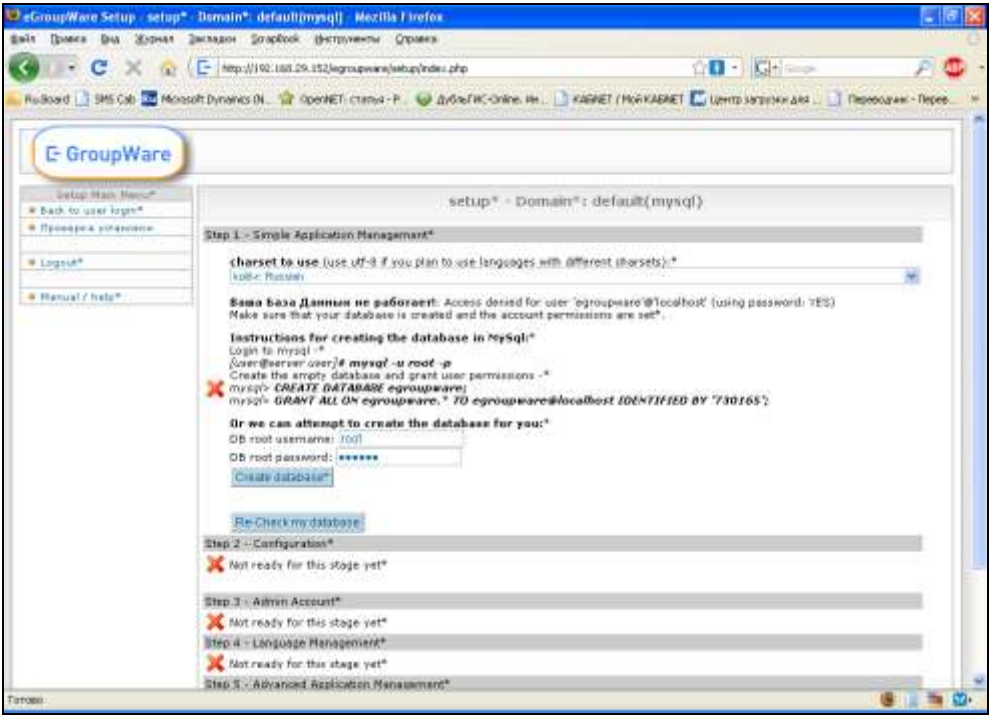


Рис. 7.11. Настройка параметров портала eGroupware

Настройка диаграммы Ганта

Пакет eGroupware можно использовать для планирования работ в организации (создания *проектов*). Традиционно в проектах принято отражать работы в виде диаграммы Ганта. Желательно сразу обновить программу для построения диаграмм Ганта, входящую в eGroupware. Для этого загрузите последнюю версию программы со страницы **http://www.aditus.nu/jpgraph/jpdownload.php**, разархивируйте ее (`tar xzvf` *имя*) и переместите содержимое полученной папки в /usr/share/jpgraph (эту папку нужно создать; для Ubuntu есть некоторые отличия от стандартных рекомендаций по обновлению `jpgraph`). Теперь укажите в настройках путь к этой папке, для чего отредактируйте файл /etc/egroupware/apache.conf. Найдите в нем строку, начинающуюся с php_admin_value open_basedir /usr/share/egroupware, и добавьте в ее конец путь к созданной папке. В результате строка будет выглядеть примерно так:

```
php_admin_value open_basedir /usr/share/egroupware:/var/lib/egroupware:/
tmp:/usr/share/php:/usr/share/jpgraph
```

После этих настроек система перестанет выдавать сообщения о необходимости обновления программы jpgraph. Однако при построении диаграммы Ганта русский текст будет выводиться в виде знаков вопроса.

Описание исправления этой ошибки и необходимые файлы представлены на странице **http://nk-rec.narod.ru/samples/uprod/phpegroupware/**. Из-за различий версий не все операции по установке патча прошли на моем компьютере автоматически. Поэтому кратко приведу необходимые действия.

Скачайте файл патча и разархивируйте его. Вы получите пять файлов различий между оригинальными файлами и исправленными. Для внесения изменений в оригинальные файлы следует установить программу `patch` (`apt-get install patch`) и выполнить команды, приведенные в листинге 7.3.

Листинг 7.3

```
patch /usr/share/egroupware/projectmanager/inc/
class.projectmanager_admin.inc.php
class.projectmanager_admin.inc.php.diff

patch
/usr/share/egroupware/projectmanager/inc/class.projectmanager_ganttchart.
inc.php class.projectmanager_ganttchart.inc.php.diff

patch /usr/share/jpgraph/src/jpgraph_ttf.inc.php jpgraph_ttf.inc.php.diff

patch /usr/share/jpgraph/src/jpgraph_gantt.php jpgraph_gantt.php.diff

patch /usr/share/jpgraph/src/jpg-config.inc.php jpg-config.inc.php.diff
```

Замечание

В текущей папке при выполнении команд должны быть файлы *.diff.

В файлы, которые не удается отредактировать указанным способом, изменения нужно внести вручную по информации из файлов *.diff (знаками "–" отмечены удаляемые из исходного файла строки, знаками "+" — добавляемые). В итоге интерфейс диаграммы Ганта будет полностью локализован (рис. 7.12).

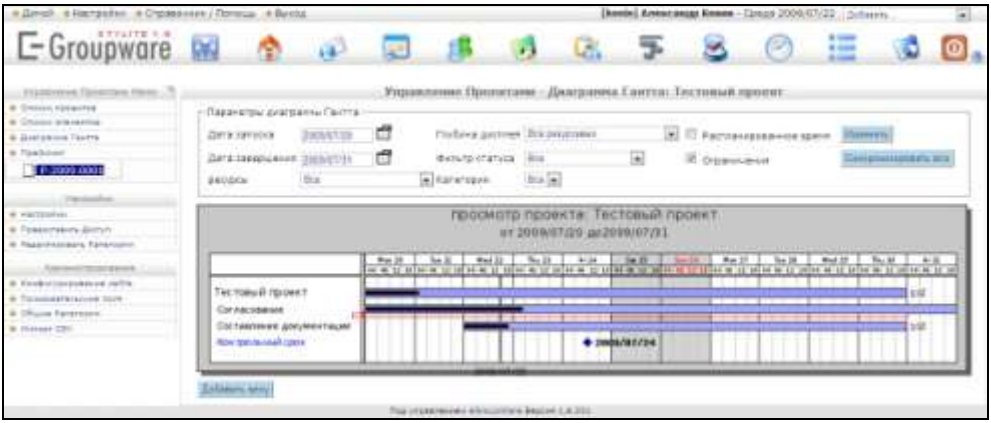


Рис. 7.12. Диаграмма Ганта, сформированная системой eGroupware

Установка служб Windows SharePoint Services

Службы Windows SharePoint Services входят в состав выпусков Windows Server 200*x* R2 и Windows Small Business Server. Если вы захотите обновить эти версии, то, особенно для выпуска Windows Small Business Server, необходима специальная подготовка операционной системы. Подробности ее описаны в статье **http://technet.microsoft.com/en-us/library/cc671966%28WS.10%29.aspx**. В составе версий Windows 200*x* Server служб Windows SharePoint Services нет, но их можно бесплатно загрузить по следующим ссылкам:

- для 32-битовых серверов — **http://go.microsoft.com/fwlink/?LinkId=105656;**
- для 64-битовых — **http://go.microsoft.com/fwlink/?LinkId=105802**.

Примечание

Windows SharePoint Services позволяют распределить нагрузку на несколько серверов, если выполнить установку *фермы*. В данной книге мы не будем рассматривать этот вариант, поскольку режимы установки отличаются несущественно и необходимые действия хорошо описаны в документации. Следует также учесть, что установка в режиме фермы предполагает наличие сервера баз данных, являющегося коммерческим продуктом.

Службы Windows SharePoint Services являются весьма "тяжелым" продуктом, для достижения приемлемой производительности необходимо устанавливать их на современный, не менее чем двухпроцессорный сервер с объемом оперативной памяти не менее 2 Гбайт и, желательно, с дисками, объединенными в RAID-массив. В противном случае задержки при выполнении операций сделают работу пользователей некомфортной.

До начала установки служб в системе следует включить роль Web-сервера и установить Microsoft .NET Framework 3.0 или Microsoft .NET Framework 3.5. Первый пакет можно включить как компонент Windows Server 2008, а второй следует загрузить по ссылке **http://go.microsoft.com/fwlink/?linkid=110508**.

> ***Примечание***
>
> На момент подготовки книги последней версией пакета был Microsoft .NET Framework 3.5 с интегрированным первым пакетом обновления. Кроме того, разработчик настоятельно рекомендует после установки Microsoft .NET Framework внести исправление KB959209, устраняющее ряд замеченных ошибок в работе.

Если в крупных организациях можно распределять различные функции служб SharePoint по нескольким серверам, то в малых и средних компаниях вся установка выполняется на один сервер. Если еще использовать для хранения данных бесплатную версию SQL-сервера, то такой вариант соответствует опции стандартной конфигурации мастера установки. В иных случаях следует выбирать установку только Web-компонентов SharePoint с последующим указанием параметров необходимых служб.

> ***Замечание***
>
> Если вы предполагаете оставить уже существующий SQL-сервер, то необходимо выбрать путь расширенной установки.

Если вы ставите службы SharePoint не в первый раз (например, ранее удалили службы и пытаетесь поставить их заново), то необходимо вручную удалить существующую базу до начала операций.

После ввода в ответ на запросы мастера необходимой информации будет проведена установка пакета и вам предложат открыть страницу по умолчанию для рабочей группы (рис. 7.13). Эта страница создана при установке служб SharePoint 3.0 автоматически. Она готова к работе, но для функционирования служб в полном объеме следует завершить операции настройки так, как описано в настоящей книге.

Несмотря на то, что вы увидели Web-страницу рабочей группы и можете уже выполнять с ней различные операции, настройка служб SharePoint еще не завершена. Во-первых, необходимо настроить параметры служб, а во-вторых, — добавить компоненты, которые могут расширить функциональность сервера.

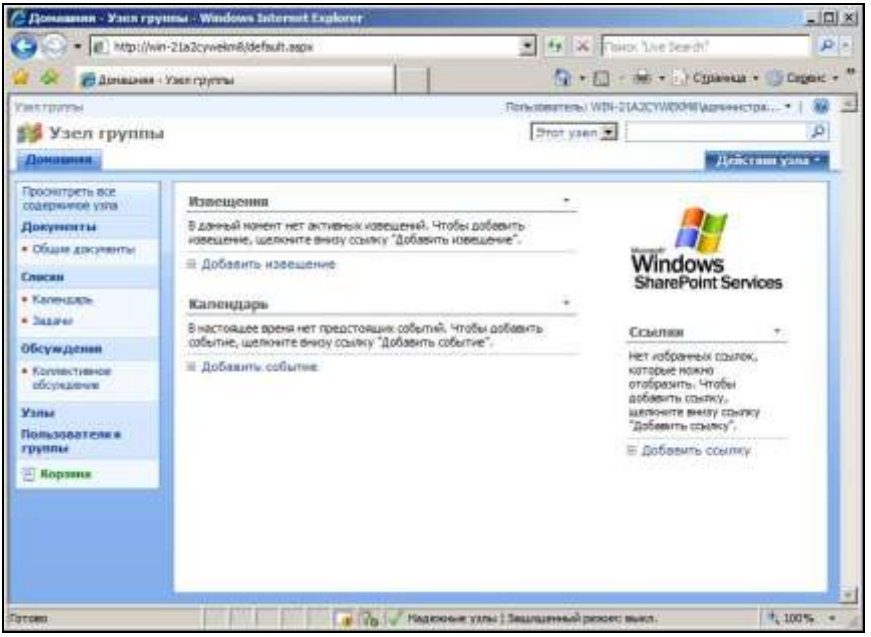


Рис. 7.13. Домашняя страница узла группы

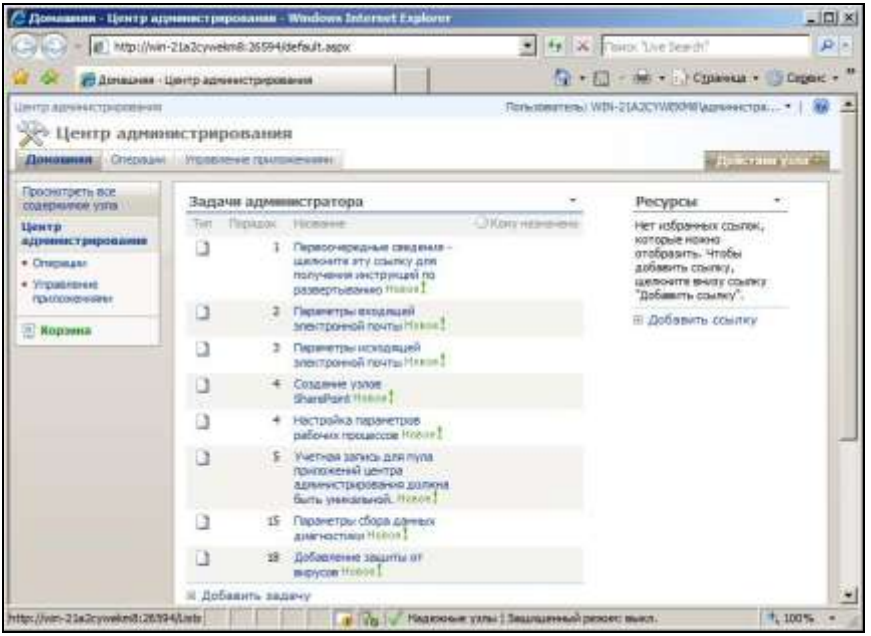


Рис. 7.14. Окно задачи администрирования служб SharePoint 3.0 при первом входе

После установки служб SharePoint в разделе **Административные задачи** появляются две ссылки: **Мастер настройки продуктов и технологий SharePoint** и **Центр администрирования SharePoint 3.0**. Первая ссылка — это вызов мастера настроек (того, что работал сразу после установки продукта). Единственное, ради чего стоит вызывать этот мастер, — это восстановление вашего узла SharePoint. Ситуация достаточно редкая, но возможная. Задача **Центр администрирования SharePoint 3.0** объединяет в себе административные операции над узлом и при первом посещении отображает список задач, которые должен выполнить администратор узла (рис. 7.14). Достаточно поочередно перейти по соответствующим ссылкам и настроить те параметры, о которых сообщает система. Каждая задача содержит подробное описание необходимых действий и ссылки для перехода к соответствующим интерфейсам управления.

> ***Примечание***
>
> Задача администрирования SharePoint включает возможность настройки многих дополнительных опций (например, создание нового пула приложений). Начиная работу с SharePoint, не стоит менять настройки по умолчанию для неизвестных вам опций.

Обычно на первом этапе администрирования служб следует сконфигурировать почтовый сервер, определиться с учетными записями администраторов и настроить параметры резервного копирования.

Установка дополнительных шаблонов SharePoint

Для служб SharePoint можно бесплатно загрузить и установить с **http://www.microsoft.com/downloads/details.aspx?familyid=AAE4CB5A-91D2-4F1B-9A45-3BB894E218F8&displaylang=ru** некоторые шаблоны, которые помогут быстро создать преднастроенные Web-узлы. В частности, пакет "*Шаблоны приложений Windows SharePoint Services 3.0*" добавляет следующие шаблоны:

- Управление запросами на отгулы и расписанием отпусков.
- Бюджетирование и отслеживание нескольких проектов.
- База данных ошибок.
- Центр обработки вызовов.
- Управление запросами на изменение.
- Узел поддержки процесса обеспечения соответствия.
- Управление контактами.
- Ревизия и библиотека документов.

- Планирование мероприятий.
- Утверждение и возмещение расходов.
- Служба поддержки.
- Отслеживание запасов.
- Рабочее место для группы ИТ.
- Управление объявлениями о вакансиях и интервью.
- База знаний.
- Библиотека сведений об аренде.
- Отслеживание и управление физическими активами.
- Рабочее место для отслеживания проекта.
- Заказ помещений и оборудования.
- Канал продаж.

Для установки этих шаблонов предварительно необходимо добавить шаблон "*Application Template Core*"

(http://www.microsoft.com/downloads/details.aspx?displaylang=ru&FamilyID=c1039e13-94da-4d7d-8cae-3b96fa5a4045).

Шаблоны устанавливает команда администрирования службами SharePoint `stsadm.exe`, которая расположена в папке %PROGRAMFILES%\common files\microsoft shared\Web server extensions\12\bin (для 32-битовой версии) или в папке %drive%\program files (x86)\common files\microsoft shared\Web server extensions\12\bin (для 64-битовой версии). Загруженные с сайта Microsoft файлы шаблонов представляют собой самораспаковывающиеся архивы. После их запуска в указанную вами папку добавляются файлы с расширением wsp. Там же создается файл с инструкциями по установке шаблонов.

Последовательность операций одинакова при установке любого шаблона. Необходимо добавить шаблон в библиотеку решений, после чего установить его и, в завершении, скопировать коды. Выполняются эти шаги командами, приведенными в листинге 7.4 (в примере указано имя базового шаблона, которое нужно заменить впоследствии на устанавливаемые шаблоны).

Листинг 7.4

```
stsadm -o addsolution -filename <путь>\ApplicationTemplateCore.wsp
stsadm -o deploysolution -name ApplicationTemplateCore.wsp
-allowgacdeployment -local
stsadm -o copyappbincontent
```

После установки шаблонов необходимо перезагрузить Web-сервер командой `iisreset`.

Архив шаблонов администрирования включает более 20 файлов. Для ускорения выполнения операций (если вы предполагаете установить все шаблоны) можно последовательно выполнить в консоли команды, которые обеспечат установку всех шаблонов из указанной папки (листинг 7.5).

Листинг 7.5

```
for %I in (<путь к файлам wsp>\*.wsp) do stsadm -o addsolution
-filename %I
for %I in (<путь к файлам wsp>\*.wsp) do stsadm -o deploysolution
-name %~nxI -allowgacdeployment -local
stsadm -o copyappbincontent
```

Для того чтобы создать новый узел на основе добавленных шаблонов, достаточно зайти на страницу SharePoint с правами администратора, открыть список **Действие узла** в правой верхней части страницы, выбрать вариант **Создание**, перейти по ссылке **Веб-страницы | Узлы и рабочие области**, заполнить необходимые опции на открывшейся странице и отметить нужный шаблон среди базы шаблонов (вкладка **Шаблоны приложений**).

После добавления желаемого количества узлов вы получите подготовленные формы для совместной работы.

Настройка страниц узла

Шаблоны фактически являются страницами узла с типовыми элементами, которые настроены для практических целей. Например, заменены заголовки списков, другие имена даны столбцам списков и т. п.

Подобную оптимизацию легко выполнить на любой странице. Зайдите на необходимую страницу с административными правами и перейдите в режим редактирования (нажатием на кнопку **Действия узла** в правом верхнем углу). В этом режиме можно как отредактировать параметры Web-частей, так и добавить на страницу новые элементы (рис. 7.15).

Примечание

В узел можно добавлять Web-части (*Web-part*). Некоторые из них доступны бесплатно в Сети. Однако в большинстве случаев для прикладных целей необходима разработка новых Web-частей. При отсутствии в штате компании специалистов, имеющих опыт программирования, соответствующие работы придется заказывать в специализирующихся компаниях.



Рис. 7.15. Добавление веб-частей на страницы узла SharePoint

Используйте возможности штатных элементов SharePoint

Входящие в состав SharePoint элементы обладают рядом интересных возможностей, на которые часто не обращают внимания, сохраняя настройки по умолчанию.

Так, библиотеки документов можно настроить на *версионность*. Иными словами, если какой-то документ, хранящийся на узле, будет изменен, то на сервере сохранятся как исходная копия, так и отредактированная версия. Это очень удобная функция, которая включается в свойствах библиотеки.

Другая возможность — наличие оповещений. При включении этой функции вы можете настроить получение сообщений по электронной почте в случае появления в библиотеке нового документа или изменении существующего. Таким способом очень удобно следить, например, за библиотекой нормативных документов в компании.

Узлы SharePoint создаются буквально одним щелчком мыши. Поэтому создать новый узел очень удобно, например, для подготовки конкретного совещания. На узле можно разместить обсуждаемые документы, список участников, перечень заданий (с отслеживанием состояния), организовать обсуждение (по типу онлайновых конференций) или опрос.

Установка поискового сервера по общим ресурсам

Поддерживать идеальную структуру хранения документов на практике невозможно. Поэтому функция поиска зачастую становится единственной возможностью быстро найти необходимый документ. При использовании служб Windows SharePoint Services можно легко добавить в среду совместной работы возможности поиска по сайтам SharePoint, файловым ресурсам общего доступа, Web-сайтам, общим папкам Exchange и сторонним репозиториям с помощью Microsoft Search Server 2008 Express.

Express-выпуск поискового сервера бесплатен, доступен к загрузке со страницы **http://www.microsoft.com/enterprisesearch/serverproducts/searchserverexpress/download.aspx**. Сервер можно установить вместе с существующими службами SharePoint, при этом возможен как вариант смены основного узла группы на поисковый интерфейс, так и установка поискового сервера в качестве нового узла с доступом по произвольному порту.

> ***Примечание***
>
> Добавление функции поискового сервера еще больше увеличивает нагрузку на компьютер. Обратите внимание, что полноценная работа возможна только при наличии в системе не менее 4 Гбайт оперативной памяти и современного многоядерного процессора.

Сайт поискового сервера нуждается в административной настройке. Для нормальной работы нужно указать, что индексировать, как (какой учетной записью, необходимость прокси-сервера) и когда (создать расписание). Кроме того, необходимо определить параметры электронной почты, поскольку они потребуются для создания оповещений.

Чтобы указать поисковому серверу, какие документы и где нужно индексировать, следует выполнить операцию **Добавление источника содержимого** (рис. 7.16).

В окне, показанном на рис. 7.16, необходимо указать пути к индексируемому ресурсу, особенности индексирования (например, просматривать документы только с этого сервера или индексировать на глубину до трех уровней вложения). На этой же странице определяются расписания, по которым сервер будет индексировать документы.

По умолчанию поисковый сервер использует учетную запись локальной системы. Эта запись не имеет прав доступа к сетевым ресурсам, поэтому в правилах обхода следует определить учетную запись для соответствующей области поиска.

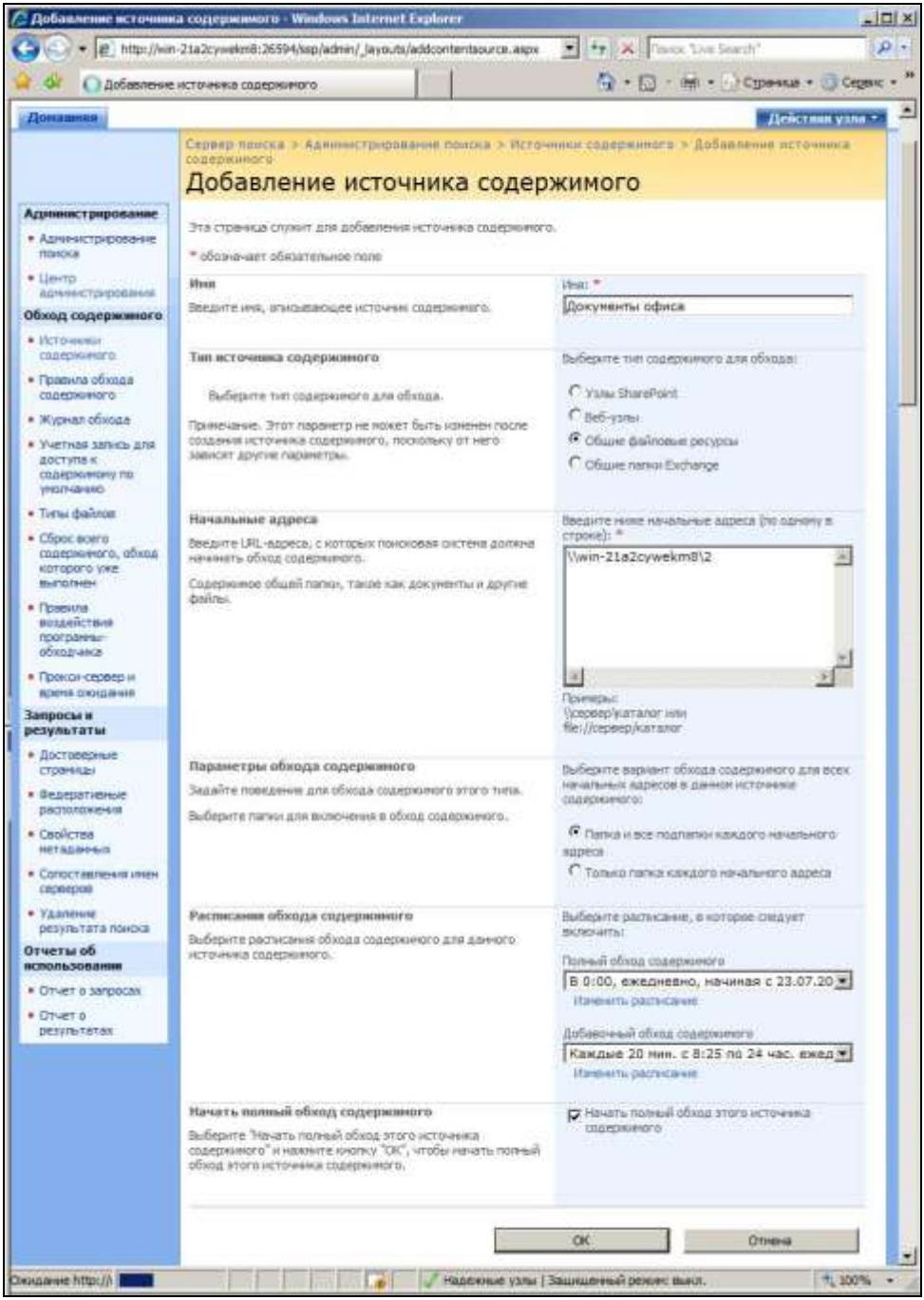


Рис. 7.16. Добавление источника содержимого к настройкам поискового сервера

Замечание

Можно сменить и учетную запись поискового сервера по умолчанию в соответствующем пункте навигационного меню.

Обратите внимание, что эта учетная запись должна иметь права для чтения файлов из области поиска, но желательно, чтобы эти права не были административными на удаленном сервере. При большом объеме индексируемых документов можно ограничить интенсивность операции через пункт меню **Правила воздействия программы-обходчика**.

После добавления областей поиска и запуска индексирования поисковый сервер готов к работе. Другие операции (например, резервное копирование, смену оформления страниц и т. п.) вы можете проделать в последующее время.

Настройка автоматических оповещений об изменениях документов на чужих серверах

В службах SharePoint, как уже говорилось, настраиваются оповещения по электронной почте об изменениях любого элемента (библиотеки, списка, документа и т. д.). Этот функционал позволяет с помощью поискового сервера наблюдать за различными Web-страницами (не только в локальной сети, но и в Интернете) и оповещать вас по электронной почте в случае их изменения. Так вы сможете следить за новостями по интересующим вас темам.

Для этого достаточно сформировать запрос, который будет показывать в качестве результатов документы с нужной вам страницы Интернета. При отображении результатов запроса в заголовке поискового сервера появляется пункт **Оповещать меня**. Если перейти по этой ссылке, то вы попадете на страницу настройки оповещений. Выберите наиболее подходящий вариант контроля и предоставьте серверу самостоятельно отслеживать изменения и сообщать об этом вам.

Глава 8



Обеспечение удаленной работы пользователей

Сегодня обеспечение работы мобильных пользователей становится едва ли не главной задачей администратора информационной системы. Пользователь должен из любого места получить доступ по сети Интернета к той информации организации, которая ему потребуется. Кроме того, создание филиалов компаний требует настройки их взаимодействия с информационной системой центрального офиса. При этом возникает еще одна, сугубо внутренняя, задача дистанционного управления оборудованием удаленного офиса.

Традиционные способы решения перечисленных задач:

- организацией удаленного доступа к почтовым ресурсам и порталу компании;
- настройкой терминального доступа;
- предоставлением пользователям прав доступа к внутренней сети по технологии VPN;
- настройкой транспорта между удаленными офисами (VLAN, VPN);
- внедрением технологий управления по сети Интернет (управление по отдельной сети, управление поверх IP).

Удаленный доступ к почте и порталу обычно реализуется по протоколу HTTP соответствующей настройкой межсетевого экрана. Описанные в этой книге почтовые системы (Microsoft Exchange, Zimbra Collaboration Suite) предоставляют доступ пользователей по этому протоколу, поэтому сложностей в реализации данного требования у администраторов обычно не возникает. Рассмотрим более подробно специфику выполнения оставшихся требований.

Терминальный доступ

Терминальный доступ обеспечивает работу пользователя на удаленной системе. Все вычисления производятся на мощном удаленном компьютере (его называют *терминальным сервером*), а пользовательский компьютер является

лишь локальной консолью. Данные и команды, которые пользователь вводит (с клавиатуры, мышью), передаются на терминальный сервер, где они обрабатываются, а пользователю возвращаются лишь графические изменения в интерфейсе. Иными словами, пользовательский компьютер практически использует только монитор, клавиатуру, мышь.

Терминальные решения существуют как для систем Windows (режим терминального сервера требует оплаты дополнительных лицензий), так и для Linux (существуют как проприетарные решения, например, SunRay от компании Sun Microsystems, так и бесплатные продукты — NX Server/Client).

Терминальные серверы от Microsoft

Серверы Windows включают в себя все необходимое для настройки терминального сервера. При этом включение режима терминального сервера возможно в двух вариантах. Один предназначен только для настройки системы администраторами сервера. Он называется подключением к удаленному рабочему столу, включается в свойствах сервера и разрешает одновременное функционирование до двух учетных записей администраторов. Терминальный режим позволяет подключить неограниченное количество пользователей (лимитируется только мощностью аппаратной части и числом лицензий), но требует приобретения дополнительных лицензий.

Для использования терминального сервера в локальной сети должен присутствовать сервер лицензий. Установка сервера лицензий производится через задачу **Установка и удаление программ** выбором соответствующей позиции. Сервер лицензий обязательно должен быть активизирован через сайт изготовителя. То же относится к клиентским лицензиям. Без активизации лицензий сервер создает временные лицензии, которые действуют в течение 90 дней.

> ***ЗАМЕЧАНИЕ***
>
> При необходимости администраторы легко найдут в Сети любые рекомендации по выполнению данной операции.

Постоянные лицензии "привязываются" к пользователям или компьютерам (в зависимости от приобретенного типа), но периодически обновляются (эта возможность присутствует с Windows 2000 SP3), чтобы восстановить лицензии, "отданные" компьютерам, которые уже больше не работают в сети (например, вышли из строя).

Установка самого терминального сервера не представляет сложности. Достаточно добавить соответствующий компонент (роль) системы.

Особенности установки ПО на сервере терминалов

Режим терминального сервера не предназначен для работы программ, вызывающих интенсивную нагрузку на процессор. Этот режим не рекомендуется для мультимедийных и аналогичных приложений. Такие задачи целесообразнее решать на локальных системах. Терминальный сервер предназначен прежде всего для "обычных" офисных программ.

Установка прикладных программ в режиме приложений подразумевает наличие специальных условий, которые реализуются автоматически при запуске установки через утилиту установки и удаления программ, расположенную в **Панели управления**. Этот режим автоматически включается при попытке запуска стандартных файлов установки (`setup.exe`), но в него можно перейти и вручную, если набрать в командной строке `change user /install`. А по завершении установки восстановить нормальный режим командой `change user /execute`.

После установки приложения имеет смысл проанализировать дополнения, внесенные в раздел `Run` реестра. Например, многие программы, инсталлируемые на терминал, выводят в системной области панели задач некие индикаторы. Так, антивирусная программа показывает наличие и состояние защиты на компьютере. В большинстве случаев такие индикаторы только отнимают лишние ресурсы системы и могут быть отключены в целях повышения производительности.

Некоторым программам могут понадобиться особые конфигурации установки для режима терминальных служб. Например, пакет MS Office XP невозможно установить без специального файла настроек, который следует загрузить с информационного сервера Microsoft.

> ***Замечание***
>
> Разработчики не гарантируют работоспособность всех прикладных программ на терминальном сервере в режиме приложений. Но за все время работы с терминальным сервером автору не приходилось встречаться с ситуацией, когда прикладная программа не работала в этих условиях.

Для корректной работы приложений в режиме терминального сервера должен выполняться ряд условий, прежде всего, отсутствие записи данных в каталоги самой программы или в четко прописанные папки жесткого диска. Понятно, что на практике можно встретить программу, которая будет некорректно работать в режиме терминала. Исправить подобную ситуацию призваны специальные сценарии, исполняемые при входе пользователя в систему.

По умолчанию при каждом входе в терминальную сессию исполняется сценарий USRLOGON.CMD, вызывающий, в свою очередь, несколько других

командных файлов. Если администратор не настраивал сценарии совместимости, то запуск этого сценария с настройками по умолчанию не производит каких-либо операций. Если программе необходима дополнительная подготовка окружения, то ее можно включить в подобный сценарий.

Замечание

Администратор может добавить свои файлы сценариев, выполняемых при входе в систему, откорректировав значение параметра `AppSetup` в ключе `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`.

Безопасность при работе с терминальным сервером

В Windows Server по умолчанию подключение к терминалу разрешено только администраторам и членам группы **Пользователи удаленного рабочего стола**. Поскольку эта группа первоначально пуста, то в нее нужно добавить соответствующих пользователей.

Второе место, где контролируется право работы в терминале, — это параметр учетной записи пользователя, разрешающий такое подключение. По умолчанию это право *включено* для каждой учетной записи. Но администраторы могут задействовать этот параметр для индивидуальных запретов или разрешений.

Данные, передаваемые по каналу связи, в режиме терминального доступа, шифруются. Существуют три уровня шифрования. Выбор степени стойкости осуществляет администратор терминального сервера, устанавливая соответствующие параметры соединения (через задачу настройки терминальных подключений в группе **Административные задачи**).

При подключении к терминальной сессии возможен также вход с помощью смарт-карты. Это существенно повышает безопасность работы в системе.

Администратор терминального сервера (точнее, тот пользователь, которому такое право дано протоколом RDP. По умолчанию это только администраторы терминального сервера. Но при необходимости данное значение можно изменить, воспользовавшись оснасткой управления параметрами RDP-протокола.) имеет возможность подключиться к пользовательской сессии и полностью видеть все, что делает пользователь. Данный режим обычно служит для оказания помощи пользователям сервера. Эта возможность включается через задачу управления терминальными сессиями. По умолчанию для подключения администратора система сначала запрашивает согласие пользователя. Но администратор может включить режим, при котором подключение будет происходить и без согласия пользователя.

Удаленные приложения

Часто пользователи подключаются к терминальному серверу для работы только в каком-либо конкретном приложении. Существуют специальные технологии публикации одного приложения, лидером таких решений являются продукты Citrix. Для терминалов Microsoft можно реализовать такие настройки подключения, которые внешне соответствуют подключению к одной задаче.

В версии терминальных серверов Windows 2000/2003 подобная настройка решалась просто. Достаточно в свойствах подключения на вкладке **Программы** указать параметры вызываемой задачи (рис. 8.1). Настройку запускаемого приложения администраторы обычно выполняли для бухгалтеров: подключение к терминальному серверу для них воспринималось просто как запуск программы 1С.

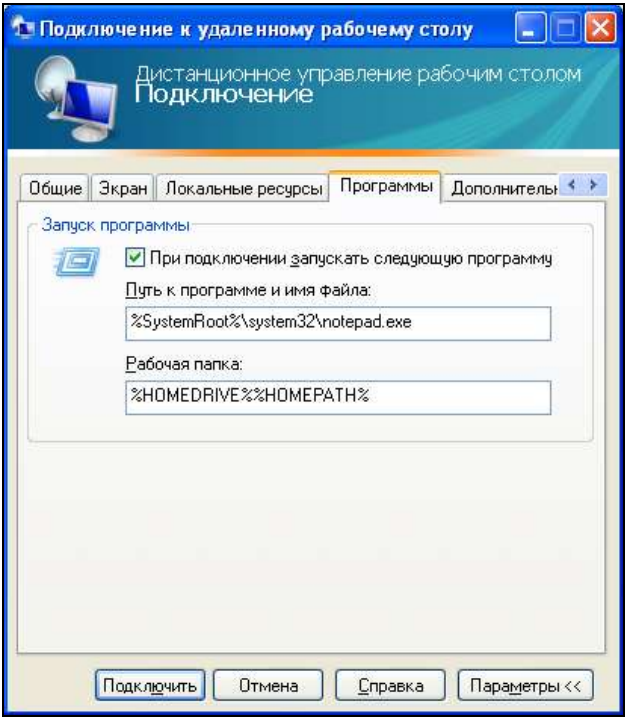


Рис. 8.1. Настройка запуска в терминальной сессии заданного приложения

После этого при подключении пользователя к терминальному серверу автоматически запускалось указанное приложение. Если пользователь завершал

работу в приложении, то вслед за его закрытием прерывалось и подключение к терминальному серверу.

С появлением новой версии протокола подключения к терминальному серверу возможность указания запускаемого приложения появилась не только на клиентской стороне, но и на сервере. При этом технология подключения не изменилась. При подключении пользователя также полностью формируется терминальная сессия и только после этого осуществляется запуск программы. Причем для клиентов, использующих предыдущую версию протокола (предыдущую версию программного обеспечения терминального клиента), будет просто открываться рабочий стол терминального сервера — параметры настройки подключаемого приложения игнорируются.

Удаленные приложения (RemoteApp) в Windows 2008 настраиваются через **Диспетчер удаленных приложений (RemoteApp) служб терминала** выбором опции **Добавить удаленное приложение** в правой панели навигации. После этого мастер проведет вас через все шаги назначения параметров удаленного приложения. Перечень всех приложений, настроенных для удаленного использования, доступен в нижней части окна оснастки (рис. 8.2). Данная оснастка позволяет из одного места настраивать основные параметры терминального сервера. Панель навигации в правой части окна отображает операции, доступные для каждого выделяемого объекта.

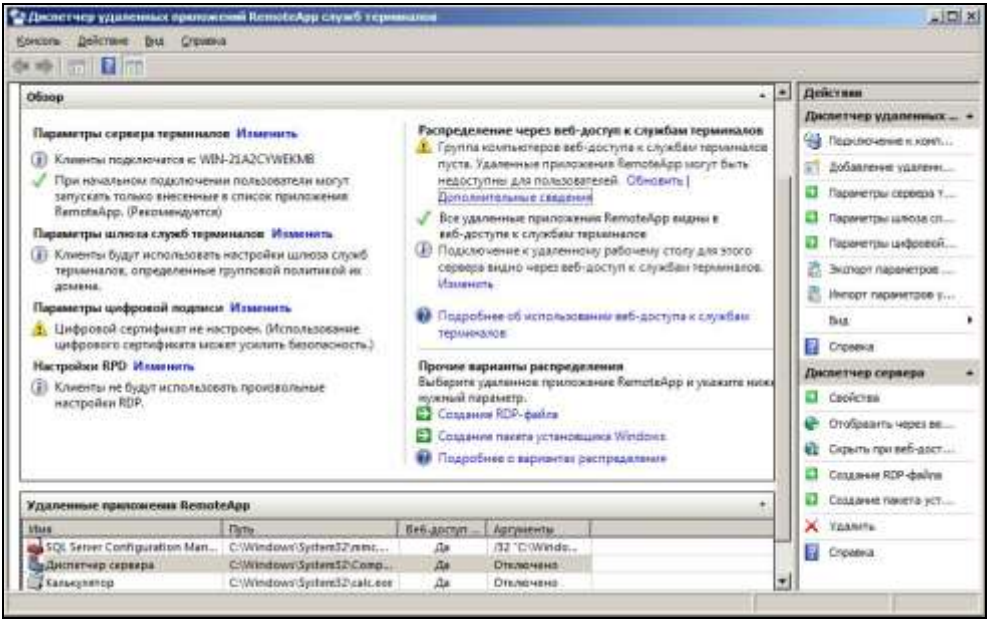


Рис. 8.2. Диспетчер удаленных подключений

Перенос настроек приложения в параметры подключения предоставил администраторам дополнительные возможности. Удаленное приложение стало возможным *публиковать* или устанавливать: достаточно любым средством (через групповые политики, с помощью специализированного ПО — System Management Server, Acronis и др., создавая файл установки msi и т. п.) предоставить пользователю файл настроек подключения. Более подробно способы публикации удаленных приложений описаны в онлайновой справке.

Web-доступ к терминальному серверу. Шлюз терминалов

Web-доступ к терминальному серверу появился в тот момент, когда программное обеспечение терминальных клиентов не устанавливалось по умолчанию на рабочих станциях Windows. Фактически это решение представляет собой ActiveX-модуль, автоматически устанавливаемый на локальный компьютер при обращении из обозревателя к терминальному серверу. Соответственно, работать можно только с Internet Explorer и требуются права и необходимые разрешающие настройки обозревателя для установки ActiveX. Реальное подключение к терминальной сессии осуществляется по протоколу RDP, что требует открытого порта 3389.

Web-доступ в версии Windows 2008 несколько изменился. Теперь на исходной странице публикуются не только ссылки на доступ к терминальной сессии, но и перечень опубликованных приложений (рис. 8.3).

По умолчанию Web-интерфейс доступен по пути **http://<*имя_сервера*>/ts**.

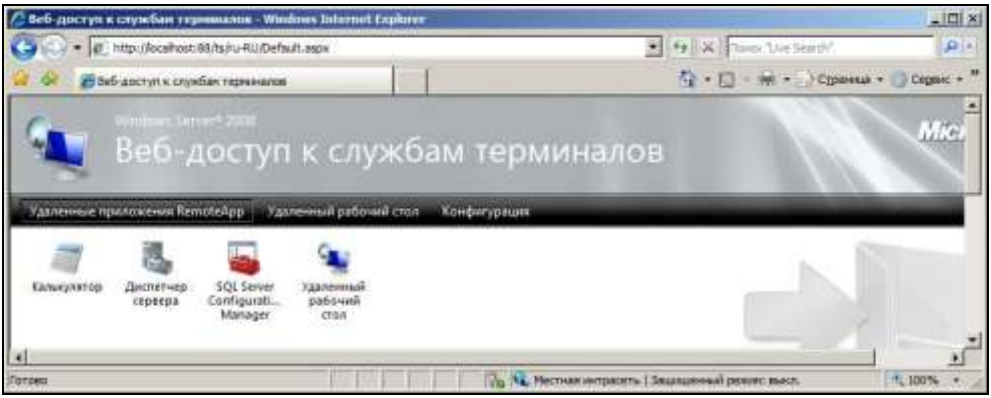


Рис. 8.3. Web-интерфейс терминального сервера

Web-интерфейс удобен для разового доступа к необходимому приложению не с компьютеров локальной сети. При постоянной работе рациональнее ссылку на такое приложение сохранить на локальном компьютере. Админи-

страторы могут настроить Web-интерфейс так, что на нем будут опубликованы приложения с различных терминальных серверов внутри организации. Но это, конечно, решение уже для крупных предприятий.

Отметим интересную новую возможность Windows 2008 Server — наличие шлюза терминалов. Шлюз терминалов позволяет публиковать в Интернет несколько внутренних терминальных серверов, подключение к которым производится в зависимости от устанавливаемых политик. И, главное, доступ к шлюзу, а потом к терминальному серверу, осуществляется клиентом по порту 443 — это порт протокола HTTPS, который обычно открыт в межсетевых экранах. Это расширяет возможности доступа к терминальным серверам из Интернета.

Настройка шлюза терминалов не представляет особой сложности, и мы не будем специально останавливаться на ней.

Некоторые особенности работы в режиме терминального доступа

Пользователь может подключать к терминальному серверу свои локальные ресурсы. Это позволит сохранять результаты работы непосредственно на локальный диск. Администратор должен разрешить или запретить возможность такой операции, исходя из принятых в организации правил.

Обычно пользователям разрешают подключать локальные принтеры. Драйвер принтера будет автоматически устанавливаться только при наличии цифровой подписи. В противном случае лучший выход — предварительная установка драйвера администратором сервера.

Поскольку терминальный сервер предоставляется многим пользователям, то администратору крайне важно сохранить его работоспособность, не давая пользователям устанавливать лишние программное обеспечение, менять настройки и т. д. Мы не будем останавливаться на описании возможных административных настроек, отметим только, что для терминального сервера очень развиты опции тюнинга через политики безопасности. В политиках безопасности можно установить практически любые ограничения. В Windows 2008 удобно ввести ограничения и через настройку удаленных приложений (включая опцию разрешения запуска только RemoteApp).

Одна из наиболее часто происходящих проблем на терминальном сервере — зависания заданий печати пользователей в различных сессиях. Для того чтобы удалить их, достаточно периодически выполнять следующий сценарий:

```
net stop spooler
del %systemroot%\system32\spool\printers\*.* /q
net start spooler
```

Подключение к консоли

Если вы работали за консолью сервера (вошли в систему локально с клавиатуры), а потом попытаетесь подключиться для удаленного управления, то по умолчанию будет создана новая сессия. Локальный экран терминального сервера будет недоступен. Это не всегда удобно для администраторов. Иногда необходимо увидеть сообщения, которые отображаются после старта системы (например, сообщения от системы контроля серверной платформой или предупреждения о неудачном запуске службы).

Для работы с экраном консоли нужно запустить клиент подключения к удаленному рабочему столу с ключом `/console`:

```
MSTSC /console
```

Кроме того, есть возможность переключиться в консольную сессию, уже работая в терминале. Среди команд терминала есть утилита `SHADOW`, позволяющая подключиться к любой терминальной сессии. А поскольку сессия консоли всегда имеет нулевой номер, то достаточно выполнить команду:

```
SHADOW 0
```

В отличие от запуска подключения с ключом — `MSTSC /console` — данная команда не сможет подключить к консоли, если с последней предварительно не был произведен вход в систему.

Командная строка управления терминальными сессиями

Ранее уже упоминались команды `change user`, `SHADOW`. Перечислю еще несколько команд, которые будут полезны администраторам для управления режимом терминальных служб. Подробности использования команд легко уточнить по справочной документации системы.

- `change logon` — разрешает или запрещает новые подключения пользователей к терминальному серверу. Программа полезна, если вы хотите временно, на период работ по настройке сервера, запретить пользователям создавать новые сессии.
- `query` — в числе прочего команда позволяет запросить список терминальных серверов организации, что вряд ли представляет особую ценность. Главное — команда показывает список текущих пользователей на сервере, идентификаторы их сессий. Эта информация полезна, если вы захотите отключить конкретного пользователя (например, в случае зависания его сессии) от терминала.
- `logoff` — завершает работу пользователя и удаляет его сессию. В параметрах команды нужно указать тот номер, который вы получили при запросе параметров пользователя командой `query`.

- `reset session` — в отличие от предыдущей команды завершает сеанс пользователя "силовыми методами". Полезно в случае зависших сеансов.
- `MSG` — позволяет послать сообщение пользователю терминальной сессии (конкретному или всем). Например, если вы выключаете сервер, то с помощью этой команды можно попросить пользователей завершить работу к заданному сроку.
- `TSPROF` — копирует профиль пользователя.
- `TSSHUTDN` — выключает (перезагружает) сервер.

Терминальные серверы в Linux

Linux-системы изначально являются многопользовательскими операционными системами и необходимости устанавливать какое-то дополнительное ПО, чтобы превратить их в терминальные серверы, нет.

Традиционно для работы в Linux используются консольные клиенты (командная строка). Выбор их многообразен и определяется только личными предпочтениями (*см. разд. "Работа в Ubuntu с компьютеров под управлением Windows"* далее в этой книге). Наиболее распространена программа VNC, входящая в каждый дистрибутив Linux. Чтобы включить доступ к серверу Linux, необходимо запустить на нем сервер VNC. После чего просмотр (подключение к рабочему столу) осуществляется с помощью VNC-клиента (существует в версиях для Windows, Linux, Solaris и др.).

Если пользователям необходимы дополнительные возможности, предоставляемые современными терминальными клиентами (например, копирование данных в сессии между серверов и клиентом), то можно применить современные разработки, например, версии NX NoMachine (страница загрузки **http://www.nomachine.com/download.php**, имеются бесплатные версии).

Можно отметить также решения SunRay (**http://www.sun.com/**), предоставляющие терминальный доступ как к серверам на основе Linux, так и Microsoft. В отличие от других продуктов, SunRay представляют собой комплекс из тонких клиентов (бездисковых станций) и специализированного программного обеспечения, устанавливаемого на серверы Solaris или Linux.

Технологии доставки виртуального рабочего стола

С развитием технологий виртуализации появилась возможность создания виртуальных систем не только для серверов, но и для рабочих станций. В этом случае для каждого рабочего места создается отдельная виртуальная машина.

Преимущество такого подхода по сравнению с терминальными режимами состоит в бóльших возможностях настройки параметров рабочих станций и управления их ресурсами. При этом созданы решения, позволяющие экономить ресурсы сервера, например, хранить типовые файлы различных рабочих станций (файлы операционных систем, программного обеспечения и т. д.) централизованно.

Однако на сегодня технологии доставки виртуального рабочего стола испытывают сложности, если:

- на рабочей станции требуется использовать технологии аппаратного ускорения (например, DirectX);
- необходима передача голосового трафика на рабочую станцию;
- требуется использование локально подключенного принтера;
- используются аппаратные ключи защиты ПО от копирования;
- необходимо использовать сканер, видеокамеру и другое оборудование, подключенное к рабочей станции.

Кроме того, до сих пор многие вопросы лицензирования в таких конфигурациях остаются неясными. Учитывая стоимость подобных решений, можно сделать вывод, что их применение в условиях небольшого предприятия является преждевременным.

Удаленное подключение пользователей к внутренней сети предприятия

Обеспечить доступ пользователей ко всем ресурсам внутренней сети предприятия можно на основе технологии VPN. В этом случае удаленный компьютер пользователя становится членом локальной сети предприятия.

Данные между компьютером пользователя и офисом по сети Интернета передаются безопасным образом (с применением шифрования). Возможные проблемы вызваны тем фактом, что специалисты офиса не контролируют подключаемый компьютер. Поэтому на нем могут быть вирусы или другое опасное программное обеспечение, средства, которые можно использовать для подготовки атаки на информационную систему предприятия и т. п. Несмотря на развитие технологий контроля доступа в сеть, обеспечить полную безопасность информационной системы со стороны пользовательского компьютера практически невозможно. Поэтому возможность подключения по VPN следует предоставить только администраторам систем (обычно необходимо для управления) и доверенным пользователям. Тем более что

к основным информационным ресурсам пользователи могут обратиться через терминальный доступ или порталы (в том числе, и к корпоративной почте).

Подключение по VPN можно создать на любой операционной системе.

Создание входящего VPN-подключения на рабочих станциях Windows

Входящие подключения по VPN можно настроить на рабочих станциях Windows 2000/XP/Vista.

Для создания входящего соединения в Windows 2000/XP следует запустить мастер создания новых подключений.

- В мастере создания новых подключений выберите вариант **Установить прямое подключение к другому компьютеру**.
- Отметьте, что соединение должно обрабатывать входящие соединения (опция **Принимать входящие подключения**).
- На вкладке о VPN-подключениях укажите, что вы хотите разрешить VPN-подключение, выберите пользователей, кому разрешено данное подключение.
- На вкладке программного обеспечения в меню определения свойств IP-протокола настройте опции подключения удаленных пользователей к локальной сети: либо только к данному компьютеру (снят флажок **Разрешить звонящим доступ к локальной сети**), либо разрешить подключение и к другим компьютерам локальной сети (флажок установлен). Также нужно определить параметры TCP/IP-протокола, которые будут использованы внешним клиентом.

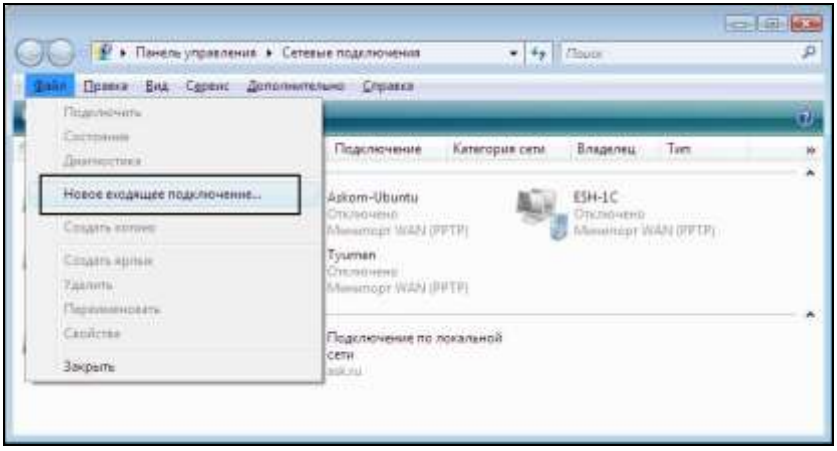


Рис. 8.4. Установка входящего подключения для Windows Vista

В Windows Vista операция создания входящего подключения несколько сложнее. Для ее выполнения вы должны перейти к задаче **Панель управления | Сетевые подключения** и *открыть ее меню* (нажать клавишу <Alt>). В этом меню в разделе **Файл** представлена опция создания нового входящего подключения (рис. 8.4). Дальнейшие операции выполняются ответами на запрос мастера и не вызывают никаких сложностей.

Создание входящих VPN-подключений на серверах Windows

VPN-доступ в серверных операционных системах реализуется **Службой маршрутизации и удаленного доступа** (RRAS). Администратору необходимо добавить столько портов для VPN-подключений, сколько потребуется в работе организации. Эта операция выполняется либо с помощью мастера настройки RRAS, либо вручную — простым добавлением нужного числа портов.

> ***Примечание***
>
> Обратите внимание, что удаленное подключение будет доступно только тем пользователям, которым политикой сервера маршрутизации и удаленного доступа разрешены *входящие звонки*.

Служба маршрутизации и удаленного доступа установлена в серверах Windows Server 2000/2003. В Windows 2008 эту службу необходимо установить путем добавления роли **Службы политики сети и доступа.** При добавлении роли следует выбрать в ее составе в списке **Службы маршрутизации и удаленного доступа.**

Служба маршрутизации на серверах по умолчанию отключена до момента ее настройки, которая запускается при первом открытии оснастки управления.

Для того чтобы сервер смог принимать входящие VPN-подключения, достаточно в мастере настройки выбрать соответствующую опцию (или при ручной настройке — добавить необходимое число портов подключения).

Безопасное объединение локальных сетей офисов

Существуют несколько вариантов объединения локальных сетей офисов в единую сеть. Сети офиса можно соединить:

- с использованием технологии, аналогичной VLAN;
- подключением по протоколу PPTP;

- подключением по протоколу L2TP;
- подключением по протоколу IPSEC.

Последние два варианта отличаются, скорее, терминологически, но мы сохраним такую структуру, поскольку в мастере подключений офисов в программе Microsoft ISA Server применено именно такое название.

Офисы можно подключить как с помощью возможностей коммутационного оборудования (в этом случае процессорные мощности для поддержания соединения использоваться не будут), так и программными средствами. Лучший вариант — организовать соединение средствами оборудования, но не каждая организация имеет в наличии соответствующие модели коммутаторов (маршрутизаторов) или может их приобрести. Надежно и быстро работают маршрутизаторы на основе Linux-систем. Мы опишем далее подробно их настройки при установке на обычный компьютер. И самым ненадежным, обычно и недешевым (если учесть стоимость программного обеспечения и всех необходимых лицензий) является программная реализация на базе серверов Windows. Хотя этот вариант наиболее распространен в небольших структурах в силу доминирующего положения операционной системы Windows.

На практике наиболее распространен вариант организации связи между офисами на основе протокола PPTP в силу исторических причин. Преимущества L2TP и ipsec в том, что они исходно разрабатывались для коммутационного оборудования и могут быть реализованы специальными аппаратными модулями.

Подключение офисов предусматривает не только двустороннюю организацию канала связи между локальными сетями, но и последующую настройку маршрутизации подключенных сетей.

Подключение офисов по VLAN

Современные модели коммутаторов имеют возможность "пробрасывания" VLAN по сети Интернета. Это самый простой способ объединения офисов. Провайдер просто предоставляет вам параметры IP-адреса, а вы настраиваете необходимую маршрутизацию.

Технология (MPLS) позволяет назначать пакетам конечные точки маршрута, что обеспечивает доставку данных, например, из одного диапазона локальных адресов в другой. Функционал обеспечивается исключительно средствами оборудования сети передачи данных, поэтому он доступен только для тех офисов, которые подключены к совместимому оборудованию. К сожалению, это выполняется лишь в крупных городах и далеко не у всех провайдеров.

Преимущества данной технологии, кроме простоты создания соединения двух частных сетей, состоит в обеспечении заданного качества обслуживания: прежде всего, такой канал может обеспечить гарантированную полосу пропускания от точки входа до точки выхода.

Минусы технологии, кроме упомянутой малодоступности на сегодняшний день, в том, что пакеты данных передаются через глобальные сети в незашифрованном виде. Это потенциально позволяет легко прослушивать такой трафик. Кроме того, провайдеры обычно берут за данную услугу арендную плату, что ограничивает ее доступность для некрупных организаций.

Подключение удаленных офисов с использованием VPN-серверов Windows

Подобный вариант подключения в Windows носит название *интерфейса по требованию* (dial-in-интерфейса).

Создание интерфейса по требованию осуществляет мастер. Достаточно выбрать в меню **Службы маршрутизации и удаленного доступа** опцию создания нового интерфейса по требованию, дать ему имя, указать параметры учетной записи, с помощью которых будет осуществляться подключение к другому серверу, и ввести параметры удаленной сети (для создания статической маршрутизации).

Система различает подключение удаленного пользователя от подключения интерфейса по требованию *только по имени пользователя,* выполняющего эту попытку. Поэтому при настройке подключений двух сетей *имя* подключающегося *пользователя должно совпадать с названием интерфейса*. Иными словами, на сервере с интерфейсом по требованию с именем `Int1` должен быть указан пользователь `Int2` для подключения к удаленному интерфейсу по требованию с именем `Int2`, а на другом сервере — `Int1`.

> ***Примечания***
>
> В Windows Server 2003 параметры статической маршрутизации интерфейса по требованию вводятся в процессе работы мастера создания интерфейса.
>
> В Windows 2000 после создания интерфейса по требованию в RRAS необходимо задать вручную статические маршруты, которые будут включаться при подсоединении этого интерфейса. Для этого выделите заголовок **Static Route**, вызовите команду создания статических маршрутов, выберите интерфейс по требованию и введите параметры удаленной сети. Эту операцию следует выполнить с обеих сторон канала связи офисов.

