SYNGRESS®

РУССКАЯ РЕДАКЦИЯ

bhv®

ДЭВИД АЛЛЕН

ПЕРЕХОД с WINDOWS на LINUX

Полное описание стратегий миграции и развертывания инфраструктуры Linux

Инструменты и руководства по переходу с Windows NT/2000 на любой дистрибутив Linux, приложения защиты от вирусов и спама

Автоматизация задач перехода на Linux с помощью сценариев, размещенных на компакт-диске

+CD

С И С А Д М И Н
СИСТЕМНЫЙ АДМИНИСТРАТОР

ПЕРЕХОД с WINDOWS на LINUX

Дэвид Аллен
Эндрю Скотт
Герберт Льюис
Джон Стайл
Тимоти Такк

«Русская Редакция» **«БХВ-Петербург»**

2005

УДК 681.3.06
ББК 32.973.81-018.2
А21

Аллен Дэвид и др.

А21 Переход с Windows на Linux: Пер. с англ. — М.: Издательско-торговый дом «Русская Редакция»; СПб.: «БХВ-Петербург», 2005. — 480 стр.: ил.

ISBN 5-94157-720-6 («БХВ-Петербург»)
ISBN 5-7502-0068-X («Русская Редакция»)

Книга содержит подробное описание планирования процесса перехода с Windows (Windows 9x/Me, NT4, Windows 2000 и Windows XP) на любой дистрибутив Linux, сценарии автоматизированного перехода с помощью программ, размещенных на прилагаемом компакт-диске, понятия оценки уязвимости и защиты систем.

Для системных администраторов

УДК 681.3.06
ББК 32.973.81-018.2

Copyright © 2004 by Syngress Publishing, Inc. All rights reserved. Printed in the United States of America. Translation Copyright © 2005 by BHV-St.Petersburg. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

© 2004 by Syngress Publishing, Inc. Перевод на русский язык © 2005 «БХВ-Петербург». Все права защищены. За исключением публикаций, разрешенных Актом о защите прав от 1976 года, никакая часть настоящей книги не может быть воспроизведена или передана в какой бы то ни было форме и какими бы то ни было средствами, будь то электронные или механические, включая фотокопирование, запись на магнитный носитель или сканирование, записана в базы данных или размещена в электронных средствах распространения, если на то нет предварительного письменного разрешения издательства, за исключением листингов программ, которые можно вводить, сохранять и выполнять на компьютере, но нельзя воспроизводить для публикации.

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 30.08.05.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 38,7.
Тираж 3000 экз. Заказ № 1269
«БХВ-Петербург», 194354, Санкт-Петербург, ул. Есенина, 5Б.

Санитарно-эпидемиологическое заключение на продукцию
№ 77.99.02.953.Д.006421.11.04 от 11.11.2004 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 1-931836-39-6 (англ.)
ISBN 5-94157-720-6
(«БХВ-Петербург»)
ISBN 5-7502-0068-X
(«Русская Редакция»)

© 2004 by Syngress Publishing, Inc.

© Перевод на русский язык, «БХВ-Петербург» 2005

© Оформление издательско-торговый дом «Русская Редакция», 2005

Оглавление

Благодарности XV
Об авторах XVI
Благодарности от автора XVIII
Информация о CD-ROM XIX
Предисловие XX

Глава 1 Порядок осуществления миграции сетевых служб 1
Введение 2
Оценка существующей инфраструктуры 2
Повесть о двух предприятиях 2
Опись серверов 5
Создание схемы инфраструктуры 5
Документирование дополнительной оценочной информации 7
Определение требований к инфраструктуре Linux 7
Создание списка функциональных требований 7
Выявление сдерживающих факторов 9
Проектирование инфраструктуры Linux 10
Создание проекта постмиграционной инфраструктуры 10
Тестирование инфраструктуры Linux 12
Составление плана испытаний 12
Развертывание инфраструктуры Linux 14
Переход к инфраструктуре Linux 14
Резюме 15
Краткое резюме по разделам 16

Глава 2 Основные сетевые службы TCP/IP 17
Введение 18
Принципы работы служб присвоения IP-адресов 19
Понятие «клиент DHCP» 20
Конфигурирование серверов DHCP 24

Принципы работы служб разрешения имен ... 26
Процесс разрешения имен на основе файла ... 26
Процесс разрешения имен на основе DNS ... 27
Понятие динамического DNS (DDNS) ... 28
Конфигурирование BIND и DHCP для динамического DNS ... 28
Принципы работы служб временной синхронизации ... 29
Понятие о синхронизирующем сетевом протоколе ... 29
Понятие о клиентах NTP для Linux ... 30
Понятие клиентов служб времени Windows ... 31
Перенос MS-DNS/DHCP на BIND/DHCPD Linux ... 32
Перенос областей действия и функций DHCP ... 32
Перенос информации DNS ... 36
Резюме ... 39
Краткое резюме по разделам ... 40
Часто задаваемые вопросы ... 41

Глава 3 Службы каталогов ... 43

Введение ... 44
Принципы работы LDAP и каталогов ... 44
Понятие терминов LDAP ... 45
Подключение к серверу каталогов ... 47
Понятие запросов LDAP ... 48
Принципы работы служб каталогов Microsoft ... 49
Понятие Windows NT SAM ... 49
Понятие служб каталогов Exchange 5.5 ... 49
Понятие Active Directory ... 50
Принципы работы OpenLDAP ... 51
Понятие демонов («сторожевых» процессов) сервера OpenLDAP ... 51
Понятие утилит OpenLDAP ... 51
Проектирование служб каталогов на базе Linux ... 52
Проектирование Дерева информации каталога ... 52
Проектирование инфраструктуры OpenLDAP ... 53
Конфигурирование и тестирование серверов OpenDLAP ... 55
Резюме ... 56
Краткое резюме по разделам ... 57
Часто задаваемые вопросы ... 59

Глава 4 Службы аутентификации ... 60
Введение ... 61
Принципы аутентификации в Windows ... 62
Регистрация в Windows 98/NT ... 62
Регистрация в Windows 2000/XP ... 63
Принципы аутентификации в Linux ... 63
Понятие аутентификации LDAP ... 64
Аутентификация /etc/passwd/shadow ... 65
Аутентификация NIS ... 66
Настройки аутентификации клиента Linux ... 66
Понятие PAM ... 67
Проектирование служб аутентификации на базе Linux ... 70
Проектирование межплатформенных служб аутентификации ... 71
Установка и конфигурирование Samba ... 73
Переход от NT/Exchange или Active Directory ... 76
Подготовка к процессу перехода ... 76
Путь перехода NT / Exchange 5.5 ... 77
Путь перехода Active Directory ... 81
Перенос файлов аутентификации при регистрации в Windows ... 85
Тестирование служб аутентификации ... 85
Активизация шифрования ... 85
Резюме ... 87
Краткое резюме по разделам ... 88
Часто задаваемые вопросы ... 90

Глава 5 Файловые службы ... 91
Введение ... 92
Понятие файловых систем Windows ... 92
Понятие о файловых системах семейства Windows FAT ... 92
Понятие файловых систем семейства Windows NTFS ... 95
Понятие файловых систем Linux ... 98
Понятие Ext2/3 ... 98
Понятие о ReiserFS ... 100
Понятие управления полномочиями (управления доступом) ... 103
Понятие создания резервных копий файлов, их восстановления и возможностей репликации ... 108
Определение критичных файлов для резервирования ... 109
Определение способа создания резервных копий ... 110

Определение типа носителя резервирования 110
Планирование создания резервных копий....112
План обращения и архивирования носителей 112
AMANDA 114
Процесс резервирования системой AMANDA....115
Установка AMANDA....117
Организация сервера резервирования 122
Проектирование файловых служб на базе Linux 123
Аппаратные ресурсы 123
Перенос файловых служб в систему Linux 125
Перенос полномочий на использование файлов 126
Утилита showwaccs инструментальных средств поддержки....127
Краткое резюме по разделам....128
Часто задаваемые вопросы....131

Глава 6 Службы печати 132

Введение....133
Понятие служб печати Windows....133
Понятие служб печати Linux 134
Конфигурирование печати на Linux с помощью BSD или SYSV 136
Конфигурирование печати на Linux с помощью CUPS 138
Совместное использование печатающих устройств через Samba....144
Понятие автоматической загрузки драйвера печатающего устройства....152
Перенос служб печати Windows на CUPS/Samba 158
Резюме 159
Краткое резюме по разделам....159
Часто задаваемые вопросы....161

Глава 7 Службы передачи сообщений 162

Введение....163
Понятие служб передачи сообщений Microsoft....164
Принципы передачи информации в Exchange 5.5 165
Принципы передачи информации в Exchange 2000....167
Понятие служб передачи сообщений на базе Linux....168
Отправка и получение электронной почты по Интернет....168
Понятие компонентов системы передачи информации Linux 170
Анализ открытых серверных программных средств передачи сообщений....178

Проектирование служб передачи сообщений на базе Linux....186
Определение архитектуры электронной почты Интернет....187
Выбор программных средств передачи сообщений....190
Определение способа хранения электронных сообщений....191
Создание схемы почтового сервера Linux....192
Интегрирование служб защиты от спама и вирусов....194
Понятие спама....194
Понятие вирусов....198
Обзор открытых приложений защиты от спама и вирусов....200
Проектирование служб защиты от спама и вирусов....202
Перенос информации из Exchange в Linux....206
Подготовка Exchange к переносу....206
Установка серверного набора Courier IMAP....208
Перевод службы электронной почты на систему Linux....209
Резюме....210
Краткое резюме по разделам....211
Часто задаваемые вопросы....213

Глава 8 Службы коллективного пользования и ведение календаря....214

Введение....215
Понятие служб Exchange, служб коллективного пользования Outlook и календаря....215
Понятие служб коллективного пользования и календаря на базе Linux....217
Понятие eGroupware....217
Понятие Horde....218
Обзор OPEN-XCHANGE (OX)....219
Понятие программного пакета коллективного пользования TWiki....220
Переход к службам коллективного пользования и календарю Linux....222
Понятие Outport....222
Другие способы переноса информации....223
Резюме....224
Краткое резюме по разделам....225
Часто задаваемые вопросы....226

Глава 9 Web-службы. Сравнительный анализ Информационного сервера Интернет и Apache....227

Введение....228
Предыстория: Протокол передачи гипертекстовых документов....229

Информационный сервер Интернет 230
Перед началом работы 230
Создание индексной страницы по умолчанию 231
Создание Web-сайта по умолчанию 233
Виртуальные каталоги 234
Защита 235
Виртуальные серверы 239
Web-сервер Apache 241
Предыстория Apache 242
Установка 243
Запуск, остановка и проверка состояния 243
Конфигурация 244
Web-страница по умолчанию 248
Псевдонимы и псевдонимы сценариев 250
Защита и разрешения 251
Файлы .htaccess 253
Виртуальный хостинг 254
Модули 260
Графические инструменты 261
Перенос статичных сайтов с IIS на Apache 263
Резюме 264
Краткое резюме по разделам 264
Часто задаваемые вопросы 266

Глава 10 Порядок миграции настольных систем 268

Введение 269
Оценка текущей настольной среды 271
Типы пользователей 271
Составление списка активов настольной системы 272
Каталогизация форматов файлов 275
Спецификация функциональных требований 276
Проектирование настольной системы Linux 276
Спецификация функциональной замены 279
Компоновка компьютеров для обучения 280
Тестирование настольной системы Linux 281
Перенос данных программных приложений и профилей 281
Резервирование данных с настольных рабочих станций 282
Установка Linux 283

Импортирование профилей пользователей и предпочтений 283
Обучение пользователей настольных систем 283
Обучающие руководства....284
Отличия настольных рабочих станций Linux от Windows....285
Развертывание настольных систем Linux 289
Документация 289
Резюме 289
Краткое резюме по разделам....290
Часто задаваемые вопросы 291

Глава 11 Внутренняя структура настольной рабочей станции Linux 292

Введение....293
Традиционные настольные среды....293
Gnome....294
KDE 295
Общие особенности....298
Установка обеих настольных сред, одной — по умолчанию 298
Альтернативные диспетчеры окон 299
Серверы X Window и диспетчеры управления окнами 299
Сравнительный анализ серверов X Window и диспетчеров управления окнами....300
Диспетчеры управления окнами как альтернатива настольным рабочим средам....302
Клиенты электронной почты и управления персональной информацией....304
Evolution 305
KDE Suite/KMail 307
Aethera....308
Mozilla Mail/Thunderbird 308
Sylpheed 310
Существенная информация 311
Рекомендуемые программные средства для работы с электронной почтой и PIM 312
Перенос электронной почты 312
Web-браузеры....317
Mozilla 317
Firefox 319
Galeon 320
Konqueror....320

Opera 320
Перенос закладок 321
Подключаемые модули браузера 322
Офисные пакеты 324
OpenOffice.org 325
StarOffice 329
KOffice 329
Hancom Office 330
Запуск приложений Windows на Linux 330
Программные средства уровня совместимости 330
Резюме 333
Краткое резюме по разделам 334
Часто задаваемые вопросы 336

Приложения по вопросам защиты 337

Приложение А Введение в сетевой анализ и Ethereal 339

Введение 340
Понятие сетевого анализа и анализа пакетов 340
Кому нужен сетевой анализ? 343
Как взломщики сетей используют анализаторы пакетов? 344
Как выглядят «прослушанные» данные? 346
Обычные сетевые анализаторы 347
Принципы работы сетевого анализатора 352
Понятие Ethernet 352
Понятие модели OSI 353
CSMA/CD 357
Аппаратные средства: отводы, концентраторы, коммутаторы 358
Зеркальное отражение портов 361
«Разгром» коммутаторов 362
Обнаружение сетевых анализаторов пакетов 364
Защита от сетевых анализаторов пакетов 368
Сетевой анализ и корпоративная политика 369
Резюме 370
Краткое резюме по разделам 372
Часто задаваемые вопросы 374

Приложение В Введение в системы обнаружения несанкционированного вторжения в сеть и Snort 376

Введение в системы обнаружения несанкционированного вторжения в сеть.....377
Что такое несанкционированное вторжение?.....377
Принципы работы IDS.....384
Ответы на общие вопросы по IDS.....401
Обоснование необходимости систем обнаружения несанкционированных вторжений.....401
Почему брандмауэр не может выполнять функции IDS?.....402
Чем я так заинтересовал хакеров?.....402
Как IDS соответствует общему плану сетевой защиты?.....404
Где искать несанкционированные вторжения?.....405
В чем заключается помощь IDS?.....408
В чем бессильны IDS?.....412
Дополнительные преимущества обнаружения несанкционированных вторжений.....415
Ввод Snort в архитектуру сетевой защиты.....415
Вирусы, черви и Snort.....416
Известные инструменты сетевого нападения и Snort.....416
Написание авторских подписей с помощью Snort.....417
Использование IDS для мониторинга корпоративной политики.....417
Определение аспектов проектирования и конфигурирования IDS.....417
Ложные и полезные сигналы тревоги.....418
«Обман» IDS.....418
Прибыль на инвестиции: стоит ли игра свеч?.....420
Терминология IDS.....421
Системы предотвращения незаконного проникновения (HIPS и NIPS).....421
IDS-шлюз.....421
IDS главного узла.....421
Анализ протоколов.....422
IDS на базе целевой системы.....422
Резюме.....422
Краткое резюме по разделам.....423
Часто задаваемые вопросы.....424

Приложение C Понятие оценки уязвимости систем и Nessus 426
Введение 427
Что такое оценка уязвимости системы? 427
Зачем нужна оценка уязвимости? 430
Типы оценок 432
Автоматические системы оценки 433
Сравнение автономных программных продуктов и полученных по подписке 434
Процесс оценки 435
Два подхода 442
Административный подход 443
Внешний подход 444
Смешанный подход 445
Реалистические виды на будущее 447
Ограничения автоматизации 449
Резюме 450
Краткое резюме по разделам 451
Часто задаваемые вопросы 452

Благодарности

Издательство Syngress выражает благодарность следующим людям, без которых выход данной книги был бы невозможен

Книги Syngress распространяются в США и Канаде компанией O'Reilly Media, Inc. Энтузиазм и рабочая этика в O'Reilly — невероятные, и авторам хотелось бы поблагодарить всех сотрудников компании за их время и усилия, направленные на подготовку книги к печати: Тима О'Рейли (Tim O'Reilly), Лауру Болдуин (Laura Baldwin), Марка Брокеринга (Mark Brokering), Майка Леонарда (Mike Leonard), Донну Селенко (Donna Selenko), Бонни Шихан (Bonnie Sheehan), Синди Дэвис (Cindy Davis), Гранта Киккерта (Grant Kikkert), Опола Матсутаро (Opol Matsutaro), Стива Хэйзелвуда (Steve Hazelwood), Марка Уилсона (Mark Wilson), Рика Брауна (Rick Brown), Лесли Беккер (Leslie Becker), Джил Лотроп (Jill Lothrop), Тима Хинтона (Tim Hinton), Кайла Харта (Kyle Hart), Сэйру Уиндж (Sara Winge), Си-Джей Рэйхилла (C. J. Rayhill), Питера Пардо (Peter Pardo), Лесли Крэнделла (Leslie Crandell), Валери Дау (Valerie Dow), Регину Аджио (Regina Aggio), Паскаля Хоншера (Pascal Honscher), Престона Пола (Preston Paull), Сьюзан Томпсон (Susan Thompson), Брюса Стюарта (Bruce Stewart), Лауру Шмир (Laura Schmier), Сью Уиллинг (Sue Willing), Марка Джейкобсена (Mark Jacobsen), Бетси Валижевски (Betsy Waliszewski), Дона Манна (Dawn Mann), Катрин Баррета (Kathryn Barrett), Джона Чодаки (John Chodacki) и Роба Баллингтона (Rob Bullington).

На редкость трудолюбивую рабочую группу компании Elsevier Science, включая Джонатана Банкелла (Jonathan Bunkell), Иэна Сигера (Ian Seager), Дункана Энрайта (Duncan Enright), Дэвида Бертона (David Burton), Розану Рамачиотти (Rosanna Ramacciotti), Роберта Фэрбразера (Robert Fairbrother), Мигеля Санчеса (Miguel Sanchez), Клауса Берана (Klaus Beran), Эмму Уайатт (Emma Wyatt), Рози Мосс (Rosie Moss), Криса Хоссака (Chris Hossack), Марка Ханта (Mark Hunt) и Кристу Леппико (Krista Leppiko), за помощь в распространении наших профессиональных взглядов.

Дэвида Бакленда (David Buckland), Мари Чиенг (Marie Chieng), Люси Чонг (Lucy Chong), Лесли Лим (Leslie Lim), Одри Ган (Audrey Gan), Панг Аи Хуа (Pang Ai Hua) и Джозефа Чана (Joseph Chan) из компании STP Distributors за энтузиазм, с которым была принята книга.

Квона Сунга Джун (Kwon Sung June) из издательства Acorn Publishing за поддержку.

Дэвида Скотта (David Scott), Трисию Уилден (Tricia Wilden), Мариллу Берджесс (Marilla Burgess), Аннетт Скотт (Annette Scott), Эндрю Суоффера (Andrew Swaffer), Стефена О'Донахью (Stephen O'Donoghue), Бека Лоу (Bec Lowe) и Марка Лэнгли (Mark Langley) из компании Woodslane за помощь в распространении книги в Австралии, Новой Зеландии, Папуа Новой Гвинее, Фиджи Тонга, на Соломоновых островах и островах Кука.

Уинстона Лима (Winston Lim) из издательства Global Publishing за помощь и поддержку в распространении книг Syngress на Филиппинах.

Ведущий автор

Дэвид Аллен (David Allen) (Президент CRCI) — ведущий автор и технический редактор книги «Руководство по переходу с Windows на Linux». В восьмилетнем возрасте Дэвид увлекся программированием и уже свыше двух десятилетий занимается вычислительной техникой. Руководил больше чем 25 000 проектов перехода в компаниях на пяти континентах. Работал в международных банках (Schwab, Credit Suisse, JPMorgan), в технологических компаниях и государственных организациях, включая НАСА. В течение многих лет являлся сторонником Open Source и спикером LinuxWorld и Open Source Convention O'Рейли.

Дэвид основал компанию Computer Resources Consulting Inc., предоставляющую консалтинговые услуги клиентам по всему миру. CRCI обеспечивает переход, техническое обслуживание, обучение и предоставляет консультации по системной защите с помощью открытых программных решений. Более подробная информация о CRCI и службах перехода, обеспечиваемых авторами книги имеется на web-сайте *www.crconsulting.com*, телефон — (800) 884-9885.

Соавторы

Герберт Льюис (Herbert Lewis) с 1997 года являлся членом рабочей группы Samba. В настоящее время работает в Panasas Inc., обеспечивая техническое обслуживание CIFS-шлюза программного пакета, использующего программное обеспечение Samba. Ранее работал в компании SGI, занимался разработкой и обслуживанием программного обеспечения Samba а также некоторых открытых программных средств на операционной системе IRIX. Имеет степень бакалавра Американской академии Coast Guard и степень магистра Стэнфордского университета. Дипломированный инженер.

Джон Стритон Стайл (John Streeton Stile) — старший инженер компании Pervasive Netwerks, занимающейся проектированием открытых решений для сред Windows и Unix. Имея степень бакалавра биохимии Университета Калифорнии в Дэвисе (University of California, Davis) и опыт исследования лекарственных препаратов, Джон применяет в своей работе научный метод исследований, инженерного проектирования, а также устранения неисправностей программных решений для сетей и вычислительной техники.

В компьютерной индустрии Джон начал свою деятельность в 1997 году; в 1999 году начал изучение Unix, обнаружив, что, в отличие от биологии, компьютерные проблемы, так или иначе, решить можно всегда. Он работал в крупных и мелких организациях, как государственных, так и частных, в разных сферах деятельности. В число компаний и корпораций, сотрудником которых он являлся, входят Industrial Light and Magic, Adobe Systems, Ohlone College, Certicom и Skyflow.

Джон Стайл благодарит Джона Х. Терпстра (John H. Terpstra) за консультативную помощь, за обновление RPM'ов и личный вклад в процесс написания данной книги. Является автором книги «Samba-3 на примерах» (*Samba-3 By Example*) и готовящейся к выпуску книги «OpenLDAP на примерах» (*OpenLDAP By Example*). Подрядчик программных решений Samba.

Джеймс Стэнжер (James Stanger) (доктор наук, CIW Master Administrator, Linux+, Security+, A+, CTP) — Вице-президент по сертификации компании ProsoftTraining. Председатель Консультативного совета LPI, занимается подготовкой экзамена CIW, а также разрабатывал сер-

тификаты Symantec и CompTIA. Плодовитый писатель, Джеймс готовил материалы для ComputerPREP, Symantec, Syngress, Sybex и McGraw Hill. В число его книг входят такие работы, как «Защита Linux» (*Hack Proofing Linux*), «Руководство по защите электронной почты от вирусов» (*E-mail Virus Protection Handbook*) и «Усовершенствованное управление службами Интернет» (*Advanced Internet Services Management*). Он также является консультантом по сетевым решениям, специализирующимся на аудите сетевой безопасности, по переходу с платформы Windows на Linux, а также по организации виртуальных магазинов на базе LAMP.

Эндрю Тейлор Скотт (Andrew Taylor Scott) — студент факультета вычислительной техники и философии Сити-колледжа в Сан-Франциско (City College of San Francisco); дает консультации по Linux для некоммерческих организаций, стремящихся к внедрению открытых программных средств. До возвращения в колледж работал в компании Linuxcare Inc. — передовой организации, обеспечивающей техническое обслуживание для пользователей любых дистрибутивов и предоставляющей профессиональные услуги производственным компаниям, заинтересованным в переходе на программные средства для Linux. Во время работы в Linuxcare, Эндрю занимал должности инженера по техническому обслуживанию, консультанта по профессиональным службам. Он также работал техническим писателем с разработкой учебных курсов в SGML для обучения инженеров Linux работе с главными почтовыми и web-системами на GNU/Linux. Пользуясь благоприятными возможностями в компании Linuxcare он продолжал собственное обучение работе с GNU/Linux и развитию Открытых программных средств путем участия в разработке и выпуске нескольких версий мини-дистрибутивов Linuxcare Bootable Business Card (LNX-BBC). После этого работал консультантом по нескольким пользовательским программным решениям Linux с разработкой web-приложений с Linux, Apache, MySQL и PHP (LAMP).

В число клиентов Эндрю входят Thrasher Magazine, Theme-Co-op Promotions, Fast Country, Институт совместных изменений и ассоциированных студенческих советов в CCSF. Завершил несколько сертификаций по системам Linux и сетевому администрированию в университете Linuxcare, включая LNX-102, LNX-201, LNX-202 и LNX-301. Получил сертификат 1-й степени в области администрирования системы Sun Solaris и показал очень хорошие результаты в подробных обучающих курсах по внутреннему устройству операционных систем Unix и Linux и по программированию на C++. Эндрю имеет реальный практический опыт развертывания серверов Linux в корпоративных и коллокационных сетях с установкой аппаратных средств и сетевых служб, а также проектирования соответствующих устройств Linux часто с гораздо меньшими затратами, по сравнению с коммерческими патентованными решениями. Сейчас занят разработкой открытых программных пакетов коллективного пользования с LAMP для виртуальных хостов.

Тимоти Такк (Timothy Tuck) — Президент Pervasive Netwerks и основатель Хейвордской группы пользователей Linux (Hayward Linux Users), известной как LinuxDojo.net. Специализируется на платформе Linux и переходе с Windows на Linux. В настоящее время его компания предоставляет ИТ-услуги более чем 70 компаниям, расположенным в районе Кремниевой долины. Тимоти начинал карьеру на должностях исследователя и разработчика опытных образцов для корпорации Logitech и старшего технического инженера и администратора лаборатории в Cisco Systems. Последние 20 лет занимается вычислительной техникой; в течение 6 лет пользуется системой Linux. Проживает в Хейворде (Hayward), Калифорния, женат на самой прекрасной женщине в мире — Луизе Чен (Louise Cheng).

Тимоти чрезвычайно признателен Дэвиду Алену за его замысел данной книги, Джейму Квигли (Jaime Quigley) за помощь в процессе написания, Эндрю Скотту за помощь в редактировании глав и Рику Муну (Rick Moen) за ценные рекомендации. Огромное «спасибо» всем хакерам и программистам, вносящим свой вклад в развитие Open Source (именно благодаря ему данная книга увидела свет), Линусу Торвальдсу (Linus Torvalds) за такой подарок миру — систему Linux, которая продолжает свое победное шествие, всем сотрудникам LinuxDojo.net, чей вклад в пользовательскую группу месяц за месяцем обеспечивал ее деятельность. Следует особо отметить жену Тима, которая бросила все свои дела и приехала за полмира, чтобы помогать мужу в течение бесконечных часов практических исследований.

Технический редактор

Кристиан Лахти (Christian Lahti) — старший консультант CRCI, имеющий 15-летний опыт работы в области информационных технологий. Является экспертом в сфере защиты, систем и организации сетей, разрабатывал и реализовывал глобальные ИТ-инфраструктуры с особым упором на Linux и открытые программные средства. Предоставлял консалтинговые услуги по успешной межплатформенной интеграции и сетевому взаимодействию. Кроме этого, Кристиан имеет опыт проектирования баз данных и web-разработок. Является спикером и преподавателем OSCON Linux World и O'Reilly.

Благодарности от автора

Несмотря на то, что автор является наиболее заметной фигурой в создании книги, ему помогает огромное количество людей, важность и необходимость работы которых при подготовке издания трудно переоценить.

Мне хочется искренне поблагодарить замечательный коллектив издательства Syngress, в частности Эндрю Уильямса (Andrew Williams) и Джейма Квигли (Jaime Quigley). Их опыт в издательском деле и редактировании вкупе с трудолюбием и преданностью позволили мне превратить «Руководство по переходу с Windows на Linux» из идеи в живую книгу.

Особая благодарность — Кристиану Лахти (Christian Lahti), автору программных сценариев книги и составителю прилагаемого CD-ROM. Бессонные ночи, проведенные за «шлифовкой» сценариев, его желание развития лаборатории Iceberg (места, откуда Acme Widgets и Ballystyx Engineering пришли в этот мир!) и неоценимые проницательность и поддержка в процессе написания книги внесли значительный вклад в качество предложенного материала, что сделало книгу реальностью. Созданный им код автоматизированного перехода с платформы Windows на Linux будет использоваться в компаниях по всему миру. Спасибо, Крис.

Я также признателен всем моим друзьям и семье, особенно родителям. Благодарю Стефена Хоффмана (Stephen Hoffman), Дрейтона Баулса (Drayton Bowles) и Боба Кули (Bob Cooley) за поддержку и понимание на протяжении длительного процесса создания книги.

Херб Льюис (Herb Lewis), Эндрю Скотт (Andrew Scott), Джеймс Стэнжер (James Stanger), Питер Тоуни (Peter Thoeny), Сэм Варшавчик (Sam Varshavchik), Джон Стайл (John Stile) и Тим Такк (Tim Tuck) были авторами глав. Большое спасибо всем!

Спасибо — Джереми Эллисону (Jeremy Allison) за его поддержку в процессе написания книги и — что немаловажно! — за написание Samba!

Дэвид Ален

7 октября 2004 года

Информация о CD-ROM

На прилагаемом к книге CD-ROM содержатся сценарии Инструментального набора для перехода с Windows на Linux и файлы конфигурации, а также (по главам) краткое описание конфигурационных файлов, используемых вымышленными компаниями Acme Widgets и Ballystyx Engineering. Упрощенное руководство по материалам диска содержится в **index.html**.

В приведенной ниже таблице перечислены все каталоги, их связи с соответствующими главами, а также описаны файлы каталогов. Важно отметить, что, несмотря на то, что перечисленный указатель пакетов содержит последние версии открытых инструментальных средств на время публикации книги, открытые проекты развиваются с космической скоростью, поэтому многие сценарии могут казаться устаревшими. Самые последние версии программных продуктов имеются на соответствующих web-сайтах, включая «Руководство по переходу с Windows на Linux» (W2Lmt) — *www.syngress.com/solutions* и *http://sourceforge.net/projects/w2lmt*.

Каталог	Глава	Содержание
Chap01	Порядок осуществления миграции сетевых служб	—
Chap02	Основные сетевые службы TCP/IP	Файлы конфигурации DHCP/DNS и сценария переноса
Chap03	Службы каталогов	Файлы конфигурации OpenLDAP
Chap04	Службы аутентификации	Файлы конфигурации сценария переноса Samba и служб каталогов/аутентификации
Chap05	Файловые службы	—
Chap06	Службы печати	—
Chap07	Службы передачи сообщений	Файлы конфигурации сценария переноса почтовых ящиков
Chap08	Службы коллективного пользования и ведение календаря	Инструмент Outlook Export
Chap09	Web-службы	—
Chap10	Порядок миграции настольных систем	—
Chap11	Внутренняя структура настольной рабочей станции Linux	—

▶▶

Каталог	Глава	Содержание
Etc	ВСЕ	Базовые файлы конфигурации для W2Lmt с комментариями
Package	ВСЕ	Бинарные файлы в пакетах и сжатые исходные файлы многих рассмотренных в книге инструментальных средств, включая инструментарий перехода с Windows на Linux; а также все зависимости, необходимые для установки
Src	ВСЕ	Сценарии W2Lmt в исходных текстах
et_sn_ns	Приложение A	Ethereal
et_sn_ns	Приложение B	Snort
et_sn_ns	Приложение C	Nessus

Предисловие

На протяжении более двух десятков лет операционная система и прикладное программное обеспечение под маркой Microsoft удовлетворяли рыночную потребность и превратились в хрестоматийный для Америки пример успешного ведения бизнеса. В условиях стремительно меняющейся экономической ситуации корпорация Microsoft процветала как в периоды спадов, так и подъемов. Однако, аналогично тому, как конкуренты Генри Форда (Henry Ford) гнались за рыночной стабильностью и монополией автомобиля Модели Т, группа пингвинов напористо прокладывала себе путь к успеху наперерез исполинскому грузовику из Редмонда.

Линус Торвальдс (Linus Torvalds) и не мечтал конкурировать с Microsoft, когда в августе 1991 года впервые разместил в сети Usenet сообщение о разработанном им новом ядре. Но именно в этот день мир информационных технологий изменился навсегда. Результатом первых робких начинаний Линуса стал совершенно ошеломительный коммерческий успех: десятки миллионов пользователей на всех континентах. 25 августа 1991 года Линус изложил коллегам идеи об открытой системе. Он писал:

```
От: torvalds@klaava.Helsinki.FI (Linus Benedict Torvalds)
Конференция: comp.os.minix
Тема: Что Вам больше всего хотелось бы увидеть в minix?
Дата: 25 августа 1991 г. 20:57:08 GMT
Привет всем, кто имеет дело с minix!

Я разрабатываю (бесплатную) операционную систему (просто хобби; система совсем
небольшая и не такая профессиональная, как GNU) для клонов AT 386(486). Работа идет
полным ходом с апреля, и все уже почти готово. Мне бы хотелось получить любые
отзывы, как положительные, так и отрицательные, от людей, работающих в minix,
потому что моя система чем-то ее напоминает (помимо прочего, по практическим
причинам, здесь такая же физическая структура файловой системы).

В данный момент я перенес bash (1.08) и GCC (1.40), и все, вроде, работает.
Это означает, что через несколько месяцев у меня появится нечто более-менее
осязаемое, и поэтому хочется узнать, что большинство компьютерщиков хотело бы
получить в результате. Приветствуются любые предложения, но я не обещаю,
что все они будут реализованы. ☺
```

Вместо того чтобы попытаться нажиться на интеллектуальной собственности, Линус решил бесплатно распространить плоды своих исследований, чтобы любой мог внести посильный вклад в проект, которому в скором времени будет суждено стать одной из самых популярных в мире открытых операционных систем. С этой целью он выбрал для Linux Общественную Лицензию GNU — GNU Public License (GPL). (Ранние версии ядра Linux распространялись по другой лицензии, ограничивающей коммерческое распространение. — *Примеч. науч. ред.*).

На веб-сайте *www.dwheeler.com/oss_fs_why.html* Дэвид Уилер (David Wheeler) отмечал многочисленные преимущества использования открытых программных средств (open source software, OSS).

1. OSS защищает пользователей от рисков и недостатков работы с системами одного поставщика.
2. OSS защищает пользователей от судебных исков по вопросам лицензирования и управленческих затрат.
3. OSS обладают большей гибкостью, нежели закрытые (патентованные) программные средства.
4. Использование OSS подразумевает позитивный общественный, моральный или этический подтекст.
5. Существуют убедительные свидетельства того, что OSS стимулируют, а не сдерживают инновации.

Дэвид Ален (David Allen) — президент и основатель компании «Си-Ар Консалтинг» (CR Consulting) — также является сторонником системы Linux и открытых систем. В книге *«Методология перехода от Windows к Linux»* («Windows to Linux Migration Toolkit», Syngress Publishing, 2004, ISBN 1-931-83639-6. — *Примеч. ред.)* Дэвид описывает переход от патентованных технологий к открытым системам с существующей или улучшенной функциональностью. На основе собранной из множества источников информации о переходе от Windows к Linux описаны способы ухода от однообразия рутинного механического обновления с помощью поэтапных инструкций, самых совершенных методик и автоматизированных сценариев миграции от Windows к Linux. При наличии более 25 000 прецедентов такой миграции на пяти континентах трудно переоценить ценность знаний и опыта Дэвида Алена в области управления проектами, проектирования систем на базе Linux и планирования процесса перехода. Многие из предлагавшихся им методик применялись в таких компаниях, как JPMorgan Chase, Applied Materials и NASA.

Дэвид Ален писал, что ни предприниматели, ни потребители не хотят превращаться в заложников производителей. Предприниматели чаще всего предпочитают приобретать продукцию определенной группы конкурирующих между собой поставщиков, потому что конкуренция снижает риски: если что-то не устраивает, другие производители предлагают более выгодные цены, а в случае выхода из коммерческой обоймы постоянного поставщика всегда можно обратиться к другому. Все это отражается на самой продукции: если заказчики могут предпочесть один товар другому, то цены на товары снижаются, их качество повышается, в результате чего выигрывает потребитель.

В данной книге представлены простейшие пути перехода от Windows к Linux. Приступайте и — вперед!

Дрэйтон Баулз
Октябрь 2004 года

Глава 1

Порядок осуществления миграции сетевых служб

Разделы:

- Оценка существующей инфраструктуры
- Определение требований к инфраструктуре Linux
- Проектирование инфраструктуры Linux
- Тестирование инфраструктуры Linux
- Развертывание инфраструктуры Linux
- Переход к инфраструктуре Linux

☑ Резюме

☑ Краткое резюме по разделам

Введение

После ознакомления с материалом данной главы вы научитесь планировать сетевые службы и управлять ими в процессе перехода от Windows к Linux. Если вы являетесь системным администратором (сисадмином) и не интересуетесь ни планированием, ни управлением перехода, то можете смело пропустить эту главу, особенно если решение этих вопросов входит в обязанности других сотрудников. Для ИТ-менеджеров, руководителей проектов или консультантов по переходу с одной системы на другую данная глава будет чрезвычайно полезной. В ней представлены структура и сетевой график подготовки успешного проекта перехода от Windows к Linux, а также поэтапные инструкции для беспрепятственного его осуществления.

Управление проектом перехода представляет собой подраздел общего управления проектами. Подобно большинству проектов развертывания программных средств, проекты миграции включают в себя фазы оценки, определения требований, проектирования, тестирования и собственно развертывания. Данная глава посвящена управлению проектом на каждой фазе проекта, а также практическим методам, используемым при переходе от Windows к Linux.

Несмотря на то, что управленческая и плановая деятельность может потребовать значительных капиталовложений в проект, впоследствии они неизбежно окупятся плавным и беспроблемным переходом от одной системы к другой. Данный уровень планирования и управления особенно важен для крупных проектов. Несколько дополнительных часов подготовки на ранних этапах реализации проекта часто экономят дни работы на последующих этапах.

Оценка существующей инфраструктуры

Миграционные проекты подобны автомобильному путешествию. В обоих случаях имеется отправная точка, собственно путешествие и место назначения. Первым шагом планирования перехода является получение информации об отправной точке: составление письменной оценки существующей информационной среды организации. В оценке подробно описывается отправная точка, а также определяется масштаб миграционного проекта.

Как минимум оценка должна включать в себя все данные, относящиеся к целевым областям миграции. Так как оценка инфраструктуры, как правило, представляет собой значительный единовременный объем работ, то имеет смысл собрать как можно больше полезной информации о системах и сетевой инфраструктуре.

Повесть о двух предприятиях

Для более наглядной иллюстрации различных потребностей инфраструктуры компании при переходе от Windows к Linux в книге будут рассматриваться два принци-

пиально разных предприятия на пути их гипотетического перехода с одной системы на другую. В каждой главе будет прослеживаться миграционный процесс в компаниях Acme Widgets и Ballystyx Engineering на примере реальных сценариев, прибыли, трудностей и ориентировочных затрат, на которые может пойти администратор.

Краткие сведения о компании Acme Widgets

Полное название: Acme Widgets Manufacturing, Inc.

Местонахождение: Ноксвилл, штат Теннеси.

Опыт коммерческой деятельности: 5 лет.

Персонал: 6 человек.

Консультант процесса перехода: Сэм Астер.

В течение последних пяти лет компания Acme Widgets, занимающаяся специализированным приборостроением, переживает период подъема. По мере расширения штата сотрудников с трех до шести человек сервер Exchange, настроенный по умолчанию, и настольные рабочие станции с операционной системой Windows вполне удовлетворяли технические потребности фирмы.

Месяц назад компьютер оказался инфицирован вирусом и перестал загружаться. Поскольку вирус уничтожил всю информацию с жесткого диска, Сэм запросил у представителей Acme Widgets установочный носитель для повторной установки операционной системы. После непродолжительных поисков выяснилось отсутствие как установочных носителей, так и лицензий на все используемые программные средства: для установки программных продуктов стоимостью несколько тысяч долларов нанятый компьютерщик использовал пиратские регистрационные номера.

Для запуска настольной рабочей станции была приобретена лицензионная система Windows 2000 Desktop для легальной утановки Windows на пораженную вирусом машину. Поскольку финансовое положение компании не позволяло приобрести лицензионный Microsoft Office, на другие компьютеры Сэм установил OpenOffice.

После ознакомления с уведомлением об ответственности за использование пиратской продукции («Report Piracy») на веб-сайте Альянса производителей коммерческого программного обеспечения (Business Software Alliance, BSA) Сэм сделал вывод, что переход на систему Linux сэкономит компании Acme Widgets тысячи долларов. Сэм планировал осуществить перевод компьютеров с нелицензионным программным обеспечением на Linux с использованием приложений Mozilla, OpenOffice и Evolution. Для замены сервера Exchange он решил собрать новый сервер.

Краткие сведения о компании Ballystyx Engineering

Полное название: Ballystyx Global Semiconductor Engineering, Inc.

Местонахождение: Кремниевая Долина, США; Бангалор, Индия.

Опыт коммерческой деятельности: 10 лет.

Персонал: 76 человек.

ИТ-менеджер: Виджей Шринивасан.

Более десяти лет компания Ballystyx Engineering занималась созданием микросхем для расчета траекторий и баллистики. Дела шли ровно и стабильно.

В течение всех десяти лет компания страдала от становящейся все более насущной проблемы спама и вирусов, передаваемых по электронной почте. Ситуация стала настолько серьезной, что некоторые пользователи ежедневно тратили более двадцати минут на просмотр и удаление ненужной информации. В результате кое-кто из руководства среднего звена попросил ИТ-менеджера Виджея оценить затраты на установку в систему передачи и получения электронной почты средств защиты от спама и вирусов.

Поскольку для передачи сообщений в компании использовался Exchange, Виджей связался с поставщиками программных средств защиты от спама и вирусов продуктов, интегрированных с Exchange. Он выяснил, что установка указанных средств в Exchange обойдется в 7000 долларов, поэтому было принято решение о подготовке предложения по установке открытых программ-антивирусов и антиспама в Hydrogen, Linux-сервер компании. Хотя программы защиты немного снижают скорость работы сервера, они устраняют проблемы появления вирусов и спама без оплаты дорогостоящих лицензий.

Просматривая приобретенные лицензии на программные продукты при подготовке отчета руководству, Виджей обнаружил наличие лицензий на сервер Exchange и клиенты Outlook и отсутствие лицензий на клиентский доступ к Exchange (client access license, CAL). Проверка сервера Exchange показала лицензирование 999 пользователей — число в любом случае некорректное. Кто-то «подобрал» строку регистрации и избежал необходимости покупки лицензий клиентского доступа Exchange стоимостью 5000 долларов.

Помимо проблемы спама и вирусов возникла очень щекотливая дилемма: заплатить 5000 долларов или отказаться от использования Exchange. Теоретически открытые программные средства могли обеспечить необходимые компании Ballystyx Engineering функции, подобные функциям Exchange, причем не по ценам Exchange. Виджей знал об этих возможностях открытых программ, но не предполагал, что они могут заменить всю инфраструктуру Exchange и службы каталогов Active Directory. Ballystyx Engineering могла бы избавиться от инфраструктуры Windows Server, перенести все сетевые приложения и даже полностью перейти на операционную систему Linux.

Опись серверов

Первым шагом при выполнении оценки перехода является создание описи всех серверов (см. табл. 1.1 и 1.2). Минимальная опись должна включать в себя имя сервера, IP-адрес, сетевые приложения, версию операционной системы и некоторую информацию об аппаратных средствах.

Табл. 1.1. Опись сервера Acme Widgets (маленькая компания)

Имя	ОС	Программное обеспечение	Память	CPU	IP-адрес
SERVER 1	WinNT SP6a	PDC Работа с файлами/Печать Exchange	384 Мб	P3-866 МГц	192.168.100.2

Табл. 1.2. Опись сервера Ballystyx Engineering (средняя/крупная компания)

Имя	ОС	Программное обеспечение	Память	CPU	IP-адрес
HYDROGEN	Debian Unstable	Apache PostgreSQL (postgres)	2 Гб	2 x 1,4 ГГц	192.168.1.10
HELIUM	Win2K SP3	Бухгалтерия и финансы	2 Гб	1 x 1,4 ГГц	192.168.1.11
LITHIUM	Win2K SP3	AD, DNS, DHCP, работа с файлами/Печать	1 Гб	1 x 2 ГГц	192.168.1.12
BERYLLIUM	Win2K SP3	Exchange	2 Гб	1 x 2 ГГц	192.168.1.13

Собранная информация будет использована для планирования и реализации всех последующих этапов проекта, поэтому ее корректность имеет особое значение. Если на ранних этапах планирования ошибочные данные становятся частью проекта, то возникает «каскадный» эффект, поскольку из исходной ошибки генерируются ошибочные данные.

Помимо создания описи сервера может оказаться полезным создание описи рабочих станций, особенно если планируется миграция к рабочим станциям Linux. Опись рабочих станций во многих случаях может помочь в определении требований к серверу. Информация о создании описи рабочих станций представлена в главе 11.

Создание схемы инфраструктуры

Системная и сетевая схемы (см. рис. 1.1 и 1.2) существующей инфраструктуры наглядно демонстрируют отправную точку миграции. Для создания подобных схем можно использовать пакеты Visio и Dia (www.gnome.com/projects/dia).

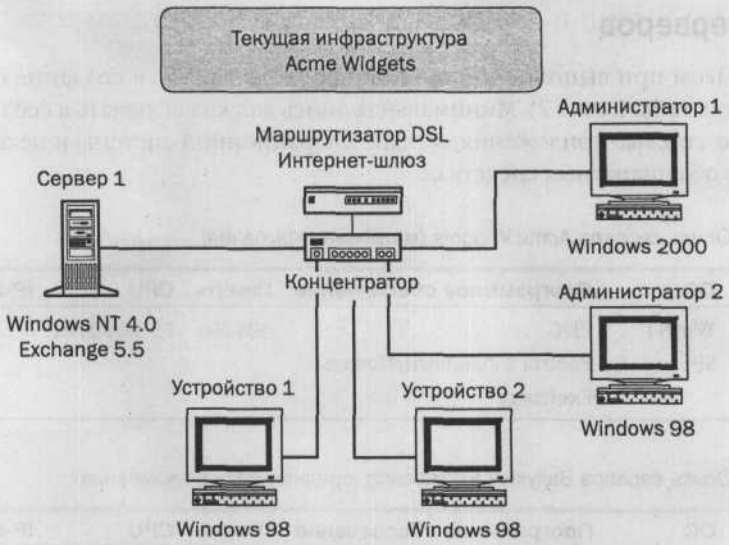

Рис. 1.1. Существующая схема инфраструктуры компании Acme Widgets

Рис. 1.2. Существующая схема инфраструктуры компании Ballystyx Engineering

Документирование дополнительной оценочной информации

При наличии времени и необходимости в подробной документации в оценку следует внести дополнительную информацию:

- инвентарный и/или серийный номер аппаратного средства;
- наименование производителя и модель аппаратного средства;
- общий объем жесткого диска и свободного пространства;
- наименование производителя сетевого оборудования, модель и конфигурация.

Определение требований к инфраструктуре Linux

После завершения оценки существующей инфраструктуры начинается следующий этап: определение требований к инфраструктуре Linux. Попытаемся обеспечить функциональность, по меньшей мере сходную с заменяемой инфраструктурой Windows. Во многих ситуациях Linux предлагает расширенные возможности, которые можно регулировать, особенно когда требования определяются на ранних этапах реализации проекта.

Вообще говоря, требования должны определяться производственной необходимостью. Может возникнуть соблазн превратить в «требование» некую функцию программного продукта только потому, что она поддерживается. Однако с развертыванием и последующей поддержкой дополнительных функций связаны дополнительные издержки. Поэтому имеет смысл подготовить списки того, что должно присутствовать «обязательно» и «желательно», либо просто определить приоритеты каждого требования. Если затраты (время, обучение, обслуживание) на то или иное требование минимальны, то его включение в проект может быть целесообразным, даже несмотря на его низкий приоритет.

Создание списка функциональных требований

В списке функциональных требований описывается функциональность, обеспечиваемая инфраструктурой для подтверждения собственной приемлемости. Впоследствии список функциональных требований используется для составления плана тестирования.

В табл. 1.3 представлен список функциональных требований для компании Acme Widgets. Структура этого документа по группам сетевых служб аналогична структуре глав данной книги, посвященных миграции сетевых служб. С помощью этого шаблона для создания собственного списка функциональных требований будет проще придерживаться описанной в книге методологии миграции сетевых служб.

Табл. 1.3. Список функциональных требований компании Acme Widgets

Службы	Требования
1. Основные сетевые службы	
1.1. Присвоение IP-адреса	Использование статических IP-адресов (не DHCP)
1.2. Разрешение имен	Использование разрешения имени узла через файл
1.3. Временная синхронизация	Установка программных средств временной синхронизации на все компьютеры
2. Службы каталогов	
2.1. Служба каталогов	Установка и конфигурирование OpenLDAP
2.2. Миграция служб каталогов	Перенос информации с Exchange и NT SAM на OpenLDAP
3. Службы аутентификации	
3.1. Службы аутентификации	Установка и конфигурирование служб аутентификации Samba
3.2. Миграция служб аутентификации	Пользователям необходимо сменить пароли
4. Файловые службы	
4.1. Файловые службы	Установка и конфигурирование файловых служб Samba
4.2. Миграция файловых служб	Копирование всех файлов данных на новый сервер и настройка возможности коллективного использования по сети
5. Службы печати	
5.1. Службы печати	Установка и конфигурирование CUPS
5.2. Миграция служб печати	Перенос очереди заданий на печать из Windows
6. Службы передачи сообщений	
6.1. Службы MTA (агент передачи сообщений)	Установка и конфигурирование Courier-MTA
6.2. Службы хранения (MAA) сообщений	Установка и конфигурирование Courier-IMAP
6.3. Службы передачи сообщений по Интернету	Требований нет
6.4. Антиспам	Предоставляется поставщиком услуг Интернета (ISP)
6.5. Антивирус	Предоставляется ISP
6.6. Миграция служб передачи сообщений	Перенос информации из хранилища сообщений
7. Службы автоматизации коллективного пользования и календарной регистрации	
7.1. Службы календарной регистрации	Установка и конфигурирование сервера календарной регистрации

▶▶

Табл. 1.3. *(окончание)*

Службы	Требования
7.2. Службы автоматизации коллективного пользования	Подлежат определению
7.3. Миграция службы календарной регистрации	Перенос информации календарного справочника
7.4. Миграция службы автоматизации коллективного пользования	Подлежат определению
8. Веб-службы	Требования отсутствуют

Выявление сдерживающих факторов

Помимо производственных и/или технических требований могут иметь место юридические, финансовые, временные, организационные и прочие сдерживающие факторы. Они могут обусловить изменение определенных требований, приоритетов или запланированной последовательности событий. В табл. 1.4 приведены примеры сдерживающих факторов и действий, необходимых для корректирования неожиданных ситуаций.

Табл. 1.4. Сдерживающие факторы миграции и их корректирование

Сдерживающий фактор	Пример	Решения
Финансовый	Не хватает средств на приобретение четырех новых серверов. На данный момент компания имеет свободные средства только на один	Вместо использования новых серверов в качестве серверов Linux будут использованы все существующие серверы Windows, кроме одного. Один сервер Windows используется как испытательный компьютер. Тогда потребуются три свободные настольные рабочие станции в качестве испытательных компьютеров
Юридический	Из соображений конфиденциальности электронные сообщения руководителей и рядовых сотрудников не должны храниться на одном физическом сервере	Необходимо приобрести дополнительный сервер
Временной	Из-за отпуска одного из сотрудников переход нельзя осуществлять с 2 по 16 февраля	Переход должен быть перенесен на следующую неделю после 16 февраля
Процедурный	Из-за корпоративного выставления счетов на конец месяца в последний день месяца нельзя ни перезагружать, ни создавать резервные копии расчетных систем	Создание резервных копий на серверах создания счетов должно быть приостановлено в последний день месяца. Любое обслуживание серверов создания счетов не должно планироваться на последний день месяца

Проектирование инфраструктуры Linux

После определения требований можно приступать к высокоуровневому проектированию инфраструктуры Linux, включающему определение общей структуры сервера и сети для постмиграционной инфраструктуры. При этом будут определены системы, подлежащие сохранению, замене, обновлению или добавлению.

На данном этапе перехода еще рано определять низкоуровневые детали новой инфраструктуры. Подробные руководства по проектированию каждого компонента сетевых служб представлены в следующих главах.

Создание проекта постмиграционной инфраструктуры

Проектирование новой инфраструктуры потребует определения количества серверов, их размещения и выполняющихся на каждом из них специализированных служб. Для небольших компаний обычно достаточно одного или двух серверов (см. рис. 1.3).

Рис. 1.3. Схема проекта постмиграционной инфраструктуры компании Acme Widgets

В крупных компаниях, имеющих головной офис и филиалы, серверы корпоративных баз данных, Intranet, почтовые и др. расположены в головном офисе, а в каждом филиале (со своими размерами/пропускной способностью/пользователями) имеется один сервер с файловыми службами и, возможно, со службами аутентификации,

каталогов и/или почтовой службой для работников филиала (см. рис. 1.4). Такая структура обеспечивает работоспособность филиала даже при выходе из строя WAN и/или Internet.

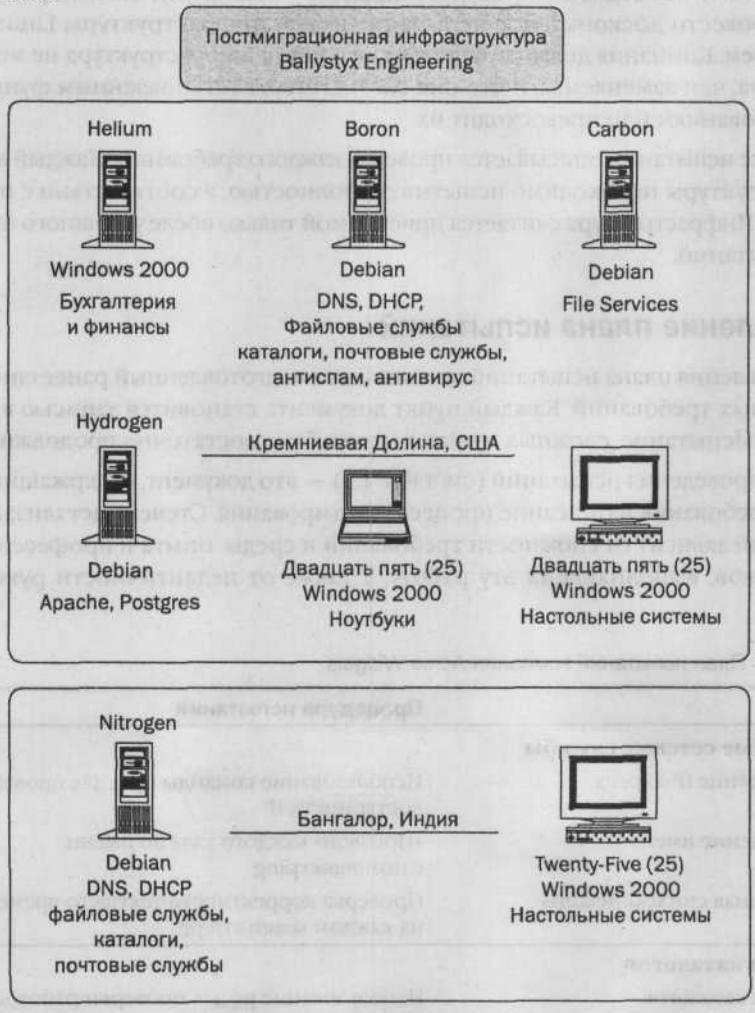

Рис. 1.4. Схема проекта постмиграционной инфраструктуры компании Ballystyx Engineering

Подробные проектные работы включают в себя документирование конфигурации сервера и приложений на основе спецификации требований. В главах, посвященных сетевым службам, представлены специальные руководства по конфигурации приложений сетевых служб в разных средах.

2 Зак. 1269

Тестирование инфраструктуры Linux

Подобно тому, как водитель проверяет новый грузовик перед важным рейсом, имеет смысл провести доскональное испытание новой инфраструктуры Linux перед ее внедрением. Компания должна убедиться, что новая инфраструктура не менее функциональна, чем заменяемая, и что она соответствует установленным функциональным требованиям или превосходит их.

В плане испытаний описывается проверка каждого требования. Каждый компонент инфраструктуры необходимо испытывать полностью, в соответствии с планом испытаний. Инфраструктура считается приемлемой только после успешного проведения всех испытаний.

Составление плана испытаний

Для составления плана испытаний используется подготовленный ранее список функциональных требований. Каждый пункт документа становится записью в плане испытаний. Испытание сложных пунктов может быть достаточно продолжительным.

План проведения испытаний (см. табл. 1.5) — это документ, содержащий испытываемые требования и описание процесса тестирования. Степень детализации плана испытаний зависит от сложности требований и среды, опыта и профессионализма сотрудников, выполняющих эту работу, а также от педантичности руководителя проекта.

Табл. 1.5. План испытаний компании Acme Widgets

Службы	Процедура испытаний
1. Основные сетевые службы	
1.1. Присвоение IP-адреса	Использование команды ping для проверки доступности IP
1.2. Разрешение имен	«Прозвон» каждого узла по имени с помощью ping
1.3. Временная синхронизация	Проверка корректности текущего времени на каждом компьютере
2. Службы каталогов	
2.1. Служба каталогов	Использование gq для проверки работоспособности запросов LDAP
2.2. Миграция служб каталогов	Использование gq для подтверждения корректного переноса записей с Exchange и NT SAM на OpenLDAP
3. Службы аутентификации	
3.1. Службы аутентификации	Подтверждение возможности регистрации пользователей на настольных системах Windows и Linux

▶▶

▶▶ **Табл. 1.5.** *(окончание)*

Службы	Процедура испытаний
3.2. Миграция служб аутентификации	Подтверждение смены пользователями паролей, заданных по умолчанию
4. Файловые службы	
4.1. Файловые службы	Использование smbmount для проверки работоспособности файловых служб
4.2. Миграция файловых служб	Подтверждение успешного копирования всех файлов
5. Службы печати	
5.1. Службы печати	Распечатка тестовой страницы
5.2. Миграция служб печати	Подтверждение корректности печати со всех компьютеров
6. Службы передачи сообщений	
6.1. Службы MTA (агент передачи сообщений)	Отправка тестового электронного сообщения в Интернет и внутренним пользователям
6.2. Службы хранения (MAA) сообщений	Использование Outlook и Evolution для подтверждения доступа к хранилищу сообщений
6.3. Службы передачи сообщений по Интернету	Требований нет
6.4. Антиспам	Предоставляется поставщиком услуг Интернет (ISP)
6.5. Антивирус	Предоставляется ISP
6.6. Миграция служб передачи сообщений	Подтверждение корректного переноса почтового ящика Exchange
7. Службы автоматизации коллективного пользования и календарной регистрации	
7.1. Службы календарной регистрации	Создание тестовой записи о встрече и совещании
7.2. Службы автоматизации коллективного пользования	Подлежат определению
7.3. Миграция службы календарной регистрации	Подтверждение корректного копирования записи о встрече и совещании
7.4. Миграция службы автоматизации коллективного пользования	Подлежат определению
8. Веб-службы	Требования отсутствуют

В Acme Widgets процедура проверки функциональности электронной почты заключается в отправке тестового сообщения в Интернет и внутренним пользователям. В данном случае достаточно короткого описания: отправить сообщение на электронный адрес и убедиться в его получении.

В крупных компаниях с более сложными средой и требованиями к службам процедура тестирования функциональности электронной почты может быть настолько длительной, что потребует наличия отдельного документа. Процедура тестирования электронной почты в плане испытаний Ballystyx Engineering гласит: «Убедитесь, что электронное сообщение размером 4 Кб, отправленное с рабочей станции в Кремниевой долине, поступило на почтовый сервер в Бангалоре менее чем за пять минут».

Настоятельно рекомендуется пользоваться испытательной лабораторией. Она обеспечивает сетевую среду, отделенную или изолированную от рабочей сети. Испытания изменений конфигурации аппаратных и программных средств должны проводиться в лаборатории до испытаний в рабочей сети или до развертывания пользователям.

Развертывание инфраструктуры Linux

После успешных лабораторных испытаний инфраструктуру Linux можно развернуть в рабочей сети для дополнительных испытаний выборочной (испытательской) группой пользователей. Лучше всего обеспечить каждого пользователя-испытателя инструкцией и бланком обратной связи, а затем с каждым полученные замечания. Как правило, на первых порах в испытательские группы входит ИТ-персонал и сотрудники, разбирающиеся в технических вопросах, затем постепенно вводятся основные пользователи. Для выявления всех вопросов и решения их до начала процесса перехода в испытательскую группу должны входить представители всех групп пользователей.

Переход к инфраструктуре Linux

Убедившись, что новая инфраструктура Linux работает в производственной среде так, как предполагалось, можно начинать перевод в новую инфраструктуру пользователей и систем. Как правило, ИТ-персонал и испытательская группа — первые, кто переходит на новую инфраструктуру. Существует несколько факторов, определяющих очередность перехода других пользователей:

- потребность в новых функциях, предлагаемых Linux (зависит от возможностей);
- производственная единица или подразделение (зависит от производственной группы);
- местоположение офиса (зависит от географических особенностей).

Существует несколько способов управления планом перехода. Важность (и сложность) управления планом перехода повышается с увеличением размеров и количества рабочих групп, переводимых на новую инфраструктуру. При реализации крупных миграционных проектов полезно назначить сотрудника, ответственного за взаимодействие между ИТ-персоналом и группой или филиалом. Он может помогать определять пользователей, готовых к переходу, а также даты и сроки перехода. Идеальным вариантом будет назначение контактных лиц рабочих групп ответственными за составление

списков пользователей для перехода, чтобы группа ИТ-персонала могла сосредоточиться на фактическом процессе перехода и обслуживании новых пользователей. Процесс перехода будет успешным при оперативном взаимодействии рабочих групп с ИТ-персоналом, а также при четком распределении обязанностей каждой группы.

Миграции некоторых служб, например службы аутентификации, могут быть прозрачными для конечного пользователя либо стать прозрачными после выхода из системы и перезагрузки. Конечные пользователи должны быть проинформированы о сделанных изменениях; с их стороны может не требоваться никаких действий. В других случаях переходы могут оказывать более ощутимое воздействие, например при переносе домашних каталогов на новый сервер с новым именем или при переходе на использование новой программы почтовых сообщений или веб-браузер. Подобные изменения необходимо тщательно планировать, и сообщения о них должны быть доведены до каждого сотрудника. В случаях, когда предполагается переход с одной системы на другую большого количества пользователей, целесообразна автоматизация максимального количества задач. Автоматизация миграционных процессов помогает свести к минимуму требования к работе технического персонала и риск субъективных ошибок.

Не следует забывать о планировании обучения. Если разворачиваются новые приложения или изменяются существующие процессы, то знания о них необходимо передавать заинтересованным сотрудникам вместе с обновленной документацией и сеансами обучения. Переход будет плавным, и люди не будут бояться, зная, что их потребности учитываются в полной мере.

Наконец, во всех случаях планирования процесса перехода следует придерживаться соответствующих процедур. Требуйте подробного документирования всех предложенных изменений. Планируйте регулярные совещания между ответственными лицами и техническим персоналом для обсуждения предлагаемых изменений и их понимания до фактического внедрения.

Резюме

Планирование и управление представляют собой важные аспекты успешного перехода от Windows к Linux. В крупных проектах эти аспекты являются критическими. Первоначальные вложения в планирование помогают обеспечить плавность процесса миграции. На первый взгляд работы очень много, однако прилагаемые шаблоны позволят выполнить ее быстро и легко.

Предполагается, что после ознакомления с материалом данной главы читатель получит представление об этапах планирования и управления, необходимых при переходе от Windows к сетевым службам Linux. В результате последовательного выполнения всех инструкций будет получена законченная оценка, опись сервера, список функциональных требований, высокоуровневый проект инфраструктуры Linux и план проведения испытаний. Итак, вы на пути успешного перехода от Windows к сетевым службам Linux!

Краткое резюме по разделам

Оценка существующей инфраструктуры

- ☑ Опись серверов с помощью прилагаемых шаблонов.
- ☑ Создание схемы существующей инфраструктуры.
- ☑ Документирование дополнительной информации для оценки (по необходимости).

Определение требований к инфраструктуре Linux

- ☑ Создание списка функциональных требований с помощью прилагаемых шаблонов.
- ☑ Выявление сдерживающих факторов. Часто в бюджетах проектов или планах сдерживающие факторы принимают форму ограничений.

Проектирование инфраструктуры Linux

- ☑ Создание схемы постмиграционной инфраструктуры. В схеме должно быть указано количество серверов, их расположение, а также перечислены выполняющиеся на каждом из них сетевые службы.
- ☑ Подробная проектная работа проводится на более поздних этапах переходного процесса.

Испытание инфраструктуры Linux

- ☑ Испытания новой инфраструктуры необходимо проводить до ее развертывания.
- ☑ Создание плана проведения испытаний.

Развертывание инфраструктуры Linux

- ☑ После успешных лабораторных испытаний осуществляется развертывание инфраструктуры Linux в рабочей сети для дополнительного тестирования.
- ☑ Предоставление выбранной группе пользователей (испытательской группе) возможности испытания инфраструктуры Linux на предмет ее работоспособности с точки зрения конечного пользователя.

Переход к инфраструктуре Linux

- ☑ После приемки инфраструктуры Linux испытательской группой можно начать перевод на новую инфраструктуру других пользователей и систем.
- ☑ План перехода лучше всего оправдывает себя при четком определении обязанностей производственными единицами и ИТ-персоналом до начала планирования или реализации детального перехода.

Глава 2

Основные сетевые службы TCP/IP

Разделы:

- Принципы работы служб присвоения IP-адресов
- Принципы работы служб разрешения имен
- Принципы работы служб временной синхронизации
- Перенос MS-DNS/DHCP на BIND/DHCPD Linux

☑ Резюме

☑ Краткое резюме по разделам

☑ Часто задаваемые вопросы

Введение

Адресация протокола сети Интернет (Internet Protocol, IP) формирует основу практически всех современных информационных сетей, включая Интернет. Авторы предполагают, что читателям известны следующие понятия, связанные с фундаментальным транспортным протоколом TCP/IP:

- IP-адреса и подсети;
- трансляция и маршрутизация IP-пакетов;
- сокеты TCP/UDP и синтаксис;
- инструментальные средства устранения сетевых неисправностей: ping, traceroute, nmap, telnet и tcpdump;
- серверы DNS, структурные типы и инструменты запроса, такие как nslookup и dig.

При необходимости, можно найти в Интернете пособия для начинающих о Службе доменных имен (DNS) и/или о TCP/IP либо обратиться к базовому учебнику по TCP/IP; подробным руководством по Службам доменных имен на базе Linux является книга О'Рейлли (O'Reilly) «DNS и BIND»[1].

В настоящей главе описываются некоторые базовые сетевые службы, используемые практически везде, где присутствуют сети TCP/IP. DNS, DHCP (протокол динамического управления хостом) и службы синхронизации времени — это, как правило, основные сетевые службы, потому что именно они формулируют основополагающие требования, необходимые для работы с другими упоминающимися в книге сетевыми службами. На сегодняшний день некоторые из этих основополагающих служб могут обеспечиваться различными специализированными или встроенными устройствами, однако в данной книге особо рассматриваются службы DHCP/DNS на базе Linux. Рассмотрение временных служб включает в себя корректную настройку многих свободно доступных временных серверов в Интернете.

DHCP, DNS и временные службы кратко описаны ниже. В оставшейся части главы в общих чертах рассказывается о работе этих служб на платформах Microsoft и Linux и объясняются принципы перехода от служб DNS/DHCP Microsoft к службам BIND/DHCPD на базе Linux.

DHCP — это сетевой протокол динамического присвоения IP-адресов и параметров сетевой конфигурации корректно сконфигурированным хостам. В то время как в большинстве серверов используются статические IP-адреса, рабочие станции получают динамически выделяемые IP-адреса, помимо прочей информации, обеспечивающей взаимодействие с другими хостами сети. Для присвоения динамической сетевой информации практически во всех компаниях используются серверы DHCP. В данной главе будет рассмотрен процесс получения права аренды первичного DHCP, а также процесс обновления аренды.

[1] «DNS and BIND», Paul Albitz, Cricket Liu; O'Railly, 2001, ISBN 0-596-00158-4.

Службы разрешения имен — еще одна важная часть инфраструктуры компьютерной сети. Способность перевода имен хостов с легко запоминающихся английских слов в IP-адреса создает основное удобство и простоту использования, являющиеся фундаментом компьютерных сетей любых размеров и типов, от мелких LAN (локальных сетей) до глобальной Интернет. При отсутствии служб разрешения имен IP-адреса было бы чрезвычайно сложно запоминать. DNS предоставляет эти возможности системам Windows и Linux. Для упрощения процесса перевода этих служб на платформу Linux в данной главе будут рассмотрены конфигурации DNS как для Windows, так и для Linux.

Другой основной сетевой службой, рассматриваемой в главе, является функция синхронизации часов на всех компьютерах сети. Некоторые части компьютерной сети могут корректно работать без синхронизации часов, но определенные сетевые службы требуют их синхронизации до разницы в несколько минут. Кроме этого, анализ и сопоставление событий при изучении системных журналов компьютеров с не синхронизированными часами может оказаться крайне сложной задачей. Обязательная синхронизация всех компьютерных часов является одной из первых рекомендаций технических служб ФБР для упрощения проверки данных во время судебных разбирательств.

Принципы работы служб присвоения IP-адресов

В сети Интернет и в корпоративных средах большинство серверов имеет статические IP-адреса. Конфигурация статических IP-адресов отличается от динамических по следующим фундаментальным признакам (см. табл. 2.1):

Табл. 2.1. Различия конфигураций статического и динамического IP

Статическое присвоение IP-адреса	Динамическое присвоение IP-адресов
Информация IP-адреса меняется редко	Информация IP-адреса может изменяться
IP-адрес меняется после переноса или технического обслуживания	При изменении физического местоположения изменяется информация об IP-адресе
Информация об IP-адресе сохраняется локально	Информация об IP-адресе кэшируется локально, а сохраняется внешне
Не требует внешнего сервера	Информация об IP-адресе присваивается сервером DHCP

В большинстве ноутбуков и настольных рабочих станций статические IP-адреса не используются. Вместо этого IP-адрес «арендуется» у сервера DHCP. После перезагрузки или по истечении срока аренды рабочая станция связывается с сервером DHCP для обновления аренды или получения нового IP-адреса. Основным преимуществом такой настройки является отсутствие необходимости настройки сетевой конфигурации для каждого клиента, и любые изменения в сети, которые могут произойти в будущем, будут распространяться на клиентов при обновлении ими права пользования сетью, как описано ниже.

Понятие «клиент DHCP»

Клиент DHCP — это любое сетевое устройство: компьютер, принтер или подключенная через сеть гитара, использующее DHCP для получения информации об IP-адресе. При запуске сетевого интерфейса клиента DHCP это устройство попытается воспользоваться IP-адресом. Процедура получения нового IP-адреса состоит из четырех этапов; ее еще часто называют четырехходовым квитированием.