В качестве учетных записей, используемых в интерфейсах по требованию, целесообразно применять только локальных пользователей, чтобы не зави-

сеть от доступности контроллера домена (если сеть построена по доменному варианту).

Другие настройки подключений интерфейсов по требованию (должно ли соединение инициироваться сервером или ему следует только ожидать попытки подключения, время "простоя", после которого можно разъединять связь, или необходимость постоянного соединения и т. п.) достаточно очевидны и легко настраиваются через консоль управления **Службой маршрутизации и удаленного доступа**. Состояние соединений контролируется оснасткой службы (рис. 8.5).

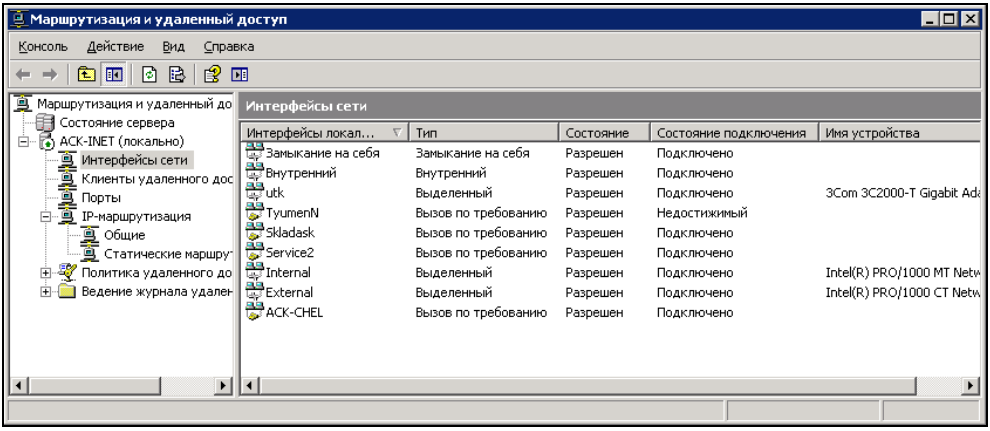


Рис. 8.5. Окно программы маршрутизации и удаленного доступа Windows 2003 Server

Фильтрация VPN-трафика

Для создания связи между офисами необходимо с обеих сторон установить VPN-серверы. Хорошо, если ваши маршрутизаторы поддерживают такую возможность. Обычно дешевые модели шлюзов для подключения к Интернету не могут выступать в роли VPN-сервера, их можно настроить только на пропуск шифрованного трафика до какой-либо системы внутри сети. Опишем протоколы, которые необходимо настроить в таком случае для нормальной работы VPN-сервера внутри периметра организации.

❒ Для подключения к VPN-серверу по протоколу PPTP следует разрешить:

- IP-протокол на порт 1723 (это разрешает передачу управляющего трафика PPTP);
- IP-протокол с идентификатором 47 (разрешение передачи данных по PPTP);

- IP-протокол на порт 1723 в варианте **TCP [established]** (настройка нужна в случае, если инициатором соединения выступает сам VPN-сервер).

Не забывайте, что необходимо разрешить прохождение как *входных* пакетов, так и соответствующих симметричных *выходных*.

- ❐ При подключении к VPN-серверу по протоколу L2TP необходимо разрешить:
  - пакеты на UDP-порт номер 500;
  - прохождение протокола с идентификатором 50;
  - пакеты на UDP-порт номер 1701.

Как и в предыдущем примере, фильтры должны быть настроены симметрично для входных и выходных пакетов.

В случае разрыва канала при доменной организации офиса...

Удаленные офисы небольших предприятий обычно укомплектованы всего лишь несколькими компьютерами. Достаточно часто качество канала связи с центральным офисом (Интернетом) оставляет желать лучшего. В результате при обрыве связи удаленные пользователи теряют возможность доступа не только к ресурсам головного офиса, но и к локальным (документы, хранимые в папках совместного доступа на компьютерах других сотрудников филиала, локальный принтер и т. п.), если для доступа к ресурсам применяются *доменные учетные записи*.

Существуют несколько возможных путей решения данной проблемы. Первый — это создание на удаленных компьютерах локальных учетных записей, совпадающих по имени с доменными и имеющими тот же пароль, что в домене. Тогда при обрыве связи и недоступности контроллера домена доступ к ресурсам на других компьютерах будет осуществляться по *локальным учетным записям*. Недостаток этого варианта состоит в том, что необходимо постоянно синхронизовать учетные записи домена и локальных компьютеров в случае смены паролей пользователей.

Второй путь — размещение таких ресурсов филиала (общие папки, принтер) на *терминальном сервере*. Поскольку в новых версиях Windows существует кэширование параметров последних входов пользователя, то при обрыве связи пользователь сможет войти на терминальный сервер *без наличия подключения к контроллеру домена*, используя параметры последнего входа, хранимые в кэше. Однако подключиться к совместным папкам на других компьютерах будет невозможно.

Третий путь заключается в установке в филиале контроллера домена. До выхода сервера Windows 2008 такой способ был опасен тем, что в филиалах сложно обеспечить физическую безопасность контроллеров. А при доступе злоумышленника к контроллеру возможен легкий доступ ко всем паролям организации. В Windows 2008 появилась возможность создания контроллера домена только для чтения, на котором хранится только тот набор учетных записей, который определен администратором.

Read-only domain controllers

Read-only domain controllers (RODC) — контроллеры домена только для чтения, появились с выходом серверов Windows 2008. Эти контроллеры хранят только копии для чтения разделов службы каталогов и копии SYSVOL. На них можно организовать хранение паролей для выбранных учетных записей, что дает возможность продолжать работу при потере связи с головным офисом. В случае дискредитации такого контроллера (например, несанкционированного доступа к нему посторонних лиц) соответствующие учетные записи легко заблокировать и заставить сменить пароль (предусмотрена специальная операция в оснастке — рис. 8.6).

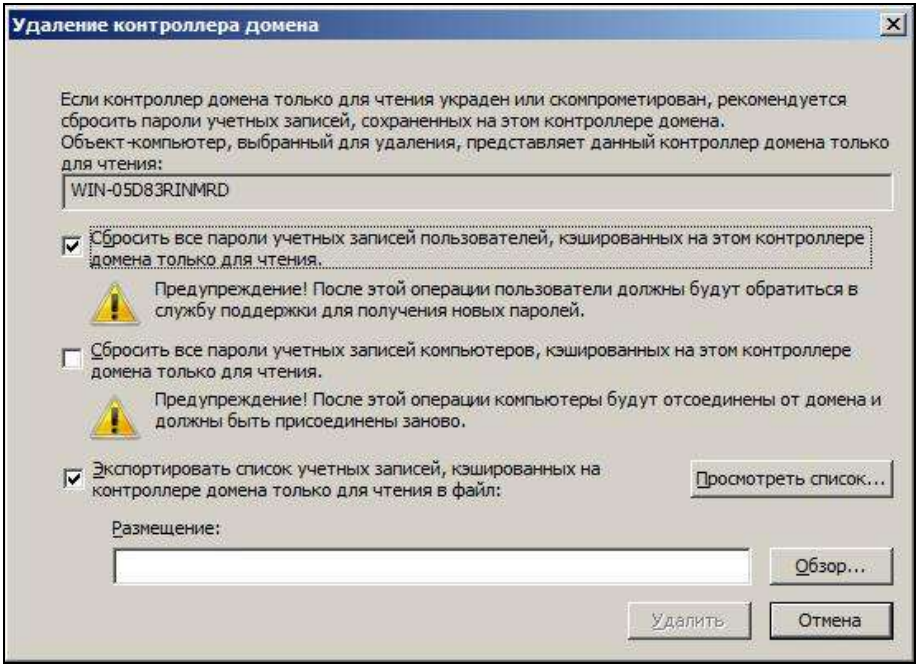


Рис. 8.6. Удаление учетной записи скомпрометированного контроллера домена

Если RODC скомпрометирован, то достаточно выполнить операцию его удаления в оснастке **AD – пользователи компьютеры**. Мастер операций сразу же предложит вам сбросить все пароли учетных записей, которые были реплицированы на этот сервер.

RODC можно установить в домене, который обслуживается контроллерами на основе серверов Windows 2003. Для этого необходимо лишь добавить схему в службу каталогов и установить RODC в филиал на основе операционной системы Windows 2008.

Дополнение схемы службы каталогов выполняется один раз на любом контроллере домена. Выполните следующую команду (утилита adprep находится на установочном диске сервера Windows 2008, обычно это папка /sources/adprep):

```
adprep /rodcprep
```

> ***ПРИМЕЧАНИЕ***
>
> Клиенты с операционными системами Windows XP, Windows 2003 Server, Windows Vista (без пакета обновления) имеют проблемы совместимости с RODC. На них необходимо установить исправление, описанное в KB944043 (**http://go.microsoft.com/fwlink/?LinkId=120375**). Для клиентов с операционными системами Windows 2000 на момент выпуска книги такого обновления еще не существовало.

Настройку RODC следует начинать с создания учетной записи предполагаемого контроллера домена с помощью оснастки **Active Directory – пользователи и компьютеры**.

> ***ПРИМЕЧАНИЕ***
>
> Сервер, которому предполагается предоставить роль RDOC, не должен быть включен в состав домена.

Откройте ее, перейдите к контейнеру **Domain Controllers** и выполните (из динамического меню) операцию **Создать заранее учетную запись контроллера домена только для чтения...**. После ответов на вопросы мастера операции в контейнере должен появиться значок, отображающий будущий RODC (рис. 8.7).

Обратите внимание, что вы можете делегировать установку контроллера любому пользователю: достаточно указать его параметры мастеру операции. При этом доступа этого пользователя к защищаемой информации в домене не будет. Определите для создаваемого RODC политику хранения паролей — укажите, для каких ученых записей пароли могут храниться на этой системе (рис. 8.8).

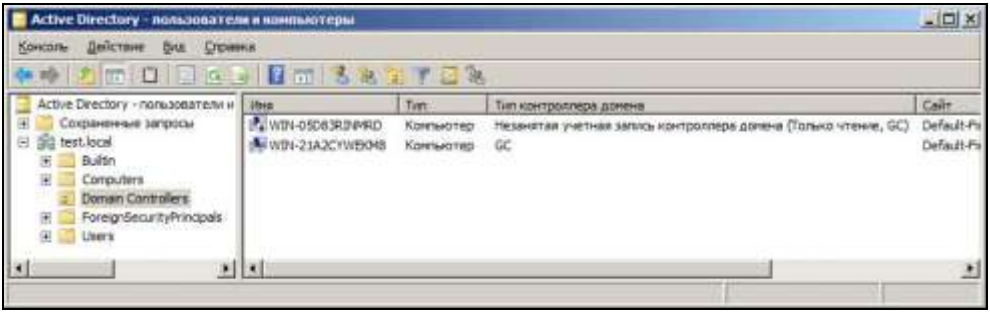


Рис. 8.7. Объект RODC в оснастке управления

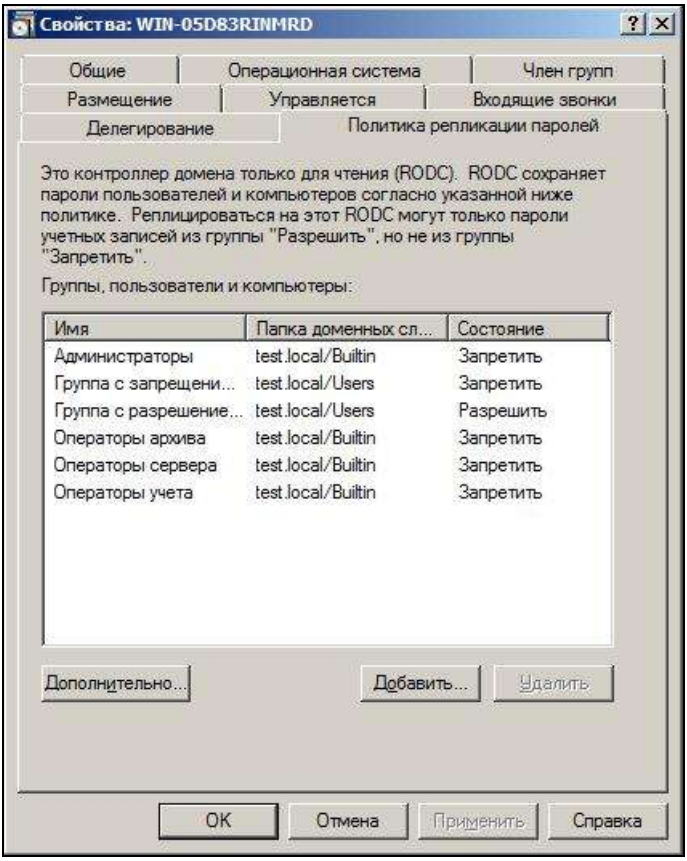


Рис. 8.8. Настройка политики хранения паролей RODC

Если вновь создаваемый RODC будет подключен по медленному каналу связи, то для ускорения его ввода в эксплуатацию и снижения первоначального объема трафика репликации, данные с существующего контроллера домена можно перенести на сменном носителе. Для Windows 2003 Server для этого нужно было сделать штатными средствами резервную копию контроллера домена и восстановить ее в другую папку на новом сервере. После чего мастеру операций указать на расположение этой папки (мастер должен быть запущен в расширенном режиме — `/adv`). Однако такая копия содержит в себе, в том числе, и пароли пользователей, которые не должны попасть в удаленный офис. Поэтому в Windows 2008 появилась специальная команда, которая готовит для переноса только минимальный объем данных.

Это новая функция утилиты `ntdsutil`. Запустите ее и в консоли введите последовательно:

```
activate instance ntds
ifm
Create rodc <путь_к_папке_с_носителем>
```

В результате в папку, указанную в команде, будут скопированы данные, необходимые для установки RODC.

> ***Примечание***
>
> Эта же команда позволяет переносить данные при создании полнофункционального контроллера. В этом случае последней командой должна быть строка `Create Full <путь_к_папке_с_носителем>`.

Подключение удаленного сервера в качестве RODC осуществляется либо с использованием графической оснастки `dcpromo`, либо в режиме командной строки (если сервер установлен в варианте только ядра). Если при работе мастера операций графического режима сложностей обычно не возникает, то в режиме командной строки необходимо правильно сформировать все параметры. Для этого можно либо заранее подготовить файл ответов, на который указать команде `dcpromo`, либо ввести все параметры в строке запуска. Полный перечень параметров, доступных при запуске `dcpromo`, указан на странице **http://technet.microsoft.com/en-us/library/cc733048%28WS.10%29.aspx**. Неиспользуемые параметры можно опустить, обычно достаточно ограничиться следующей строкой:

```
dcpromo /UseExistingAccount:Attach /replicaDomainDNSName:test.local
/safeModeAdminPassword:пароль /UserDomain:TEST
/UserName:TEST\Администратор /Password:пароль
```

После выполнения этой команды и перезагрузки вы получите новый контроллер домена только для чтения.

Замечание

Если параметр не указан, то будут определены значения по умолчанию. Например, при отсутствии указания об установке DNS, команда установит на систему DNS и настроит сетевой интерфейс на использование локального DNS в качестве сервера имен. А если в числе параметров, например, не будет задан пароль пользователя, то операция завершится ошибкой с сообщением о неудачном подключении к контроллеру домена.

Подключение удаленных офисов с использованием ПО Microsoft ISA Server

Если ваша организация использует для доступа в Интернет сервер Microsoft ISA, то в этом случае соединение двух сетей производится с помощью мастера операций после вызова опции установки подключения офиса к офису (Create VPN Site-to-Site connection, рис. 8.9).

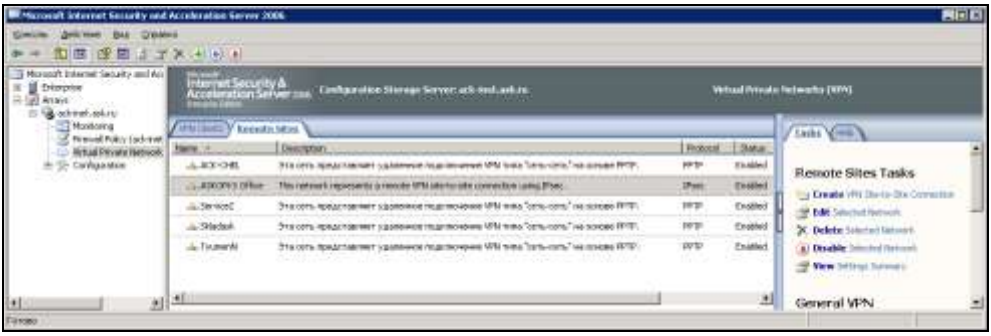


Рис. 8.9. Управление подключениями офис-офис в Microsoft ISA Server

После завершения работы мастера остается только настроить правила фильтрации пакетов из одной сети в другую. Кроме того, не забывайте, что должны быть установлены отношения маршрутизации между сетями различных офисов.

Подключение удаленных офисов с помощью VPN-серверов Ubuntu

VPN-сервер очень легко настраивается в Ubuntu. Сам сервер VPN устанавливается командой

```
sudo apt-get install pptpd
```

Параметры настройки сервера по умолчанию обеспечивают подключение клиентов VPN, в том числе и с компьютеров под управлением операционных систем Microsoft Windows. Единственное, что нужно указать, — это описать

IP-адреса сервера (его самого и диапазон адресов, предоставляемых клиентам) и добавить параметры учетных записей, которым разрешено подключение. Для настройки VPN-сервера откройте файл /etc/pptpd.conf. Укажите адрес сервера и диапазон адресов для клиентов:

```
localip 192.168.0.1
remoteip 192.168.0.200-250,192.168.0.252
```

> ***ПРИМЕЧАНИЕ***
>
> Настройки по умолчанию предполагают возможность одновременного подключения до 100 клиентов. Если диапазон выделенных IP-адресов меньше, то число клиентов будет ограничено этим значением. При необходимости подключения более 100 клиентов, эту настройку необходимо осуществить для VPN-сервера.

Для VPN-клиентов с операционных систем MS Windows желательно также указать получаемые ими параметры DNS-сервера и WINS-сервера (при наличии). Эта настройка осуществляется в файле /etc/ppp/pptpd-options в строках

```
ms-dns 10.0.0.1
ms-wins 10.0.0.2
```

Учетные записи, которые должны быть использованы для подключения, нужно указать в файле /etc/ppp/chap-secrets по следующему образцу:

```
user pptpd password *
```

В этом примере "`*`" означает, что клиент при подключении получит адрес из указанного в настройках сервера диапазона. Если клиенту нужно предоставить определенный адрес, то вместо "`*`" укажите его значение (или диапазон адресов, например, 192.168.0.0/24).

После выполнения этих настроек перестартуйте сервер:

```
/etc/init.d/pptpd restart
```

Для того чтобы клиенты могли подключаться к вашему серверу, необходимо также создать разрешающие правила для межсетевого экрана (открыть порт 1723 и разрешить протокол GRE):

```
iptables -A INPUT -p gre -j ACCEPT
iptables -A INPUT -m tcp -p tcp --dport 1723 -j ACCEPT
```

В рабочей среде следует разрешать подключения *только* с определенных адресов, поэтому приведенные примеры правил iptables нужно конкретизировать.

Чтобы компьютеры из одной сети, подключенной по VPN к другой, могли достигать компьютеров в другой сети, необходимо настроить маршрутизацию (или NAT с помощью iptables). Для этого вы должны знать, какие диа-

пазоны IP-адресов задействованы в подключаемой сети. Кроме того, после подключения вам необходимо настроить правила фильтрации трафика (iptables).

В реальных условиях могут требоваться несколько VPN-подключений, осуществляемых независимо и в произвольное время. В этой ситуации для создания правил необходимо знать, какое подключение выполняется. В табл. 8.1 приведен перечень переменных при выполнении сценариев PPP-подключения, позволяющих получить информацию о том подключении, которое выполнено в текущий момент (полный список переменных см. в файле /etc/ppp/ip-up).

Таблица 8.1. *Список переменных для PPP-подключения*

Переменная	Описание
PPP_LOCAL	IP-адрес, получаемый от VPN-сервера, к которому осуществляется подключение, либо IP-адрес локального VPN-сервера (если регистрируется входящее подключение)
PPP_IPPARAM	Название туннеля при исходящем подключении либо IP-адрес клиента, который подключается к локальному VPN-серверу
PPP_REMOTE	Адрес удаленного VPN-сервера (при исходящем подключении) или адрес, который получил удаленный клиент при входящем VPN-подключении
PPP_IFACE	Имя интерфейса (подключаемого или отключаемого)

В листинге 8.1 приведен пример сценария подключения.

Листинг 8.1

```
#!/bin/sh
case "$PPP_IPPARAM" in
    my_provider)
        route add default dev $PPP_IFACE
        ;;
    1.2.3.4)
        route add -net 192.168.10.0 netmask 255.255.255.0 dev
$PPP_IFACE
        iptables --insert INPUT 1 \
           --source 192.168.10.0/24 \
```

```
            --destination 0.0.0.0/0.0.0.0 \
            --jump ACCEPT --in-interface ${IFNAME}
        ;;
    *)
        echo "No PPP_IPPARAM defined"
        ;;
esac
```

При подключении `my_provider` мы добавляем маршрут по умолчанию через установленное соединение, при подключении с внешнего адреса 1.2.3.4 добавляем в таблицу маршрутизации маршрут на подключаемую сеть и разрешаем с нее получение пакетов. Понятно, что набор этих команд вы должны определить на основе своих потребностей.

Сценарии, которые выполняются при установлении соединения, нужно сохранить в папке /etc/ppp/ip-up.d/. Соответственно, сценарий удаления маршрутов следует сохранить в папке /etc/ppp/if-down.d/. Не забудьте после сохранения сценариев предоставить на созданные файлы права выполнения:

```
chmod +x /etc/ppp/ip-up.d/имя_файла
```

Подключение "офис - офис" на основе технологии SSH

Для UNIX-систем более удобно настроить подключение к сети офиса (или соединить сети двух офисов) на основе технологии SSH. Описываемый далее вариант подключения легко настроить с одного рабочего места, имея только возможность удаленного подключения к другому офису для своей учетной записи.

По опыту работы SSH-подключение обеспечивает большую надежность связи, поэтому именно этот вариант следует выбирать при использовании в качестве шлюзов Linux-систем.

Опишем, как настроить связь по зашифрованному каналу с применением технологии SSH между двумя офисами.

> ***Замечание***
>
> Мы приводим описание настройки подключения с помощью пакета OpenSSH, который устанавливается в Ubuntu (версию можно уточнить командой `ssh -V`). При подключении к системам с SSH2 необходимо конвертировать ключи ssh2 в формат OpenSSH. Соответствующие рекомендации легко найти в Интернете.

Для этого нужно:

- настроить SSH для использования ключей, чтобы при подключении не возникала необходимость ручного ввода пароля;
- настроить туннель между офисами.

Рассмотрим последовательно эти операции.

Для использования ключей вместо паролей предварительно нужно их сгенерировать. Для этого служит утилита ssh-keygen. Согласитесь на все запросы команды с параметрами по умолчанию, в том числе не указывайте пароль доступа к ключу. Это позволит впоследствии осуществить аутентификацию по ключу в автоматическом режиме.

> ***Примечание***
>
> Ключи доступа часто применяют для аутентификации на удаленных компьютерах. Обычно один и тот же ключ служит для входа на многие системы. Поэтому необходимо предотвратить возможность его появления в чужих руках. Для этого следует указать при генерации достаточно сложный пароль, что потребует обязательного знания секретной фразы при попытке применения ключа. Данный пароль будет запрошен только один раз и будет храниться в памяти системы до завершения сессии. Поэтому целесообразно создавать не один ключ. (Безопаснее создавать отдельные ключи для различных подключений к удаленным серверам, если предполагается наличие нескольких туннелей.) Первый ключ может быть применен для образования туннеля к конкретной системе, при этом он должен быть создан без пароля. Второй, который будет вводить администратор для личной аутентификации, следует защитить сложной парольной фразой. Для этого достаточно при генерации пароля указать различные имена ключей в каждом случае, а при использовании ключей явно указывать пути соответствующего файла.

При выполнении команды вы увидите текст листинга 8.2 (в этом примере `имя` условно обозначает название учетной записи пользователя).

Листинг 8.2

```
ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/имя/.ssh/id_rsa):
Created directory '/home/имя/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/имя/.ssh/id_rsa.
Your public key has been saved in /home/имя/.ssh/id_rsa.pub.
The key fingerprint is:
97:e0:13:c3:ea:00:c8:5b:15:c0:33:70:c3:24:71:32 имя@сервер
```

В результате выполнения этой команды создана пара файлов: публичный ключ (если вы не указывали свое имя) — /home/имя/.ssh/id_rsa.pub и персональный ключ — /home/имя/.ssh/id_rsa. Далее в примерах мы будем предполагать, что вы создали ключи с именем *my_tunnel*.

На созданные файлы (точнее, на открытый ключ) необходимо назначить права, предотвращающие их использование другими учетными записями. В противном случае при попытке выполнения команды с указанием ключа вы получите предупреждение и отказ в выполнении команды:

```
chmod 600 /root/.ssh/my_tunnel.pub
```

Для того чтобы на удаленный компьютер можно было зайти по протоколу SSH без ввода пароля, публичный ключ необходимо скопировать на него и добавить содержимое файла ключа в файл /home/имя/.ssh/authorized_keys. Проще всего это сделать с помощью имеющегося сценария `ssh-copy-id`:

```
ssh-copy-id -i ~/.ssh/my_tunnel.pub удаленный_сервер
```

В этом варианте ключ будет установлен в папку суперпользователя. Если вы хотите получить подключение с правами иной учетной записи, то укажите название сервера как `имя_пользователя@имя_сервера`. Программа запросит пароль доступа к удаленному серверу и выполнит операцию по добавлению данных ключа в файл authorized_keys профиля суперпользователя.

> ***Примечание***
>
> Первый вход на удаленную систему происходит достаточно долго. Целесообразно вначале просто подключиться к серверу по протоколу SSH и подтвердить доверие.

Теперь настройки для подключения без паролей выполнены. Чтобы подключиться к удаленному серверу, достаточно предоставить ему созданный таким образом ключ. Сделать это можно двумя способами.

Если вы подключаетесь вручную, то следует загрузить специального агента, который будет предоставлять идентификационные данные. В пакетном режиме достаточно явно указать в параметрах команды SSH путь к идентификационному файлу.

Для загрузки агента выполните следующие две команды:

```
ssh-agent $SHELL
ssh-add
```

Вторая команда, запущенная без параметров, добавляет ключи, расположенные в папке по умолчанию. При ее выполнении необходимо указать введенный при создании ключа пароль (если таковой был назначен). Проверить загрузку ключей можно командой `ssh-add -L`.

В пакетных режимах допустим синтаксис с явным указанием пути к публичному ключу учетной записи, что предотвратит просьбы ввода пароля:

```
ssh -i /root/.ssh/my_tunnel имя_сервера
```

> ***ВНИМАНИЕ***
>
> Обратите внимание, что в этой команде указывается только имя ключа, без ввода расширения.

Для успешной аутентификации по ключам на удаленном сервере должна быть разрешена эта опция. По умолчанию в Ubuntu она отключена. Для ее включения необходимо на сервере раскомментировать строку AuthorizedKeysFile в файле /etc/ssh/sshd_config. Кроме того, в конфигурации SSH необходимо включить опцию, разрешающую создавать каналы. Для этого добавьте в файл /etc/ssh/sshd_config строку

```
PermitTunnel yes
```

и перестартуйте SSH (/etc/init.d/ssh restart).

> ***ЗАМЕЧАНИЕ***
>
> Можно более безопасно настроить конфигурацию SSH, разрешив вход учетной записи суперпользователя только для создания туннелей и явно настроив разрешенные к выполнению операции. Это потребует некоторых ручных операций редактирования конфигурации, которые описаны, например, в http://www.debian-administration.org/articles/539.

Канал между двумя системами создается следующей командой:

```
ssh -f -w 0:0 -i /root/.ssh/my_tunnel имя_сервера true
```

В этой команде параметр `-f` определяет запуск команды в фоновом режиме, параметр `-w` указывает номера создаваемых туннелей. Номера выдаются, начиная с нуля, так что в примере показано создание первого туннеля; если туннель уже существует на одной из систем, то номер нужно увеличить (например, `-w 0:1`).

После образования туннеля нужно создать его сетевые интерфейсы как на клиенте, так и на сервере и настроить маршрутизацию. Интерфейсы туннеля должны иметь свои IP-адреса из отдельной подсети. Выберите любую подсеть, которая не задействована в вашей структуре, и присвойте ее адреса интерфейсу туннеля с одной стороны и с другой.

Например, на клиенте:

```
ifconfig tun0 10.0.0.1 10.0.0.2 netmask 255.255.255.252
```

И на сервере:

```
ifconfig tun0 10.0.0.2 10.0.0.1 netmask 255.255.255.252
```

Обратите внимание, что адреса на клиенте и на сервере указаны в разном порядке (сначала "свой", потом адрес интерфейса с другой стороны).

Чтобы через созданный туннель осуществлялась связь между сетями, необходимо добавить маршруты в сеть удаленного офиса через созданные интерфейсы и разрешить прием пакетов на него в межсетевом экране, например, так:

на клиенте:

```
route add -net 192.168.10.0 netmask 255.255.255.0 gw 10.0.0.2
iptables -A INPUT -i tun0 -j ACCEPT
```

на сервере:

```
route add -net 192.168.20.0 netmask 255.255.255.0 gw 10.0.0.1
iptables -A INPUT -i tun0 -j ACCEPT
```

На этом настройка туннелей завершена. Проверьте достижимость сетей удаленного офиса, например, командой `ping`.

Для автоматического создания туннелей при запуске системы соответствующие команды можно добавить в /etc/network/interfaces. При этом лучше добавить в команду установки туннеля опции поддержания его в активном состоянии и включение так называемого мастер-режима, позволяющего совместно использовать данное подключение. Поскольку соединение инициируется только с одной стороны и протокол SSH позволяет выполнить на удаленном сервере необходимые команды, то конфигурацию интерфейса можно осуществить только на клиенте так, как показано в листинге 8.3.

Листинг 8.3

```
auto tun0
iface tun0 inet static
pre-up ssh -i /root/.ssh/my_tunnel -S /var/run/my_tunnel.pid -M -f -
w 0:0 -o 'TCPKeepAlive yes' имя_сервера true
       pre-up  sleep 5
       address 10.10.10.1
       pointopoint 10.10.10.2
       netmask 255.255.255.252
       up route add -net 192.168.10.0/24 gw 10.10.10.2 tun0
       up ssh -i /root/.ssh/my_tunnel имя_сервера ifconfig tun0
10.10.10.1 10.10.10.2 netmask 255.255.255.252
       up ssh -i /root/.ssh/my_tunnel route add -net 192.168.10.0/24
gw 10.10.10.1 tun0
     post-down ssh -S /var/run/my_tunnel.pid -O exit имя_сервера
     post-down ssh -i /root/.ssh/my_tunnel имя_сервера ifconfig tun0 down
       post-down ssh -i /root/.ssh/my_tunnel имя_сервера route del -
net 192.168.10.0/24
```

Примечание

В примере опущены команды создания и удаления правил межсетевого экрана. При наличии запрещающей политики по умолчанию вам необходимо добавить разрешающие правила для туннелей.

Применение Ubuntu для маршрутизации в сети филиалов

Достаточно сложно настроить маршрутизацию клиентов удаленного доступа, подключаемых к межсетевым экранам на основе Microsoft ISA, к компьютерам сетей филиалов, подключенных по технологиям "сеть – сеть" с использованием указанного сервера. В этом случае помочь сможет маршрутизация, которую легко настроить с помощью Linux.

Предположим, что необходимо обеспечить доступ к рабочему столу компьютера сети филиала. Добавьте в правила межсетевого экрана на Ubuntu всего две строки:

```
iptables -A PREROUTING -i eth0 -p tcp --dport 3390 -d
локальный_адрес -j DNAT --to-destination удаленный_компьютер:3389 -t
nat
```

```
iptables -A POSTROUTING -i eth0 -p tcp --dport 3389 -d
удаленный_компьютер -j SNAT -to  локальный_адрес -t nat
```

Первая команда обеспечивает пересылку входных пакетов на порт 3390 на адрес удаленного компьютера на порт 3389. Вторая команда преобразует пакеты так, как будто они отсылаются самим компьютером (если бы этой команды не было, то ответные пакеты высылались бы удаленным компьютером на исходный адрес и терялись бы; указанная команда включает для нужных нам пакетов функцию NAT).

Управление оборудованием по сети Интернет

Администратор должен иметь возможность выполнить в удаленном офисе любые операции, в том числе и восстановить работоспособность "зависшей" системы, иметь возможность установить операционную систему "с нуля", используя локальный дистрибутив и т. п. Подобные ситуации хотя и встречаются не столь часто в обыденной работе, могут принести существенные убытки компании из-за остановки в обслуживании.

Существует несколько вариантов решения таких проблем.

Intelligent Platform Management Interface

Современные серверы поддерживают внешнее управление по спецификации IPMI (Intelligent Platform Management Interface). Обычно серверные платформы имеют специально выделенный порт для такого управления, но некоторые модели могут использовать одно сетевое подключение как для нормальной работы, так и для управления.

> ***ЗАМЕЧАНИЕ***
>
> В этом случае в подсистеме управления сетевой интерфейс независим от основного: имеет свой MAC-адрес и параметры настройки IP-протокола.

Если сервер не имеет такого порта, то в некоторых случаях в него можно добавить специальный модуль, который будет реализовывать эту функциональность (возможность следует уточнить по документации).

Мониторинг и управление через порт IPMI может осуществляться даже при зависании операционной системы. Главное, чтобы сохранялась доступность порта по сети передачи данных. Именно поэтому в серьезных проектах для подсистемы управления и мониторинга создают выделенную сеть, а такой вариант контроля называют *out-of-band management*.

Подключение к серверу для удаленного администрирования можно осуществить и через последовательный порт (обычно через модем). Это вариант для самого критического случая, когда все другие возможности связи с сервером потеряны.

> ***ЗАМЕЧАНИЕ***
>
> Модем позволяет подключиться к серверу даже при полном отказе инфраструктуры. Стоимость же данного решения (модем плюс один внутренний номер на АТС предприятия) весьма невысока.

Для управления через порт IPMI предусмотрены специальные программы. Обычно консоли управления реализуются в виде Web-интерфейсов с подключением по безопасному каналу (HTTPS). Кроме того, через этот порт можно обычно управлять и в режиме командной строки, и по SNMP-протоколу.

Данный вариант управления дает возможность администратору:

- удаленно включать, выключать и перезагружать сервер независимо от состояния операционной системы;
- обновлять BIOS;

- просматривать состояние сервера (температуру, уровни напряжения, состояние датчиков, установленных на сервере), в том числе, автоматически получать по сети оповещения о событиях в работе системы;
- подключать к серверу локальные CD/DVD или их образы.

В качестве примера на рис. 8.10 представлен интерфейс удаленного управления сервером Sun.

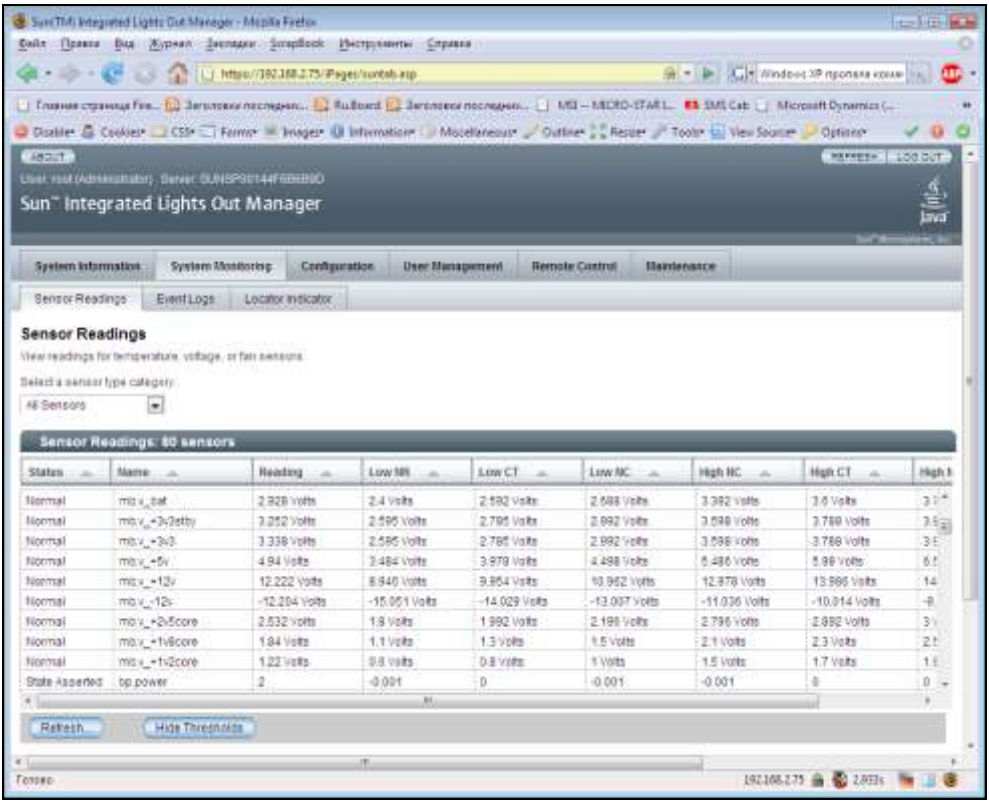


Рис. 8.10. Удаленное управление серверной платформой

На рис. 8.10 показано одно из окон программы удаленного управления серверной платформой — Integrated Lights Out Manager. Программа представляет собой Java-приложение и позволяет удаленно по безопасному каналу (HTTPS) контролировать работу сервера. В число возможностей программы входят мониторинг сенсоров платформы (на рисунке), управление электропитанием (в том числе присутствует функция как корректного выключения

с сохранением данных средствами операционной системы, так и простое отключение питания), удаленный контроль системы. Вы имеете также возможность подключить к серверу удаленный CD-ROM, гибкий диск или их образы.

Управление оборудованием по сети IP

Устройства, которые не снабжены возможностью независимого управления (подобно описанной технологии IMPI), также могут стать причиной отказа информационной системы. Для их удаленного обслуживания можно использовать KVM-переключатели с управлением по сети IP, а также удаленно управляемые распределители питания.

KVM с управлением по сети IP представляют собой переключатели клавиатуры, мыши и монитора, которые обеспечивают передачу нажатий клавиш и движений мышью по сети IP и отображение монитора удаленного компьютера на локальной системе. Иными словами, вы можете сидеть за своим компьютером, подключиться к удаленной системе через сеть Интернета, выполнять любые действия клавиатурой и мышью и видеть, что происходит на экране чужой системы (в том числе и в моменты ее перезагрузки).

Существуют различные модели, рассчитанные как на одно устройство (для управления несколькими системами нужно подключить KVM-переключатель), так и сразу на несколько. Современные модели могут подключать к удаленной системе не только клавиатуру и мышь, но и устройства USB. В этом случае к удаленному компьютеру можно подключить и флэш-память, и DVD-ROM и обеспечить с него загрузку компьютера.

Управление такими коммутаторами производится либо через обозреватель, либо при помощи специальной программы по защищенному каналу.

Понятно, что таким способом не всегда можно перезагрузить удаленный компьютер — кнопка "Reset" такими устройствами не поддерживается. Поэтому для особо важных случаев можно применить распределители питания с управлением по сети. При этом можно отключить питание с конкретной розетки и потом снова включить его, решив таким образом проблему холодной перезагрузки системы.

Мы не приводим описания конкретных моделей. Выпускаются они несколькими вендорами, и необходимую информацию легко найти в Интернете.

Утилиты удаленного управления Windows

Хотя для Windows присутствует возможность удаленного подключения к рабочему столу, на практике администраторы часто прибегают к программам сторонних разработчиков. Отметим некоторые, наиболее распространенные продукты.

- VNC (Virtual Network Computing, **www.realvnc.com**) — позволяет удаленно просматривать любые платформы (UNIX, Win32, Mac, мобильные клиенты и т. п.). Это кросс-платформенное приложение, имеется вариант на Java, который позволяет управлять рабочим столом из любого обозревателя Интернета.

  Коды программы открыты с 1998 года; пользователи загрузили более 20 млн ее копий. Программа включена в состав популярной операционной системы Linux. По данным ее сайта, VNC используют все компании, входящие в список Fortune 500.

  Технологию VNC используют многие пакеты, предназначенные для администрирования Windows-сетей.

- Hidden Administrator (**www.hidadmin.ru**) — бесплатная программа российского автора. Подобно другим программам она обеспечивает полный доступ к ресурсам удаленного компьютера, предоставляет администратору возможности скрытого наблюдения и управления, обмена файлами и т. п. Отметим также наличие опции удаленного включения системы (Wake on LAN).

  Замечание

  Следует учитывать, что часть антивирусных программ рассматривает утилиты удаленного управления в качестве вредоносного кода. Например, антивирус Касперского таковыми считает Hidden Administrator и Remote Administrator.

- Remote Administrator (RAdmin) — еще одна популярная программа удаленного управления для платформы Windows. Она также позволяет работать одновременно с несколькими удаленными компьютерами с помощью обычного графического интерфейса. Учитывая, что эта задача разработана для Win32, она реализует методы аутентификации пользователей, принятые в Windows.

  Программа позволяет осуществить копирование файлов на управляемый компьютер, поэтому ее достаточно часто применяют для управления Windows-серверами в Интернете.



Глава 9

Мониторинг информационной системы

Зачем нужен мониторинг

Большинство начинающих системных администраторов обычно сопровождают несколько небольших информационных систем (сервер плюс до десятка рабочих станций) и слабо представляют, зачем нужны системы мониторинга.

Мониторинг компьютеров и сетевых устройств дает возможность:

- Узнавать о неисправностях не от руководства или рассерженных пользователей, а от системы контроля. Это позволяет получить некоторый запас времени на поиск причин ошибок и восстановление работы, а в некоторых случаях пользователи могут даже и не узнать о том, что система какой-то промежуток времени была частично неработоспособной.
- Для повторяющихся ситуаций системы мониторинга позволяют настроить автоматическое реагирование на возникающие события. В результате неисправность можно устранить сразу после ее возникновения, не влияя на работу сотрудников предприятия.
- Мониторинг систем часто способен *предупредить* отказ той или иной службы. Простейший пример: контроль за свободным пространством на жестких дисках может предотвратить отказ, вызванный нехваткой места для записи новой информации. Таких "предсказывающих" параметров существует достаточно много, и они активно используются в сценариях мониторинга.

Это лишь несколько примеров, свидетельствующих о крайней желательности реализации возможностей систем мониторинга.

В то же время нужно четко представлять, что системы мониторинга могут предупреждать только о тех ошибках, для контроля которых они *настроены*. Например, если в системе есть RAID-массив, а программное управление

им отсутствует, то вы не будете предупреждены, например, об отказе одного из дисков в массиве.

Поэтому никакая система мониторинга не сможет заменить квалифицированного системного администратора, она в состоянии только избавить его от рутинных операций.

Системы мониторинга

Контролировать состояние информационной системы можно различными способами, причем в случае необходимости можно обойтись "подручными" средствами (*см. разд. "Контроль журналов Windows"* далее в этой главе). Учитывая, что любой контроль — это анализ возвращаемых сценариями наблюдения данных, простую систему для ограниченных целей нетрудно собрать на основе образцов скриптов из Интернета.

Существующие системы мониторинга позволяют не изобретать велосипед, а воспользоваться уже готовыми проработками. В сообществе присутствует много разработок для мониторинга информационных систем как небольших организаций, так и крупных предприятий с многочисленными филиалами. Комплексные системы управления, такие как HP Open View, Tivoli и аналогичные, практически не доступны, прежде всего, по экономическим соображениям, средним и даже многим крупным предприятиям нашей страны. Поэтому особое внимание привлекают продукты, либо приемлемые по цене для большинства заказчиков, либо полностью бесплатные (построенные на основе Open Source). Среди таких систем можно выделить Microsoft System Control Center (коммерческий продукт для мониторинга систем на основе Windows) и Nagios (бесплатное решение, работающее практически со всем спектром систем).

Многие вендоры выпустили специальные версии систем мониторинга, предназначенные для небольших организаций. Эти версии либо отличаются крайне низкой стоимостью, либо вообще бесплатны. Например, OpManager (**http://www.manageengine.com/products/opmanager/download.html**), который может контролировать бесплатно до 10 систем (серверов Windows и Linux, активное сетевое оборудование).

Кроме собственно контроля состояния систем, пакеты мониторинга имеют развитые возможности отображения данных в виде тех или иных графиков или отчетов, предполагают участие в контроле различных категорий пользователей с разделением обязанностей и т. п. В общем, ведут себя как большие серьезные информационные системы.

Принципы мониторинга систем

Контролировать систему можно несколькими способами. Во-первых, можно проверять реакцию служб на внешние запросы, например, ответ почтового сервера при подключении по одному из почтовых протоколов или результаты запроса какой-либо информации с сервера баз данных. Такой способ не требует "вмешательства" в контролируемые системы, но предполагает достаточную интеллектуальность программы, которая должна смоделировать все правила общения с удаленной службой и проанализировать ответ (естественно, что простейшие методы контроля, например, проверку достижимости систем командой `ping`, можно реализовать очень просто). Понятно, что возможности контроля ограничены тем функционалом, который доступен извне контролируемой системы.

Второй способ предполагает установку на контролируемую систему некоторой программы (ее принято называть *агентом*), который либо самостоятельно выполняет проверки по заданному графику, либо обеспечивает выполнение задания контроля, получаемого с сервера. Результаты проверки агентом возвращаются на сервер мониторинга. При данном способе контроля наблюдению доступны практически любые параметры как оборудования, так и программной среды. Недостатки этого способа — необходимость предварительной установки агентов, затраты производительности на исполнение агентов (ресурсы отнимаются от основных задач, для которых и установлен сервер). В зависимости от числа проверок, их частоты, производительности контролируемой системы и т. п. накладные затраты могут достигать величины 3–5% и более.

Контроль журналов Windows

Операционная система постоянно фиксирует состояние выполнения тех или иных операций в *журналах*. На практике записи в журналах являются для администратора "первой ласточкой", предупреждающей о неполадках в работе. Однако при увеличении числа обслуживаемых администратором систем своевременно прочитывать информацию журналов на всех компьютерах у администратора не хватает времени.

В этом случае требуются специальные возможности оснастки просмотра журналов, которые появились, начиная с Windows Vista и Windows 2008.

Во-первых, администратор может создать собственное представление в журнале, в котором он будет отображать только интересующие его события. Например, только сообщения об ошибках. При этом возможности фильтрации

при создании такого представления обычно покрывают все потребности администраторов (рис. 9.1).

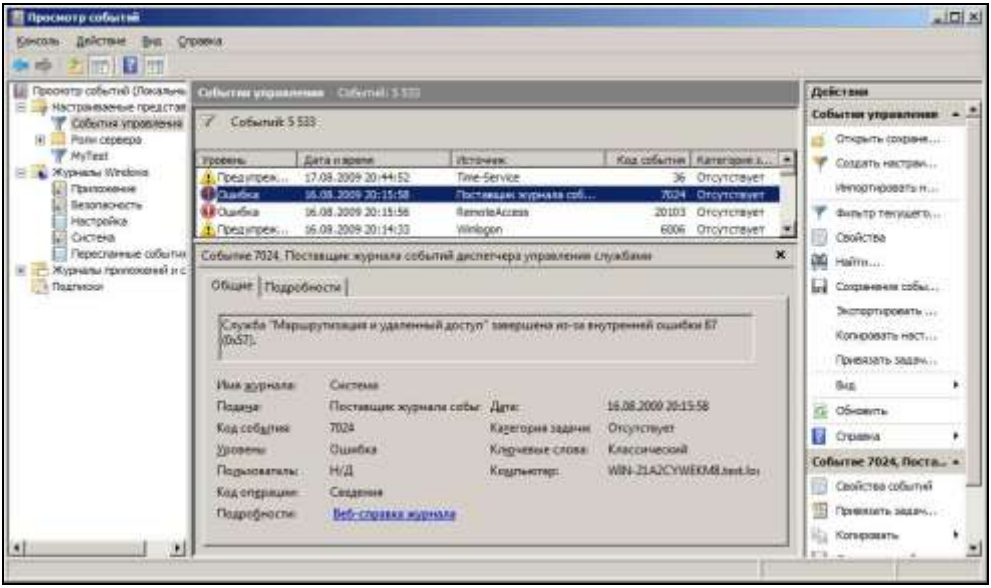


Рис. 9.1. Окно программы просмотра журнала событий

На рис. 9.1 показан вариант настраиваемого представления, существующего по умолчанию, где отображаются сообщения об ошибках, содержащиеся во всех журналах данного компьютера. Для создания нового представления достаточно выбрать соответствующий пункт из динамического меню оснастки и настроить правила, в соответствии с которыми будут отбираться события для отображения в журнале.

Во-вторых, оснастка просмотра события позволяет собирать сообщения и с других компьютеров. Для этого достаточно настроить *подписку*: указать правила сбора сообщений, определить компьютеры, с которых ведется сбор данных и т. д. Обычно все собранные таким образом сообщения направляют в журнал **Пересланные события**, который можно использовать при создании собственных настраиваемых сообщений.

В серверах Windows 2000/2003 подобная функциональность в оснастке просмотра событий отсутствует. Но вы можете воспользоваться бесплатной утилитой EventCombMT из состава Resource Kit для сбора событий с нескольких систем. Утилита входит в состав Account Lockouts Tools (см. KB824209) и позволяет собирать события с учетом фильтрации по номеру (точное сов-

падение, диапазон номеров и т. п.), по источнику события, по тексту сообщения, по времени события и т. д. (рис. 9.2). В составе утилиты присутствует подробная справка, которая помогает составить любой необходимый фильтр поиска сообщений.

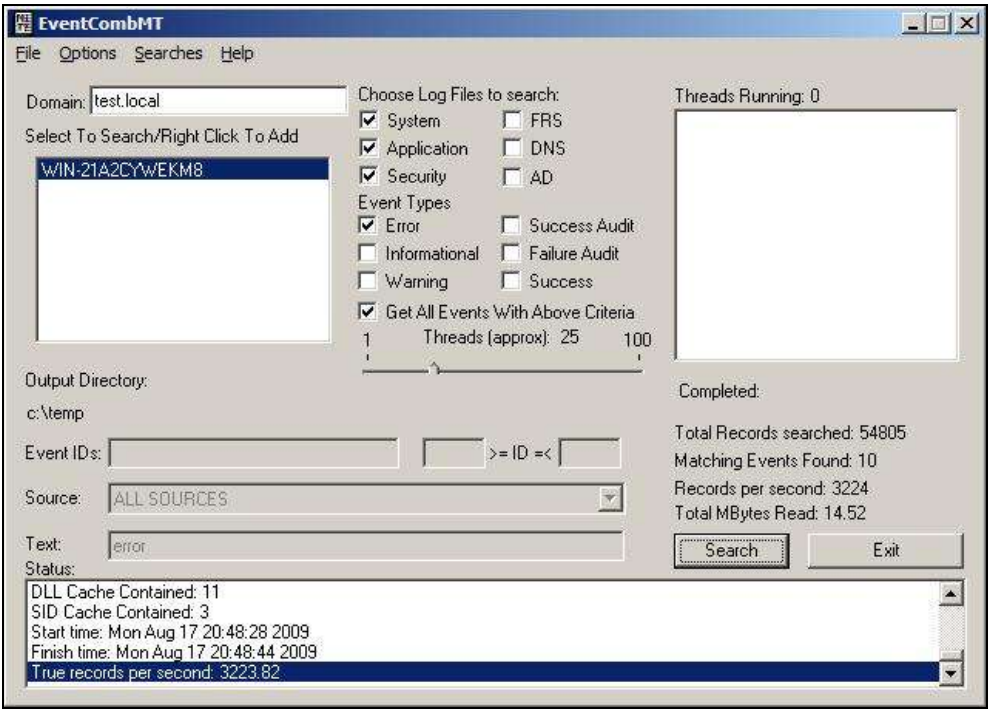


Рис. 9.2. Утилита EventCombMT

Администратор может достаточно просто настроить фильтры для поиска сообщений на любом числе компьютеров. Утилита специально спроектирована для многопоточного поиска, что позволяет быстро осуществлять поиск заданного события на многих компьютерах. Результаты работы утилиты сохраняются в текстовый файл.

Примечания

В Windows Server 2003 есть также сценарий EVENTQUERY.vbs, который позволяет вывести события как с локального, так и с удаленных компьютеров, используя необходимые фильтры (по дате, по номеру события, типу и т. п.).

Кроме того, анализировать журнал событий можно и другими средствами. Так, утилита LogParser позволяет в том числе подключаться к журналам событий различных компьютеров и осуществлять произвольные выборки сообщений.

Основной недостаток описанных вариантов просмотра состоит в том, что информацию о важном событии администратор получит только тогда, когда он запустит соответствующий поиск или откроет оснастку. Обычно необходимо оповестить администратора сразу после возникновения потенциально критического события.

Поможет в этом возможность *привязки задания к событию*. Для этого в панели **Действия** оснастки **Просмотр событий** необходимо выбрать операцию **Привязать задачу к …** и настроить необходимые параметры оповещения. В качестве реакций можно назначать запуск программы, оповещение по электронной почте и т. д. Существуют различные возможности привязки задачи: можно выполнять ее при появлении нового сообщения в каком-либо журнале, при возникновении сообщения с заданным ID и т. д. Все определяется целями создания такой задачи.

Созданная задача будет отображаться в оснастке **Планировщик заданий**. На рис. 9.3 показано задание, которое отсылает сообщение по электронной почте на указанный адрес при появлении нового сообщения в созданном администратором настраиваемом представлении журнала событий.

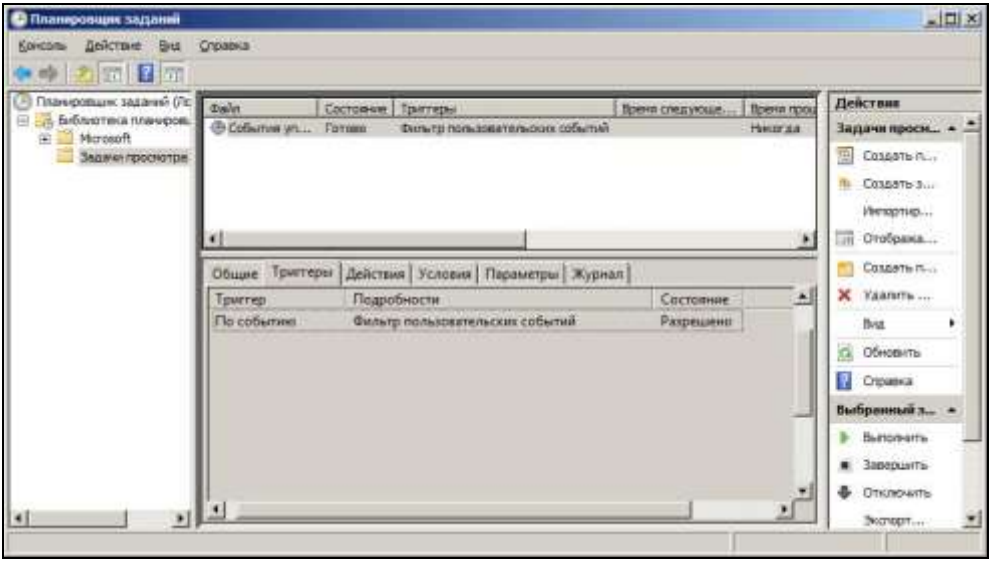


Рис. 9.3. Планировщик заданий Windows 2008

В сервере Windows 2003 такой возможности в оснастке просмотра событий нет. Но можно воспользоваться специальным сценарием — `EVENTTRIGGERS`, который позволяет настроить автоматические действия системы на то или

иное событие. Справочная система к этой команде подробно описывает, как следует создать триггер, настроенный на появление определенного события. Поэтому мы не будем останавливаться на этом описании.

Поскольку мы уже умеем реагировать на события в журналах системы, то для настройки действий на любое другое событие в системе можно поступить очень просто: достаточно внести о нем запись в системный журнал, а далее уже воспользоваться стандартными средствами привязки задачи к такому событию.

Начиная с Windows 2003 в составе операционной системы присутствует команда `EVENTCREATE`. С ее помощью можно записать в любой журнал событие заданного типа (информация, ошибка и т. п.). Применение утилиты подробно описано в ее справке (`EVENTCREATE /?`), к которой мы отошлем читателя.

Конечно, ручная настройка подобного реагирования на события — дело трудоемкое. При увеличении числа контролируемых систем можно либо воспользоваться системами мониторинга, либо приобрести коммерческие продукты, в которых уже настроены возможные операции для администратора. Например, можно заносить в базу данных параметры заданий на печать (кто, какой документ, сколько страниц и т. п. распечатал на данном принтере). Среди подобных программ отметим EvenTrigger от компании IS Decisions (**www.eventrigger.com**), GFI LANGuard Security EventLog Monitor и другие.

Operation Manager 2007

Для контроля систем на основе Windows разработан сервер Microsoft System Center Operation Manager (SCOM). На момент подготовки книги последняя доступная версия была SCOM 2007 R2. Этот продукт хорошо подходит для контроля и управления системами на основе Microsoft Windows, хотя в ограниченных пределах может обеспечивать мониторинг и Linux-систем, и систем, контролируемых по протоколу SNMP.

> ***Примечание***
>
> Мы не будем останавливаться на выпусках SCOM. При необходимости информацию о версии, наиболее подходящей для мониторинга конкретной системы заданной архитектуры, можно получить, кратко ознакомившись с описаниями на сайте Microsoft.

В состав SCOM 2007 входит много компонентов, обеспечивающих мониторинг систем различной сложности: от самых простых до территориально распределенных с подключением офисов через сеть Интернет, модули сбора и анализа отчетов, формирования графических представлений и т. п. Сразу скажем, что разобраться в настройках SCOM и использовать данную систему

для контроля собственных параметров достаточно сложно. Внедрение SCOM — трудоемкий и дорогостоящий процесс, требующий хорошей подготовки. Мы лишь коснемся основ установки и настройки сервера и посоветуем внимательней ознакомиться с доступной справочной документацией:

- страницу сервера на сайте Microsoft TechNet: **http://technet.microsoft.com/ru-ru/opsmgr/bb498238%28en-us%29.aspx**;
- русскоязычный сайт, посвященный SCOM: **http://opsmgr.ru/**;
- сайт System Center Forum, с которого можно загрузить различные справочные руководства (howto), примеры, сценарии и т. п. **http://www.systemcenterforum.org/downloads/#OperationsManager2007**.

Установка сервера Operation Manager 2007

Сервер мониторинга от Microsoft — весьма ресурсоемкий продукт: для комфортной работы с ним требуется производительный сервер. Только рекомендуемое значение оперативной памяти составляет 2 Гбайта. Кроме того, это программное обеспечение предполагает предварительную установку сервера баз данных (Microsoft SQL Server, коммерческого продукта).

Для работы SCOM требует установки на сервер ряда компонентов. Их состав зависит от версии операционной системы. Проще всего запустить встроенную в SCOM проверку выполнения условий установки (рис. 9.4) и устранить отмеченные проблемы.

Опция контроля конфигурации проверяет наличие необходимых компонентов в системе и формирует журнал, в котором содержатся рекомендации по необходимым операциям. Если нажать на кнопку **More** в соответствующей строке, то вы увидите описание необходимых шагов вплоть до ссылок на загрузку необходимых пакетов установки.

Сама установка предполагает указание администратором типовых параметров (путь установки, имя сервера баз данных и т. п.). Как правило, ответы на вопросы мастера установки легко дать любому администратору.

После завершения установки управление сервером будет осуществляться через его консоль. На рис. 9.5 показана консоль управления сервером SCOM 2007 R2. Это основной инструмент как для настройки, так и для текущей работы с сервером SCOM. Основные операции доступны через ссылки в правой части окна; кроме того, возможен вызов операций через контекстное меню пунктов навигатора (в левой части). Данную консоль можно установить на рабочие места операторов SCOM (в том числе, и на операционные системы рабочих станций).

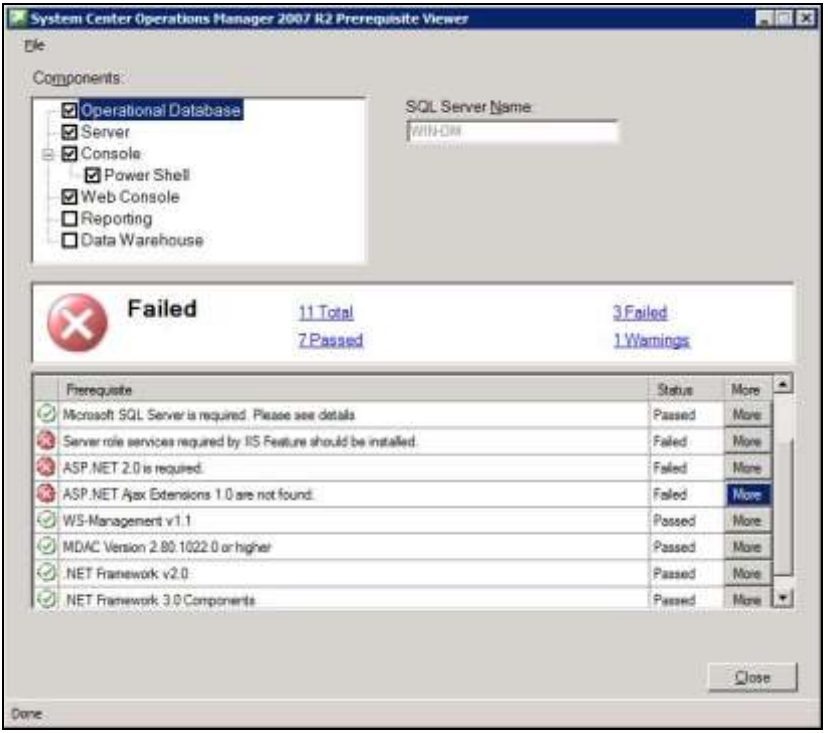


Рис. 9.4. Контроль требуемой для установки SCOM конфигурации

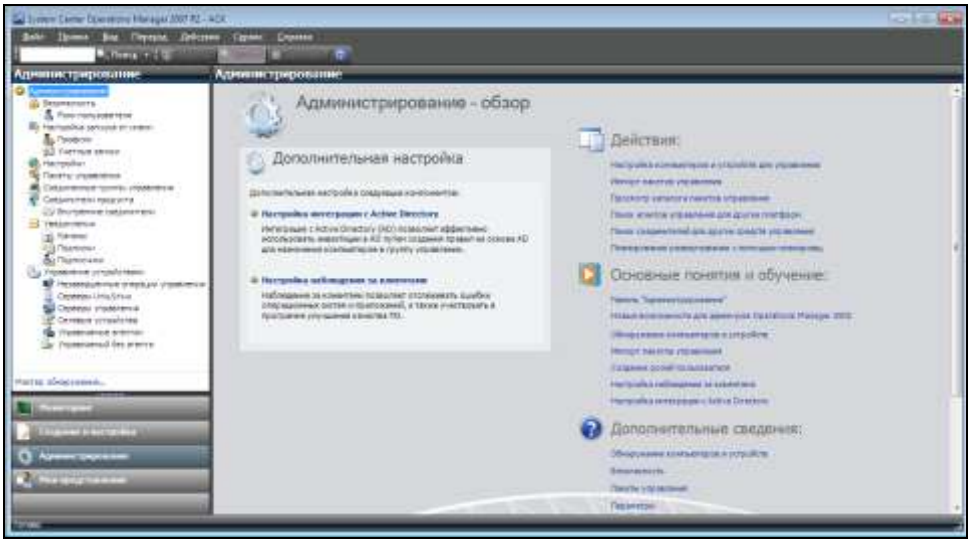


Рис. 9.5. Административная консоль SCOM 2007

Необходимые операции по настройке сервера после установки

Сразу после завершения процесса инсталляции сервер SCOM практически не может выполнять свое назначение. Чтобы начать контролировать системы, необходимо:

- установить пакеты мониторинга;
- добавить системы, которые будут контролироваться;
- настроить оповещения по возникающим событиям для администраторов информационной системы.

Впоследствии вы можете настроить личное рабочее пространство в SCOM, разместив служебную информацию наиболее удобным способом, создавать собственные сценарии контроля и т. п. Так же, как и во всякой большой системе, необходимо будет настроить права тех специалистов, которые будут эксплуатировать SCOM. Но это уже задачи периода опытной эксплуатации.

Импорт пакетов мониторинга

Пакеты мониторинга (*Management Packs*) представляют собой подготовленные комплекты сценариев проверки, правил обработки собираемой информации, программ для настройки соответствующих служб, базы знаний (описаний проблем) по контролируемым параметрам, форм отчетов и т. п. Существуют как бесплатные пакеты (в основном, это разработки от Microsoft), так и коммерческие (доступны бесплатно только в триальном периоде).

На сайте Microsoft создан каталог пакетов мониторинга, доступный по адресу **http://go.microsoft.com/fwlink/?LinkId=57329**. В начале этой страницы есть возможность выбора версии операционной системы, вендора и т. п.; прямая ссылка на пакеты от Microsoft для версии SCOM 2007 будет **http://www.microsoft.com/technet/prodtechnol/scp/mtps/opsmgr07.aspx?SCPProdID=3&Vendor=Microsoft**.

Для каждой контролируемой службы необходимо загрузить и импортировать в SCOM соответствующий пакет. Так, существуют пакеты для мониторинга сервера баз данных, службы DHCP и DNS, состояния контроллеров домена, для проверки почтового сервера Exchange и работы SharePoint-сервера и т. д. Я рекомендую просмотреть весь список пакетов от Microsoft и загрузить те из них, которые соответствуют службам, эксплуатируемым в вашей информационной системе.

Пакеты необходимо загрузить на компьютер и запустить их на выполнение (установку). Выполнение пакета — это просто разархивирование содержащихся в нем файлов в отдельную папку. Обратите внимание, что вместе

с файлами, которые потом будут импортированы в SCOM, в папке часто находится документация. Перед установкой пакета обязательно прочтите сопутствующие документы, поскольку для нормального функционирования выбранного средства контроля могут понадобиться дополнительные действия. Например, придется создать почтовый ящик, используемый для отправки/приема контрольных сообщений, или настроить значения порогов, в соответствии с которыми получаемые данные будут расцениваться как нормальные или критические, и т. п.

Импорт пакетов производится командой в навигационной панели **Actions** консоли управления сервером или по операции в контекстном меню объекта **Management Pack**. Программа импорта предложит либо загрузить пакеты с сервера каталогов, либо импортировать их с локального диска.

Добавление контролируемых систем

SCOM нужно сообщить, какие системы он должен контролировать. Существует вариант как ручного, так и автоматического добавления систем. В любом случае процесс начинается операцией Discovery (рис. 9.6).

Процесс добавления систем одинаков для различных платформ: необходимо указать критерии поиска (например, по части имени, по каким-либо атрибутам в службе каталогов и т. п.), ввести параметры учетной записи, необходимой для подключения к системам и установки программного обеспечения клиента (или параметры *community* в случае использования SNMP), начать процесс установки клиента на удаленную систему.

При *ручном* варианте вы указываете критерии поиска, отмечаете системы, которые будете контролировать, и устанавливаете на них агента (или реализуете вариант без агента). После запуска установки можно закрыть окно установки и контролировать итоги в окне **Tasks** (рис. 9.7).

Многие задания в SCOM можно назначить к выполнению и затем просто контролировать ход их реализации в окне Tasks. В данном примере в окне задач вы видите состояние заданий по установке агентов мониторинга на удаленные системы.

В случае настройки *автоматической* установки агентов вы в мастере операций определяете критерии, которым должны удовлетворять системы, чтобы для них включился мониторинг. Например, самый простой способ состоит в том, чтобы указать все объекты в каком-либо контейнере службы каталогов. SCOM будет периодически искать системы, удовлетворяющие такому критерию, и, при их появлении, либо автоматически установит агента, либо поместит систему в очередь для последующей ручной установки (варианты выбираются администратором при формировании правила). Такой автоматический способ называется интеграцией со службой каталогов (*Active Directory Integration*).

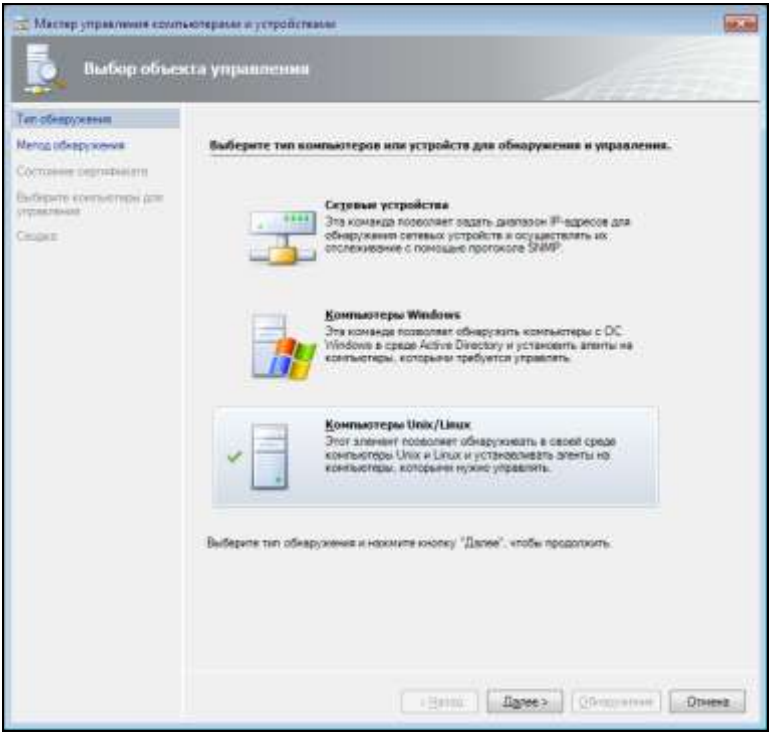


Рис. 9.6. Операция выбора контролируемых систем

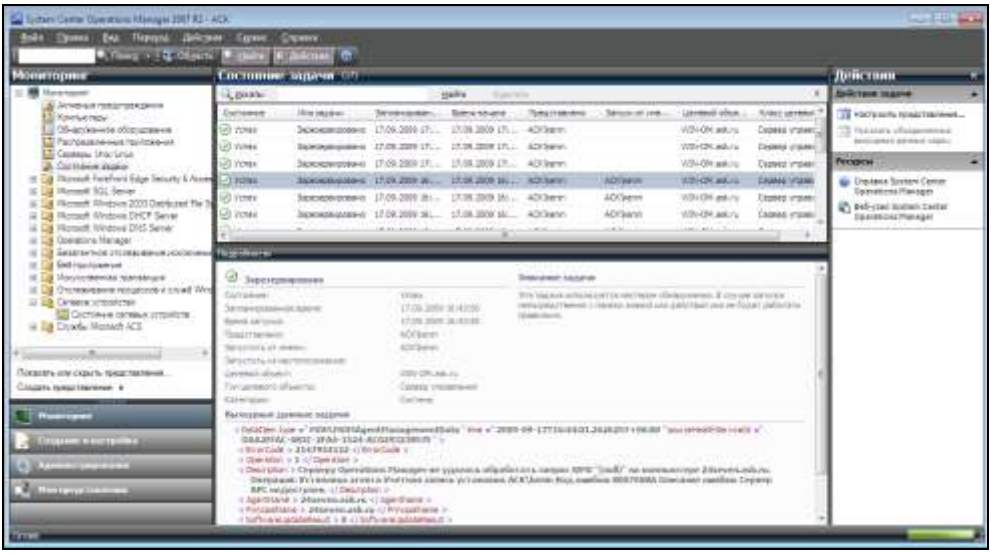


Рис. 9.7. Окно состояния выполнения заданий

SCOM позволяет добавлять в список контролируемых объектов оборудование, управляемое по протоколу SNMP. Для этого следует указать при сканировании сети мастером операции правильные значения строк идентификации (*community*).

Кроме того, в SCOM имеется возможность контролировать ряд параметров систем на основе Linux. К сожалению, перечень таких систем ограничивается только коммерческими выпусками (SuSe, RedHat, HPUX, AIX). Конечно, установочные пакеты для этих систем имеются в папках SCOM, и вы можете преобразовать, например, пакеты RPM в пакеты DEB. Но такие действия вы будет производить на свой страх и риск и надеяться только на собственные силы при устранении сбоев, которые могут возникнуть при мониторинге. Без установки агента на Linux-системы вы можете только контролировать сообщения Syslog. Для этого необходимо настроить сбор таких сообщений и написать сценарии для их обработки (см. KB942863).

Настройка оповещений SCOM

Администраторы должны получать сообщения о неисправностях не только тогда, когда они работают в консоли SCOM, но и в любое другое время, предусмотренное регламентом обслуживания информационной системы. Для этого в SCOM необходимо настроить оповещения, т. е. выполнить следующие операции:

- ❒ настроить каналы оповещений;
- ❒ настроить параметры операторов для оповещений;
- ❒ настроить критерии, в соответствии с которыми оповещения должны или не должны отсылаться данному оператору.

Канал оповещения (notification channel) — это способ передачи сообщения оператору. Например, отправка по электронной почте (SMTP-channel), отправка мгновенных сообщений (IM), посылка SMS и т. п. Естественно, что в системе должны существовать соответствующие службы. Например, для использования SMTP (рис. 9.8) необходимо иметь работающий почтовый сервер, для отправки SMS следует установить программное обеспечение для работы с сотовым телефоном (и подключить сам телефон) и т. д.

На рис. 9.8 показано, что при выборе варианта оповещения по электронной почте мастер предложит указать параметры почтового сервера и определить текст сообщения, которое будет отсылаться в случае возникновения непредвиденных ситуаций.

Настройка операторов для получения оповещений, или, в терминах SCOM, — подписчиков (*subscriber*), сложности не представляет. Вы должны только указать параметры для всех доступных данному оператору каналов.

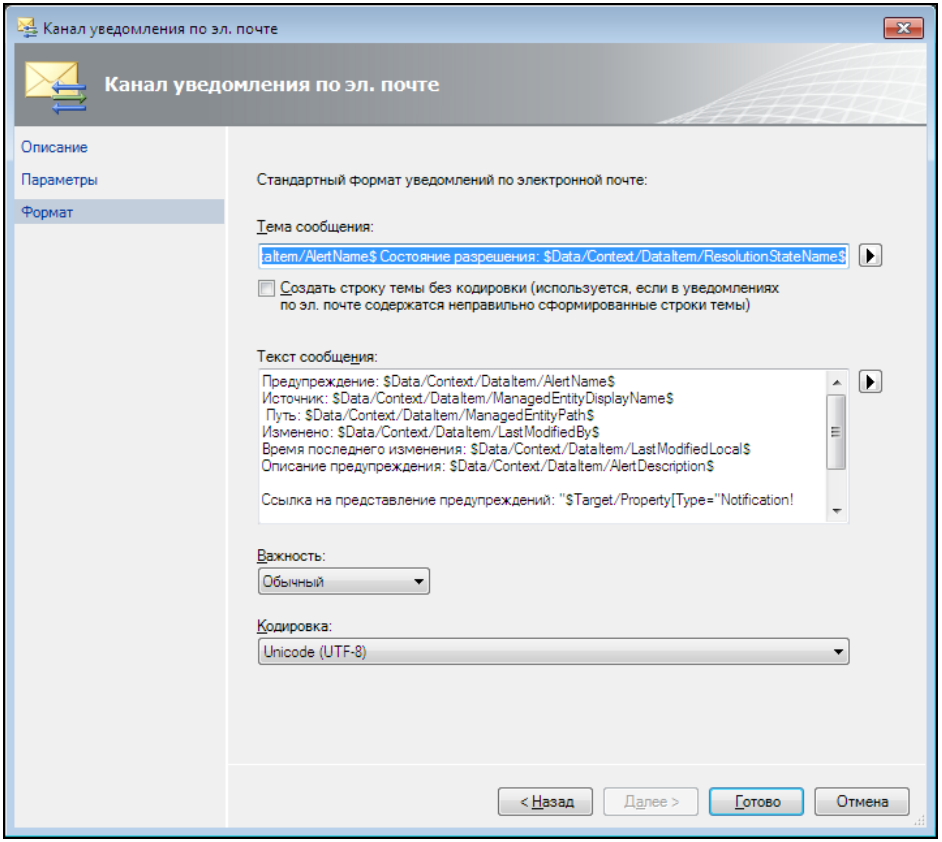


Рис. 9.8. Настройка каналов оповещения

Более трудоемка настройка подписок (*subscriptions*). В некотором смысле операция напоминает создание правил автоматической обработки сообщений в почтовом клиенте: нужно выбрать и настроить все критерии, при соответствии которым сообщения будут отправлены данному оператору.

> ***Совет***
>
> Начиная работу с SCOM, в качестве критерия выберите отправку всех сообщений о критических событиях (critical). Получив некоторый опыт работы, вы можете оптимизировать критерии подписок.

Немного о структуре объектов SCOM

Приступая к работе с SCOM, достаточно сложно понять назначение различных его элементов и принципы их использования. Поясним кратко основные моменты.

Как правило, SCOM работает с *группами* — логическими объединениями нескольких элементов. Обычно группы формируются при установке пакетов мониторинга, но их можно создать и вручную. Пакеты мониторинга обычно устанавливают и правила, по которым объекты включаются в ту или иную группу. Например, по итогам анализа служб Windows делается оценка о наличии действующего сервера DHCP и система помещается в соответствующую группу (по версии операционной системы; в свою очередь, такая группа входит в общую группу DHCP-серверов).

Для групп пакеты мониторинга создают *мониторы*, которые получают данные о работе необходимых служб. Полученные от них данные анализируются с помощью *правил* (*rules*).

Администраторы имеют возможность как создавать собственные объекты (группы, мониторы и т. п.), так и модифицировать существующие (например, изменить пороги классификации событий с критических на предупреждение и т. п.).

Установка Nagios

SCOM — коммерческий продукт. Но с не меньшей результативностью контролировать информационные системы можно с помощью бесплатных продуктов. Nagios является, на мой взгляд, одним из самых популярных OpenSource-проектов мониторинга информационных систем. Nagios для пользователей Ubuntu доступен в качестве готового пакета, который можно установить командой

```
apt-get install nagios2
```

Это гарантирует установку всех необходимых для его работы библиотек и является самым простым способом, рекомендуемым для обычных пользователей. Однако в Сети доступна более свежая версия этого пакета (третья на момент подготовки издания), которую мы и установим из исходных кодов.

> ***Замечание***
>
> Например, можно упомянуть также проекты Cacti (**http://cacti.net/**), Munin (**http://munin.projects.linpro.no/**), OpenNMS (**http://www.opennms.org/**), ZABBIX (**http://www.zabbix.com/**) и др. Для каждого из этих проектов в Сети доступны многочисленные расширения, позволяющие достаточно просто обеспечить контроль работы информационной системы.

Процедура быстрой установки программы на Ubuntu описана на сайте в разделе документации (**http://nagios.sourceforge.net/docs/3_0/quickstart-ubuntu.html**). Хотя статья описывает процесс для седьмой версии сервера Ubuntu, все рекомендации применимы и для версий 8.*x*. Мы приведем далее описание уста-

новки Nagios с краткими пояснениями, поскольку страницы указанного сайта не доступны в русской локализации.

Итак, предварительно на сервер следует установить пакет apache:

```
apt-get install apache2
```

Командой `dpkg -list <имя_пакета>` проверьте наличие в системе пакетов, необходимых для компиляции (`build-essential`) и для отображения графики (`libgd-tools`, `libgd2-xpm-dev`, `libpng12-dev`, `libjpeg63-dev`, `libglib1.2-dev`). Установите их в случае отсутствия командой `apt-get install <имя_пакета>`.

> ***ЗАМЕЧАНИЕ***
>
> Версии пакетов могут меняться, поэтому лучше для последних двух пакетов указать `apt-get install libpng-dev libjpeg-dev` и выбрать версию, предложенную программой.

Загрузите с сайта **http://www.libgd.org/releases/** последнюю версию GD-библиотеки (она потребуется для прорисовки схем сети), разархивируйте ее и установите (листинг 9.1).

Листинг 9.1

```
wget http://www.libgd.org/releases/gd-2.0.35.tar.gz
tar zvfx gd-2.0.35.tar.gz
cd gd-2.0.35/
./configure '--with-jpeg=/usr/local' '--with-png=/usr/local' '--with-
zlib-dir=/usr/local'
make
make install
```

Перейдите в режим суперпользователя (`sudo -s`) и создайте учетные записи, группы, которые будут использованы программой мониторинга. Назначьте созданным пользователям пароли и введите их в соответствующие группы. (Пароли можно не запоминать, поскольку эта операция необходима фактически только для разблокирования учетной записи). Эти операции выполняются командами, приведенными в листинге 9.2.

Листинг 9.2

```
useradd -m nagios
passwd nagios
groupadd nagios
usermod -G nagios nagios
```

```
groupadd nagcmd
usermod -a -G nagcmd nagios
usermod -a -G nagcmd www-data
```

Загрузите с сайта Nagios (**http://www.nagios.org/download/**) последнюю стабильную версию программы, плагины и add-one. Разархивируйте загруженные с сайта Nagios исходные коды программы и ее дополнений:

```
tar xzf nagios-3.0.6.tar.gz
tar xzf nagios-plugins-1.4.13.tar.gz
```

Перейдите в папку с кодами

```
cd  nagios-3.0.6
```

и выполните конфигурацию программы с указанием названия группы, созданной ранее:

```
./configure —with-command-group=nagcmd
```

> ***ЗАМЕЧАНИЕ***
>
> В примерах использованы названия версий пакетов на момент написания книги. На практике необходимо подставить названия пакетов актуальных версий программы.

Проверьте, что конфигурирование прошло нормально и что настройка параметров вас удовлетворяет. После этого запустите процесс компиляции и установки самой программы, сценария запуска, примеров, настройки прав на сценарии мониторинга и настройки Web-интерфейса (листинг 9.3).

Листинг 9.3

```
make all
make install
make install-init
make install-config
make install-commandmode
make install-Webconf
```

Создайте пользователя, которому будет разрешен доступ к Web-интерфейсу программы, и назначьте ему пароль (этот пароль необходимо запомнить для последующей работы) командой:

```
htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Перезагрузите конфигурацию Web-сервера для вступления в силу внесенных изменений:

```
/etc/init.d/apache2 reload
```

После этих операций Nagios практически готов к работе.

Примечание

После указанных операций конфигурация Nagios будет сохранена в нескольких файлах в папке /usr/local/nagios/etc. Для начала работы минимально необходимо исправить в файле /usr/local/nagios/etc/objects/contacts.cfg адрес электронной почты администратора, которому будут высылаться предупреждения программы мониторинга. Изменения в остальных файлах конфигурации будут описаны далее в разделах настройки наблюдения за компьютерами, хостами, коммутаторами и т. д.

Теперь необходимо установить базовые дополнения (plugin) Nagios. Для этого перейдите в папку, в которую были разархивированы их исходные коды (nagios-plugins-1.4.13), и выполните следующие команды:

```
./configure --with-nagios-user=nagios --with-nagios-group=nagios
make
make install
```

Состав плагинов для Nagios весьма обширен. Приведенная выше установка включает в себя базовые модули. А только на сайте **http://www.monitoringexchange.org/** представлено более 1800 различных плагинов. Поэтому, если вы хотите расширить функциональность Nagios и контролировать какие-либо собственные параметры, то посетите вначале этот сайт. Возможно, что задача, аналогичная вашей, уже решена, и достаточно только загрузить нужный модуль и настроить его в системе.

Теперь остается только проверить настройки программы командой

```
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

и запустить ее:

```
/etc/init.d/nagios start
```

Для того чтобы система мониторинга запускалась автоматически, необходимо добавить ссылки на сценарий запуска в соответствующие папки каталога запуска. Проще всего сделать это командой update-rc.d (см. *Приложение*):

```
update-rc.d nagios defaults
```

Первичное подключение к Nagios

Для отображения информации системы мониторинга достаточно открыть страницу **http://localhost/nagios/** (вместо *localhost* следует указать имя сервера Nagios при открытии страницы с удаленного компьютера). На запрос параметров авторизации необходимо ввести имя nagiosadmin и тот пароль, который вы назначили для этой учетной записи на предыдущих шагах.

На рис. 9.9 показана одна из страниц программы — структура контролируемой Nagios небольшой системы.

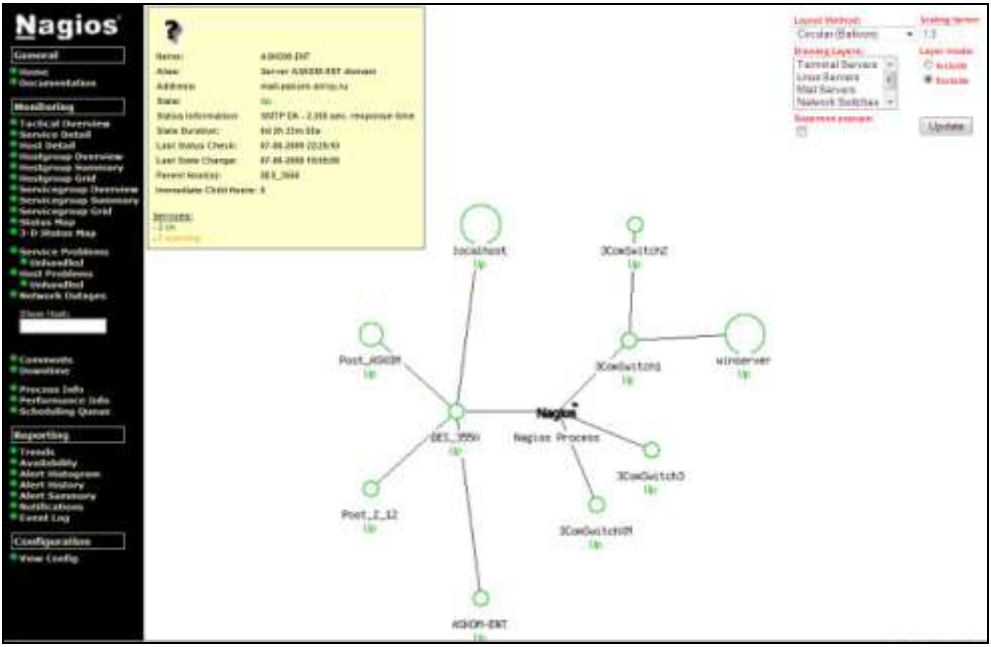


Рис. 9.9. Схема сети в Nagios

Немного о логике работы Nagios

Nagios можно представить условно в виде двух частей: сервер (собственно о его установке и велась речь в предыдущем разделе) и клиент — небольшой программы, которая должна быть установлена на контролируемую систему и осуществлять сбор необходимых данных.

Существуют различные версии клиентов, но наиболее часто для систем на основе Linux используется программа NRPE (ссылка на этот плагин присутствует на официальном сайте Nagios — **http://www.nagios.org/**), а для Windows-компьютеров — NSClient++ (**http://trac.nakednuns.org/nscp/**). Способы автоматической установки клиентов на все системы в этой книге не рассматриваются, интересующегося читателя мы отошлем, например, к нашей предыдущей книге (Кенин А. М. "Самоучитель системного администратора", вып. 2. СПб.: БХВ-Петербург, 2008). Обратим только внимание на то, что для каждого клиента должна быть настроена конфигурация так, как описано в последующих разделах.

Замечания

Можно осуществлять и сбор данных без установки клиента, например, путем анализа поступающих трапов SNMP. Но обычный вариант контроля — установка на клиентский компьютер агента для сбора и пересылки данных.

Исторически первым клиентом для Windows был вариант программы NPRE. В целях совместимости в NSClient++ сохранен протокол, используемый в NPRE. Вы можете в настройках клиента указать как любой вариант работы, так и оба (некоторые плагины, например, разработаны под конкретную версию клиента). Учтите, что в ряде ситуаций NPRE предоставляет больше возможностей для контроля, например, с его помощью легко настроить выполнение сценариев на самой контролируемой системе.

При помощи клиентов происходит *активный* мониторинг работы: сервер инициирует на клиенте заданную настройками команду и анализирует полученные данные. Кроме того, возможен *пассивный* режим работы в тех случаях, когда данные на сервер пересылаются по инициативе клиента. Например, так происходит обработка SNMP-трапов (*см. разд. "Мониторинг систем с использованием протокола SNMP"*).

Как уже говорилось, для получения информации от клиента на сервере Nagios запускаются специальные команды (или программы). В терминах Nagios эти команды принято называть *плагинами* (*plugin*). Для того чтобы система мониторинга могла их использовать, такие команды должны быть *описаны* в специальном конфигурационном файле — *commands.cfg*. Именно эти описания в терминах Nagios и называются *командами* контроля.

Замечание

Плагины несложно найти в Сети: с сайта Nagios есть ссылка на проекты на SourceForge.net, существует сайт обмена плагинами
http://www.monitoringexchange.org/
и другие источники.

Кроме описания самой команды, системе мониторинга нужно знать, какие системы проверять, как часто запускать команду проверки, делать ли перерывы в ее использовании (например, не выполнять в определенные дни недели или в заданные периоды суток и т. п.). Совокупность таких настроек в Nagios принято называть *службой* (service), а определяются они отдельным блоком в файле, описывающим параметры контролируемой системы. Поскольку параметров в службе много (около полутора десятков) и многие из них обычно повторяются, то принято описывать их в *шаблонах* (template), а непосредственно в описании службы просто указывать на такой шаблон (описания шаблонов хранятся в файле templates.cfg).

Замечание

Обратите внимание, что в шаблонах допускаются вложения: какую-то часть параметров можно выделить в отдельный шаблон и повторить его в других описаниях.

Каждую контролируемую систему необходимо описать в конфигурации Nagios. Для удобства делается это в отдельных файлах (по типам устройств), которые при старте сервера включаются в общую конфигурацию. Первоначально ссылки на эти файлы "по направлениям" закомментированы, поэтому при необходимости контроля какого-либо класса устройств сначала следует удалить символ # в соответствующей строке файла nagios.cfg, а потом добавить блок описания системы в требуемый файл.

В результате Nagios периодически выполняет на контролируемых системах заданные команды, собирает результаты и при возникновении критического события оповещает операторов. Результаты контроля можно сохранять (по умолчанию данные производительности не хранятся) и представлять для анализа в графическом виде (*см. разд. "Отображение собранных данных на графиках"*). Также Nagios позволяет описать команды, которые будут выполнены на хостах при возникновении событий. Таким способом можно автоматически устранять возникающие неисправности (*см. разд. "Автоматическое реагирование на сбои в работе контролируемых систем"*).

Если в вашей системе будет контролироваться много компьютеров и устройств, то их удобно сгруппировать. В Nagios можно создать группы из компьютеров (устройств) и служб. Например, если нужно наблюдать за состоянием всех служб на серверах, то следует создать группу, в которую включить названия этих систем. А если вы хотите контролировать состояние, например, службы разрешения имен DNS, которая работает на нескольких физических системах, то в этом случае удобно создать группу для службы: достаточно будет видеть состояние всей группы как нормальное, чтобы быть уверенным в работе служб DNS на всех компьютерах.

Из общих конфигурационных настроек отметим еще параметры операторов — тех людей, кому программа будет отправлять сообщения при возникновении тех или иных событий. В Nagios индивидуальных операторов также можно объединять в группы и настраивать отправку сообщений определенного типа конкретной группе специалистов. Также можно настраивать периоды времени, например, для различных типов контроля в рабочие и выходные дни, для разных способов оповещения администраторов (например, днем по электронной почте, а ночью — на пейджер) и т. д.

Обратите также внимание, что оповещения могут "эскалироваться" (иными словами, при появлении повторяющихся событий оповещение может быть послано следующему специалисту).

Структура конфигурационных файлов Nagios

Описание команд Nagios

Команды Nagios описываются в файле `commands.cfg` (путь по умолчанию /usr/local/nagios/etc/object/commands.cfg).

На практике в файле `commands.cfg` обычно необходимо указать расположение исполняемого файла, его название, которое будет использовано в Nagios, и параметры строки запуска. По умолчанию в файле конфигурации установленной системы уже содержатся некоторые описания типовых команд проверки (проверки пингом — `check_ping`, проверки HTTP-сервера — `check_http` и многие другие). По этим образцам легко можно создать собственные команды проверки, хотя обычно берут готовые разработки, которые, практически для любого варианта контроля, легко найти в Сети. В листинге 9.4 приведен пример описания простейшей команды — проверки достижимости хоста при помощи команды `ping`.

Листинг 9.4

```
define command{
   command_name    check-host-alive
   command_line    $USER1$/check_ping -H $HOSTADDRESS$ -w $ARG1$ -c $ARG2$ -p 5
   }
```

Это описание создает команду с именем `check-host-alive`, в качестве исполняемого файла используется команда `check_ping` из установленных утилит Nagios. Символы, заключенные в знаки доллара, указывают переменные. `$HOSTADDRESS$` традиционно заменяется при вызове на имя тестируемой системы, а `$ARG1$`, `$ARG2$` и т. д. — последовательно на аргументы, указываемые в описании службы.

> ***Замечание***
>
> В терминах Nagios это макросы (macros), которые заменяются значениями в момент выполнения. Поскольку обычно мы привыкли к другому определению макросов, в этой книге будем называть эти названия переменными.

Ключи `w` и `c` определяют значения, которые будут использованы для формирования статуса предупреждения (`w`) или ошибки (`c`). Как правило, можно задавать абсолютные или относительные значения (или все вместе: в типовой конфигурации, например, параметр `w` обозначается как `3000.0,80%`). Последний ключ (`-p`) указывает, что команда `ping` должна послать пять проверочных пакетов.

Описание шаблонов служб

Службы обычно описываются в файлах конфигурации отдельно для каждого типа контролируемых систем (в общую конфигурацию nagios такие файлы импортируются директивами `cgf_file=...` в файле nagios.cfg). Построение файлов конфигураций начинается с описания шаблонов, за которыми следуют описания хостов и потом описания служб.

Посмотрите параметры, которые указаны в шаблоне для контроля Windows-систем, и их краткие пояснения (листинг 9.5).

Листинг 9.5

```
define host{
     name                windows-server     ; название шаблона
     use                 generic-host       ;   данный шаблон сам включает
                                            ;в себя настройки из этого шаблона
     check_period          24x7      ; по умолчанию система контролируется
                                     ; круглосуточно
     check_interval          5       ; команда контроля запускается каждые
                                     ; 5 минут
     retry_interval          1        ; повтор осуществляется через минуту
                                      ; (если система не ответила)
     max_check_attempts     10        ; максимальное число попыток 10
     check_command          check-host-alive    ; здесь указана команда
                                                ; контроля
     notification_period     24x7   ; определен период, когда отсылаются
                                    ; оповещения — круглосуточно
     notification_interval     30   ; определен период для повторной
                                    ; отправки предупреждений (оповещения
                                    ; будут отправляться непрерывно, пока
                                    ; система не перейдет в нормальное
                                    ; состояние
     notification_options     d,r   ; здесь указаны состояния системы,
                                    ; для которых высылаются
                                    ; предупреждения
     contact_groups          admins      ; здесь определяются операторы,
                                         ; которым будет высылаться
                                         ; оповещение
     hostgroups          windows-servers ; эта строка определяет группы,
                                          ; в которые будет входить
                                          ; система
     register          0          ; в данном случае 0, поскольку
                                  ; регистрировать не нужно — это шаблон
     }
```

Примечание

В Nagios существуют следующие состояния контролируемой системы (они отличаются для хоста и службы): для хоста: Unreachable (u), Down (d), Recovered (r), Flapping (f); для службы: Unknown (u), Critical (c), Warning (w), Recovered (r), Flapping (f). Название состояния говорит само за себя. Поясним только состояние *Flapping*. В этом состоянии система периодически то работает нормально, то переходит в состояние ошибки.

Описания служб Nagios

В описании службы уже можно не повторять общие значения из шаблонов, поэтому типовое определение службы может выглядеть примерно так, как в листинге 9.6.

Листинг 9.6

```
define service{
     use                generic-service
     host_name          winserver
     service_description     Memory Usage
     check_command           check_nt!MEMUSE!-w 80 -c 90
     }
```

В этом примере служба с названием `Memory Usage` использует для работы настройки из шаблона `generic-service` для хоста, описанного под именем `winserver`. В качестве команды служба запускает `check_nt` с параметрами командной строки `MEMUSE` и `-w 80 -c 90` (вторые параметры указывают, какое возвращаемое значение используемой памяти нужно считать критическим — 90%, а для какого установить состояние в предупреждение — от 80 до 90%; сами параметры перечисляются через символ `!`).

Обычно контроль однотипных устройств можно осуществить одинаковой командой. В этом случае в описании службы достаточно перечислить все такие устройства через запятую (листинг 9.7).

Листинг 9.7

```
define service{
     use                      generic-service
     host_name
3ComSwitch1,3ComSwitch2,3ComSwitchXM,DES_3550
```

```
    service_description     PING
    check_command           check_ping!200.0,20%!600.0,60%
    …
       }
```

Для служб можно определять зависимости (*dependencies*). Делается это для того, чтобы скрыть "лишние" предупреждения. Например, если часть систем находится в локальной сети после маршрутизатора, то можно определить зависимость их от этого устройства. Понятно, что если этот маршрутизатор выйдет из строя, то и все устройства, находящиеся за ним, окажутся недоступными. Настройка зависимости позволит в случае его аварии скрыть предупреждения о недоступности зависимых устройств, пока не восстановится работа коммутатора, и не выполнять на них проверку состояния соответствующих служб.

Описание контролируемых систем в Nagios

Для удобства различные типы контролируемых систем принято описывать в разных конфигурационных файлах. В следующем примере конфигурации Nagios (файл usr/local/nagios/etc/nagios.cfg) включен импорт описаний для Linux- и Windows-систем, но отсутствует мониторинг сетевых принтеров и коммутаторов (листинг 9.8).

Листинг 9.8

```
...

# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg

# Definitions for monitoring a Windows machine
cfg_file=/usr/local/nagios/etc/objects/windows.cfg

# Definitions for monitoring a router/switch
#cfg_file=/usr/local/nagios/etc/objects/switch.cfg

# Definitions for monitoring a network printer
#cfg_file=/usr/local/nagios/etc/objects/printer.cfg



...
```

Если вам потребуется контролировать коммутаторы в сети, то раскомментируйте строку `#cfg_file=/usr/local/nagios/etc/objects/switch.cfg` и т. д.

Само описание хоста (оно будет содержаться в файле windows.cfg, или switch.cfg, или printer.cfg и т. д.) минимально может выглядеть в этом случае так, как показано в листинге 9.9.

Листинг 9.9

```
define host{
   host_name               myHost  ; имя системы
   alias                   My Best Host    ; полное имя системы
                                           ; (можно использовать пробелы
                                              и т. п.)
   address                 192.168.1.254   ; IP-адрес системы
}
```

В описание хоста можно включать два параметра, которые будут определять действия, выполняемые при сбоях в работе системы:

```
event_handler           server-reboot
check_command           check-host-alive
```

Nagios станет выполнять команду проверки `check-host-alive` и, как только будет обнаружена смена состояния хоста, начнется выполнение программы `server-reboot`. Таким способом можно, например, запускать остановившиеся службы на контролируемых серверах, перезагружать системы и т. п.

> ***Примечание***
>
> Мониторинг за событиями позволяет более оперативно восстановить работу систем. Если Nagios не получил ответа о нормальной работе системы, он через период, заданный параметром `retry_interval`, будет повторять контроль до достижения лимита, также определенного настройками (`max_check_attempts`). Событие же обрабатывается сразу после получения первой информации о "ненормальном" состоянии хоста.

Для удобства анализа хосты можно объединять в группы. Для этого необходимо описать группу в файле конфигурации (листинг 9.10).

Листинг 9.10

```
define hostgroup{
        hostgroup_name имя_группы
        alias          полное имя группы ; допускаются пробелы и т. д.
        }
```

Членство в группе можно определять как в самом описании группы (параметр `hostgroup_members`), перечисляя членов группы через запятую, так и в описании хоста (параметр `hostgroups` — см. листинг 9.11).

Так же, как и для служб, для хостов можно описывать зависимости одних систем от других. Для того чтобы описать для данной системы *родительский* хост (т. е. тот хост, от которого она зависит), необходимо указать имя этого хоста в параметре `parents` (листинг 9.11).

Листинг 9.11

```
define host{
        host_name имя
        display_name отображаемое имя
        address адрес
        parents имя родительской системы
        hostgroups имя группы
        check_command имя команды
        …
}
```

Схема сети, показанная на рис. 9.9, построена Nagios на основе данных об отношениях устройств, которые описаны при их создании.

Описание временных параметров

Временные параметры используются в различных конфигурациях: в описаниях хостов (периоды, когда нужно осуществлять мониторинг и отправлять сообщения), служб и контактов (периоды, когда можно отправлять сообщения по хостам и по службам). Синтаксис определения нового периода легко понять из примеров, включенных в файл /usr/local/nagios/etc/objects/timeperiods.cfg.

В описании необходимо дать название шаблону и перечислить построчно диапазоны времени, которые в него включаются. Причем допустимы названия дней недели, месяцев и порядковые номера (последний/первый понедельник месяца). Периоды времени можно перечислять через запятую. При необходимости из одного шаблона можно исключать периоды, описанные в другом шаблоне, если указать директиву `exclude` с последующим перечислением периодов времени (через запятую). В листинге 9.12 приведены примеры описания временных диапазонов.

Листинг 9.12

```
monday       09:00-12:00,13:00-18:00
tuesday         00:00-24:00
2009-05-01 / 7       00:00-24:00 ; Каждый седьмой день, начиная
                                   с 1 мая 2009 года
day 1 - 15   00:00-24:00      ; с 1 по 15 число каждого месяца
day 1 - 15 / 3        00:00-24:00 ; Каждый третий день с 1
                                    по 15 число каждого месяца
february -1  00:00-24:00   ; Каждый последний день февраля
```

Использование встроенных в Nagios команд контроля

При стандартной установке Nagios и плагинов в нем присутствует ряд команд (плагинов), которые можно использовать для контроля систем (табл. 9.1).

Таблица 9.1. *Список плагинов Nagios*

Утилита	Назначение
check_apt	Контроль обновлений систем Linux, производимых с помощью команд `apt-get`. Позволяет запустить процесс обновления при соответствующей настройке
check_breeze	Контроль мощности сигнала WiFi стандарта Breezecom
check_by_ssh	Этот плагин позволяет запускать на удаленной системе команды, используя протокол SSH
check_clamd	Проверка соединения CLAMD (антивирусная программа) с удаленным хостом
check_cluster	Проверка состояния хостов в кластере Linux
check_dhcp	Проверка доступности DHCP-серверов в сети
check_dig	Проверка работы DNS-службы на хосте (командой `dig`)
check_disk	Проверка объемов использования дискового пространства (собственных и примонтированных дисков)
check_disk_smb	Проверка объемов использования дисков, подключенных по протоколу SMB (обычно это диски от Windows-систем)

Таблица 9.1 *(продолжение)*

Утилита	**Назначение**
check_dns	Проверка работы сервера DNS с помощью программы *nslookup*
check_dummy	Плагин для настройки: просто возвращает численный параметр и строку, описанные при его запуске
check_file_age	Проверка времени создания файлов
check_flexlm	Проверка службы *Flexlm license manager*
check_ftp	Проверка FTP-соединения с удаленным хостом
check_hpjd	Проверка состояния принтеров Hewlett Packard с установленной картой JetDirect (проверка осуществляется по протоколу SNMP)
check_http	Проверка HTTP-соединений с удаленной системой. Проверка может осуществляться как по протоколу HTTP, так и по HTTPS. Можно контролировать время установки соединения, срок действия сертификатов сервера, а также ответ сервера (по поиску в ответе некоторой заданной строки, в том числе, допускается использование регулярных выражений)
check_icmp	Проверка удаленных хостов по протоколу ICMP
check_ide_smart	Проверка состояния локального диска (в Linux-системе) по технологии SMART
check_ifoperstatus	Проверка состояния работы сетевого интерфейса на заданной Linux-системе
check_ifstatus	Проверка состояния сетевого интерфейса на заданной Linux-системе
check_imap	Проверка работы удаленного хоста по протоколу IMAP. Можно анализировать ответ сервера на посылаемую на него строку imap-запроса
check_ircd	Проверка IRCD-плагина Nagios
check_jabber	Проверка JABBER-подключения к удаленному хосту
check_ldap	Проверка LDAP-сервера (можно отправить запрос на поиск соответствующего атрибута)

Таблица 9.1 *(продолжение)*

Утилита	Назначение
check_ldaps	Тоже проверка LDAP-сервера, только с использованием защищенных соединений (по протоколу SSL)
check_load	Проверка загрузки Linux-системы
check_log	Проверка журналов Linux-системы на наличие некоторой последовательности символов
check_mailq	Проверка числа сообщений в очереди почтового сервера (работает с различными версиями sendmail, qmail)
check_mrtg	Проверяет заданную переменную в логе MRTG (Multi Router Traffic Grapher) на минимальное/максимальное значения (для контроля параметров производительности необходимо использовать check_mrtgtraf)
check_mrtgtraf	Проверяет значения исходящего и входящего трафика коммутаторов, записанные в журнал MRTG. Требуется первоначальная установка пакета MRTG (http://ee-staff.ethz.ch/~oetiker/Webtools/mrtg/mrtg.html)
check_nagios	Проверяет состояние процесса nagios на локальной машине
check_nntp	Проверка NNTP-соединения с указываемым хостом
check_nntps	То же, но с использованием протокола NNTPS
check_nrpe	NRPE плагин Nagios
check_nt	Этот плагин осуществляет сбор данных со службы NSClient на Windows-системах
check_ntp	Проверка NTP-сервера. Вместо этого плагина рекомендуется применять check_ntp_peer
check_ntp_peer	Проверка NTP-сервера. Позволяет оценивать, в том числе, дрожание (jitter) сигнала времени
check_ntp_time	Этот плагин проверяет разницу времени между локальным сервером и указываемым удаленным NTP-сервером
check_nwstat	Служит для сбора данных с Novell-серверов. Требует установки дополнительных пакетов

Таблица 9.1 *(продолжение)*

Утилита	Назначение
check_oracle	Проверяет подключение к серверу Oracle, позволяет оценить размеры баз данных и наличие свободного места, состояние буферов кэширования и т. д.
check_overcr	Проверяет состояние Over-CR collector daemon на удаленной системе (**http://www.molitor.org/overcr**)
check_ping	Проверяет соединение с удаленной системой с использованием пакетов `ping`
check_pop	Проверка удаленных хостов по протоколу POP. Позволяет отправить на почтовый сервер строку запроса и проанализировать ответ сервера
check_procs	Проверяет состояние процессов Linux-системы
check_real	Проверяет состояние службы REAL (RTCP-подключений)
check_rpc	Проверяет состояние RPC-службы на указанном хосте
check_sensors	Проверяет состояние аппаратных датчиков системы Linux. Информация с датчиков получается с помощью пакета lm_sensors
check_simap	Проверяет IMAP-подключение по безопасному каналу к серверу. Контролируется время ответа и содержание (по анализу ответа на заданный запрос), валидность сертификатов
check_smtp	Проверяет SMTP-подключение к серверу. Ответ почтового сервера может анализироваться на наличие заданных строк. Также контролируется время отклика
check_snmp	Проверка удаленных систем (и получение с них данных) по протоколу SNMP
check_spop	Проверяет POP-подключение по безопасному каналу к серверу. Контролируется время ответа и содержание (по анализу ответа на заданный запрос), валидность сертификатов
check_ssh	Проверка подключения к SSH-серверу
check_ssmtp	Проверяет SMTP-подключение по безопасному каналу к серверу. Ответ почтового сервера может анализироваться на наличие заданных строк. Также контролируется время отклика

Таблица 9.1 *(окончание)*

Утилита	Назначение
check_swap	Проверяет свободное пространство в SWAP-файле локальной системы
check_tcp	Проверка TCP-подключения к указанной системе. Проверяется наличие отклика, его время, присутствие в отклике заданных строк и т. п.
check_time	Проверка времени на указанном хосте
check_udp	Проверка UDP-подключения к указанной системе. Проверяется наличие отклика, его время, присутствие в отклике заданных строк и т. п.
check_ups	Проверка состояния источников бесперебойного питания на локальной или удаленной Linux-системе. Для работы плагина требуется, чтобы в системе был установлен UPSD daemon (**http://www.networkupstools.org**)
check_users	Проверка числа пользователей, вошедших в локальную систему
check_wave	Проверка уровня WiFi-сигнала

Каждый из этих плагинов содержит справочную информацию, описывающую особенности его применения (вывод справки по команде `<плагин> -h`).

Для того чтобы задействовать плагин для мониторинга систем, в Nagios должна быть описана использующая его команда. В файле commands.cfg приведено несколько наиболее часто употребляемых примеров контроля систем. При практической работе с Nagios этот файл нужно расширить за счет ваших собственных команд контроля.

Настройка мониторинга серверов Windows

Для мониторинга систем на основе Windows разработано несколько различных агентов. Наиболее распространенные из них: NSClient++, NC_NET (**http://sourceforge.net/projects/nc-net**) и OpMonAgent (**http://www.opmon.org/project/opmonagent.zip**). Функционал данных агентов практически идентичен, поэтому мы рассмотрим агент NSClient++, который, на взгляд автора, наиболее популярен.

Агент NSClient++ доступен со страницы **http://trac.nakednuns.org/nscp/**. Эту программу можно загрузить как в виде архива (zip), так и установочным

файлом (msi), причем для 32- и 64-битовых платформ предусмотрены различные версии агента. Если вы загрузили архив, то его необходимо распаковать в желаемую папку и установить службу Windows командой

```
NSClient++ -install
```

Удобнее воспользоваться msi-файлом, поскольку в этом случае мастер установки сразу внесет в конфигурацию агента часть настроек по результатам ваших ответов (рис. 9.10).

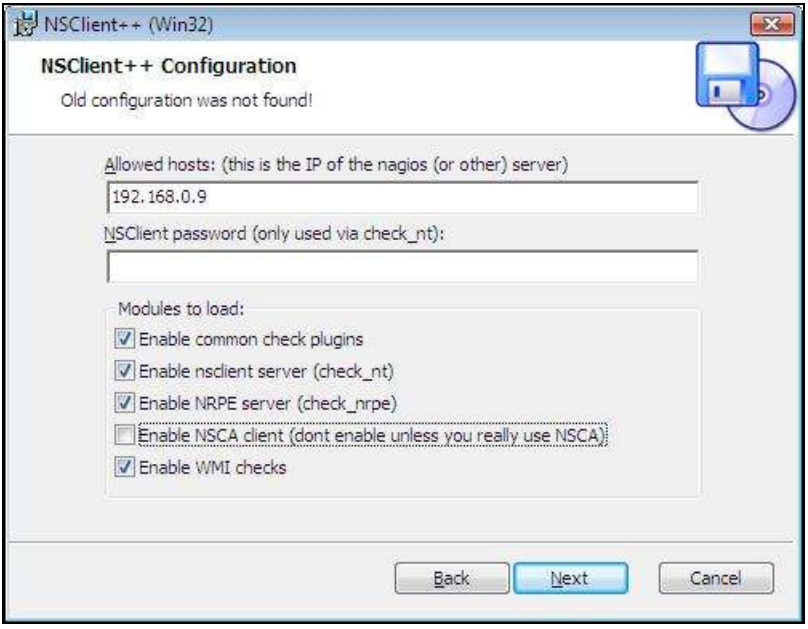


Рис. 9.10. Установка NSClient++

После установки необходимо разрешить взаимодействие службы с рабочим столом, для чего следует открыть свойства службы (**Панель управления** | **Администрирование** | **Службы** | найти службу **NSClientpp...** (полное название зависит от версии) и открыть ее свойства) и включить опцию **Разрешить взаимодействие с рабочим столом** (рис. 9.11).

Примечание

Служба NSClient++ имеет в составе модуль отображения/управления, который нужно установить (при необходимости) дополнительно командой `NSClient++ SysTray install`. После этого в зоне *systemtray* появляется пиктограмма управления службой NSClient++.

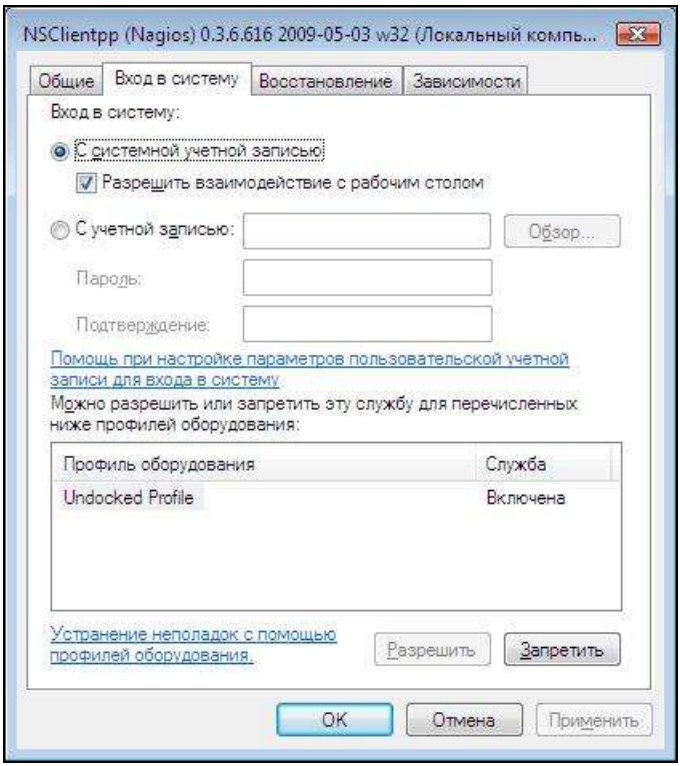


Рис. 9.11. Настройка параметров службы NSClient++

Перед запуском службы следует *обязательно* настроить параметры ее работы, причем делать это желательно и в случае предварительной частичной настройки конфигурации мастером установки. Для этого откройте файл `nsc.ini` (в папке установки агента) и снимите комментарий с тех строк, которые соответствуют модулям программы, предполагаемым к использованию для мониторинга системы. Достаточно подробные описания параметров конфигурации приведены в документации плагина на странице **http://trac.nakednuns.org/nscp/wiki/doc/Configuration**.

При настройке конфигурации нужно исходить из принципа, что не следует включать больше опций, чем это необходимо в текущий момент. Например, если вы не планируете получать информацию посредством WMI-запросов, то и не стоит загружать модуль CheckWMI.dll.

Администраторам, не имевшим опыта работы с Nagios, обычно не удается правильно построить строку параметров запроса состояния Windows-системы. Поэтому обратите внимание на возможность запуска агента в диагностиче-

ском режиме. При этом вы сможете увидеть потенциальные ошибки в конфигурационном файле и отладить собственные запросы (рис. 9.12).

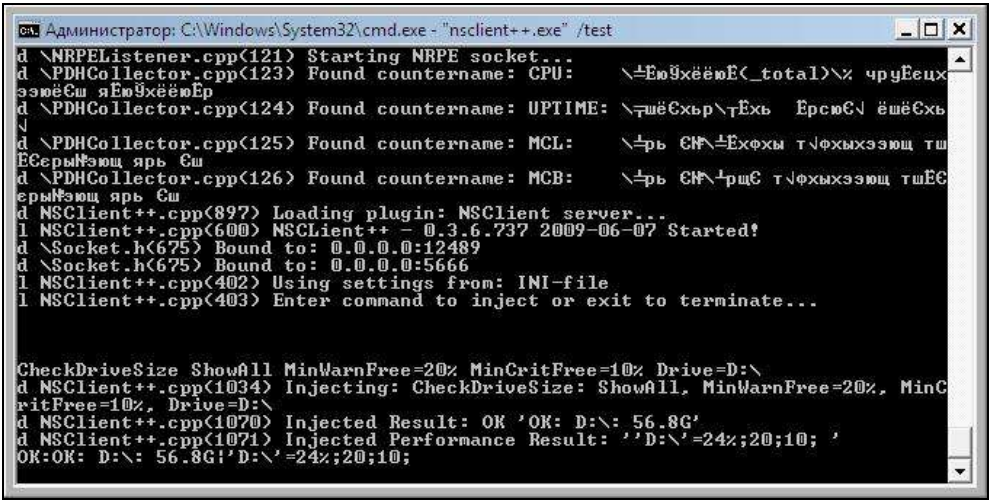


Рис. 9.12. Окно программы NSClient++ в диагностическом режиме

В диагностическом режиме в окне программы отражаются результаты выполнения операций контроля. Здесь вы можете увидеть и проанализировать причины ошибок. Кроме того, в этом окне можно осуществить разовый ручной запуск команды контроля.