Получение первоначального права аренды DHCP

Когда компьютер подключается к сети, не известно никакой информации о серверах DHCP. Поэтому для нахождения сервера DHCP компьютер должен направить широковещательный запрос.

Обнаружение сервера(ов) DHCP

Для инициирования процесса аренды DHCP клиент отправляет пакет DHCP-DISCOVER в широковещательном режиме с порта UDP (User Datagram Protocol) 68 на порт UDP 67. Этот пакет имеет исходный адрес 0.0.0.0 и адрес назначения 255.255.255.255 (рис. 2.1).

Рис. 2.1. Обнаружение сервера(ов) DHCP

Получение предложения(й) об аренде DHCP

Сервер DHCP, ожидающий на локальной подсети, отвечает на широковещательный запрос DHCP-DISCOVER. В крупных сетях коммутатор switch, маршрутизатор или другой ретранслятор DHCP может отправлять пакеты DHCP. Если запрос действителен и IP-адрес доступен, то сервер DHCP ответит пакетом DHCP-OFFER. В это предложение входит IP-адрес клиента, маска подсети и маршрутизатор по умолчанию (рис. 2.2).

Рис. 2.2. Получение предложения(й) об аренде DHCP

Выбор и принятие предложения об аренде DHCP

При нормальной работе служб DHCP клиент получит минимум одно предложение DHCP (DHCP-OFFER). Клиент выбирает предложение об аренде (обычно первое полученное) и отправляет пакет DHCP-REQUEST на сервер DHCP. Несмотря на то, что клиент знает IP-адрес сервера DHCP, этот пакет отправляется в широковещательном режиме, поэтому другие серверы DHCP «знают» выбранное предложение DHCP-OFFER (рис. 2.3).

Рис. 2.3. Прием аренды DHCP

Получение подтверждения присвоения аренды DHCP

После получения пакета DHCP-REQUEST сервер DHCP отправляет пакет DHCP-ACK, подтверждающий присвоение аренды DHCP. Этот пакет отправляется в широковещательном режиме, поэтому другие серверы DHCP «знают» подтвержденный пакет DHCP-REQUEST (рис. 2.4).

Рис. 2.4. Получение подтверждения присвоения аренды DHCP

После получения пакета DHCP-ACK клиент официально вводится в сеть с действующим IP-адресом, подсетью и маршрутизатором, заданным по умолчанию. Все последующие DHCP-коммуникации (через тот же сервер DHCP) будут осуществляться через пакеты однонаправленной (unicast) передачи.

При возникновении проблем с пакетом DHCP-REQUEST, полученным от клиента, сервер отправит пакет DHCP-NACK и дождется повторного подключения клиента.

Обновление права аренды DHCP

По истечении от 50 до 90% срока аренды клиент DHCP будет предпринимать попытки к обновлению срока пользования услугой. Процедура обновления сходна с двумя последними шагами процесса четырехходовой квитизации первоначальной аренды DHCP.

Запрос обновления аренды DHCP

До истечения срока аренды клиент отправляет пакет DHCP-REQUEST на сервер DHCP. В этом пакете содержатся текущие настройки IP-адреса клиента (рис. 2.5).

Рис. 2.5. Запрос обновления аренды DHCP

Получение подтверждения обновления аренды DHCP

После получения пакета обновления DHCP-REQUEST сервер DHCP отправляет пакет DHCP-ACK, подтверждающий обновление права аренды DHCP. При возникновении проблем с получением от клиента пакета DHCP-REQUEST сервер отправит пакет DHCP-NACK (рис. 2.6).

Рис. 2.6. Получение подтверждения обновления аренды DHCP

Снятие права аренды DHCP

Последний шаг процесса соединения с DHCP — снятие права аренды DHCP. Во время последовательности выключения сетевого интерфейса клиента DHCP отправляет пакет DHCP-RELEASE на сервер DHCP, который, в свою очередь, приостанавливает право аренды DHCP и возвращает IP-адрес клиента в пул доступных IP-адресов.

Примеры и упражнения

Сбор и анализ трафика DHCP

При глубоком анализе темы без сбора реальных данных обойтись невозможно. Самым простым способом сбора трафика DHCP является запуск **tcpdump** на сервере DHCP. Для сбора пакетов DHCP на eth0 и их записи в file/dhcp-sniff введите следующее:

```
tcpdump -I eth0 -w /dhcp-sniff udp port 67 or udp port 68
```

По завершении сбора пакетов остановите tcpdump нажатием клавиш **Ctrl + C**. После этого запустите ethereal со следующей командой:

```
ethereal /dhcp-sniff
```

При этом данные DHCP будут просматриваться и анализироваться графически. Более подробную информацию о Ethereal см. в Ethereal Packet Sniffing (Syngress).

Конфигурирование серверов DHCP

Теперь, когда становится понятно, как клиент DHCP связывается с сервером DHCP, обратим внимание на конфигурацию сервера. Для демонстрации работы сервера DHCP воспользуемся DHCPD www.isc.org/sw/dhcp/ от Internet System Consortium (ISC). DHCPD — это самый популярный в мире открытый сервер DHCP, который и будет использоваться в Linux.

DHCPD сохраняет информацию о конфигурации в **dhcpd.conf**. Ниже перечислено большинство постмиграционных файлов dhcpd.conf для серверов Ballystyx Engineering в Кремниевой Долине и в Индии. Запись **ddns-update-style** рассматривается далее. Этой информацией можно пользоваться в качестве шаблона при конфигурировании сервера DHCP. Все значения времени выражены в секундах.

```
ddns-update-style ad-hoc;

# Ballystyx Silicon Valley
subnet 192.168.1.0 netmask 255.255.255.0 {
      range 192.168.1.130 192.168.1.250;
      default-lease-time 43200;
      max-lease-time 86400;

      option routers 192.168.1.1;
      option subnet-mask 255.255.255.0;
      option broadcast-address 192.168.1.255;

      option domain-name "ballystyx.com";
      option domain-name-servers 192.168.1.12, 192.168.2.10;
}

# Ballystyx India
subnet 192.168.2.0 netmask 255.255.255.0 {
      range 192.168.2.130 192.168.2.250;
      default-lease-time 43200;
      max-lease-time 86400;

      option routers 192.168.2.1;
      option subnet-mask 255.255.255.0;
      option broadcast-address 192.168.2.255;

      option domain-name "ballystyx.com";
      option domain-name-servers 192.168.2.10, 192.168.1.12;
}
```

Обратите внимание, что в Ballystyx Engineering используются два сервера DNS — 192.168.1.12 и 192.168.2.10. В Кремниевой Долине первичный сервер DNS —

192.168.1.12, а вторичный — 192.168.2.10. В Индии ситуация обратная. Этим обеспечивается, что каждый клиент DHCP сначала будет пытаться наладить контакт с локальным сервером DNS.

Замечание о безопасности

Что такое сервер Rogue DHCP?

Хотя из-за своей простоты DHCP кажется безобидным сервером, он обладает потенциальным недостатком в плане информационной безопасности. Что произойдет, если компьютерные злоумышленники попытаются внедрить в сеть сервер DHCP с дефектами с целью передачи недостоверной информации клиентам DHCP? Информация подобного рода может включать в себя следующее.

- **Недействительные IP-адреса**, например уже используемые где-либо. В этом случае возникнут конфликты адресов со всеми вытекающими сбоями сетевой работы и прочими проблемами.
- **Недействительную информацию маршрутизации**, например IP-адрес дефектного маршрутизатора или службы маршрутизации, выполняющийся на компьютере, контролируемом хакером.
- **Недействительную информацию DNS**, например дефектные или фиктивные серверы DNS. При этом клиент потеряет способность разрешать доменные имена либо фиктивный сервер будет рассматриваться как заслуживающий доверия узел.

Как видно, фиктивный сервер DHCP может спровоцировать большое количество сетевых сбоев, потому что очень многое зависит от корректной сортировки IP-адресов и прав аренды. К счастью, существуют способы защиты от проблем фиктивных серверов DHCP и/или их предотвращения.

- **Сетевое зондирование.** Отправьте различные типы пакетов DHCP для определения местоположения серверов DHCP в сети. Если отвечающий сервер DHCP не соответствует перечисленным в списке известных IP-адресов (или другому выбранному способу управления доступом), то следует предупредить об этом администратора и/или избегать использования такого сервера.
- **Использование систем обнаружения атак (вторжений).** Сконфигурируйте систему обнаружения атак для регистрации пакетов UDP на портах 67/68 и предупреждения о подозрительном трафике.
- **Конфигурирование маршрутизатора и коммутатора**. Ограничьте пропускание UDP-пакетов портами 67/68 на маршрутизаторах и коммутаторах.

Следует помнить о том, что работа служб DHCP может прерываться на короткое время в процессе работы сети, особенно если никакие из компьютеров не перемещались и срок аренды достаточно продолжителен. Однако лучше использовать процесс мониторинга, а не обращаться к администратору при каждом сбое в работе служб DHCP.

Принципы работы служб разрешения имен

Как уже упоминалось в настоящей главе, возможность преобразования имен хостов из легко запоминаемых английских слов в IP-адреса представляет собой основополагающее удобство работы с компьютерными сетями всех размеров и типов. Действительно, легче ввести (и запомнить) адрес www.google.com, а не комбинацию чисел 216.239.39.99.

Службы разрешения имен во всем их разнообразии существуют столько же, сколько сам Интернет. Изначально все имена хостов Интернет сохранялись в одном текстовом файле на одном сервере. По всей видимости, такой способ не слишком хорошо масштабируется, поскольку с течением времени требовалась все большая пропускная способность и вычислительная мощность для обработки постоянных запросов на скачивание этого текстового файла. На сегодняшний день существуют два основных способа управления службами преобразования имен хостов в IP: на основе файла и на основе DNS. В следующих разделах обе методологии будут рассматриваться более подробно.

Процесс разрешения имен на основе файла

Наиболее простым способом разрешения имен является сохранение всех имен и соответствующих IP-адресов в локальном файле. В большинстве случаев данный файл имеет имя hosts. Ниже приведено содержание файла имен хостов компании Acme Widgets:

```
127.0.0.1        localhost    localhost.localdomain
192.168.100.1    router1      router1.acmewidgets.com
192.168.100.2    server1      server1.acmewidgets.com
192.168.100.3    admin1       admin1.acmewidgets.com
192.168.100.4    admin2       admin2.acmewidgets.com
192.168.100.5    widget1      widget1.acmewidgets.com
192.168.100.6    widget2      widget2.acmewidgets.com
192.168.100.7    printer1     printer1.acmewidgets.com
192.168.100.8    printer 2    printer2.acmewidgets.com
```

Как видно, здесь представлены все основные возможности поиска имен для небольшой LAN (локальная сеть). Однако данный метод не обеспечивает никакой другой функциональности, например динамической регистрации имени или определения срока окончания регистрации.

Как правило, в Windows и Linux используется файл хостов. В табл. 2.2 представлено стандартное местоположение этого файла в различных операционных системах.

Табл. 2.2. Местоположения файла хостов в разных типах операционных систем

Различные версии Linux	/etc/hosts
Windows 95 / 98 / Me	C:\Windows\hosts
Windows NT / 2000 / XP	C:\Winnt\system32\drivers\etc\hosts

Иногда установочный каталог Windows имеет имя WINNT. В других случаях каталог называется WINDOWS или имеет другое имя, выбираемое пользователем.

Процесс разрешения имен на основе DNS

Хотя метод разрешения имен на основе файла удовлетворяет основным требованиями, он чересчур ограничен и подходит только для небольших сетей со статическими IP-адресами. Он не обеспечивает доступности, расширяемости или возможностей динамически распределенной системы, например DNS. DNS — это основной способ преобразования имен в IP-адреса для ОС Windows (2000 и более поздних версий) и Linux, а также является признанным механизмом разрешения имен для Интернета.

Одной из причин хорошей расширяемости DNS является возможность разбиения разрешения имен по доменам (например, syngress.com), а службы расширения имен для каждого домена можно разбить по нескольким серверам для обеспечения резервирования и общей доступности. Проблемы DNS одного домена, как правило, не влияют на другие домены. Если сервер не знает ответа на запрос DNS, то он автоматически будет отсылать клиента к серверу DNS, являющемуся уполномоченным для данного домена.

Существует 13 серверов DNS высшего уровня (называемых *корневыми серверами*), поддерживаемых различными организациями по всему миру. Приблизительно половина из них физически размещена в США. Более подробную информацию об этих корневых серверах можно найти на сайте www.root-servers.org.

Помимо служб преобразования имен в IP, DNS может осуществлять и обратные процедуры. Данная функция обратного поиска управляется через домен in-addr.arpa и записи PTR (указатель). Чтобы узнать имя хоста с IP-адресом 192.168.1.12, клиент DNS выполняет PTR-поиск по записи 12.1.168.192.in-addr.arpa. Уполномоченный для данной подсети сервер DNS вернет имя, ассоциированное с этим IP-адресом. Обратный поиск часто используется для верификации имени сервера, в частности, в случае передачи сообщений по электронной почте. Все хосты, доступ к которым осуществляется через Интернет, должны иметь запись PTR для успешного обратного поиска. Для внутренних серверов DNS также настоятельно рекомендуется иметь зоны обратного поиска in-addr.arpa.

Понятие динамического DNS (DDNS)

На заре появления DNS записи управлялись вручную — редактированием текстового файла, называемого *файлом данных зоны* (zone file), содержащего имена, IP-адреса и типы записей. В то время IP-адреса компьютеров менялись редко и периодического добавления/изменения имени и IP-информации, а также обновления регистрационного номера было вполне достаточно.

С появлением динамически присваиваемых IP-адресов редактирование файлов зоны DNS вручную превратилось в нерешаемую задачу для вечно занятых сисадминов, поэтому требовался некий способ динамической регистрации компьютерных имен. Это является основой RFC 2136 и *динамического DNS* (DDNS). Далее в книге будем говорить о DNS, подразумевая под этим и динамические DNS.

В среде DDNS клиенты (или серверы DHCP) регистрируют имена и IP-адреса с уполномоченным для конкретного домена именем сервера, как это определено в записи SOA (Start of Authority — начало полномочий). Клиенты также регистрируют запись PTR в домене in-addr.arpa сервера, являющегося SOA для их подсети.

Конфигурирование BIND и DHCP для динамического DNS

В конфигурации по умолчанию клиенты Windows 2000 и Windows XP автоматически регистрируются с помощью динамического DNS после получения IP-адреса. Следующая запись в dhcpd.conf позволяет корректно это осуществить:

```
ddns-update-style ad-hoc;
```

Если в сети есть клиенты Windows 98 и NT, то они не будут автоматически регистрироваться с помощью динамического DNS. Вместо этого сервер DHCP можно сконфигурировать для регистрации имени их хоста и записи PTR/TXT для их IP-адреса:

```
ddns-update-style interim;
```

Такой способ обновления информации DDNS немного отличается от (ратифицируемых в настоящее время) стандартов RFC, но он эффективен для работы с клиентами нижнего уровня. Для получения дополнительной информации о dchpd введите **man dhcpd.conf** в приглашении оболочки.

Для конфигурирования BIND с целью получения обновлений динамических DNS-записей убедитесь, что в named.conf имеется следующая строка:

```
allow-update;
```

ПРИМЕЧАНИЕ Существует Служба имен Интернет для Windows (WINS), которая используется в сетях Microsoft, особенно в сетях NT и Windows 3.x/95/98. За пределами сетей Microsoft WINS используется редко, даже Microsoft предпочитает DNS.

В случае абсолютной необходимости использования постмиграционного сервера WINS уместен продукт Samba с предлагаемыми им функциями (описывается ниже). Впрочем, практически в любых обстоятельствах DNS предпочтительнее, и именно он используется во всех современных операционных системах.

Принципы работы служб временной синхронизации

Важность временно́й синхронизации переоценить сложно. Точные установки времени часов клиентов и серверов являются критичными. Если разница во времени (*расфазировка*) превышает пять минут, то некоторые службы (например, Kerberos) работать не будут вообще. Другие функции могут работать некорректно, например почтовый сервер будет указывать, что электронное сообщение получено за 10 минут до времени фактического отправления. Кроме этого, при некорректной установке часов затрудняется устранение неисправностей в компьютерах и сетях. Это особенно важно при попытках временно́го соотнесения регистрационных записей на большом количестве компьютеров.

Для выполнения временно́й синхронизации существует много способов и протоколов, однако наиболее популярным и проверенным является синхронизирующий сетевой протокол (NTP-протокол).

Понятие о синхронизирующем сетевом протоколе

В современных операционных системах для выполнения временной синхронизации выбирается протокол NTP. NTPv3 определен в RFC (Request For Comments, Запросы на комментарии) 1305. NTPv4 еще не имеет официального статуса IETF RFC, но включен в существующую версию пакета NTP. Подмножество NTP, называемое Simple NTP (SNTP), определенное в RFC 2030, может применяться, если время отклика между сервером и клиентом минимально, что типично для корпоративных локальных сетей (LAN). По умолчанию в компьютерах с системами Windows 2000/XP для синхронизации времени с серверами Windows используется SNTP.

Функциональность NTP основана на понятии главных серверов времени (называемых серверами *первого эшелона*), получающих сведения о точном времени из высокоточных источников, например от локально подключенной Глобальной системы рекогносцировки (GPS) или снимающих их с цезиевых часов. Сервер, синхронизирующийся с сервером первого эшелона, называется сервером второго эшелона — эшелона исходного сервера + 1. По мере увеличения номера слоя точность времени может слегка снижаться.

Принципиальными проблемами синхронизации времени являются учет сетевого ожидания и времени обработки пакетов и серверы с неточной установкой времени. Например, если сервер времени отправляет пакет «Точное время — 12:00:00, устано-

вите часы на 12:00:00», а пакету требуется 2 секунды на достижение места назначения, то часы на клиентском компьютере будут отставать на 2 секунды. Если на обработку пакета клиенту требуется еще 1 секунда, тогда клиентский компьютер будет отставать на 3 секунды.

NTP преодолевает эти проблемы несколькими способами:

- измерением времени ожидания с помощью временных меток клиента и сервера;
- учетом времени, необходимого на обработку сетевых пакетов;
- использованием кратных выборок с множественных серверов для обеспечения точности;
- составлением «черных списков» серверов, выдающих непоследовательные или неточные результаты.

NTP использует порт 123 UDP. Более подробную информацию о NTP см. на www.ntp.org.

Понятие о клиентах NTP для Linux

Самым популярным клиентом NTP для Linux является реализация ntp.org, которая создает полный пакет клиент-сервер, поддерживающий NTPv3 и NTPv4. В пакет входит следующее:

- **ntpq** для запроса серверов NTP;
- **ntpd** поддерживает точность локальных часов и (опционально) обеспечивает клиентам службу NTP;
- **ntptrace** прослеживает цепь сервера NTP к исходному серверу;
- **ntpdate** — одноразовая программа обновления часов (в ближайшем будущем устареет).

Ntpd (демон NTP) может выполняться как NTP-клиент и/или сервер. При конфигурировании одного или нескольких серверов Linux в качестве серверов NTP службы временной синхронизации можно предоставить внутренней инфраструктуре. Однако эта идея не всегда так хороша, как кажется на первый взгляд. Если хакер или неопытный сисадмин изменяет настройки часов серверов времени, то при отсутствии точных данных времени это изменение может распространиться на все компьютеры, синхронизирующиеся с серверами времени.

Лучшим вариантом является запуск службы ntpd на всех компьютерах Linux и настройка их синхронизации со списком серверов второго и/или третьего эшелона в Интернете. Хотя для синхронизации времени можно использовать серверы первого эшелона, это считается сетевым моветоном, если только вы не предоставляете свой сервер второго эшелона другим пользователям Интернета.

Файл ntpd.conf управляет настройками конфигурации ntpd. Обычно достаточно файла конфигурации по умолчанию. Если предпочтительно использование набора серверов NTP, перечисленных на pool.ntp.org, введите следующую строку в ntpd.conf:

```
server pool.ntp.org
```

Более подробную информацию об ntpd и ntpd.conf можно получить, введя man ntpd. Подробная информация о пуле сервера времени ntp.org доступна на сайте www.pool.ntp.org.

Понятие клиентов служб времени Windows

Windows 2000 и Windows XP поставляются с клиентом SNTP Microsoft — Службой Времени Windows. Последняя активизируется автоматически, когда компьютеры присоединяются к домену. Для компьютеров Windows, не являющихся членами домена, служба должна запускаться вручную.

В Windows 2000 и Windows XP часы можно синхронизировать сервером времени pool.ntp.org с помощью следующей команды:

```
net time /setsntp:pool.ntp.org
```

Во многих случаях Windows выдает сообщение: «Команда успешно завершена», хотя время не установлено. Кроме этого, данная команда не срабатывает в Windows 98 и NT.

Лучшим выбором для синхронизации времени в Windows является Automachron. Automachron — это бесплатное программное обеспечение (freeware) (www.oneguycoding.com/automachron/). В отличие от службы времени Windows, Automachron работает со всеми версиями 32-битовой системы Windows и имеет простой в управлении пользовательский графический интерфейс (GUI) для настройки конфигурации. Диалоговое окно Automachron показано на рис. 2.7.

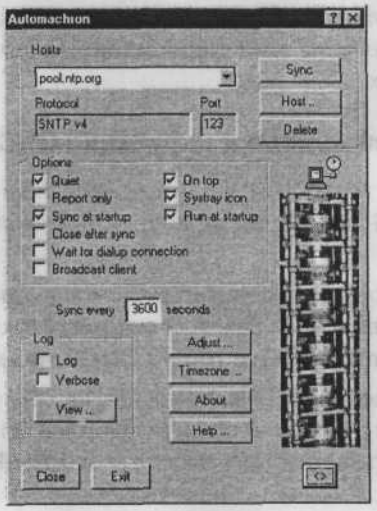

Рис. 2.7. Диалоговое окно конфигурации Automachron

Если функции, предоставляемые Automachron, вам подходят, то следует зайти на сайт www.oneguycoding.com и рассмотреть возможность пожертвования автору через PayPal.

Замечание о безопасности

Трафик NTP

Для синхронизации с серверами времени Internet убедитесь в том, что конфигурация брандмауэра обеспечивает входящий и исходящий трафик через порт 123 UDP. По соображениям безопасности лучше всего ограничить трафик NTP только IP-адресами серверов NTP, используемых в вашей компании.

Перенос MS-DNS/DHCP на BIND/DHCPD Linux

В данном разделе описан перенос DHCP и DNS. Несмотря на то, что это два разных процесса, выполняться они должны скоординировано, из-за взаимосвязи DHCP и DNS.

Перенос областей действия и функций DHCP

Переход от DHCP на базе Windows к DHCP на базе Linux прежде всего включает: определение всех областей действия и важнейших функций, конфигурирование DHCPD для возможности использования этой информации, закрытие служб Microsoft DHCP и запуск служб DHCP Linux.

Определение областей действия и функций DHCP Windows NT

Первым шагом переноса служб DHCP является определение всех областей действия DHCP, обслуживаемых MS-DHCP, а также подробных свойств каждой области действия.

В Windows 4.0 Server этот шаг выполняется с помощью диспетчера (DHCP Manager) (dhcpadmn.exe). Для доступа к DHCP Manager (см. рис. 2.8) с помощью мыши выберите **Start / Programs / Administrative Tools / DHCP Manager**.

На рисунке показан список всех областей действия, обслуживаемых этим сервером DHCP, вместе с функциями DHCP этой области действия. Для получения информации о свойствах области действия (рис. 2.9) выберите **Scope / Properties**.

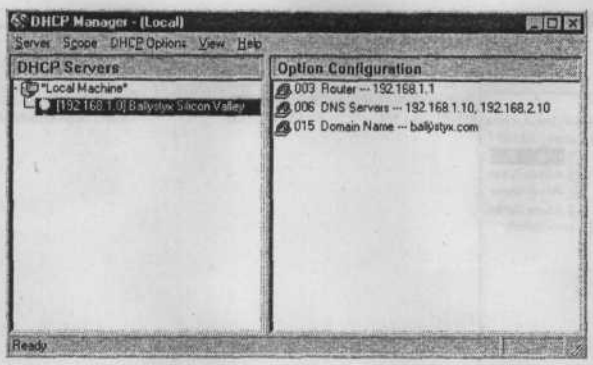

Рис. 2.8. DHCP Manager Windows NT — Ballystyx, Кремниевая Долина

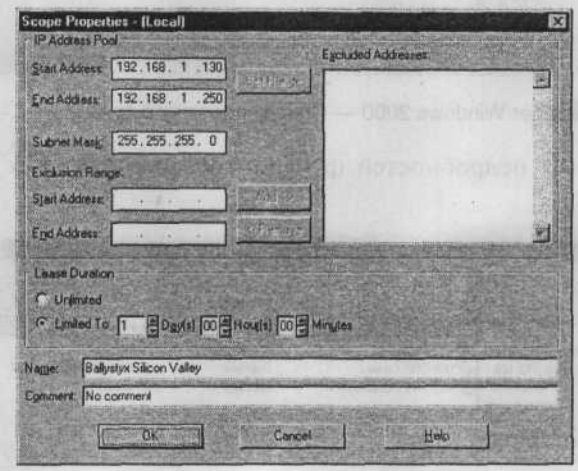

Рис. 2.9. DHCP Manager Windows NT — Подробная информация об области действия

Определение областей действия и функций DHCP Windows 2000

Для получения информации об области DHCP и IP-адресе сервера Windows 2000 выберите **Start / Programs / Administrative Tools / DHCP**. На рис. 2.10 перечислены все области действия, обслуживаемые сервером DHCP, а также адресный пул DHCP, права аренды, резервирование и функции области действия. Для вывода списка IP-адресов, предоставляемых данной областью действия, нажмите Address Pool.

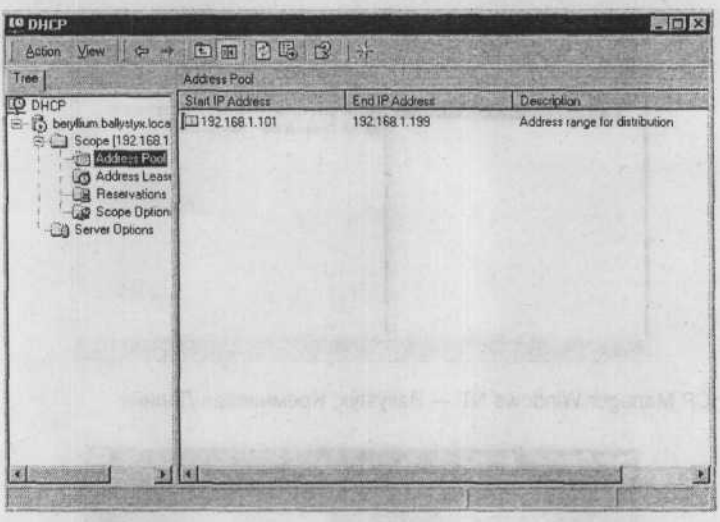

Рис. 2.10. DHCP Manager Windows 2000 — Список адресного пула

Для определения подробностей функций области действия нажмите **Scope Options** (рис. 2.11).

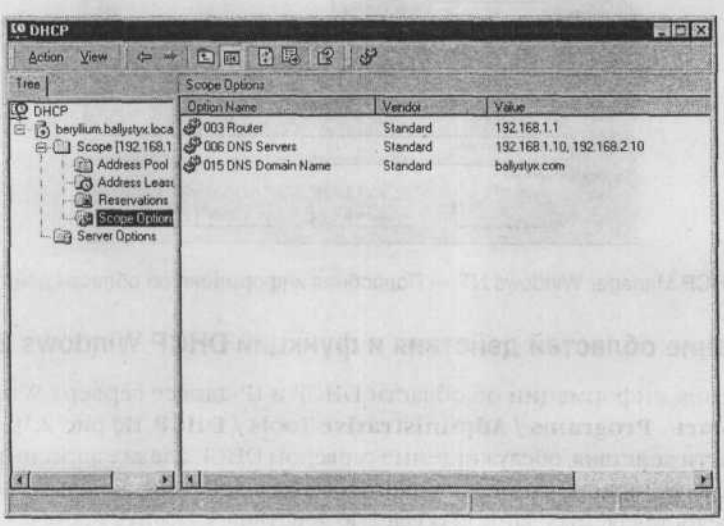

Рис. 2.11. DHCP Manager Windows 2000 — Подробная информация об области действия

Запись областей действия и функций DHCP

Запишите всю информацию DHCP на бумаге или в текстовый или табличный файл. Минимальное ее содержание приведено ниже в табл. 2.3. Если время аренды по умолчанию для имеющейся версии сервера DHCP не приведено, то можно задать либо максимальное значение, либо 50% от максимального значения времени аренды.

Табл. 2.3. Информация об областях действия и функциях DHCP

Компонент	Значение(я)
Подсеть	192.168.1.0
Сетевая маска	255.255.255.0
Диапазон	от 192.168.1.130 до 192.168.1.250
Время аренды по умолчанию	43200 секунд
Максимальное время аренды	86400 секунд
Маршрутизатор(ы)	192.168.1.1
Маска подсети	255.255.255.0
Широковещательный адрес	192.168.1.255
Имя домена	ballystyx.com
Имена серверов DNS	192.168.1.12, 192.168.2.10

После сбора и записи информации о каждой области действия DHCP можно приступать к конфигурированию инфраструктуры DHCP Linux.

Конфигурирование сервера ISC DHCPD

Для настройки служб DHCP на базе Linux скомпилируйте и установите пакет существующего сервера ISC DHCP либо установите текущую версию сервера DHCP из дистрибутива Linux на сервере, установленном в испытательной лаборатории. Запустите любой текстовый редактор и отредактируйте файл dhcpd.conf. Для компании Ballystyx, Кремниевая Долина, dhcpd.conf выглядит следующим образом:

```
ddns-update-style ad-hoc;
# Ballystyx, Кремниевая Долина
subnet 192.168.1.0 netmask 255.255.255.0 {
      range 192.168.1.130 192.168.1.250;
      default-lease-time 43200;
      max-lease- time 86400;

      option routers 192.168.1.1;
      option subnet-mask 255.255.255.0;
      option broadcast-address 192.168.1.255;

      option domain-name "ballystyx.com";
      option domain-name-servers 192.168.1.12, 192.168.2.10;
}
```

Запустите DHCPD. Подтвердите получение испытательной рабочей станцией IP-адреса и необходимых функций DHCP.

Переход от служб DHCP Microsoft к службам DHCP Linux

Скопируйте известный файл dhcpd.conf с сервера-лаборатории на рабочий сервер Linux DHCP. Остановите выполнение служб DHCP Microsoft. Запустите службы DHCP Linux. Загрузите рабочую станцию и проверьте функциональность DHCP, убедившись в том, что настольными рабочими станциями Windows и другими клиентами получены IP-адреса и другая информация DHCP.

Откат при сбое процесса переноса DHCP

В некоторых случаях новые службы DHCP Linux могут работать некорректно, а рабочие станции могут не получить IP-адресов. При возникновении подобной ситуации остановите выполнение служб DHCP Linux и перезапустите службы DHCP Microsoft. Повторите тестирование и, если необходимо, воспользуйтесь процедурой анализа DHCP (описана выше во врезке) для устранения проблем.

Перенос информации DNS

Существует множество способов переноса информации DNS из MS-DNS в BIND. Если записей DNS немного, то перенос можно осуществить вручную простым копированием и вставкой информации. Информацию DNS можно получить из диспетчера DNS Microsoft или из файлов с расширением dns в каталоге C:\WINNT\sytsem32\dns\ и в соответствующих подкаталогах. Если записей много, этот способ требует достаточно много времени. Для большинства организаций самым простым способом переноса информации будет перенос зоны DNS (AXFR).

Установка и конфигурирование BIND

Скомпилируйте и установите существующий пакет ISC BIND либо установите существующий пакет сервера BIND из дистрибутива Linux на тестовый сервер. Запустите текстовый редактор и отредактируйте named.conf, файл конфигурации BIND. Запись ballystyx.com в файле named.conf выглядит следующим образом:

```
zone "ballystyx.com" {
      type master;
      file "/etc/bind/ballystyx.com.hosts";
};
```

Перенос информации DNS

Большинство серверов DNS Windows сконфигурированы для обеспечения переносов зон DNS (AXFR) по умолчанию (это вредит безопасности, но полезно для переноса

данных!), так что данная опция, как правило, доступна или ее можно сделать доступной. В Windows 2000 настройки можно верифицировать запуском диспетчера DNS, переходом к вкладке **Forward Lookup Zones** (зоны прямого поиска) и нажатием правой кнопкой мыши имени домена и выбором команды **Properties**. Выберите закладку **Zone Transfers** и убедитесь в том, что опция **Allow zone transfers** отмечена, как показано на рис. 2.12.

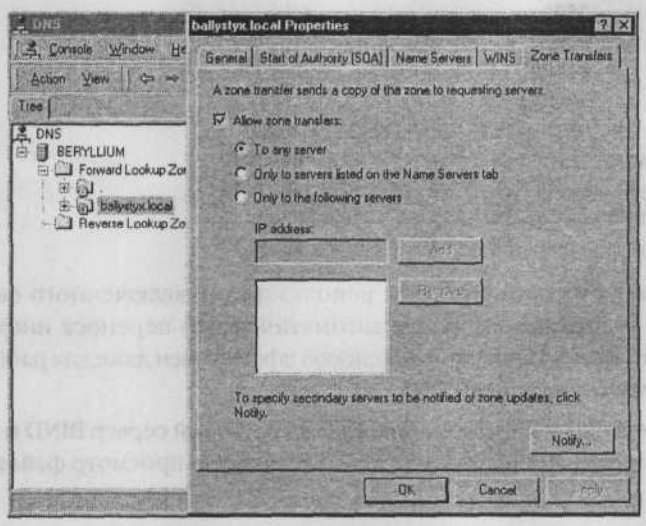

Рис. 2.12. Диалоговое окно диспетчера переноса зон DNS Windows 2000

Следующая команда выполняет перенос зон DNS в компании Ballystyx:

```
dig @lithium ballystyx.com axfr
```

Здесь перечислен список записей в домене ballystyx.com. Формат схож с форматом файла зоны BIND. Выходные данные из **dig** выглядят следующим образом:

```
; <<>> DIG 9.2 4rc5 <<>> @lithium ballystyx.com axfr
;; global options:  printcmd
ballystyx.com.        3600        IN      SOA     lithium.ballystyx.com.
admin.ballystyx.com. 5  3600  600  86400  3600
ballystyx.com.        3600        IN      NS      lithium.ballystyx.com.
hydrogen.ballystyx.com.           3600    IN      A       192.168.1.10
helium.ballystyx.com.             3600    IN      A       192.168.1.11
lithium.ballystyx.com.            3600    IN      A       192.168.1.12
beryllium.ballystyx.com.          3600    IN      A       192.168.1.13
;; Query time: 2 msec
;; SERVER:  lithium#53 (192.168.1.12)
;; WHEN:  Sat Jul 24 08:07:27 2004
;; XFR size:  6 records
```

Записи можно скопировать вручную и вставить в файл зоны BIND или воспользоваться графическим инструментом настройки (например, Webmin) для ввода данных. Данный способ лучше всего работает при небольшом количестве записей DNS. По окончании ввода файл зоны выглядит следующим образом:

```
ballystyx.com.IN   SOA   lithium.ballystyx.com.   admin.ballystyx.com.     (
                   5
                   3600
                   600
                   86400
                   3600 )
ballystyx.com. IN  NS    lithium.ballystyx.com.
hydrogen.ballystyx.com.  IN    A     192.168.1.10
helium.ballystyx.com.    IN    A     192.168.1.11
lithium.ballystyx.com.   IN    A     192.168.1.12
beryllium.ballystyx.com. IN    A     192.168.1.13
```

Другим способом является использование включенного сценария перехода — migrate-dns — для автоматического переноса информации DNS из Windows в Linux. Данный способ эффективен даже для работы с большим количеством записей DNS.