Для запуска NSClient++ в диагностическом режиме достаточно выполнить в командной строке

```
NSClient++ /test
```

Примечание

Эту команду можно использовать для отладки службы даже без ее установки.

В окне NSClient++ вы сможете, во-первых, увидеть результаты загрузки всех модулей, а во-вторых, вводить собственные команды и видеть результаты выполнения как запросов со стороны сервера Nagios, так и локальных команд. На рис. 9.12 показано окно отладки плагина, в котором введена команда `CheckDriveSize ShowAll MinWarnFree=20% MinCritFree=10% Drive=D:\` и виден ответ системы.

Плагин NSClient++ позволяет контролировать параметры, приведенные в табл. 9.2. Подробности использования подробно описаны в технической документации (**http://trac.nakednuns.org/nscp/wiki/CheckCommands**)

и по имеющимся примерам легко составить собственные команды контроля состояния Windows.

Таблица 9.2. *Параметры, контролируемые NSClient++*

Параметр	Описание
`CheckFileSize`	Контролирует размер файла или папки
`CheckDriveSize`	Контролирует размер свободного или использованного пространства жестких или сменных дисков (тип диска можно выбирать в команде)
`CheckFile`	Контролирует файлы по критериям даты их создания, времени последнего доступа, записи в файл или по размеру файла
`CheckEventLog`	Ищет сообщения об ошибках в файле журнала. Поскольку таких сообщения обычно много, использование данного контроля сильно загружает систему
`CheckCPU`	Контролирует загрузку процессора в течение задаваемого периода времени
`CheckUpTime`	Контролирует время работы системы
`CheckServiceState`	Контролирует состояние службы Windows (критическое сообщение формируется в случае несоответствия фактического состояния службы заданному в качестве параметра в команде). Можно контролировать все службы одновременно с заданием исключения. В качестве названия службы нужно указывать то, которое отображается в свойствах службы (на рис. 9.13; выделено рамкой и стрелкой)
`CheckProcState`	Контролирует состояние процессов Windows. Фактически позволяет наблюдать за состоянием процесса, найденного по имени исполняемого файла. Можно контролировать также по числу одновременно запущенных процессов
`CheckMem`	Контролирует состояние виртуальной и физической памяти; доступен параметр количества записанных страниц памяти (commited pages)
`CheckCounter`	Контролирует значения счетчиков производительности. Объекты счетчиков желательно (для удобства использования) задавать в описаниях команд (служб)

Таблица 9.2 *(окончание)*

Параметр	Описание

`CheckAlwaysOK`
`CheckAlwaysCRITICAL`
`CheckAlwaysWARNING`
`CheckMultiple`
`CheckOK`
`CheckCRITICAL`
`CheckWARNING`
`CheckVersion`
	Так называемые *хэлперы*. Возвращают заранее определенное значение (какое — можно судить по названию команды). Применяются при настройке и отладке системы

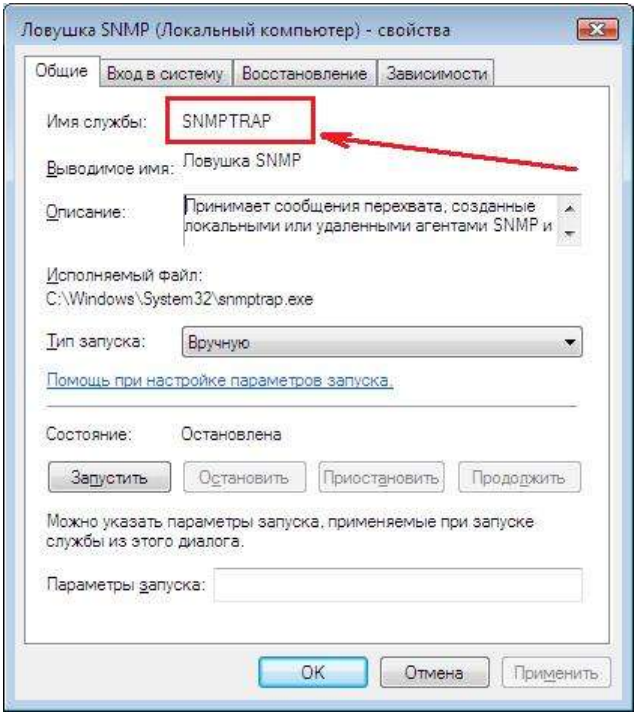


Рис. 9.13. Имя службы, которое следует указывать в настройках NSClient++

Перечисленным списком не ограничиваются возможности контроля Windows-систем. Вы можете добавить любое количество контролируемых параметров, например, за счет использования внешних сценариев (см. далее *разд. "Использование собственных программ мониторинга"*).

Мониторинг систем Windows может осуществляться на основе различных протоколов. Наиболее часто встречаются протоколы NSClient и NRPE. На практике можно применять любой из них, необходимо только включить/выключить соответствующие модули в файле настроек клиента (nsc.ini). В то же время, на взгляд автора, протокол NRPE несколько более гибок в использовании и обеспечивает шифрование данных обмена.

Примечания

Для "пассивного" мониторинга существует также протокол NSCA, о котором более подробно можно прочесть в онлайновой документации.

По умолчанию команда `check_nt`, использующая протокол NSClient, устанавливается на сервере Nagios. Чтобы работать по протоколу NRPE, на сервере Nagios следует установить плагин NRPE.

При использовании NRPE синтаксис команд строится следующим образом:

```
check_nrpe … -c <команда> -a <аргументы>
```

Например, проверить доступную физическую память можно так:

```
check_nrpe -H 192.168.0.9 -c CheckMem -a MaxWarn=70% MaxCrit=>80%
type=physical
```

При работе по протоколу NSClient потребуется другой синтаксис:

```
check_nt … -v <значение> -w <значение> -c <значение> -l <значение>
```

Проверку памяти, аналогичную описанной, можно было бы осуществить так:

```
check_nt -H 192.168.0.9 -p 12489 -v MEMUSE -w 70 -c 80
```

Замечание

По умолчанию check_nt использует порт номер 1248, а клиент, устанавливаемый в Windows, имеет настройку в файле конфигурации на порт 12489. Поэтому в данной команде мы явно указали номер порта. В случае сервера Nagios номер порта определяется в файле конфигурации *commands.cfg*.

Обратите внимание, что здесь указана не *команда* `CheckMem`, которая описана в документации на команды NSClient, а *переменная* `MEMUSE` (после ключа `v`). Чтобы узнать, какие переменные можно и нужно указывать в командной строке check_nt для контроля соответствующих параметров Windows-системы, необходимо ознакомиться с внутренней справкой команды, доступной при вызове команды с ключом `-h`:

```
check_nt -h
```

Примечание

Если в параметрах команд проверки необходимо указывать не точные значения порога, а, например, сравнение "больше или равно", то для этого придется разрешить в конфигурации клиента так называемые nasty_meta_chars (для символа < или >). Этот вариант не рекомендуется, предпочтительнее следующие сочетания: `gt` вместо >; `lt` вместо <; `ne` вместо != (или <>).

Настройка мониторинга серверов Linux

Как уже говорилось, работу серверов Linux контролируют с помощью плагина NRPE, причем на сервере Nagios он должен быть установлен как плагин, а на контролируемой системе Linux — в качестве демона. Для установки пригодна как подготовленная версия (такую установку лучше выполнять для контролируемых систем), так и исходные коды плагина.

Установка плагина NRPE из исходных кодов

Для установки NRPE необходимо скачать его последнюю версию с сайта **http://www.nagios.org/download/addons/**. На момент написания книги последней стабильной версией была NRPE 2.12, процесс установки которой мы и опишем далее.

Поскольку обмен данными с контролируемой системой осуществляется по защищенному каналу, то на сервер с Nagios необходимо предварительно установить OpenSSL. Делается это следующими двумя командами:

```
apt-get install openssl
apt-get install libcurl4-openssl-dev
```

Загруженный с сайта пакет NRPE необходимо распаковать и установить (листинг 9.13; такая установка выполняется на сервере Nagios).

Листинг 9.13

```
tar xzf nrpe-2.12.tar.gz
cd  nrpe-2.12/
./configure
make all
make install-plugin
```

Обратите внимание, чтобы по итогам выполнения команд конфигурирования и установки не было сообщений об ошибках.

Демон NRPE устанавливается аналогично (на всех контролируемых системах), только вместо последней операции (make install-plugin) необходимо выполнить (вторая команда позволяет установить демо-конфигурацию, которую можно будет отредактировать для упрощения настройки):

```
make install-daemon
make install-daemon-config
```

Установка NRPE из подготовленных пакетов для контроля Linux-системы

Для использования NRPE на контролируемой системе нужно установить его в режиме сервера (демона). Существует подготовленный пакет, который можно быстро установить программой apt-get:

```
apt-get install nagios-nrpe-server
```

Успешность установки демона можно проверить командой

```
netstat -an | grep 5666
```

Если NRPE работает, то порт 5666 должен им прослушиваться, о чем вы получите примерно такую информацию:

```
tcp   0   0 0.0.0.0:5666    0.0.0.0:*       LISTEN
```

После установки пакета необходимо отредактировать файл настроек. По умолчанию в данном случае настройки хранятся в папке /etc/nagios. В ней находится два файла: nrpe.cfg и nrpe_local.cfg. Первый файл лучше использовать только для смены глобальных параметров, а все локальные настройки меняйте в файле nrpe_local.cfg.

Обязательно смените адрес системы, с которой можно контролировать данный хост. Это параметр `allowed_hosts` в файле nrpe.cfg. По умолчанию разрешена только локальная работа (указан адрес 127.0.0.1).

В конфигурации необходимо определить все команды контроля, которые вам потребуются на данной системе. Чтобы избежать ошибок, желательно все необходимые настройки сразу прописывать в команде, чтобы не указывать параметры в строке вызова.

> ***Примечания***
>
> Если вы собираетесь использовать параметры, то необходимо разрешить эту опцию в файле глобальной настройки.
>
> Обратите внимание, что после установки NRPE в качестве демона или плагина, никакие дополнительные плагины в систему не инсталлируются. Поэтому образцы команд проверки, приведенные в файлах конфигурации, не будут работать.

Если вы предполагаете контролировать состояние с помощью плагина NRPE, то его необходимо также установить командой

```
apt-get install nagios-nrpe-plugin
```

Эта команда установит плагин в папку /usr/lib/nagios/plugins/. Именно этот путь и нужно будет указывать в командной строке. Обратите внимание, что синтаксис NRPE несколько отличается от описаний команд в Nagios. Команды необходимо определять в конфигурации по следующему образцу:

```
command[check_users]=<команда>
```

После завершения настроек конфигурации следует перезагрузить конфигурацию командой

```
/etc/init.d/nagios-nrpe-server reload
```

Установка дополнительных плагинов

Для Linux-систем существует множество плагинов (*см. разд. "Описание команд nagios"*), которые пригодны для контроля различных параметров системы. Необходимо только описать соответствующие команды и службы в конфигурациях Nagios.

Использование прокси-NRPE

Используя NRPE, можно на контролируемом хосте вызвать команду `check_nrpe` для проверки другого хоста. Таким способом можно контролировать некоторую подсеть через один компьютер. При такой организации контроля на хосте, функционирующем в качестве прокси, обязательно должны быть установлены как демон NRPE, так и плагин.

Вариантов передачи команды контроля может быть много. Вы можете разрешить использование аргументов и сообщать нужную командную строку непосредственно при исполнении запроса. Но лучше описать необходимые команды контроля в файле конфигурации. Это позволит уменьшить число ошибок и более безопасно контролировать сеть (поскольку при контроле будут запрещены параметры, не определенные заранее в файле конфигурации).

Команды, которые предназначены для контроля других систем, описываются в файле конфигурации демона NRPE (/etc/nagios/ nrpe_local.cfg). Причем в параметрах командной строки следует явно указать адрес удаленной системы. В этом случае, когда сервер Nagios вызовет на хосте такую команду, будет выполнена описанная в ней команда, но уже на удаленной системе.

Мониторинг журналов событий Windows

С помощью клиента NSClient++ (модуль CheckEventLog.dll) можно контролировать содержимое журналов Windows. Настройки параметров контроля, как правило, достаточно сложны для неподготовленного администратора, поскольку предполагают включение большого числа фильтров для отбора желаемых записей. Поэтому мы остановимся более подробно на синтаксисе модуля чтения журналов Windows.

Существует две стратегии отбора событий. Первая предполагает отбор *всех* событий, кроме явно указанных. Это фильтр `out`. При второй стратегии необходимо указывать критерии, по которым будут отбираться желаемые

сообщения (фильтр `in`). В обоих случаях необходимо также указывать параметр `filter=new` (это сделано для совместимости с предыдущими версиями).

> ***Примечание***
>
> Один и тот же результат отбора можно получить с помощью как первой, так и второй стратегии. В каждом случае оптимальный вариант нужно выбирать самому администратору.

Первая стратегия удобна, если контролируется, например, просто наличие записей о критических событиях в журнале системы. Вторая — если требуется отобрать записи, связанные с конкретным оборудованием или программной службой. Особо следует обратить внимание, что при второй стратегии программа ищет *первую удовлетворяющую условиям поиска запись*. Поэтому крайне важен порядок записи фильтров. Кроме того, обычно для ускорения работы агента рекомендуется сначала записывать те условия, которые *максимально сузят* зону поиска.

Структура фильтра приведена на рис. 9.14. Фильтр начинается всегда с ключевого слова `filter`, потом записывается режим фильтра (`filter mode`), потом — тип фильтра. Далее следует знак "равно", а только после него — оператор. Поэтому в случае, если фильтр задает точное совпадение (=), то в его записи необходимо указать *два* знака равно. Завершают строку фильтра оператор и значение, с которым происходит сравнение.

При определении команды обычно придерживаются такой последовательности: указывают анализируемые журналы (параметр `file`), тип фильтра (два параметра: первый `out` или `in`, второй — `new`), указывают границы для формирования предупреждений, записывают правила фильтрации и определяют дополнительную информацию, которая будет возвращена командой (время генерации, текст сообщений и т. д. — см. справочную документацию).

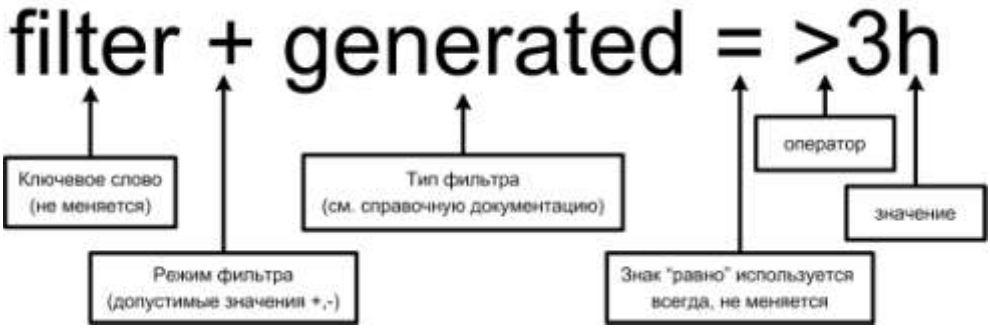


Рис. 9.14. Структура фильтра в Nagios

Основная проблема в реализации контроля журналов событий состоит в некорректном отображении текстов событий при работе с русскоязычными системами. Практически вы ограничены необходимостью работы только с источниками событий, датами, кодами возврата и т. п.

Подробно описание допустимых типов фильтров, опций и т. п. приведено на странице **http://trac.nakednuns.org/nscp/wiki/CheckEventLog/CheckEventLog**.

Мониторинг систем с использованием протокола SNMP

Nagios позволяет осуществлять контроль систем посредством протокола SNMP. SNMP — Simple Network Management Protocol — исторически первый протокол управления сетью. Устройства, которые допускают управление по протоколу SNMP, могут принимать из сети команды, выполнять их и передавать информацию о параметрах своей работы. Например, после получения сообщения о пропадании электроэнергии от управляемых аварийных источников питания по протоколу SNMP можно запросить данные об уровне зарядки аккумуляторных батарей и отложить отключение компьютеров до момента практически полной разрядки.

> ***Примечание***
>
> Существуют различные версии протокола SNMP (в настоящее время — первая, вторая и третья). Многие устройства, уже давно эксплуатируемые в сети, предполагают возможность управления только по версии 1.0. Данная версия не предусматривает никакой защиты, имена устройств передаются по сети в открытом виде, что легко позволяет перехватить их снифферами. Поэтому обращайте внимание на то, что имена (*community* в терминологии SNMP) ни в коем случае не должны оставаться в значениях по умолчанию, их следует хотя бы заменить на достаточно длинные и сложные названия. А интерфейсы управления такими устройствами желательно выделить в отдельную виртуальную сеть. Третья версия протокола уже предполагает как аутентификацию при подаче команды, так и шифрование трафика протокола SNMP.

SNMP в первую очередь применяется для управления активным сетевым оборудованием: маршрутизаторами и коммутаторами, аварийными источниками питания, модемами и т. п. Протокол SNMP можно использовать и для контроля компьютеров, если в системе установлена соответствующая служба. Но обычно число параметров, доступных для контроля через SNMP-протокол, существенно уступает другим технологиям контроля программных сред. Со списком субагентов, доступных для использования в операционных системах Windows, можно ознакомиться, например, на странице **http://support.microsoft.com/kb/237295/ru**.

Примечание

Современное активное оборудование в настройках по умолчанию не задействует протокол SNMP, его нужно включить соответствующими командами управления. В устройствах, находящихся в эксплуатации длительный период, данный протокол может быть включен. В любом случае состояние SNMP-управления устройства необходимо проверить штатными (для данного оборудования) средствами, например, по протоколу Telnet или через Web-интерфейс.

Все SNMP-совместимые устройства имеют стандартизованную конфигурацию параметров. Эта конфигурация представляет собой некое дерево идентификаторов: для доступа к какому-либо значению необходимо указать полный путь к нему от самого корня. Например, чтобы получить состояние порта коммутатора, нужно запросить значение для идентификатора .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOperStatus.101. Причем обычно разрешено опускать первую часть символов, одинаковых для контролируемых параметров (.iso.org.dod.internet.mgmt.mib-2.). Иными словами, при запросе административного состояния порта коммутатора было бы достаточно только указать interfaces.ifTable.ifEntry.ifOperStatus.101.

Замечание

Эти идентификаторы называются OID. Структура идентификаторов описывается в специальных файлах, которые называются MIB-файлами. Основная часть структуры стандартизована, но отдельные параметры описаны в проприетарных MIB-файлах (доступны к загрузке с сайтов разработчика оборудования). Интересующиеся читатели могут посетить страницу **http://www.mibdepot.com/index.shtml**, на которой собрано множество MIB как стандартных, так и разработки отдельных вендоров.

На рис. 9.15 показан интерфейс одной из программ просмотра MIB. С помощью таких программ можно найти название и цифровой индекс того параметра, значение которого предполагается контролировать в системе мониторинга.

В запросах Nagios допустимы не только символьные, но и численные наименования идентификаторов. Так, указанному выше параметру соответствует индекс .1.3.6.1.2.1.2.2.1.8.101. Причем именно цифровые идентификаторы рекомендуется применять для повышения производительности системы контроля.

Примечание

При использовании параметров, специфичных для данного вендора, необходимо загрузить соответствующий MIB-файл (параметр `-m` команды `check_snmp`). В этом случае отображаемая информация команды примет более читабельный вид.

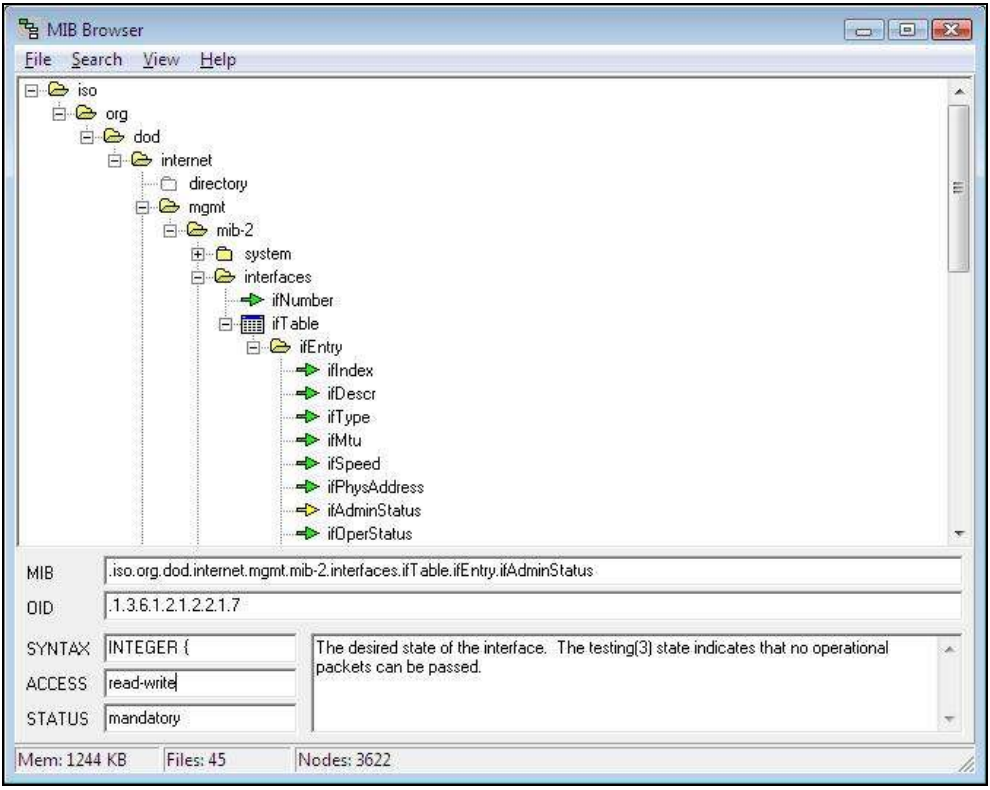


Рис. 9.15. MIB-browser

Для отображения структуры MIB создано много утилит просмотра, которые легко можно найти в Сети по ключевым словам "*mib browser*". Кроме того, на сетевых ресурсах легко найти аналогичные описания, в качестве примера можно указать страницу **http://support.ipmonitor.com/mibs_byoidtree.aspx**. На рис. 9.16 показана страница одного из сайтов с отображением глобальной структуры MIB. Такие источники помогают правильно выбрать контролируемые параметры.

SNMP-управляемые устройства могут как самостоятельно отправлять сообщения при возникновении каких-либо событий (эти сообщения называются *trap* — "трапами" на сленге IT-специалистов), так и отвечать на получаемые извне команды. В Nagios возможен как первый, так и второй способ. Но если для первого варианта (работа с трапами) необходимо установить пакет, который будет принимать эти сообщения и передавать их в Nagios, то модуль активного (со стороны Nagios-сервера) мониторинга уже включен в установку. Именно его использование мы и опишем далее в этом разделе.



Рис. 9.16. Глобальная структура MIB

ЗАМЕЧАНИЕ

Настройки, определяющие события, для которых формируются трапы, и системы, на которые отправляются оповещения, должны быть созданы администраторами контролируемых систем по правилам соответствующего оборудования.

Для работы с SNMP в Nagios должен быть установлен соответствующий плагин. Он включен в состав плагинов Nagios (установка их описана в настоящей книге в *разд. "Установка Nagios"*), но воспользоваться ими можно только в том случае, если предварительно был установлен пакет net-snmp.

Поэтому, если предполагается применение SNMP-модуля, данный пакет необходимо загрузить с сервера **http://net-snmp.sourceforge.net/**, после чего заново перекомпилировать плагины и повторно установить их.

Примечания

Автор рекомендует при новой установке сначала выполнить команду `make clean`, которая очистила бы настройки предыдущей инсталляции.

На сайте **http://net-snmp.sourceforge.net/** необходимый пакет представлен только в исходных кодах или в формате rpm. Удобнее переконвертировать формат пакета с помощью программы alien (см. *приложение*) командой `alien -d net-snmp-<версия>.rmp -scripts`.

После настройки возможности контроля по протоколу SNMP необходимо протестировать работоспособность на простейших запросах, например, проверить длительность работы устройства:

```
/usr/local/nagios/libexec/check_snmp -H <адрес_устройства>
-C <community> -o sysUpTime.0
```

В ответ вы должны получить примерно такое сообщение:

```
SNMP OK - Timeticks: (622339555) 72 days, 0:43:15.55 |
```

Замечание

В примерах использован протокол SNMP версии 1. В реальных условиях обычно встречается протокол версии 3, поэтому примеры необходимо дополнить параметрами аутентификации.

Команда `check_snmp` может запрашивать параметр, принимающий численное значение, и проверять соответствие его значения некоторому диапазону. Так, можно указать значения для состояния предупреждения и критического (ключи `-w` и `-c`) или диапазон значений (через двоеточие).

Внимание

Обратите внимание, что если вы хотите, чтобы, например, критическим значением интерпретировалось бы возвращаемое число в диапазоне от *a* до *b* (b > a), то диапазон нужно указывать ***b:a***. Если указать диапазон в "привычном" виде, как *a:b*, то если возвращаемое значение *попадает* в этот диапазон, результат будет считаться нормальным состоянием, а если не попадает — то как предупреждение или критическое состояние (в зависимости от указанного ключа).

Кроме того, команда может проверять возвращаемое строковое значение (значение, с которым проверяется ответ, следует указать в ключе `-s`) или даже выполнять проверку с использованием регулярных выражений (ключи `-r`, `-R`).

Также в запросе можно проверять сразу несколько параметров, перечисляя их OID через запятую, например, так:

```
//usr/local/nagios/libexec/check_snmp -H <адрес> -C <community> -o
.1.3.6.1.2.1.2.2.1.7.101,.1.3.6.1.2.1.2.2.1.7.102,.1.3.6.1.2.1.2.2.1.7.103
SNMP OK - 1 1 1 | iso.3.6.1.2.1.2.2.1.7.101=1 iso.3.6.1.2.1.2.2.1.7.102=
1 iso.3.6.1.2.1.2.2.1.7.103=1
```

Check_snmp снабжена подробной справкой (`check_snmp -h`), которая пригодится при составлении запросов к устройству. После того как запрос будет составлен и отлажен, достаточно описать новую команду в файле commands.cfg и добавить нужные службы в файлы описания контролируемых устройств. В Сети можно найти достаточное число примеров настройки Nagios для контроля устройств с использованием протокола SNMP, которые можно применить на практике. Так, по адресу **http://wiki.nagios.org/index.php/Howtos:snmp-apc-smart-ups** содержится описание настроек, с помощью которых можно контролировать состояние источников бесперебойного питания от APC (состояние батареи, параметры напряжения, температуру и т. д.).

Мониторинг Windows-систем на основе WMI

В состав NSClient++ входит модуль CheckWMI.dll, позволяющий контролировать Windows-систему с помощью инструментария WMI.

Windows Management Interface (WMI) — это технология управления Windows-компьютерами, реализующая стандарты Web-управления предприятием (WBEM, Web-based Enterprise Management). Хотя с помощью WMI можно выполнять и настройки системам, модуль CheckWMI обеспечивает лишь *получение* данных (аналогично режиму *только для чтения*). Если вы захотите выполнить какую-либо WMI-команду, то делать это следует путем создания WMI-сценария и исполнения его в интерпретаторе *wmic*.

> ***Примечания***
>
> WBEM разработан Distributed Management Task Force — **http://www.dmtf.org/**. В некотором смысле можно считать WMI "развитием" протокола SNMP для программных сред.
>
> Технология WMI реализована для всех операционных систем Windows, начиная с Windows 95. Однако устанавливается эта подсистема по умолчанию только в Windows Millennium Edition, Windows 2000, Windows XP, Windows Server 2003 и последующих операционных системах. Для других поддерживаемых версий Windows файлы установки доступны для бесплатной загрузки.

Практическое использование WMI для получения данных о состоянии оборудования или программной среды во многом напоминает работу с базой данных: вам необходимо указать, какие параметры должны быть получены

от какого объекта и при каких ограничениях (фильтрах). Язык запросов для WMI так и называют — WMI Query Language (WQL). Даже команды WQL принято называть *запросами*.

В Windows WMI выполняет функции сбора данных и управления конфигурацией компьютера через специализированные программные модули, называемые *провайдерами* (providers). Существуют провайдеры для управления драйверами Windows, операционной системой, Internet Explorer, Microsoft Office, службами каталогов и т. п. Этот список постоянно пополняется, и при установке на компьютер какого-либо программного обеспечения перечень управляемых объектов может существенно расшириться.

На практике для применения WMI для контроля системы нужно знать, какие классы и пространства имен доступны, какие названия имеют соответствующие элементы (*instance*). Полный перечень доступных к использованию в конкретной системе элементов WMI можно получить, например, с помощью средств WMI Object Browser и WMI CIM Studio, входящих в состав WMI Administrative Tools (рис. 9.17).

> ***ЗАМЕЧАНИЕ***
>
> Эти программы бесплатно можно загрузить с сайта по ссылке **http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=6430f853-1120-48db-8cc5-f2abdc3ed314**. Хотя, чтобы не набирать столь длинную строку, быстрее будет воспользоваться поиском на странице загрузки Microsoft по их названию.

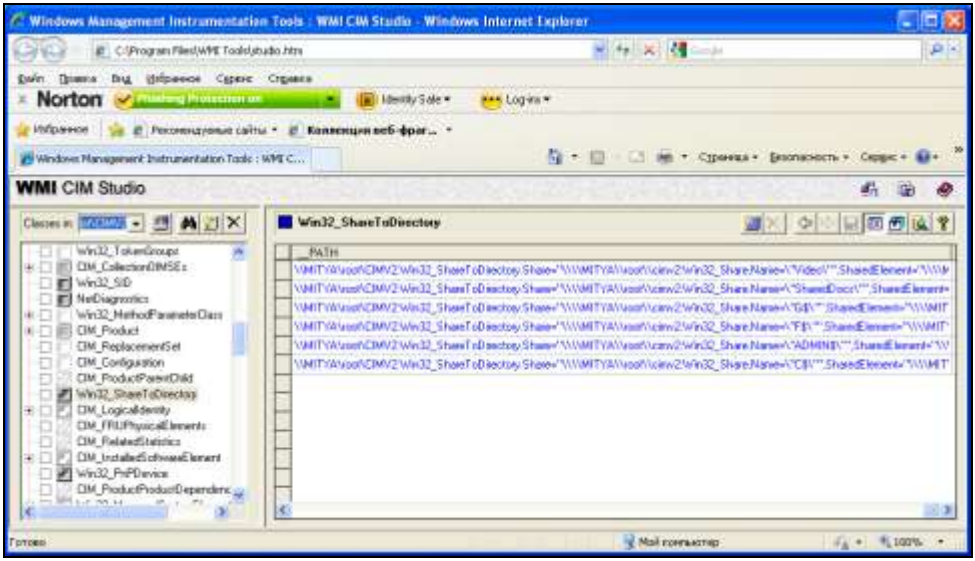


Рис. 9.17. Один из экранов WMI Administrative Tools

Для использования WMI необходимо знать иерархическую структуру объектов системы. Запомнить ее практически невозможно, поэтому при составлении запросов могут помочь такие продукты, как WMI CIM Studio. С помощью данной программы администратор имеет возможность подключиться к любому пространству имен, зарегистрированному в системе, отобразить существующие классы объектов, увидеть свойства класса (те характеристики, которые можно получить при исполнении запроса) и методы (те параметры, которые можно установить в команде), перечислить существующие экземпляры. Здесь же можно открыть окно, в котором попробовать создать собственный WMI-запрос и сразу увидеть его результаты. WMI Administrative Tools удобны тем, что наряду с просмотром существующих на компьютере классов WMI администратор может получить значения реальных объектов (на рисунке показано перечисление всех предоставляемых в совместный доступ папок на компьютере), составить и отладить WQL-запросы.

Эти утилиты отображают полный список существующих классов, значения их свойств и т. п. Часто требуется получить значения типовых характеристик, например, состояния служб, параметров физических или логических дисков и т. д. В этом случае можно воспользоваться подборкой уже готовых WMI-сценариев — программой Scriptomatic (бесплатно доступна к загрузке с сайта Microsoft по ссылке **http://www.microsoft.com/downloads/details.aspx?familyid=09DFC342-648B-4119-B7EB-783B0F7D1178&displaylang=en**).

> ***Замечание***
>
> Доступна также и подборка бесплатных сценариев TechNet Script Center Sample Scripts — **http://www.microsoft.com/downloads/details.aspx?familyid=B4CB2678-DAFB-4E30-B2DA-B8814FE2DA5A&displaylang=en**. Большая подборка решений представлена в TechNet Script Repository и т. д.

Scriptomatic (рис. 9.18) позволяет найти сценарий, с помощью которого можно получить желаемые сведения о работе системы, и на его основе составить WQL-запрос для использования в CheckWMI. Утилита содержит большую подборку готовых сценариев, пригодных для составления необходимых запросов.

Теперь, когда мы получили общее представление о WMI, можно перейти к реализации этой технологии в Nagios.

Модуль CheckWMI фактически состоит из двух подмодулей: CheckWMIValue и CheckWMI. CheckWMIValue оптимизирован для контроля численных значений, например, текущей загруженности процессора (это число процентов загрузки) или разрешения монитора (число пикселов) и т. п. В этой команде вы можете просто указать контролируемые параметры и минимальные/максимальные допустимые для них значения, например, так:

```
CheckWMIValue "Query=Select PelsWidth from win32_DisplayConfiguration"
MinCrit=640 MinWarn=800 Check:Width=PelsWidth
```

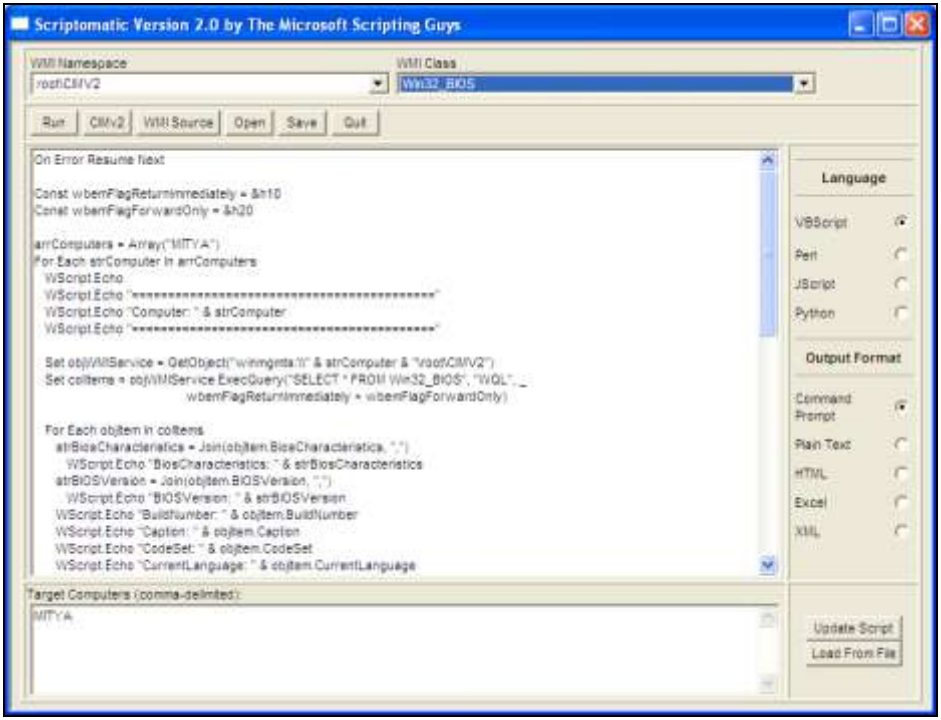


Рис. 9.18. Утилита Scriptomatic 2.0

Приведенная команда составлена для работы в режиме отладки (*nsclient++ /test*). Она запрашивает разрешение дисплея по горизонтали и сообщает о критическом состоянии в случае, если оно равно или менее 640, и выдает предупреждение, если значение не превосходит 800. Из особенностей применения этой команды отметим, что после строки запроса (которая заключена в кавычки) нужно писать параметры минимальных/максимальных значений и только потом указывать название параметра, который контролируется командой (PelsWidth). Поясним также опцию `Check`, указанную в командной строке. После `Check` необходимо вписать название параметра, которое будет применяться в системе контроля (можно сохранить и название из описания в WMI, но часто более удобно ввести собственное название), и название, соответствующее объекту класса (то, которое отображается, например, в утилите просмотра WMI Object Browser).

Другие примеры (в том числе в вариантах для конфигурации Nagios) приведены на странице **http://trac.nakednuns.org/nscp/wiki/CheckWMIValue**.

Модуль CheckWMI потребуется в тех случаях, когда предполагается либо анализ строкового параметра, возвращаемого в результате WMI-запроса,

либо запрос нескольких значений. При использовании CheckWMI строки запроса несколько усложняются из-за необходимости применения фильтров. Синтаксис CheckWMI описан на странице **http://nsclient.org/nscp/wiki/CheckWMI/CheckWMI**. По своему построению запросы CheckWMI сходны с фильтрами анализа журналов работы системы, которые описаны в настоящей книге.

Мониторинг коммутационного оборудования

Активное оборудование сети — коммутаторы, концентраторы, модемы и т. п. контролируются по протоколу SNMP (управляемые модели). Технологии, описанные в *разд. "Мониторинг систем с использованием протокола SNMP"*, позволяют получать состояния портов оборудования, выдавать предупреждения при возникновении на портах некоторого числа ошибок передачи пакетов, наблюдать за температурой устройства и количеством VPN-сессий. Нужно только выбрать соответствующие идентификаторы по описанию для мониторинга по протоколу SNMP. В большинстве случаев этого достаточно для контроля.

Однако, кроме указанных параметров, администраторы часто хотят знать реальную загрузку оборудования, фактическое использование полосы пропускания. Эти значения нельзя получить, запрашивая тот или иной параметр состояния оборудования. Их вычисляют на основе анализа периодически получаемых данных. Специально для такого мониторинга создана одна из самых популярных программ — MRTG. Ее возможности обработки параметров коммутаторов используются в Nagios.

MRTG собирает статистику по протоколу SNMP с активного оборудования, которая при помощи плагина check_mrtgtraf впоследствии передается в Nagios для отображения.

Установить MRTG можно командой `apt-get`:

```
apt-get install mrtg
```

После установки для пакета необходимо создать файлы настроек, в которых указать устройства и значения параметров, которые программа будет собирать. Эти настройки следует привести в файле /etc/mrtg.conf. Формирование конфигурации MRTG — достаточно сложная задача, поэтому в пакете предусмотрена специальная программа, которая автоматически опросит устройство и сформирует файл конфигурации — `cfgmaker`. При ее запуске в качестве параметров нужно указать строку *community* и адрес устройства. Вывод программы следует перенаправить в файл, значения из которого потом мы про-

сто импортируем в файл настроек. В качестве имени такого файла удобно указать имя (или адрес) опрашиваемого устройства:

```
cfgmaker community@адрес > /etc/mrtg/адрес.cfg
```

При формировании конфигурации программа закомментирует блоки, относящиеся к временно отключенным портам. Вы можете потом включить эти блоки, удалив комментарий (символ # в начале соответствующих строк).

По итогам работы `cfgmaker` достаточно только оставить в файле конфигурации те блоки данных, которые предполагается анализировать для конкретного устройства. Учитывая, что по информации файла программа создает заголовки и служебные описания на страницах графика, имеет смысл откорректировать названия и описания тех позиций, которые предполагается отображать на графиках. Поскольку анализировать пропускную способность по портам, к которым подключены оконечные устройства (серверы, рабочие станции) не имеет смысла, то целесообразно сохранить мониторинг пропускной способности только для магистральных портов (портов, которые подключены к другим коммутаторам или концентраторам).

После редактирования файла настроек можно запустить программу `mrtg`, указав в качестве параметра конфигурацию устройства. Для систем с кодировкой UTF-8 команда запуска будет выглядеть так:

```
env LANG=C /usr/bin/mrtg /etc/mrtg.cfg
```

При первых двух запусках с новой конфигурацией вы получите предупреждения от команды; это нормально, поскольку в системе не сформированы еще файлы журналов, с которыми работает данная утилита.

При установке пакета MRTG в системе настраивается автоматический сбор информации с коммутаторов раз в пять минут. При желании этот период можно увеличить, если отредактировать соответствующим образом файл /etc/cron.d/mrtg.

Автоматический запуск MRTG осуществляется с конфигурацией, сохраненной в файле /etc/mrtg.cfg. Если вы предварительно тестировали настройки с использованием файла для конкретного устройства, то их необходимо импортировать в /etc/mrtg.cfg. Сделать это можно, например, следующей командой:

```
cat <индивидуальный_файл_настроек> >> /etc/mrtg.cfg
```

По умолчанию MRTG записывает данные, полученные с коммутаторов, в журналы в папке /var/www/mrtg. Имена журналов начинаются с адресов контролируемых устройств, для каждого порта устройства программа создает отдельный файл журнала.

Примечание

Графики производительности по отдельным портам устройств можно просмотреть, если открыть в обозревателе папку **http://nagiosserver/mrtg/** и выбрать соответствующий файл. При желании с помощью команды `indexmaker` можно сформировать общий индексный файл для упрощения отображения. Необходимые ключи для формирования файла легко уточнить по справочной информации после вызова `indexmaker -h`.

После этих шагов можно собирать данные с устройств командами `Nagios check_mrtg` и `check_mrtgtraf`. Команда `check_mrtgtraf` требует указания следующих параметров:

```
check_mrtgtraf -F <имя_файла_журнала> -a <AVG | MAX> -w входящий,
исходящий-с входящий,исходящий -e период_устаревания
```

В этом примере параметр `-a` указывает, будет ли браться в учет максимальное значение (MAX) за период анализа или же программа оценит среднее значение (AVG). После ключей `w` и с указывают пары лимитов для исходящего и входящего трафика по данному порту. Порт, по которому система будет контролировать данные, определяется выбранным файлом журнала.

К стандартным командам Nagios относится `check_local_mrtgtraf`, позволяющая описать службы контроля производительности портов. Поскольку MRTG формирует необходимые страницы графиков, то можно не создавать описания для пакета nagiosgraph, а просто сослаться на эти файлы (листинг 9.14).

Листинг 9.14

```
define service{
       use                     generic-service
       host_name               DES_3550
       service_description     Bandwidth_Usage
       check_command
check_local_mrtgtraf!/var/www/mrtg/192.168.0.19_1_49.log!AVG!10000000,
10000000!50000000,50000000!10
}

define serviceextinfo{
       host_name               DES_3550
       service_description     Bandwidth_Usage
       notes_url               /mrtg/192.168.0.19_1_49.html
}
```

На рис. 9.19 приведен пример графика, формируемого пакетом `mrtg`. Это реальный график, сформированный пакетом `mrtg` со значениями по умолчанию. На графике представлены усредненные значения полосы пропускания за некоторый период (видны за 5 мин и за неделю).

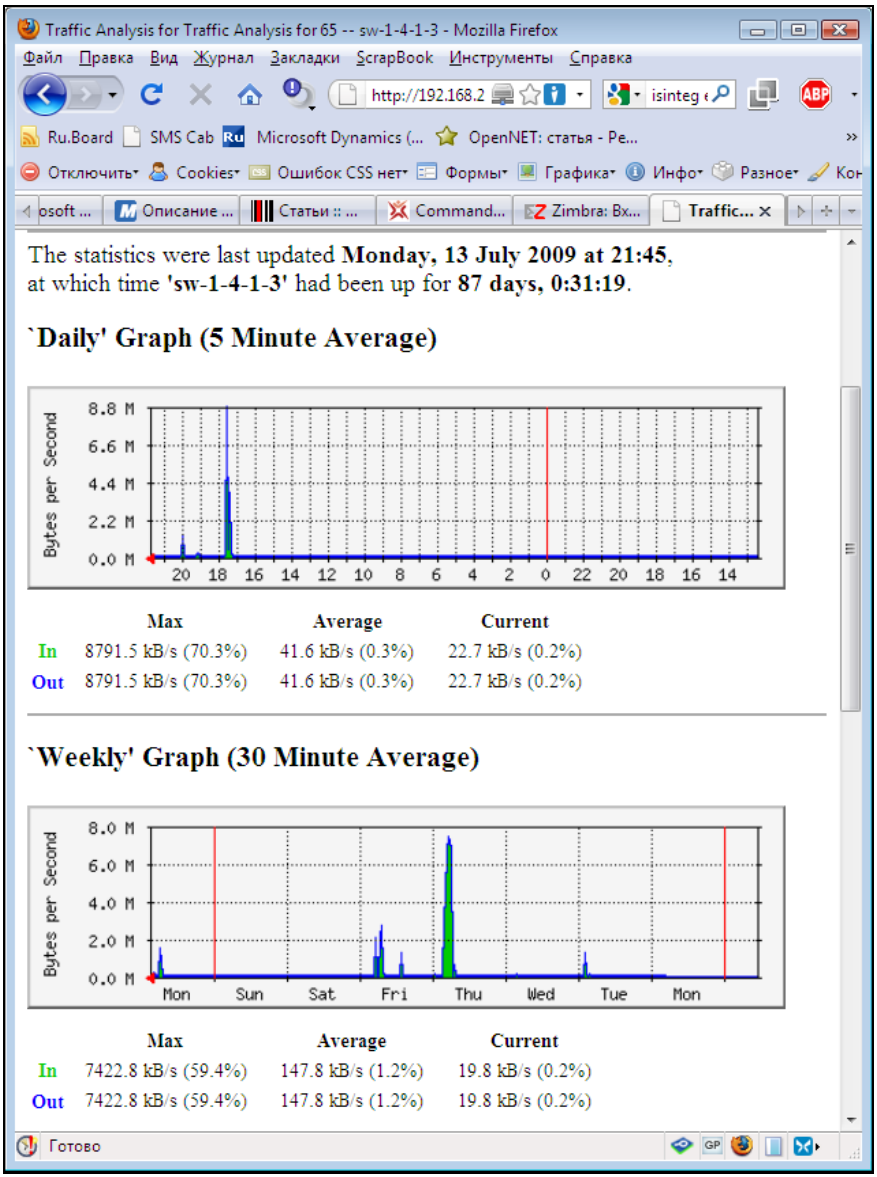


Рис. 9.19. График загрузки порта коммутатора

Использование собственных программ мониторинга

Nagios позволяет легко создать собственные плагины для мониторинга любой системы. Это могут быть любые исполняемые файлы. Необходимо только обеспечить, чтобы они сообщали код завершения работы в соответствии с табл. 9.3.

Таблица 9.3. *Коды возврата программ мониторинга системы для Nagios*

Возвращаемый код	Значение для Nagios
0	Нормально (OK)
1	Предупреждение (Warning)
2	Критическое значение (Critical)
3	Неопределенное значение (Unknown)

Листинг 9.15 иллюстрирует пример сценария для Ubuntu.

Листинг 9.15

```
#!/bin/sh
if <некоторое проверяемое условие>
then
  exit 0
else
   exit 2
fi
```

В случае создания сценария на VisualBasic под Windows его можно оформить так, как в листинге 9.16.

Листинг 9.16

```
Dim status
status = 0
if <некоторое проверяемое условие> then
```

```
wscript.echo <здесь может быть выводимое дополнительно сообщение
предупреждения>
status = 1
elseif <некоторое проверяемое условие>  then
wscript.echo <здесь может быть выводимое дополнительно критическое
сообщение>
status = 2
else
status = 0
end if
wscript.quit(status)
```

В качестве собственных программ мониторинга администраторам проще всего использовать сценарии на одном из известных им языках программирования, например, на VisualBasic или PowerShell. Обычно собственные сценарии пишут на основе небольшой модернизации готового кода, найденного в Сети. Так, по ссылке **http://www.microsoft.com/technet/scriptcenter/scripts/msh/default.mspx?mfr=true** вы найдете большую библиотеку сценариев PowerShell на сайте Microsoft, а страница **http://www.microsoft.com/technet/scriptcenter/scripts/default.mspx?mfr=true** позволит найти сценарий, с помощью которого можно проконтролировать системы на основе Windows Server 2008, Windows Server 2003, Windows Vista, Windows XP и Windows 2000.

При создании сценариев необходимо учитывать, что запускаться они будут от имени службы агента мониторинга. По умолчанию эта служба имеет максимальные права для локальной системы, но не может взаимодействовать с компьютерами сети. Если вы предполагаете с помощью сценариев собирать данные с других компьютеров, то необходимо либо включать технологии имперсонализации, либо запускать агент под другой учетной записью.

Отображение собранных данных на графиках

Команды Nagios, при помощи которых контролируются системы, возвращают не только состояние (хорошо или плохо), но и данные по конкретным параметрам (например, процент загрузки диска или число вошедших в систему пользователей). Эти данные по умолчанию не сохраняются, но могут быть использованы, например, для прорисовки графиков соответствующих служб.

Для реализации такой возможности необходимо установить дополнительный плагин. Один из наиболее популярных плагинов для создания графиков в Nagios — пакет `nagiosgraph`, доступный к загрузке с сайта **http://sourceforge.net/projects/nagiosgraph/**. На момент создания книги это была версия 1.3.0, которую мы и рассмотрим в дальнейших примерах.

Как это работает

Как уже говорилось, команды Nagios возвращают данные о производительности контролируемых систем. После внесения настроек в файлы конфигурации эти данные сервер начинает сохранять в файле. Плагин nagiosgraph устанавливает сценарий, который просматривает данный файл и разбирает строки с данными по правилам, содержащимся в его настройках. А именно как разбирать данные каждой службы, описано в файле map, а куда сохранить — в файлах hostdb.conf и servdb.conf. Данные записываются в циклические базы, создаваемые для каждой службы. График формируется специальным пакетом `rrdtools` из этих баз на основе специального запроса.

Для включения в интерфейс nagios пиктограммы, щелчком по которой можно отобразить график для соответствующей службы, вносят изменения в описания служб (для каждой службы добавляют блоки *serviceextinfo*).

> ***Примечание***
>
> Nagiosgraph отслеживает по умолчанию только данные о производительности основных служб. Для отображения произвольной службы необходимо создать описания по образцу, содержащемуся в файлах /etc/nagios/nagiograph/hostdb.conf, /etc/nagios/nagiograph/servdb.conf и /etc/nagios/nagiograph/map.

Установка Nagiosgraph

Пакет `nagiosgraph` требует наличия в системе пакетов perl, rrdtool, librrds-perl, которые необходимо предварительно установить командой `apt-get install` (кроме указанных при установке будут загружены и связанные с ними пакеты). Затем необходимо загрузить пакет `nagiosgraph` и сохранить его в какой-либо папке.

> ***Замечание***
>
> Рекомендуемая папка /usr/local/src; выбор папки не имеет принципиального значения.

Разархивируйте загруженный файл и перейдите в созданную папку:

```
tar xvzf nagiosgraph-1.3.0.tar.gz
cd nagiosgraph-1.3.0/
```

Пакет устанавливается стандартно при помощи сценария install.pl, находящегося в этой папке. А действия, выполняемые этим сценарием, описаны в файле INSTALL. Для правильной работы сценария необходимо будет ответить на несколько вопросов, касающихся расположения файлов настроек и данных. Поскольку неопытному пользователю в первый раз достаточно сложно сделать верный выбор, опишем кратко необходимые для ручной установки действия с небольшими пояснениями.

Скопируйте содержимое папки etc в папку, где будут храниться настройки пакета nagiosgraph. Поскольку эти настройки задействованы в сценариях пакета, то, чтобы избежать лишней ручной правки конфигураций, создайте папку /etc/nagios/nagiosgraph и скопируйте файлы именно в нее.

Содержимое папки lib скопируйте в папку /usr/local/nagios/sbin. Именно эта папка при настройках по умолчанию определена как папка cgi-bin Web-интерфейса nagios. Файл share/action.gif скопируйте в папку /usr/local/nagios/share/images, файл share/nagiosgraph.css — в папку /usr/local/nagios/share/stylesheets и файл share/nagiosgraph.js — в папку /usr/local/nagios/share (это папки Web-сервера Nagios).

Создайте папку /usr/local/nagios/nagiosgraph/rrd и назначьте на нее полные права для пользователя nagios:

```
mkdir -p /usr/local/nagios/nagiosgraph/rrd
chown -R nagios.nagios /usr/local/nagios/nagiosgraph
chmod 2775 /usr/local/nagios/nagiosgraph
```

Создайте файл журнала для пакета nagiosgraph и назначьте ему права:

```
touch /var/log/nagiosgraph.log
chown nagios.nagios /var/log/nagiosgraph.log
chmod 664 /var/log/nagiosgraph.log
```

Проверьте, что в файле /etc/nagios/nagiosgraph.conf строки, описывающие расположение файлов, указывают на те папки, которые вы использовали на предыдущих шагах.

Теперь необходимо изменить настройки самого Nagios, чтобы он начал сохранять данные. Для этого откройте в редакторе файл /usr/local/nagios/etc/nagios.cfg, найдите указанные ниже строки, раскомментируйте их и исправьте значения в необходимых случаях (листинг 9.17).

Листинг 9.17

```
process_performance_data=1
service_perfdata_file=/var/spool/nagios/perfdata.log
service_perfdata_file_template=$LASTSERVICECHECK$||$HOSTNAME$||
$SERVICEDESC$||$SERVICEOUTPUT$||$SERVICEPERFDATA$
service_perfdata_file_mode=a
service_perfdata_file_processing_interval=30
service_perfdata_file_processing_command=process-service-perfdata
```

В файле /usr/local/nagios/etc/objects/commands.cfg измените описание команды сбора данных (process-service-perfdata). Ее вид иллюстрирует листинг 9.18.

Листинг 9.18

```
define command {
       command_name  process-service-perfdata
       command_line  /usr/lib/nagios/insert.pl
     }
```

После этих шагов осталось настроить только Web-интерфейс. Во-первых, необходимо указать в Web-сервере настройки папки со сценариями пакета nagiosgraph. Для этого откройте в редакторе файл /etc/apache2/conf.d/nagios.conf и вставьте в его конец блок, приведенный в листинге 9.19 (для быстроты можно скопировать аналогичный блок для другой папки nagios и изменить только пути к соответствующей папке).

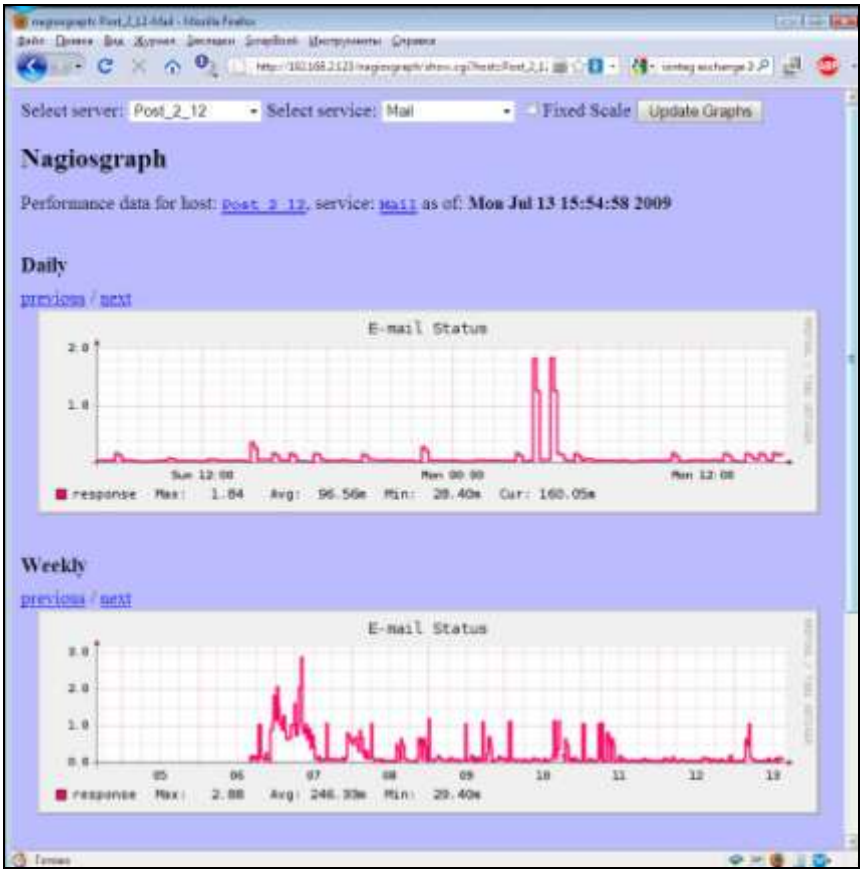


Рис. 9.20. Пример графика производительности, построенный пакетом `nagiosgraph`

Листинг 9.19

```
ScriptAlias /nagiosgraph/ /usr/lib/nagios/cgi-bin/
<Directory "/usr/lib/nagios/cgi-bin">
#  SSLRequireSSL
   Options None
   AllowOverride None
   Order allow,deny
   Allow from all
#  Order deny,allow
#  Deny from all
#  Allow from 127.0.0.1
   AuthName "Nagios Access"
   AuthType Basic
   AuthUserFile /opt/nagios/etc/htpasswd.users
   Require valid-user
</Directory>
```

На рис. 9.20 представлен пример одного из графиков, который формирует пакет `nagiosgraph`.

Редактирование интерфейса Nagios

Для того чтобы рядом с названием контролируемой службы расположить иконку перехода на показ графиков ее данных, необходимо дополнить описания служб Nagios. Для каждой контролируемой службы, для которой вы собираетесь отображать графические данные, создайте блок описания *serviceextinfo*, в котором должны повторяться параметры `host_name` и `service_description` и появиться новый параметр — `notes_url`. Параметр `notes_url` должен формироваться по следующим правилам:

```
/nagiosgraph/show.cgi?host=$HOSTNAME$&service=$SERVICEDESC$&db=
load,avg1min,avg5min,avg15min&geom=500x100&rrdopts=%2Dl%200%20%2Du
%2010%20%2Dt%20CPU%2DLoad
```

Начало этого параметра стандартно для всех служб:

```
/nagiosgraph/show.cgi?host=$HOSTNAME$&service=$SERVICEDESC$.
```

Это путь к сценарию, имя контролируемой системы и название службы. В большинстве случаев для определения достаточно только этой части строки. В этом случае nagiosgraph отобразит списки выбора в верху страницы.