Перенесите информацию DNS на тестовый сервер BIND и убедитесь, что перенос осуществлен корректно (выполните просмотр файла зоны и поиск DNS).

Переход от служб DNS Microsoft к службам DNS Linux

Убедившись в работоспособности конфигурации тестового сервера Linux BIND, скопируйте известный файл named.conf на рабочий сервер Linux BIND. Затем выполните перенос зоны вручную либо с помощью сценария перехода migrate-dns. Вам придется изменить записи SOA и NS, чтобы отразить сведения о вашем реально существующем сервере Linux

Загрузите рабочую станцию и протестируйте функциональность DNS проверкой корректности преобразования имен в IP-адреса настольными рабочими станциями Windows и другими клиентами. При использовании DDNS для регистрации клиентов DHCP убедитесь, что клиентские имена корректно зарегистрированы в DNS. При наличии возможностей обратного поиска DNS убедитесь, что запись PTR зарегистрирована в соответствующей зоне in-addr.arpa.

При использовании служб DHCP в dhcpd.conf необходимо изменить запись domain-n**ame-servers** для включения нового сервера Linux DNS, если его IP-адрес отличается от приведенного. Если на данном этапе целесообразной является перезагрузка рабочих станций, выполните ее. При

этом рабочие станции получат обновленную информацию DNS и протестируют все функции, перенос которых на серверы Linux описан в данной главе. Если перезагрузка слишком разрушительна, то можно принудительно обновить права аренды DHCP.

Откат при сбое процесса переноса DNS

В некоторых случаях новые службы DNS Linux могут работать некорректно, а службы регистрации имен DDNS могут не работать вообще. При возникновении подобных ситуаций попробуйте внести изменения в запись **ddns-update-style**. Если функциональность по-прежнему не восстанавливается, остановите выполнение служб DNS Linux и перезапустите службы DNS Microsoft. Повторите тестирование и, если необходимо, воспользуйтесь процедурой анализа трафика через порт 53 для устранения проблем. Если вам удалось выяснить причину неполадок, повторите перенос.

Microsoft отмечает, что служба каталогов Active Directory будет работать корректно с любым сервером DNS (например, BIND 9), поддерживающим динамический DNS (RFC 2136) и записи SRV (RFC 2782). Однако на практике часто происходит иначе, особенно в сложных средах. При наличии проблем во время переноса DHCP и DNS серверам Windows 2000, возможно, придется подождать замены всех прочих служб, зависимых от MS-DNS (Active Directory и Exchange 2000), и только потом начинать перенос DNS и DHCP на Linux.

Резюме

Службы присвоения IP-адресов, разрешения имен и временной синхронизации являются основными службами любой сети TCP/IP, обеспечивающими функционирование всех прочих сетевых служб, описываемых в книге. DHCP, DNS и NTP — протоколы, обеспечивающие предоставление этих служб клиентам Windows и Linux. Обеспечиваемая этими службами функциональность практически одинакова при работе как с Windows, так и с Linux, кроме интеграции Active Directory со службами DNS Windows 2000.

Часть процесса переноса сетевых служб DHCP и DNS обычно не вызывает затруднений при переносе с системы Windows NT. Службы DHCP и DNS Windows NT проще служб DHCP и DNS Windows 2000 и, следовательно, их легче переносить. Переход от служб DHCP и DNS Windows NT к службам DHCP и DNS Linux обладает дополнительными функциями (например, DDNS), отсутствующими в Windows NT.

Как правило, переход от Windows 2000 проходит без проблем в простых средах с одним доменом, но может быть затруднен в сложных средах. При невозможности переноса служб DHCP и DNS с Windows 2000 на Linux из-за технических проблем, эти службы можно перенести после замены служб, зависимых от MS-DNS, например Active Directory и Exchange 2000 (также зависимой от Active Directory).

Краткое резюме по разделам

Принципы работы служб присвоения IP-адресов

- ☑ Существует два типа систем присвоения IP-адресов — статические и динамические. Большинству серверов присваиваются статические IP-адреса; большинству ноутбуков и настольных рабочих станций присваиваются динамические IP-адреса.
- ☑ DHCP — это протокол, динамически присваивающий хостам IP-адрес и параметры сетевой конфигурации.
- ☑ Для получения первоначального права аренды DHCP клиенты DHCP используют четырехходовой широковещательный процесс (также называемый четырехходовым квитированием). Для обновления права аренды DHCP клиенты используют двухэтапный не широковещательный процесс.
- ☑ Консорциум систем Интернет (ISC) разрабатывает и обслуживает самый популярный в мире открытый сервер DHCP и клиентские приложения. Практически все версии Linux используют программное обеспечение от ISC для обеспечения служб DHCP. Подробную информацию об ISC см. на сайте www.isc.org.

Принципы работы служб разрешения имен

- ☑ Возможность преобразования имен хостов в IP-адреса представляет собой основополагающее удобство работы с компьютерными сетями всех размеров и типов.
- ☑ Существует два типа методологий разрешения имен: на базе файлов и на базе DNS. Использование файла хостов приемлемо только для очень небольших статических сетей. Во всех других сетях для разрешения имен применяется DNS.
- ☑ Динамические DNS позволяют клиентам (или серверам DHCP) регистрировать свои имена и IP-адреса на ведущем сервере имен в домене, как определено записью SOA. Клиенты (или сервера DHCP) также регистрируют запись PTR в домене in-addr.arpa сервера, являющимся SOA для их подсети.

Принципы работы служб временной синхронизации

- ☑ Важность временно́й синхронизации переоценить сложно. Если часы компьютеров клиентов и серверов не синхронизированы, то некоторые службы могут не работать либо работать некорректно.
- ☑ Для всех современных операционных систем используется NTP — протокол, обеспечивающий синхронизацию времени в сети.
- ☑ Ntpd — наиболее популярная служба синхронизации времени для клиентов (и/или серверов) Linux. Automachron — популярная клиентская служба синхронизации времени для Windows 98, NT, 2000 и XP.

- ☑ Несмотря на то, что работа сервера синхронизации времени NTP во внутренней сети может показаться технически целесообразной, лучше открыть порт UDP 123 на брандмауэре и синхронизировать установки времени с временными серверами низкого эшелона Интернет, например с pool.ntp.org.

Перенос MS-DNS/DHCP на BIND/DHCPD Linux

- ☑ Несмотря на то, что перенос служб DHCP и DNS — это два раздельных процесса, выполняться они должны скоординировано, из-за взаимосвязи DHCP и DNS.
- ☑ Прежде всего, переход от служб DHCP на базе Windows к службам DHCP на базе Linux заключается в записи всех областей действия DHCP и их функций, конфигурировании DHCPD с использованием этой информации, закрытии служб Windows DHCP и запуске служб DHCP Linux.
- ☑ Переход от служб DHCP на базе Windows к службам DHCP на базе Linux также заключается в установке сервера BIND, сборе информации DNS через механизм переноса зоны и вводе этой информации в BIND. Приложенный сценарий migrate-dns автоматизирует этот процесс.
- ☑ При наличии проблем во время переноса DHCP и DNS на Linux на серверах Windows 2000 может возникнуть необходимость в предварительной замене всех прочих служб, зависимых от MS-DNS (Active Directory и Exchange 2000).

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма «**Ask the Author**»). Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: Существует ли графическое инструментальное средство для конфигурирования служб DHCP и DNS?

О: Да! Webmin — основанный на web инструмент, подходящий для конфигурирования DHCP, DNS и других рассматриваемых в книге сетевых служб. Подробная информация о Webmin и его модулях имеется на сайте www.webmin.com.

В: Является ли DHCP единственной системой присвоения динамического IP-адреса?

О: BOOTP — протокол самонастройки — более старая система присвоения динамических IP-адресов, обладающая лишь частью богатых возможностей DHCP. BOOTP иногда применяется на бездисковых рабочих станциях. К счастью, dhcpd может обслуживать клиентов как DHCP, так и BOOTP.

В: Возможно ли сделать так, чтобы отдельно взятые клиенты DHCP всегда получали один и тот же IP-адрес?

О: Да. Этот процесс называется резервированием DHCP и управляется через аппаратный адрес MAC (протокол управления доступом к передающей среде) сетевого адаптера (NIC) клиента DHCP. Для выполнения введите следующие строки в **dhcpd.conf**, заменив имя хоста, MAC и информацию об IP-адресе компьютера (компьютеров) на используемые вами:

```
host hostname.example.com {
hardware ethernet 00:11:22:33:44:55;
fixed-address 192.168.1.100;
}
```

В: Существует ли способ, обеспечивающий получение IP-адресов только известными клиентами DHCP?

О: Да. Идея хороша с точки зрения безопасности, хотя и слегка увеличивает нагрузку на сисадмина. Для выполнения введите следующую запись в соответствующий раздел **dhcpd.conf**:

```
deny unknown clients;
```

Глава 3

Службы каталогов

Разделы:

- **Принципы работы LDAP и каталогов**
- **Принципы работы служб каталогов Microsoft**
- **Принципы работы OpenLDAP**
- **Проектирование служб каталогов на базе Linux**

☑ Резюме

☑ Краткое резюме по разделам

☑ Часто задаваемые вопросы

Введение

Службы каталогов — это ключевой компонент управления и каталогизации таких объектов, как учетные записи пользователей и настроек профилей, групп, компьютеров, принтеров, электронной почты, а также других объектов сетей и инфраструктуры. Подобно тому, как основные сетевые службы являются базой служб каталогов, последние — это база (или предпочтительная точка интегрирования) для других сетевых служб — аутентификации, обмена сообщениями и служб коллективной работы.

В начале данной главы в общем виде рассматриваются службы каталогов и облегченный протокол доступа к ним (Lightweight Directory Acces Protocol, LDAP), затем описываются фундаментальные положения LDAP, включая концепцию *Дерева информации каталога* (Directory Information Tree, DIT), соглашение об Отличительном имени (Distinguished Name, DN), объектные классы, компоненты схемы и другие аспекты LDAP, а также рассматриваются запросы и соединения LDAP.

После этого приведены решения служб каталогов Microsoft, которые за период от разработки Windows NT/Exchange 5.5 до Windows 2000 претерпели значительные изменения. В Windows NT вся информация учетных записей пользователей сохраняется в Администраторе учетных данных в SAM (Security Accounts Manager), а Exchange 5.5 предоставляет расширенную информацию о контактах и обмене сообщениями. В Windows 2000 обе эти функции объединены в Active Directory (AD).

В следующем разделе рассматривается OpenLDAP — основной открытый сервер каталогов. Сюда входит описание таких функций набора OpenLDAP, как серверные демоны, клиентские и серверные утилиты, распределенные службы каталогов, а также импортирование/экспортирование данных.

Службы каталогов небольшой компании могут состоять из одного не выделенного сервера, а крупных компаний — могут быть распределенными, избыточными либо использоваться в качестве точки интегрирования множества других сетевых служб. Раздел под названием «Проектирование служб каталогов на базе Linux» поможет определить ключевые требования к службам каталогов компании и спроектировать гибкое решение, удовлетворяющее существующим требованиям и рассчитанное на последующее усовершенствование.

Принципы работы LDAP и каталогов

LDAP — это межплатформенный протокол, обеспечивающий взаимодействие с сервером каталогов. LDAP является результатом развития DAP (Directory Access Protocol, протокол доступа к каталогам) системы X.500. В число первоочередных функций LDAP входят аутентификация и операции запросов с каталогом типа X.500. В книге имеется в виду версия LDAPv3.

Понятие терминов LDAP

Начнем обсуждение LDAP с обзора терминов описания структуры каталогов и их объектов. Для понимания материала данной главы рекомендуется полностью освоить эту основополагающую информацию. Для подробного анализа LDAP предлагается ознакомиться с презентацией Адама Уильямса (Adam Williams) *«LDAP и OpenLDAP на платформе Linux»* (ftp://kalamazoolinux.org/pub/pdf/ldapv3.pdf).

Понятие структуры каталогов

Каталог имеет иерархическую структуру, которая называется Деревом информации каталога, или DIT. Структура DIT начинается с базового отличительного имени (также называемого *суффиксом*) и разделена логически на объекты организационных единиц (OE). Как правило, DIT-ы структурированы по типам объектов, содержащихся в каждом дереве. На проектирование DIT может влиять географическая или организационная структура предприятия.

На рис. 3.1 представлено DIT, подходящее большинству компаний, в том числе Widgets и Ballystyx.

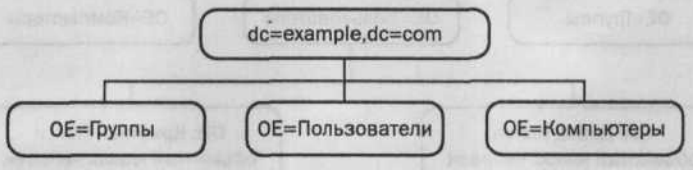

Рис. 3.1. Дерево информации каталога — Простая модель

На рис. 3.2 показано DIT для компании с четким разграничением производственных единиц, функционирующих с минимальным взаимодействием между собой и совместным использованием информации рабочими группами.

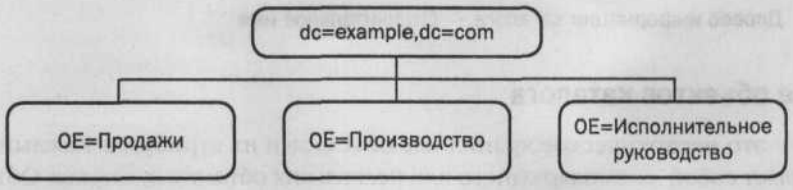

Рис. 3.2. Дерево информации каталога — Модель для рабочей группы

На рис. 3.3 показано DIT для крупной корпорации со множеством расширенных представительств в разных частях света. В данном случае все административные технические функции и ИТ разделены по континентам по юридическим, финансовым, техническим и иным производственным причинам. Для большинства компаний такая структура не пригодна, однако она иллюстрирует еще один тип структуры и проектирования каталогов.

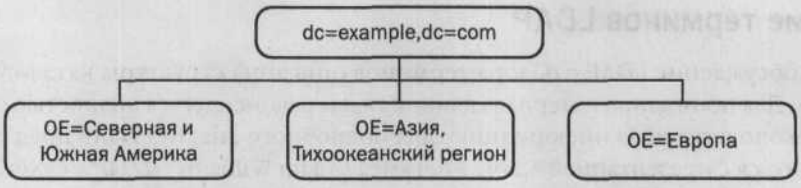

Рис. 3.3. Дерево информации каталога — Географическая модель

Каждый объект в каталоге уникально идентифицирован определенным отличительным именем. Оно состоит из атрибута, уникально определяющего этот объект (обычно с общепринятым именем (ОИ) или с идентификатором пользователя (UID)), за которым следует путь, определяющий местоположение этого объекта в рамках DIT. На рис. 3.4 представлены два объекта людей-примеров и соответствующее отличительное имя.

Рис. 3.4. Дерево информации каталога — Отличительное имя

Понятие объектов каталога

Каталог — это иерархическое хранилище объектов и их атрибутов. Каждый объект представляет собой экземпляр одного или нескольких объектных классов. Объектные классы определяют набор атрибутов, которыми могут или должны обладать эти типы объектов. Атрибуты могут содержать в себе текст, числа, двоичные данные или данные других типов.

Набор объектных классов, поддерживаемый сервером каталогов, называется схемой каталога. Файлы схемы (подобные включенным в OpenLDAP и Samba) содержат объектный класс, атрибуты и определения синтаксиса. Каждый из этих элементов ассоциируется с Идентификатором объекта (OID). Идентификаторы объектов пред-

ставлены в иерархической записи с разделительными точками и уникально обозначают объект, атрибут и определения синтаксиса. Ниже показано определение для объектного класса «человек» в **core.schema**:

```
Objectclass (2.5.6.6 NAME        'person'
      DESC 'RFC2256: a person'
      SUP top STRUCTURAL
      MUST ( sn $ cn)
      MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )
```

В данном определении объектного класса перечислены атрибуты, которые *должны* входить в объект-человек (общепринятое имя и фамилия), и атрибуты, которые *могут* присутствовать (userPassword (пароль пользователя), telephoneNumber (номер телефона), seeAlso (см. также), description (описание)). Ниже приведено описание выбранных атрибутов:

```
attributetype ( 2.5.4.3 NAME ( 'cn' 'commonName' )
      DESC 'RFC2256: общепринятое имя (имена), по которому элемент опознается'
      SUP name )
attributetype ( 2.5.4.4 NAME ( 'sn' 'surname' )
      DESC 'RFC2256: фамилия, по которой элемент опознается'
      SUP name )
attributetype ( 2.5.4.20 NAME ( 'telephoneNumber'
      DESC 'RFC2256: Номер телефона'
      EQUALITY telephoneNumberMatch
      SUBSTR telephoneNumberSubstringsMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.50 {32} )
```

Подключение к серверу каталогов

Для выполнения таких операций, как запросы LDAP клиенту, сначала необходимо подключиться к серверу каталогов. На языке LDAP это называется операцией *связывания* (bind). Существуют четыре типа операций связывания:

- анонимное связывание;
- простое связывание;
- простое связывание с безопасностью транспортного уровня (Transport Layer Security, TLS);
- простое связывание с простым уровнем аутентификации и безопасности (Simple Authentication and Security Layer, SASL).

При анонимном связывании клиент LDAP предоставляет пустое связывающее отличительное имя и пароль. При аутентификационном связывании клиент LDAP предоставляет отличительное имя объекта каталога для связывания, а также мандат — пароль. Простые связывания (без шифрования) имеют недостаток — пароль передается по сети в открытом виде.

Для защиты пароля от обнаружения следует использовать определенную форму его шифрования. Большинство версий LDAP поддерживает использование операции StartTLS, шифрующей все последующие взаимодействия между клиентом и сервером. SASL — более сложная форма аутентификации, поддерживающая Kerberos и общий программный интерфейс службы защиты — Generic Security Services Application Programming Interface (GSSAPI). Более подробно аутентификация и шифрование описываются в главе 4. На данном этапе важнее помнить, что неанонимные связывания, при которых пароли передаются в открытом виде, создают потенциальную проблему защиты информации.

Понятие запросов LDAP

После успешного подключения к серверу каталогов клиент обычно направляет запрос. Запрос LDAP состоит из следующих частей:

- **База поиска.** Содержит отличительное имя части дерева каталога, с которой должен начаться поиск. Обычно выражается в форме dc=domain,dc=com, хотя в устаревших версиях встречаются обозначения o=organization,c=country. Иногда называется суффиксом поиска.
- **Область поиска.** Может быть **base**, **one** или **sub**. Область базового поиска осуществляет его только на базовом уровне. Область поиска **one** осуществляет поиск на один уровень ниже базового. Область поиска **sub** будет осуществлять поиск на всех уровнях, включая базовый.
- **Фильтр поиска.** Указывает, какие типы объектов и атрибутов должен возвратить сервер каталогов. Фильтры поиска задаются с помощью регулярных выражений.
- **Атрибуты поиска.** Содержит все атрибуты для возврата в запросе LDAP. Если поле атрибутов поиска не заполнено, то будут возвращены все атрибуты объекта. Для минимизации воздействия на производительность сервера каталогов оптимальным считается запрос только необходимых атрибутов.

Другим способом представления поиска LDAP является использование Универсального индикатора ресурса (URI). Базовый формат LDAP URI следующий:

```
'ldap://' [hostport] ['/' [dn ['?' [attributes] ['?' [scope] ['?'
[filter]]]]]]
```

Более подробная информация о фильтрах поиска LDAP имеется в RFC 2254 «Строковое представление фильтров поиска LDAP». Подробная информация о формате LDAP URI имеется в RFC 2255 «Формат LDAP URI».

Принципы работы служб каталогов Microsoft

В сервере Windows NT и Windows 2000 используют три сервера каталогов: NT Security Accounts Manager, Exchange 5.5 Directory Services и Windows 2000 Active Directory. Эти три сервера рассматриваются ниже.

Понятие Windows NT SAM

Для сохранения объектов пользователей в Windows NT используется SAM (администратор учетных данных в системе защиты). SAM Windows NT управляется Диспетчером пользователей или утилитами третьих сторон и по сравнению с другими службами каталогов содержит меньше информации. Для SAM NT не существует интерфейса LDAP.

Windows NT SAM также поддерживает использование групп, включая вложенные. SAM разбивает группы на два типа: локальные и глобальные. Локальные группы могут содержать глобальные, а глобальные группы не могут включать в себя локальные.

Windows NT SAM сохраняет имена пользователей и учетные записи компьютеров в виде Идентификатора защиты (SID). Учетная запись пользователя также содержит хэши паролей LAN (Диспетчер LAN) и NTLM (NT LANMAN), полное имя пользователя, описание, домашний каталог, путь профиля, сценарий регистрации, время регистрации и состояние учетной записи.

Windows NT — служба каталогов с одним главным устройством. Этот главный сервер каталогов (для чтения и записи) называется Главным контроллером домена (PDC), а подчиненный сервер каталогов (только для чтения) называется Резервным контроллером домена (BDC). В домене Windows NT имеется только один PDC, а BDC может не быть вообще или быть несколько.

Домены Windows NT не являются иерархическими, а зависят от доверительных отношений при взаимодействии. В данной книге будет рассматриваться модель с одним доменом. При наличии нескольких доменов можно воспользоваться миграционными методиками для одного домена для отдельного переноса частей каждого домена. Эти домены могут содержаться раздельно или быть объединены в один.

Понятие служб каталогов Exchange 5.5

Сервер Exchange представляет собой первую версию служб каталогов Microsoft, имеющую многосерверную репликацию и поддержку LDAP. Сервер каталогов Exchange 5.5 поддерживает LDAPv3 и большой набор объектов и атрибутов. Каждый сервер Exchange содержит полную копию каталога. Изменения, вносимые в каталог Exchange на одном сервере Exchange, распространяются на все другие серверы Exchange в рамках организации Exchange.

Exchange поддерживает использование групп для создания списков рассылки. В Exchange 5.5 эти группы называются *Списками распространения*. Эти группы —

не то же самое, что группы NT SAM, и они не взаимозаменяемы. Одно из преимуществ Active Directory перед каталогом Exchange 5.5 заключается в том, что группы AD можно использовать как для управления рассылкой электронных сообщений, так и для управления доступом.

Exchange 5.5 поддерживает концепцию внешних адресатов. Эти адресаты называются *пользовательскими*, и, как правило, с помощью каталога Exchange к ним может получить доступ любой пользователь. Они похожи на контактные лица в Outlook и в других почтовых клиентах, но существуют в каталоге, а не у локального почтового клиента.

Exchange 5.5 связывает объекты пользователей NT SAM с пользовательскими почтовыми ящиками полем Первичной учетной записи Windows NT (Assoc-NT-Account). В Exchange Administrator данное поле показано как учетная запись Windows NT, хотя на самом деле оно сохранено как SID в каталоге Exchange.

Каталог Exchange является предшественником Active Directory и содержит подмножество функций Active Directory.

Понятие Active Directory

Active Directory — это реализация службы каталогов Windows 2000 от Microsoft. Active Directory используется как сервер каталогов для промышленного внедрения доменов Microsoft и необходим для работы многих продуктов Microsoft, включая Exchange Server. Active Directory выполняется только на серверах Windows.

Active Directory реализует интерфейс LDAP, хотя Интерфейс служб Active Directory (ADSI) — наиболее широко используемый метод доступа к объектам Active Directory. Active Directory тесно интегрирован с реализацией Службы имен доменов (DNS) Microsoft Windows 2000 и Протокола динамической конфигурации хостов (DHCP) и для корректного функционирования требует наличия служб DNS.

Active Directory выполняет схожие с моделью доменов NT базовые функции, но существуют и некоторые различия между этими двумя службами каталогов (см. табл. 3.1).

Табл. 3.1. Различия между доменами Windows NT и Active Directory

Домены Active Directory	Домены Windows NT
Интеграция с DNS	Отсутствие интеграции с DNS
Иерархическая транзитивная модель доверия	«Островная» модель с различными типами доверительных отношений
Сохраняют мандаты для аутентификации Kerberos и NT/LANMAN	Сохраняют мандаты для аутентификации NT/LANMAN. Поддержка Kerberos отсутствует
Сохранение расширенной контактной информации для пользователя	Сохраняет ограниченную контактную информацию для пользователя
Модель многосерверной репликации	Модель односерверной репликации

Active Directory сохраняет значительный объем информации и представляет собой расширенную версию NT SAM и каталога Exchange 5.5. В Active Directory сохраняется имя пользователя, полное имя, описание, хэши паролей, домашний каталог, путь профиля, контактная информация, адрес(а) электронной почты и другая информация. Более подробная информация об Active Directory доступна на сайте www.microsoft.com/windows2000/technologies/directory/.

Принципы работы OpenLDAP

OpenLDAP — первое открытое решение для работы со службами каталогов. Пакет содержит полный набор компонентов клиентов и серверов, необходимый для реализации и использования служб каталогов. OpenLDAP работает на всех версиях Linux и отличается устойчивой поддержкой репликации распределенных служб каталогов. OpenLDAP — проверенный продукт. Он разработан в Университете Мичигана, но в настоящее время управляется фондом OpenLDAP. Более подробная информация об OpenLDAP доступна на сайте www.openldap.org.

Понятие демонов («сторожевых» процессов) сервера OpenLDAP

Slapd (автономный демон LDAP) — это серверный процесс OpenLDAP, прослушивающий сетевые порты и отвечающий на подключение клиентов к LDAP. Slapd управляется через файл slapd.conf, обычно находящийся в /etc/openldap или /etc/ldap.

Slurpd (автономный демон обновления репликации) активизирует распределенные службы каталогов путем предоставления возможностей репликации (дублирования). Slurpd доступны модели репликации типа «мастер-подчиненный» (с одним главным сервером) или «мастер-мастер» (с несколькими главными серверами). Репликация типа «мастер-подчиненный» работает путем поддержки одной копии каталога для чтения-записи (главной) и репликации каталога в одну или несколько копий только чтения (подчиненных). Репликация с одним главным сервером — более легкий способ, используемый в большинстве организаций. Slurpd использует репликацию типа «проталкивания», что означает инициацию подключения главного сервера к другим серверам, который «проталкивает» в них обновленную информацию.

При репликации с несколькими главными серверами серверы каталогов имеют возможность записи в каталог. При внесении изменения сервер каталогов, обрабатывающий операцию записи, отправляет обновленную информацию на другие серверы каталогов.

Понятие утилит OpenLDAP

Пакет OpenLDAP имеет множество клиентских утилит и библиотек. В табл. 3.2 перечислены наиболее часто используемые утилиты OpenLDAP.

Табл. 3.2. Наиболее часто используемые утилиты OpenLDAP

Название утилиты OpenLDAP	Описание
Idapsearch	Запрос сервера каталогов
Idapadd	Добавление объекта каталога
Idapmodify	Изменение объекта каталога
Idapdelete	Удаление объекта каталога
Idappasswd	Изменение пароля объекта каталога
slappasswd	Создание зашифрованных паролей
Slapcat	Запись содержимого каталога в файл LDIF
Slapadd	Добавление содержимого каталога из файла LDIF, созданного slapcat
Slapindex	Регенерация указателей slapd

Для сохранения непротиворечивости базы данных при выполнении операции **slapcat** или **slapindex** slapd необходимо закрыть (или запустить в режиме «только чтение»). Slapd также необходимо закрывать во время выполнения операции **slapadd**. В большинстве случаев файл LDIF задается во входных данных при выполнении **ldapadd**, **ldapmodify** или **ldapdelete**, особенно если изменения затрагивают несколько объектов. Более подробную информацию об утилитах OpenLDAP можно получить при вводе **man** *utilityname*, где *utilityname* – имя утилиты.

Проектирование служб каталогов на базе Linux

Поняв принципы функционирования служб каталогов, LDAP и OpenLDAP, читатель готов к проектированию и развертыванию служб каталогов на базе Linux. Последующие разделы помогут определить наилучший способ соответствия служб каталогов требованиям конкретной организации.

Проектирование Дерева информации каталога

Первым шагом проектирования служб каталогов является определение структуры деревьев информации каталогов компании. Данный процесс начинается с определения базового отличительного имени. Для компании с именем домена Интернет .com это обычно означает использование **dc=*имя_домена*,dc=com** в качестве базового отличительного имени. Для компании без доменного имени Интернет можно рассматривать использование **dc=*название_компании*,dc=local**.

После определения базового отличительного имени необходимо определить способ логического разделения иерархии каталога на организационные единицы. Для подавляющего большинства компаний необходимо не более четырех организационных единиц. На рис. 3.5 показана рекомендуемая структура дерева информации каталогов.

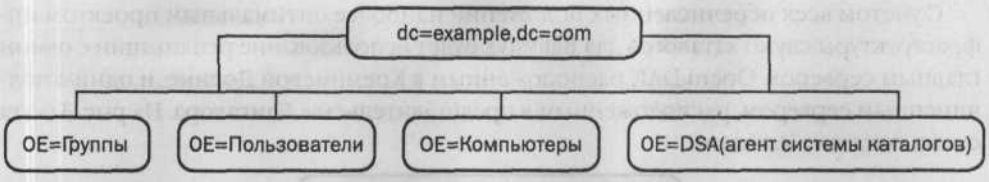

Рис. 3.5. Рекомендуемая структура Дерева информации каталога

Одним из преимуществ данной структуры DIT является то, что она позволяет напрямую использовать модули Webmin www.webmin.com, созданные IDEALX для администрирования LDAP учетных записей Samba и Posix. Для управления каталогом рекомендуется использование модулей idxldapaccounts. Информация и материалы для скачивания доступны на сайте www.idealx.org/prj/webmin/index.en.html.

Если организация крупная и совместное использование ресурсов разными производственными единицами и/или представительствами пренебрежимо мало, тогда можно рассматривать более сложную структуру DIT. Однако в большинстве случаев лучше всего использовать рекомендуемое DIT, добавляя при необходимости дополнительные организационные единицы высшего уровня.

Проектирование инфраструктуры OpenLDAP

После определения структуры дерева информации каталогов необходимо определить тип, размещение и количество серверов OpenLDAP в организации. Для такой маленькой организации, как Acme Widgets, с несколькими сотрудниками и одним сервером, выбор прост: Acme Widgets устанавливает OpenLDAP на единственном сервере.

Для такой компании, как Ballystyx, с большим количеством сотрудников, множеством представительств и пятью серверами, выбор шире. Следующие критерии помогают принять решение для средних и крупных организаций:

- использование пропускной способности и работоспособности;
- работоспособность и расширяемость сервера;
- модели использования служб каталогов, включая:
  - модели использования клиентами-конечными пользователями (например, поиски адресов электронной почты),
  - модели использования клиентами-серверами (например, аутентификация и обмен сообщениями),
  - модели использования в каждом представительстве, а также количество представительств, требующих службы каталогов;
- частота и тип операций чтения и записи каталогов;
- репликация каталогов и соображения устранения радикальных сбоев;
- правовые соображения и вопросы безопасности;
- доступность персонала службы технической поддержки.

С учетом всех перечисленных положений наиболее оптимальным проектом инфраструктуры служб каталогов для Ballystyx будет использование репликации с одним главным сервером OpenLDAP, расположенным в Кремниевой Долине, и одним подчиненным сервером, расположенным в представительстве Бангалора. На рис. 3.6 эта схема показана наглядно.

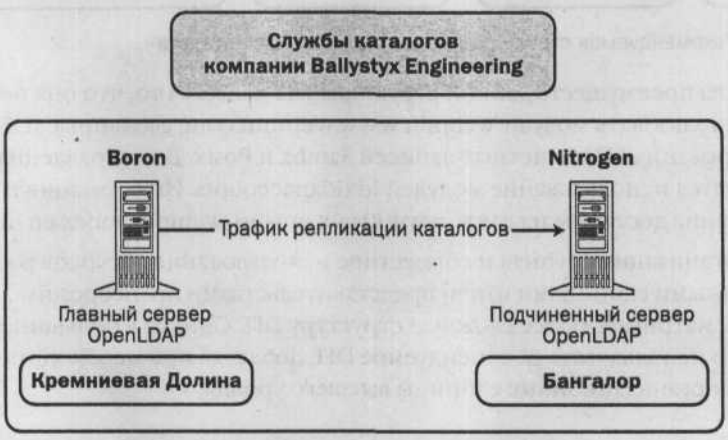

Рис. 3.6. Службы каталогов компании Ballystyx Engineering

Проектирование и планирование

Бизнес-критичные службы каталогов

В такой организации, как Ballystyx Global Semiconductor Engineering, службы каталогов являются бизнес-критичными и должны быть доступны в любое время. Одной из причин этого является зависимость от функционирования служб каталогов других бизнес-критичных сетевых служб, например служб аутентификации, обмена сообщениями и коллективного использования ресурсов.

Для выполнения этой задачи в Ballystyx имеются два сервера каталогов — один в Кремниевой Долине, а другой — в Бангалоре. Этим обеспечивается работа одного сервера каталогов при выходе из строя второго до тех пор, пока между Кремниевой Долиной и Индией сохраняется связь. По мере роста бюджета и штата сотрудников в Кремниевой Долине и Бангалоре будут разворачиваться дополнительные серверы OpenLDAP для обеспечения избыточных служб каталогов с балансировкой нагрузки в обоих представительствах.

Конфигурирование и тестирование серверов OpenDLAP

После определения типа и места размещения сервера (серверов) в испытательной лаборатории можно приступать к тестированию служб каталогов. Скомпилируйте и установите на испытательный стенд существующий пакет OpenLDAP либо пакет OpenLDAP, входящий в дистрибутив. В зависимости от необходимых функций OpenLDAP в **./configure** может потребоваться ввод переключателей командной строки для активизации особых опций в процессе компиляции. При установке пакета OpenLDAP из дистрибутива в нем могут оказаться несколько версий с одинаковыми названиями, скомпилированные с разными параметрами. Для установки базовых нешифрованных служб каталогов подойдут настройки по умолчанию. При необходимости внести дополнительные возможности OpenLDAP можно перекомпилировать или обновить позже. Более подробная информация о компоновке и установке OpenLDAP имеется на сайте www.opendlap.org/doc/admin22/install.html.

После установки OpenLDAP необходимо отредактировать файл конфигурации — slapd.conf, чтобы обеспечить его соответствие вашему окружению. Ниже приведен файл slapd.conf для компании Acme Widgets.

```
#   Schema   files (файлы схемы)
include      /etc/openladap/schema/core.schema
include      /etc/openladap/schema/cosine.schema
include      /etc/openladap/schema/inetorgperson.schema
include      /etc/openladap/schema/nis.schema
include      /etc/openladap/schema/samba.schema

schemacheck  on
lastmod      on

# This section defines the acmewidgets.com directory database (в данном разделе
определен каталог базы данных acmewidgets.com)
database bdb
suffix       "dc=acmewidgets,dc=com"
rootdn       "cn=Manager,dc=acmewidgets,dc=com"
rootpw       "secret"
directory  /var/lib/ldap

# These database indices improve performance (эти индексы базы данных повышают
производительность)
index        objectClass, uidNumber, gidNumber                    eq
index        cn, sn, uid, displayName                                pres,sub,eq
index        mail, givenname, memberUid                              eq,subinitial
index        sambaSID, sambaPrimarygroupSID,sambaDomainName      eq

#  Access  Control  (управление доступом)
access to attrs=userassword,sambaNTPassword,sambaLMPassword
```

```
        by self write
        by anonymous auth
        by * none

# all other attributes are readable to everybody (все прочие атрибуты открыты для
чтения любыми пользователями)
access to *
        by * read
```

Обратите внимание на определение схемы. Во многих случаях **samba.schema** необходимо копировать из пакета Samba. Эти схемы необходимы для предоставления следующих объектных классов, которые будут использоваться для переноса:

- top;
- posixAccount;
- shadowAccount;
- sambaAccount;
- sambaSAMAccount;
- sambaDomain;
- person;
- organizationalPerson;
- inetOrgPerson;
- posixGroup;
- sambaGroupMapping.

После корректной настройки slapd.conf запустите сервер OpenLDAP и выполните простую операцию связывания с помощью мандата rootdn (cn=Manager,dc=yourdomain,dc=com). Хотя вы не увидите никаких данных, кроме собственно схемы, проверка возможности подключения к серверу каталогов будет произведена. Теперь все готово для заполнения каталога данными.

Резюме

Службы каталогов обеспечивают иерархическое сохранение и централизованное управление информацией о пользователях, группах, компьютерах и других элементах сети и инфраструктуры. Поскольку службы каталогов являются основой (или желаемой точкой интеграции) других сетевых служб, рассматриваемых в данной книге, развертывание служб каталогов на базе Linux представляет собой основополагающую базу для всех прочих сетевых служб.

В следующей главе читатель познакомится с пакетом Samba, который интегрируется с каталогом OpenLDAP для обеспечения аутентификации. Также будет рассмотрен перенос информации NT, Exchange 5.5 и/или Active Directory.

Краткое резюме по разделам

Принципы работы LDAP и каталогов

- ☑ Каталогом называется иерархическое хранилище объектов и их атрибутов. Облегченный протокол службы каталогов (LDAP) обеспечивает выполнение операций аутентификации и запросов сервера каталогов.
- ☑ Иерархическая структура каталога называется Деревом информации каталога (DIT). DIT начинается с базового отличительного имени (суффикса директории), такого как, например dc=example,dc=com. Объекты организационной единицы (OE) используются для создания иерархической структуры, подобной дереву. Деревья каталогов обычно структурируются по типу объектов, но могут и по географическим признакам, и по производственным единицам.
- ☑ Схема определяет объектные классы и атрибуты, поддерживаемые каталогом. В определении объектного класса перечислены атрибуты, которые должны или могут содержаться в объекте данного типа. Ссылки на объектные классы и атрибуты делаются посредством уникального Идентификатора объекта (OID).
- ☑ Перед выполнением запроса клиента LDAP связывается с сервером каталогов. Связывание может быть анонимным или аутентифицированным.
- ☑ Запросы LDAP состоят из базы поиска, области действия, фильтра и/или списка атрибутов. Запрос LDAP может определяться аргументами командной строки либо представляться Уникальным индикатором ресурса (URI). Более подробную информацию о фильтрах поиска LDAP и URI см. в RFC 2254 и 2255.

Принципы работы служб каталогов Microsoft

- ☑ В сервере Windows NT и Windows 2000 имеются три типа служб каталогов: Администратор учетных данных в системе защиты NT (SAM), службы каталогов Exchange 5.5 и Active Directory.
- ☑ Windows NT SAM — очень простая служба каталогов, сохраняющая информацию об учетных записях пользователей, компьютеров и групп. Домены Windows NT содержат Главный контроллер домена (PDC) и от нуля до нескольких Резервных контроллеров домена (BDC). Домены NT используют репликацию с одним главным сервером с PDC, содержащим копию каталога с возможностью чтения и записи в него, и с BDC, содержащим(и) копию каталога только для чтения.
- ☑ Каталог Exchange 5.5 поддерживает репликацию с несколькими главными серверами и LDAP, а также содержит обширный набор объектов и атрибутов. Каталог Exchange поддерживает обслуживание почтовых ящиков пользователей, группы (для списков рассылки) и пользовательских абонентов. Почтовые ящики пользователей связаны с NT SAM через поле **Primary Windows NT Account**.

- ☑ Active Directory — реализация промышленной службы каталогов Microsoft Windows 2000. Active Directory содержит расширенный набор информации в каталогах NT SAM и Exchange 5.5. Более подробная информация об Active Directory доступна на сайте www.microsoft.com/windows2000/technologies/directory/.

Принципы работы OpenLDAP

- ☑ OpenLDAP — первое открытое решение для работы со службами каталогов. Пакет содержит полный набор компонентов клиентов и серверов, необходимый для реализации и использования служб каталогов.
- ☑ Slapd (автономный демон LDAP) — это серверный процесс OpenLDAP, отвечающий на подключение клиентов к LDAP. Slurpd (автономный демон обновления репликации) активизирует распределенные службы каталогов путем предоставления возможностей репликации.
- ☑ Пакет OpenLDAP имеет множество утилит, включая OpenLDAP ldapsearch, ldapadd, ldapmodify, ldapdelete, ldappasswd, slappasswd, slapcat, slapadd и slapindex. Более подробную информацию об утилитах OpenLDAP можно получить при вводе **man** *имя утилиты*.

Проектирование служб каталогов на базе Linux

- ☑ Первым шагом проектирования служб каталогов на базе Linux является определение структуры деревьев информации каталогов компании и отличительного имени (суффикса каталога). Для компании с именем домена Интернет .com это обычно означает использование dc=*имя_домена*,dc=com.
- ☑ Следующим шагом является определение типа, местоположения и количества серверов OpenLDAP в организации. Пропускная способность, доступность/расширяемость сервера, модели использования каталога, репликация, восстановление после сбоев и аспекты технического обслуживания формируют процесс принятия решения.
- ☑ В последний этап перед развертыванием входит установка, конфигурирование и тестирование служб каталогов в испытательной лаборатории. Файл slapd.conf необходимо настроить под нужды конкретной организации; сюда входит определение файлов схемы, базового отличительного имени, конфигурирование и элементы управления доступом.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма «**Ask the Author**»). Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: Существует ли простой способ резервирования или восстановление содержимого каталога OpenLDAP?

О: Для этих целей рекомендуется использовать slapcat и slapadd. Не пытайтесь копировать файл рабочей базы данных, выполняющей операции записи; база данных может находиться в противоречивом состоянии, и операция восстановления выполнена не будет.

В: Почему Windows SAM считается сервером каталогов?

О: Несмотря на то, что Windows SAM не является каталогом типа X.500, не имеет интерфейса LDAP, эта система является механизмом сохранения и запросов для пользователей и групп объектов. По этой причине Windows SAM объединен в группу с другими серверами каталогов Microsoft.

В: Скольких серверов OpenLDAP — одного, двух или трех — достаточно для моей организации? Как лучше расширять службы каталогов и каковы типичные проблемы?

О: В организации с оптимально спроектированными распределенными службами каталогов обычно имеется один сервер OpenLDAP с возможностью записи и чтения (главный) в головном представительстве и по одному серверу с возможностью только чтения в каждом филиале. Если определенные приложения (например, серверы postfix или Samba) выполняют значительный объем поиска в каталогах, тогда для них может быть выделен отдельный сервер OpenLDAP с возможностью только чтения.

В: Существует ли простой способ переадресации клиентов на другой сервер каталогов при выходе из строя одного из них?

О: Использование круговых (round-robin) DNS является лучшим способом активизации распределения нагрузки, избыточности и служб каталогов высокой доступности.

Глава 4

Службы аутентификации

Разделы:

- Принципы аутентификации в Windows
- Принципы аутентификации в Linux
- Проектирование служб аутентификации на базе Linux
- Переход от NT/Exchange или Active Directory

☑ Резюме

☑ Краткое резюме по разделам

☑ Часто задаваемые вопросы

Введение

Аутентификация — это одна из наиболее важных и широко используемых сетевых служб. Возможность управления доступом к сетевым ресурсам в первую очередь зависит от возможности уверенной идентификации САМОГО СЕБЯ. В большинстве случаев аутентификация пользователей заключается в подтверждении мандатов (полномочий), состоящих из одного или нескольких факторов: чего-то известного вам (имя пользователя, пароль), чего-то имеющегося у вас в наличии (аппаратный ключ) или чего-то, чем вы являетесь (биометрическая идентификация).

Аутентификация может заключаться в простом сравнении введенного пароля с открытым паролем, хранящемся в локальном файле. Однако требования безопасности, расширяемости, надежности и набора функций во всех, кроме микроскопических по размерам, организациях означают использование так называемой схемы аутентификации, имеющей службу аутентификации, взаимодействующую со службой каталогов, которая может быть, а может и не быть запущена на данной машине. Идентификационные мандаты (имена пользователей и хэши паролей) хранятся в каталоге, а не в службе аутентификации. Если каталог служит централизованным хранилищем этой информации, то можно создать гибкие методологии аутентификации, которые обеспечили бы централизованное управление распределенными разнородными службами аутентификации.

Для конечного пользователя, сидящего за своим компьютером, одним из наиболее очевидных примеров аутентификации является ввод им имени пользователя, пароля и последующего получения разрешения на работу на данной машине. В разделе «Принципы аутентификации в Windows» рассматривается собственно аутентификация, сценарий регистрации, подключение дисков и другие процессы, происходящие во время начала сеанса работы на терминале с системой Windows.

В следующем разделе — «Принципы аутентификации в Linux» — рассматриваются различные типы аутентификации, включая /etc/passwd/shadow, LDAP (облегченный протокол службы каталогов) и NIS (сетевая информационная система). Раздел завершается обзором Подключаемых модулей аутентификации (PAM) — гибкого механизма аутентификации, независимого от методологий.

Раздел «Проектирование служб аутентификации на базе Linux» поможет при определении ключевых требований аутентификации, исходя из конкретных требований информационной защиты, принятых в организации, ее географического положения, поддержки со стороны операционной системы и пр. Будут рассмотрены службы аутентификации, предоставляемые Samba и OpenLDAP, а также рекомендации по установке и интегрированию пакета Samba с OpenLDAP.

В завершающем разделе представлена информация по выполнению операций перехода с NT / Exchange 5.5 / Active Directory (AD) в OpenLDAP с помощью поставляемых сценариев переноса. Здесь также описан перенос информации пользователя, группы и информации о компьютере.

Принципы аутентификации в Windows

Начиная с Windows NT 3.1, для аутентификации регистраций пользователей корпорация Microsoft использовала реализацию протокола LANMAN (нынешнее воплощение — NT LAN Manager или NTLM). Реализация протокола LANMAN от Microsoft позаимствована из реализации LANMAN, выполненной IBM в OS/2.

В Windows 2000 Microsoft представила механизм аутентификации на базе Kerberos. Использование последнего обеспечило инфраструктуре Microsoft повышенную защиту, расширяемость и возможность использования его крупными компаниями, а интеграция с Active Directory упростила администрирование того, что считается сложным протоколом аутентификации.

Функциональность Kerberos от Microsoft взаимодействует — или замещает — множество открытых серверов или служб Kerberos, выполненных не Microsoft. Одной из проблем совместимости с Active Directory является то, что Microsoft «приняла и расширила» протокол аутентификации Kerberos с целью включения криптографически подписанного аутентификационного компонента в поле PAC (автоматическое конфигурирование прокси) Kerberos. Для клиентов Linux это не имело особого значения, однако клиенты Windows 2000/XP ожидали и требовали заполненное поле PAC. Несмотря на то, что сервер Kerberos Microsoft может аутентифицировать клиентов как Windows Kerberos, так и не-Windows Kerberos, сервер Heimdal (или MIT Linux Kerberos) не мог корректно аутентифицировать клиентов Windows. Существуют клиенты Windows Kerberos третьих фирм, не имеющие этого ограничения (которые, следовательно, могли бы аутентифицироваться с помощью сервера Linux Kerberos), но на некоторых клиентов (например, из Национального Центра Суперкомпьютерных приложений — NCSA) было наложено ограничение законами об экспорте США по причине использования сильных алгоритмов шифрования данных.

Регистрация в Windows 98/NT

Каждое утро миллионы пользователей как домашних, так и корпоративных компьютеров, подходят к свои машинам, включают монитор и видят окно, показанное на рис. 4.1.

Пользователь вводит «имя пользователя» (как правило, сохраненное с последнего входа), пароль, домен (обычно уже введен) и нажимает **OK**. Система аутентификации вызывается только при входе в домен, т. е. если авторизация происходит не на локальном компьютере. С помощью системы разрешения имен обнаруживается контроллер домена, к которому осуществляется подключение. Для передачи на сервер аутентификации имени пользователя, хэша пароля и мандата домена в Windows 98 применяется протокол LANMAN, а в Windows NT — протокол NTLM. Сервер аутентификации (на языке Windows NT — главный контроллер домена (PDC) или резервный контроллер домена — (BDC)) анализирует полученную информацию и пытается сравнить

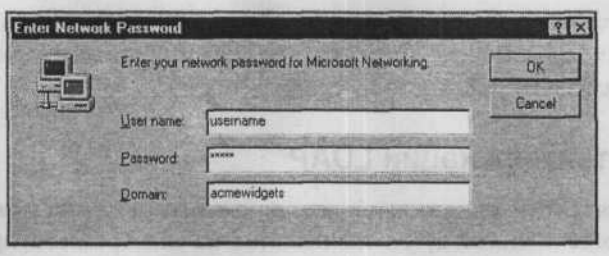

Рис. 4.1. Окно регистрации пользователя в Windows 98

переданные параметры полномочий (мандат) с имеющимися в базе данных SAM (администратор учетных данных в системе защиты). При действительном мандате клиенту передается опознавательный признак (authorization token). При неверном мандате клиенту возвращается сообщение об ошибке. При наличии у пользователя сконфигурированного сетевого профиля с сервера будет загружена его (профиля) копия, если он создан позже локального профиля. При наличии сконфигурированного сценария регистрации этот файл также будет запущен. Доступ к сценариям регистрации обычно осуществляется посредством совместного ресурса NETLOGON.

Регистрация в Windows 2000/XP

Процесс регистрации для Windows 2000/XP похож на процесс в Windows 98/NT. Однако Windows 2000 и Windows XP делают попытку аутентификации Kerberos по умолчанию, хотя они также сохраняют обратную совместимость с аутентификацией NTLM. При попытке аутентификации NTLM процесс практически идентичен процессу регистрации в NT, описанному выше.

Active Directory Windows 2000 обеспечивает Объекты групповых политик (Group Policy Objects, GPO) для применения настроек конфигурации и запуска (или установки) приложений на настольных рабочих станциях Windows 2000/XP. В момент написания данного материала управление / эмуляция GPO были невозможны для открытых реализаций каталогов. Если для нормального функционирования настольных рабочих станций Windows 2000/XP принципиально наличие настроек GPO, то следует воспользоваться другим способом применения настроек и запуска приложений, например перемещением этих функций в сценарий регистрации.

Принципы аутентификации в Linux

Различные формы аутентификации UNIX существуют уже более сорока лет. В настоящее время применяются разнообразные способы аутентификации — от почтенного /etc/passwd до современного PAM для регистрации в рабочих станциях *nix. В данном

разделе рассматриваются методики аутентификации, функционирующие во многих разновидностях Linux. Во многих случаях данная информация также применима к Solaris, BSD, MacOS и HP-UX.

Понятие аутентификации LDAP

Аутентификация LDAP — одна из наиболее широко используемых межплатформенных промышленных технологий аутентификации. Она универсальна, проста в обслуживании и отличается поддержкой надежного шифрования. Как отмечалось выше, службы аутентификации часто интегрируются со службами каталогов. В случае с LDAP служба аутентификации является службой каталога. В небольших компаниях с несложными требованиями к аутентификации в качестве сервера аутентификации для систем *nix часто используется OpenLDAP.

Несмотря на простоту, аутентификация LDAP имеет недостатки, если используется только как служба аутентификации. LDAP никогда не предназначался для использования исключительно в качестве промышленного протокола аутентификации, как LANMAN и Kerberos. LDAP не задействует те же опознавательные признаки или компоненты защиты. Следовательно, с помощью одной лишь аутентификации простого связывания LDAP трудно добиться безболезненной одновременной авторизации сразу в нескольких местах.

К счастью, утилиту аутентификации LDAP можно значительно усовершенствовать использованием SASL (простой уровень аутентификации и защиты) и TLS/SSL (защита транспортного уровня / протокол защищенных сокетов). SASL предоставляет обширный набор технологий аутентификации, а TLS/SSL обеспечивает шифрование для обеспечения конфиденциальности данных и пароля (хэша). SASL поддерживает следующие механизмы аутентификации:

- ANONYMOUS;
- CRAM-MD5;
- PLAIN;
- DIGEST-MD5;
- GSSAPI.

Одной из привлекательных особенностей GSSAPI (общий интерфейс прикладного программирования для служб безопасности) является то, что он еще в большей степени расширяет возможности аутентификации SASL, благодаря многофункциональному API (интерфейс прикладного программирования). GSSAPI также позволяет использовать Kerberos в качестве механизма аутентификации. SASL разработан в университете Карнеги-Меллона; дополнительная информация о реализации Cyrus SASL, также созданной в этом университете, доступна по адресу: http://asg.web.cmu.edu/sasl/.

Другой важной функцией аутентификации LDAP является выполнение им роли *наименьшего общего знаменателя* служб аутентификации. Поскольку почти все службы аутентификации могут использовать LDAP для связи с сервером каталогов, в котором сохранены комбинации «имя пользователя/пароль», то часто новые службы аутентификации легко развернуть при наличии сервера LDAP с активизированной поддержкой аутентификации.

Аутентификация /etc/passwd/shadow

Одним из простейших способов управления аутентификацией является использование локального файла, содержащего имена пользователей и пароли. Более безопасным способом управления локальной аутентификацией является шифрование паролей и их сохранение в отдельном файле.

В случае с современной автономной рабочей станцией Linux информация о пользователях сохраняется в /etc/passwd, а информация о паролях — в /etc/shadow. Права доступа к этим файлам позволяют любому пользователю читать /etc/passwd, но только суперпользователь (root) может считывать хэши паролей из /etc/shadow. На рис. 4.2 и 4.3 показаны фрагменты /etc/passwd и /etc/shadow, соответственно.

```
root :x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
dallen:x:1000:1000:david Allen,,,:/home/dallen:/bin/bash
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
```

Рис. 4.2. Информация файла /etc/passwd

```
root:$1$6wDYOdeM$teP1Vco3v9sCG5W4TRbLO.:12655:0:99999:7:::
daemon: *:12590:0:99999:7:::
bin:*:12590:0:99999:7:::
sys:*:12590:0:99999:7:::
lp:*:12590:0:99999:7:::
dallen:$1$hxo7GmPU$kT34Rhw2VV5c0dqjXb.qt.:12655:0:99999:7:::
nobody:*:12590:0:99999:7:::
```

Рис. 4.3. Информация файла /etc/shadow

Как показано на рис. 4.3, системные учетные записи (*daemon*, *bin* и *lp*) не имеют пароля. Пароли для *root* и *dallen* являются хэшами слова «secret».

Аутентификация NIS

Сетевые информационные службы (NIS) идут несколько дальше подхода, основанного на файлах /etc/passwd и /etc/shadow. В случае NIS сервер сохраняет сетевых пользователей, пароли, группы и другую информацию, соответствующую информации, хранящейся в локальных файлах.

Впрочем, NIS имеет несколько недостатков в области безопасности. Во-первых, не используется кодирование. По этой и другим причинам в сетях не рекомендуется использовать аутентификацию на базе NIS. Она спроектирована на заре развития сетевых технологий и не соответствует требованиям современной сетевой защиты. Даже корпорация Sun (разработчик NIS) обозначила «кончину» NIS с выпуском Solaris 10.

NIS+ — это усовершенствованная версия NIS. При наличии клиента NIS+ для Linux для этой операционной системы не существует открытого сервера NIS+, и развитие Linux NIS+ приостановилось. Несмотря на недостатки, NIS по-прежнему остается широко используемым механизмом аутентификации, особенно в старых сетях UNIX, не обновлявшихся для использование более защищенных протоколов.

Настройки аутентификации клиента Linux

До сих пор авторы рассматривали возможности аутентификации Linux, не затрагивая файлов конфигурации клиента Linux. В данном разделе описаны настройки двух важных файлов — nsswitch.conf и ldap.conf. Почти во всех версиях Linux, Solaris, BSD, MacOS и HP-UX эти два файла (вместе с PAM) управляют важными настройками аутентификации для LDAP и glibc.

Понятие Коммутатора службы имен (nsswitch.conf)

Коммутатор службы имен (NSS) — это программная библиотека C, разработанная корпорацией Sun и предназначенная для возвращения атрибутов пользовательских объектов. Позже NSS был расширен включением карт, имеющихся в службе NIS от Sun (хосты, протоколы, passwd, shadow, автоматическое монтирование и т. д.).

Сегодня все они являются обращениями к функциям в библиотеке GNU C Library (glibc). В Linux и других операционных системах, где используется glibc, конфигурация NSS управляется файлом nsswitch.conf, расположенным в каталоге /etc. Nsswitch.conf содержит список баз данных и их источники. При вызове функции glibc для разрешения этих типов объектов каждый источник запрашивается в порядке перечисления в списке. Для файла nsswitch.conf, показанного на рис. 4.4, система сконфигурирована так, что сначала делается попытка использования локальных **файлов**, а если они не могут ответить на запрос, используется **ldap**.

```
#/etc/nsswitch.conf
passwd:     files ldap
shadow:     files ldap
group:      files ldap
hosts:      files ldap
```

Рис. 4.4. Конфигурация NSS

В nsswitch.conf имеются дополнительные типы баз данных, источников и элементы действия для задания гранулярных средств управления процессом поиска. Для получения расширенной информации введите man **nsswitch.conf**.

Настройки конфигурации LDAP (ldap.conf)

Конфигурация LDAP в системе Linux главным образом управляется файлом /etc/ldap.conf. Этот файл содержит настройки, необходимые для связи с сервером LDAP и управления аутентификацией и запросами, используемыми NSS. Настройки в ldap.conf используются модулями nss_ldap и pam_ldap.

На рис. 4.5 показан файл ldap.conf, имеющийся в настольных рабочих станциях с Linux-системой Fedora Core в компании Acme Widgets. В Fedora в эти файлы аутентификации можно легко вносить изменения с помощью authconfig.

```
#entry for server2 is in /etc/hosts file (запись для сервера2 находится
#в файле /etc/hosts)
host server2
#Acme Widgets base BT (directory suffix)
base dc=acmewidgets,dc=com

#Settings for nss_ldap (настройки для nss_ldap)
nss_base_passwd ou=Users,dc=acmewidgets,dc=com
nss_base_shadow ou=Users,dc=acmewidgets,dc=com
nss_base_group ou=Groups,dc=acmewidgets,dc=com
```

Рис. 4.5. Файл ldap.conf настольных систем компании Acme Widgets

Понятие PAM

PAM (Подключаемые модули аутентификации) — это гибкий абстрактный механизм аутентификации, обеспечивающий конфигурацию аутентификации для каждого приложения, которая будет сохранена в файле конфигурации. В результате части приложения, ответственные непосредственно за подтверждение или отклонение

реквизитов пользователя, могут быть выделены в отдельную подсистему, которая может быть динамически перенастроена для поддержки любой схемы аутентификации без перекомпиляции или перестройки самого приложения.

Разработанные корпорацией Sun Microsystems PAM используются в текущей версии Solaris. Реализация Solaris PAM немного отличается от реализации Linux PAM местоположением файлов, кодов ошибок и методологии конфигурации. В данной книге при упоминании PAM авторы имеют в виду Linux PAM. Все современные дистрибутивы Linux, включая Red Hat, Debian, Suse, Mandrake и пр., поддерживают PAM.

В структуре PAM имеется библиотека функций для запросов аутентификации пользователей. Когда приложению необходимо идентифицировать пользователя, оно обращается к соответствующей функции, и подсистема PAM обрабатывает запрос. PAM сделает попытку считывания файла конфигурации PAM для этого приложения, который обычно сохраняется как /etc/pam.d/*названиеприложения*. В некоторых случаях конфигурация может сохраняться в одном файле **(/etc/pam.conf)**. При наличии каталога /etc/pam.d/ большинство реализаций PAM будет игнорировать настройки в /etc/pam.conf.

Файл конфигурации PAM состоит из множества строк, в которых перечислены опознавательные признаки PAM в следующем формате:

```
service-name module-type  control-flag module-path  [args]
```

В системах с несколькими файлами конфигурации PAM в /etc/pam.d/*названиеприложения*, service-name — это просто имя файла конфигурации, и оно не приводится в файле в виде записи. В файлах конфигурации такого типа в качестве первого элемента приводится элемент **module-type**. В табл. 4.1 описывается каждый из этих опознавательных признаков, а также их использование.

Табл. 4.1. Типы опознавательных признаков PAM и их описания

Опознавательный признак PAM	Описание
service-name (название службы)	Название службы или приложения, относящихся к данной записи
module-type (тип модуля)	Тип модуля PAM (auth, account, session или password)
control-flag (контрольный флажок)	Управляет реакцией модуля на успешный или безуспешный запрос PAM
module-path (путь модуля)	Относительный или абсолютный путь к модулю
args (аргументы)	Аргументы для передачи в модуль (не все модули используют аргументы)

Файлы конфигурации PAM разделяют функции аутентификации на четыре типа: аутентификация пользователя (*auth*), наложение ограничений на учетную запись (*account*), запуск/остановка сессии (*session*) и обновление пароля (опознавательного

признака аутентификации) (*password*). Характеристики этих четырех модулей PAM приведены в табл. 4.2.

Табл. 4.2. Типы модулей PAM и их описания

Тип модуля PAM	Описание
auth	Обеспечивает службы аутентификации для установления личности и предоставления полномочий. Модуль auth подтверждает идентичность с помощью мандатов (пароль, биометрические признаки, аппаратные ключи или другие механизмы аутентификации)
account	Управляет характеристиками учетной записи, не относящимися к аутентификации. Модуль account может ограничить доступ или запретить его, исходя из срока действия пароля, времени суток или доступности системных ресурсов
session	Управляет характеристиками запроса, подлежащего выполнению до того, как пользователь получит доступ к службе, либо после окончания использования службы. Модуль session, как правило, выполняет такие задачи, как ведение журнала или подключение/отключение домашнего каталога
password	Используется для обновления опознавательного признака, связанного с пользователем. Модуль password выполняет функцию смены пароля пользователя

Контрольные флажки PAM определяют, как успешная работа или сбой модуля PAM повлияют на стек PAM. В табл. 4.3 приведены четыре типа контрольных флажков.

Табл. 4.3. Контрольные флажки PAM и их описания

Контрольный флажок PAM	Описание
requisite (необходимый)	Сбой модуля requisite сразу прерывает процесс аутентификации, что заканчивается ее сбоем
required (требуемый)	Сбой модуля required приведет к сбою аутентификации, но оставшаяся часть стека будет выполняться
sufficient (достаточный)	Успешное выполнение модуля sufficient приведет к успешной аутентификации, даже при сбое предыдущего требуемого модуля. Сбой модуля sufficient не приведет к сбою аутентификации
optional (опциональный)	Успешная работа или сбой модуля optional не повлияет на успешное выполнение или сбой аутентификации, если модуль optional не является единственным в списке

Для получения дополнительной информации о контрольных флажках, модулях и аргументах PAM введите **man pam** или **man pam.conf** либо обратитесь на сайт www.redhat.com/docs/manuals/enterprise/RHEL-3-Manual/ref-guide/s1-pam-sample-simple.html.

Проектирование служб аутентификации на базе Linux

Проектирование служб аутентификации на базе Linux часто относительно простой процесс. Обычно вопрос заключается только в определении требований аутентификации для компьютерных систем организации и развертывании необходимых серверов аутентификации с определением их размеров, количества и мест расположения.

Несмотря на прямолинейность процесса проектирования служб аутентификации, особую важность приобретает «правильность» его выполнения. Аутентификация — основа безопасности: она подтверждает, действительно ли пользователь является тем, за кого себя выдает. Практически во всех случаях эта операция выполняется через комбинацию «имя пользователя-пароль». Этот метод аутентификации понятен и универсален, однако существуют определенные соображения безопасности, в частности, связанные с управлением паролями.

Из всех служб, где цена ошибки может быть очень высокой, несомненно, основной является аутентификация. Если в компании случится сбой службы аутентификации, то во многих случаях системы попросту перестанут осуществлять регистрацию новых пользователей, и время действия существующих сессий начнет истекать. Если служба аутентификации сохраняет мандаты в каталоге, а сервер каталогов отключается либо отсутствует сетевое соединение между сервером аутентификации и сервером каталогов (если это разные машины), то, как правило, работа службы аутентификации прекращается.

Эти потенциальные проблемы следует принимать во внимание при проектировании инфраструктуры аутентификации. Если сбой в работе службы аутентификации обходится слишком дорого (обычно это так и бывает в компаниях со сравнительно большим штатом сотрудников), то уместной стратегией при проектировании будет повышение доступности служб аутентификации путем создания резервирования в инфраструктуре. Кроме использования отказоустойчивых аппаратных средств, для большинства производств и крупных компаний настоятельно рекомендуется применение нескольких серверов аутентификации (и серверов каталогов).

Для обеспечения повышенной защиты обязательным является применение надежных (устойчивых к взлому) паролей и обязательная смена паролей пользователей. При этом запоминать пароли становится немного сложнее, но эта проблема не идет в сравнение с возможным «взломом» серверов или их неправильной конфигурацией при отсутствии дополнительных уровней защиты. Даже если «взломщику» удается получить закодированные пароли, то он не сможет их декодировать до того, как очередной нужный пароль будет сменен. Во всех организациях, где руководство обращает серьезное внимание на информационную защиту, соответствующие службы

должны требовать от пользователей регулярной смены паролей доступа. Периодичность смены зависит от рода деятельности компании и других специфических аспектов бизнеса, но в большинстве корпораций интервалы смены паролей составляют от одного до шести месяцев.

Проектирование межплатформенных служб аутентификации

Специфика проектирования служб аутентификации зависит от требований. Представленные ниже текст и цифры описывают решения аутентификации для компаний Acme Widgets и Ballystyx Engineering. Так как Acme Widgets необходимо аутентифицировать рабочие станции Windows и Linux, службы аутентификации должны работать одинаково хорошо для обеих платформ. По этой причине в Acme Widgets применяется решение аутентификации на базе Linux с OpenLDAP для сохранения мандатов аутентификации и обеспечения аутентификации LDAP и с Samba для предоставления служб аутентификации NTLM для клиентов Windows. На рис. 4.6 показан проект службы аутентификации компании Acme Widgets.

Рис. 4.6. Проект служб аутентификации компании Acme Widgets

Проект служб аутентификации для компании Ballystyx Engineering основан на тех же принципах, что и для Acme Widgets, но расширен для соответствия потребностям крупной компании. Так же, как и в Acme Widgets, рабочие станции Windows будут использовать аутентификацию NTLM, а системы Linux — простые связывания LDAP с шифрованием TLS. На рис. 4.7 показаны службы аутентификации для Ballystyx Engineering.

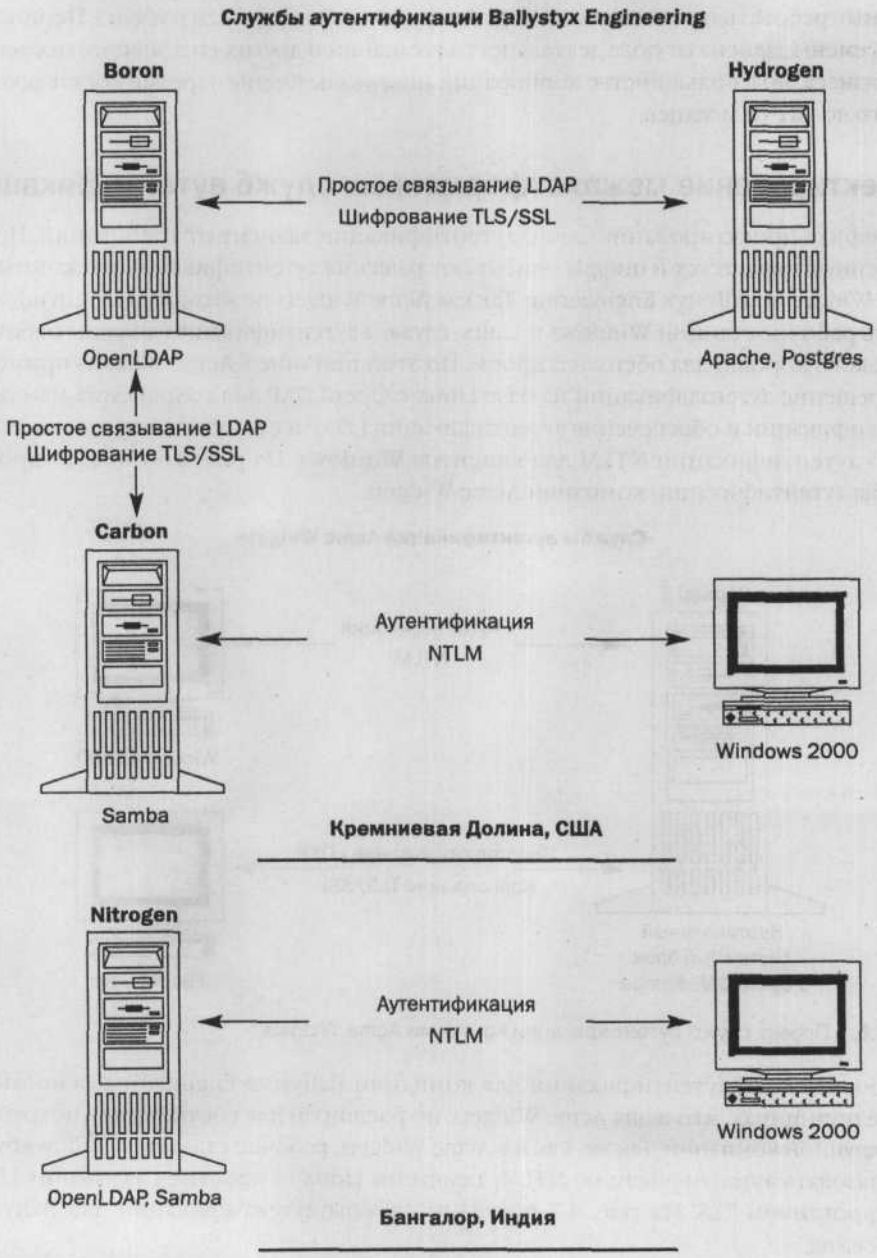

Рис. 4.7. Проект служб аутентификации компании Ballystyx Engineering

Исходя из бюджета, Виджей планирует развертывание дополнительных серверов для обеспечения высокой доступности служб аутентификации. Резервные серверы обеспечат постоянную аутентификацию, благодаря чему сисадмин будет спать спокойно, даже если один из серверов вдруг выйдет из строя среди ночи (последнее представляется сомнительным, — *прим. науч. ред.*).

Установка и конфигурирование Samba

Установка и конфигурирование Samba — первый шаг обеспечения аутентификации NTLM. Скомпилируйте и установите на испытательном сервере существующий пакет сервера Samba (версия 3.0.6 на время написания книги) либо установите пакет сервера Samba из вашего дистрибутива Linux. При самостоятельном компилировании самого последнего пакета Samba следует помнить, что проще использовать пакет, представленный на дистрибутиве Linux.

После установки Samba запустите текстовый редактор и отредактируйте файл smb.conf. Альтернативным способом редактирования файла может быть выбор инструмента графической конфигурации (Webmin — www.webmin.com) или SWAT (Samba Web Administration Tool). На рис. 4.8 показан файл smb.conf для компании Acme Widgets. В качестве отправной точки рекомендуется использовать образец, представленный в Инструментарии перехода от Windows к Linux.