Параметр `db` задает базу, из которой берутся данные для формирования графика (load), и названия колонок (avg1min, avg5min, avg15min). Для других

служб соответствующие данные можно уточнить по файлам /etc/nagios/nagiograph/hostdb.conf, /etc/nagios/nagiograph/servdb.conf (название базы) и /etc/nagios/nagiograph/map (названия параметров).

Ключ `geom` задает размеры графика, а после параметра `rrdopts` можно указать дополнительные параметры, например, названия осей, верхнюю и нижнюю границы осей, названия графика и т. п. Перечень всех допустимых параметров для `rrdopts` можно уточнить на странице **http://oss.oetiker.ch/rrdtool/doc/rrdgraph.en.html**. В нашем примере указаны границы значений оси y (`-l` — нижняя граница, `-u` — верхняя граница) и название графика (CPU-Load).

> ***Замечание***
>
> Для URL-строк пробел нужно заменить на `%20`, а тире — на `%2D`. Фактически написана следующая строка: `rrdopts=-l 0 -u 10 -t CPU-Load`.

Таким образом, описание служб должно выглядеть примерно так, как в листинге 9.20. Сначала указан уже существующий блок описания, потом — новый блок с описанием `serviceextinfo` для службы, приведенной в этом примере.

Листинг 9.20

```
...
define service{
       use                     local-service
       host_name               localhost
       service_description     Current Load
       check_command           check_local_load!5.0,4.0,3.0!10.0,6.0,4.0
       }


define serviceextinfo{
       host_name               localhost
       service_description     Current Load
       notes_url
/nagiosgraph/show.cgi?host=$HOSTNAME$&service=
$ SERVICEDESC$&db=load,avg1min,avg5min,avg15min&geom=500x100&rrdopts=
%2Dl%200%20%2Du %2010%20%2Dt%20CPU%2DLoad
       }
...
```

Завершение установки

Для завершения установки и вступления изменений в силу перезапустите nagios и Web-сервер:

```
/etc/init.d/apache2 restart
/etc/init.d/nagios restart
```

Создание графиков новых служб

В конфигурациях nagiosgraph представлены настройки для основных контролируемых служб. Если вы захотите включить в Nagios графическое отображение параметров работы какой-либо службы, созданной вами, то настройки nagiosgraph необходимо дополнить.

Во-первых, добавьте в файл servdb.conf (hostdb.conf) название вашей службы и сопоставьте ему название новой RRD-базы. Во-вторых, и это самое сложное, необходимо отредактировать файл map так, чтобы сценарий insert.pl смог правильно разобрать строку данных. Разбор строки осуществляется с использованием регулярных выражений в соответствующем правиле. Поэтому от вас потребуется достаточно серьезное изучение синтаксиса регулярных выражений, чтобы правильно составить нужный запрос. Помощь при составлении запроса могут оказать другие примеры, содержащиеся в этом файле.

> ***Примечание***
>
> Не забывайте, что в настройках nagiosgraph имеются параметры, позволяющие включить разные уровни отладки, которые помогут быстрее найти и исправить возможные ошибки.

Автоматическое реагирование на сбои в работе контролируемых систем

Как уже говорилось в *разд. "Описание контролируемых систем в Nagios"*, в параметрах конфигурации хоста можно указывать команду, которая должна выполниться при возникновении критической ситуации. По умолчанию Nagios отправляет сообщения по электронной почте (или иным описанным в конфигурации способом) операторам, закрепленным в конфигурации для данного типа хоста. Это сообщение отправляется в случае, когда Nagios окончательно фиксирует состояние аварии. Если вы помните, то в параметрах конфигурации контроля можно задать несколько повторных проверок состояния через некоторый промежуток времени. Именно после выполнения *всех* проверок и подтверждения состояния предупреждение будет выслано.

Но команда, заданная параметром `event_handler`, будет исполнена уже по получении *первого* результата, свидетельствующего об ошибках в работе систем.

Понятно, что подобные команды реагирования уникальны и должны создаваться индивидуально для каждой контролируемой службы. В качестве примера приведем сценарий со страницы **http://vadimszenins.blogspot.com/2008/12/nagios-restart-windows-failed-services.html**, который осуществляет перезапуск остановившейся службы в Windows 2003 Server (листинг 9.21).

Листинг 9.21

```
    @echo on
    :: ************************************************
    :: File: win_service_restart.cmd
    :: Author: Vadims Zenins http://vadimszenins.blogspot.com
    :: Version: 1.04
    :: Date: 20/04/2009 17:41
    :: Windows Failed Service restart batch file for Nagios Event Handler
    ::
    :: Copy win_service_restart.cmd to \NSClient++\scripts\ folder.
    ::
    :: Nagios commands.cfg:
    :: define command{
    :: command_name win_service_restart
    :: command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -p 5666 -c
win_service_restart -a "$SERVICEDESC$" $SERVICESTATE$ $SERVICESTATETYPE$
$SERVICEATTEMPT$
    :: }
    ::
    :: Nagios template-services_common-win.cfg
    :: define service{
    :: name generic-service-win-wuauserv
    :: service_description wuauserv
    :: display_name Automatic Updates
    :: event_handler win_service_restart
    :: event_handler_enabled 1
    :: check_command check_nt!SERVICESTATE!-d SHOWALL -l $SERVICEDESC$
    :: }
    ::
    :: NSCLIENT++ NSC.ini:
    :: [NRPE]
    :: allowed_hosts=192.168.1.1/32 ; your Nagios server IP
    :: allow_arguments=1
    :: [External Script]
    :: allow_arguments=1
```

```
    :: allow_nasty_meta_chars=1
    :: [NRPE Handlers]
    :: command[win_service_restart]=scripts\win_service_restart.cmd
"$ARG1$" $ARG2$ $ARG3$ $ARG4$
    ::
    :: Version 1.04 revision:
    :: Double restart of the service is fixed
    :: Version 1.03 revision:
    :: Description is changed
    :: Version 1.02 revision:
    :: @NET changed to @SC
    :: Version 1.01 revision:
    :: Service name's with space problem is fixed
    ::
    :: This code is made available as is, without warranty of any kind.
The entire risk
    :: of the use or the results from the use of this code remains with
the user.
    :: ***********************************************

    ::echo 1: %1 2: %2 3: %3 4: %4

    @SETLOCAL ENABLEEXTENSIONS ENABLEDELAYEDEXPANSION
    FOR %%I IN ( "%0" ) DO SET SCRIPTNAME=%%~nxI
    :: Replace "
    SET SCRIPTNAME=%SCRIPTNAME:"=%
    SET LOGDIR=C:\tools\logs
    SET SERVICENAME=%1
    :: Replace "
    SET SERVICENAME1=%SERVICENAME:"=%
    SET LOGFILE=%1
    SET LOGFILE=%LOGFILE:"=%
    :: Replace space by _
    SET LOGFILE=%LOGFILE: =_%
    SET LOGFILE=%LOGDIR%\%LOGFILE%.log
    if "%SERVICENAME1%"=="" SET LOGFILE=%LOGDIR%\NO_SERVICENAME.log
    ::@echo servicename: %SERVICENAME%
    ::@echo logfile: %LOGFILE%
    ::@echo SERVICENAME1: %SERVICENAME1%
    :: ============================================================
    if not exist %LOGDIR% md %LOGDIR%
    echo ===================== >> %LOGFILE%
```

```
echo %DATE% %TIME% %SCRIPTNAME% has started >> %LOGFILE%
@if "%SERVICENAME1%"=="" goto usage
@if "%SERVICENAME1%"=="/?" goto usage
@if "%SERVICENAME1%"=="-?" goto usage
::@echo Variables: %1 %2 %3
@echo Variables 1: %1 2: %2 3: %3 4: %4 >> %LOGFILE%
@SC query %SERVICENAME% >> %LOGFILE%
@SC query %SERVICENAME% | FIND /I "RUNNING" 2>>&1
if .%ERRORLEVEL%.==.0. goto END
:RESTART
@echo %DATE% %TIME% Restarting %SERVICENAME% services... >> %LOGFILE%
@net stop %SERVICENAME% /y >> %LOGFILE%
@sleep 5
@net start %SERVICENAME% >> %LOGFILE% 2>>&1
@goto end
:USAGE
@echo Usage: >> %LOGFILE%
@echo win_service_restart "^" ^ ^ ^ >> %LOGFILE%
@echo ^ is "Service name", dont't mix with "Display name" >> %LOGFILE%
@echo ^, ^ and ^ are optional >> %LOGFILE%
::exit 64
:END
echo %DATE% %TIME% %SCRIPTNAME% has finished >> %LOGFILE%
@echo %SCRIPTNAME% has finished
@echo. >> %LOGFILE%
exit 0
```

Код сценария содержит все необходимые комментарии по описаниям службы и хоста (строки комментариев начинаются со знаков двоеточия), так что читателю не составит большого труда разобраться с особенностями использования такого способа реагирования на состояния систем и применить его в собственных системах. Тем не менее, дадим некоторые пояснения.

После проверок синтаксиса вызова сценария, программа запрашивает состояние службы с помощью команды `SC` из состава Windows 2003 Server и ищет в ее результатах слово `running`. Если служба не запущена, то сценарий пытается перестартовать ее, выполняя команды останова и запуска службы. Все действия сценария протоколируются в журнале, который сохраняется в папке C:\tools\logs (папка создается при ее отсутствии).



Глава 10

Поиск и устранение неисправностей

Отказы в работе информационных систем неизбежны. Главное для администратора — быть подготовленным к любому отказу и не терять голову при любой аварии. Если произошел отказ, не спешите сразу же что-то предпринимать. Попробуйте успокоиться, может быть, выпить кофе, подумать.

Прежде всего, попытайтесь получить максимум информации о неисправности как от пользователей, так и по данным объективного контроля. Составьте предварительный перечень возможных причин отказа с оценкой времени устранения по каждой позиции. Старайтесь не начинать ремонт с наиболее затратных позиций, если только вы абсолютно не уверены, что именно они явились причиной неисправности.

Протоколируйте все свои шаги. Часто, если систему не удается восстановить за короткое время, без таких записей очень сложно вернуться к начальной точке. Обязательно по результатам инцидента составьте какой-нибудь документ, чтобы специалист, который придет на ваше место, смог легче ориентироваться в состоянии системы.

И если вы долго не можете справиться с отказом, попробуйте рассказать о неисправности кому-либо еще. Во-первых, пытаясь объяснить проблему, вы разложите ее для себя "по полочкам". А, во-вторых, часто советы неспециалистов могут направить вас на неожиданный путь решений.

Где найти помощь

Устранение неисправностей в информационной системе практически невозможно без обращения к внешним источникам знаний. Существует несколько ресурсов, где системный администратор может получить "подсказку".

- **Windows Help.**

  Первое, к чему необходимо обратиться при возникновении любой проблемы в работе компьютера, — это встроенная справочная система.

С каждой новой версией Windows эти системы становятся все более содержательными и полезными (если только вы знаете, что хотите найти, и правильно формулируете условия поиска).

- **Resource Kit.**

  Если необходима информация, уточняющая те или иные аспекты настройки операционной системы, описывающая тонкости ее работы, то следует обратиться к документации, содержащейся в пакете программ Resource Kit.

  Resource Kit — это дополнительный набор утилит, предназначеных для опытных пользователей и администраторов систем. Например, пакет для Windows Server содержит утилиты, которые позволяют протестировать процессор в режиме максимальной загрузки, зарегистрировать программу в качестве службы, выполнить различные операции управления компьютером в режиме командной строки с использованием сценариев и т. п. Обычно в состав пакета включено несколько сотен таких утилит.

  Кроме этого, в пакете присутствует справочная документация, которая подробно описывает функционирование различных служб операционной системы. Если вы испытываете сложности в настройке Windows для выполнения определенных функций, то в данной документации обычно можно найти необходимое пояснение.

  > ***Замечание***
  >
  > Пакет Resource Kit существует только на английском языке. Так что для его использования необходимо обладать хотя бы минимальным знанием технического английского языка.

- **Онлайновая база данных Microsoft.**

  Громадный объем документации содержится на сайте корпорации Microsoft по адресу **http://msdn.microsoft.com/**. В различных разделах этого ресурса вы можете найти как описания работы отдельных компонентов операционной системы, так и технические статьи, описывающие обнаруженные ошибки и методы их устранения.

  Онлайновая справочная база Microsoft *большей частью* локализована. Можно перейти на соответствующие страницы с русской версии сайта корпорации, находящейся по адресу **http://www.microsoft.com/rus/**. Однако без поиска на английском языке, как правило, найти необходимые советы не удается.

- **Материалы Интернета.**

  Способы разрешения многих проблем, особенно если таковые случились не только у одного пользователя, можно найти на многочисленных сайтах

сети Интернета. В первую очередь это специализированные сайты, посвященные конкретным прикладным вопросам, сайты известных специалистов, другие серверы, на которых хранятся различные справочные материалы (например, на многих серверах Сети хранятся ответы на типовые вопросы по функционированию системы — FAQ). Такие ресурсы легко находятся при помощи обычных поисковых серверов Интернета.

- **Конференции Интернета.**

  Если вы не нашли описания своей проблемы на таких узлах Сети, то можно обратиться с соответствующим вопросом в специализированную телеконференцию. Хотя не стоит надеяться, что вы гарантированно получите ответ, но обращение в конференцию является одним из наиболее эффективных способов получения необходимой помощи.

  Примечание

  Подобные конференции обычно поддерживаются как на сайтах разработчиков, так и на других ресурсах, посвященных компьютерной тематике. Определенную помощь может оказать изучение списка конференций, поддерживаемых новостным сервером вашего провайдера.

- **Техническая поддержка производителя.**

  Крупные производители программного обеспечения имеют специализированные службы для оказания технической поддержки. Обращение в такую службу обычно помогает существенно снизить время решения возникшей проблемы. Особенно, если уровень подготовки технических специалистов на предприятии недостаточен для квалифицированного сопровождения инфраструктуры.

  Обычно подобная поддержка является платной услугой, причем уровень цен не позволяет заказывать ее малым и средним организациям. Постепенно начинает развиваться сервис коммерческого предоставления технической поддержки третьими фирмами. К сожалению, в этом вопросе очень много субъективных факторов, влияющих на качество такого сопровождения. Поэтому решение на приобретение данной поддержки должно приниматься индивидуально с учетом анализа опыта других предприятий.

Что может отказать

Отказ в обслуживании может возникнуть из-за неисправности любого элемента системы: повреждения кабельной системы, неполадок в работе коммутирующих устройств, выхода из строя узлов компьютера, зависания операционной системы, ошибок программного обеспечения бизнес-уровня и уровня приложений и т. п. Администратору важно выяснить первопричину отказа.

Неисправности кабельной подсистемы

Неисправности на уровне физических носителей могут приводить к ошибкам копирования файлов, "зависанию" приложений, работающих с сетевыми ресурсами, и т. п. Подобные неисправности могут иметь случайный характер (например, при переломе кабеля и восстановлении/пропадании сигнала при незначительном изгибе).

Как правило, специализированного оборудования для проверки кабельных трасс у администраторов небольших предприятий нет. А приглашать специализированную организацию, когда нет полной уверенности относительно качества кабелей, достаточно накладно. Поэтому для выявления таких неисправностей необходимо задействовать сетевые анализаторы и контролировать число ошибочных пакетов.

Существуют бесплатные анализаторы сетевого трафика, функциональности которых достаточно для проверки сети организации. Наиболее известен пакет Wireshark (**http://www.wireshark.org/**). Программа доступна для загрузки в различных версиях, в том числе, есть и переносимая сборка (*portable*), которая позволяет записать программу на сменный носитель и запускать на компьютере без установки.

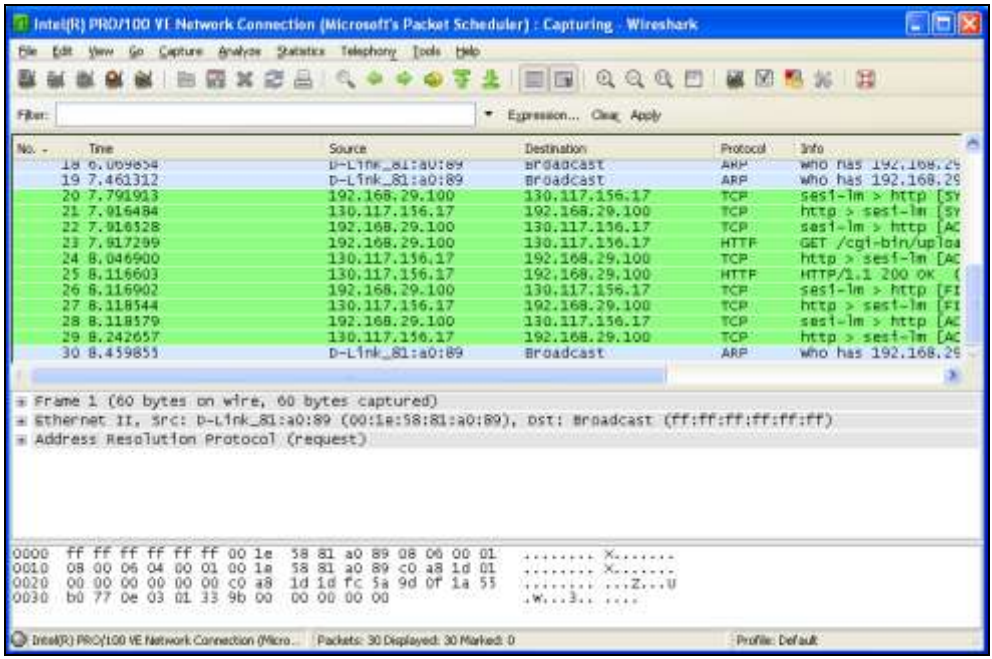


Рис. 10.1. Окно программы Whireshark

На рис. 10.1 показано окно программы в режиме сбора пакетов. Ранее программа была известна под названием Ethereal. Программа снабжена простым анализатором, который может собрать поток пакетов (например, восстановить звонок IP-телефонии или отобразить связанные пакеты). В большинстве случаев возможностей программы достаточно для анализа. При потребности в более глубоком и комплексном анализе данных на уровне пакетов следует обратиться к коммерческим версиям сетевых анализаторов.

Программа для мониторинга сети из состава Windows (Network Monitor), которую можно также бесплатно загрузить с сайта разработчика, позволяет перехватывать пакеты, передаваемые по сети, но не содержит серьезных средств анализа полученных данных. Поэтому мы рекомендуем именно пакет Wireshark.

При проведении анализа сети обратите внимание на следующие параметры.

- **Коэффициент использования пропускной способности сети.** Реально сеть Ethernet обеспечивает уверенную работу при загруженности не более 30–40%. Максимально можно достичь примерно на 70% от декларируемой полосы пропускания сети. При увеличении нагрузки резко возрастает число коллизий, падает реальная производительность системы. Если какие-либо сегменты показывают высокую нагрузку, то следует предпринять меры для расшивки этого узкого места. Например, заменить сетевое оборудование на более производительное, подключить дублирующие каналы связи (иное название, транки, EtherChannel).
- **Число ошибочных пакетов.** Сниффер позволяет получить данные о коллизиях, о числе пакетов, содержащих те или иные ошибки (ошибки CRC, слишком малые или слишком длинные пакеты и т. п.). При нормальной работе число ошибочных кадров не должно превышать десятых долей процента передаваемой информации. Обычно большой процент ошибок контрольной суммы свидетельствует о низком качестве сети (контакты, помехи в кабеле, неисправности портов оборудования). Неверные длины пакетов — признак неисправности сетевых адаптеров и их драйверов.
- **Величина коллизий.** В нормально работающей сети величина коллизий не должна превышать нескольких процентов. Большая величина — это признак низкого качества сети (локальные коллизии), наличие ошибок адаптеров или неверного проектирования сети (late collision — коллизия, обнаруживаемая после передачи первых 64 байтов. Причиной late collision часто бывает большое число повторителей в локальной сети.).

Если у вас сеть построена на управляемых коммутаторах, то статистическую информацию по ошибочным пакетам можно получить от их программ управления (см. рис. 1.8). Если вы заметили подобную статистику на порту комму-

татора, то необходимо обязательно выяснить ее причины. Часто наличие ошибок свидетельствует о физическом повреждении кабеля. При наличии системы мониторинга ее можно настроить на автоматический контроль возникновения подобных ошибок.

Если в вашей организации создана отказоустойчивая структура сети (с дублированием каналов и устройств), то обязательно следует постоянно проверять ее состояние. В противном случае единичный отказ не будет обнаружен, и вы столкнетесь с серьезной аварией в случае второго отказа.

Неисправности активного (коммутационного) оборудования

Несмотря на часто декларируемую "пожизненную" гарантию, активные устройства (концентраторы, коммутаторы, маршрутизаторы, кабельные модемы и т. п.) могут зависать, выходить из строя, неадекватно вести себя в особых ситуациях.

Заподозрить неисправность такого устройства достаточно сложно, именно из-за малой вероятности подобных отказов. Устройство может также "мигать" своими портами, но при этом не обеспечивать нормальную передачу информации. Косвенным признаком отказа может служить потеря управления устройством по сети.

Как правило, такое состояние лечится только холодной перезагрузкой устройства.

Неисправности аппаратной части компьютеров

Это весьма тяжело детектируемые неисправности, особенно если происходят достаточно случайно. "Хорошо", если неисправность аппаратной части компьютера приводит к его полной неработоспособности. А выявить "исчезающую" неисправность, обусловленную проблемами "железа", крайне сложно. Как правило, компьютер в таких случаях прекрасно проходит специальное тестирование, но все же постоянно "подвисает" на определенных задачах.

При подозрении на аппаратную неисправность необходимо вначале выполнить следующие операции:

- Обновить BIOS материнской платы компьютера до последней версии изготовителя.
- Выполнить чистую установку операционной системы (без каких-либо "лишних" прикладных программ); после чего установить все обновления от ее изготовителя.

- Установить последние версии драйверов для материнской платы, видеоадаптера и т. п. Драйверы оборудования прилагаются к системному блоку. Вам следует обязательно убедиться, что изготовитель не предлагает на сайте новые версии. И если новые версии обнаружены, то скачать и установить именно их. Обратите внимание, что при наличии сертифицированных версий и новых разработок (бета-версии) обязательно следует устанавливать последние сертифицированные варианты.
- Если неисправность наблюдается в прикладном программном обеспечении, то следует установить его и все имеющиеся для него обновления.

После выполнения этих операций нужно попытаться воспроизвести неисправность. Если неисправность будет периодически возникать, то такой блок следует передать на техническое обслуживание.

> ***Примечание***
>
> На практике часто встречаются случаи, когда простая замена одних узлов на аналогичные, причем той же модели, часто ликвидировала такие исчезающие неисправности.

Резервирование узлов компьютера

По опыту работы, наиболее ненадежными узлами компьютерных систем являются жесткие диски. Следующая наиболее часто встречающаяся причина нестабильной работы — некачественная память. Отказывают и материнские платы, и процессоры, и периферийные устройства.

Обычно стараются резервировать (с возможностью горячей замены) наиболее часто отказывающие узлы — жесткие диски и блоки питания.

Жесткие диски, как правило, объединяют в RAID-массивы того или иного уровня с возможностью горячей замены. При необходимости серьезной экономии можно создать такие массивы программным способом и использовать SATA-диски. Поскольку RAID обычно конфигурируется с избыточной надежностью, то единичный отказ жесткого диска сохраняет работоспособность устройства хранения. Поэтому администратору необходимо либо постоянно следить за состоянием RAID, либо автоматизировать получение предупреждения о возникновении отказа. Иначе второй отказ может привести к краху системы.

Применение систем с резервированием других узлов (например, памяти) часто экономически не оправдано. Если необходимо обеспечить работоспособность службы при выходе из строя аппаратной части компьютера, обычно применяют *кластерные* решения (параллельная работа нескольких компьютеров; решение дорогое и не подходит для небольших организаций) или решения

высокой доступности для виртуальных систем (также в силу стоимости, практически, доступны только для крупных информационных систем).

Контроль теплового режима работы системы

При повышении температуры на несколько градусов вероятность отказа компьютера повышается на десятки процентов. Поэтому контроль теплового режима — важная задача.

Одним из самых ненадежных узлов компьютера являются вентиляторы охлаждения. Они служат для поддержания необходимого теплового режима процессора, видеоадаптера, в блоке питания и т. п. Число вентиляторов варьируется в зависимости от модели компьютера.

Обычно через полтора-два года эксплуатации компьютера дешевые модели вентиляторов снижают скорость вращения лопастей (или даже могут полностью остановиться). Современные материнские платы имеют в поставке программы, которые автоматически контролируют скорость вращения вентиляторов и температурный режим внутри системного блока. При наличии таких программ их следует обязательно установить и своевременно реагировать на их сообщения. При отсутствии средств контроля необходимо периодически (каждый раз, когда вы открываете системный блок) визуально контролировать скорость вращения лопастей вентилятора и своевременно заменять неисправные.

Примечания

Допустимо смазывать оси вентиляторов специальной смазкой. Но после такой операции следует проверять данные вентиляторы не реже одного раза в три-четыре месяца.

При отсутствии штатных средств контроля температуры материнской платы компьютера можно воспользоваться бесплатными программами, контролирующими температуру жестких дисков. Одна из таких программ — HDD Thermometer разработки Rdssoft, например, контролирует температуру дисков и может формировать предупреждения администраторам в случае превышения установленных лимитов.

Температура внутри корпуса компьютера может повыситься не только из-за ухудшения качества вентиляторов. Так, причиной перегрева могут стать дополнительные устройства (дополнительные жесткие диски), установленные в компьютер. Вполне возможно, что конструкция корпуса просто не рассчитана на такое количество оборудования. Свою лепту вносят и крайне жаркие дни, которых наблюдается все больше в последние годы.

Все эти причины могут привести к перегреву компьютера и, как следствие, возникновению сбоев в его работе или даже выходу из строя.

Если оборудование установлено в шкафу и температура внутри шкафа измеряется, то для грубой оценки можно ориентироваться на следующие цифры. Температура внутри корпуса компьютера обычно на 15–20° превышает температуру окружающей среды. Поэтому администратор должен начать предпринимать срочные меры, если температура внутри серверного шкафа превысит 30 °С.

Ошибки программного обеспечения

Основная часть отказов Windows-систем связана преимущественно с ошибками в программном обеспечении. Как уже говорилось, это могут быть ошибки самой операционной системы или установленного прикладного продукта.

Если проблема возникала только один раз, то выявить ее причины обычно практически невозможно. Если событие повторилось, то администратору следует тщательно проанализировать всю сопутствующую информацию и выявить события, связанные с инцидентом. Чем тщательнее будет проведен предварительный анализ, тем больше вероятность точного решения. Следует попытаться изолировать данную неисправность от других событий и составить необходимый план действий, предусматривающий возможность операций "отката", если лечение проблемы само вызовет другие отказы.

И, естественно, администратор не может не обратиться к поиску аналогичных инцидентов и рекомендаций по их разрешению в той или иной базе знаний.

Выяснение причин катастрофических ошибок в программном обеспечении

При аварийном завершении работы прикладной программы или всей операционной системы часто достаточно сложно определить виновника. Как правило, на компьютере установлено много программ, остались следы от ранее использованных и т. п. Все это может влиять на случившийся отказ программного обеспечения. Существуют специальные продукты, которые могут помочь в таких случаях администратору.

На странице **http://www.microsoft.com/whdc/devtools/debugging/default.mspx/** представлены средства отладки Windows — *Debugging Tools for Windows*. Понятно, что предназначены они для специалистов, но получить базовую информацию по неисправности можно достаточно простыми способами.

На рис. 10.2 показано окно, в котором необходимо настроить варианты поведения системы в случае аварийного завершения работы. Обычно достаточно включить автоматическую перезагрузку (это значение по умолчанию) и включить малый дамп памяти.

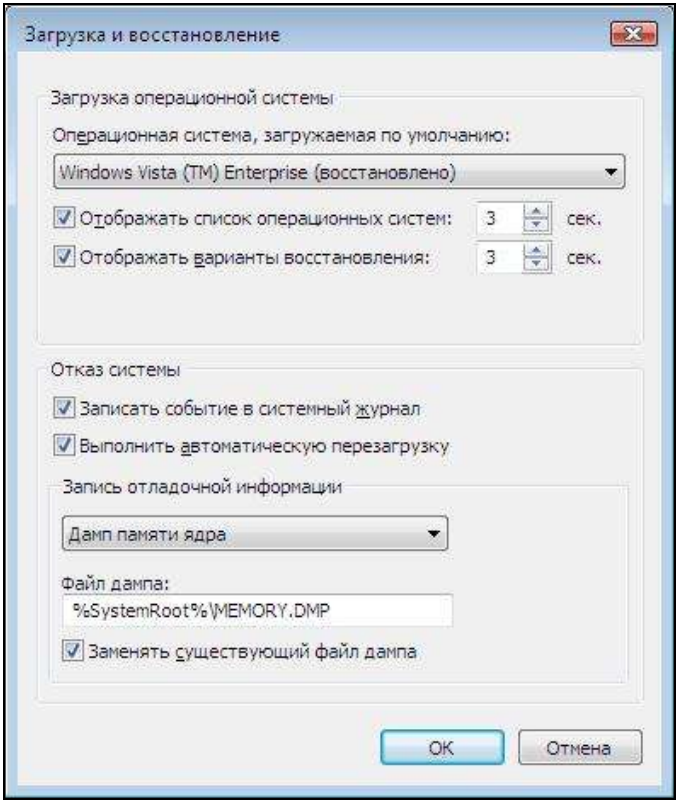


Рис. 10.2. Настройка автоматической перезагрузки и записи отладочной информации в случае аварийных отказов

Загрузите с сайта средства отладки и, обязательно, наборы символов для вашей операционной системы (наборы символов нужны, чтобы сделать вывод информации более читабельным). Наборы символов отличаются для различных версий Windows, в том числе, необходимо подключать различные наборы для систем с установленными пакетами обновлений и без них. Можно сначала установить средства отладки, а потом, имея подключение к Интернету, загрузить необходимые символы. Но учитывая их объем (несколько сотен мегабайт загрузки и более 1,5 Гбайт в установленном виде), лучше это сделать заблаговременно.

Примечание

Установка символов и самой программы отладчика выполняется независимо. Типовая ошибка начинающих пользователей — отсутствие настройки пути к папке символов в отладчике. Не забудьте при старте программы открыть меню **File** и настроить параметр **Symbol File Path**.

После установки отладчик можно использовать двумя основными способами: открыть для анализа файл дампа памяти или подключиться к работающему процессу (командой **File** | **Attach to Process...**) и ожидать момента аварийного его завершения. Для того чтобы файл дампа памяти формировался при отказе операционной системы, соответствующие настройки нужно включить в свойствах компьютера (см. рис. 10.2).

После получения отладчиком информации об аварии обычно в консоли достаточно ввести команду

```
!Analyze -v
```

и попытаться проанализировать результат. Нужная информация, как правило, представлена в строках *image_name* и *module_name* (рис. 10.3).

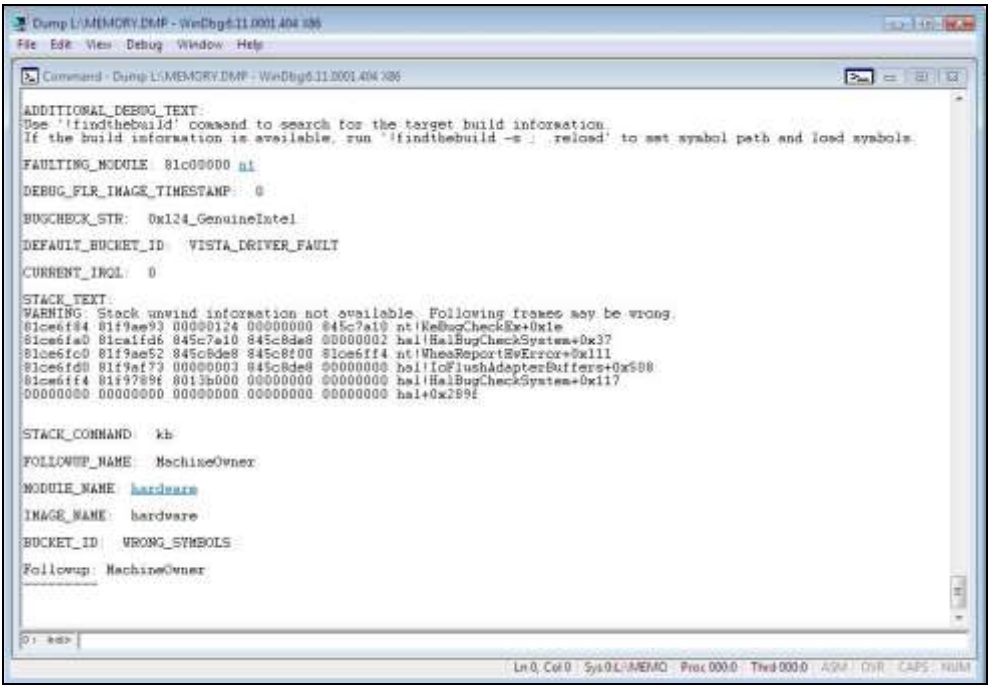


Рис. 10.3. Окно отладчика Windows

На рис. 10.3 показано окно отладчика после выполнения анализа дампа памяти "упавшей" системы. По информации можно сделать вывод, что причина отказа — плохой драйвер оборудования из состава Vista. Исправить именно эту ошибку администратор, естественно, не в силах. Но зато он узнал, что нужно искать новый драйвер оборудования.

Восстановление "упавших" систем

Если операционная система на базе Windows перестала нормально загружаться, то администратор имеет несколько штатных средств восстановления ее работоспособности:

- загрузка в безопасном режиме;
- загрузка последней удачной конфигурации — вариант загрузки выбирается после нажатия клавиши <F8> в момент старта системы;
- восстановление системы из консоли восстановления;
- восстановление из программы установки;
- использование программ сторонних разработчиков.

Если администратор готовился к возможным отказам, то он сможет запустить процесс восстановления с использованием сохраненных настроек и данных (например, *режим автоматического восстановления*). Эта операция возможна при запуске процесса установки ОС с дистрибутивного компакт-диска.

Если у администратора нет сохраненных настроек, то можно попытаться восстановить систему путем новой установки в режиме восстановления. Этот режим возможен не для всех систем на основе Windows и запускается он из процесса установки ОС. В случае, если программа установки обнаруживает на диске операционную систему и она совпадает с версией дистрибутива, то в опциях появляется возможность *восстановления*. Практически это будет новая установка ОС с сохранением всех установленных на компьютере программ и имеющихся настроек.

После такого восстановления необходимо сразу же установить все обновления, имевшиеся на исходной системе. В противном случае возможны ошибки в работе.

Существует много программ, реализующих дополнительные возможности восстановления. Например, путем создания точек восстановления и последующего "отката" к ним неисправной системы при загрузке с соответствующего компакт-диска.

Загрузка в безопасном режиме

Загрузка в безопасном режиме позволяет решить следующие проблемы:

- ошибки конфигурации системного программного обеспечения;
- сбои из-за установки новых устройств или программ, в том числе и ошибки, возникшие вследствие установки пакетов обновлений.

Загрузка последней удачной конфигурации

Загрузка последней удачной конфигурации поможет в случае:

- ошибок конфигурации во время последней сессии;
- установки неверного драйвера устройства.

Думаю, что каждый администратор не раз использовал эти режимы, и необходимости более подробного объяснения нет.

Консоль восстановления

В течение многих лет практической работы автора подавляющее большинство случаев отказа загрузки систем на базе Windows было связано с нарушениями структуры жесткого диска (повреждения загрузочного сектора, загрузочных и системных файлов) или с последствиями установки новых устройств (драйверов). Эти неисправности можно устранить при помощи *консоли восстановления*.

Консоль восстановления — это режим командной строки, в который можно загрузить проблемную операционную систему. В этом режиме доступен ограниченный набор команд, с помощью которых можно выполнить операции настройки системы и восстановления структуры жесткого диска. Так, можно восстановить загрузочные секторы, скопировать любые файлы с компакт-диска на жесткий диск, выполнить проверку диска (и устранить ошибки) с помощью программы `chkdsk`, изменить параметры запуска служб операционной системы (например, отключить ту или иную службу) и т. п. Полный перечень команд доступен путем вызова справки в режиме командной строки (`help /?`).

В режим консоли восстановления проще всего перейти выбором соответствующей опции при загрузке с установочного диска.

Приведем основные операции, которые приходится выполнять в режиме консоли восстановления.

- **Восстановление загрузочных областей диска** — для этой цели следует использовать команды `fixboot` и `fixmbr`.
- **Восстановление отсутствующих загрузочных или системных файлов** — поскольку в режиме консоли восстановления доступен привод CD-ROM, то вы можете просто скопировать нужные файлы с дистрибутива в соответствующие папки. Обратите только внимание, что буквы логических дисков в режиме консоли восстановления могут не совпадать с названием логических дисков в работающей системе. Вам следует ориентироваться, например, по размерам дисков, находящимся в них папкам и т. п.

- **Проблемы со службой (драйвером нового устройства)** — воспользуйтесь командой `listsvc` для отображения списка служб и устройств и командой `enable` для отключения подозрительных служб (драйверов).
- **Восстановление структуры жесткого диска** — выполняется стандартно командой `chkdsk`. Единственное, что программа может запросить у вас, — вручную указать путь к файлу библиотек, используемому при запуске этой утилиты (если повреждена системная папка; следует указать папку на компакт-диске).
- **Нарушения реестра** — часто система не может загрузиться из-за нарушений структуры реестра. Причем выбор последней удачной конфигурации не приводит к успеху. Попробуйте вручную восстановить последнюю копию той ветви реестра, о которой сообщает программа загрузки. Для этого перейдите в каталог SYSTEM32\CONFIG, найдите файл реестра и переименуйте его (по умолчанию текущие файлы не имеют расширения), после чего скопируйте (переименуйте) одноименный файл с расширением sav в файл без расширения. Другое место, откуда можно взять файлы копий реестра системы, — это папки точек восстановления.

  После выполнения операции перезагрузите систему в нормальном режиме.

> ***Примечание***
>
> Режим консоли не будет работать, если для доступа к диску потребуется драйвер, не входящий в состав дистрибутива операционной системы. Например, такая ситуация встречается при установке Windows XP или Windows 2003 Server на SATA-диски. Как подготовить в этом случае загрузочный диск консоли восстановления, подробно описано, например, в предыдущей книге автора ("Самоучитель системного администратора", БХВ, 2008).

Режим восстановления в Windows XP SP2/Windows 2003 Server

Если ваша система перестала запускаться, загрузитесь с установочного компакт-диска и начните установку. После того как вы укажете для установки диск, на котором ранее была установлена операционная система, программа обнаружит это и предложит произвести *восстановление*. После подтверждения от вас установка продолжится, внешне не отличаясь от обычного режима. Однако после ее завершения вы обнаружите, что все ранее установленные программы сохранили свою работоспособность.

Однако режим восстановления не будет доступен, если вы:

- применяете для восстановления не тот вариант дистрибутива, с которого была установлена система (например, пытаетесь восстановить с дистрибутива на другом языке);

- в системе возникли серьезные повреждения (например, разрушения файловой структуры, в результате чего программа не может обнаружить папки установленной системы).

Варианты восстановления Windows Vista/Windows Server 2008

В состав Windows Vista включена специальная среда для восстановления операционной системы. Она запускается при загрузке компьютера с установочного диска. В некотором смысле это аналог консоли восстановления Windows XP. Только исполнена она на основе Windows PE (Windows Preinstallation Environment), который сменил "загрузочные дискеты" Windows, и содержит ряд *автоматизированных* операций по восстановлению загрузки.

Для работы со средствами восстановления необходимо загрузиться с установочного диска Windows Vista. При обнаружении проблем система автоматически начнет операции проверки, пытаясь восстановить работоспособность (рис. 10.4).

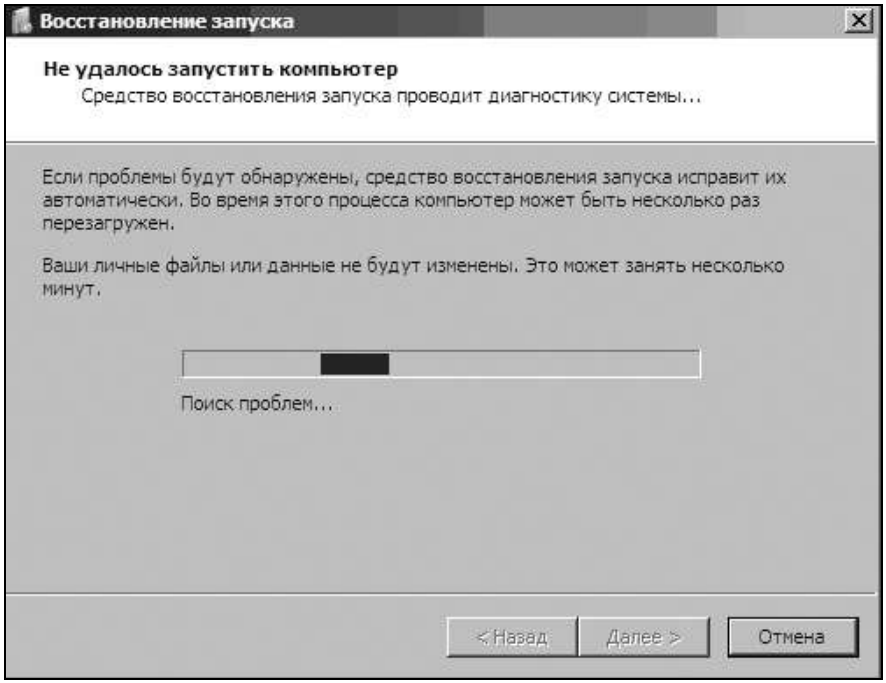


Рис. 10.4. Процесс автоматического восстановления системы

Восстановление реестра из файлов точек восстановления системы

Последние версии ОС автоматически сохраняют значения основных настроек в *точках восстановления*. Восстановление прежних настроек штатно предусмотрено только при работе операционной системы (в Vista — также при загрузке с компакт-диска). Однако администратор может использовать сохраненные параметры в режиме консоли восстановления или запустить программы типа ERD Commander, позволяющие выполнить откат к точке восстановления в режиме загрузки с компакт-диска (рис. 10.5).

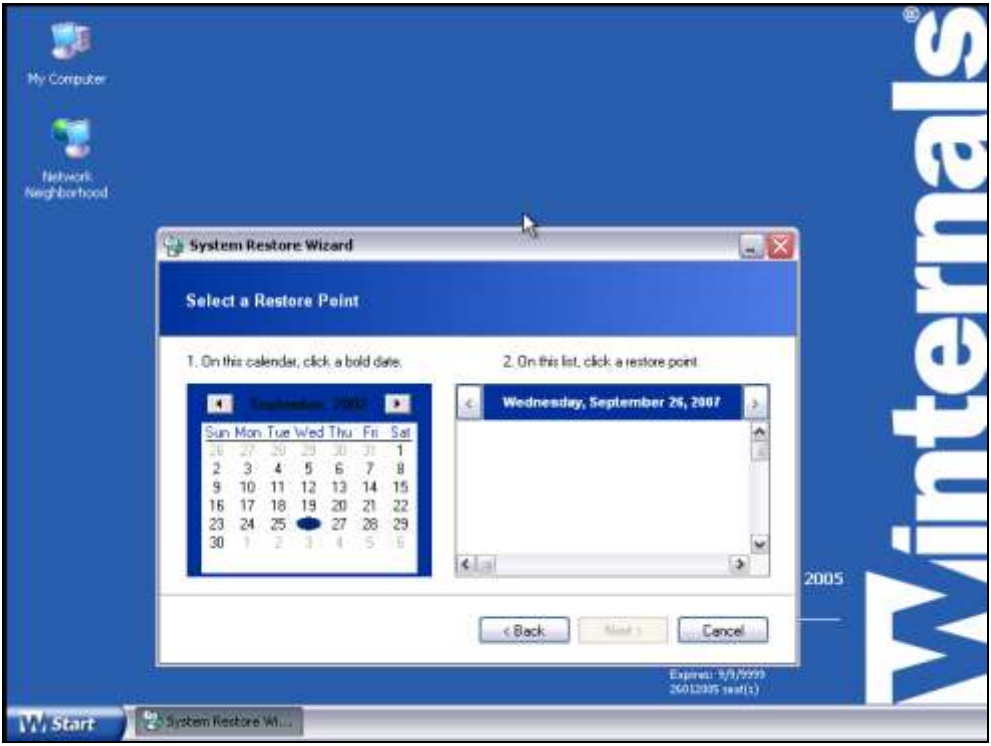


Рис. 10.5. Мастер отката к предыдущим точкам восстановления системы при загрузке с внешнего компакт-диска (пакет ERD Commander 2005)

Значения реестра системы сохраняются в папках точек контрольного восстановления системы — System Volume Information. Эти параметры обычно более точно соответствуют последним настройкам системы, чем копии реестра, например, в папке \Windows\Repai.

Замечание

Здесь и далее в примерах этого раздела считается, что система установлена в папку C:\Windows. Иначе следует заменить название каталога.

По умолчанию (при использовании NTFS) содержимое папки с точками восстановления недоступно пользователю. Чтобы получить доступ к этим данным в режиме нормальной работы ОС, необходимо добавить соответствующее право текущему пользователю для папки System Volume Information, например:

```
cacls "C:\System Volume Information" /E /G имя_пользователя:F
```

При работе в консоли восстановления права доступа не контролируются. Поэтому в указанную папку можно "зайти" с помощью обычных команд.

В папке System Volume Information сохраняются данные точек восстановления в каталогах с именами, аналогичными _restore{CFA91D90-58C3-4176-A156-29790E9DAF6B} (после *restore* идет значение GUID).

Следует зайти в папку, которая соответствует более поздней дате восстановления, открыть в ней каталог RP*номер* и зайти в папку snapshot.

В папке snapshot сохранены файлы реестра, правда, под именами, отличающимися от тех, которые используются в папке конфигурации. Поэтому для замены файлов реестра администратору необходимо скопировать файлы, перечисленные в табл. 10.1, в папку \Windows\System32\Config и переименовать их так, как указано в правом столбце.

Таблица 10.1. *Соответствие имен файлов*

Имя файла в папке восстановления	Должно быть переименовано в
_REGISTRY_USER_.DEFAULT	DEFAULT
_REGISTRY_MACHINE_SECURITY	SECURITY
_REGISTRY_MACHINE_SOFTWARE	SOFTWARE
_REGISTRY_MACHINE_SYSTEM	SYSTEM
_REGISTRY_MACHINE_SAM	SAM

Примечание

К сожалению, программа копирования режима консоли восстановления не поддерживает использование шаблонов. Поэтому для копирования нескольких файлов придется выполнить соответствующее число операций. Также в этом режиме не работает функция завершения набора имени файла по первым символам, что потребует точного ручного ввода всех используемых в операциях имен файлов и папок.

Использование программ типа ERD Commander

Специально для восстановления проблемных систем были разработаны программы, позволяющие выполнить загрузку компьютера с компакт-диска и получить доступ к жесткому диску системы. Самая известная программа такого типа — пакет ERD Commander от Winternals Software LP (**www.winternals.com**).

ERD Commander позволяет выполнить запуск системы с компакт-диска в оболочке, внешне идентичной интерфейсу Windows XP. После запуска пользователь получает доступ к жесткому диску (может просматривать файлы, редактировать их, сбросить права доступа к файловым объектам и т. п.), имеет возможность выполнять сетевые операции (можно предоставить папки для совместного доступа и подключиться к другим ресурсам). Можно выбрать любую точку отката из числа сохраненных в системе и восстановить состояние на момент ее создания. Есть возможность заменить пароль администратора. Доступны оснастки управления службами системы (можно изменить тип запуска и т. п.) и т. д.

> ***ЗАМЕЧАНИЕ***
>
> ERD Commander является частью пакета Administrator's Pak (на момент подготовки книги последняя версия этого пакета была 5), который содержит целый набор утилит для восстановления систем. Например, утилиту Remote Recover, позволяющую запустить компьютер с дискеты и подключить его локальные диски к удаленной консоли. Таким образом можно выполнить необходимые операции (заменить файлы, сбросить пароль администратора и т. п.) для восстановления системы.

Автор встречался с несколькими версиями "доработанных" загрузочных дисков, в которых были добавлены опции запуска популярных прикладных программ (файловых менеджеров, программ восстановления диска и т. п.). При необходимости подобное расширение функций может осуществить и сам администратор, редактируя образ компакт-диска, сформированный данной программой.

На взгляд автора наличие программы типа ERD Commander должно быть обязательным в арсенале системного администратора.

Восстановление удаленных данных

Восстанавливать один-два файла, удаленных пользователем, из резервной копии — занятие неблагодарное, прежде всего из-за длительности операции (обычные объемы файлов резервных копий составляют несколько гигабайт). В этом случае можно воспользоваться технологиями, позволяющими восстанавливать удаленные данные. Это программы-аналоги Корзины Windows, технология Volume Shadow Copy и различные утилиты для восстановления данных.

Корзины

"Штатная" Корзина Windows малоэффективна из-за того, что при значительном числе операций удаления файлы просто не попадают в нее (например, при удалении по сети или из командной строки). Существует большое число вариантов Корзин, ориентированных на локальную систему (например, Norton Protected Recycle Bin) и позволяющих восстановить практически любой удаленный файл.

Конечно, в условиях компьютерной сети более функциональны специализированные серверные решения. Например, Executive Undelete от Executive Software International, Inc.

Эта программа может быть централизованно установлена администратором на рабочие станции и позволяет выполнять операции восстановления как непосредственно пользователем, так и администратором при подключении к Корзине по сети.

Восстановление из теневых копий

В Windows 2003/2008 и Windows Vista имеется возможность восстановления предыдущей версии документа. Эта технология называется *теневым копированием* (shadow copy) и суть ее состоит в создании копий информации по графику, определяемому администратором. Такую копию можно создать, в том числе, и для открытых файлов (тех, с которыми в момент создания копии ведется работа). Одновременно могут храниться несколько копий документов на разные моменты времени (рис. 10.6). Предел определяется только размером дискового пространства, отведенного для данной операции. Причем резервирования нескольких сотен мегабайт диска может хватить на хранение промежуточных копий за несколько месяцев интенсивной работы.

Технология теневого копирования позволяет, во-первых, осуществлять резервное копирование *всех* данных (ранее штатная программа ntbackup пропускала при создании копий те файлы, к которым она не могла получить доступ; иными словами, те файлы, которые редактировались пользователем). Во-вторых, у пользователей появилась прекрасная возможность без всяких дополнительных затрат иметь *несколько версий* документа. Например, после внесения очередных правок вы поняли, что более правильным решением был предыдущий вариант договора. Если он не был сохранен в качестве отдельного документа, то вернуться к прежним формулировкам ранее было затруднительно. При реализации технологии теневого копирования достаточно посмотреть перечень предыдущих версий документа и восстановить необходимую.

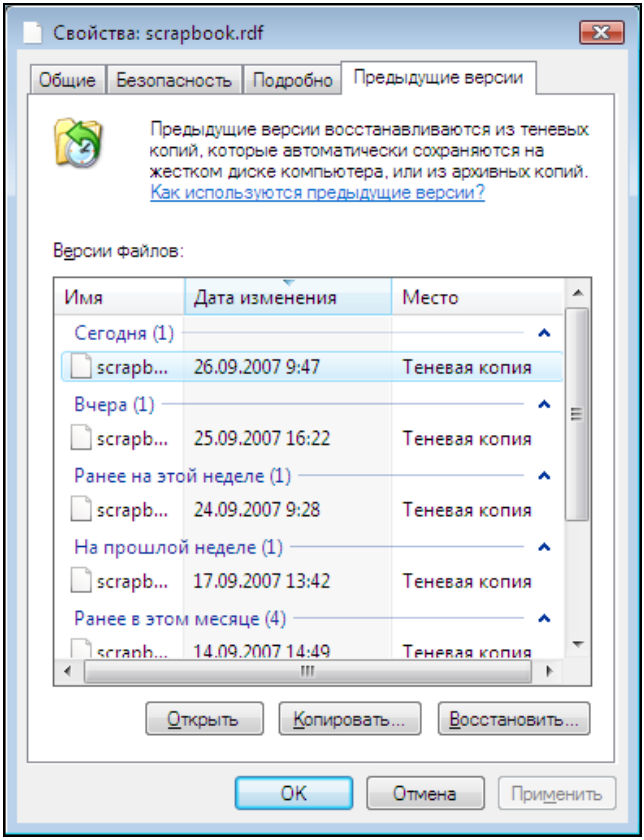


Рис. 10.6. Просмотр предыдущих версий файла на Windows Vista

Для работы с предыдущими версиями файлов пользователям Windows XP необходимо установить специальный клиент. Его установочные файлы находятся в папке установки сервера по пути Windows\system32\clients\twclient\ и далее — в зависимости от типа платформы клиента. После установки этой программы при открытии свойств файла в сетевой папке появляется дополнительная вкладка **Предыдущие версии**. На этой вкладке можно выполнить необходимые операции восстановления информации. В Windows Vista возможность создания предыдущих версий включена в состав операционной системы рабочей станции. Причем данная возможность доступна и для файлов локального диска.

Замечание

В Windows 2003 функции восстановления предыдущих версий были доступны пользователям только для сетевых папок сервера.

В Windows Vista теневые копии выполняются в момент создания точек восстановления (иными словами, обычно раз в день). При необходимости операцию можно выполнить вручную (через задачу *Центр архивации и восстановления*). В Windows 2003 необходимо настроить расписание создания теневых копий, используя задачу **Управление компьютером** | **Общие папки**, в динамическом меню выбрать задачу создания теневых копий и далее настроить ее параметры (рис. 10.7).

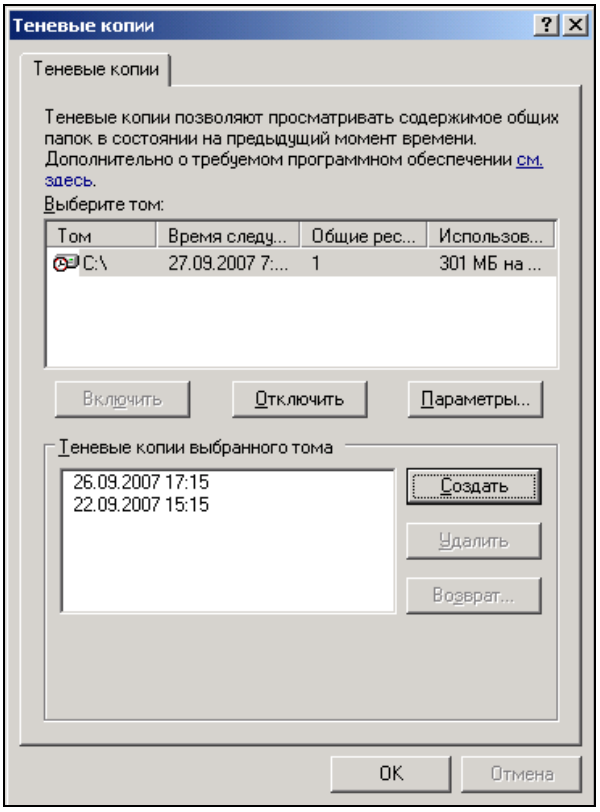


Рис. 10.7. Настройка расписания создания теневых копий в Windows 2003

Восстановление данных с жестких дисков

В Windows не предусмотрено никаких штатных средств для лечения жестких дисков, кроме программы `chkdsk`. Эта утилита позволяет проверить целостность файловой системы, "закрыть" сбойные участки жесткого диска. Но она будет практически бесполезна в случае серьезных повреждений.

Для восстановления информации с жестких дисков чаще всего применяют программы Easy Recovery (Ontrack Data Recovery, Inc, **www.ontrack.com**) и GetDataBack (RunTime Software, **www.runtime.org**).

Эти программы позволяют восстановить данные даже с тех дисков, которые не определяются в BIOS компьютера. Имеется возможность восстановления после форматирования диска, "сборки" файлов на основе их типа и т. п.

Работа с данными программами достаточно очевидна. Сначала анализируется структура жесткого диска, предлагается определить восстанавливаемый раздел и тип файловой системы, после чего начинается поиск информации. Найденный список можно отфильтровать при необходимости по тем или иным критериям (например, восстанавливать только файлы документов), после чего можно выполнить восстановление.

Восстановление всегда производится на другой диск, чтобы не повредить исходные данные. Поэтому при отсутствии сетевых подключений необходимо позаботиться о дополнительном устройстве хранения.

Если возникли дефекты устройства хранения данных (чаще всего переносные устройства — дискеты, реже — жесткие диски, компакт-диски), то обычно повреждается лишь небольшой участок файла. Но это, как правило, приводит к тому, что соответствующий файл не открывается в программе его редактирования.

Для восстановления таких поврежденных файлов разработано много утилит, которые можно найти в Сети. При этом чем популярнее формат файлов данных, тем больше вероятность того, что для этого типа информации существуют утилиты восстановления. Например, можно перечислить утилиты восстановления для офисных файлов (Microsoft Word, Excel, Access, PowerPoint), для файлов личных папок офиса (pst), для файлов архива (zip), файлов баз данных (dbf) и т. п. Версии этих утилит меняются с модификацией основных программ, поэтому я отошлю читателя к самостоятельному поиску в Интернете.

Принцип работы таких утилит достаточно прост. Они анализируют структуру файла, находят поврежденный блок данных и корректно восстанавливают структуру файла так, чтобы он мог быть открыт в основной программе с минимальными потерями.

Анализ производительности

Определить оптимальную конфигурацию системы даже для выполнения конкретной прикладной задачи крайне сложно. Часто с течением времени компьютер перестает удовлетворять ожиданиям по производительности и взамен его приобретают более совершенную модель.

Однако во многих случаях причиной неудовлетворительной работы является какое-либо узкое место в конфигурации системы ("бутылочное горлышко", Bottleneck). И "расшивка" его может оказаться экономически существенно более оправданной, чем замена всей компьютерной системы.

Удовлетворенность производительностью системы — субъективная оценка. Она зависит от объема выполняемых пользователем бизнес-задач, частоты тех или иных операций и т. п. Обычно IT-специалисту необходимо проанализировать влияние многих параметров. Например, медленная работа Web-приложения, используемого работниками предприятия, может быть вызвана недостаточным качеством канала передачи данных, низкой производительностью брандмауэра, нехваткой ресурсов сервера интернет-приложений, проблемами сервера с базами данных и т. д.