Для служб Samba в компании Acme Widgets используется тот же хост, что и для служб LDAP. Если эти приложения установлены на нескольких машинах, то файлу конфигурации необходимо сделать ссылку на другой сервер по его DNS-имени или по IP-адресу. Полное описание этих настроек для smb.conf можно получить на странице руководства **man smb.conf**, однако некоторые настройки заслуживают рассмотрения в данном разделе. В первых нескольких строках видно, что данная установка Samba взаимодействует с LDAP (облегченный протокол службы каталогов) и что части файла smb.conf, отвечающие за настройку LDAP, соответствуют конфигурационному файлу сервера каталогов slapd.conf. Приведен каталог LDAP — admin dn (в терминологии slapd.conf — rootdn), а также суффикс и организационные единицы, содержащие пользователей, группы и компьютеры. Эти настройки соответствуют дереву информационных каталогов компании Acme Widgets, заданному в главе 3. Также заслуживают объяснения настройки **domain logins = yes** и **domain master = no**. Данная конфигурация превращает сервер Samba в резервный контроллер домена для права получения копии объектов аутентификации из существующего домена Windows. По завершении процесса перехода и сброса Windows PDC (главный контроллер домена) сисадмин (Сэм) изменит значение записи **domain master** на «**yes**» и перезапустит Samba. При этом сервер Samba из подчиненного (BDC) превратится в главный (PDC). Подробно данная процедура описана ниже, в разделе о переносе.

```
[global]
    workgroup = ACMEWIDGETS
    netbios name = SERVER2
    server string = Samba Server
    passdb backend = ldapsam:ldap://127.0.0.1/
    idmap backend = ldap:ldap://127.0.0.1/
    ldap admin dn = cn=Manager,dc=acmewidgets,dc=com
    ldap suffix = dc=acmewidgets,dc=com
    ldap group suffix = ou=Groups
    ldap user suffix = ou=Users
    ldap machine suffix = ou=Computers
    ldap idmap suffix = ou=Users
    ldap ssl = no
    security = user
    domain logons = yes
    domain master = no
    log file = /var/log/samba/%m.log
    max log size = 50
    socket options = TCP_NODELAY SO_SNDBUF=8192 SO_RCVBUF=8192
    dns proxy = No
    wins support = No
    preferred master = Yes
    add user script = /usr/local/sbin/smbldap-useradd -m "%u"
    ldap delete dn = Yes
    delete user script = /usr/local/sbin/smbldap-userdel "%u"
    add machine script = /usr/local/sbin/smbldap-useradd -w "%u"
    add group script = /usr/local/sbin/smbldap-groupadd -p "%g"
    delete group script = /usr/local/sbin/smbldap-groupdel "%g"
    add user to group script = /usr/local/sbin/smbldap-groupmod -m "%u" "%g"
    delete user from script = /usr/local/sbin/smbldap-groupmod -x "%u" "%g"
    set primary group script = /usr/local/sbin/smbldap-usermod -g "%g" "%u"
```

Рис. 4.8. Файл smb.conf компании Acme Widgets

Настройки сценариев в smb.conf соответствуют инструментальным средствам IDEALX smbldap, процесс установки которых описан в разделе о переносе. Обратите внимание, что физический путь к набору инструментов smbldap может варьироваться в зависимости от способа установки. Если установка осуществлялась из файла tar.gz, то путь будет /usr/local/sbin, если из пакета RPM, то путь будет /usr/sbin. Самым простым способом определения этой информации является ввод в приглашении на ввод команды строки **which smbldap-useradd** и запись выданного этой программой пути. Если эти настройки некорректны, то переход к Samba и последующее техническое обслуживание не будут функционировать, как положено!

На рис. 4.9 приведены листинги совместно используемых сетевых ресурсов Samba в файле smb.conf, соответствующие домашнему каталогу, регистрации в сети и сохранению сетевого роуминга для служб регистрации Windows.

```
[homes]
        comment = Home Directories
        read only = No
        browseable = No
        create mask = 0644
        directory mask = 0775

[netlogon]
        path = /home/netlogon/
        browseable = No
        read only = yes

[profiles]
        path = /home/profiles
        read only = no
        create mask = 0600
        directory mask = 0700
        browseable = No
        guest ok = Yes
        profile acls = yes
        csc policy = disable
        # secures profiles by user
        force user = %U
        # allow administrative access to profiles
        valid users = %U @"Domain Admins"
```

Рис. 4.9. Совместно используемые ресурсы Samba компании Acme Widgets

После установки сервера Samba убедитесь в его нормальном запуске. Для большинства дистрибутивов Linux следующие команды запускают службы Samba и показывают подробности их текущего состояния:

```
/etc/init.d/smb start
/etc/init.d/smb status
/usr/bin/smbstatus -v
```

При отсутствии ошибок конфигурация Samba должна быть корректной. Для запуска сценариев перехода службы Samba необходимо отключить. Перед тем, как перейти к разделу переноса (миграции) остановите работу сервера Samba. В большинстве дистрибутивов Linux службы Samba останавливаются с помощью следующей команды:

```
/etc/init.d/smb.stop
```

Переход от NT/Exchange или Active Directory

В данном разделе описаны подробности переноса служб каталогов и аутентификации из Windows NT, Exchange 5.5, Windows 2000 и/или Active Directory в службы каталогов и аутентификации на базе Linux. Раздел требует корректной конфигурации серверов Samba и OpenLDAP. Службу Samba необходимо остановить, а сервер OpenLDAP должен находиться в рабочем состоянии.

Функционально процессы переноса домена Windows NT (с Exchange или без него) и Active Directory одинаковы. Они выполняются в два этапа. Сначала сценарии получают копию информации аутентификации и вставляют эти объекты в каталог. На втором этапе сценарии получают списки контактов и группы распределения, а также пользовательскую информацию, не связанную с аутентификацией, после чего эта информация вставляется в каталог.

Подготовка к процессу перехода

Для подготовки сервера (серверов) для перехода необходимо выполнить несколько дополнительных шагов. Во-первых, установите smbldap-tools из IDEALX (http://samba.idealx.org). При этом в зависимости от устанавливаемого пакета сценарии smbldap будут помещены в /usr/local/sbin или /usr/sbin, а файлы конфигурации — в /etc/smbldap-tools/. Убедитесь в том, что используется версия smbldap-tools не ниже 0.8.5. Несмотря на очевидную пользу конфигурирования с обучающей точки зрения, конфигурировать smbldap-tools на данном этапе необходимости нет, потому что нижеприведенные сценарии переноса сделают это самостоятельно.

Компоненты Samba будут использоваться для получения объектов аутентификации, а данный сервер, скорее всего, будет осуществлять поддержку учетных записей samba в будущем, поэтому очень важно убедиться в правильности его конфигурации для аутентификации на целевом сервере LDAP. Эта операция обычно выполняется через файлы /etc/pam.d/samba, /etc/ldap.conf и /etc/nsswitch.conf, описанные выше в разделе «Принципы аутентификации в Linux». Для выполнения ее на рабочих станциях компании Acme Widgets с системой Fedora Сэм просто ввел строку **authconfig** и соответствующие значения LDAP.

ПРИМЕЧАНИЕ Неправильная настройка упомянутых выше компонентов приведет к заполнению каталога информацией об учетных записях posix, которая будет непригодна к использованию (в результате запуска сценариев переноса) и нарушит настройки аутентификации сервера Samba.

На данном этапе перехода необходимо иметь корректно установленный и сконфигурированный сервер Samba (не запущенный) и установленный на локальной машине инструментальный набор IDEALX smbldap (не обязательно сконфигурированный). Помимо этого, сервер OpenLDAP должен иметь корректно сконфигурированный файл slapd.conf, как описано в главе 3, и *сервер каталогов ДОЛЖЕН быть запущен*. В небольшой компании, подобной Acme Widgets, все службы выполняются на одном сервере. В Ballystyx Engineering OpenLDAP и Samba работают на разных серверах.

Теперь можно перейти к соответствующему разделу описания, в зависимости от типа перехода (от Windows NT или Windows 2000).

Путь перехода NT / Exchange 5.5

В Windows NT в базе данных SAM сохранен ограниченный объем пользовательской информации. Информация об электронной почте пользователя, местоположении, номер телефона и другая контактная информация должна сохраняться за пределами SAM, в каталоге Exchange 5.5. Для переноса информации Exchange 5.5 для соотнесения объектов аутентификации с соответствующей информацией Exchange сценариям потребуется соотнесение *пользователя с картой почтового ящика*. Эту карту можно получить через функцию Directory Export программы-администратора Exchange 5.5. Необходимо использовать внешний файл, потому что отображение в виде карты между почтовым ящиком Exchange и соответствующей учетной записью Windows NT не проявляется в интерфейсе LDAP Exchange 5.5. Если не осуществляется переход от Exchange и/или заполнить необходимо только объекты аутентификации, то следующий шаг можно пропустить.

Для получения информации из каталога Exchange 5.5 запустите администратор Exchange 5.5 (обычно c:\exhsrvr\admin.exe). Для запуска администратора выберите Start / Programs / Microsoft Exchange / Microsoft Exchange Administrator.

Для извлечения информации о почтовом ящике пользователя из каталога Exchange выполните экспорт каталога всех пользовательских почтовых ящиков в Глобальный список адресов (GAL) выбором Tools / Directory Export. На рис. 4.10 показана подготовка программы-администратора Exchange 5.5 к экспорту каталога Acme Widgets.

Обратите внимание, что экспортировать следует только объекты почтовых ящиков, поскольку при этом передается учетная информация о карте, необходимая для процесса переноса. Остальные данные о группе, контактах и пользовательской информации будут получены через LDAP.

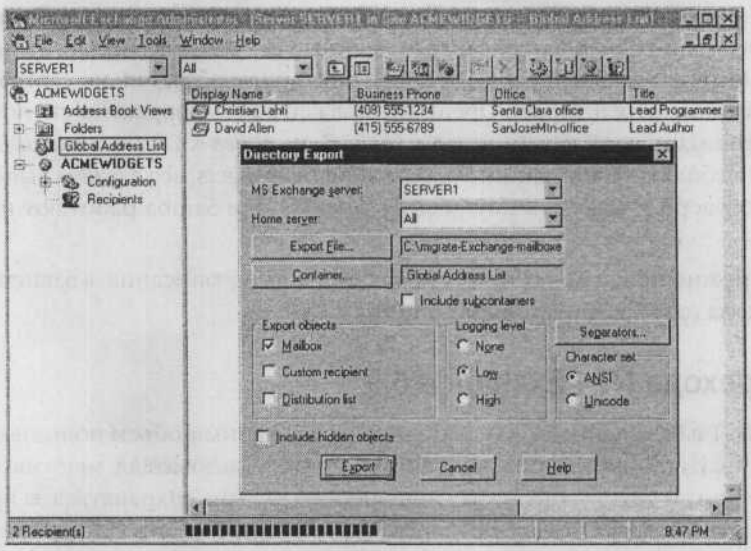

Рис. 4.10. Экспорт каталога Exchange 5.5

Теперь все готово для запуска первого сценария — w2lmt-migrate-smbauth — предназначенного для извлечения информации аутентификации. Этот сценарий требует использования файла конфигурации, хотя последующие версии сценария могут выдавать запросы по поводу требуемой информации при отсутствии файла конфигурации. На рис. 4.11 приведен файл конфигурации для компании Acme Widgets.

```
#migrate-smbauth-acmewidgets.conf
#information about source server and target server (информация об исходном
#и целевом сервере)
SourceHost="server1"
SourceDomain="ACMEWIDGETS"
SourceType= "NT4"
SourceAdminAccount="Administrator"
TargetHost="localhost"
TargetPort="389"

#locations of config files for samba and smbldap-toolkit (местоположения
#файлов конфигурации для samba и инструментального набора smbldap)
smbconf=" /etc/samba/smb.conf"
smbldap="/etc/smbldap-tools/smbldap.conf"
```

Рис. 4.11. Файл конфигурации migrate-smbauth компании Acme Widgets

Информация, содержащаяся в конфигурации migrate-smbauth, сравнительно очевидна. Сценарию должно быть известно местоположение файлов конфигурации для считывания/внесения изменений, а также то, какие хосты участвуют в процессе перехода. Для выполнения перехода на серверах компании Acme Widgets Сэм пользуется следующей командой:

```
/<path_to_scripts>/w2lmt-migrate-smbauth -f migrate-smbauth-acmewidgets.conf
```

Данная команда выполняет следующие действия.

- Проверяет наличие всего необходимого для продолжения.
- Выдает приглашение к вводу паролей как к исходному серверу NT, так и к целевому серверу OpenLDAP.
- Перечисляет идентификаторы защиты (SID) домена.
- Приглашает к вводу настроек по умолчанию (с опцией изменения/сохранения).
- Присоединяет к домену NT в виде BDC.
- Создает при необходимости организационные единицы высшего уровня в OpenLDAP.
- Вызывает компоненты Samba для извлечения пользователей, групп и машинных объектов с последующей их вставкой в сервер OpenLDAP.
- Обрабатывает информацию группового членства и модифицирует групповые объекты для добавления информации об uid (идентификаторе пользователя).

Когда каталог заполнен объектами аутентификации пользователей, следующим шагом является запуск w2lmt-directory-auth. Этот сценарий запросит сервер Exchange для обновления объектов каталогов любой сохраненной в нем нужной информацией. Этот сценарий также добавляет объекты контактов и группы распределения. Если сервер Exchange не используется или нет необходимости переноса этой информации в среду Linux, то данный шаг можно пропустить. Этот сценарий требует короткого файла конфигурации. На рис. 4.12 показан файл конфигурации каталога переноса для компании Acme Widgets.

```
#migrate-directory-acmewidgets.conf
#information about target LDAP instance (информация о целевом
#экземпляре LDAP)
SlapdPath="/etc/openldap/slapd.conf"
TargetPort="389"

#specify the relative DN here for user objects in the target LDAP
#instance. (здесь указывается относительное отличительное имя для
#объектов в целевом экземпляре LDAP)
```

▶▶

```
#you can use a different DN if you want your exchange contacts
#separate your User/Group DN. (ex.) Users would equal (можно
использовать другое отличительное имя, если необходимо отделить
контакты обмена от отличительного имени Пользователь/Группа)
'ou=Users, dc=acmewidgets,dc=com'
UsersOU="ou=Users"
ContactsOU="ou=Contacts"
GroupsOU="ou=Groups"
DistributionGroupsOU="ou=DistributionGroups"

#information about import directory (if any) (информация о
#каталоге импорта (если есть))
#valid entries are EXCH55, AD
SourceType="EXCH55"
SourceHost="server1"
SourceAdminAccount="Administrator"

#if import directory is exhange55, a map file is required (если
#каталог импорта - exchange55, тогда требуется файл с картой
#соответствия)
Exchange55CSV="/tmp/acmewidgets-exch55.csv"
```

Рис. 4.12. Файл конфигурации каталога переноса для компании Acme Widgets

Представленная выше информация конфигурации содержит запрашиваемый сценарием хост Exchange и описывает в дереве информации каталога место размещения контактов и групп распределения. Часть информации сценарий получает из файла slapd.conf, поэтому он должен выполняться на сервере каталогов. Вот как Сэм вызвал сценарий в компании Acme Widgets:

```
/<path_to_scripts>/w2lmt-migrate-directory -f migrate-directory-
acmewidgets.conf
```

Данный сценарий выполняет следующие действия.

- Проверяет наличие всего необходимого для продолжения процесса.
- Выдает приглашение к вводу паролей как к исходному серверу Exchange, так и к целевому серверу OpenLDAP.
- Добавляет при необходимости организационные единицы высокого уровня для контактов и групп распределения в OpenLDAP.
- Считывает предоставленный файл экспорта Exchange (.csv).

- Перечисляет все объекты персонального почтового ящика.
- Определяет, является объект контактом или отображаемым идентификатором пользователя (uid) NT (обратите внимание, что при нескольких почтовых ящиках, соответствующих одному uid, приоритет имеет последний, и для данного uid остается информация именно этого почтового ящика).
- Обновляет совпадающий объект пользователя в OpenLDAP с такими атрибутами, как адрес, электронная почта, номер телефона и т. д., ЛИБО добавляет его в виде контакта (по обстановке).
- Перечисляет группы распределения.
- Создает в OpenDLAP объекты, заполненные атрибутами groupOfNames.
- Обрабатывает информацию о членстве в группах распределения с контактами или отличительными именами пользователей (по обстановке).

Теперь в наличии должен быть заполненный каталог, содержащий полную информацию об аутентификации и каталогах из предыдущего домена NT и экземпляра Exchange 5.5. Все, что осталось сделать, — это изменить настройку samba smb.conf, для того, чтобы сервер Linux для домена стал главным (PDC), отключить изначальный PDC и перезапустить службы samba.

Путь перехода Active Directory

Теперь все готово для запуска первого сценария — w2lmt-migrate-smbauth, — созданного для извлечения информации аутентификации. Этот сценарий требует использования файла конфигурации, хотя в более поздних версиях сценария, при отсутствии файла конфигурации, он сможет запросить нужную информацию самостоятельно. На рис. 4.13 показан файл конфигурации для компании Ballystyx.

Примечание Если Active Directory выполняется в ***смешанном режиме*** (Mixed Mode), то в файле конфигурации сценария w2lmt-migrate-smbauth в качестве **SourceType** следует использовать настройку NT4. При использовании этой настройки сохраняются SID (идентификаторы защиты) и RID существующего домена. При выполнении Active Directory в ***«родном» режиме*** (Native Mode) сценарии будут создавать новый домен с новыми SID и RID для пользователей, групп и машин. Это происходит потому, что собственный режим Active Directory не совместим с доменом типа Samba NT4, на который осуществляется переход. Следует помнить о том, что все объединенные в этом домене машины необходимо повторно объединять в новый домен на базе Linux.

```
#migrate-smbauth-ballystyx.conf
#information about source server and target server (информация
#об исходном и целевом серверах)
SourceHost="beryllium"
SourceDomain="BALLYSTYX"
SourceType="AD"
SourceAdminAccount="Administrator"
TargetHost="localhost"
TargetPort="389"

#locations of config files for samba and smbldap-toolkit
#(местоположения файлов конфигурации для samba и
#инструментального набора smbldap)
smbconf="/etc/samba/smb.conf"
smbldap="/etc/smbldap-tools/smbldap.conf"
```

Рис. 4.13. Файл конфигурации migrate-smbauth для компании Ballystyx

Приведенная выше информация очевидна; сценарию необходимо сообщить местоположение файлов конфигурации, а также хосты, с которыми он будет взаимодействовать при переходе. Команда, представленная ниже, показывает, как Виджей активизирует сценарий на сервере Samba компании Ballystyx Engineering:

```
/<path_to_scripts>/w2lmt-migrate-smbauth -f migrate-smbauth-
ballystyx.conf
```

Сценарий выполняет следующие действия.

- Проверяет наличие всего необходимого для продолжения.
- Приглашает к вводу паролей как к исходному серверу NT, так и к целевому серверу OpenLDAP.
- Перечисляет идентификаторы защиты (SID) домена.
- Приглашает к вводу настроек по умолчанию (с опцией их изменения/сохранения).
- Присоединяет к домену NT в виде BDC.
- Создает при необходимости организационные единицы высшего уровня в OpenLDAP.
- Перечисляет групповые объекты.
- Создает групповые объекте в OpenLDAP, заполненном атрибутами posixGroup и sambaGroupMapping.

- Перечисляет объекты учетных записей компьютеров (хостов, присоединенных к существующему домену).
- Создает объекты учетной записи компьютера в OpenLDAP с заполненными атрибутами для inetOrgPerson, posixAccount и sambaAccount.
- Перечисляет все объекты аутентификации (пользователей).
- Создает пользовательские объекты в OpenLDAP с заполненными атрибутами для inetOrgPerson, posixAccount и sambaAccount.
- Обрабатывает информацию группового членства и модифицирует групповые объекты для добавления информации об uid (идентификаторов пользователя).

Следующим шагом является запрос сервера Active Directory для обновления вышеперечисленных объектов информацией, не относящейся к аутентификации (электронная почта, номера телефонов и прочая контактная информация), а также для получения информации о контактном объекте и группе распределения. При отсутствии необходимости сохранения этой информации в новой среде Linux этот шаг можно пропустить. Следующий сценарий также требует короткого файла конфигурации. На рис. 4.14 приведен файл конфигурации каталога перехода для компании Ballystyx.

```
#migrate-directory-ballystyx.conf
#information about target LDAP instance (информация о целевом
#экземпляре LDAP)
SlapdPath="/etc/openldap/slapd.conf"
TargetPort="389"

#specify the relative DN here for user objects
#in the target LDAP instance. (здесь указывается относительное
#отличительное имя для объектов в целевом экземпляре LDAP)
#you can use a different DN if you want your
#exchange contacts separate (можно использовать другое
#отличительное имя, если необходимо отделить контакты обмена от)
#your User/Group DN. (отличительных имен Пользователь/Группа)
#(ex.) Users would equal
'ou=Users, dc=ballystyx,dc=com'
UsersOU="ou=Users"
ContactsOU="ou=Contacts"
GroupsOU="ou=Groups"
DistributionGroupsOU="ou=DistributionGroups"
```

▶▶

```
#information about import directory (if any) (информация об
#импортируемом каталоге (если есть))
#valid entries are EXCH55, AD
SourceType="EXCH55"
SourceHost="beryllium"
SourceAdminAccount="Administrator"

#if import directory is exhange55, a map file is required (если
#каталог импорта - exchange55, тогда требуется файл с картой
#соответствия)
Exchange55CSV=
```

Рис. 4.14. Файл конфигурации каталога переноса для компании Ballystyx

Представленный выше файл конфигурации обычно представляет сценарию информацию о хосте Active Directory, с которым будет производиться связь, и описывает в дереве информации каталога (DIT) место размещения контактов и групп распределения. Часть информации сценарий получает из файла slapd.conf, поэтому он должен выполняться на сервере каталогов. Нижеприведенная команда показывает, как Виджей вызывает сценарий на сервере Samba в компании Ballystyx Engineering:

```
/<path_to_scripts>/w2lmt-migrate-directory -f migrate-directory-
acmewidgets.conf
```

Данный сценарий выполняет следующие действия.

- Проверяет наличие всего необходимого для продолжения процесса.
- Приглашает к вводу паролей как к исходному серверу Exchange, так и к целевому серверу OpenLDAP.
- Добавляет при необходимости организационные единицы высшего уровня для контактов и групп распределения в LDAP.
- Перечисляет группы распределения.
- Создает объекты в OpenLDAP, заполненные атрибутами groupOfNames.
- Перечисляет все объекты персонального почтового ящика.
- Обновляет совпадающие объекты пользователя в OpenLDAP с такими атрибутами, как адрес, электронная почта, номер телефона и т. д.
- Обрабатывает информацию о членстве в группах распределения для пользователя.
- Перечисляет все контактные объекты.
- Создает контактный объект в OpenLDAP с атрибутами для inetorgPerson, электронной почты, номеров телефонов и т. д.
- Обрабатывает информацию о членстве в группах распределения для контактов.

Теперь в наличии должен быть заполненный каталог, содержащий полную информацию аутентификации и каталогов из предыдущего домена NT и экземпляра Exchange 5.5. Все, что осталось сделать, — это изменить настройку Samba smb.conf, для того, чтобы сделать сервер Linux для домена главным (PDC), отключить изначальный PDC и перезапустить службы samba. Поскольку это новый домен, то в него потребуется включить оставшиеся серверы Windows 200x и рабочие станции (если таковые имеются).

Перенос файлов аутентификации при регистрации в Windows

Любые сценарии регистрации, используемые в организации, необходимо копировать из совместного ресурса NETLOGON (обычно расположен в C:\WINNT\System32\Repl\Import\Scripts\) в новое местоположение ресурса NETLOGON на сервере Samba Linux (путь по умолчанию: /home/netlogon/).

Кроме этого, при использовании сетевых профилей, файлы и каталоги, обнаруженные в каталоге профилей пользователей (включая NTUSER.DAT или USER.DAT, NTUSER.INI и др.), также необходимо копировать в соответствующий совместно используемый каталог на сервере Samba Linux (путь по умолчанию: /home/profiles/).

Для регистрации в Windows использование домашних каталогов не является строгим условием, хотя для домашнего каталога Windows обеспечивает подключение сетевого диска. Перенос содержимого домашних каталогов описан в главе 5 «Файловые службы».

Тестирование служб аутентификации

Следующим шагом после завершения переноса является тестирование служб аутентификации на базе Linux. Попробуйте зарегистрироваться с рабочей станции с помощью сервера Samba (настроенного на испытательном сервере) для аутентификации. Если это сработает, попробуйте зарегистрироваться под другими именами пользователей и убедитесь в выполнении сценариев регистрации и надлежащем обновлении информации о профиле пользователя (роуминга).

Активизация шифрования

Перед использованием этих систем для аутентификации в производственной среде необходимо активизировать шифрование. Поскольку это сложная задача, то для начала рекомендуется настроить корректную работу служб аутентификации без шифрования. Протестируйте функции регистрации на компьютерах с системами Windows и Linux. После верификации корректной работы служб аутентификации можно добавлять элементы шифрования для обеспечения надлежащей защиты.

Основные шаги активизации шифрования.

1. Получение и установка действительного сертификата сервера.
2. Конфигурирование slapd.conf для использования сертификата сервера и запрос TLS.
3. Конфигурирование smb.conf для использования TLS.
4. Конфигурирование клиентов для использования TLS.
5. Тестирование, тестирование и еще раз тестирование!

Сертификат сервера можно получить в любой Службе выдачи сертификатов (CSA), например в Verisign или CA-Cert, либо создать собственный посредством OpenSSL. Процесс создания сертификата OpenSSL описан в главе 9. После установки сертификата сервера для его использования необходимо внести изменения в файл конфигурации сервера. Дополнительная информация по конфигурации, необходимая для активизации TLS для компании Acme Widgets, приведена на рис. 4.15, 4.16, 4.17.

```
TLSCertificateFile /etc/openldap/server.pem
TLSCertificateKeyFile /etc/openldap/server.key
TLSCACertificateFile /etc/openldap/ca.pem
TLSCipherSuite :SSLv3
TLSVerifyClient demand
```

Рис. 4.15. Раздел кодирования файла конфигурации slapd.conf компании Acme Widgets

```
ldap ssl = yes
```

Рис. 4.16. Директива кодирования файла конфигурации smb.conf компании Acme Widgets

```
ssl             start_tls

TLS_REQCERT     allow
```

Рис. 4.17. Настольный клиент ldap.conf компании Acme Widgets

Если файлы конфигурации содержат ссылки ldap://URI, то их нужно изменить на ldaps://URI. Убедитесь в наличии нужных опций TLS при перезапуске slapd. Например:

```
slapd -h ldap://127.0.0.1/ ldaps:///
```

как правило, срабатывает. Пользователям Fedora потребуется обновить файл /etc/sysconfig/ldap опцией ldap:///.

Следующим шагом является повторное тестирование служб аутентификации с активизированным шифрованием. Оперативным методом тестирования работоспособности TLS на Acme Widgets является ввод следующей строки:

```
ldapsearch -x -H ldaps://localhost -b 'dc=acmewidgets,dc=com'
'(objectclass=*)'
```

Резюме

Аутентификация представляет собой одну из важнейших сетевых служб. Возможность идентификации пользователя и управления доступом к сетевым ресурсам формирует базовые средства защиты, лежащие в основе корпоративных сетей. В большинстве случаев аутентификация пользователей заключается в подтверждении мандатов, состоящих из одного или нескольких факторов: чего-то известного вам (имя пользователя, пароль), чего-то имеющегося у вас в наличии (аппаратный ключ) либо чего-то, чем вы являетесь (биометрическая идентификация). Если каталог OpenLDAP служит централизованным хранилищем информации аутентификации, тогда можно создать гибкие методологии аутентификации, которые бы обеспечивали централизованное управление распределенными разнородными службами аутентификации.

Корпорация Microsoft использовала протоколы LANMAN для осуществления аутентификации в Windows 98 и NT и добавила службы аутентификации Kerberos для Windows 2000/XP. В настоящее время не существует открытых служб аутентификации, обеспечивающих службы регистрации Kerberos готовым клиентам Windows 2000/XP. Серверы Samba обеспечивают службы аутентификации NTLM / LANMAN, которые может использовать все семейство клиентов и серверов Windows (Windows 98/NT/2000/XP).

Перенос информации Windows NT и Exchange 5.5 обычно достаточно прост, особенно при наличии прямого соответствия между учетными записями NT и почтовыми ящиками Exchange. Сценарии переноса легко свяжут эти два каталога для обеспечения унифицированного представления всех пользовательских данных в OpenLDAP. Новый домен, управляемый Samba, обеспечивает все функции домена Windows NT и даже больше.

Перенос информации Windows 2000 Active Directory, как правило, работает корректно, однако, при использовании Exchange 2000 или при невозможности переноса служб MS-DNS, интегрированных с AD, описанного в предыдущей главе, необходимо запускать службы каталогов на базе Linux параллельно до переноса зависимостей Active Directory. При использовании Active Directory в «родном» режиме (native mode) потребуется повторно интегрировать все компьютеры с системой Windows в новый домен, управляемый Linux.

Краткое резюме по разделам

Принципы аутентификации в Windows

- ☑ Для регистрации в Windows пользователь вводит имя, пароль и домен. Аутентификация в Windows 98 осуществляется с помощью протокола LANMAN, в Windows NT — NTLM, а в Windows 2000/XP применяется аутентификация Kerberos и поддерживается обратная совместимость с NTLM.
- ☑ После успешной аутентификации Windows обновляет сетевой профиль (если он сконфигурирован) и запускает сценарии регистрации.
- ☑ Для применения настроек конфигурации и запуска (или установки) программных приложений Windows 2000 может использовать Объекты групповой политики.

Принципы аутентификации в Linux

- ☑ Аутентификация LDAP — одна из самых гибких, поддерживаемых и широко используемых межплатформенных методик аутентификации в корпоративных средах. Утилиту аутентификации LDAP можно расширить с помощью Простого уровня аутентификации и защиты (SASL).
- ☑ Одним из простейших способов аутентификации является использование локальных файлов. Использование файла /etc/passwd для хранения пользовательской информации и /etc/shadow — для хранения паролей пользователей — самый простой способ выполнения локальной аутентификации.
- ☑ Файлы /etc/nsswitch.conf, /etc/ldap.conf и /etc/pam.d/*названиеприложения* содержат информацию конфигурации механизмов аутентификации, применяемых в компьютерах с системой Linux и во многих компьютерах *nix.
- ☑ Съемные модули аутентификации (PAM) — это гибкий абстрактный механизм аутентификации пользователей. PAM выделяет определенные части программного приложения, отвечающие за фактическое предоставление доступа в подсистему, доступную для переконфигурирования динамическим способом путем изменения файла /etc/pam.d/*названиеприложения*.

Проектирование служб аутентификации на базе Linux

- ☑ Первым шагом в проектировании служб аутентификации на базе Linux является определение требований аутентификации для компьютерных систем организации. Для большинства предприятий это означает использование LDAP/TLS в системах Linux и NTLM (посредством Samba) для систем Windows.
- ☑ Следующий шаг — определение типа, местоположения и количества серверов аутентификации в организации. Для маленьких компаний (Acme Widgets) достаточно одного сервера аутентификации. Для крупных компаний, таких как Ballystyx Engineering, требуется по одному серверу аутентификации для каждого филиала. Для отказоустойчивых установок требуется минимум два сервера на каждую.
- ☑ Последним шагом перед развертыванием является установка, конфигурирование и тестирование служб аутентификации на испытательном сервере. Установите систему Samba и сконфигурируйте smb.conf.

Переход от NT/Exchange или Active Directory

- ☑ Для подготовки к переходу убедитесь, что сервер Samba сконфигурирован для аутентификации с помощью протокола LDAP, а также установите smbldap-tools из IDEALX (http://samba.idealx.org).
- ☑ Если для переноса будет использоваться информация из Exchange 5.5, выполните экспорт каталога почтовых ящиков в Глобальный адресный список (GAL) Exchange 5.5 выбором в программе-администраторе Microsoft команд **Tools / Directory Export**.
- ☑ Для заполнения Samba и OpenLDAP информацией о пользователях, группах и компьютерах, переносимой из NT / Exchange или Active Directory, запустите сценарии migrate-smbauth и migrate-directory. Внимательно следуйте инструкциям и обратитесь к сайту http://sourceforge.net/projects/w2lmt для получения последних версий сценариев.
- ☑ После верификации функциональности служб аутентификации путем тестирования в испытательной лаборатории активизируйте шифрование для обеспечения дополнительной защиты. Получите и установите сертификат сервера OpenSSL и сконфигурируйте приложения для активизации кодирования TLS.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма «**Ask the Author**»). Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: В моей системе ДВА файла ldap.conf. Почему?

О: etc/ldap.conf используется pam_ldap и nss_ldap для конфигурации параметров LDAP на уровне системы, включая аутентификацию. /etc/openldap/ldap.conf (или /etc/ldap/ldap.conf) используется утилитами OpenLDAP, такими как ldapsearch.

В: Зачем повторно интегрировать Windows 200x в домен, управляемый Samba, после перехода из Active Domain, выполняющегося в родном режиме?

О: По причине того, что родной режим Active Domain использует другую схему SID/RID, нежели NT SAM, перенести идентификаторы дескриптора объекта в управляемый Samba домен в стиле NT невозможно.

Глава 5

Файловые службы

Разделы:

- Понятие файловых систем Windows
- Понятие файловых систем Linux
- Понятие управления полномочиями (управления доступом)
- Понятие создания резервных копий файлов, их восстановления и возможностей репликации
- AMANDA
- Проектирование файловых служб на базе Linux
- Перенос файловых служб в систему Linux

☑ Краткое резюме по разделам

☑ Часто задаваемые вопросы

Введение

Файловые службы — это термин, применяемый при описании доступа к файлам удаленной системы. Большинство организаций использует сетевое хранилище общедоступных данных, включая домашние каталоги, файлы подразделений и файлы ресурсов компании. Сетевое хранилище должно быть защищено от несанкционированного доступа с помощью систем управления доступом; данные должны быть защищены от утери или повреждения созданием их резервных копий, при использовании должны соответствовать требованиям конечных пользователей к производительности и быть оптимально структурированными для обеспечения возможности их пополнения. При наличии многих типов файловых служб в Linux Samba является наиболее реальным решением поддержки клиентов Windows на сервере Linux. Сложностью такого преобразования является незаметность переноса данных, совместно используемых ресурсов и списков контроля доступа (ACL) с одновременным обеспечением высокой степени их производительности и защиты.

Понятие файловых систем Windows

Файловые службы обеспечивают сетевой доступ к данным, хранящимся в файловых системах. Каждый тип файловой системы имеет свои особенности и ограничения, влияющие на способ совместного использования данных файловыми службами. Современная операционная система (OS) Microsoft предлагает локальную совместимость с файловыми системами FAT16, FAT32, NTFS4 и NTFS5, а также возможность коллективного использования файлов этих систем по сети по протоколу, называемому Общим протоколом доступа к файлам Интернет (CIFS). В данном разделе подробно рассматриваются указанные файловые системы с выделением преимуществ и особенностей каждой, а также приводится история развития файловых систем корпорацией Microsoft.

Зачем нужны файловые системы? Поверхности дисковых носителей разделены на адресные ячейки (секторы). Разделы на дисках можно создавать группированием секторов. Когда файловая система форматирует раздел, она делает попытку определения структурирования, записи, обнаружения данных, доступа к ним и их проверки в рамках секторов разделов.

Понятие о файловых системах семейства Windows FAT

Раздел, отформатированный одной из файловых систем семейства FAT (File Allocation Table, Таблица размещения файлов), объединяет секторы в кластеры, причем каждый файл занимает один кластер. Для всех систем FAT существует максимальное количество кластеров в разделе. Это количество рассчитывается по количеству битов, использованных для адресации разделов кластера, за вычетом нескольких резервных

битов. По мере увеличения объемов жестких дисков на них появляется больше секторов. Для создания раздела большего размера (по всему диску) кластер должен содержать большее количество секторов. Очень большой объем дискового пространства расходуется впустую, если размер файла меньше размера кластера (секторы на диске остаются неиспользованными).

Инструменты и ограничения

Биты FAT

- FAT12 использует 12 бит или 2 ^ 12 бит или порядка 4 086 кластеров.
- FAT16 использует 16 бит или 2 ^ 16 бит или порядка 65 526 кластеров.
- FAT32 использует 28 бит или 2 ^ 28 бит или порядка 260 миллионов кластеров.

Кроме этого, существует ограничение на размер каждого кластера. Для того, чтобы использовался весь объем большого жесткого диска, необходимо создать множество разделов и помнить, какой из них содержит сохраненные данные.

Инструменты и ограничения

Разделы FAT

- FAT12 может создать разделы по 16 Мб.
- FAT16 может создать разделы по 2 Гб в DOS версии 4.0 и более поздних, в Windows 9x и ME либо разделы по 4 Гб в NT.
- FAT32 может создать разделы по 8 терабайт (Тб), но в версиях Windows (до XP) возможно использовать только раздел в 32 Гб.

Максимальное количество файлов в каталогах

- FAT — 512 файлов или папок в каждой папке.
- FAT32 — 65 534 файла или папок в каждой папке.
- Файловая система NT (NTFS) — 4 294 967 295 файлов или папок в каждой папке.

По умолчанию FAT сохраняет резервную копию таблицы FAT в заголовке раздела; в FAT32 для ускорения доступа эту опцию можно отключить. Всем версиям FAT недостает концепции владельца файла и управления доступом, файловых блокировок и избыточности, кроме того, они легко фрагментируются. FAT поддерживает некоторые

основные атрибуты файлов, например: *«только чтение», «скрытый», «системный файл», «метка тома», «подкаталог» и «архив»*. Для именования файлов, сохраненных в разделе FAT12 или FAT16, существуют три правила.

1. Имя состоит из префикса длиной до восьми символов, за которым следует точка и суффикс из трех символов (т. е., *my_files.txt*). (Наличие точки и суффикса, также называемого расширением, не является обязательным, — *примеч. науч. ред.*)
2. Имя файла должно начинаться с буквы или цифры.
3. Регистр букв не сохраняется.

VFAT/FAT32, как и FAT16, имеет ограничение на размер файловой системы в 2.0 Гб, но с добавлением трех усовершенствований:

1. Поддержка длинных имен файлов (до 255 символов, включая пробелы и многоточия; регистр написания сохраняется, но не учитывается).
2. Повышенная производительность с помощью «32-битного доступа в защищенном режиме».
3. Повышенные возможности управления; дисковые блокировки в «эксклюзивном режиме» для доступа программы к файлу.

Виртуальная таблица размещения файлов (VFAT)/FAT32 предлагает следующие преимущества:

- Использование 32 бит на каждую запись FAT и меньший размер кластера для увеличения максимального размера файловой системы до 32 Гб.
- Каждый отдельный файл занимает один кластер; небольшой файл с меньшим размером кластера меньше пространства тратит впустую.
- Расширение к VFAT, которое имеет те же самые ограничения на имя файла, что и VFAT.
- Доступны утилиты для преобразования VFAT в FAT32 за одну операцию.
- Разделы FAT32 — больше 32 Гб, подготавливаются другими операционными системами и используются Windows.

Windows NT может использовать кластер 64 Кбит и кластер 64 Кбит, расширяющий максимальный размер файловой системы до 4 Гб на раздел VFAT.

При файловой системе FAT сетевые списки контроля совместного доступа (ACL) ограничены *полным контролем*, *изменением* и *чтением*.

В 1988 году появилась FAT16, которая использовалась с версиями DOS от 4.0, Windows 3.x, Windows 95 OEM SR1, Windows ME и Windows NT. К 1995 году появилась VFAT, которую можно было использовать с Windows 3.x, Windows 95 OEM SR1, Windows ME и Windows NT. Около 1998 года появилась FAT32, которую можно было использовать с Windows 95 OEM SR2, Windows ME, Windows 2000 и Windows XP.

Понятие файловых систем семейства Windows NTFS

В систему Windows NT4 разработчики Microsoft включили более сложную файловую систему под названием NTFS. В NTFS применяется Главная файловая таблица (Master file table, MFT) для отслеживания каждого файла в разделе с дескриптором защиты (защита и полномочия) для каждого файла. Каждый дескриптор защиты содержит Системный список контроля доступа (SACL) для аудита и Список разграничительного контроля доступа (DACL), влияющий на доступ к файлу. Каждая запись управления доступом состоит из идентификатора (ID) пользователя или группы, а также из полномочия, предоставленного этому идентификатору. Идентификатор может принадлежать пользователю в локальном или доверяемом домене либо учетной записи хоста. Полномочия NTFS напрямую влияют на доступ к локальной файловой системе и сравниваются с полномочиями на коллективное использование в ACL файлов для определения эффективности доступа к совместному ресурсу. Сообщение «В доступе отказано» (No Access) блокирует любой доступ к файлу или каталогу и имеет преимущество над всеми полномочиями (локальными или коллективными). При передаче пользователям полномочий типа «Полное управление» (Full Control) убедитесь, что они понимают методику расчета действительных полномочий на коллективное использование ресурса:

1. Проведите проверку на наличие сообщения «NO ACCESS».
2. Проверьте SHARE ACL с самой высокой степенью разрешения доступа (они являются членами всех групп).
3. Проверьте FILE ACL с самой высокой степенью разрешения доступа (они являются членами всех групп).

Действительные полномочия на пользование сетью являются самыми строгими из полномочий FILE и SHARE. Версия 1.1 NTFS (или версия 4.0) может использоваться в NT4, Windows 200x, а XP.NTFS 4.0 предлагает следующие преимущества по сравнению с FAT:

- Более эффективное распределение дискового пространства.
- ACL (множественные пользователи и группы и множественные уровни доступа).
- Шесть групп полномочий: *доступ запрещен, просмотр, чтение, добавление, добавление и чтение, изменение и полный контроль.*
- Статичную модель наследования ACL, где новые файлы наследуют из папок, в которых они находятся.
- Поддержку файлов очень большого размера (один файл может занимать целый раздел).
- Журнал вносимых в файловую систему изменений (для аудита).
- Пониженную фрагментацию (по сравнению с FAT), но она по-прежнему имеет место.
- Поддержку имен файлов, состоящих из 255 символов, с учетом регистра набора.

С появлением Windows 2000 стала доступной NTFS 1.2 (или NTFS 5.0), которую можно использовать с NT 4.0 SP4b, Windows 2000 и XP. Для доступности новых функций защиты NTFS 5.0 на NT4 SP4b необходимо установить Программу-диспетчер конфигурации защиты (Security Configuration Manager, SCM). Если к системе Windows 2000 подключен раздел NTFS 4.0, то он преобразуется в раздел NTFS 5.0 со следующими усовершенствованиями:

- **Точки повторного использования (Reparse Points)** Объект, состоящий из метаданных, и фильтр-приложение (программа), сохраненные в соответствующем файле или каталоге файловой системы. При доступе к файлу метаданные передаются через фильтр, изменяя доступ к файлу. Один файл или каталог может иметь несколько точек повторного использования. Существуют встроенные точки повторного использования, и приложение, поддерживающее NTFS 5.0, может создать:
  - **Символические ссылки** Указатели на реальный путь к файлу.
  - **Узловые (junction) точки** Символические ссылки на каталог.
  - **Точки подключения тома** Символические ссылки на точки подключения.
  - **Сервер удаленного сохранения** Управляет перемещением файлов в автономный или близкий к автономному режим сохранения; оставляет точку монтирования для обратного получения файла.
- **Новая методология защиты и присвоения полномочий (динамическое наследование)** При изменении ACL родительского каталога динамическое наследование полномочий позволяет подкаталогам наследовать эти изменения. Унаследованные полномочия и полномочия, настроенные вручную, поддерживаются раздельно. Одним из недостатков является то, что динамическое наследование усиливает нагрузку на процессор/память в большей степени, нежели статическое наследование. Элемент управления «No Access» был удален, поскольку были добавлены элементы управления «allow» (разрешить) и «deny» (отказать). Для присвоения полномочий существуют тринадцать атрибутов: *Traverse Folder/Execute file* (перейти в папку/выполнить файл), *List Folder/Read Data* (просмотреть содержимое папки/считать данные), *Read Attributes* (считать атрибуты), *Read Extended Attributes* (считать расширенные атрибуты), *Create Files/Write Data* (создать файлы/записать данные), *Create Folders/Append Data* (создать папки/добавить данные), *Write Attributes* (записать атрибуты), *Write Extended Attributes* (записать расширенные атрибуты), *Delete Subfolders and Files* (удалить подкаталоги и файлы), *Delete Read Permissions* (удалить полномочия чтения), *Change Permissions* (изменить полномочия) и *Take Ownership* (принять владение). При определении действительных полномочий следует учитывать следующие новые правила:
  - «Настроенный вручную» имеет приоритет выше, чем «унаследованный».
  - «Разрешить» имеет приоритет выше, чем «отказать».

- «Унаследованный родителем» имеет приоритет выше, чем «унаследованный «дедом».

- **Журналы изменений** Регистрация всех операций файловой системы с 64-битным порядковым номером обновления. Фактические измененные данные не сохраняются.
- **Шифрование** Данная опция, называемая Зашифрованной файловой системой (Encrypting File System, EFS), сохраняет данные в шифрованном формате. Операционная система создает 128-битовые (или 40-битовые) открытые/секретные ключи; кодирование выполняется с помощью открытого ключа, а декодирование — с помощью секретного ключа. Операции кодирования являются частью операционной, а не файловой системы. Методы EFS являются частью «жестких» и «мягких» дисковых квот NTFS 5.0, основанных на пользователях, группах и глобальных условиях.
- **Поддержка разреженных файлов** Для данных с длинными последовательностями нулей на диск записываются только ненулевые данные, вместе с информацией о местах вставки нулей. После сохранения в таком виде файл необратимо изменяется, и его нельзя преобразовать в первоначальную форму.

Драйвер ядра операционной системы Linux поддерживает NTFS в режиме «только для чтения». Поддержка режима «чтение-запись» достигается через специальные функции эмулятора Wine. Драйвер ядра Linux был создан на основе информации, полученной в ходе инженерного анализа, чтобы позволить Linux-системам подключать и читать файловые системы NTFS. На время написания данной книги драйвер позволял записывать файлы того же размера, что и имеющиеся на диске, однако Windows NT, Windows 2000 и Windows XP при перезагрузке обычно требуют проверки диска (CHKDSK) для устранения повреждений, нанесенных драйвером. С другой стороны, проект Captive предлагает модули для доступа к *чтению* и *записи* разделов NTFS с помощью эмуляции ядра Microsoft Windows NT в Wine путем повторного использования одной из исходных частей *ntoskrnl.exe* ReactOS и драйвера *ntfs.sys* Microsoft Windows. Это надежный способ доступа к файловой системе NTFS, требующий NTFSPROGS v1.8.0 (группа утилит NTFS, основанных на совместно используемой библиотеке), которая, в свою очередь, требует GLIBC v2.3 (библиотека GNU/Hurd и GNU/Linux). Домашняя страница проекта доступна на сайте: www.jankratochvil.net/project/captive/CVS.html.pl.

Поскольку большинство переносов сетевых файловых служб осуществляется копированием файлов по сети в новый сервер Linux, потребность в драйвере NTFS для Linux невелика. Однако в случаях с большими объемами дисковых данных (измеряемыми в терабайтах) сетевое копирование может занять целый день, даже при очень большой скорости передачи. В таких ситуациях гораздо проще временно установить на машину с системой Linux диски, отформатированные под NTFS, и выполнить копирование локально.

Понятие файловых систем Linux

Помимо поддержки FAT и NTFS (в основном *чтение-запись*) Linux также поддерживает множество других файловых систем. Кроме прочих ядро 2.6 самостоятельно поддерживает вторую и третью расширенные файловые системы (ext2/3) и ReiserFS. Поскольку ext2/3 и ReiserFS — наиболее широко используемые в Linux файловые системы — о них и пойдет речь в данном разделе.

Ext2/3 и ReiserFS имеют много общих атрибутов. Каждый файл и каталог имеют адрес на диске, называемый *индексным дескриптором* (inode[1]). Обе системы поддерживают концепцию жестких и мягких (символических) ссылок, где с помощью значения inode можно создать имя файла, указывающее на имя другого файла (функционально они напоминают ссылки в Windows). *Мягкая ссылка* — это файл, содержащий inode-адрес файла, в котором хранится inode на данные. *Жесткая ссылка* — это второй файл, содержащий inode целевых данных. Ext2/3 и ReiserFS — это иерархические системы, в которых каждый файл или каталог сохраняются в каталоге с именем «/» или «корень», представляющем собой вершину дерева файловой системы.

В файле Linux */etc/fstab* (таблица файловой системы) перечислены файловые системы, точки и параметры монтирования, которые синтаксически анализируются при загрузке системы. При монтировании файловой системы в файл */etc/mtab* (таблица монтирования) добавляется строка, «чистый» бит в заголовке раздела считывается, после чего устанавливается на «0». При размонтировании (например, в момент остановки системы) «чистый» бит устанавливается на «1». Если во время процесса загрузки «чистый» бит не установлен на «1», то раздел называется «грязным», и для проверки на предмет ошибок файловая система обрабатывается специальными программами. Эти программы (*fsck*, *fsck.ext2* и *fsck.reiserfs*) проверяют «достоверность» данных и метаданных на диске. Файловая система называется «непротиворечивой», если каждый блок данных либо принадлежит одному inode, либо не принадлежит никому. Блоки данных, принадлежащие более чем одному inode, считаются ошибочными, или «противоречиями», на диске и представляют собой утерянные или поврежденные данные. Если операция «записи» прошла не полностью успешно, могут быть утеряны данные в файле либо повреждена информация о связи «блок данных-файл».

Понятие Ext2/3

Ext2 была первой используемой Linux файловой системой, построенной на базе файловой системы Minix. (Исторически первой файловой системой была ext (расширенная файловая система), а Ext2 является ее второй, улучшенной версией, — *примеч. науч. ред.*) Она обеспечивает раздельные уровни доступа для пользователя, группы и «остального мира» («other»), а также обеспечивает управление доступом к операциям

[1] node, или inode — структура данных в файловой системе, в которой сохраняется основная информация о файле, каталоге или другом объекте файловой системы.

read (чтение), write (запись) и *execute (выполнение)*. Имена файлов чувствительны к регистру набора и имеют максимальную длину в 255 символов. Максимальный размер раздела или файла в разделе составляет 4 Тб. Одним из недостатков Etx2 является то, что файлы в файловой системе могут быть легко повреждены при некорректном выходе (например, при внезапном отключении питания), и это требует вмешательства пользователя при перезагрузке, включающей в себя продолжительные проверки дисков программой проверки файловой системы (file system check, FSCK), при работе с которой необходимо участие пользователя. Когда файл повреждается, он может исчезнуть или оказаться содержащим ноль байтов. Если такое происходит с критичным системным файлом, то при загрузке системы могут возникнуть проблемы.

Изначально Ext3 разработана доктором Стефаном Твиди (Stephen Tweedie) в Red Hat. Она была добавлена в ядро версии 2.4.15, но сейчас уже используется с версией 2.4.16 или более поздними. Ext3 можно рассматривать как файловую систему Ext2, но с поддержкой журналирования. Для использования Ext3 программа должна быть скомпилирована в ядро и иметь установленный набор e2fsprogs. Ext3 предлагает следующие три режима ведения журналов, установленные в файл */etc/fstab*:

- **Journal (журнал)** Регистрирует данные файла и изменения метаданных. Это наиболее медленный режим.
- **Ordered (упорядоченный)** Регистрирует изменения метаданных файла и выполняет обновления данных на диске до обновления метаданных. Это режим по умолчанию.
- **Write Back (обратная запись)** Регистрирует метаданные, без проверки изменений данных на диске. Это наиболее быстродействующий режим.

Преобразования файловой системы между ext2 и ext3 не требуют резервирования и восстановления данных, как во время преобразований в других системах. Для преобразования Ext2 в Ext3 добавьте журнал:

```
/sbin/tune2fs -o <partition>
```

Для преобразования Ext3 в Ext2 удалите функцию журналирования файловой системы. Например:

```
tune2fs -O ^has_journal <partition>
```

В преобразовании обратно в Ext2 необходимости нет, потому что файловую систему Ext3 можно смонтировать как Ext2 или Ext3. Как только Ext2 преобразована в Ext3, необходимо отредактировать */etc/fstab* для того, чтобы программа FSCK не выполняла проверки достоверности данных. Поскольку имеется журнал, теоретически для поддержания непротиворечивости системы чистый бит не требуется. В записи */etc/fstab* измените последний столбец на 0, во избежание проверки достоверности данных.

```
/dev/hda2    /data ext2  defaults    1 2
/dev/hda2    /data ext3  defaults    1 0
```

Ресурсы

Параметры ядра

- CONFIG_EXPERIMENTAL=y n # Необходим в старых ядрах
- CONFIG_EXT3_FS=y n # По умолчанию в ядре 2.6

Модули/Драйверы

`/lib/modules/2.6.5-7.104-default/kernel/fs/ext3/ext3.ko`

Инструментальные средства:

- **ext2/ext3** http://e2fsprogs.sourceforge.net/ext2.html
- **e2fsprogs** Содержит утилиты: e2fsck, mke2fs, debugfs, dumpe2fs и tune2fs.
- **e2fsck** Проверка системы на предмет поврежденных или некорректных inodes, а также обеспечение исправлений.
- **mke2fs или mkfs.ext3** Создание файловой системы ext2/3.
- **debugfs** Отладка файловой системы.
- **Dumpe2fs** Чтение параметров файловой системы
- **tune2fs** Изменение параметров файловой системы.
- **ext2ed** Программа для редактирования файловых систем ext2 размером менее 2 Гб, использующая устаревшую библиотеку Curses.
- **defrag** Утилита дефрагментации для файловой системы ext2.
- **e2image** Создание обычного или «сырого» (raw) файла-образа. Утилиты e2fsprogs работают с «сырыми» файлами.
- **fdisk** Утилита для просмотра и редактирования разделов и файловых систем на диске.
- **FSDEXT2** Драйвер Win95 для доступа к функции *«только чтение»* ext2.
- **Ext2fsd** Драйверы WinNT, Win2K и XP для файловых систем ext2.
- **MountX** Драйвер Mac OSX для файловой системы ext2.

Понятие о ReiserFS

На базе исследований Ханса Райзера (Hans Reiser) в 2001 году система ReiserFS была добавлена в ядро Linux 2.4. На время написания книги с большинством дистрибутивов Linux поставлялась версия 3 ReiserFS, но уже существовала версия 4. Домашняя страница этой файловой системы расположена на сайте компании Naming System Venture (*www.namesys.com*). Версии сохраняют обратную совместимость друг с другом, и при прямом преобразовании одной версии (путем монтирования с опцией «-o conv») утилиты предыдущих версий работать не будут. Опция «resize=<NUMBER>», доступная

в момент перемонтирования, обеспечивает расширение разделов без необходимости резервирования или восстановления данных; при этом уменьшать размеры разделов нельзя. Это — по-настоящему журналируемая файловая система, в которой ведется учет транзакций и транзакций метаданных с «повторным» и «обратным» восстановлением работоспособности системы. Последовательность технологических операций — следующая:

1. Планирование транзакции (при сбое Шага 1 информация для записи теряется).
2. Выполнение транзакции (при сбое Шага 2 система может повторно воспроизвести транзакцию или удалить ее).
3. Отметка завершения транзакции (при сбое Шага 3 система будет рассматривать сбой Шага 2).

Если файловая система оставлена «грязной» (после отключения питания), для проверки непротиворечивости и, при необходимости, повторного воспроизведения вместо запуска «долгоиграющей» программы FSCK, анализируется журнал. При этом сокращается время простоя и снижается вероятность повреждений.

ReiserFS организует файловую систему в двух областях: данные и система. Область данных состоит из каталогов, файлов и метаданных файлов, сформированных как структура данных типа «сбалансированное дерево» (в версии 3) или «танцующее дерево» (версия 4). При структуре сбалансированного дерева для отдельно взятого файла данные и метаданные можно сохранить на диске рядом с целью минимизации перемещений считывающей головки и, соответственно, повышения скорости считывания. Поиск файла в разделе с помощью структуры «сбалансированного дерева» происходит быстрее, чем способом Ext2/3, а с помощью структуры «танцующего дерева» — еще быстрее. При использовании метода сохранения точного числа блоков меньше пространства расходуется впустую, чем при использовании поблочного распределения в Ext2/3. Системная область ReiserFS состоит из суперблока, журнала и битовой карты. Журнал ReiserFS может «лечить» испорченные блоки в области данных, но не в системной области. Последняя, как правило, не повреждается, но и ее можно починить путем перестройки суперблока или дерева. Например:

```
/sbin/reiserfsck -fix-fixable -rebuild-sb /dev/hda2)
/sbin/reiserfsck -fix-fixable -rebuild-tree /dev/hda2)
```

Ядра в версиях до 2.4.7 сталкивались с проблемами с совместно используемыми NFS разделами ReiserFS, включая повреждения и сбой операций записи, однако на данном этапе эти проблемы решены. Поначалу сообщалось о проблемах с программными RAID-массивами (Redundant Array of Independent Disks — матрица независимых дисковых накопителей с избыточностью), однако аппаратные RAID всегда работали удовлетворительно. Нормального функционирования программного RAID можно добиться с помощью комбинации JFS и ReiserFS.

Версия 4 ReiserFS, самая быстродействующая файловая система, является атомарной (не имеют места повреждения транзакций), предлагает более эффективное хранение

файлов (заменой алгоритма сбалансированного дерева на танцующее), имеет возможность расширения подключаемыми модулями и является кодом военного уровня (разнообразные проверки предшествуют фактическому входу в каждую функцию).

В отличие от ext2 и ext3, для ReiserFS доступны многие параметры ядра для компилирования нового ядра (здесь не описывается) для активизации особых функций файловой системы. Для включения поддержки ReiserFS в ядре установите CONFIG_REISERFS_FS на «y»; для сборки в виде модуля — на «m». Если CONFIG_REISERFS_CHECK установлена на «y», то файловая система будет работать в режиме отладки с возможностью осуществления любой проверки (медленнее); именно поэтому обычной установкой является «n». При установке CONFIG_REISERFS_PROC_INFO на «y» будет создано большее по размеру ядро или модуль, потребуется больший объем памяти ядра и статистика файловой системы будет сохраняться в */proc/fs/reiserfs*. Также доступен патч (заплатка) ядра, добавляющий опцию под названием CONFIG_REISERFS_RAW. Ее установка на «y» обеспечит сырой доступ к внутреннему дереву ReiserFS в обход файловой системы. Дополнительная информация поставляется вместе с исходными текстами ядра в *Documentation/filesystems/reiserfs_raw.txt*. Опция ядра REISERFS_HANDLE_BADBLOCKS превращается в таковую при редактировании источника ядра и включении */linux/reiserfs_fs.h*, используемой для обнаружения и пометки испорченных блоков на смонтированном разделе ReiserFS.

Ресурсы

Модули/Драйверы

```
/lib/modules/2.6.5-7.104-default/kernel/fs/reiserfs/reiserfs.ko
```

Инструментальные средства / Утилиты

- Получение информации о разделе ReiserFS (версия, размер блока и т. д.):

```
debugreiserfs <раздел>
```

- Создание списка испорченных блоков раздела ReiserFS:

```
/sbin/badblocks [-b <reiserfs-block-size>] <раздел>
```

- Запуск проверки достоверности (непротиворечивости) информации и исправление ошибок файловой системы:

```
reiserfsck -check <раздел>
```

- Составление списка испорченных блоков раздела ReiserFS:

```
resiserfsck -badblocks <файл со списком испорченных блоков> <раздел>
```

ПРИМЕЧАНИЕ ***fsck.reiserfs*** и ***reiserfsck*** — это одна и та же программа.

- Создание системы ReiserFS:

```
mkreiserfs <раздел>
```

ПРИМЕЧАНИЕ ***mkfs.reiserfs*** **и** ***mkreiserfs*** **— это одна и та же программа.**

- Изменение размера журнала или максимального размера транзакции:

```
reiserfstune <раздел>
```

- Отметка блоков в журнале файловой системы как испорченных:

```
reiserfstune -badblocks bad_blocks.txt /dev/hda2.
```

Понятие управления полномочиями (управления доступом)

Файловые системы NTFS, ext2, ext3 и ReiserFS по-разному поддерживают управление доступом. Совместно используемые ресурсы Windows и Samba также по-разному обращаются к управлению доступом. Целью перехода от Windows к Linux является сохранение как можно большего числа ACL (списков контроля доступа) при переносе совместно используемых ресурсов на сервер Samba, а также попытки со временем упростить структуру ACL до концепций владельца, группы и т. д. в стиле UNIX. В данном разделе рассматривается доступ конечного пользователя к сетевым ресурсам коллективного пользования. Для этого сначала необходимо описать основные полномочия UNIX и функции Расширенных атрибутов (Extended Attributes, EA)/ACL в Linux.

В простой форме (и исторически в UNIX) управление доступом к файлам называется «системой рабочих групп» и состоит только из одного уровня, трех типов владения на каждый файл или каталог (один пользователь, одна группа и вся окружающая среда), а также трех типов управления доступом (*чтение*, *запись* и/или *выполнение*). Идентификация пользователя и группы традиционно задается в */etc/passwd* и */etc/group*, хотя идентификатор пользователя (UID) и идентификатор группы (GID) можно получить из других областей (например, NIS или OpenLDAP). Изменения имени и группы владельца производятся командами *chown* и *chgrp* и контролируются битами прав доступа: девятью битами режима доступа к файлу (*чтение, запись, выполнение*) и тремя специальными битами (*setuid, setgid* и *sticky*). Команду *chmod* можно использовать для задания режима доступа и специальных битов, однако некоторые команды задают три специальных бита особо (*setuid, getuid, setreuid, seteuid* и *setfsuid*). *read* (чтение) позволяет перечислять содержимое каталога, *write* (запись) — создавать в каталоге файлы, а *execute* (выполнение) — осуществлять поиск в каталоге.

В системе Linux также имеются ответы на вопросы в случае необходимости более сложных полномочий, состоящих из пяти уровней. Через патчи к коду файловой

системы в ядре (теперь они внедрены в существующие версии ядра) становятся доступными списки контроля доступа (POSIX ACL) со всеми возможными функциями и расширенные атрибуты (EA). POSIX ACL можно использовать при недостаточной детализации стандартных полномочий UNIX. Полномочия могут присваиваться пользователям (или группам) на индивидуальной основе (т. е., Джо может иметь право на чтение, запись и исполнение foo.txt, а Салли — только на чтение и запись foo.txt). Расширенные атрибуты позволяют управлять способом взаимодействия файла или каталога с файловой системой; при этом файл может стать неизменяемым (только для чтения), каталог может сжать свое содержимое или журналировать операции записи особым образом.

Для разных пользователей и групп можно задать разные права доступа. ACL является частью Windows NT, AIX (операционная система IBM Unix) и HP-UX и был доступен в виде патча для ядра Linux 2.4, но EA/ACL включены в ядро версии 2.6 для Ext2, Ext3 и XFS. Для добавления поддержки EA/ACL в систему ReiserFS ядру версии 2.6 попрежнему необходим патч, однако этот патч включен в ядро SuSE 2.6

POSIX ACL Linux добавляют в Linux полномочия в стиле NT. Команды *getfacl* и *setfacl*, использующие разделяемую библиотеку libacl.so.0 и являющиеся частью пакета e2fsprogs, обеспечивают большую глубину детализации полномочий. Разные полномочия могут быть присвоены, исходя из нескольких разных UID или GID вместо одного UID, одного GID и установки по умолчанию для всех прочих (Other). Доступ к EA можно осуществить с помощью команд *lsattr* и *chattr* (также являются частью пакета e2fsprogs), что дает пользователю возможность управлять методом обеспечения доступа к файлу файловой системой.

Атрибуты ACL наследуются из родительского каталога во время создания. Запись ACL состоит из: 1) «типа» (пользователь, группа, маска или др.); 2) пользователя/группы или пробела; 3) полномочий. Если для отдельно взятого типа «пользователь» или «группа» пользователь не указан, то полномочия применяются к пользователю или группе, владеющим файлом или каталогом. Разрешение полномочий определяется в следующем некумулятивном порядке: владелец, пользователь с именем, группа владения, группа с именем, прочие. В табл. 5.1 показаны термины, присвоенные следующим типам записей ACL.

Табл. 5.1. Термины записей ACL

Условие	Текстовая форма	Примечание
владелец	user::rwx	традиц. владелец UNIX
пользователь с именем	user::root:rwx	
группа владения	group::rwx	традиц. группа владельца UNIX
группа с именем	group::admin:rwx	
маска	mask::rwx	
«прочие» традиц. для UNIX	other::rwx	«прочие» традиц. для UNIX

Действующие полномочия рассчитываются выполнением логического AND между записями пользователя и маски. Пример представлен в табл. 5.2.

Табл. 5.2. Типы, записи и полномочия ACL

Тип	Форма записи	Полномочие
пользователь с именем	user::rwx-	чтение и запись
маска	mask::r-x	чтение и выполнение
Действующее полномочиие	r-	чтение

После того, как в файле задан «access ACL» (доступ к ACL), в листинге будет показан знак плюса (+) после битов полномочия.

```
i.e. ls -ld foo
drwxrwx--- 2 jstile users 48 2004-08-24 06:18 foo
setfacl -m user:root:rwx,group:root:rwx foo
ls -ld foo
drwxrwx---+ 2 jstile users 48 2004-08-24 06:18 foo
getfacl foo
# file: foo
#owner: jstile
# group: users
user::rwx
user:root:rwx
group::r-x
group:root:rwx
mask::rwx
other::---
```

Если функция ACL «default ACL» (с помощью опции –d) задана в каталоге, то этот каталог сохраняет свои ACL, однако новые файлы и каталоги, созданные под этим каталогом, унаследуют «default ACL».

```
Задание ACL по умолчанию в каталог 'foo':setfacl -d -m group:ntadmin:r-x
foo
getfacl foo/
# file: foo
# owner: jstile
# group: users
user:: rwx
user:root:rwx
group::r-x
group:root:rwx
mask::rwx
other::---
default:user::rwx
```

```
default:group::r-x
default:group:ntadmin:r-x
default:mask::r-x
default:other::---
```

Для удаления ACL воспользуйтесь опцией –x:

```
setfacl -d -x group:ntadmin foo
getfacl foo/
# file: foo
# owner: jstile
# group: users
user::rwx
user:root:rwx
group::r-x
group:root:rwx
mask::rwx
other::---
default:user::rwx
default:group::r-x
default:mask::r-x
default:other::---
```

ПРИМЕЧАНИЕ

Удалять или перемещать файл может только владелец/группа UNIX или root, даже если ACL предоставляет права rwx.

Вносить изменения в ACL может только владелец/группа UNIX или root, даже если ACL предоставляет rwx.

Setfacl и getfacl не перечисляют и не изменяют биты setuid, setgid или sticky. /etc/fstab должен смонтировать файловую систему с опцией ACL, иначе команды POSIX ACL выполняться не будут (т. е. /dev/hda2/ext2 acl, defaults 1 1).

chmod изменит маску ACL и предоставление ACL необходимо применить повторно, либо маску необходимо переустановить на rwx.

Если полномочия программы — 4700, а пользователю предоставлен ACL rwx, то программа не будет выполняться как setuid.

Можно создать резервную копию метаданных файловой системы EA/ACL с помощью следующей команды:

```
getfacl -R -skip-base / > /root_AE_ACL_BACKUP_'date'.acl
```

Восстановить ACL из резервного файла можно с помощью следующей команды:

```
setfacl -restore=<резервный файл>
```

Если система Samba сконфигурирована на использование PAM (подключаемые модули аутентификации), PAM сконфигурированы на использование OpenLDAP, а NSS (Коммутатор службы имен) сконфигурирован на использование OpenLDAP и wins, учетные записи облегченного протокола службы каталогов (LDAP) можно использовать для присвоения прав файлам и для аутентификации пользователей домена как пользователей главным контроллером домена (PDC) Samba. Если файловые системы «с заплатами» ext2, ext3 или ReiserFS смонтированы с опцией «acl», а файл Samba-3 *smb.conf* содержит «map acl inherit = Yes», то совместно используемые ресурсы и файлы файловой системы можно сконфигурировать с POSIX ACL. Если сервер Samba-3 конфигурируется как контроллер домена (DC) с сервером OpenLDAP и winbind, тогда пользователям доменом и группам можно предоставить права доступа к коллективным ресурсам так же, как и на файловых серверах Windows. При этом сервер Samba станет для администратора Windows очень похожим на сервер Windows, что одновременно хорошо и плохо. С одной стороны, это позволяет администратору перенести ACL в коллективные ресурсы, как на сервере Windows, что упрощает пути переноса. С другой стороны, при использовании POSIX ACL возникают две серьезные проблемы: 1) их трудно переносить с одной машины на другую и 2) сложно создавать или восстанавливать их резервные копии. Метод простого перетягивания (drag-n-drop) файлов с одного сервера на другой с помощью Windows Explorer не сохранит POSIX ACL, так же как этого не сделают инструменты Linux — SCP (команда безопасного копирования), RSYNC (команда, обеспечивающая быстрый перенос инкрементного файла) и TAR (от Tape Archiver — архиватор для магнитных носителей). Последняя версия команды *cp* сохраняет ACL с опцией «-p» при копировании в локально смонтированную файловую систему с опцией «acl».

Альтернативным способом является использование «star» («звезда») — версии TAR, совместимой с POSIX (ftp://ftp.berlios.de/pub/star/). Для создания tar каталога с включением ACL:

```
star H=exustar -acl -c <path> > archive.tar
```

Для восстановления архива, включающего ACL:

```
Star -acl -x <archive.tar
```

H=exustar заставил star создать расширенный архив pax. Стандарт POSIX 1003.1 определяет pax как формат архива, совместимый с форматом tar с прибавлением списков контроля доступа. Для переноса ACL в Windows можно использовать robotcopy (из состава Windows XP Resource Kit), xcopy с xacls (из Win2k Resource Kit) или scopy (из NT Resource Kit), однако наборы Microsoft Resource Kit поставляются не бесплатно. Долгосрочным решением является упрощение ACL по мере переноса совместных ресурсов на Samba путем попыток изменить модель защиты для использования полномочий стандартного файла UNIX (один владелец, одна группа и «прочие») с комбинацией файловой системы и управлением разделяемыми ресурсами. Вы можете установить бит sticky bit на каталог для того, чтобы только владелец файла в этом

5 Зак. 1269

каталоге мог удалить или переименовать файл. Установка бита UID или GID на каталог обеспечивает то, что всеми файлами, созданными в этом каталоге, будет владеть заданный пользователь или группа. Вместе с полномочиями, основанными на файлах, конфигурация разделяемого ресурса в *smb.conf* позволяет администратору предоставлять различные виды доступа, исходя из имени пользователя и группы. Табл. 5.3 — это часть Коллекции HOWTO Samba, в которой идентифицируются элементы управления, основанные на пользователях и группах.