Для анализа состояния системы существуют специальные встроенные средства. Прежде всего, это программа **Производительность** (Performance Monitor).

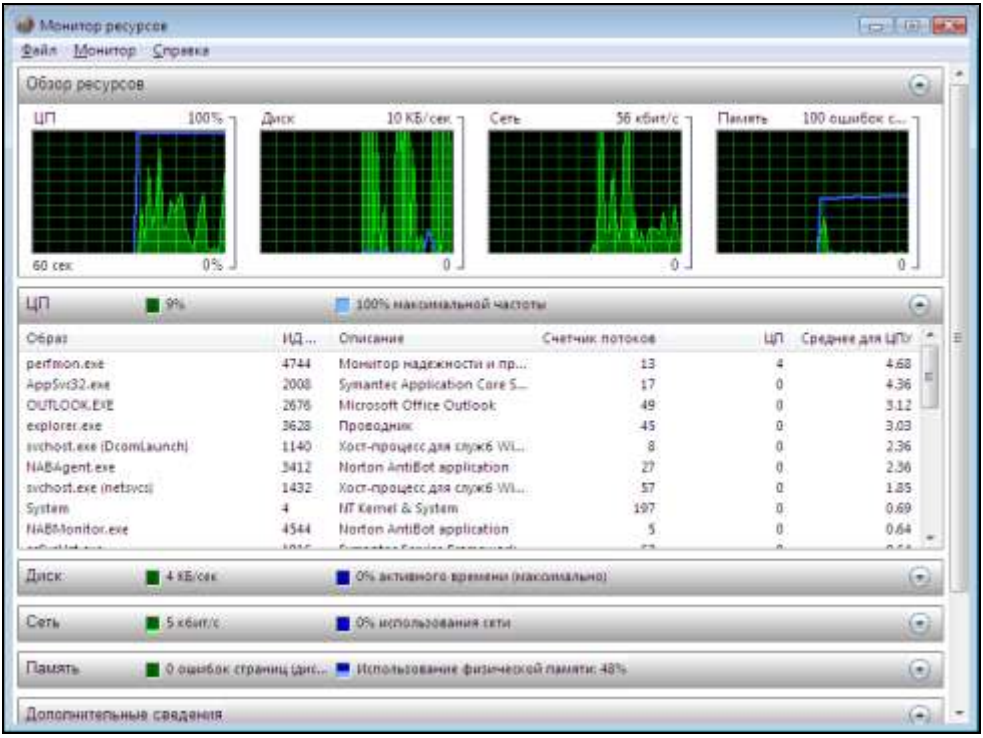


Рис. 10.8. Монитор ресурсов в Windows Vista позволяет администратору оценить вклад, вносимый различными процессами в загрузку системы

Примечание

Существует программа от Microsoft — Server Performance Advisor, которая формирует отчет по параметрам производительности системы. Эта программа позволяет оперативно собрать необходимые для первичного анализа показатели и оформить их в виде бумажного отчета. Продукт свободно доступен для загрузки.

В новых выпусках Windows возможности программ мониторинга состояния существенно расширены. Так, программа **Монитор ресурсов** (рис. 10.8) позволяет администратору легко выявить программы, задействующие тот или иной ресурс компьютера.

Счетчики состояния системы

В операционной системе на базе Windows NT существует много так называемых *счетчиков*. Счетчики *постоянно* содержат численные параметры, которые характеризуют определенные процессы как самой операционной системы, так и прикладных программ. Если разработчики устанавливаемого ПО предусмотрели свои счетчики, то они добавляются в перечень отображаемых этой программой.

Программа монитора позволяет отображать состояние большого числа счетчиков. Поскольку их точная интерпретация требует специальных знаний операционной системы, то на практике обычно используют несколько интегральных показателей.

Примечание

Кроме наблюдения за показателями в различных графических представлениях (линейном графике, гистограмме и т. п.), программа позволяет вести протокол счетчиков, например, автоматически снимая показания каждые 10 мин., задавать границы, по достижению которых система выдаст предупредительное сообщение и может запустить заданную вами программу. Эти настройки могут помочь при проведении долговременных исследований производительности системы и текущего контроля ее состояния. Например, при обследовании компьютера целесообразно получить статистику его загруженности за достаточно длительный период — порядка суток.

Для оценки производительности системы следует выполнять в период замеров обычные для данного компьютера операции. Например, для рабочей станции это открытие файлов, их печать, чтение электронной почты, работа в программах офиса или выполнение текущих операций в базе данных и т. п. Чем больше такие операции будут соответствовать типовым вариантам использования компьютера, тем точнее получатся рекомендации на основе анализа показаний счетчиков.

Узким местом производительности компьютера обычно становится один из следующих компонентов:

- процессор;
- оперативная память;
- дисковая подсистема;
- сетевой адаптер.

Оценка производительности процессора

Рассмотрим параметры, которые необходимо контролировать в программе **Производительность.**

- **Processor\% Processor Time** — величина загрузки процессора.

  В нормальных условиях эксплуатации процессор должен быть лишь незначительно загружен. Конечно, если какая-либо программа в текущий момент времени выполняет серьезные вычисления, то загрузка в 90% и выше — это нормальный показатель. В среднем же величина загрузки процессора не должна быть более 20–40%. Если данный показатель более 50–70%, то необходимо заменить процессор на более производительную модель (или перенести на другие компьютеры часть выполняемых задач).

  В многопроцессорных системах часто встречаются ситуации, когда задача выполняется медленно, а загрузка процессора по данным монитора не превосходит, например, 25%. Это признак того, что решаемая задача не может распараллелить вычисления — все расчеты выполняются только на одном процессоре. Поскольку монитор отображает среднюю загрузку, то при полном использовании одного ядра в двухпроцессорной двухъядерной системе и получится среднее значение, чуть большее 25% (100% / 4 = 25%). В таком случае может помочь только выбор процессора с большей тактовой частотой и бóльшим значением кэша первого и второго уровня. Применение систем с несколькими процессорами не поможет выполнить задачу за меньший срок.

- **Processor\% Privileged Time** — счетчик важен для оценки загрузки процессора системными задачами. Если величина загрузки привилегированного режима составляет около 40% и выше, то это свидетельствует о необходимости серьезно проанализировать работу операционной системы, проверить состояние узлов компьютера и обновить драйверы устройств. Кроме того, такое значение может свидетельствовать о неоптимальной архитектуре выполняемых задач (например, сервер многократно передает клиенту небольшие порции данных (при этом очень часто средний процент загрузки процессора остается достаточно малым) вместо того, чтобы

централизованно выполнить вычисления и сообщить только итоговый результат).

- **System\Processor Queue Length (all instances)** — показатель отображает длину очереди заданий, которые необходимо выполнить процессору. Средняя величина очереди заданий, равная двум и выше, свидетельствует о том, что процессор *не успевает* выполнять все задачи.

  Происходит это потому, что в системе одновременно выполняются различные процессы. Они достаточно случайным образом формируют задания процессору на обслуживание требующихся им вычислений. Процессор же не успевает переключаться между ними и оперативно "выполнять" возникающие требования. В результате эти задания становятся в очередь, процент загрузки процессора остается низким (основное время тратится на переключения между заданиями), а система в то же время крайне медленно реагирует на команды.

  Большая величина очереди может быть обусловлена не только значительным числом одновременно выполняющихся заданий, но и неисправностью какого-либо устройства, например, сетевого адаптера, генерирующего большое число прерываний в единицу времени. Для локализации этой причины следует провести анализ параметра **Processor\Interrupts/sec** *(см. далее)*.

  Если высокое значение параметра очереди заданий является следствием большого количества задач, которые одновременно должен выполнять компьютер, то решение проблемы заключается либо в снятии некоторых вычислений, либо перераспределении задач между несколькими компьютерами, либо замене модели на более производительную. Пользователь практически не имеет возможности оптимизировать процесс переключения между различными задачами. Можно только попробовать изменить приоритет приложений и фоновых задач (на вкладке **Дополнительно** задачи **Система** в Панели задач) и проверить результат.

  Замечание

  Часто многие процессы не являются необходимыми для данной системы. Например, можно отключить режим онлайнового контроля вирусов в те моменты, когда не поступают новые данные. Или отказаться от индексирования файлов и т. п. Кроме того, можно отключить службы Windows, которые не используются на данной системе.

- **Processor\Interrupts/sec** — счетчик показывает число запросов на обработку для процессора. Максимальное число прерываний, которое может обработать процессор, зависит от его типа. Для разных процессоров эта величина колеблется от 500 до 2000 прерываний в секунду.

Поскольку высокое значение данного счетчика может быть следствием неисправности оборудования, следует выяснить, что является источником повышенного количества запросов в единицу времени. Для этого можно задействовать счетчики объекта Thread, например, **%Processor Time**. Эти счетчики отображают в том числе состояние каждой нити, которую запускает отдельный процесс. Переключив отображение монитора системы на гистограмму, вы можете увидеть процесс, "монополизирующий" ресурсы компьютера.

Оценка использования оперативной памяти

В случае недостаточной производительности не лишним будет убедиться, что в системе установлена наиболее быстродействующая марка модулей оперативной памяти (если материнская плата поддерживает несколько модификаций).

> ***Примечание***
>
> Следует внимательно изучить рекомендации вендора по установке модулей памяти, поскольку простое увеличение числа модулей может одновременно снизить их тактовую частоту.

- **Объем свободной памяти** — в современных операционных системах этот показатель не отражает реальные потребности программ. Операционная система изначально стремится занять *всю* оперативную память, чтобы обеспечить максимальное быстродействие. Следует обратить внимание на показатели фактической загрузки памяти.
- **Memory\Pages/sec.** — один из интегральных показателей использования оперативной памяти. Счетчик демонстрирует число запросов страниц памяти из файла подкачки на диске. Критическое значение данного показателя составляет около 20 единиц. Когда системе не хватает физической памяти для текущей работы, она начинает обмен страницами памяти с файлом подкачки. Постоянный интенсивный обмен — 20 и более страниц в секунду — свидетельствует о недостатке оперативной памяти. Выход — добавить физическую память.

Оценка дисковой подсистемы

- **LogicalDisk (PhysicalDisk)\Avg. Disk Queue Length** — счетчик показывает среднюю очередь заданий (операций записи или чтения) для соответствующего диска. Интерпретация данного параметра достаточно проста. Если существует очередь на дисковые операции (значение счетчика достигает единицы и более), то это означает, что диски не справляются с записью/чтением информации.

Какие могут быть варианты решения проблемы при обнаружении узкого места в дисковой подсистеме?

Прежде всего, следует убедиться, что в системе установлено достаточно оперативной памяти. В противном случае повышается нагрузка на виртуальную память, что приводит к увеличению количества дисковых операций на служебные цели.

Обратите внимание, чтобы на дисках было достаточно свободного места (не менее 20% их объема). Проведите дефрагментацию дисков, уменьшите или исключите сжатие и шифрование файлов на тех дисках, на которых выявлена проблема низкой производительности. Отключите дополнительные задачи, ведущие запись информации на диск (например, откажитесь от протоколирования событий безопасности и т. п.).

При возможности следует разместить информацию на различных физических дисках, а лучше — на томах с чередованием записи данных, причем такую RAID-конфигурацию в крайнем случае можно создать и программным способом из нескольких дисков. Наиболее быстрая и отказоустойчивая конфигурация — RAID 0+1.

> ***Замечания***
>
> Например, на одном физическом диске расположить файл подкачки, на другом — рабочие базы данных. Или, в случае сервера баз данных, на одном диске сохранять файлы баз данных, а на другом — файлы протоколов (log files). При этом не забывайте, что не следует подключать диски различной производительности к одному контроллеру.
>
> Наиболее распространенная на практике конфигурация RAID — RAID5, практически не уступая RAID10 в операциях *чтения*, весьма существенно проигрывает по производительности в операциях *записи*.

Следует рассмотреть возможность размещения критичной по скорости обмена информации на твердотельных (SSD) дисках. Несмотря на ограниченный срок службы, SSD-диски обеспечивают производительность, сравнимую с RAID-массивом, составленным из десятка обычных жестких дисков.

Ну и последний вариант — реализация внешней специализированной системы хранения. Конечно, это дорогое решение, но часто и единственное.

- **% Disk Time** — счетчик показывает процент времени, в течение которого система "занята" операциями ввода/вывода. Значения счетчика, достигающие порядка 50%, свидетельствуют о необходимости замены дисковой подсистемы на более быструю.

Оценка работы сетевого адаптера

Для использования счетчика **Network Segment: % Net Utilization** должен быть установлен драйвер Network Packet Protocol из программы Network Monitor.

Счетчик отображает текущую загрузку сегмента компьютерной сети, к которому подключен компьютер. Для сети, выполненной по стандарту Ethernet, — а это практически все локальные компьютерные сети, величина утилизации сети 60–70% считается критической; на практике следует внимательно проанализировать работу сети уже при достижении порога утилизации порядка 30–40%. При необходимости столь интенсивной пересылки данных следует перейти на сеть с более высокой производительностью или выделить нагруженные участки в отдельный сегмент. Следует также максимально заменить сетевые концентраторы коммутаторами.

> ***Замечание***
>
> Администраторы обычно используют для оценки состояния сети различные SNMP- и RMON-мониторы, которые имеют возможность автоматически высылать предупреждения при достижении установленных пороговых значений.

Счетчики прикладных программ

После установки программного обеспечения (SQL, Axapta, Exchange и т. п.) число параметров, отображаемых в задаче **Производительность**, может увеличиваться. Анализ данных таких счетчиков следует проводить по технической документации соответствующего программного продукта.

В большинстве случаев показания счетчиков будут полезны только для высококвалифицированных специалистов служб технической поддержки, хотя администраторы могут учитывать некоторые интегральные показатели при оценке состояния системы.

В любом случае конечным итогом анализа таких счетчиков будет вывод о достаточности или о необходимости добавления одного из следующих ресурсов: процессора (в том числе, понимая под этим и замену платформы на более производительную модель), оперативной памяти, дисковой подсистемы, сетевого адаптера.

Server Performance Advisor

Для серверов Windows Server 2003 разработчик предлагает специальную программу (ее можно бесплатно загрузить с сайта разработчика) для комплексного анализа производительности — Server Performance Advisor (рис. 10.9).

Эта программа практически в автоматическом режиме собирает значения различных счетчиков операционной системы и программного обеспечения и формирует комплексный отчет.

На рис. 10.9 показана часть отчета, сформированного программой по результатам обследования производительности сервера. Как правило, необходимость в подобных отчетах возникает при подготовке материалов для руководителя соответствующего подразделения. К сожалению, возможностей оперативного формирования печатной версии документа в программе не предусмотрено.

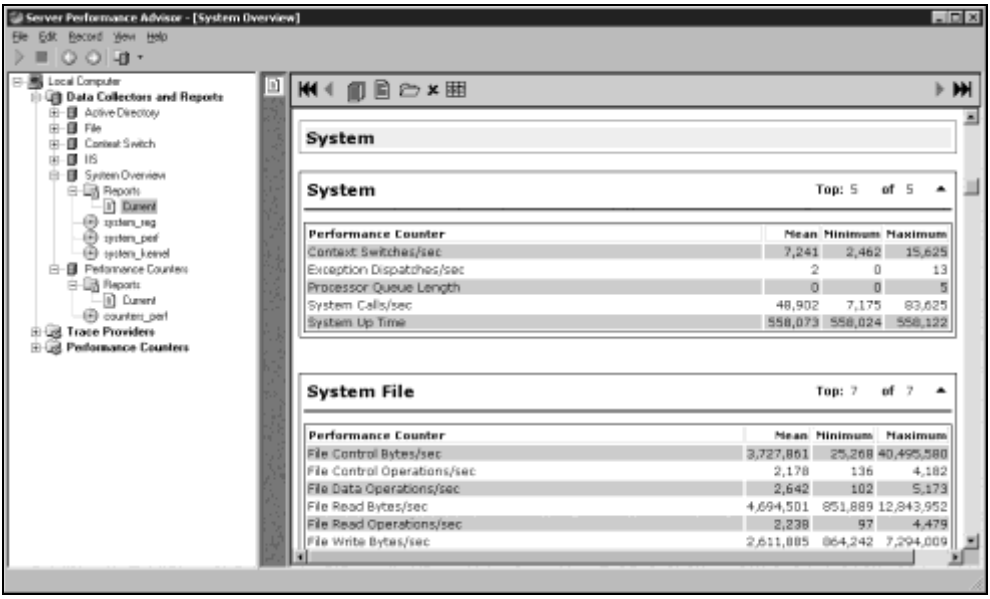


Рис. 10.9. Server Performance Advisor

Программа полезна, прежде всего, тем, что позволяет собрать за одну операцию показания многих счетчиков и усреднить их за некоторый период времени. Программа фактически помогает сделать первичный обзор состояния системы с тем, чтобы впоследствии более углубленно изучать причины конкретных узких мест. Опции программы позволяют настроить детализацию сбора информации и включить в анализ различные подсистемы. Значения усредненных показателей, получаемых программой, помогут при дальнейшем углубленном анализе производительности.

Программа предназначена для серверов Windows Server 2003 и требует для установки выполнения некоторых условий (например, поддержку .NET), что не позволяет работать с ней без дополнительных настроек на всех системах.

Диагностика доступа к ресурсам компьютера

Для поиска проблем администратору часто необходимо отслеживать процессы доступа программ к файлам, к реестру системы и т. д. Наблюдение за такими процессами может существенно помочь в выяснении причин сбоев. В этом случае могут помочь бесплатные утилиты, которые можно загрузить с сайта **www.sysinternals.com** (рис. 10.10).

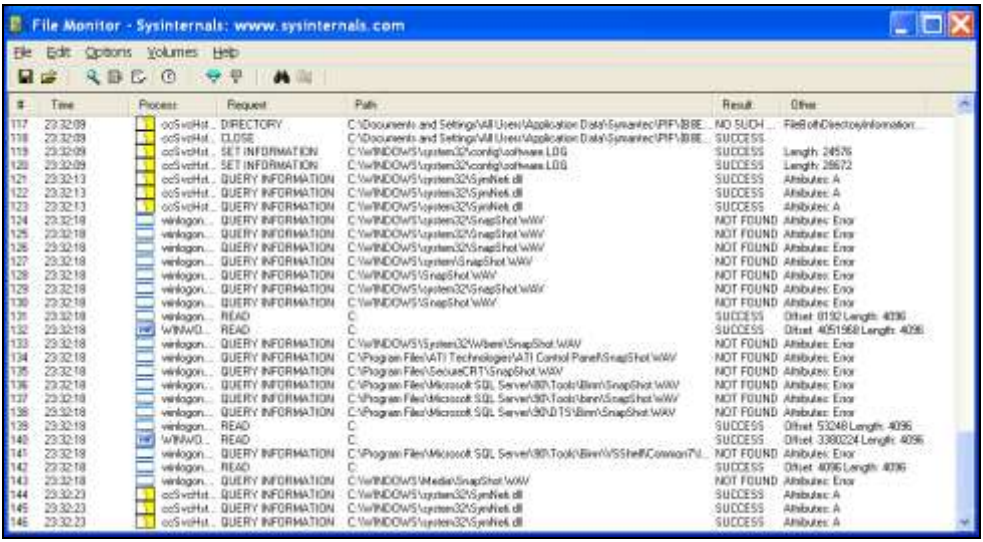


Рис. 10.10. Программа протоколирует операции доступа к файлам компьютера



Глава 11

Организация IP-телефонии офиса

Программная АТС

Телефонную станцию офиса можно создать на основе как аппаратных решений (приобрести офисную АТС), так и программными средствами. Последние используют технологию VoIP (Voice over IP) — голоса поверх Интернета.

VoIP позволяет осуществлять звонки более экономично, чем с применением традиционных каналов связи. При этом на самой АТС можно реализовать обслуживание существенно более высокого класса: внедрить систему голосового меню любой сложности ("*нажмите 2 для переключения к абоненту*"), использовать голосовую почту (запись сообщений и отправку их на адрес электронной почты), устанавливать приоритет звонков (на основе времени суток, номера звонящего и т. п.), автоматически обнаруживать, принимать факсы и пересылать их по электронной почте, настраивать автоматическую переадресацию звонка на основе любых доступных критериев и т. п.

> ***Примечание***
>
> Использование VoIP предъявляет повышенные требования к каналам передачи данных. Пакеты, передающие голосовое сообщение, должны быть доставлены без потерь и задержки. В противном случае возникают различные "бульканья", речь становится неразборчивой, возможны просто случаи разрыва связи. Поэтому обычно голосовой трафик выделяют в отдельную VLAN, для которой настраиваются особые классы обслуживания (CoS), предусматривающие приоритет передачи данных пакетов перед другими данными. В больших сетях подобная настройка является нетривиальной, поскольку требует учета параметров передачи различной информации, дополнительной конфигурации оборудования по специальным требованиям (например, изменения объемов буферов для различных очередей) и т. д.

Телефонная станция легко может быть реализована программными средствами. Существует много бесплатных программных АТС как для Linux-систем, так и предназначенных для установки на Windows (например,

FreePBX — **http://www.freepbx.org**, Trixbox — **http://www.trixbox.org**, российская разработка **http://altertex.ru/ip-telephonia/ip-acs/**, телефонная станция для Windows с поддержкой конференций, голосового меню, интеграцией с Outlook — **http://www.codeplex.com/callbutler** и др.).

Безусловный лидер программных АТС — проект Asterisk, на базе которого создано несколько предварительно сконфигурированных свободно распространяемых программных АТС. Некоторым неудобством этих проектов является то, что пользователю предлагается готовое решение на конкретной платформе Linux. С другой стороны, при использовании такого комплекта можно быть уверенным в том, что после установки для внедрения АТС достаточно будет только внести в нее конкретные настройки.

Подключение IP АТС к телефонным станциям общего пользования

Большинство руководителей плохо представляют, как можно обеспечить работу IP АТС с "обычными" телефонными станциями. Существуют различные варианты организации такого взаимодействия.

Во-первых, все больше провайдеров предлагают услуги IP-телефонии. В этом случае вы подключаетесь к АТС общего пользования через телефонную станцию провайдера. Никакого дополнительного оборудования от офисной АТС не требуется: взаимодействие с АТС провайдера происходит по тому же каналу, что и работа в Интернете.

Второй вариант предполагает использовать в качестве точки подключения специализированные сети интернет-телефонии, например, SIPNET (**http://www.sipnet.ru/**). Вы покупаете у оператора учетную запись этой сети, выбираете наиболее удобный тариф для звонков и настраиваете свою программную АТС для работы через такую сеть, указывая параметры приобретенной учетной записи в настройках SIP-прокси.

Третий способ заключается в приобретении дополнительного оборудования, которое позволит подключить программную IP АТС к обычным аналоговым телефонным линиям. Такие устройства называют голосовыми шлюзами (VoIP-шлюзами).

> ***Примечание***
>
> Стоимость голосовых шлюзов составляет менее 90 долл. в расчете на одну линию подключения к АТС, причем эта величина уменьшается при увеличении числа портов шлюза. Следует также учесть, что голосовой шлюз может работать в качестве аппаратного межсетевого экрана при организации доступа в Интернет, что еще существенно снижает стоимость чисто голосовых функций такого устройства.

При выборе модели голосового шлюза следует учитывать типы и количество портов этого устройства. Порты могут быть FXS и FSO. К портам FSX подключается оконечное оборудование: телефонные аппараты, факсы. К портам FSO подключаются линии от аналоговых АТС. Поэтому если вам необходимо подключить один обычный телефонный номер к программной АТС, то достаточно найти голосовой шлюз с одним FSO-портом.

IP-телефоны: выбор и необходимые настройки сети

Для работы с Asterisk можно выбрать любые IP-телефоны, поддерживающие протоколы SIP и/или IAX.

> ***Примечания***
>
> В Asterisk можно добавить и поддержку протокола H323 (она не входит в пакет, предоставляемый по умолчанию для установки через репозитории Ubuntu на момент написания книги; необходимо скомпилировать Asterisk из исходных кодов, включив поддержку h323). Однако этот протокол постепенно "уходит" из практики, поскольку с ним достаточно сложно обеспечить, например, работу IP-телефонов через NAT или межсетевые экраны. Поэтому мы рекомендуем ограничиться только этими протоколами.
>
> В Сети рекомендуют не использовать модели телефонов Cisco, поскольку они оптимизированы под собственные протоколы и достаточно тяжело поддаются перепрограммированию на открытые стандарты.

Еще одно интересное решение — *программный* телефон. Легко можно найти различные варианты бесплатных продуктов (например, поиском по терминам *softphone free download*), выбор только за вами.

Одним из наиболее функциональных вариантов программных бесплатных телефонов является Kapanga (**http://www.kapanga.net/**). Он поддерживает передачу голоса, видео, может принимать факсы, отправлять SMS и т. п. В силу его расширенной функциональности этот вариант может быть рекомендован для практического использования, но не является лучшим на момент первоначального знакомства с Asterisk.

Поскольку для пользователя более привычно при телефонных разговорах держать в руках трубку, то можно купить телефоны-трубки, подключающиеся непосредственно к компьютеру. Это самый дешевый вариант оборудования, однако разговаривать по телефону можно только во время работы компьютера.

Более удобны, но и более дороги модели, подключаемые в локальную сеть. У вас есть выбор от самых дешевых моделей неизвестных изготовителей до оборудования ведущих вендоров, таких как Nortel или Avaya.

IP-телефоны обычно требуют дополнительной настройки ряда сетевых служб. Как правило, необходимо настроить соответствующим образом DHCP-сервер организации, включив в него параметры, по которым IP-телефоны определяют телефонную станцию. Возможно, что также придется откорректировать сценарии для телефонов, которые они получают с сервера загрузки, и разместить на одном из серверов сети соответствующие файлы конфигураций.

Покажем на примере телефонов Avaya операции, которые потребуются для IP-телефонов.

Настройки, необходимые для работы телефона Avaya, он получает в специальной дополнительной опции DHCP-сервера (ее номер 176). Эти настройки сообщают ему адрес TFTP-сервера, с которого телефон загрузит (обновит) свою конфигурацию и IP-адрес телефонной станции.

Часто в сетевой порт подключают телефон, а уже в порт на телефоне — компьютер. В то же время принято выделять голосовой трафик в отдельную VLAN. Делается это как из соображений безопасности (чтобы нельзя было записать разговоры), так и из целей оптимизации (для VLAN проще настроить гарантированную полосу пропускания и качество обслуживания). Чтобы работать при таком варианте подключения, IP-телефоны Avaya могут получать от DHCP-сервера сведения о номере голосовой VLAN. Эти настройки игнорируются компьютером, но заставляют телефон выполнить повторный запрос на получение IP-адреса уже из состава нужной VLAN.

В листинге 11.1 приведен пример блока настроек файла конфигурации сервера DHCP для Linux (файл /etc/dhcp3/dhcpd.conf), определяющих параметры IP-адреса для компьютеров (блок `data`) и телефонов (блок `voice`).

Листинг 11.1

```
option option-176 code 176 = string;
shared-network data {
subnet 192.168.3.0 netmask 255.255.255.0 {
option routers 192.168.3.1;
option broadcast-address 192.168.3.255;
option option-176 "L2Q=1,L2QVLAN=20";
range 192.168.3.100 192.168.3.200;
}
}
shared-network voice {
subnet 192.168.2.0 netmask 255.255.255.0 {
option routers 192.168.2.1;
```

```
option broadcast-address 192.168.2.255;
option option-176
"MCIPADD=192.168.2.20,MCPORT=1719,TFTPSRVR=192.168.3.100";
range 192.168.2.100 192.168.2.200;
}
}
```

Первая строка определяет (создает) новую строковую опцию в числе параметров DHCP-сервера, а следующие два блока определяют параметры, которые получают при настройке IP-адреса клиенты. Обратите внимание на параметр 176. В блоке для компьютеров он сообщает, что голосовая сеть будет настроена как VLAN с номером 20, а в блоке для телефонов этот параметр уже сообщает адрес телефонной станции, порт подключения и адрес TFTP-сервера.

Сам TFTP-сервер необходимо установить на какой-либо компьютер, например, на тот же, на котором расположена программная АТС. Существуют различные реализации данного сервера, мы установим TFTP-сервер следующей командой:

```
apt-get install tftpd-hpa
```

После установки пакета необходимо отредактировать файл его настроек. Откройте файл /etc/default/tftpd-hpa и замените в строке `RUN_DAEMON="no"` символы `"no"` на `"yes"`. Обратите внимание также на папку, в которую необходимо будет помещать конфигурационные файлы телефонных аппаратов. По умолчанию это /var/lib/tftpboot (указано во второй строке настроек сервера TFTP). Стартовать демон можно командой /etc/init.d/tftpd-hpa start. Правильность установки можно проверить, если просмотреть файл /etc/inetd.conf и найти в нем следующую строчку:

```
tftp dgram udp wait root /usr/sbin/in.tftpd /usr/sbin/in.tftpd
-s /var/lib/tftpboot
```

Далее необходимо скачать с сайта Avaya необходимые конфигурационные файлы и скопировать их в папку /var/lib/tftpboot.

> ***Примечание***
>
> Обратите внимание, что для некоторых моделей телефонов Avaya вендор требует сначала обновить прошивку h323 до последней версии и только потом перепрограммировать их для работы с протоколом SIP.

Кроме того, следует загрузить файл настроек телефона (например, 46xxsettings.txt), отредактировать его в части используемых параметров (например, адрес SIP-сервера) и также поместить в папку TFTP-сервера.

Примечание

При желании, можно создать файлы настроек для каждого телефонного аппарата (базируясь на их MAC-адресах) и также разместить их в папке TFTP-сервера. В этом случае, например, можно установить строгие пароли, которые телефон автоматически будет вводить при включении.

Установка Asterisk

Для Ubuntu существует подготовленный пакет Asterisk, который можно установить стандартными средствами системы с использованием `apt-get`. В то же время, некоторые функции телефонной станции могут потребовать либо установки более свежей сборки пакета, либо добавления новых модулей. В этом случае необходимо провести установку АТС на основе исходных кодов.

Сразу после установки пакета АТС готова к работе: для того, чтобы она начала обслуживать пользователей, достаточно только зарегистрировать IP-телефоны и создать распределения звонков.

То, что установка Asterisk прошла успешно и телефонная станция работает, можно проверить, выполнив команду

```
asterisk -vvvvvc
```

Замечание

Последовательность символов `v` в параметре запуска указывает на необходимость отображения расширенного протоколирования в консоли Asterisk. Точно так же можно указать несколько `v` (количество `v` соответствует уровню протоколирования: чем больше, тем выше, возможные значения — до 5) в команде подключения к работающему Asterisk (`asterisk -vvvvvr`). После такого подключения Asterisk остается на соответствующем уровне протоколирования и при последующих подключениях к консоли. Чтобы отключить расширенное протоколирование, выполните в консоли команду `core set verbose 0`.

В результате ее выполнения вы должны войти в консоль управления АТС; при старте консоли будет показано много служебных сообщений программы, завершится ее загрузка отображением приглашения Asterisk. На все эти служебные сообщения не будем пока обращать внимания и завершим работу в консоли АТС командой

```
exit
```

Если АТС уже работает (демон стартовал), то для подключения к консоли следует выполнить такую команду:

```
asterisk -r
```

Существуют варианты телефонных станций, разработанных на основе Asterisk и имеющих графический интерфейс управления. Вы можете при желании

использовать и такой вариант АТС (рис. 11.1). Кроме того, доступны различные пакеты графического управления Asterisk. Например, Asterisk Manager Suite (**http://Webscripts.softpedia.com/script/Communication-Tools/Asterisk-Manager-Suite-24429.html**), GlassConsole (**http://www.asteriskvoipnews.com/asterisk_software/glassconsole_windows_xp_monitoring_console_for_asterisk_ipbx.html**) и другие. Мы не описываем их настройку, поскольку при некоторой усидчивости ее легко выполнить в режиме консоли.



Рис. 11.1. Интерфейс управления АТС Trixbox

На рис. 11.1 представлено окно управления АТС Trixbox. В графическом интерфейсе можно выполнить все конфигурирование системы (на рисунке представлена операция добавления групп вызова). Подобный графический интерфейс можно применить и для настройки Asterisk; соответствующие

программы легко найти в Интернете. Однако следует учесть, что обычно настройка станции выполняется при начале ее работы и очень редко меняется в процессе эксплуатации. Поэтому системы, обслуживающие в реальных условиях большое число пользователей, не следует обременять подобными надстройками.

Локализация Asterisk

В Asterisk есть ряд действий, связанных с речевым ответом станции. Например, при включении голосовой почты станция предупреждает звонящего о недоступности абонента и предлагает записать сообщение. Понятно, что исходный пакет Asterisk включает такие сообщения на английском языке.

В Интернете легко можно найти локализованные звуковые файлы (искать следует по ключевым словам "*asterisk coresounds ru*"). Например, они доступны со страницы **http://www.filewatcher.com/m/asterisk.1.4.coresounds.ru.tar.bz2.1493025.0.0.html**. Для локализации Asterisk проще всего загрузить эти звуковые файлы и заменить ими оригинальные версии.

Первоначальная проверка Asterisk

После установки пакета (или после инсталляции из исходных кодов с установкой файлов демо-конфигурации) в системе создан пример плана звонков, который позволяет осуществить звонки на некоторые предопределенные номера. В частности, можно позвонить на демо-номер разработчика (если соединение с Интернетом настроено), прослушать приветствие Asterisk или, например, записать свое сообщение и прослушать его (с использованием голосового меню).

Проще всего к Asterisk подключить программные телефоны. Загрузите программу любого такого телефона и установите на свой компьютер (рис. 11.2).

Как правило, в документации на программный телефон описаны те настройки, которые необходимо выполнить для подключения к Asterisk (поскольку это, практически, самая популярная IP АТС). Обычно требуется указать в конфигурации IP-адрес сервера Asterisk в качестве SIP-прокси для данного аппарата и записать настройки номера телефона и пароля подключения. В крайнем случае, соответствующие рекомендации легко найти в Сети.

После настройки параметров программного телефона зарегистрируем его в Asterisk. Для этого добавим в файл /etc/asterisk/sip.conf, который описывает обслуживаемые SIP-телефоны, блок листинга 11.2.



Рис. 11.2. Интерфейс программного телефона

Листинг 11.2

```
[20]
type=friend
host=dynamic
username=20
secret=20
```

Этим блоком мы определили пользователя 20 (параметр `username`), который будет подключаться к линии 20 (заголовок `[20]`) и имеет пароль 20 (параметр `secret`). При этом подключение может осуществиться с любого IP-адреса (параметр `dynamic`), а пользователь может как звонить, так и принимать вызовы (параметр `type`). Поскольку в параметрах явно не указан контекст звонка, то будет выбрано значение по умолчанию.

Далее, необходимо добавить в Asterisk новую телефонную линию (номер телефона). Отредактируйте файл /etc/asterisk/extensions.conf. Найдите в нем строку [default] и вставьте после нее:

```
exten => 20,1,Dial(SIP/20,20)
```

Эта строка указывает программе, что при наборе номера 20 должен быть осуществлен звонок на SIP-аппарат с зарегистрированным номером 20.

> ***Замечание***
>
> Часто пользователи путаются в понимании номеров линии и телефона. В IP-телефонии эти два номера регистрируются отдельно, что добавляет гибкости в настройки распределения вызовов.

Сохраните отредактированные вами файлы sip.conf и extensions.conf. Если Asterisk уже запущен, то зайдите в его консоль (`asterisk -r`) и перезагрузите данные из этих файлов командами

```
sip reload
dialplan reload
```

Теперь можно проверить, что ваш телефон зарегистрировался в Asterisk, командой

```
sip show peers
```

Пример ответа иллюстрирует листинг 11.3.

Листинг 11.3

```
CLI> sip show peers
Name/username              Host            Dyn Nat ACL Port     Status
20/20                      192.168.31.190   D          5060     UNREACHABLE
1 sip peers [Monitored: 0 online, 0 offline Unmonitored: 0 online, 1 offline]
```

> ***Замечание***
>
> Обычно программные аппараты сообщают на экране результаты регистрации на сервере, так что необходимость описанной проверки возникает редко.

Если телефон не отображается, то необходимо искать ошибки в настройках, скорее всего, ошибки были допущены в конфигурации программного телефона.

Если все нормально, то вы сможете проверить станцию, совершив звонок по одному из демонстрационных номеров.

> ***Замечание***
>
> Полный список легко понять, просмотрев блок `[demo]` в файле /etc/asterisk/extensions.conf.

Например, звонок по номеру 500 позволит услышать приветствие, после которого будет произведена попытка подключения к АТС разработчиков Asterisk; звонок по номеру 600 позволит записать вашу фразу и потом прослушать ее (так называемый, *эхо-тест*) и т. д.

Настройка АТС

После успешного тестового звонка необходимо приступать к настройке рабочей конфигурации телефонной станции. Для лучшей безопасности желательно сохранить существующие файлы конфигураций под другими именами и создать собственные, пустые файлы.

> ***Примечание***
>
> Внутри всех файлов конфигураций приведены подробные пояснения, которые можно использовать для самостоятельной настройки. Большинство параметров закомментировано и не используется. При недостатке опыта, можно только закомментировать тестовые номера в файле конфигурации. В этом случае рекомендации по настройке будут всегда перед глазами.

Вам необходимо как минимум выполнить две операции:

- определить в конфигурации телефонные линии (extensions) и правила набора;
- добавить в конфигурацию пользователей телефонной станции (SIP-телефоны).

Но прежде чем описывать правила составления конфигураций АТС, укажем, как можно получить дополнительную информацию для устранения возможных ошибок в процессе редактирования.

Диагностика АТС

При настройке Asterisk на первых этапах приходится часто исправлять ошибки различных конфигураций. Дополнительная информация, которая может быть выведена в консоль программы, существенно облегчит поиск подобных ошибок. Для увеличения объема отладочной информации выполните в консоли Asterisk команду

```
core set verbose 5
```

> ***Замечание***
>
> Увеличение числового параметра в этой строке увеличивает объем выводимой информации. На практике обычно достаточно указывать в качестве значения уровня подробности число 5.

Чтобы увидеть сообщения, сопровождающие процесс звонков, нужно включить режим отладки. Например, для SIP-протокола нужно выполнить

```
sip set debug
```

Если с АТС уже работает несколько телефонов, то объем информации на экране будет такой, что вы просто не сможете за ней уследить. В этом случае

удобно включить режим вывода сообщений только для того устройства, работу с которым вы настраиваете:

```
sip set debug ip IP-адрес
```

После исправления ошибок следует отключить отладку программы и установить исходный уровень сообщений (`core set verbose 0`, `sip set debug off`).

> ***Совет***
>
> В процессе настройки АТС часто возникают ошибки в создании правил плана звонков. Чтобы вывести в консоль Asterisk какую-либо информацию, показать значения переменных и т. п., используют функцию `NoOp()`. Если она указана в плане звонков, то программа выводит на экран значение выражения, содержащегося в скобках, не выполняя никаких других действий. После нахождения ошибки строку с `NoOp` можно просто закомментировать.

Настройка конфигурации SIP-телефонов

В АТС должны быть зарегистрированы телефонные аппараты, которые она обслуживает. Все телефоны определяются в файле sip.conf (при подключении по протоколу SIP). Причем в одном файле описываются все подключения: как внешние, так и локальные линии. Принципиального различия между этими номерами телефонов нет.

> ***Замечание***
>
> Существует возможность автоматической регистрации аппаратов, но мы не будет ее касаться в настоящей книге.

Каждый телефонный номер описывается отдельным блоком, который начинается с номера телефона, заключенного в квадратные скобки. Далее следует описание ряда параметров этого номера (например, отображаемое на дисплее имя, пароль подключения и т. д.).

Хотя все телефоны и описаны в одном файле, но их можно логически разделить. В этих целях применяется параметр `context`. Все телефоны, у которых параметр `context` имеет одинаковое значение, могут звонить друг другу, просто набирая номер соответствующего телефона. Если же в пределах данного контекста набираемого номера нет, то Asterisk начинает применять правила, указываемые в плане звонков. Каждому контексту в этом файле должен соответствовать контекст в плане набора.

> ***Примечание***
>
> Чтобы обезопасить станцию и исключить возможность для внешних пользователей выполнять звонки на внешние линии через телефонную станцию, входящие линии и локальные *обязательно* должны быть отнесены к различным контекстам.

Листинг 11.4 содержит примерное описание телефона.

Листинг 11.4

```
[190]
type=friend
context=office
secret=пароль
username=имя
qualify=yes
Callgroup=1
pickupgroup=1
callerid="Имя" <190>
host=dynamic
mailbox=190@office
```

Этот листинг определяет телефонный аппарат с номером 190. По сравнению с предыдущим примером, описывавшим тестовую конфигурацию, мы добавили несколько строк. Обратите также внимание, что вместо номера линии в параметре `username` указано имя пользователя, которое будет отображаться на дисплее телефонного аппарата.

Параметр `context` определяет контекст, в который будет помещена линия 190; соответственно, в файле extensions.conf должен быть определен контекст office и в него помещены правила набора для линии 190. Параметр `qualify` указывает Asterisk о необходимости контроля доступности аппарата (вы можете увидеть реальные параметры доступности, выполнив в консоли команду `sip show peers`). Параметры `callgroup` и `pickupgroup` определяют группы для данного номера абонента. Так, с номера 190 можно перехватить только звонки, поступившие на номера, также входящие в группу (pickupgroup) 1. Параметр `mailbox` указывает программе номер ящика голосовой почты; при наличии в нем сообщений, на телефонном аппарате будет выдаваться соответствующее предупреждение.

После изменения состава телефонных линий (аппаратов), с которыми будет работать Asterisk, нужно перезагрузить конфигурацию sip командой `sip reload`.

Настройка плана звонков

Практически вся функциональность телефонной станции Asterisk определяется планом звонков. План звонков — это набор инструкций для телефонной станции, которые она должны выполнить при наборе пользователем какого-

либо телефонного номера. Этот план определяется в файле /etc/asterisk/extensions.conf.

Примечания

План звонков можно определить в другом формате, более близком к синтаксису программных кодов (см. файл extensions.ael). Но мы в примерах будем придерживаться традиционных описаний.

По соображениям безопасности следует переименовать файл примера и начать настройку станции с пустого плана звонков.

Параметры конфигурации плана звонков собраны в этом файле по блокам; блоки начинаются с заголовков в квадратных скобках. Эти блоки принято называть *контекстами*. Сделано это как для удобства (легче контролировать правильность большого плана звонков, если он разбит на отдельные блоки), так и из соображений безопасности (для абонентов набор номеров доступен только в пределах одного блока; возможность набора номера, не входящего в данный контекст, должна быть явно предусмотрена правилами набора). Контексты упрощают создание автоответчиков, голосового меню и т. п.

Примечание

При составлении плана звонков следует четко представлять, как программа будет выбирать линию в случае использования шаблонов при их определении. Asterisk при выполнении плана звонков не учитывает последовательность описания номера. Если в плане звонков программа находит несколько номеров, которые удовлетворяют условиям определения номера (например, два различных шаблона, которым соответствует набираемый номер), то выполнение будет передано на самый конкретный шаблон. Если в данном контексте содержится несколько директив `include` (включение другого контекста), то extensions будут искаться в контекстах последовательно, в соответствии с очередностью включения блоков.

В начале файла обычно присутствуют два служебных блока — general, в котором определены параметры всей программы, и globals, в котором описываются глобальные переменные. Как правило, их сохраняют в значениях по умолчанию, если не необходимо иное.

Контекстам можно давать любые названия, предопределены только названия макрокоманд, которые должны начинаться с символов `macro-`.

Один контекст можно включить в другой. Делается это следующей строкой:

```
include => название_контекста
```

Примечание

На первых порах не стоит увлекаться вложением контекстов, поскольку такая конфигурация усложняет отладку телефонной станции.

Все правила набора строятся по единому синтаксису. Каждый номер должен быть зарегистрирован строками вида:

```
exten => номер,приоритет,действие
```

В качестве *номера* должен быть указан номер телефона, например, 200 (точнее, допускается название линии, состоящее из цифр и букв. Символьные названия часто используются при описании SIP-абонентов сети Интернета, а локальные номера, которые необходимо набирать с клавиатуры телефона, состоят только из цифр).

Кроме явного указания номеров телефона в Asterisk предусмотрены специальные линии (табл. 11.1).

Таблица 11.1. *Стандартные линии Asterisk*

Линия	**Назначение**
a	Этот номер будет набран, если во время приглашения голосовой почты пользователь нажмет на телефоне "*"
h	Соответствует событию прекращения разговора (например, если после того, как пользователь положил трубку, вы хотите еще воспроизвести в линию какое-либо сообщение вызывающему абоненту)
i	На эту линию будет передано управление, если номер линии неверен
o	Линия администратора (управление передается, если пользователь нажимает "0" во время приглашения голосовой почты)
s	Это начальная линия: на нее управление будет передано, если Asterisk не найдет явно указанного номера телефона
t	Линия, на которую управление перейдет при тайм-ауте звонка
T	Линия, на которую управление перейдет в случае абсолютного тайм-аута — AbsoluteTimeout()
failed	Служит для автоматического обзвона
fax	Используется в случае обнаружения сигналов передачи факса (при наличии соответствующих настроек и модулей)
talk	Применяется вместе с функцией BackgroundDetect

Номера линий можно указывать также с помощью шаблонов, это позволяет одной инструкцией определить правила обработки сразу для большого коли-

чества линий, например, для междугородних звонков. Если номер линии указан как шаблон, то он должен начинаться всегда с символа подчеркивания (_). Далее описаны правила построения шаблонов.

Для каждой линии можно определить несколько операций, которые Asterisk будет выполнять в порядке значений, указанных в поле `приоритет`. Например, сначала может быть проиграно голосовое приветствие и только потом осуществлен звонок на указанный номер. Приоритеты могут нумероваться 1, 2, 3 и т. д. (допускается пропускать номера, Asterisk будет использовать в порядке сортировки). Это не всегда удобно, особенно если для линии написано много правил: добавление новой строки приводило бы в этом случае к перенумерации всех последующих правил. Поэтому принято первой строке назначать номер 1, а последующим — *n*. В этом случае Asterisk будет выполнять операции в том порядке, в каком строки присутствуют в файле extensions.conf.

Приоритетам можно присваивать метки, например, так:

```
exten => s,n(my),Answer
```

Впоследствии на эту позицию при обработке звонка можно перейти с помощью функции `Goto(my)`.

В качестве действия в строке описания линии задается та или иная функция Asterisk: ответ на звонок, проигрывание голосового сообщения, набор конкретной линии, переадресация к голосовой почте и т. п. Посмотрите пример обработки звонка из файла примеров в макросе `stdexten` (листинг 11.5). Этой макрокоманде в качестве первого аргумента (`${ARG1}`) передается номер телефона, с которого осуществляется звонок, а вторым аргументом является номер, который должен быть набран.

Листинг 11.5

```
[macro-stdexten];
exten => s,1,Dial(${ARG2},20)
exten => s,2,Goto(s-${DIALSTATUS},1)
exten => s-NOANSWER,1,Voicemail(${ARG1},u)
exten => s-NOANSWER,2,Goto(default,s,1)
exten => s-BUSY,1,Voicemail(${ARG1},b)
exten => s-BUSY,2,Goto(default,s,1)
```

Сначала программа пытается набрать заданный номер (`${ARG2}`). Набор производится в течение 20 с. Дальнейшая обработка осуществляется в зависимости от состояния ответа, которое Asterisk хранит в переменной `${DIALSTATUS}`.

Абонент может ответить на звонок (состояние ANSWER), телефон может быть занят (BUSY), канал недостижим (CHANUNAVAIL), просто никто не поднял трубку (NOANSWER) или система перегружается (CONGESTION). Макрос переадресовывает звонок на новый номер, название которого формируется динамически, в процессе обработки звонка, например, при отсутствии ответа — на номер `s-NOANSWER`, и звонящий подключается к голосовой почте с сообщением о причинах недостижимости (проигрываются разные сообщения).

Другой способ использования состояния ответа на звонок представлен в листинге 11.6.

Листинг 11.6

```
exten => _3X,1,Dial(SIP/${EXTEN},20,tr)
exten => _3X,n,GotoIf($["${DIALSTATUS}" = "CHANUNAVAIL"]?700)
exten => _3X,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?800)
exten => _3X,n,GotoIf($["${DIALSTATUS}" = "NOANSWER"]?700)
exten => _3X,n,Hangup

exten => _3X,700,Voicemail(u${EXTEN})
exten => _3X,n,Hangup
exten => _3X,800,Voicemail(b${EXTEN})
exten => _3X,n,Hangup
```

В этом примере при звонке на линии с номерами от 30 до 39 осуществляется переход на конкретный приоритет в зависимости от результата сравнения состояния с соответствующим значением.

Действия, которые можно реализовать при обработке телефонных звонков, описаны в справке Asterisk, многочисленные примеры использования и рекомендации представлены в Сети. Далее в этой книге мы упомянем некоторые основные возможности.

Синтаксис шаблонов номеров телефонных линий

Номера в плане звонков обычно вводят в виде шаблонов. Это позволяет одним правилом задавать действия сразу для некоторой группы номеров. Например, одно правило действует для внутренних звонков, другое — при звонке на междугороднее направление, третье — для доступа к филиалу и т. п.

Чтобы отличить конкретный номер от шаблона, первым символом в шаблоне всегда должен быть знак подчеркивания (_). В табл. 11.2 приведены символы, которые имеют специальное значение при употреблении в шаблоне.

Таблица 11.2. *Специальные символы в шаблоне номера линии*

Символ	Обозначение
X	Любая цифра от 0 до 9
Z	То же от 1 до 9
N	То же от 2 до 9
[...]	Любой символ из числа написанных в скобке; допускается указание диапазона последовательных символов через тире
.	Один символ или любое количество любых символов
!	Произвольное количество любых символов, в том числе и отсутствие символа

Следующие примеры из табл. 11.3 поясняют использование рассмотренных специальных символов.

Таблица 11.3. *Примеры использования шаблонов телефонных линий*

Шаблон	Назначение
_8343XXXXXXX	Междугородние звонки на Екатеринбург (код города 343, в городе используется семизначная нумерация)
_[23]XXXXXX	Звонки на семизначный номер, начинающийся с цифр 2 или 3
_X!	Любой номер, начинающийся с цифры
_[*0-9]!	Любой номер, начинающийся с цифры или символа *
_XXX	Любой трехзначный номер

Настройка плана звонков на разные периоды времени

План звонков может отличаться для разных моментов времени. Например, в рабочее время входящие звонки должны поступать на аппараты сотрудников, в нерабочее время можно включить переадресацию на голосовую почту или на номер мобильного телефона и т. п.

Сменить план звонка можно несколькими способами. Первый способ заключается в применении функции перехода, анализирующей значения времени — `GotoIfTime()`. Синтаксис ее вызова следующий:

```
GotoIfTime(<диапазон_времени>|<дни_недели>|<дни_месяца>|<месяцы>?[context
|]extension|]pri)
```

Параметры времени могут быть заданы либо как диапазон или в явном виде (например, 17:00–21:00 для времени, mon–fri — с понедельника по пятницу — для дней недели, 1 — для обозначения первого месяца любого года и т. д.), либо опущены. В этом случае должен быть написан в соответствующем месте знак "*", а время считается соответствующим любому значению из доступного диапазона. Так, следующая запись будет определять диапазон рабочего времени с 9 утра до 18 вечера каждый рабочий день недели любого месяца:

```
9:00-18:00|mon-fri|*|*
```

Если текущее значение времени совпадает с указанным диапазоном, то при исполнении команды `GotoIfTime` управление будет передано на номер, указанный в ее параметрах. Если нет, то будет выполняться следующая за `GotoIfTime` команда. Например, команда

```
exten => s,2,GotoIfTime(*|*|1-2|May?attendant,s,5)
```

переведет вызов в любое время 1 или 2 мая в контекст `attendant` на номер `s` с приоритетом `5`.

Второй способ настройки различных планов звонков — включение контекстов звонков по временным параметрам. Например, вы можете создать контекст звонков, описывающий правила набора в рабочее время, пусть он называется `working`. И другой контекст, в котором вы определили правила для нерабочего времени — `holiday`. Таких контекстов может быть определено любое необходимое количество. Теперь необходимо добавить в контекст, определяющий правила ваших звонков, созданные контексты с условиями анализа времени (листинг 11.7).

Листинг 11.7

```
[office]
...
include => holiday|*|*|1-10|jan
include => holiday|*|*|23|feb
include => holiday|*|*|8|mar
include => holiday|*|*|1-2|may
```

```
include => holiday|*|*|9|may
include => holiday|18:00-23:59|*|31|dec
include => working|9:00-18:00|*|*|*
…
```

Как видно из данного примера, включений каждого контекста может быть несколько. Необходимо только достаточно внимательно определить диапазоны времени, чтобы не забыть настройку звонков для какого-либо периода. И исключить перекрытие диапазонов (иначе Asterisk будет использовать правила сразу из нескольких контекстов, и реальное направление звонка может оказаться далеко не тем, которое вы планировали).

Обратите особое внимание, что использование контекста определяется диапазоном времени, указанным при его импорте. Если вы определили контекст, но импортировали его без критерия времени, то такой контекст будет обрабатываться при каждом звонке, а не в то время, которое предполагалось.

Создание голосового меню

Голосовое меню позволяет звонящему осуществить самостоятельно некоторый выбор, например, перевести звонок на конкретную службу или прослушать информационное сообщение.

Голосовое меню легко создается средствами Asterisk. Логика построения меню очень проста. Специальное приложение проигрывает определенное информационное сообщение ("*Вы позвонили ..., нажмите 1 для обращения в службу технической поддержки, 2 —* ..."), а телефонная станция ожидает в это время возможных нажатий клавиш на аппарате. Если клавиша нажата, то Asterisk передает управление на линию (extension), номер которой совпадает с номером клавиши. Соответственно, для этой линии также можно определить свое меню (или перевести звонок на конкретного абонента).

Голосовое меню удобно оформлять в виде отдельного контекста, а для перевода операции использовать функции безусловного перехода.

Листинг 11.8 иллюстрирует описание контекста голосового меню `mainmenu`.

Листинг 11.8

```
[mainmenu]
exten => s,1,Answer
exten => s,2,Background(welcome-choose)
exten => 1,1,Dial(SIP/1)
```

```
exten => 2,1,VoicemailMain(23)
exten => 2,2,Hangup
exten => t,1,Goto(#,1)
exten => i,1,Playback(invalid)
```

Первая строка обеспечивает ответ станции ("поднятие трубки"), вторая — проигрывает информационное сообщение из пользовательского файла welcome-choose. Если звонящий нажимает клавишу <1>, то Asterisk осуществляет звонок на SIP-телефон с номером 1. При нажатии <2> идет обращение к голосовой почте ящика номер 23. Строки с `t` и `i` определяют действия в случае тайм-аута и нажатия неверной клавиши на телефоне (клавиши, для которой не предусмотрены операции голосового меню).

> ***Примечание***
>
> При создании голосового меню целесообразно добавлять команды, ограничивающие периоды ожидания ответов звонящего некоторыми значениями.

Настройка голосовой почты

В случае отсутствия вызываемого лица сообщение для него может быть записано в телефонной станции и, при необходимости, выслано в качестве вложения по электронной почте. Для того чтобы включить такую возможность, нужно создать ящики голосовой почты, а в правила обработки вызовов включить команды обращения к голосовой почте.

Параметры ящиков голосовой почты определяются в файле voicemail.conf. Минимально необходимо определить ящик, указав для него пароль, имя и адрес электронной почты (*опционально*):

```
1234 => 2222, My name, my_mail@domain.com
```

В этом примере `1234` — номер ящика голосовой почты, `2222` — пароль голосовой почты, `my_mail@domain.com` — адрес, на который будет отослана запись сообщения.

Если вы используете Asterisk совместно с почтовой системой Zimbra, описанной в этой книге, то в ее настройках необходимо разрешить прием файлов с расширением wav. (По умолчанию прием файлов данного типа в Zimbra запрещен.)

Синтакис дополнительных опций достаточно хорошо описан в комментариях файла конфигурации.

Для записи сообщения в почтовый ящик пользователя достаточно добавить в соответствующую позицию плана звонков строку, аналогичную приведенной:

```
exten => 222,n,VoiceMail(222,b)
```

Эта настройка создаст сообщение в ящике 222, предварительно проиграв оповещение, что вызываемый абонент занят (аргумент `b`). Есть также сообщения о недоступности (аргумент `u`) и возможность отказа от информационного сообщения (`s`).

Если телефонный аппарат имеет индикацию наличия сообщений голосовой почты, то в его настройки в файле sip.conf нужно добавить строку с указанием на номер ящика голосовой почты этого аппарата:

```
[222]
…
mailbox=222
…
```

> ***Примечания***
>
> Из опыта работы известно, что телефонные аппараты Avaya "зависают" при наличии в конфигурации строки с указанием электронного ящика.
>
> Ящики голосовой почты также могут быть размещены по контекстам. В этом случае для указания ящика в приложениях к его номеру следует добавить через символ `@` название контекста: `222@default`.

Для прослушивания сообщений почты предназначено приложение VoiceMailMain. В качестве аргумента этого приложения можно указать любой ящик голосовой почты (в том числе, возможен запрос ввода номера). Но обычно в плане звонков создается специальный номер, по которому можно прослушать сообщения. При этом в качестве номера ящика голосовой почты подставляется номер звонящего:

```
exten => 777,1,VoiceMailMain(${CALLERID(num)})
```

> ***Примечание***
>
> Просмотр существующих ящиков почты и количества сообщений в них выполняется командой `voicemail show users`.

Настройка групп вызова и перехвата звонка

Часто приходится настраивать вызов так, чтобы звонок одновременно был на нескольких аппаратах. Например, при переводе звонка в службу техподдержки телефон должен зазвонить у всех специалистов, входящих в ее состав. В терминологии специалистов АТС такая возможность называется созданием группы вызова.

В Asterisk для того, чтобы позвонить одновременно на несколько линий, достаточно просто указать все эти линии в соответствующей инструкции. Например, правило

```
exten => 999,1,Dial(SIP/1&SIP/2&SIP/3)
```

при наборе номера 999 осуществляет одновременный звонок на телефоны, зарегистрированные в sip.conf с номерами 1, 2 и 3.

В большинстве случаев данная функциональность обеспечивает все потребности офиса. Создайте несколько подобных групповых номеров и используйте их в работе.

> ***Примечание***
>
> В центрах обработки вызовов можно задействовать возможности Asterisk по расширенной настройке групп обработки вызовов, когда пользователи могут самостоятельно подключаться к определенной группе и прекращать регистрацию в ней, когда для группы применимы различные технологии распределения звонков и т. п. Поскольку это достаточно специализированная возможность, мы отошлем читателя к самостоятельному изучению возможностей *агентов* (agents, см. описание некоторых настроек в комментариях в файле agents.conf).

Перехватом вызова называют возможность ответить на вызов, осуществляемый по другому номеру. Например, вы слышите, как звенит телефон на соседнем столе, поднимаете свою трубку, набираете определенный код и отвечаете на этот вызов.

По умолчанию код перехвата вызова — "*8", его можно переопределить в файле features.conf. При наборе этого кода будет перехвачен не каждый звонок, а только тот звонок, который осуществляется на группу вызова, для которой в настройках данного телефона эта операция разрешена. Иначе говоря, в настройках телефонов должны быть определены группы вызовов, к которым принадлежит номер, и группы перехвата вызова, которые определяют номера групп вызова, звонки из которых могут быть перехвачены. При этом в настройках можно указывать несколько номеров групп:

```
callgroup=1
pickupgroup=1,2,3
```

Подобные блоки необходимо вставить в файл конфигурации sip-телефонов (sip.conf) в описания каждого телефона.

Запись звукового сообщения

В Asterisk голосовое сообщение записывают в различных случаях:

- при создании сообщений, которые предполагается использовать для голосового меню, различных служебных сообщений системы и т. п.;

- при протоколировании телефонных переговоров, например, для обеспечения возможностей рассмотрения претензий к операторам центров обработки вызова и т. д.;
- для записи текущего разговора самими пользователями (например, чтобы сохранить для себя некоторые важные моменты).

Для записи голосового сообщения предусмотрено приложение Record. При его вызове нужно указать имя файла для записи с обязательным расширением, которое определяет формат записи. Запись можно осуществить в любом поддерживаемом формате, но удобнее тот, который соответствует применяемому кодеку в разговорах. Все поддерживаемые форматы файлов можно отобразить по следующей команде в консоли Asterisk:

```
core show file formats
```

Если не указать полный путь для хранения записей, то Asterisk будет пытаться сохранить записи разговоров в папке /usr/share/asterisk/sounds. При установке в Ubuntu по умолчанию из загрузочного пакета на эту папку полные права предоставлены только суперпользователю, значит Asterisk, использующий одноименную учетную запись, не сможет записать туда файлы. Поэтому на эту папку следует предоставить полные права учетной записи Asterisk.

В качестве параметров в программе записи можно указать длительность периода тишины, по истечении которого запись должна быть прекращена, максимальную длительность записи и несколько опций (не проигрывать стартовый гудок, добавить запись в файл вместо создания новой, назначить кнопку "*" для завершения записи или продолжать запись, игнорируя команды завершения операции до момента, когда трубка телефона будет положена).

Следующий пример (листинг 11.9) определяет в плане звонков номер 999, при звонке на который после трехсекундной паузы после поднятия трубки раздастся короткий гудок и начнется запись сообщения. Запись прервется либо после трех секунд тишины, либо по нажатию звонящим клавиши "#" на телефоне; максимальная длительность записи установлена в 20 с. После завершения записи через 3 с новое сообщение будет проиграно, после чего сеанс будет завершен.

Листинг 11.9

```
exten => 999,1,Answer
exten => 999,n,Wait(3)
exten => 999,n,Record(myfile.ulaw,3,20)
exten => 999,n,Wait(3)
exten => 999,n,Playback(myfile)
exten => 999,n,Hangup
```

Внимание

Обратите внимание, что в приложении, проигрывающим записанный файл, в скобках стоит только имя файла, без расширения. Если будет указано расширение имени файла, воспроизведение завершится с ошибкой!

При повторном вызове программы с указанием того же файла (если позвонить снова, как в приведенном примере, на линию 999), Asterisk просто перезаписывает его содержимое. Чтобы можно было использовать одно определение номера для записи нескольких фраз, в имя файла следует включить символы `%d`, которые будут заменены на последовательные номера при каждой последующей записи. В этом случае вместо имени файла, которое будет неизвестно на момент программирования, нужно указать переменную, соответствующую имени текущей записи (листинг 11.10).

Листинг 11.10

```
exten => 999,1,Answer
exten => 999,n,Wait(3)
exten => 999,n,Record(myfile-%d.ulaw)
exten => 999,n,Wait(3)
exten => 999,n,Playback(${RECORDED_FILE})
exten => 999,n,Hangup
```

На основе этих приложений легко можно сформировать различные варианты записи и проигрывания фраз.

Для протоколирования разговора в Asterisk есть несколько приложений, предусматривающих возможности приостановки записи, увеличения/уменьшения громкости и т. п. Мы опустим такие настройки, продемонстрировав только на простом примере данную функциональность.

Примечание

Протокол SIP позволяет двум телефонам, установившим связь через телефонную станцию, создать соединение непосредственно друг с другом. В этом случае аудиопоток минует Asterisk и поэтому такой разговор нельзя записать. Для обеспечения протоколирования разговоров необходимо отключить такую возможность, добавив в настройки телефонов (в файл sip.conf) строку `canreinvite=no`. Возможность прямого потока аудиоданных также отключается при использовании некоторых опций набора, которые не допускают такого перенаправления (параметры `t`, `T`, `h`, `H`, `w`, `W` или `L` в приложении *Dial*).

Для записи разговоров удобно приложение MixMonitor, сохраняющее весь разговор в одном файле. В качестве аргументов указываются имя файла и опции (переписывать файл или дописывать разговор, включать запись

только после установки соединения или сразу и т. д.). Если полный путь к файлу не указан, то Asterisk сохраняет запись в папке monitor каталога, определенного в настройках программы (в файле asterisk.conf) как значение параметра `astspooldir` (по умолчанию /var/spool/asterisk).

> ***Замечание***
>
> Приложение Monitor записывает, например, разговор от каждой линии в отдельный файл.

Следующий пример включает протоколирование разговора при звонке на номер 555 в файл file_555.wav в папке по умолчанию:

```
...
exten => 555,n,MixMonitor(file_555.wav,a)
...
```

Каждый последующий разговор будет дозаписываться в этот же файл. Другие команды обслуживания звонка (подъем трубки, пересылки в случае занятости/недоступности и т. п.) опущены для удобства.

> ***Примечание***
>
> Анализировать разговоры, записанные в один файл, достаточно неудобно. Поэтому имя файла обычно формируют динамически: составляют его из номера линии и текущего времени.

Чтобы звонящие сами могли включать запись своего разговора, необходимо соответствующие возможности предусмотреть в конфигурации Asterisk. Во-первых, нужно раскомментировать строку `automon => *1` в файле features.conf.

> ***Замечание***
>
> Эта строка определяет включение/выключение записи разговора с помощью нажатия двух клавиш *1. Естественно, что вы можете переопределить эти настройки на свои значения. Обратите внимание, что в этом же файле определяется максимальное время между нажатиями этих двух клавиш — 0,5 с (параметр `featuredigittimeout`). Возможно, что это значение придется немного откорректировать для удобства пользователей и четкого включения/отключения режима записи, поскольку с параметрами по умолчанию режим записи большинством пользователей не всегда четко включается. Автор рекомендует раскомментировать строку `courtesytone = beep` в файле features.conf. Эта настройка включит для пользователя короткий гудок при переходе в режим записи, что позволит быть уверенным в начале операции.

Во-вторых, чтобы этот параметр настроек начал действовать, необходимо перезагрузить соответствующий модуль. Проще всего это осуществить, перестартовав Asterisk путем исполнения в его консоли следующей команды:

```
restart gracefully
```

Далее необходимо в глобальной переменной указать наличие такой возможности. Сделать это можно в опциях набора для соответствующих линий (`Set(DYNAMIC_FEATURES=automon)`), но удобнее определить в секции global файла extensions.conf (если вы используете несколько опций (кроме `automon`), то их нужно перечислить, разделяя символом `#`):

```
DYNAMIC_FEATURES=>automon
```

Запись разговора можно включить только для тех случаев, когда в команде набора явно указано разрешение на включение записи разговора тому, кто звонит, и тому, кому звонят. Обычно включают разрешение для обоих участников разговора, добавляя параметры `w` и `W`:

```
exten =>_xxx,n,Dial(SIP/${EXTEN},,wW)
```

После этого запись разговора может быть включена нажатием клавиш *1, повторное их нажатие выключит запись.

Сама запись осуществляется по умолчанию в папку /var/spool/asterisk/monitor. Запись ведется в два файла (в отдельные файлы записываются слова каждого участника), а после окончания разговора эти два файла объединяются в один. Для этого Asterisk запускает команду `sox`.

Если вы устанавливали Asterisk в Ubuntu из готового пакета, то эта программа будет отсутствовать. Кроме того, необходимо установить библиотеку различных форматов звуков, поскольку сама программа sox после установки не понимает формат wav, в котором осуществляет запись разговора Asterisk:

```
apt-get install sox libsox-fmt-all
```

Разговоры записываются в файлы, названия которых имеют такой вид:

```
auto-1233980998-200-101.wav
```

Вторая часть названия файла (`1233980998`) соответствует времени записи, третья и четвертая — номерам линий участников разговора. Готовых опций прослушивания такого файла нет. Вы можете либо сами создать сценарий, позволяющий проигрывать эти файлы участникам разговора, или реализовать какую-либо иную возможность.

Телефонная книга

В Asterisk есть внутренняя база данных, в которой можно хранить, например, справочник телефонных номеров контактов компании. В результате на телефоне вместо номера вызывающего можно будет отобразить название компании.

Для работы с базой предусмотрены функции `DB(<family>/<key>)` — для чтения или записи данных в базу, `DB_DELETE(<family>/<key>)` — для удаления

данных, DB_EXISTS(<family>/<key>) — для проверки существования данных. Занести данные в базу можно разными способами, самый простой — ввести в режиме консоли с использованием команды

```
database put <family> <key> <value>
```

Условно можно считать, что <family> — это название таблицы, <key> — параметр, а <value> — его значение. Например, вы можете создать телефонную книгу компании, запоминая номера телефонов следующим образом:

```
database put myphone 73433333333 My_Company
```

> ***Примечание***
>
> Для работы с базой данных в режиме консоли применяются команды database del — для удаления данных, database deltree — для удаления таблицы, database get — для получения данных, database put — для ввода данных, database show — для отображения всех значений, хранимых в базе, и database showkey — для показа параметра. Справку по командам можно получить, выполнив help команда.

В качестве примера покажем возможность замены номера звонящего на запись из телефонной книги. Первая строка кода присваивает переменной myvar значение номера звонящего, который получается из параметров SIP-звонка. Вторая строка проверяет (функция DB_EXISTS) наличие в базе записи для этого номера. Если запись существует, то ее значение (оно присваивается переменной DB_RESULT при выполнении команды DB_EXISTS) присваивается переменной myvar2, если записи нет, то переменной присваивается значение переменной myvar. Последняя строка присваивает идентификатору звонящего имя, которое находится в переменной myvar2.

```
exten => 99,1,Set(myvar=${SIPCHANINFO(from):4:11})
exten => 99,n,Set(myvar2=${IF(${DB_EXISTS(phone/
${myvar})}="1"?${DB_RESULT}:${myvar})})
exten => 99,n,Set(CALLERID(name)=${myvar2})
```

В приведенном примере для лучшего восприятия кода он разделен на несколько строк. В рабочей конфигурации необходимые проверки и присвоения могут быть записаны в одной строке.

Конференции

Конференция — это возможность одновременного разговора сразу нескольких человек. В Asterisk конференция организуется как совещательная комната (настройки в файле meetme.conf), переход в которую осуществляется командой MeetMe. В совещательной комнате можно назначить администратора (управляет конференцией, определяется по административному пин-коду при

подключении к конференции), запись конференции, меню управления конференции с использованием DTMF-кодов (нажатием клавиш телефонного аппарата) и т. п.

Однако для работы конференции необходим специальный модуль, генерирующий сигналы времени. Этот модуль либо присутствует в специализированных платах телефонии для Asterisk, либо возможна установка его эмуляции (ztdummy). Для установки программного эмулятора потребуется компиляция Asterisk из исходных кодов с выбором соответствующих опций.

Некоторые дополнительные возможности Asterisk

Asterisk позволяет выполнять некоторые операции во время разговора по командам, подаваемым нажатием клавиш на телефонном аппарате. Соответствующие функции настраиваются в файле features.conf. Некоторые типовые возможности этих настроек описаны далее в этом разделе.

> ***Примечание***
>
> Описанные возможности включаются в файле features.conf раскомментированием соответствующих строк. Для того чтобы они начали работать, необходимо перезагрузить Asterisk. Кроме того, глобальная переменная должна содержать значение такой опции. Проще всего это выполнить, определив значение переменной `DYNAMIC_FEATURES` в блоке global файла extensions.conf: `DYNAMIC_FEATURES=> automon# blindxfer# atxfer` (необходимо перечислить все включенные опции из файла features.conf).

- **Парковка вызова** — это временная приостановка разговора, например, для того, чтобы ответить по другой линии. По умолчанию для быстрой парковки предлагается сочетание #72.
- **Перевод звонка** — в Asterisk возможны два варианта перевода звонка. При первом, так называемом, *слепом переводе (blindxfer)*, при нажатии функциональных клавиш текущий звонок паркуется, на аппарате набирается новый номер и звонящий переводится на него. При *контролируемом переводе (atxfer)* звонка, разговор также паркуется, но после набора номера тот, кто переводит звонок, может дождаться ответа, объяснить ситуацию и только после того, как он положит трубку, звонок будет соединен на новый номер.

Обе возможности включаются в файле features.conf. Необходимо раскомментировать соответствующие строки. В нем же можно переопределить используемые по умолчанию сочетания клавиш и звуки, которые будут проигрываться при переводе звонка и ожидании соединения.

Функции и приложения в Asterisk

Действия по обработке вызова, которые можно определить в плане звонков, по терминологии Asterisk подразделяются на функции (*functions*) и приложения (*applications*). Функции служат для того, чтобы получить какое-либо значение (например, назначить или получить значение глобальной переменной, получить результат проверки некоторого условия и т. п.). Названия функций принято писать прописными символами.

К функциям нельзя обратиться непосредственно в плане звонка (нужно выполнить присвоение с помощью `Set()`), но можно применить их название в качестве переменной, если взять имя функции в фигурные скобки и поставить перед ними символ `$`.

Список доступных функций можно отобразить в консоли Asterisk вводом команды

```
core show functions
```

А получить описание конкретной функции можно, применив следующую команду (последний аргумент — имя функции, по которой требуется справка):

```
core show function STRPTIME
```

Список доступных приложений и описание конкретного приложения можно получить аналогичными командами в консоли:

```
core show applications
core show application VoiceMail
```

Варианты приложений в Asterisk широко представлены в Сети, основные приложения упомянуты в примерах настоящего издания. Поэтому за более подробной информацией, которая может потребоваться при тонкой настройке Asterisk, мы отошлем читателя к онлайновой справочной информации.



Приложение

Базовые правила работы с Ubuntu

Помощь

Для Ubuntu в сети представлено много советов, которые помогут вам решить любую проблему. Основной источник информации — wiki-сайт продукта — **https://wiki.ubuntu.com/**.

Кроме того, поскольку операционная система Ubuntu создана на основе клона Debian, то вам пригодятся все рекомендации, которые будут найдены по интересующей проблеме для Debian.

Установка Ubuntu

Перед началом установки желательно определиться с будущими ролями сервера, чтобы не пришлось устанавливать лишнее ПО.

Если вы не имели опыта работы с Linux-системами, то целесообразно первоначально установить ПО рабочей станции (имеющее графический интерфейс), приобрести некоторый опыт и после этого уже приступать к установке сервера.

Ведущие вендоры обеспечивают свое оборудование необходимыми драйверами для Linux, кроме того, сами дистрибутивы Linux обычно включают драйверы в существенно большем объеме, чем дистрибутивы Windows. Так что у вас не должно возникнуть проблем с использованием оборудования.

Установка Ubuntu начинается с загрузки с компакт-диска дистрибутива. На первом экране следует выбрать русский язык, после чего практически все диалоги программы установки не потребуют знания английского (рис. П1).

Замечание

Дистрибутив Ubuntu русифицирован не полностью. Поэтому при выборе некоторых специализированных опций, например, при установке шифрования на диск

или при создании защищенной папки документов пользователя, программа будет выводить запрос на английском языке. Имея незначительный опыт администрирования систем, вы легко сможете разобраться с данными запросами и ввести верный ответ.

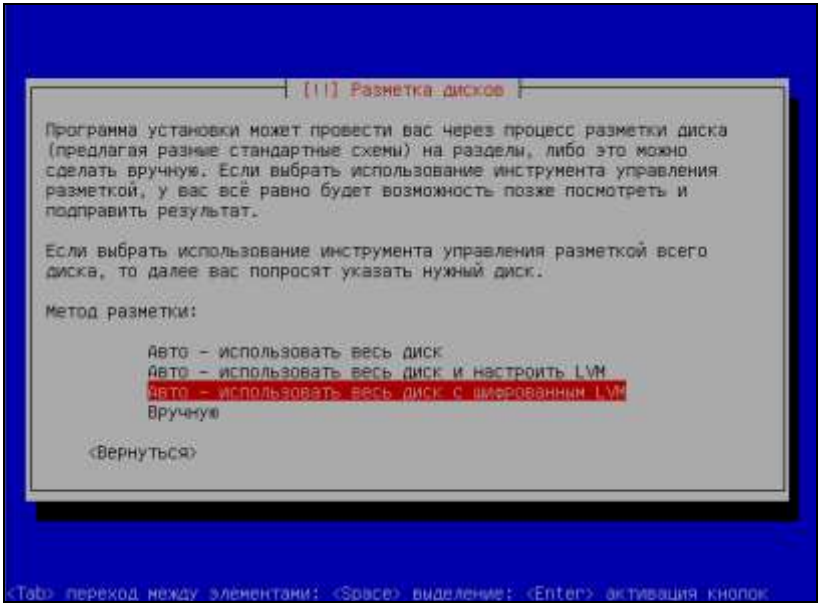


Рис. П1. Один из экранов установки Ubuntu

Не следует пренебрегать возможностью выбора русской клавиатуры перед началом установки (через опцию нажатия клавиши <F3>). Это несколько сократит ответы на вопросы, и вам не придется выбирать тип клавиатуры, отмечая на запросы программы те клавиши, которые имеются на вашем компьютере.

Состав устанавливаемых программ выбирается, исходя из будущих задач сервера. Но в любом случае следует установить пакет SSH для обеспечения удаленного доступа к серверу.

Настройка локализованной консоли

Несмотря на выбор русского языка в опциях программы, после установки консоль неверно отображает русские символы. Для исправления достаточно выполнить переконфигурацию консоли при помощи команды:

```
sudo dpkg-reconfigure console-setup
```

Замечание

Можно установить пакет локализации консоли командой `sudo apt-get install console-cyrillic`, но для меня было достаточно ограничиться описанной процедурой.

На первые запросы программы следует согласиться с предложениями по умолчанию (если вы только не хотите выбрать иные сочетания клавиш переключения) и дойти до запроса о выборе поддерживаемых наборов символов. Этот запрос выводится следующим после запроса варианта раскладки, который хорошо "читается", поскольку отображен латинскими символами (по умолчанию выбран вариант UTF-8). В окне поддерживаемых наборов символов следует перейти на строчку, в которой есть сочетания KOI-8R и KOI8-U (это третья строка сверху, рис. П2).

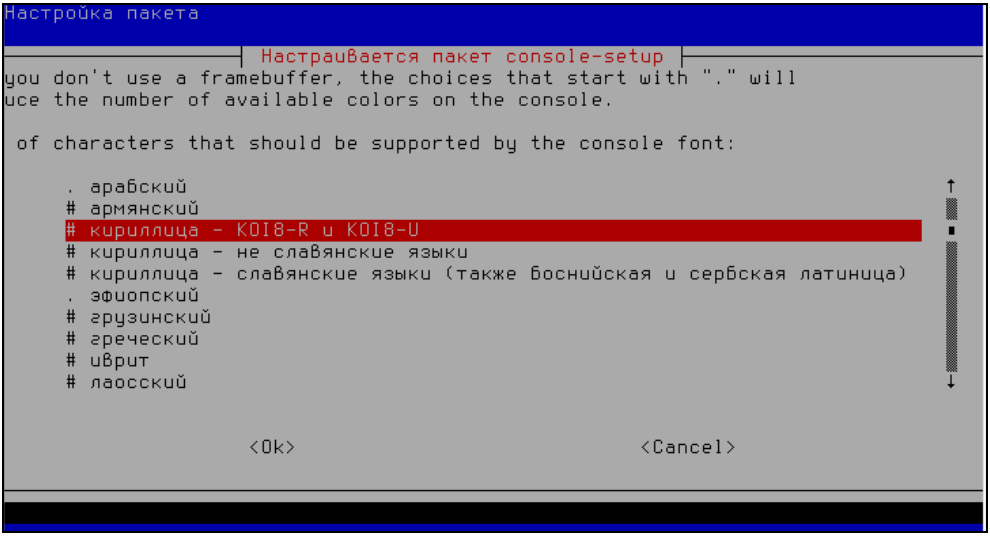


Рис. П2. Настройка русской консоли Ubuntu

Далее выберите любой вариант шрифта (Terminus, VGA и т. д. — через следующий запрос программы, на который нужно просто ответить ОК) и завершите настройку консоли.

Настройка сетевых параметров

Если во время установки программного обеспечения сервера последний был подключен к сети с работающей службой DHCP, то параметры сетевого интерфейса настроены на автоматический режим. Это не лучший вариант для сервера.

Если на время установки сервера физически отключить сетевой провод, то в этом случае установка произойдет в режиме ручного назначения сетевых параметров. Но можно и сменить параметры сети редактированием файлов настройки. Назначение параметров сетевого интерфейса осуществляется в файле конфигурации, который расположен по пути /etc/network/interfaces с последующим указанием параметров DNS-сервера в файле /etc/resolv.conf.

Для редактирования можно воспользоваться программой vi, nano или другими — в зависимости от личных предпочтений. Откройте файл конфигурации сетевого интерфейса, например, так

```
sudo vi /etc/network/interfaces,
```

найдите блок параметров (начинается со строки `# The primary network interface`) и замените строки после `auto eth0` (начинаются с `iface eth0 inet dhcp`) на текст листинга П1 (естественно, указав свои значения настроек).

Листинг П1

```
iface eth0 inet static
       address 192.168.0.2
       netmask 255.255.255.0
       network 192.168.0.0
       broadcast 192.168.0.255
       gateway 192.168.0.1
```

Откройте файл resolv.conf (например, sudo vi /etc/resolv.conf) и внесите изменения в параметры сервера DNS. Содержимое файла должно выглядеть примерно следующим образом:

```
search суффикс
nameserver ip_адрес
nameserver ip_адрес
```

Где *суффикс* — суффикс, который будет добавляться к имени системы при поиске полного DNS-имени (FDQN), а *ip_адрес* — IP-адреса серверов DNS.

Проверьте содержимое файла /etc/hosts. Для нормальной работы почтовой системы и других служб необходимо, чтобы он включал в себя как полное доменное имя системы, так и краткое.

Чтобы внесенные изменения вступили в силу, перестартуйте сеть командой

```
sudo  /etc/init.d/networking  restart
```

В завершение проверьте действующие параметры сетевого интерфейса командой

```
ifconfig -a
```

Примерный текст команды иллюстрирует листинг П2. Обратите внимание, что для настраиваемого интерфейса в его свойствах должны отображаться состояния UP и RUNNING.

Листинг П2

```
ubuntu:~$ ifconfig –a
ethl     Link encap:Ethernet  HWaddr 00:0c:29:14:4d:d5
     inet addr:192.168.0.2  Bcast:192.168.0.255 Mask:255.255.252
     inet6 addr: fe80::20c:29ff:fel4:4dd5/64 Scope:Link
     UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
     RX packets:1438 errors:0 dropped:0 overruns:0 frame:0
     TX packets:461 errors:0 dropped:0 overruns:© carrier:0
     collisions:0 txqueuelen:1000
     RX bytes:168370 (168.3 KB)  TX bytes:84826 (84.8 KB)
     Interrupt:18 Base address:0x2000
lo     Link encap:Local Loopback
     inet addr:127.0.0.1 Nask:255.0.0.0
     inet6 addr: ::1/128 Scope:Host
     UP LOOPBACK RUNNING MTU:16436 Metric:1
     RX packets:54 errors:0 dropped:0 overruns:0 frame:0
     TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:0
     RX bytes:23153 (23.1 KB)  TX bytes:23153 (23.1 KB)
```

Настройка синхронизации времени

При использовании строгих технологий аутентификации (работе на Ubuntu в составе домена Windows) существенное значение имеет точное значение текущего времени систем. В процессе установки Ubuntu производится синхронизация времени компьютера с одним из серверов Интернета. Поскольку спешка или отставание локальных часов компьютера неизбежны, следует настроить систему на автоматическую синхронизацию.

Самый простой способ решения заключается в настройке автоматического ежедневного исполнения команды синхронизации времени. Для этого создайте файл в папке /etc/cron.daily/, например, с именем ntpdate, который должен содержать следующую строку:

```
ntpdate 1.ru.pool.ntp.org
```

Замечания

При настройке выполнения задания по графику обратите внимание на особенности использования `cron`, описанные в *разд. "Выполнение заданий по расписанию".*

Можно указать также серверы 2.ru.pool.ntp.org, 3.ru.pool.ntp.org и т. д.

Не забудьте, что этот файл должен быть исполняемым, поэтому дайте разрешения на его исполнение:

```
sudo chmod +x /etc/cron.daily/ntpdate
```

Файл /etc/cron.daily/ntpdate будет ежедневно исполняться планировщиком системы. При этом будет запускаться команда синхронизации времени `ntpdate`, которой в качестве параметра передается имя сервера времени (1.ru.pool.ntp.org). 1.ru.pool.ntp.org — это имя сервера (можно указать также серверы 2.ru.pool.ntp.org, 3.ru.pool.ntp.org и т. д.) в проекте виртуальных кластеров серверов времени (**http://www.pool.ntp.org/**). Данный проект обеспечивает предоставление IP-адреса реально работающего сервера времени. Этот IP-адрес может случайным образом меняться в зависимости от проверки работоспособности участвующих в проекте серверов времени.

Установка программ

Установка последних обновлений

Перед началом настройки сервера следует установить на него последние доступные обновления. Если ваш дистрибутив загружен только что с первоисточника, то можно быть уверенными в том, что на нем представлена последняя версия сервера. В противном случае первоначально необходимо проверить (и установить при обнаружении обновления) версию сервера.

Ubuntu устанавливает заранее подготовленные пакеты программ, используя данные со специальных серверов — *репозиториев*. Список репозиториев представлен в файле /etc/apt/sources.list. При установке операционной системы в этот файл заносятся параметры серверов, оптимизированные для района эксплуатации. При этом по умолчанию настройки обеспечивают доступ к сертифицированным для данного выпуска пакетам. Вы можете несколько расширить перечень доступных к установке пакетов, если раскомментировать соответствующие строки в этом файле.

Перед установкой любого пакета (или обновлением сервера) необходимо синхронизовать информацию сервера с данными репозиториев. Для этого достаточно выполнить команду

```
sudo apt-get update
```

Вы должны увидеть в консоли информацию об успешной загрузке нужных файлов. После чего необходимо выполнить команду

```
sudo apt-get upgrade
```

которая обновит все установленные на компьютере программы.

Обновление программ происходит без перерыва в обслуживании и без перезагрузки сервера. Поэтому многие Windows-администраторы будут удивлены ходом выполнения операций обновления: объемы загружаемых обновлений исчисляются всего несколькими сотнями килобайт, а сама процедура полностью "безболезненна" для приложений.

Пакеты обновлений безопасности можно устанавливать в автоматическом режиме. В этих целях используется пакет *unattended-upgrades*. Пакет должен быть установлен командой apt-get install и является, по сути, сценарием для этой утилиты. Загрузка и установка обновлений прописываются в ежедневно выполняемый сценарий (/etc/cron.daily/apt). Обратите внимание, что устанавливаться будут только те обновления, которые находятся в сконфигурированных репозиториях.

Обновление версии сервера

Описанная ранее процедура обновляет установленные программы, но делает это в пределах текущей версии сервера. Если в Сети доступны новые версии Ubuntu, то для перехода на них необходимо выполнить команду

```
sudo do-release-upgrade
```

> ***Примечание***
>
> Обновление на новую версию можно выполнить и командой `apt-get dist-upgrade`, но разработчик рекомендует осуществлять эту операцию с использованием `do-release-upgrade`.

На практике обновление версии сервера является достаточно критичной операцией, после выполнения которой могут возникнуть проблемы в работе прикладных приложений. Поэтому такой переход требует предварительного тестирования и не выполняется без подготовки на рабочих серверах.

Установка и удаление программ

Новые программы в Ubuntu можно устанавливать как из исходных файлов, так и из специально подготовленных пакетов. Установка из исходных файлов будет описана в следующем разделе, а сейчас мы рассмотрим процесс установки подготовленных пакетов.

Подготовленный пакет не потребует от пользователя никаких дополнительных операций: достаточно просто получить на локальный диск системы нужный файл и запустить его установку. Дополнительные программы загружаются из Интернета с официальных сайтов, которые прописаны в настройках программы. В некоторых случаях от вас может потребоваться откорректировать этот список или же явно выполнить загрузку файла.

Установка новых пакетов и удаление ненужных выполняется при помощи команд `apt-get` и `aptitude` (далее приведено их описание). Для установки новой программы следует выполнить

```
apt-get install <имя_программы>
```

Для удаления пакета нужно использовать команду

```
apt-get remove <имя_программы>
```

> ***Замечание***
>
> Команда `apt-get` фактически является надстройкой над утилитой управления пакетами dpkg. При помощи dpkg вы можете получить существенно больше информации по конкретному пакету при необходимости. Например, `dpkg -s apache2` выведет на экран полную версию об установленном в системе Web-сервере.

Если устанавливаемый пакет требует предварительной установки других программ, то `apt-get` выведет соответствующее сообщение и загрузит все дополнительные пакеты.

В качестве источника пакетов обычно выбирается Интернет, тем более что объем пакетов установки невелик — обычно несколько сотен килобайт. Но если вы хотите установить программу с компакт-диска, то для этого необходимо включить этот диск в число источников пакетов командой `sudo apt-cdrom add`.

Перечень узлов, с которых система загружает обновления, содержится в файле /etc/apt/sources.list. Обычно менять его не следует, но иногда может потребоваться добавление новых путей. Например, чтобы иметь возможность автоматически устанавливать пакеты, подготовленные фирмой Oracle, следует в этот файл добавить такую строчку:

```
deb http://oss.oracle.com/debian unstable main non-free
```

Описание подобных изменений и дополнительных действий обычно доступно в соответствующих руководствах.

> ***Замечание***
>
> Например, при добавлении в репозитории сайта Oracle рекомендуется скопировать на систему параметры его цифровой подписи, чтобы контролировать идентичность загружаемого файла: *wget http://oss.oracle.com/el4/RPM-GPG-KEY-oracle -O- | sudo apt-key add -* .

После добавления ссылки на новый репозиторий необходимо обновить данные командой

```
apt-get update
```

Многие пакеты содержат в своем названии номер версии. Поскольку это значение обычно заранее не известно и правильно указать имя пакета в команд-

ной строке программы `apt-get` не удается, то для получения точного названия следует воспользоваться поиском. Сделать это можно как в программе aptitude, так и простой операцией поиска по кэшу пакетов:

```
apt-cache search <ключевое_слово>
```

В качестве параметров команды установки можно указать сразу несколько пакетов, все они будут последовательно загружены из сети и установлены в систему:

```
sudo apt-get install build-essential linux-headers-2.6.24-19-server libncurses5-dev
```

В Ubuntu существует и другая команда для установки программного обеспечения, отличающаяся от `apt-get` наличием графического интерфейса в режиме консоли. Это Aptitude (рис. П3). Кроме удобного представления пакетов (в древовидной форме) программа позволяет легко осуществить поиск пакета, увидеть в этом же окне зависимости пакета и названия пакетов, с которым конфликтует данное программное обеспечение и т. д.

Выбор той или иной команды для установки определяется только предпочтениями пользователя.

Программы `apt-get` и `aptitude` устанавливают пакеты с возможностью загрузки их из Сети. Если пакет уже скопирован на диск системы, то для его установки следует использовать команду `dpkg`:

```
dpkg -i <имя_пакета>
```

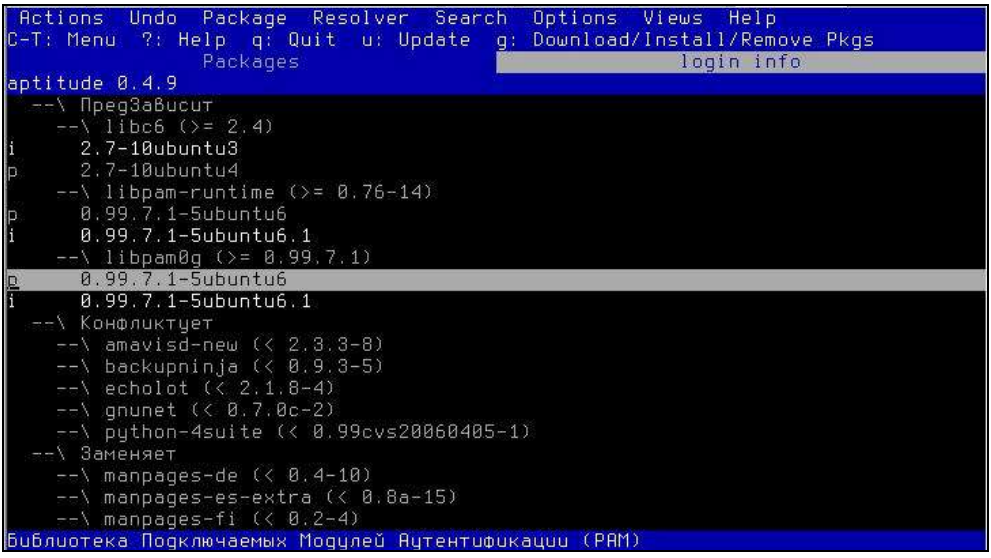


Рис. П3. Утилита Aptitude

Эта команда позволяет также отобразить на экране список установленных пакетов — достаточно выполнить команду

```
dpkg --get-selections
```

В качестве параметров можно указать шаблоны для отображения только определенных пакетов.

> ***Замечание***
>
> Заметьте, что если сохранить вывод этой команды в файл, то потом можно перенести список установленных пакетов на новую систему командой `dpkg --set-selections`, после чего установка пакетов должна быть произведена командой `dselect` (сам пакет `dselect` необходимо сначала установить).

Переконвертация пакетов

Бывает, что нужно установить пакет, подготовленный для другого клона Linux. Например, много пакетов подготовлено в формате rpm (для Red Hut Linux). Самый простой способ в этом случае состоит в переконвертации установочного пакета из одного формата в другой. Для этого подходит программа `alien` (`apt-get install alien`). Установка потребует загрузки ряда дополнительных пакетов (например, у автора объем загрузки был около 18 Мбайт). После установки конвертация осуществляется следующим образом:

```
alien -d <имя_пакета.rpm>
```

После выполнения этой команды на диске появится пакет в формате Debian, который можно будет установить командой `dpkg`. Установку пакета можно провести за один шаг вместе с конвертацией, если указать ключ `-i`. Однако автор предпочитает разбивать подобные операции на несколько шагов для удобства работы с ошибками.

Настройка параметров прокси-сервера для команды обновлений

При установке системы вы отвечаете на вопрос о параметрах прокси-сервера, используемого для загрузки пакетов. Эти параметры можно изменить следующим образом. Во-первых, создать файл /etc/apt/apt.conf со следующим содержимым:

```
ACQUIRE
{
http::Proxy "http://DOMAIN\NAME:PASS@host.proxy:PORT"
}
```

ЗАМЕЧАНИЕ

Допустима запись в одну строку: Acquire: `http::Proxy "http://domain\name:pass@host:port"`.

В этом примере `DOMAIN\NAME` — имя доменной учетной записи, `PASS` — ее пароль, `host.proxy` — имя (или IP-адрес) прокси-сервера, а `PORT` — его порт, используемый для подключения клиентов.

Другой способ заключается в определении параметров прокси-сервера в самой операционной системе. Для этого выполните команды

```
export http_proxy=http://domain\name:pass@host.proxy:port
export ftp_proxy=http://domain\name:pass@host.proxy:port
```

При необходимости эту команду можно включить при каждом входе пользователя (включить в файл ~/.bashrc).

Проблемы с прокси-сервером обычно возникают в случае работы с Microsoft ISA-сервером. По умолчанию на этом прокси-сервере используется NTLM-аутентификация пользователей, настройка которой вызывает определенные сложности. Для решения проблемы вы можете либо разрешить прохождение пакетов через ISA-сервер для Ubuntu без проверки (для всех пользователей, контроль только по MAC-адресу), либо установить и настроить в Ubuntu пакет ntlmaps.

Установка программ из исходных кодов

В "нормальных условиях" следует стремиться к установке программ из специально подготовленных пакетов. Однако в некоторых случаях может возникнуть ситуация, когда программу необходимо будет собрать из исходных кодов. В этом случае на компьютере предварительно следует установить компилятор. Целесообразно инсталлировать не только сам компилятор, а набор утилит *build-essential*:

```
sudo apt-get install build-essential
```

Прикладные программы, которые вы захотите установить, могут потребовать наличия связанных пакетов.

Установку программы из исходных кодов мы проиллюстрируем на примере АТС проекта Asterisk, описанной в *главе 11* настоящей книги.

Загрузить исходный код АТС можно как с сайта разработчика (**ftp://ftp.digium.com/pub/asterisk**), так и с различных зеркал (легко найти обычным поиском). Лучше использовать стабильную версию решения, на момент подготовки книги это была версия 1.4.23. Например, следующая команда загрузит исходные коды программы в домашнюю папку пользователя:

```
wget http://downloads.digium.com/pub/asterisk/releases/asterisk-1.4.23.1.tar.gz
```

Обычно для хранения исходных кодов в Ubuntu применяется папка /usr/src; для записи в нее необходимы права суперпользователя. В дальнейших примерах мы будем считать, что работа происходит с такими правами.

Переместите загруженный файл в папку /usr/src и разархивируйте его следующей командой:

```
tar zxvf asterisk-1.4.22.tar.gz
```

Для компиляции программной АТС в операционной системе должны быть установлены дополнительные пакеты. Чтобы установить их, выполните следующую команду:

```
sudo apt-get install linux-headers-2.6.24-23-server libncurses5-dev
```

> ***Замечание***
>
> Перечень устанавливаемых пакетов приведен для операционной системы Ubuntu 8.04 с обновлениями всех пакетов по состоянию на момент подготовки книги. Если на систему будут установлены последующие обновления, то названия пакетов могут измениться (например, будет указана другая версия ядра Linux). Уточнить доступные к установке пакеты можно с использованием поиска в утилите `aptitude`.

Обычно пакеты, которые требуется предварительно иметь в системе для нормальной установки пакета, перечислены либо в файле README, либо INSTALL. Поэтому знакомству с этими файлами необходимо обязательно уделить некоторое время.

Все команды следует запускать из папки, в которой расположены исходные коды программы. Компиляция прикладной программы и установка обычно состоит из следующих шагов:

- запуск программы конфигурирования;
- компиляция пакета командой `make`;
- установка программы командой `make install`.

Перед установкой можно выполнить команду `make check`, которая запустит процедуру тестирования, а после установки можно удалить временные (промежуточные) файлы командами `make clean` и `make distclean`.

Итак, в соответствии с описанной процедурой, переходим в папку asterisk-1.4.23 и запускаем конфигурирование программы:

```
cd asterisk-1.4.23/
./configure
```

На экран будет выведено достаточно много строк. Самое главное, что в итоге вы не должны увидеть сообщений об ошибках, только сообщение примерно такого содержания:

```
configure: Package configured for:
configure: OS type  : linux-gnu
configure: Host CPU : i686
```

Если программа сообщит об ошибках, то необходимо устранить вызвавшие их причины.

> ***Примечание***
>
> До компиляции пакета можно установить некоторые опции запуском команды `make menuselect`. В результате выполнения этой команды на экране появится набор опций; выбирая пункты меню, можно устанавливать те или иные параметры (рис. П4).

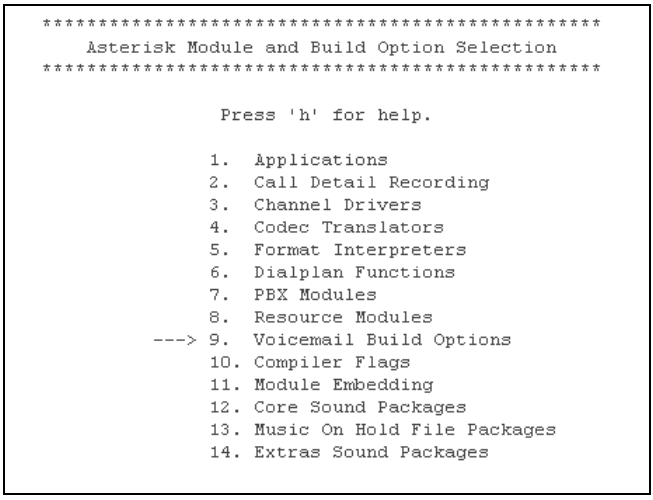


Рис. П4. Результаты вызова команды `make menuselect`

Для компиляции и установки программы последовательно выполните команды

```
make
make install
```

В итоге их работы АТС будет установлена, о чем программы сообщат в конце своей работы.

Если необходимо установить примеры файлов конфигураций, то выполните еще команду

```
make samples
```

В результате вы получили работающую программу, самостоятельно скомпилированную из исходных кодов.

Если приходится повторно устанавливать программу (например, в случае возникновения ошибок и попыток их устранения), то перед конфигурированием программы следует очистить предыдущие настройки командой

```
make clean
```

Иногда при конфигурировании необходимо задать дополнительные параметры. Такие ситуации разрешаются путем изучения документации и поиска в Сети.

Для некоторых пакетов могут потребоваться дополнительные опции установки. Например, при установке пакета NRPE (*см. разд. "Настройка мониторинга серверов Linux"*) требуются дополнительные шаги (`make install-plugin`, `make install-daemon`, `make install-daemon-config`). Необходимость в подобных шагах также уточняется по документации к программе.

Изоляция приложений

Одной из методик повышения безопасности работы сервера является изоляция приложений. Суть идеи очень проста. Приложение запускается в специальном режиме в надежных условиях, когда есть уверенность в отсутствии каких-либо вредоносных кодов. Работа в приложении происходит "под наблюдением" специальной программы, которая фиксирует всю активность. После чего информация о тех ресурсах, которыми пользуется прикладная программа, заносится в специальный профиль. Впоследствии приложение уже не сможет, например, получить доступ к персональным данным пользователя, если оно будет тем или иным способом дискредитировано.

> ***Примечание***
>
> Часто используют также программу `chroot` для того, чтобы приложение на сервере в качестве файловой системы видело только свою папку.

Для Ubuntu существует специальный пакет — `AppArmor`, реализующий данную методику. Он устанавливается на сервере по умолчанию и включается для некоторых программ (например, для защиты DNS-сервера). В то же время, с его помощью вы можете защитить и другие программы.

Для включения защиты `AppArmor` для какой-либо программы необходимо иметь ее *профиль*. Для наиболее популярных пакетов существуют подготовленные профили, которые можно загрузить командой

```
sudo apt-get install apparmor-profiles
```

В общем случае профиль для программы можно сформировать самостоятельно. Принцип создания достаточно прост, хотя для этого может потребоваться достаточно длительный период времени на отладку и тестирование. Прикладная программа запускается в контролируемом режиме, при этом все ее действия протоколируются, например, доступ к каким-либо файлам, вызов других программ и т. п. На основе анализа этих записей специальной утилитой создается профиль программы. Далее обучение продолжается с учетом созданных настроек профиля. По истечении некоторого периода тестирования, когда вы посчитаете, что с использованием программы выполнялись все возможные операции, режим обучения прекращается, создается окончательный профиль и работа программы переводится в режим полной защиты.

> ***Примечание***
>
> Режим обучения называется *complain*, режим защиты — *enforce*, если программа не контролируется и не тестируется в режиме обучения, то ее статус показывается как *not confined*.

Указанные операции выполняются при помощи следующих команд:

- Просмотр списка пакетов, для которых используется режим `AppArmor`:

  ```
  sudo apparmor_status
  ```

- Создание профиля защиты и включение режима обучения для программы (путь к исполняемому файлу программы можно отобразить, набрав команду `which` *`программа`*):

  ```
  sudo aa-genprof /путь_к_исполняемому_файлу_программы
  ```

Утилита предложит вам получить данные из репозитария профилей, после чего создаст начальный профиль программы и переведет ее в режим обучения. Для обучения вам необходимо запустить программу в другой консоли, не закрывая `aa-genprof`, и выполнять типовые операции. Для внесения изменений в созданный профиль, нужно вернуться в окно команды `aa-genprof` и выполнить операцию `Scan`.

Если программа, для которой проводится обучение, вызывает, в свою очередь, другую программу, то при сканировании журналов вам будет предложено либо *Inherit* — использовать профиль основной программы для вызываемой, либо *Profile* — создать новый профиль, либо *Unconfined* — запустить эту программу без защиты AppArmor. Последний вариант не стоит выбирать, поскольку вы решили защищать основную программу. Оптимальный вариант — создание собственного профиля.

Вам придется ответить также на ряд вопросов, разрешая или запрещая определенный доступ для программы. После чего вы можете либо продолжить

режим обучения, либо завершить его (выбрав команду `Finish`). Это переведет программу в режим защиты.

- Если вы хотите перевести программу в режим обучения, то выполните:

```
sudo aa-complain /путь_к_исполняемому_файлу_программы
```

- Чтобы внести изменения в профили программ, нужно использовать следующую команду:

```
sudo aa-logprof
```

- Перевод конкретной программы в режим защиты осуществляется по команде:

```
sudo aa-enforce /путь_к_исполняемому_файлу_программы
```

Если на сервере существует профиль защиты для программы, то отключить защиту можно (для включения защиты после этого необходимо просто удалить эту ссылку. После чего включить для программы защиту, загрузив профиль командой `apparmor_parser -a` с указанием имени профиля), если создать ссылку на этот профиль в папке /etc/apparmor.d/disable (в ней хранятся отключенные профили), например, командой:

```
sudo ln -s /etc/apparmor.d/имя_профиля /etc/apparmor.d/disable/
```

Чтобы отключить защиту без перезагрузки сервера, нужно задать команду:

```
sudo apparmor_parser -R /etc/apparmor.d/имя_профиля
```

Основные правила работы в Ubuntu

Ubuntu является одним из дистрибутивов Linux. Собственно сам Linux — это только *ядро*. Остальное — это приложения и службы, которые вы устанавливаете. Нечетные номера версий — экспериментальные, четные (2.8 и т. д.) представляют собой стабильные сборки.

Графический интерфейс

Сервер Ubuntu устанавливается в режиме консоли, без графического интерфейса. Для сервера графический интерфейс представляет только лишний расход ресурсов системы. В данной книге все рекомендации по настройке параметров системы приводятся для условий работы в консоли (командной строке). И установка графического интерфейса не требуется.

Неким альтернативным вариантом может быть использование файлового менеджера Midnight Commander (рис. П5), позволяющего проводить операции над файлами в псевдографическом режиме. Данный менеджер очень удобен для проведения файловых операций (копирования, переноса, архивирования файлов, редактирования файлов в архиве и т. п.). Интерфейс программы традиционен для файловых менеджеров.

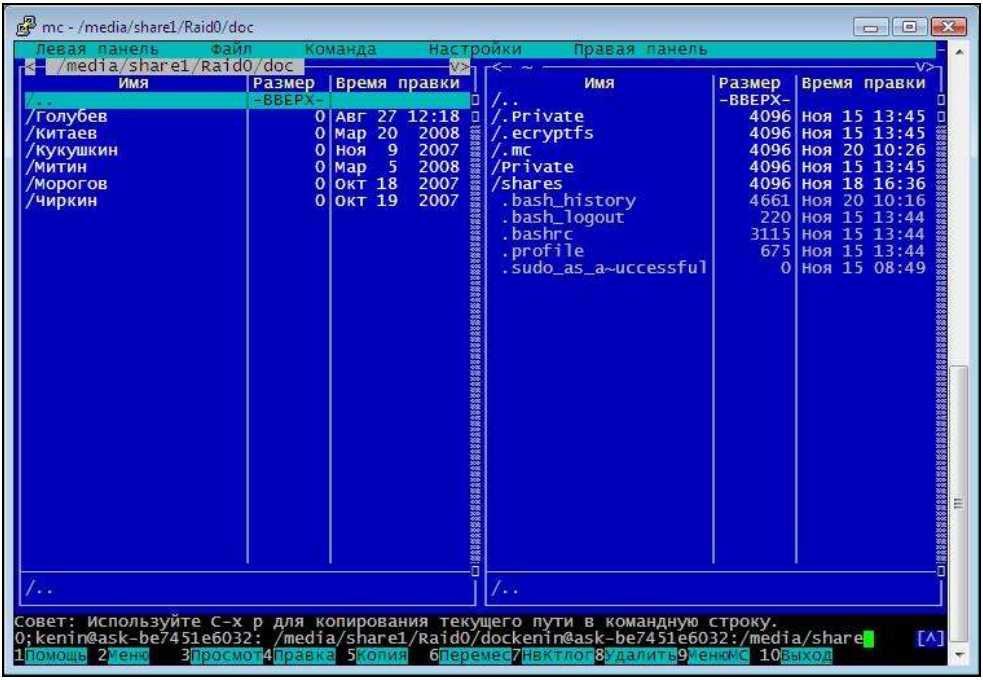


Рис. П5. Окно программы Midnight Commander, запущенной в консоли Putty

Если вы чувствуете себя недостаточно уверенным в управлении сервером в режиме консоли, а в качестве платформы использована достаточно мощная модель, то добавить графический интерфейс можно командой

```
sudo apt-get install ubuntu-desktop
```

или

```
sudo apt-get install kubuntu-desktop,
```

если вы сторонник другого варианта графического интерфейса — KDE.

При этом на систему будет установлено несколько сотен новых пакетов, а объем загрузки из Интернета составит около 450 Мбайт. Такой вариант нельзя рекомендовать для системы, работающей на реальных задачах, поскольку функциональности серверу графический интерфейс не добавляет, а производительность и надежность системы снижаются.

Примечание

Возможно, что более рациональным решением могла бы стать предварительная тренировка на рабочей станции Ubuntu, которая также бесплатна и устанавливается по умолчанию с графическим интерфейсом.

Вход и выход пользователя, завершение работы

Для входа в систему достаточно ввести имя пользователя и пароль. При использовании доменной учетной записи имя пользователя следует вводить как Domain\имя.

Для завершения сеанса работы нужно ввести команду `logout` или `exit`.

Сервер на основе Linux обычно не нуждается в перезагрузке из-за проблем в работе программного обеспечения. В нормальной ситуации достаточно завершить работу в консоли. Чтобы перезагрузить компьютер, нужно выполнить команду `sudo reboot`. Для выключения — набрать

```
sudo shutdown -h now
```

Команда `shutdown` по умолчанию выключает систему и вызывает меню восстановления (*Recovery Menu*). Ключ `-h` (от *halt*) сообщает, что компьютер надо выключить. А параметр `now` определяет момент выключения — сразу же (вы можете определить в этой команде время выключения).

Работа в консоли

Основная работа администратора на сервере Ubuntu ведется в консоли.

Хотя существует много различных графических интерфейсов, облегчающих выполнение той или иной операции, самые большие возможности тонкой настройки доступны только в командной строке (консоли).

По умолчанию в строке приветствия отображаются имя пользователя, имя сервера и текущий каталог:

```
user@ubuntu:/media$
```

В этом примере `user` — имя текущего пользователя, `ubuntu` — имя сервера, `/media` — текущий каталог. Домашняя папка обозначается символом `~`, поэтому при входе в систему приглашение будет выглядеть как `user@ubuntu:~$`.

> ***Замечание***
>
> Вид приглашения легко переопределить путем редактирования файла *.profile в пользовательской домашней папке. За подробностями мы отошлем читателя к справочной документации.

Работа в нескольких консолях

В Linux можно открыть одновременно несколько консолей. Новый сеанс запускается с помощью нажатия комбинаций клавиш <Alt>+<F2>, <Alt>+<F3> и т. д. Так что если вы не можете "справиться" с текущей программой, то можете переключиться в новую консоль, найти процесс, соответствующий задаче, которую нужно удалить, и завершить его.

Замечание

Переходить в другой сеанс можно нажатием клавиш <Alt>+<F*n*>. Графический режим соответствует нажатию <Alt>+<F7>. Если вы работаете в графическом режиме, то переключение нужно осуществлять с добавлением нажатия клавиши <Ctrl>, например, <Ctrl>+<Alt>+<F3>.

Две консоли удобны при поиске ошибок запуска программ. Например, в одной консоли запускают непрерывное отображение журнала событий:

```
tail -f /var/log/messages
```

А в другой — стартуют нужную программу. После чего достаточно вернуться в консоль, в которой выводятся сообщения журнала событий, чтобы увидеть результаты запуска программы. При обнаружении ошибок можно опять переключить консоли, откорректировать, например, конфигурацию программы, запустить ее и вновь в другой консоли проверить сообщения.

Путь к исполняемому файлу

Когда вы набираете команду для выполнения, то система будет искать ее в папках, указанных в переменной пути поиска. Если там команда не будет найдена, то придется указывать полный путь к исполняемому файлу (для упрощения — см. *разд. Alias*). Если нужно запустить исполняемый файл из текущей папки, то следует указать перед его именем символы `./`.

Дополнить путь поиска файлов позволяет команда `export`. В следующем примере эта команда (в первой строке) определяет значение переменной `ORACLE_HOME`, а во второй — добавляет путь, указанный с помощью этой переменной к ранее заданной переменной пути:

```
export ORACLE_HOME=/usr/lib/oracle/xe/app/oracle/product/10.2.0/server
export PATH=$ORACLE_HOME/bin:$PATH
```

Исполняемые файлы

Обратите внимание, что в Linux расширения имени файлов не используются для ассоциации выполняемых операций. Любой файл может быть исполняемым, необходимо только предоставить на него соответствующее разрешение. Кстати, это повышает безопасность системы.

Регистрозависимость

Команды в Linux чувствительны к регистру. Например, ключи `R` и `r` могут обозначать различные операции.

Автозаполнение

Часто нужно при написании команды указывать путь к тому или иному файлу. В этом случае система позволяет автоматически дополнять ввод с клавиа-

туры по нажатию клавиши <Tab>. Например, если требуется скопировать файл, то достаточно набрать команду (`cp`), первые символы имени файла и нажать <Tab>. Если первые символы однозначно определяют имя файла (или команды), то система автоматически допишет полное название. В противном случае никаких изменений на экране не будет. Можно нажать <Tab> второй раз и на экран будет выведен полный перечень имен, начинающихся с введенных символов.

Фоновое выполнение команд

Команды можно запустить в фоновом режиме. При этом вы запускаете выполнение команды и можете продолжать работать в консоли. Для запуска команды в фоновом режиме следует добавить в конец строки символ `&`:

```
ping имя &
```

Вывести список всех команд, работающих в фоновом режиме, можно командой `jobs`. Она выведет на экран перечень заданий с указанием их номеров. Чтобы перевести какое-либо задание из фонового режима в режим консоли, достаточно выполнить команду `fg` с указанием в качестве параметра номера задания (листинг П3).

Листинг П3

```
$ jobs
[1]+  Stopped                 ping 192.168.29.100
$ fg 1
ping 192.168.29.100
64 bytes from 192.168.29.100: icmp_seq=46 ttl=128 time=0.206 ms
...
```

После выполнения `fg` команда `ping` перешла в активный режим.

> ***Примечание***
>
> Если команда уже запущена на выполнение, то перевести ее в фоновый режим можно, сначала приостановив выполнение задания, нажав клавиши <Ctrl>+<Z>, а потом, задав команду, продолжить работу в фоне — `bg`.

Перенаправление потоков

В Linux часто используют результаты выполнения одной команды в качестве входных данных для другой команды. Такой способ называют *перенаправлением потоков*. Такие цепочки можно строить практически любой длины для получения желаемого результата. Например, для прекращения работы какой-либо

задачи можно вывести список всех процессов, найти в нем строку, соответствующую этой команде, извлечь из нее номер процесса и передать его в команду удаления процесса:

```
$ kill $(ps aux | grep ping | grep -v grep | awk '{ print $2 }')
```

В этом примере выполняется команда `kill`, которая удаляет процессы, номера которых заданы в качестве ее параметра. Номер удаляемого процесса вычисляется выражением в скобках (знак доллара перед скобками указывает, что параметром должна быть строка, полученная в результате вычислений в скобках). В скобках мы использовали: `ps aux` — для вывода всех процессов системы, этот вывод попадает на вход команды `grep`, которая фильтрует (оставляет) только те строки, которые содержат символы `ping`. Полученный вывод мы снова фильтруем, удаляя строку, в которой есть слово "grep" (поскольку в числе процессов первоначально будет показано и само задание по поиску). Далее из этой строки с помощью команды `awk` мы извлекаем номер процесса (он выводится второй группой символов). Итог передается в команду `kill` для уничтожения найденного процесса.

> ***Замечание***
>
> Можно было бы обойтись возможностями только программы awk по фильтрации вывода. Но для пользователей, не часто прибегающих к программированию, данный пример хотя и не будет изящным, зато легко воспроизводимым.

Вывод команды можно записать в файл: символ `>` используется в случае создания нового файла, два символа `>>` — когда требуется добавить информацию в файл (если файла нет, то он создается). В команду можно передавать данные из файла, для этого достаточно просто изменить направление уголка (`<`).

> ***Примечание***
>
> В консоль направляются как сообщения вывода команды, так и сообщения об ошибках. При перенаправлении в файл в пакетных заданиях, ошибки (например, сообщения о недостаточности прав доступа) в файл не попадут. Для включения сообщений об ошибках добавьте в конец команды символы `2>$1`. Допускается также сокращенная запись такой команды: `команда &> файл`.

В одной строме можно писать несколько команд, достаточно разделить их точками с запятой. Если между командами поместить символы `&&`, то это будет обозначать выполнение второй команды только при успешном завершении первой. А если между командами поставить символы `||`, то вторая команда будет запущена в случае, если первая команда возвратила ошибку.

Если обрамить команды круглыми скобками, то это будет обозначать запуск команд в скобках в отдельной оболочке. Если поставить фигурные скобки, то будет использована текущая оболочка. При этом между скобками и коман-

дами должны обязательно быть пробелы как после левой скобки, так и перед правой. Взятие в круглые скобки с пробелами часто применяется, если нужно возвратить в результате операции какую-либо величину.

Подсказка по командам

Для команд обычно краткая подсказка доступна при вводе ключа `--help` (обратите внимание на два дефиса). Подробную справку можно прочесть, воспользовавшись командой `man`:

```
man имя_команды
```

Иногда в справке приводятся ссылки на различные секции документации, например, chmod(2). В этом случае команду `man` следует вызывать так:

```
man 2 chmod
```

Выход из режима чтения справочной документации — так же, как из текстового редактора VI, вводом команды `:q`.

Ссылки

В Linux активно используются *ссылки* на файлы и папки. Например, в качестве места размещения какой-нибудь программы может быть ссылка, указывающая на последнюю версию соответствующего пакета. Так, файл /usr/bin/python является ссылкой на исполняемый файл python2.5. Кроме того, создание ссылки на какую-либо программу в текущей папке позволяет избежать ввода полного пути ее расположения.

При установке новой версии достаточно будет поменять ссылку так, чтобы она указывала на новую папку. А все прикладные программы по-прежнему будут обращаться к той же папке /usr/bin/python.

Ссылки создаются командой `ln`. Так, для создания в текущей папке символической ссылки на какой-либо файл, достаточно выполнить:

```
ln -s <путь_к_исходному_файлу> ./
```

Эта команда создаст в текущей папке (`./`) символическую ссылку на исходный файл. Имя ссылки будет совпадать с именем исходного файла. Более подробные сведения можно получить из справки команды.

Alias

В Linux-операционных системах обычно при вводе команд нужно указывать достаточно много параметров. Если каким-либо набором параметров приходится часто пользоваться, то для удобства можно создать для него синоним (alias). Например, чтобы каждый раз не указывать параметры для вывода

подробных данных о правилах iptables с указанием нумерации строк, можно создать следующий alias:

```
alias iptables='iptables -L -v -n –line-numbers'
```

После этого набор `iptables` будет аналогичен по результату `iptables -L -v -n –line-numbers`.

Чтобы удалить alias, наберите

```
unalias iptables
```

Добавление пользователей

Для добавления (и удаления) учетных записей пользователей в Ubuntu возможны "классические" команды Linux — `useradd` (`userdel` соответственно). При этом чтобы новый пользователь смог начать работу, вы должны создать его учетную запись, сформировать домашнюю папку (можно выполнить с помощью ключа `-d` команды `useradd`) и назначить пользователю пароль командой `passwd`.

> ***ЗАМЕЧАНИЕ***
>
> Мы не рассматриваем параметры дополнительных настроек вновь создаваемой учетной записи, например, включение ее в ту или иную группу и т. п. При необходимости уточнить данные параметры легко в справочной системе — `man useradd`.

В Ubuntu новую учетную запись пользователя можно создать в ходе одной операции, если воспользоваться командой `adduser`:

```
sudo adduser имя_пользователя
```

В ходе выполнения этой команды будут созданы все необходимые настройки, например, подготовлен к работе почтовый ящик нового пользователя и т. п.

Соответственно, для корректного удаления пользователей предусмотрена команда `deluser`.

Каждый пользователь состоит в какой-либо группе. Ее можно указать как при создании пользователя, так и изменить с помощью команды `usermod`:

```
useradd -G admins,ftp,www,nagios <login>
```

Для того чтобы узнать, каким группам принадлежит учетная запись, следует выполнить

```
groups <учетная_запись>
```

Если команда набрана без имени учетной записи, то на экране появится информация по вашей учетной записи.

Иногда необходимо добавить пользователя в существующую группу. Для этого можно воспользоваться следующей командой:

```
usermod -a -G group пользователь
```

Эта команда добавит учетную запись *пользователь* в группу *group*.

Иногда необходимо временно отключить учетную запись. Проще всего выполнить это командой, используемой для смены пароля:

```
passwd -l <учетная запись>
```

> ***ЗАМЕЧАНИЕ***
>
> Некоторые администраторы предпочитают просто поставить вместо *x* звездочку в файле паролей (/etc/passwd) или отключить доступ пользователю к командному процессору (`usermod -s /bin/false <учетная_запись>`). Но предпочтительнее стандартный способ блокировки учетной записи.

Для включения учетной записи нужно выполнить такую же команду, только с ключом `-u`. Для запоминания: l — сокращение от *lock*, u — *unlock*.

Права суперпользователя

В Ubuntu по умолчанию не предусмотрено переключение в сеанс пользователя root. Поэтому команды, требующие наличия административных прав, следует выполнять, указывая в начале строки символы `sudo`, например, так:

```
sudo apt-get update
```

При этом в качестве ответа на запрос системы следует вводить пароль текущего пользователя (можно отключить запрос ввода пароля для определенных пользователей и групп, отредактировав файл настроек так, как указано далее).

Применение `sudo` более безопасно, чем переключение в режим суперпользователя. Во-первых, эта команда отключает ряд переменных среды, что исключает риск подмены библиотек. Во-вторых, с помощью `sudo` можно осуществить точные настройки прав пользователей, например, явно указав, какие команды можно выполнить данному пользователю с правами суперпользователя и т. п.

По умолчанию право работы с командой `sudo` предоставлено членам группы adm (пользователь, имя которого было введено в момент установки системы, включен в эту группу). Настроить права на использование команды `sudo` можно, открыв файл настройки следующей командой:

```
sudo visudo
```

> ***ЗАМЕЧАНИЕ***
>
> Прямое редактирование файла sudoers в текстовом редакторе не рекомендуется. Хотя внешне данная операция идентична работе в редакторе nano, но, например, при попытке сохранения изменений в файле конфигурации система проверяет синтаксис и не дает выйти из режима редактирования до устранения

ошибок. Или такой вызов предупреждает одновременное редактирование файла sudoers двумя пользователями и т. п. Все это позволяет избежать ошибок настройки параметров.

Например, чтобы предоставить администраторам домена возможность выполнять операции на сервере Ubuntu с правами суперпользователя, добавьте в конец файла следующую строку:

```
%DOMAIN\\Domain\ Admins ALL=(ALL) ALL
```

Примечание

Обратите внимание, что символ \ предваряет слеш в паре домен-пользователь и пробел в названии группы.

Фактически такая настройка предоставляет права локальных администраторов администраторам домена Windows, если данная система Ubuntu является членом этого домена.

Те, кто хочет сохранить традиционное использование учетной записи root, могут включить данную возможность, присвоив этой учетной записи пароль:

```
sudo passwd root
```

После назначения пароля вы можете переключаться в учетную запись root с помощью команды `su -`.

Если необходимо выполнить несколько операций с полными правами, то можно временно переключиться в режим суперпользователя, применив ключ `-s` в команде `sudo`:

```
sudo -s
```

В результате выполнения этой команды откроется новая консоль с правами пользователя root (это можно сразу увидеть по приглашению командной строки). Кстати, таким способом можно запустить выполнение программ от имени другого пользователя, пароль которого вы не знаете или для которого он отсутствует — так же, как для учетной записи root. Переключиться в нужную учетную запись можно командой `su - <имя>` (при переключении из консоли суперпользователя в консоль другого пользователя ввод пароля в Linux не требуется).

Кто работает на компьютере

Чтобы узнать, кто работает на компьютере, достаточно набрать в командной строке одну букву `w`:

```
$ w
 12:32:12 up 1 day,  1:32,  1 user,  load average: 0,00, 0,00, 0,00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
kenin    pts/0    192.168.0.9      10:35    1.00s  0.08s  0.00s w
```

Вывести на экран имя пользователя текущего сеанса можно командой `who`. Обратите внимание, что команда отображает имя пользователя, вошедшего в систему, а не того, с параметрами которого он сейчас работает. Например, если вы переключились в сеанс с правами суперпользователя, то на экране отобразится не его имя, а исходное:

```
root@geny:~# who
kenin    pts/0        2008-12-26 11:35 (192.168.31.252)
```

Несколько полезных команд

В табл. П1 приведены некоторые полезные команды.

Таблица П1. *Несколько полезных команд для работы в Ubuntu*

Команда	Назначение
`uptime`	Показывает время работы системы
`last`	Выводит историю входов пользователей в систему и моментов перезагрузки
`lastlog`	Показывает время последнего входа в систему существующего пользователя (в том числе по всем служебным учетным записям)
`lsof -l`	Выводит на экран все текущие соединения
`route`	Отображает таблицу маршрутизации; позволяет настроить собственные маршруты
`env`	Отображает на экране все переменные среды
`tar -zcvf <имя создаваемого архива>.tar.gz <файлы>`	Создает из указанных файлов архив
`tar -zxvf <файлы>`	Распаковывает файлы архива в текущую папку (воссоздает структуру папок архива)
`kill <номер>`	Завершает процесс с указанным номером. Чтобы узнать номер процесса, обычно сначала запускают команду `ps aux`
`ps`	Выводит на экран список процессов компьютера: обычно используют для отображения процессов всех пользователей с ключами `aux`: `ps aux`
`top`	Отображает в реальном времени состояние системы и список наиболее активных процессов (в порядке убывания); для выхода можно использовать нажатие клавиши <q> или сочетание <Ctrl>+<C>

Права доступа

Для файлов и папок присутствуют права доступа. Права назначаются для владельца файла (тот, кто его создал), для группы, в которую входит владелец файла, и для всех остальных пользователей. В Linux принято отображать права доступа в виде последовательности символов — `-rwxr-x--x`. Первый символ обозначает тип файла (`-` — обычный файл, `d` — папка, возможны также псевдофайлы), следующие три символа обозначают права владельца файла, следующие три — права группы, к которой принадлежит владелец, и последние три символа обозначают права для всех остальных пользователей. В каждой тройке первый символ свидетельствует о наличии права чтения (`r` или нет права — дефис), второй — право записи (`w`) и третий — исполнения (`x`). Часто права записывают также в виде трех цифр, например, `753`. Если представить каждую цифру в двоичном виде, то получится `111101011`, что соответствует `rwxr-x-wx`.

Для настройки прав доступа к файлам и папкам используются команды `chown`, `chgrp`, `chmod`.

Предоставить (отобрать) права на файл/папку можно командой `chmod`. Обычно в качестве параметров указывают, кому нужно предоставить права (в формате `ugoa` — сначала пользователь, потом его группа, потом группа остальных пользователей, а потом — все пользователи; если этот параметр опущен, то подразумевается назначение прав для всех пользователей), добавить, удалить или назначить — `+/-/=` и какие права (варианты — `rwxXst` или в цифровом виде, например, `777`). Чтобы назначить права на все вложенные папки/файлы, добавьте ключ `-R`.

Например, чтобы отобрать права чтения файла для остальных пользователей, выполните

```
chmod o-r файл
```

А для предоставления права запуска файла всем пользователям можно выполнить команду:

```
chmod +x файл
```

Команда `chown` осуществляет смену владельца файла/папки. Обычно ее применяют, когда администратору нужно настроить права доступа для тех объектов, к которым у него нет доступа. Сначала администратор становится владельцем файла, а после этого уже может назначить желаемые права. Пример использования, когда администратор становится владельцем папки /1 и всех вложенных в нее папок и файлов:

```
chown -R root /1
```

Для смены группы у данного файла или папки служит команда `chgrp`.

На первых порах, пока вы не приобретете уверенность в использовании команд назначения прав, можно прибегнуть к программе Midnight Commander для установки необходимых разрешений доступа.

Принципы размещения данных в Ubuntu

Для пользователей, привыкших к Windows, определенную новизну представляет структура папок. В Linux не принято хранить файлы "абы где". Есть достаточно четкая структура размещения информации, поэтому, например, все пользовательские данные будут находиться только в соответствующей домашней папке.

В Linux принято не подключать жесткие диски под именами логических дисков (диск C, D, E и т. д.). Диски *монтируются*: они добавляются в качестве новой папки в определенное место файловой структуры. Например, по умолчанию CD-ROM подключается как /media/cdrom.

В табл. П2 приведены наиболее "значимые" папки системы.

Таблица П2. *Типовая структура папок в Linux*

Папка	Назначение
/sbin	Папка с программами редактирования и проверки структуры диска, изменения состояния системы
/dev	Содержит записи, соответствующие устройствам, подключенным к системе
/etc	В этой папке находится основная часть файлов локальной конфигурации системы. Большинство конфигураций хранятся в папках, названия которых соответствуют программам (например, конфигурация Squid расположена в папке /etc/squid, настройки сетевых интерфейсов можно найти в папке /etc/networks, параметры VPN-подключений — а это фактически настройки PPP-протокола — в папке /etc/ppp и т. д.)
/etc/init.d	Скрипты запуска системы. В самой папке хранятся сами сценарии, а запуск их производится ссылками из папок соответствующего уровня запуска — /etc/rc?.d (? — цифра от 0 до 6, соответствует уровню запуска)
/home/*username*	Домашняя папка пользователя *username.* Для каждого пользователя системы в папке /home создается своя папка
/usr	Используется для установки программ пользователя (обычно в папки /usr/local, /usr/bin). Документация к установленным программам, как правило, помещается а папку /usr/share/doc. Исходные коды программ копируют в папку /etc/src и т. д.

Таблица П2 *(окончание)*

Папка	Назначение
/lib	Папка с программными библиотеками
/mnt	Обычно используется для подключения устройств (диски, CD-ROM и т. д.)
/opt	Папка, в которой обычно размещаются установленные программы большого объема
/proc	Папка специальных файлов, формируемых ядром системы
/var	Папка для изменяемых данных. Содержит, в том числе, папки журналов системы — они находятся в папке /var/log и далее в соответствии с названием программы. Системные журналы, которые обычно анализируются при поиске причин тех или иных неисправностей, — это /var/log/messages и /var/log/syslog

Текстовый редактор VI

Настройка параметров программного обеспечения сервера Ubuntu осуществляется путем редактирования текстовых файлов. Вы можете работать с любым доступным в системе текстовым редактором, например, `nano`. Но я рекомендую освоить работу в VI, или его улучшенной модификации в Ubuntu — VIM. Этот редактор входит во все дистрибутивы Linux, так что освоение его поможет в любой аварийной ситуации.

Редактор запускается командой `vi`. В качестве параметра можно указать имя файла (в том числе и отсутствующего — он будет создан при сохранении документа). При необходимости редактирования документа с правами суперпользователя пример командной строки вызова программы может быть следующим:

```
sudo vi /etc/samba/smb.conf
```

Особенность редактора VI (VIM) заключается в том, что по умолчанию вы попадаете в *командный* режим работы. В этом режиме можно выполнять операции над текстом путем ввода специальных команд — поиска, замены, удаления и т. п., часть их которых приведена далее.

Чтобы начать набирать текст, нужно установить курсор в желаемую точку ввода текста и перейти в режим *редактирования*, который позволяет вводить новый текст. Для того чтобы перейти из редактирования в режим ввода команд, достаточно нажать клавишу <Esc>.

Примечание

Стандартная ошибка всех новых пользователей программы — попытка в этом режиме перейти к вводу символов в другое место текста. Нажатие клавиш перемещения курсора приведет, как правило, к появлению новых строк с буквой A, B, C или D. В этом случае нужно выйти из режима редактирования, нажав клавишу <Esc>, и удалить лишние строки, используя, например, команду `dd` при нахождении курсора в такой строке.

Чтобы сохранить измененный документ, нужно выполнить команду `:w`, для выхода без сохранения — `:q!`. Для открытия другого документа достаточно выполнить команду `:e`.

В редакторе доступно много команд, которые позволяют опытным администраторам выполнять операции редактирования текста практически в автоматическом режиме. Их описание доступно в справке, очень много рекомендаций представлено в Интернете. Мы приведем лишь самые основные команды (табл. П3), которые позволят вам выполнить простейшие операции с текстом. Не забудьте, что выполняются они в командном режиме, в который можно перейти по нажатию клавиши <Esc>.

Таблица П3. *Наиболее часто используемые команды текстового редактора VI*

Команда	**Действие**
A	Добавить. Переход в режим ввода текста *справа* от курсора
I	Вставить. Переход в режим ввода текста *слева* от курсора
Клавиши перемещения курсора	Перемещают курсор в документе в командном режиме. Для перемещения курсора служат также четыре расположенные в ряд клавиши <h> (влево), <l> (вправо), <j> (вниз) и <k> (вверх). Можно использовать их вместе с цифрами: например, ввод команды 9k переместит курсор на 9 строк вверх
<Ctrl>+<F>/ <Ctrl>+<B>	Перемещение на страницу вперед/назад
G	Переход на последнюю строку документа
*n*G	Переход на строку с номером *n*. Команда 1G переместит курсор в начало документа. Перейти на строку с номером *n* можно также командой *:n*
X	Удаление символа над курсором
X	Удаление слова, в котором стоит курсор
yy	Копирование текущей строки в буфер
p|P	Вставка из буфера (P — вставляет в предыдущую строку, p — в последующую)
:1,2t3	Скопировать строки 1 и 2 и вставить их после строки 3

Таблица П3 *(окончание)*

Команда	Действие
:1,3m5	Удалить строки с 1 по 3 в буфер и вставить их после строки 5
dw	Удаление от текущего символа до конца слова; ввод команды `4dw` приведет к удалению *четырех* слов
d$	Удаление от текущего символа до конца строки
/*слово*	Поиск символов *слово* вперед
?*слово*	Поиск символов *слово* назад
:g/*поиск*/s/*замена*/g	Замена всех слов *поиск* в редактируемом файле на *замена*
u	Отмена последней операции (можно отменить несколько шагов)
<Ctrl>+<R>	Восстановление последней отмененной операции
:w	Сохранение файла. Если после *w* указать имя файла, то программа сохранит результат в файл с новым именем
:8,15w *имя*	Сохранить строки с 8 по 15 в новый файл *имя*
:wq	Сохранить файл и выйти из режима редактирования
ZZ	То же, что и :wq — сохранить и выйти
:q	Выйти из редактора (операция выполнится, только если не было несохраненных изменений)
:q!	Выйти без сохранения
:! *command*	Выполнение внешней команды (*command*)
<Ctrl>+<G>	"Помогает" вспомнить, какой файл вы редактируете и в каком его месте находитесь

Команды для работы с файлами и дисками

Просмотр существующих дисков

Увидеть диски, установленные в системы, можно командой

```
sudo fdisk -l
```

Листинг П4 иллюстрирует пример вывода информации этой командой.

Листинг П4

```
Disk /dev/sda: 250.0 GB, 250059350016 bytes
255 heads, 63 sectors/track, 30401 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
```

```
Disk identifier: 0xe8a3e8a3

Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        1       30024   241167748+  83  Linux
/dev/sda2        30025       30401     3028252+   5  Extended
/dev/sda5        30025       30401     3028221   82  Linux swap / Solaris

Disk /dev/sdb: 500.1 GB, 500107862016 bytes
255 heads, 63 sectors/track, 60801 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x000bb27f

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1               1       60801   488384001   83  Linux
```

В системе установлено два диска (показаны как /dev/sda и /dev/sdb). На первом диске созданы три партиции, на втором — одна. Видна информация по размерам соответствующих элементов.

Увидеть, куда подключены устройства, можно командой `mount` без параметров. Среди всего вывода команды нужно найти требуемые устройства (листинг П5).

Листинг П5

```
/dev/sda1 on / type ext3 (rw,relatime,errors=remount-ro)
proc on /proc type proc (rw,noexec,nosuid,nodev)
/sys on /sys type sysfs (rw,noexec,nosuid,nodev)
varrun on /var/run type tmpfs (rw,noexec,nosuid,nodev,mode=0755)
varlock on /var/lock type tmpfs (rw,noexec,nosuid,nodev,mode=1777)
udev on /dev type tmpfs (rw,mode=0755)
devshm on /dev/shm type tmpfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
securityfs on /sys/kernel/security type securityfs (rw)
/dev/mapper/secdisk on /home/test/secdisk type ext3 (rw)
```

Подключенные диски отображаются в строках, начинающихся с символов `/dev`. По информации листинга можно увидеть, что первый диск подключен в качестве корня файловой системы (`/`), а на втором создана шифрованная файловая система, подключенная в точку /home/test/secdisk.

Оценить свободное место на дисках можно командой `df` (листинг П6).

Листинг П6

```
~$ df
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/sda1            239267908    801852 226407672  1% /
varrun                  517396        44    517352  1% /var/run
varlock                 517396         0    517396  0% /var/lock
udev                    517396        44    517352  1% /dev
devshm                  517396         0    517396  0% /dev/shm
/dev/mapper/secdisk  484534988 175690356 284425460  39% /home/test/secdisk
```

Размеры папок и файлов

А увидеть размеры файлов и папок можно с помощью команды `du`, в параметрах которой указать имя файла (папки) (листинг П7).

Листинг П7

```
~$ du -h ~
du: cannot read directory `/home/kenin/.mc/cedit': Permission denied
4,0K    /home/kenin/.mc/cedit
24K     /home/kenin/.mc
8,0K    /home/kenin/.ssh
12M     /home/kenin
```

Примечания

Параметр `-h` указан для отображения вывода в "дружелюбном" для человека варианте (с обозначениями K — килобайты, M — мегабайты и т. п.). Символ `~` обозначает в Linux домашнюю папку пользователя.

При отображении многостраничной информации, например, в случае запуска команды по папке с большим числом файлов, следует воспользоваться командами перенаправления потоков: `du / -h | less`.

Команда `ls` допускает сортировку вывода. Чтобы увидеть список файлов в какой-либо папке, команду `ls` обычно дополняют ключами `-a` и `-l` для отображения скрытых файлов и вывода полной информации по файлам (показа прав доступа и т. п.). Пример иллюстрирует листинг П8.

Листинг П8

```
~$ ls -al ~
total 11540
drwxr-xr-x 4 kenin kenin    4096 2008-12-26 11:41 .
drwxr-xr-x 3 root  root     4096 2008-12-17 19:58 ..
-rw------- 1 kenin kenin    4747 2008-12-25 11:16 .bash_history
-rw-r--r-- 1 kenin kenin     220 2008-12-17 19:58 .bash_logout
-rw-r--r-- 1 kenin kenin    2940 2008-12-17 19:58 .bashrc
drwxr-xr-x 3 kenin kenin    4096 2008-12-26 11:41 .mc
-rw-r--r-- 1 kenin kenin     586 2008-12-17 19:58 .profile
-rw------- 1 root  root     1024 2008-12-24 17:45 .rnd
-rw------- 2 root  root   154953 2008-12-24 17:45 squid.conf
drwx------ 2 kenin kenin    4096 2008-12-19 17:49 .ssh
-rw-r--r-- 1 kenin kenin       0 2008-12-18 15:41 .sudo_as_admin_successful
```

Обратите внимание, что команда отобразила права доступа к соответствующим элементам (указаны в самой правой позиции), типы объектов (1 — родительский каталог, 2 — ссылка, 3 —папка), авторов элементов, их размеры и дату.

Подключение ISO-образа в Ubuntu

В последнее время многие дистрибутивы распространяются в виде образов CD- или DVD-дисков — как ISO-файлы. В Ubuntu очень легко штатными средствами подключить такой файл в качестве устройства.

Создайте точку подключения (пустую папку, пусть для примера это будет /mnt — пустая папка, присутствующая в системе). Выполните следующую команду для подключения файла образа диска:

```
mount -t iso9660 -o loop файл.iso /mnt
```

Для отключения образа достаточно выполнить

```
umount /mnt
```

Подключив образ диска, вы сможете работать с файлами, включенными в него, обычным способом (копировать в другую папку, просматривать и т. п.).

Подключение CD-ROM

В Ubuntu настройки сервера по умолчанию не предполагают автоматического монтирования CD-ROM после его замены. Для того чтобы система "увидела" новый CD-диск, выполните команду

```
mount /media/cdrom0
```

> ***ЗАМЕЧАНИЕ***
>
> По умолчанию первому CD-ROM присваивается имя `cdrom0`.

Подключение flash-карт

Ubuntu автоматически обнаруживает подключение нового flash-устройства, но не подключает его файловую систему. Чтобы начать работу с данными на переносном устройстве, сначала следует узнать, с каким именем оно подключено к системе. Для этого выполните команду

```
fdisk -l
```

А затем примонтируйте саму флешку командой

```
mount <имя устройства> <точка монтирования>
```

А перед завершением работы выполните команду `umount <имя>`.

Команды работы с файлами и папками

Проверить диск на наличие физических ошибок можно командой `fsck`, но применять ее следует только к отключенным (*не монтированным*) дискам.

Самые распространенные команды для работы с файлами приведены в табл. П4.

Таблица П4. *Наиболее часто используемые команды работы с файлами и дисками*

Команда	Назначение	Описание
`cp`	Копирование файлов	В параметрах нужно указать, что копировать и куда (новый путь)
`mv`	Переименование файлов	В качестве параметров нужно указать, что переименовывать (исходный файл) и новое имя
`rm`	Удаление файлов	Программа удаляет как файлы, так и папки. Но для удаления папки обязательно нужно указывать ключ `-r`. Этот же ключ используется для рекурсивной операции (удалить все вложенные папки и файлы)

Таблица П4 *(окончание)*

Команда	Назначение	Описание
`ln`	Создание ссылок	Для создания ссылки нужно в качестве параметров команды указать объект, для которого создается ссылка, и потом ее имя. Имя можно не указывать, в этом случае ссылка создается в текущей папке с тем же именем, что и исходный объект
`cd`	Переход в другой каталог	В качестве параметра указывается путь к папке. Допустимы символы `\` для перехода в корневой каталог и `..` — для перехода в родительскую папку (на один уровень вверх)
`pwd`	Выводит путь текущей папки	Чтобы легче запомнить команду: `print working directory`
`mkdir`	Создание папки	–
`rmdir`	Удаление папки	Команду можно применить с ключом, включающим рекурсивное удаление вложенных папок. Будьте очень внимательны при использовании данной функции, поскольку очень легко ошибиться и безвозвратно потерять очень много данных
`cat`	Просмотр файла	Служит для быстрого просмотра файла
`less`	Просмотр файла по частям	Используется для просмотра файла частями — столько, сколько размещается на экране. Эффект тот же, что и у команды `more`, однако `less` позволяет перемещать отображаемый участок вперед и назад. Работает быстрее, чем просмотр, например, в vi. Выход из режима просмотра — вводом символа `q`
`head`	Просмотр начала файла	Выводит на экран начало файла. По умолчанию это 10 строк, но их число можно задать с помощью параметра `-n`
`tail`	Просмотр файла с конца	Выводит последние 10 строк файла. Обычно используется для просмотра файлов журналов. Число отображаемых строк меняется параметром `-n` Обратите внимание на ключ `-f`. Он позволяет не закрывать команду и отображать все изменения в файле, которые будут в него вноситься в момент просмотра. Такой режим часто используется при просмотре файлов журналов системы (запуск такой команды удобен в отдельной консоли)
`tmask`	Настройка прав доступа к файлам по умолчанию	Позволяет задать права доступа для вновь создаваемых файлов. При вызове без параметров выводит текущее значение. Результат не сохраняется после завершения сессии. Реальные права получаются вычитанием из 777 параметра, указываемого в данной команде. Так, значение `tmask 022` соответствует правам 755 для вновь создаваемых файлов

Поиск файлов

Найти файл на компьютере можно с помощью команды `find`. В ее параметрах обязательно нужно указать, в какой папке искать и каковы параметры поиска. Например, так мы можем найти все папки и файлы в компьютере (поиск в корневом каталоге — /), которые называются squid:

```
find / -name squid
```

В качестве параметров можно указывать различные критерии, например, можно найти файлы, которые разрешены для изменения конкретному пользователю, или найти объекты, измененные в заданное время, и выполнить над ними некоторые команды и т. п. Соответствующие подробности необходимо уточнить по справочной документации команды.

Вместо команды `find` можно использовать команду `locate`, осуществляющую поиск файлов и папок по указанной подстроке:

```
locate squid
```

Программа выведет на экран существенно больше итогов, поскольку отобразит все пути, в составе которых есть подстрока "squid". Однако поиск с помощью locate может быть неполным. Программа задействует индексную базу, которая меняется только раз в сутки командой `cron`. Поэтому, если необходимо использовать `locate` для поиска в измененной структуре файлов, лучше предварительно обновить базу командой `updatedb`.

Найти исполняемые файлы можно командой `which`:

```
$ which squid
/usr/sbin/squid
```

Обратите внимание, что `which` показывает путь к исполняемому файлу, который был бы выполнен при вводе команды. Команда не найдет существующие файлы, если папки, в которых они хранятся, не включены в пути поиска исполняемых файлов (в переменную `PATH`). Поскольку путь поиска исполняемых файлов зависит от конкретной среды, например, от того, под чьей учетной записью была выполнена команда `which`, то результаты вывода этой команды будут разными для разных учетных записей.

Найти расположение командных файлов, исходных кодов (ключ `-s`) и документации (ключ `-m`) к программе позволяет команда `whereis`. Она работает быстрее `find`, но объем выводимой информации ограничен.

```
~$ whereis squid
squid: /usr/sbin/squid /etc/squid /usr/lib/squid /usr/share/squid
/usr/share/man/man8/squid.8.gz
```

Создание шифрованного диска

При установке последних версий Ubuntu вам предлагают создать зашифрованные разделы. Эту операцию (создание шифрованного диска) можно осуществить и после установки системы следующим способом.

Допустим, в вашем компьютере есть диск, который необходимо зашифровать. Предположим, что в системе он виден под именем /dev/sdb.

> ***Примечание***
>
> Для большей безопасности рекомендуется первоначально заполнить диск случайными данными. Эта операция длится очень долго (порядка 5 мин на каждый гигабайт объема диска) и в большинстве случаев реальной необходимости в ней нет. Но, если есть потребность, запустите (до начала работ с диском) следующую команду: `dd if=/dev/urandom of=/dev/sdb`.

Установите пакет `cryptsetup`:

```
apt-get install cryptsetup
```

Создайте на новом диске раздел. Сделать это можно командой `fdisk`:

```
fdisk /dev/sdb
```

Следуйте вопросам программы, создайте раздел желаемого объема и не забудьте завершить работу в утилите командой `w`, которая запишет все установки на диск (до момента записи никакие указания, вводимые вами, не будут записаны на диск). Предположим, что вы хотите зашифровать раздел, который назван в результате выполнения предыдущей операции /dev/sdb1. Выполните команду

```
cryptsetup --verbose --verify-passphrase luksFormat /dev/sdb1
```

В процессе выполнения от вас потребуют подтвердить операцию набором YES (именно заглавными символами) и указать (дважды, второй раз — подтверждение) пароль для доступа к зашифрованному диску. После выполнения этой команды откройте новое устройство (потребуется указать пароль):

```
cryptsetup luksOpen /dev/sdb1 <имя>
```

В этой команде в качестве `<имя>` необходимо дать имя новому устройству. Можете назвать его также sdb1, можете ввести, как в случае дальнейших примеров, mydisk и т. п. Проверить открытие диска можно командой

```
ls -l /dev/mapper/
```

которая должна показать строку с именем control и с названием вашего диска:

```
# ls -l /dev/mapper/
total 0
crw-rw---- 1 root root  10, 63 2008-12-25 13:36 control
brw-rw---- 1 root disk 254,  0 2008-12-25 13:42 mydisk
```

Теперь нужно отформатировать новый диск, например, так:

```
/sbin/mkfs.ext3 -j -m 1 -O dir_index,filetype,sparse_super /dev/mapper/mydisk
```

В итоге все готово к тому, чтобы подключить диск как обычное устройство:

```
mount /dev/mapper/mydisk /mydisk
```

> ***Замечание***
>
> Естественно, что *до* начала операции вы должны создать пустую папку /mydisk.

В дальнейшем, чтобы подключить шифрованный диск, необходимо выполнить две команды:

```
cryptsetup luksOpen /dev/sdb1 mydisk
mount /dev/mapper/mydisk /mydisk
```

А чтобы отключить:

```
umount /mydisk
cryptsetup luksClose mydisk
```

> ***Примечание***
>
> Для зашифрованного указанным способом раздела можно добавить новый пароль для открытия командой `cryptsetup luksAddKey /dev/sdb1` или удалить — `cryptsetup luksDelKey /dev/sdb1 0`. В последней команде `0` обозначает первый установленный пароль, если указать `1` — будет удален пароль, заведенный вторым, и т. д. Будьте внимательны и не удалите все пароли, иначе все данные на диске будут потеряны!

Работа в Ubuntu с компьютеров под управлением Windows

Для работы с компьютерами с операционной системой Linux из-под Windows созданы многочисленные как коммерческие утилиты, так и бесплатные программы. Самой большой популярностью пользуется бесплатный SSH-клиент Putty, доступный к загрузке с многих серверов Сети (страница создателя программы **http://www.chiark.greenend.org.uk/~sgtatham/putty/**; последняя версия имеет номер beta 0.60, это стабильно работающая версия, и не стоит обращать внимание на слово beta).

Эта утилита не требует установки. После запуска достаточно ввести имя удаленной системы, выбрать команду подключения, чтобы достаточно быстро появилось окно с приглашением ввода параметров учетной записи. При работе с несколькими серверами, параметры подключения и настройки клиента можно сохранить в конфигурационном файле.

Замечание

Putty также позволяет использовать ключи аутентификации для доступа к удаленным системам. Чтобы сгенерировать ключи, необходимо загрузить соответствующие утилиты с сайта разработчика (или найти версию программы, включающую эти утилиты комплектом).

Для подключения к системам Ubuntu в настройки сессии необходимо внести только одно изменение — указать использование кодировки UTF-8. Это можно сделать уже на подключенной сессии (щелкнуть мышью по пиктограмме программы в окне сессии и выбрать команду **Change Settings...**; изменения наступят после обновления окна — при отображении результатов следующей команды), так и сохранить в параметрах сессии по умолчанию, если вы подключаетесь ко многим системам (в блоке **Category** выбрать пункт **Window | Translation** и указать в правой части окна кодировку UTF-8 для параметра **Received data assumed to be in which character set:**).

Putty хорошо работает с Midnight Commander (см. рис. П5), понимает его функциональные клавиши (<F5>, <F8> и т. п.). С помощью Putty легко организовывать SSH-туннели к другим компьютерам в удаленной сети. Предположим, что в удаленной сети есть компьютеры с операционной системой Windows, и вы хотите подключиться к рабочему столу одного из таких компьютеров. Для этого достаточно создать туннель, соединяющий какой-либо порт локального компьютера и порт 3389 соответствующей станции в удаленной сети. Введите эти параметры в опции сессии (это можно сделать уже для подключенной сессии, не забудьте только после ввода параметров нажать на Apply, рис. П6). На локальном компьютере откройте программу подключения к удаленному рабочему столу и введите в строке адреса 127.0.0.1:81 (81 — номер локального порта, который вы указали в настройках туннеля). Вы увидите, как быстро компьютер подключится к удаленному рабочему столу, время подключения будет существенно ниже, чем в случае подключения с использованием клиента VPN.

Вторая операция, которая часто необходима при работе с Windows компьютеров, — это копирование файлов. Для этих целей существуют бесплатные утилиты, например, WinSCP (**http://winscp.net**). Интерфейс программы создан по типу Norton Commander, на одной панели которого отображаются локальные данные, а на вторую выводятся папки подключенной системы (рис. П7). Поэтому никаких проблем с ее использованием ни у кого возникнуть не должно.

Замечание

Опции копирования файлов обычно уже включены в коммерческие версии SSH-клиентов, например, SecureCRT.

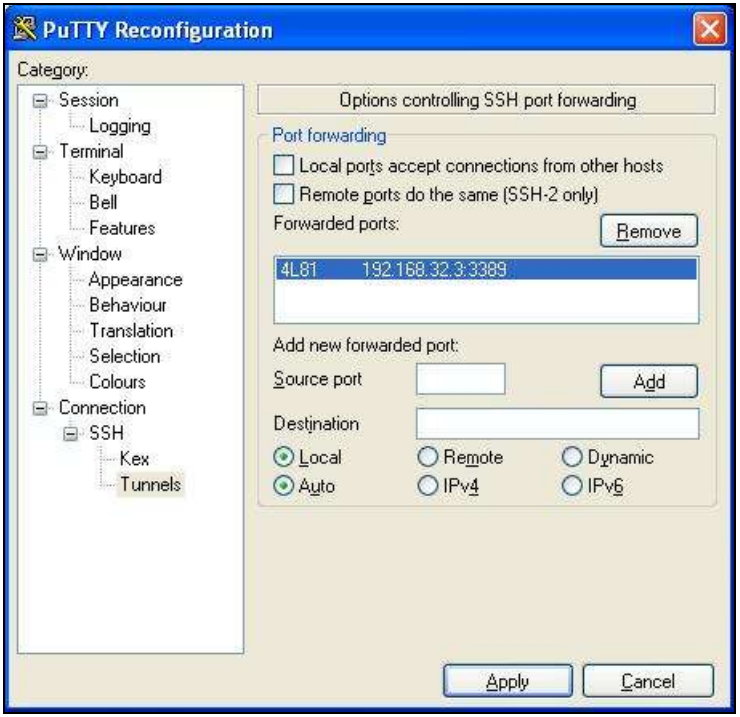


Рис. П6. Создание туннеля средствами Putty

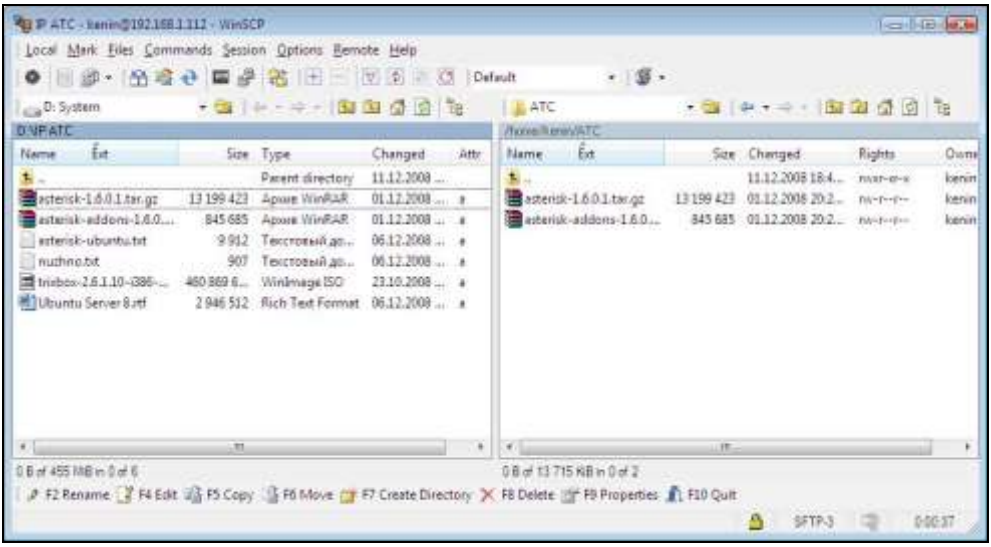


Рис. П7. Программа WinSCP

Акцентируем внимание читателя только на двух моментах. Поскольку к Ubuntu по умолчанию невозможно подключиться с правами суперпользователя, то при файловых операциях вы будете ограничены правами той учетной записи, которая использована для подключения. Если необходимо скопировать файлы, для которых требуются права суперпользователя, то лучше всего подключиться к системе при помощи Putty, далее командой `sudo` предоставить необходимые права (например, сначала скопировать файл в папку пользователя, а потом назначить на него полные права) и уже после этого выполнить файловую операцию в WinSCP.

Второй момент, на который обычно не обращают внимания, — это наличие опции, включающей доступ к дополнительным параметрам (Advanced Options). Дополнительные настройки позволяют использовать WinSCP при доступе в Интернет через прокси-сервер, а также подключаться по SSH-туннелям.

Подключение Windows-сетевых дисков

Вручную подключить сетевые диски можно командой `mount`:

```
sudo mount -t cifs //сервер/ресурс /точка_монтирования iocharset=utf8,
codepage=cp866,user=имя
```

`//сервер/ресурс` — это имя подключаемого сетевого ресурса на Windows-системе, /точка_монтирования — это папка на локальной системе Ubuntu, в которую будет подключен (на сленге линуксоидов *"подмонтирован"*) сетевой ресурс. Эту папку нужно создать *до* выполнения команды, она должна быть пустой при вызове команды монтирования ресурса. `Имя` — это учетная запись пользователя Windows, от имени которого будет осуществляться подключение ресурса. Кроме указанных ключей, которые обеспечивают правильное отображение русских букв и подключение от имени заданного пользователя, можно использовать также параметры, описывающие права на подключаемый ресурс. Их можно при необходимости легко найти в справочной документации.

> ***Замечания***
>
> Указание в качестве параметров команды кодовых таблиц необходимо, чтобы в Ubuntu правильно отображались русские символы в названиях папок и файлов Windows.
>
> Если имя ресурса содержит пробелы, то оно должно быть заключено в кавычки. При использовании в `fstab` пробелы следует заменить на символы `\040`, например так: `//сервер/имя\040ресурса`.

После введения команды вам будет предложено сначала указать пароль пользователя Ubuntu (для переключения в режим суперпользователя), а потом ввести пароль пользователя Windows, после чего будет осуществлено подключение ресурса.

Чтобы отключить ресурс, нужно выполнить команду

```
sudo umount /точка_монтирования
```

Если сетевой ресурс необходимо подключать после каждой перезагрузки Ubuntu, параметры подключения следует указать в файле /etc/fstab. Из соображений безопасности параметры учетной записи подключения (имя пользователя и пароль) не следует сохранять в этом файле. Поэтому предварительно создайте в режиме суперпользователя в текстовом редакторе файл, в который внесите две строчки с именем и паролем учетной записи, которая будет подключать необходимый сетевой ресурс:

```
username=myusername
password=mypassword
```

Сохраните файл в папке с именем, начинающимся с точки (например, .credit). Это скроет файл от "обычных" вариантов просмотра каталога.

> ***ЗАМЕЧАНИЕ***
>
> Выполнить эти операции можно, если, например, открыть текстовый редактор следующим образом: `sudo nano /etc/.credit`.

Назначьте файлу права только для суперпользователя (условно принято, что файл сохранен в папке /etc):

```
sudo chmod 700 /etc/.credit
```

Теперь откройте файл fstab с правами суперпользователя в текстовом редакторе и добавьте в него следующую строчку:

```
//сервер/ресурс /точка_монтирования cifs  rw,credentials=/etc/
.credit,codepage=cp866,iocharset=utf8  0  0
```

Обратите внимание, чтобы в строке было только пять пробелов, все параметры должны быть введены слитно, через запятую и без единого пробела.

После перезагрузки данный ресурс будет автоматически подключен к системе в режиме записи-чтения (`rw`).

> ***ЗАМЕЧАНИЕ***
>
> Права на запись-чтение можно указать более точно, если в строке параметров указать `dmask=маска,fmask=маска`.

Выполнение команд на удаленном компьютере

Часто возникает необходимость выполнить какую-либо операцию на удаленной системе. В Linux существует несколько команд, обеспечивающих выполнение операций на удаленном компьютере, например, `rlogin`, `rsh`. В некоторых случаях, как например, в пакете управления производством Infor (ранее известным как Baan), требуется конкретная утилита. Но при возможности выбора следует остановиться на технологии использования SSH для выполнения команд на удаленной системе.

Для использования SSH необходимо на сервере установить пакет OpenSSH. Лучше всего это сделать в момент установки операционной системы, поскольку потребность в этом пакете возникает практически с первого момента работы с сервером.

Синтаксис операции удаленного выполнения команды следующий:

```
ssh имя@сервер команда
```

После запуска команды система запросит пароль указанного в параметрах пользователя и при удачном подключении выведет на локальный экран итоги исполнения команды на удаленном компьютере. Например, `ssh имя@сервер pwd` позволит сменить пароль учетной записи `имя` на системе `сервер`. А команда `ssh имя@сервер ls ~ -la` отобразит подробное содержимое папки профиля пользователя (в листинге П9 часть вывода опущена).

Листинг П9

```
$ ssh имя@сервер ls ~ -la
имя@сервер's password:
Tunnel device open failed.
Could not request tunnel forwarding.
total 100
drwxr-xr-x 7 имя имя 4096 2009-01-20 09:47 .
drwxr-xr-x 3 root  root   4096 2008-12-22 17:49 ..
drwxr-xr-x 2 имя имя 12288 2009-01-15 13:47 1
-rw------- 1 имя имя 8354 2009-01-27 18:00 .bash_history
...
drwx------ 2 имя имя  4096 2009-01-15 10:59 .ssh
-rw-r--r-- 1 имя имя  0 2008-12-22 18:02 .sudo_as_admin_successful
```

Для копирования файлов между компьютерами удобна команда `scp`, входящая в состав пакета SSH:

```
scp имя1@host1:file1 имя2@host2:file2
```

В этом примере команда скопирует файл `file1`, который находится на компьютере `host1`, к которому мы подключимся с использованием учетной записи `имя1`, на компьютер `host2` в файл `file2` при подключении с именем `имя2`.

Команда запросит соответствующие пароли учетных записей. Для работы в пакетном режиме можно указать на соответствующие ключи аутентификации с помощью параметра `-i`. Более подробно о ключах команды можно прочесть в ее справочной документации.

Создание и удаление демонов

Автоматически запускаемые при старте компьютера программы называют демонами. Сценарии их запуска и остановки принято помещать в папку /etc/init.d. А непосредственный запуск — в зависимости от уровня запуска — осуществляется из папок /etc/rc0.d, /etc/rc1.d, … /etc/rcS.d. В этих папках фактически располагаются ссылки на сценарии запуска из папки /etc/init.d, причем если имя ссылки начинается с символа K, то это свидетельствует о команде остановки процесса, а если S — то о запуске. Цифры после символов S или K указывают на последовательность запуска/остановки.

Чтобы программа автоматически выполнялась при запуске сервера, скрипт ее запуска должен находиться в папке /etc/init.d. Для упрощения создания ссылок в соответствующих папках, применяется команда `update-rc.d`. Например, с ее помощью можно отключить запуск того или иного демона без удаления соответствующего пакета.

Команду `update-rc.d` следует запустить с указанием имени сценария, после чего соответствующие ссылки в папках запуска (для вариантов запуска по умолчанию: старт для уровней 2345 и останов для уровней 016) будут созданы. С ключом `remove` эта команда удаляет соответствующие ссылки. Следующие примеры показывают отключение и включения демона AppArmor:

```
sudo update-rc.d -f apparmor remove
sudo update-rc.d apparmor defaults
```

Выполнение заданий по расписанию

В Linux за запуск задания в нужное время отвечает специальная программа — `cron`, которая устанавливается по умолчанию при инсталляции системы. Чтобы назначить на какое-то время выполнение задания, нужно добавить

соответствующую запись в настройки `cron`. Для этого предназначена команда `crontab`:

```
crontab -e
```

> ***Примечание***
>
> Список заданий создается для каждого пользователя. Если администратору необходимо создать задание, которое будет исполняться от имени другого пользователя системы, то следует воспользоваться командой `crontab -u <имя> -e`. Если необходимо настроить права использования данной программы для различных пользователей, то соответствующие указания по редактированию конфигурации доступны в справочной системе.

Команда открывает файл настроек, в который нужно ввести необходимые параметры, указываемые в одной строке в следующем порядке:

```
минуты часы дни месяц день_недели команда
```

Первые параметры определяют, когда должна быть запущена команда, определенная в конце этой строки. Вы можете указывать точное значение (например, для минут значения от 0 до 59, часов — от 0 до 23 и т. п., дни недели — от 0 до 6 (воскресенье имеет номер 0)), * — если команда должна быть выполнена при любом значении данного параметра, несколько значений (например, 15,30 — для минут — через запятую), диапазон (например, если нужно выполнять команду только в первые три месяца, то можно указать 1-3), периодичность (*/2 означает выполнение, например, каждый второй час, если это указано для определения часов). Кроме того, возможно применение специальных названий: @reboot — для выполнения при каждой загрузке, @yearly или @annually — для выполнения один раз в год (первого числа в 0 часов 0 минут), @monthly, @weekly, @daily или @midnight, @hourly — соответственно, для запуска 1 раз в месяц, неделю, день, час (в этом случае в строке останется только это название и команда).

> ***Замечания***
>
> Можно также указывать сокращенные английские названия, например, jan, feb, mon, tue и т. п. Подробности можно уточнить в документации.
>
> По умолчанию `cron` сообщает о результатах запуска задания по электронной почте (на адрес владельца задания). Чтобы исключить это, добавьте в конец команды символы `>/dev/null 2>&1`.

После команды можно указывать комментарий, который должен начинаться с символа `#`. Можно включить запуск нескольких команд, в этом случае их нужно написать в этой же строке, разделяя символами `&&`.

По завершении определения команд нужно сохранить файл (при редактировании по умолчанию файл настроек открывается в программе nano, нужно воспользоваться командами редактирования, которые отражаются на экране).

Приведем примеры возможных записей таких заданий (листинг П10).

Листинг П10

```
30 15 * * * <команда>
#Команда запускается каждый день в 15 часов 30 минут
0 0-11/2 01 05 * <команда>
#Команда запускается каждый второй час первого мая
@monthly <команда>
# Команда запускается первого числа каждого месяца в 0 часов 0 минут
```

Для просмотра существующих заданий нужно воспользоваться командой `crontab -l`

Для удаления всех заданий достаточно выполнить команду `crontab -r`.

Существует еще ряд заданий, выполняемых `cron` каждый час, день, неделю и месяц. Эти задания описаны в файлах /etc/cron.hourly, /etc/cron.daily, /etc/cron.weekly и /etc/cron.monthly. Точное время выполнения этих заданий определяется в файле /etc/crontab по описанным выше правилам.

Выполнение заданий с помощью `cron` происходит в собственном окружении, в котором отсутствуют определения различных системных переменных, в том числе переменных пути, локализации и т. п. Поэтому при планировании заданий с использованием `cron` в расписании необходимо указывать полный путь к исполняемому файлу команды. Например, для выключения компьютера следует указывать не просто `shutdown`, а `/sbin/shutdown` с последующими ключами. А если назначенная к выполнению по графику команда задействует какие-либо языковые настройки (например, программа формирования отчета прокси-сервера free-sa и т. п.), то их следует определить в параметрах запуска команды либо задать соответствующие переменные среды в запускающем сценарии.

Сброс пароля администратора

Достаточно часто администраторов просят помочь с настройками чужого компьютера. При этом нередко пользователи не могут сообщить пароль административной учетной записи. В таких случаях приходится прибегать к *сбросу* пароля.

Для систем на основе Linux существует простая процедура смены пароля. Необходимо только загрузить компьютер в *однопользовательском режиме*.

Примечание

В большинстве систем сегодня используют загрузчик на основе Grub. В этом случае необходимо при запуске компьютера войти в меню загрузки (обычно нажать клавишу <Esc> при отображении соответствующей записи), выбрать в вариантах загрузки ту строку, которая начинается с *kernel*, открыть ее для редактирования (нажать клавишу <e>). В конец строки параметров загрузки следует добавить символ "S", сохранить изменения (нажать <Enter>) и загрузиться в этом варианте (нажать клавишу <b>). Перед вводом команды смены пароля необходимо убедиться, что жесткий диск подключен в режиме записи-чтения (командой `mount`), в противном случае — выполнить `mount -o remount,rw / диск`.

В Ubuntu для сброса пароля следует войти в режим восстановления (зайти в меню загрузки системы и указать второй вариант загрузки). После выполнения ряда команд на экран будет выведено приглашение выбора варианта дальнейшей загрузки (рис. П8). Необходимо выбрать третью строку (root Drop to root shell prompt).

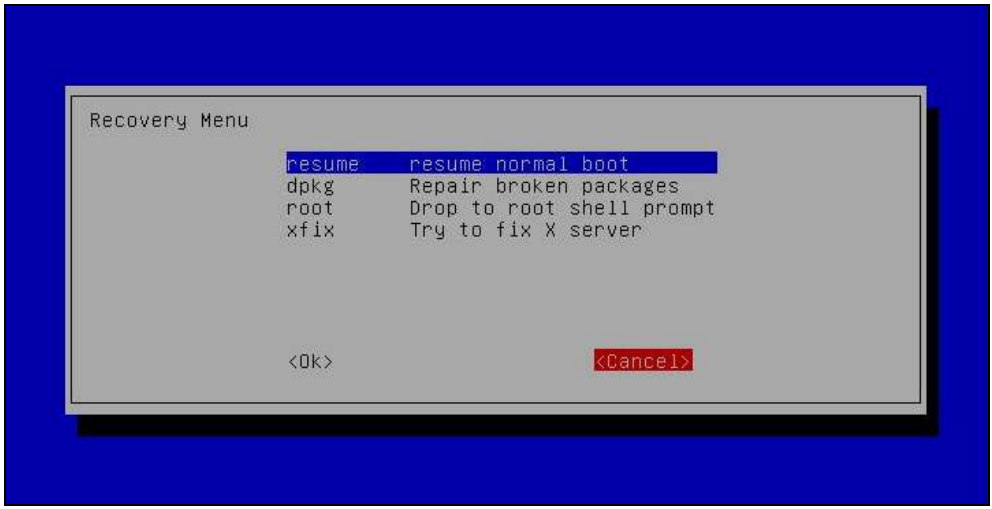


Рис. П8. Меню загрузки Ubuntu

После завершения загрузки по этому варианту вы войдете в режим консоли с правами суперпользователя. Здесь вы можете сменить пароль пользователя (`passwd имя`), но, поскольку обычно в чужой системе имя пользователя с правами администратора заранее не известно, проще назначить пароль суперпользователю командой

```
passwd
```

после чего перезагрузить систему и войти в нее суперпользователем.

Предметный указатель

8

802.1d 23
802.1s 24
802.1w 23
802.3ad 27

A

Active Directory (AD) 153
ADSI Edit 157

B

Bridge Protocol Data Units (BPDU) 23

D

Default gateway 34
DHCP,
  отказоустойчивая конфигурация 52
Distributed File System (DFS) 210
DNS-зона 54
DNS split 58
Domain Name System (DNS) 54
  сервер 54
Dynamic Host Configuration Protocol (DHCP) 31, 48

E

Easy Recovery 362
ERD Commander 130, 356, 358
EtherChannel 28
EvenTrigger 281

F

Flexible Single Master Operation role (FSMO) 137

G

Gateway 33
GetDataBack 362
GHost 125, 130
Global Catalog (GC) 138

H

Hardware Abstraction Layer (HAL) 126
Hidden Administrator 274
Hypertext Transfer Protocol (HTTP) 163

I

Insight for Active Directory 157, 158
Internet Control Message Protocol (ICMP) 29
Internet Message Access Protocol (IMAP) 163
IP:
  маска адреса 31
  порт 35
  шлюз 33
IP Multicast Addressing 30
IPv6 29
IP-адрес 29
  динамический 48
  статический 60

L

Late collision 345
Lightweight Directory Access Protocol (LDAP) 135
Link Aggregation Control Protocol 27
LogParser 279

M

MLT 28
Multi Spanning Tree Protocol (MSTP) 24

N

NetBIOS-имя 37
Network Address Translator (NAT) 75
Network Monitor 369

O

Offline NT Password Editor 130
Organization Unit (OU) 136

P

Performance Monitor 363
Port Knocking 94
Post Office Protocol 3 (POP3) 162
Provider 323

R

Rapid Spanning Tree Protocol (RSTP) 23
Remote Administrator 274
Remote Procedure Call (RPC) 163
Resource records 57
Routing 34

S

Server Performance Advisor 369
Simple Mail Transfer Protocol (SMTP) 162
Sites 137
Spanning Tree Protocol (STP) 23
Stub-зона 56

T

Transmission Control Protocol (TCP) 29

U

User Datagram Protocol (UDP) 29

V

VI 431
Virtual Network Computing 274
Virtual Routing Reduntance Protocol (VRRP) 25
Volume Shadow Copy 358

W

Web-based Enterprise Management (WBEM) 322
Windows Management Interface (WMI) 322

А

Адрес:
динамический 31
самостоятельное назначение 47

Б

Брандмауэр 35, 41

В

Вентилятор 348
Восстановление:
данных с жестких дисков 361
удаленных файлов 358

Д

Домен:
второго уровня 37
имя 37
первого уровня 37
создание 139

З

Запись ресурса 57
Запрос 323

К

Кабель оптический:
многомодовый 10
одномодовый 10
Клонирование рабочих станций 125
Команда:
change logon 249
chkdsk 354, 361
dcdiag 155
dnsdiag 70
enable 354
EVENTTRIGGERS 280
fixboot 353
fixmbr 353
ipconfig 39
ipv6 29
listsvc 354
logoff 249
MSG 250
MSTSC 249
netsh 45
netstat 35
nslookup 68, 158
ntdsutil 137
ping 40
portqry 41
query 249
reset session 250
route 34
SHADOW 249
TSPROF 250
TSSHUTDN 250
Корзина 359

Л

Лес 136

М

Маска адреса 31

О

Отказоустойчивая конфигурация:
на основе протоколов второго уровня 23
на основе протоколов третьего уровня 25
шлюз по умолчанию 25

П

Подразделение 136
Подсеть 31
Политика
групповая 136
Порт 35
well-known 35
сканирование 36
Провайдер 323
Протокол:
Hypertext Transfer Protocol (HTTP) 163
Internet Control Message Protocol (ICMP) 29
Internet Message Access Protocol (IMAP) 163
Post Office Protocol 3 (POP3) 162
Simple Mail Transfer Protocol (SMTP) 162
Transmission Control Protocol (TCP) 29
User Datagram Protocol (UDP) 29
сетевой 28

Р

Разделение DNS 58
Ресурс
административный 151

С

Сайт 137
Сервер:
BIND 139
глобального каталога 138
индивидуальная настройка 119
терминальный 241
установка 60
Сеть:
локальная 30
Служба:
DHCP 62
каталогов 62, 153
Сниффер 317, 345
Счетчик 364

Т

Таблица маршрутизации 34
Технология трансляции адресов 75
Точка восстановления 356
Трансляция адресов 30

У

Утилита:
dcpromo 139
ntdsutil.exe 157
ldp.exe 157
sysprep 126

Ф

Файл:
hosts 53
lmhosts 54
networks 53
wpad.dat 99

Ш

Шлюз 33