Табл. 5.3. Элементы управления, основанные на пользователях и группах

Параметр управления	Описание
Admin users (пользователи-администраторы)	Список пользователей с полным управлением всеми функциями данного ресурса коллективного использования
Force group (принудительное назначение группы)	Любой, использующий данный коллективный ресурс, рассматривается как член этой группы
Force user (принудительное назначение пользователя)	Любой, использующий данный коллективный ресурс, рассматривается как указанный пользователь
Guest ok (гостевой доступ)	Для доступа к данному коллективному ресурсу аутентификация не требуется
Invalid users (недействительные пользователи)	Список пользователей, доступ которым к данному коллективному ресурсу заблокирован
Only user (только пользователь)	??? не уверены ??? Не дает пользователям доступа к коллективному ресурсу, если они не внесены в список администратора
Read list (список чтения)	Список пользователей с допуском только чтения элементов в данном коллективном ресурсе
Username (имя пользователя)	???
Valid users (действительные пользователи)	Список пользователей с правом доступа к данному коллективному ресурсу
Write list (список записи)	Список пользователей с правом чтения элементов коллективного ресурса и записи в него

Понятие создания резервных копий файлов, их восстановления и возможностей репликации

Файловые службы и хранение файлов нельзя рассматривать, не затрагивая темы создания резервных копий, восстановления файлов и репликации. Файлы любой организации содержат ценную интеллектуальную собственность и их необходимо соответствующим образом защищать, поэтому на случай непредвиденных обстоятельств необходим план решения любых проблем: от случайного удаления файла или каталога до полного разрушения серверов и дисков.

Для защиты от такого рода случайностей (вернее, для подготовки к ним) необходимо создавать резервные копии данных на съемных носителях для безопасного

хранения. Репликация (тиражирование, дублирование) может быть одноразовой, запланированной или непрерывной. Создание резервных копий файлов операционной системы позволит в кратчайшие сроки восстановить ее в случае радикального сбоя. Успешные стратегии утверждают, что определенная часть резервных носителей должна храниться за пределами помещения организации. Если это целесообразно, то резервные носители в пределах организации следует хранить в несгораемых шкафах.

Оптические носители с возможностью перезаписи полезны для создания одноразовых резервных копий небольшого количества данных , но при выборе среды для резервирования объемов данных, измеряемых десятками, сотнями и тысячами гигабайт, предпочтение отдается ленточным накопителям.

Для большинства сисадминов актуальна не *необходимость* восстановления данных, а определение момента времени его выполнения.

Бесполезно создавать резервные копии на лентах, если в нужный момент необходимые данные невозможно найти. Планирование создания резервных копий имеет такую же важность, как и планирование служб восстановления файлов (и, возможно, сервера). Тестовые восстановления данных из резервных копий лучше всего проводить ежемесячно. Обнаружить, что зарезервированные данные не восстанавливаются из-за бракованной пленки, неправильного форматирования или других сбоев, всегда лучше до возникновения проблемы, а не после. Стратегия резервирования отвечает на пять возможных вопросов:

1. Резервные копии каких файлов следует создавать?
2. Каким образом следует создавать резервные копии?
3. Какой носитель лучше подходит для резервирования?
4. Когда и каких типов следует создавать резервные копии?
5. Когда следует отказываться от резервных копий?

Определение критичных файлов для резервирования

Определенные файлы восстанавливать очень трудно, например файлы, содержащие интеллектуальную собственность компании, файлы конфигурации, системные журналы, домашние каталоги, а также программы, скомпилированные под определенного пользователя. Как правило, файлы таких типов расположены в каталогах /etc /var /home /root и /opt. Другие файлы, например стандартные пакеты дистрибутивов, временные файлы ядра или файлы устройств, сравнительно легко поддаются восстановлению и в создании их резервных копий необходимости нет. Такие файлы, как правило, являются частью /dev, /proc, а также входят в стандартный пакет установки Linux. Выбор только самых необходимых элементов для резервирования сократит объем каждого резервного сохранения и расход ресурсов на проектирование решения резервирования. Группирование критичных файлов в стандартных местах также упростит процесс резервирования.

Неплохо всегда иметь под рукой клон каждого типа компьютера для оперативного создания новых машин. Клонированные образы следует хранить на устройствах с автоматически устанавливаемыми носителями (подобных жесткому диску), поскольку магнитная лента может работать очень медленно. При выходе из строя дисковода их можно очень быстро установить на диск, после чего критичные файлы восстанавливаются быстрее, чем с магнитного носителя. System Imager (часть установочного дистрибутива System Installer) — прекрасное решение клонирования, независимое от дистрибутива.

Определение способа создания резервных копий

Существует много способов планирования резервирования. Некоторые включают следующее:

- Запуск резервных копий на каждом хосте с определенным носителем резервирования. Данный способ действен для небольшого количества машин, но это решение не подлежит расширению.
- Копирование всех нужных файлов на сервер резервного копирования (с *rsync*), где они будут записаны на носитель резервирования с помощью утилиты командной строки.
- Резервирование нескольких машин можно осуществить без специальных программных средств.
- Настройка клиент-серверного набора для резервирования. При данном решении каждый резервируемый клиент запускает демон, а сервер с носителем резервирования запускает серверный демон.
- Серверный демон будет взаимодействовать с каждым демоном клиента, передавая данные на носитель резервирования (например, в Расширенный сетевой дисковый автоматический архиватор Maryland (AMANDA), HP Omni Back, ARKEIA, Veritas NetBackup).

Определение типа носителя резервирования

По мере увеличения скорости передачи данных и емкости разных типов носителей увеличивается и их стоимость. Цена носителя и устройства для его воспроизведения составляет большую часть всех расходов на резервирование; помимо этого существуют дополнительные ежегодные расходы. Носители резервирования всегда рекомендуется приобретать оптом (цена ниже), это снизит долгосрочные затраты. Приобретение библиотеки (устройства с несколькими кассетными деками) поможет снизить накладные расходы на перенос данных с пленки. Еще следует учесть, что, несмотря на долговечность, магнитные носители (пленки) устаревают морально, потому что постепенно их попросту становится не на чем воспроизводить. В число примеров входят бобинные магнитофоны, носители exabyte, jaz, zip и Magneto Optical.

Поэтому при выборе носителя для архива подумайте также о наличии устройства, способного читать этот носитель и драйвера для него. Либо включите перенос старых архивов на новый носитель в свою стратегию совершенствования процесса резервирования. В любом случае, за обновление системы придется заплатить, но при этом администратор никогда не будет иметь дело с архивами, которые не доступны в принципе.

В число обычно используемых носителей входят компакт-диски (CD), универсальные цифровые диски (DVD), цифровые аудиокассеты (DAT), ленты для цифровой записи с последовательным доступом (DLT) и открытые для записи ленты с последовательным доступом (LTO). CD/DVD (объемом порядка 4 Гб) стоят недорого и считываются приводом CD/DVD, который сейчас имеется практически на всех современных персональных компьютерах. У них, впрочем, имеются недостатки. Создание резервного CD достаточно рутинная работа, требующая идеальной организации труда. Для создания резервных копий всякий раз требуется новая «болванка» (пустой диск). Затраты на носители зависят от количества планируемых резервных копий и от количества дисков, необходимого для создания резервной копии требуемых данных. Выяснилось, что определенные носители со временем портятся, что делает недоступными записанные на них данные. Помимо неизбежного появления царапин, может отслаиваться покрытие (то же относится к посеребренному покрытию рабочей плоскости), пластмасса может терять прозрачность... Диски с большим объемом передают данные с большей скоростью и представляют собой недорогой тип носителя (в соотношении объем данных/стоимость).

Очень популярными стали приводы FireWire; в этом формате заархивированы некоторые художественные фильмы. Их недостатком является частый выход из строя механических компонентов, и сами дисководы очень восприимчивы к внешним воздействиям. На протяжении многих лет в качестве среды хранения резервных копий использовались пленки DAT (объемом от 20 до 40 Гб).

Ленточные накопители долговечны, не занимают много места, данные на них можно перезаписывать много раз, и деки с несколькими кассетами сравнительно недороги. Однако работают они достаточно медленно и сохраняют не очень большой объем данных.

В настоящее время распространенным носителем резервных копий являются ленты DLT (от 40 до 80 Гб). Скорость передачи данных у них выше (от 1,2 до 16 мегабит в секунду), данных можно сохранить больше, они долговечны и обладают возможностью перезаписи. При этом сами носители и устройства для их воспроизведения стоят дороже.

LTO Ultrim (с объемом от 100 до 200 Гб) — популярный носитель для хранения резервных копий в больших сетях. Скорость передачи данных у них очень высокая (от 20 до 40 мегабит в секунду), по размеру они практически такие же, как DLT, долговечны и обладают возможностью перезаписи. Проблема заключается в том, что эти носители очень дорогие.

Планирование создания резервных копий

Планы резервирования включают в себя полное и инкрементальное копирование. Полное копирование означает, что восстановить файл можно только с помощью самых последних зарезервированных данных. Создание полных резервных копий требует больше времени и занимает больше места, нежели инкрементальных, однако восстановление из полных копий занимает меньше времени. Инкрементальное копирование означает, что файл можно восстановить с помощью носителя последней полной копии и нескольких дополнений. При планировании учитывайте количество допустимого времени на ожидание запроса о восстановлении, а также время на создание полной резервной копии. Чем чаще планируется создание полных копий, тем выше годовые затраты на носители. Руководители и сисадмины должны согласовать план создания резервных копий для того, чтобы выбрать наиболее оптимальные носители по соотношению «цена-эффективность». Если руководству необходима договоренность на служебном уровне о восстановлении файлов из резервных копий в течение одного часа, то в этом случае потребуется большее количество полных резервных копий (больше носителей и устройств их воспроизведения).

Ведение *календаря* позволяет легко отслеживать время создания резервных копий и планировать сроки их создания. Также полезно вести журнал описания каждого резервирования. Эти данные можно хранить в базе или в простом файле. Некоторые коммерческие решения предлагают свои собственные методы, позволяющие сисадминам и пользователям быстро находить пленки с нужными материалами и обнаруживать поврежденные резервные копии.

План обращения и архивирования носителей

Полные резервные копии (но не все) лучше всего архивировать для долгосрочного хранения. По мере старения резервной копии стоимость носителей повышается, данные на них устаревают, и их пригодность снижается. Компромиссный подход к удалению резервных копий представляет собой вопрос степени детализации: только одна резервная копия будет представлять больший временной интервал резервирования. Многие формы носителей можно использовать многократно. Для предотвращения устойчивого роста потребности в новых носителях для каждого резервирования имеется возможность освобождения старых носителей и их повторного использования. При этом следует обращать внимание на то, сколько раз носитель уже использовался (по серийному номеру или по отметкам на носителе). Следует помнить о том, что ничего вечного не бывает, поэтому не стоит доверять резервные копии (свою безопасность) поврежденным или не функционирующим носителям.

Создавайте резервные копии расширенных атрибутов всех ACL в файле:

```
getfacl -R --skip-base / > /backup.acl
getfattr -dhR -m- -e hex / > /backup.ea
```

```
Восстановите EA/ACL's:
cd/
setfacl --restore=backup.aclsetfacl --restore=backup.acl
```

Зарезервируйте базу данных *mysql*:

```
mysqldump --tab=/path/to/some/dir --opt db_name
```

В системе Linux для ленточных накопителей SCSI устройство с «перемоткой» (rewind) обычно называется */dev/st0*, «без перемотки» (no rewind) — */dev/nst0*. При наличии библиотеки SCSI драйвер сменного механизма — */dev/sg0*, а библиотеки — */dev/sg1*. Для ленточных накопителей IDE устройство перемотки — */dev/ht0*, «без перемотки» — */dev/nht0*.

Для сжатия файла (файлов), а также для записи на носитель резервирования существует много программ командной строки. Сюда входят Copy In и Out (*cpio*), *tar* (или GNU tar), *dump/restore*, *mt*, *dd* и *cdrecord*. Сами по себе эти программы можно использовать для создания простого в технологическом отношении решения резервирования и восстановления. Команда *mt* используется для операций *operate* (функционирование), *read* (чтение), *seek* (поиск) и *write* (запись) с магнитной пленкой, а команды *xmt* и *loaderinfo* используются для работы со сменным механизмом библиотеки, содержащей несколько лент.

Следующие примеры демонстрируют использование команд *cpio*, *mt* и *xmt*:

- Перемотка и извлечение пленки из лентопротяжного механизма:

```
mt -f /dev/st0 rewind
mt -f /dev/st0 eject
```

- Составление списка содержимого:

```
cpio -itv -I /dev/st0
```

- Резервирование каталога /data на пленку с помощью команды cpio:

```
cd /data
find . -print | cpio -ovH crc -O /dev/st0
```

- Резервирование каталога /data на пленку с помощью команды tar:

```
cd /data
tar -clpMvf /dev/st0 *    # резервирование каталога на пленку
tar -dMf /dev/st0         # верификация содержимого
```

- Резервирование всего содержимого, за исключением */proc* и */dev*, командой tar:

```
tar - cpfM /dev/st0 / --exclude=/proc, /dev
```

- Резервирование с помощью команды dump:

```
dump 0f /dev/nst0 /
```

- Восстановление данных с пленки с помощью команды cpio:

```
cpio -icvmuld -I /dev/st0
```

- Восстановление всего содержимого с пленки с помощью команды tar:

```
tar -xpf /dev/st0 -C /
```

- Составление списка пленок в библиотеке:

```
mtx -f /dev/sg1 inventory (инвентаризация)
mtx -f /dev/sg1 status (состояние)
```

- Загрузка пленки 1 в библиотеке в лентопротяжный механизм:

```
mtx -f /dev/sg1 load 1 0
```

Лучшим решением будет использование открытого набора для резервирования (Mondo, StoreBackup или AMANDA). Эти программы представляют собой «обертки» для упомянутых выше команд оболочки, но они обладают такими дополнительными функциями, как ведение журнальных файлов, планирование и т. д. Mondo — это решение резервирования на базе компакт-дисков для одного хоста; StoreBackup — решение резервирования с диска на диск так же для одного хоста. Для создания системного диска и дисков с данными в Mondo применяется команда *cdrecord*. StoreBackup создает дубликат на другом диске.

AMANDA

AMANDA — это набор «клиент/сервер» с оболочкой для автоматизации резервирования нескольких объединенных в сеть хостов на одном хосте с ленточным накопителем (накопителями). Текущая версия 2.4.4p3 находится на сайте http://AMANDA.org. Система AMANDA создана Джоном Р. Джексоном (John R. Jackson) и Александром Олива (Alexandre Oliva), она предлагает функции планирования резервирования, ведения журнальных файлов, резервирования на нескольких устройствах/пленках, а также параллельного резервирования на удаленном хосте. Система обеспечивает резервирование даже при возникновении проблем с пленкой. AMANDA может использовать библиотеки на устройстве сменных пленок и выполнять полное или инкрементальное резервирование так же, как при работе с командой dump.

Поддерживаются следующие типы дампов:

- уровень 0 — полная резервная копия;
- уровень 1 — изменения с последнего уровня 0;
- уровень 2 — изменения с последнего уровня 1.

Система AMANDA поддерживает журнальные файлы дублирования, отслеживает использование пленки и распечатывает метки для лент.

С помощью сценария оболочки — amplot — AMANDA может создавать графическое отображение зарезервированной информации. *dumpcycle* обозначает частоту выполнения системой AMANDA полного дампа (вывода) типа -f0-. С множественными сетевыми платами на сервере AMANDA сетевой трафик можно направить на использование специального интерфейса.

Процесс резервирования системой AMANDA

AMDUMP запускается из cron (демона Unix, исполняющего команды по расписанию) на сервере AMANDA с ленточным накопителем от имени пользователя «AMANDA-user» и группы «backup» с паузой, если в каталоге домена *config* имеется файл с именем «hold» (*/opt/AMANDA/etc/MyCompany.con/hold*). Если файл с именем «hold» не обнаружен, а последнее резервирование было отменено или завершено некорректно, запускается *amcleanup*, записывающая любые данные с диска на пленку, после чего запускается *amflush*. Для стирания всех данных из некорректного резервного файла следует запустить *amflush* и *планировщик* (planner), запрашивающий клиентов и информацию планирования на соответствующем уровне резервирования. Запускается программа-драйвер с ленточным процессом (один поток *reader* и один поток *write*) и с одним процессом вывода для каждой строки плана. Каждый процесс выводит резервную копию от клиента в область промежуточного хранения или непосредственно на пленку.

Наконец, сценарий amreport переименовывает отчет о регистрации, отправляет его по электронной почте, и amtrmidx обновляет индексную адресацию.

AMANDA выполняется на хостах UNIX и может резервировать хосты Microsoft Windows с помощью Samba и kerbrose.

При резервировании хоста MS Windows следует помнить о выводе системного реестра в файл, резервную копию которого можно создать с помощью утилиты *regback.exe* из набора Windows NT Resource Kit и утилиты *regrest.exe* для восстановления, которая не является открытой.

Следующий командный файл резервирует системный реестр:

```
regback.bat
del C:\regbkp\my_host_name\*.* /q
regback C:\regbkp\my_host_name
```

Следует отметить, что изменение базы данных v.2.4.0 не дает возможности считывания файлов резервирования, созданных в версиях до v.2.4.0.

Для решения этой проблемы:

1. Обновите базы данных версий более ранних, чем v.2.4.0.
2. Экспортируйте базу данных с клиентом версий до 2.4.0.
3. Импортируйте базу данных с клиентом версий до 2.4.0.

В AMANDA для создания резервных копий используются команды dump и tar, а также устройства «без перемотки» (no rewind) */dev/nst0* при записи на пленку.

Самым эффективным методом работы для AMANDA будет вывод резервной информации на «диск промежуточного хранения» (рабочий каталог) перед сбросом данных на пленку. Этот способ имеет три преимущества:

1. Поскольку операция *dump* (вывод на диск) обычно выполняется быстрее операции *write* (запись на пленку), то запись на пленку будет выполняться постоянным потоком, что снизит износ устройства и пленки.
2. Множественные выводы данных могут происходить параллельно, что сократит временной интервал, неизбежный при резервировании на удаленные хосты.
3. Если в системе кончается пленка, то резервируемая информация продолжает записываться на диск промежуточного хранения с переходом на пленку после ее загрузки.

Если система перезагружается либо происходит сбой операции записи на пленку, необходимо запустить команду amflush для вывода содержимого диска промежуточного хранения на пленку.

AMANDA имеет инструмент конфигурации для определения оптимальных настроек лентопротяжного устройства:

```
amtapetype -t "BNCHMARK DLT1" -a /dev/nst0
```

Выполнение этой команды занимает очень много времени, однако при этом определяются необходимые настройки для устройства, носителя и конфигурации SCSI. Данный инструмент необходим только в случае наличия лентопротяжного устройства, не внесенного в список по умолчанию *AMANDA.conf*.

Вывод с использованием платы Adaptec 2940UW (скорость передачи — 20 000 Мб в секунду) устройством BNCHMARK DLT1 с картриджем DLT IV (от 40 до 80 Гб) в amtapetype (сгенерированное определение типа пленки), выполняющийся в течение 13 часов, — следующий:

```
amtape -t "BNCHMARK_DLT1" -f /dev/nst0
Запись 256 Мб      сжимаемые данные: 35 сек
Запись 256 Мб      несжимаемые данные: 118 сек
ПРЕДУПРЕЖДЕНИЕ: Лентопротяжный механизм с активизированным аппаратным сжатием
Расчетное время для записи 2 * 1024 Мб: 944 сек = 0 ч 15 мин              #<--
заняло 15 минут
записано 9800012 32 Кб блоков в 2997 файлах за 22248 секунд (короткая запись)
#< -- заняло 6 часов
записано 950290 32 Кб блоков в 5830 файлах за 28447 секунд (короткая запись)
#< -- заняло 7 часов

define tapetype BNCHMARK_DLT1 {
 comment "just produced by tapetype prog (hardware compression on)"
```

```
length 31604 mbytes
filemark 335 kbytes
speed 1239 kps
}
```

Вывод amtapetype — дескриптор типа пленки, который необходимо добавить в *AMANDA.conf*.

Установка AMANDA

Возможно, у каждого пользователя имеется свой вариант установки пакета AMANDA. Пользователи Debian используют *apt-get*:

```
Найти:
      apt-cache search AMANDA
Установить:
      apt-get AMANDA
SuSE, Mandrake и Red Hat используют пакеты rpm
      rpm -I AMANDA-1.4.4p3.rpm
```

При необходимости специального патча, разнородной среды UNIX или особых опций компиляции, AMANDA необходимо устанавливать «с нуля»:

1. Скачайте последний выпуск с http://www.AMANDA.org/download.php:

   ```
   wget http:
   //easynews.dl.sourceforge.net/sourceforge/AMANDA/AMANDA-2.4.4p3.tar.gz
   ```

2. Поместите созданный утилитой Unix tar (tarball) архив файлов в предназначенный для сборки каталог:

   ```
   mv amanda.1.4.4p3.tar.gz /usr/src/
   pushd /usr/src/
         Распакуйте
   tar -zxvpf amanda.1.4.4p3.tar.gz
   cd amanda.1.4.4p3
   ```

3. Создайте каталоги для AMANDA:

   ```
   mkdir -p /opt/Amanda/ {doc, etc, lib, libexec, man, share}
   chown -R Amanda-user.backup /opt/amanda
         Build AMANDA:
   ./configure -prefix=/opt/amanda \
   --with-config=MyCompany.con \
   --with-user=amanda-user \
   --with-group=backup \
   --with-ownre=amanda \
         --with-smbclient=/usr/bin/smbclient \
   --with-fqdn
   ```

Команда *--prefix=<directory>* устанавливает все файлы AMANDA в одно место. Команда *--with-config=<name>* создает образец *AMANDA.config* с доменом *<name>*.

Команды *--with-user*, *--with-group* и *--with-owner* задают пользователя и группу, от имени которых будет выполняться AMANDA.

Команда *--with-smbclient=* позволяет AMANDA выполнять резервирование клиентов MS Windows (фактически, она задает местоположение утилиты smbclient, которая входит в пакет Samba и используется для подключения к разделяемым ресурсам Windows, — *примеч. науч. ред.*). Команда *--with-fqdn* позволяет AMANDA использовать полностью квалифицированные имена хостов.

ПРИМЕЧАНИЕ При компилировании для клиента, который никогда не будет использоваться как сервер, добавьте опцию --without-server.

Для компилирования AMANDA:

```
make
      Смените текущий пользователь на root и добавьте группу
      и пользователя AMANDA
su root
groupadd -g 37 backup
useradd -u 37 -g backup -d /opt/amanda -c 'AMANDA admin' -s /bin/false -k
/dev/null -m amanda-user
      Установка
make install
```

В /opt/amanda будут созданы следующие каталоги:

```
sbin         Серверная часть AMANDA
libexec      Клиенты резервирования AMANDA
lib          Динамические библиотеки AMANDA
man          Страницы руководства
etc/example  Образцы файлов конфигурации, включая AMANDA.conf и disklist
doc          Документация
contrib.     Дополнительные сценарии
```

ПРИМЕЧАНИЕ При необходимости установки или удаления всех созданных файлов это делается из каталога, в котором производилась сборка

```
make uninstall
make clean
rm -rf /opt/amanda
```

На сервере

После установки AMANDA:

1. Скопируйте дополнительные данные из исходного дерева в установочные каталоги AMANDA:

```
mv amplot contrib docs /opt/amanda/
mv example /opt/amanda/etc
chmod +x /opt/amanda/amplot/amplot.sh
```

2. Создайте каталог для диска промежуточного хранения:

```
mkdir -p /dumps1/AMANDA
```

3. Исправьте информацию о владельце, которая могла измениться:

```
chown -R amanda-user.backup /opt/AMANDA
chown -R amanda-user.backup    /dumps1
```

4. Добавьте AMANDA в /etc/services на сервер с ленточным накопителем:

```
amanda    10080/udp
amandaidx    10082 /tcp
amidxtape    10083/tcp
```

5. Отредактируйте файл *xinetd* для AMANDA:

```
vi    /etc/xinetd.d/amandaidx
# default: off
# description: сервер резервирования AMANDA с возможностями индексирования
#
service amandaidx
{
      socket_type  = stream
      protocol     = tcp
      wait         = no
      user         = amanda-user
      group        = backup
      server       = /opt/amanda/libexec/amandad
      disable      = yes
      }
```

6. Создайте каталог для домена резервирования:

```
mkdir /opt/Amanda/etc/MyCompany.con
```

7. Создайте файл *amanda.conf* путем копирования файла-образца *amanda.conf* в каталог домена резервирования.

```
      cp /opt/amanda/etc/example/amanda.conf
/opt/amanda/etc/MyCompany.con/
```

Прочитайте и при необходимости отредактируйте файл *amanda.conf*. В нем содержится большая часть информации о конфигурации пакета AMANDA. В число настроек входит пользователь/группа, от имени которых выполняется программа, настройки kerberose, настройки лентопротяжного механизма (tapetype), настройки сменного устройства библиотек (tpchanger), промежуточного сохранения на диске (holdingdisk), все основные опции резервирования (dumptypes) и сетевой адаптер (NIC) для резервирования (interface). В файле *amanda.conf* имеются две основные области: диск промежуточного сохранения (holdingdisk) и основные опции резервирования (dumptypes). Определения holdingdisk задают местоположения резервных данных до их записи на диск. Для одновременного резервирования рекомендуется конфигурировать несколько дисков промежуточного хранения с достаточным объемом свободного пространства для размещения одного блока резервных данных на одном диске, поскольку они предназначены для хранения произвольных резервных копий. При отсутствии диска промежуточного хранения резервных данных последние будут записываться непосредственно на пленку, а все дополнительные резервируемые данные будут дожидаться освобождения лентопротяжного устройства. Ниже приведен пример записи для диска промежуточного хранения данных:

```
holdingdisk hd2 {
directory " /dumps1/AMANDA"
use 30000 Mb
}
```

Следующей обширной областью файла *amanda.conf* являются определения dumptype (тип вывода). В одном файле *amanda.conf* может быть много определений типов вывода, и одно определение можно использовать в других для объединения (консолидирования) общих настроек. Ниже приведен пример определения типа вывода с некоторыми описаниями:

```
define dumptype mother {
auth  bsd    # bsd/krb4
comment"my          backups" # decription
#comprate    0.50, 0.50   # compression rate (степень сжатия)
compress     none  #none/client best/client fast/server best/server fast
dumpcycle    30    #days between full dumps (дней между полными выводами)
exclude"./dev/"    #file or pattern to exclude (файл или шаблон для исключения)
exclude"./proc/"   #file or pattern to exclude (файл или шаблон для исключения)
holdingdisk  yes   #use holding disk (yes/no) (использование диска промежуточного
хранения (да/нет))
#ignore      #don't use this backup (не использовать эту резервную копию)
index no     #keep index (no/yes) (поддерживать указатель (нет/да))
kencrypt     no    #encrypt transfer (no/yes) (зашифрованная передача данных
(нет/да))
maxdumps     1     #concurrent dumps on client. Default: 1 (параллельные выводы
клиенту. По умолчанию: 1)
```

```
maxpromoteday      0      #Default: 10000
priority    high
program"GNUTAR"            # DUMP/GNUTAR
record yes   #record dump to /etc/dumpdates. (записывать вывод в /etc/dumpdates)
skip-incr    0      #Skip the disk when dump 0 is not due. (Пропускать диск при
ненадлежащем дампе 0).
}
```

Сконфигурируйте резервирование созданием файла конфигурации «disklist» (список дисков) в каталоге домена резервирования (*/opt/amanda/etc/MyCompany.con/*). Каждая строка в файле списка дисков представляет одно устройство или совместно используемый ресурс для копирования. В каждой строке должно присутствовать полностью определенное имя домена (FQDN) клиента для резервирования, устройство/раздел для резервирования и тип вывода (dumptype). Формат строки в списке диска — следующий:

```
hostname diskdev dumptype [spindle [interface]]
```

Ниже приведено несколько примеров синтаксиса списка диска:

- Для резервирования */home* на сервере AMANDA:

```
localhost    sda1  nocomp-root
```

- Для резервирования коллективно используемого ресурса Windows с именем *\\Host\C* укажите сервер Samba в качестве имени хоста:

```
samba_host.domain.com     "//ms_windows_pc/C$."     nocomp-root
```

- Для резервирования */home* на другом хосте Linux:

```
linux_host.domain.com     /home                    no comp-rootmkdir -p
/opt/sbin/amanda/MyCompany.con/amdump
chown -R amanda-user.backup /opt/amanda/MyCompany.con
```

Клиенты Linux

Клиентам Linux следует рассмотреть выполнение следующих шагов:

1. Пользователь Amanda-user должен иметь возможность подключиться с сервера AMANDA:

```
echo '' <<EOF > /opt/amanda/.amandahosts
192.168.0.221              amanda
EOF
```

2. Задайте имена владельца и права доступа:

```
chown amanda-user. /backup /opt/AMANDA/.amandahosts
chmod 0400         /opt/amanda/.amandahosts
```

3. Сконфигурируйте *xinetd* (при наличии) и запустите:

```
vi /etc/xinetd.d/amanda
      #default:    off
      #description:      amanda backup client
      #
      service amanda
      {
            socket_type  = dgram
            protocol     = udp
            wait         = yes
            user         = amanda-user
            group        = backup
            server       = /opt/amanda/sbin/amandad
                  disable          = yes
      }
/etc/init.d/xinetd restart
```

При наличии файла inetd сконфигурируйте и запустите демон inetd.

```
vi /etc/inetd.conf
      amanda       dgram udp   wait  amanda
/usr/lib/amanda/amandad  amanda
      /etc/init.d/inetd reastarted
```

Для клиентов Windows

Добавьте пароль *разделяемого ресурса* к паролям */etc/amanda* на сервере Samba, который будет использоваться для монтирования клиентов Windows.

AMANDA установит связь с сервером Samba, который, в свою очередь, свяжется с клиентом Windows.

Организация сервера резервирования

Пользователи Amanda должны иметь чистую пленку в устройстве и записать на нее метку. Резервные копии, сделанные на AMANDA, не могут использовать пленку без метки.

```
amlabel MyCompany.con Label1
```

1. Проверьте *config* и устраните все возникшие проблемы.

```
amcheck MyCompany.con
```

Выходные данные будут выглядеть следующим образом:

```
AMANDA Tape Server Host Check
-----------------------------------------
Диск промежуточного хранения /dumps1/AMANDA: Доступно 51309004 Килобайта
```

```
дискового пространства (это много)
ОШИБКА: невозможно переписать метку1 активной пленки
      (ожидание новой пленки)
ПРИМЕЧАНИЕ: пропуск теста записи на пленку
ПРИМЕЧАНИЕ: info dir
/var/lib/Amanda/MyCompany.con/curinfo/motherin.MyCompany.con/_: не существует
ПРИМЕЧАНИЕ: index dir / /Amanda/MyCompany.con/index: не существует
Проверка сервера заняла 6.408 секунд
Проверка хостов клиентов резервирования AMANDA
----------------------------------------
Проверка клиента: 1 хост проверен за 0.312 секунд, проблем не обнаружено
```

2. Выполните резервирование вручную:

```
amdump MyCompany.con
```

3. Настройте AMANDA для запуска из cron и автоматического создания резервных копий:

```
# checks the tapes (проверка пленок)
0 16 * * 1-5 /usr/sbin/amcheck -m /etc/AMANDA/MyCompany.con/amanda.conf
# runs the backup (выполнение резервирования)
45 0 * * 2-6 /usr/sbin/amdump /etc/AMANDA/MyCompany.con/amanda.conf
```

Проектирование файловых служб на базе Linux

Проектирование файловых служб на базе Linux — одна из самых видимых областей сетевого проектирования, потому что эти службы непосредственно влияют на конечных пользователей. Последние будут жаловаться, если их домашний каталог будет расположен в глобальной сети (WAN) на сервере, который работает очень медленно или перегружен подписчиками, если нужный файл вдруг станет недоступным или пропадет возможность сохранения документов. Для выбора оптимального сценария, лучше всего придерживаться общих правил. В оптимизациях учитываются сетевая топология (медленные WAN, подсети, география), аппаратные средства (диск, сеть, объем памяти, характеристики центрального процессора), резервируемость (возможность дублирования данных), а также конфигурация пользовательского профиля (профили роуминга, несинхронизированные файлы, переадресация папок).

Аппаратные ресурсы

Путь трафика проходит от NIC (сетевой адаптер) к памяти и на диск. Точка на этом пути с наиболее медленным срабатыванием аппаратных средств и будет «узким местом». Рекомендуется планировать скорость передачи данных порядка 100 Килобит в секунду на каждого пользователя и объем каталога профиля порядка 200 Мб на пользователя (в зависимости от того, насколько хорошо ограничены профили).

Успешность применения нового сервера Samba напрямую зависит от того, насколько хорошо рассчитаны емкость и пропускная способность.

Скорость передачи данных по сети постоянно растет, и с каждым годом передаваемые пользователями файлы увеличиваются в размерах. При настройке каналов связи рассчитывайте скорость в 0,1 мегабит в секунду на каждого пользователя в канале связи, в котором расположен домашний каталог этого пользователя, и удваивайте этот показатель при расчете максимальной загруженности сети. Если канал связи обслуживает и другие файлы, то пропускная способность должна быть еще выше. При расчетных 100 Килобит в секунду 30 пользователей будут «забирать» с сервера 3 Мегабита в секунду. Для эффективной производительности планируйте установку плат Ethernet с емкостью минимум 1 Гб. При использовании нескольких плат рассмотрите возможность «объединения каналов» (в терминологии Intel это называется «группирование»), т. е. организации плат в виде единого интерфейса, а также конфигурирование соответствующего управляющего коммутатора. Проверьте аппаратное автосогласование между сетевыми адаптерами и коммутаторами или маршрутизаторами, где часто возникают проблемы с выбором оптимальных настроек, что выражается в низкой производительности. Сравните производительность сети с жестко запрограммированными настройками и с настройками автоматического согласования на предмет параметров двусторонней связи, скорости передачи данных и управления их потоками.

Для обработки запросов ввода/вывода (I/O) доступ к диску должен быть равен или приближаться к пропускной способности сети, иначе нагрузка будет очень высокой (из-за ждущих процессов). При наличии стандартной шины PCI (Peripheral Component Interconnect) можно получить скорость порядка 132 Мегабита в секунду. С шиной PCI-X и контроллером SCSI можно добиться 450 Мегабитов в секунду (источник «*Samba-3 на примерах*», автор Джон Х. Терпстра (John H. Terpstra)). Альтернативой локальному хранению файлов может стать перенос хранилища файлов в сетевое хранилище (SAN) или устройство хранения, подключаемое к сети (Network Attached Storage — NAS) с соответствующим переносом нагрузки с диска и сетевого ввода/вывода на специально предназначенные для этого аппаратные средства. Система SAN позволяет системному администратору делать вложения в единую систему, а не в устройство каждого канала в отдельности.

Если памяти недостаточно, то сервер будет тратить больше времени на поиски и постраничную подкачку на диске (это происходит достаточно медленно), и операциям придется дожидаться высвобождения ресурсов, что вызовет снижение производительности и возможное блокирование сервера. Если позволяют средства, то с самого начала серверы должны быть оснащены максимальным объемом памяти. Автору довелось столкнуться со следующими расчетными данными по необходимой памяти на каждого пользователя и на поддержку каждой службы: DHCP (протокол динамической конфигурации хоста) — 2,5 Мб, Служба доменных имен (DNS) — 16 Мб, NMBD — 16 Мб, WINBIND —16 Мб SMBD 4 Мб, APACHE — 10 Мб, CUPS 3,5 Мб и основная операционная система 256 Мб (источник «*Samba-3 на примерах*», автор Джон Х. Терпстра).

Перенос файловых служб в систему Linux

Перенос файловых служб в Linux — многоэтапный процесс. К сожалению, готовых сценариев не существует, однако ведется постоянная работа по добавлению необходимых команд в Samba для получения информации, которая могла бы помочь упростить процесс создания такого сценария.

Перед началом переноса совместно используемых ресурсов и файлов на сервер Samba убедитесь в его корректной интеграции в домене и в настройке всех необходимых учетных записей пользователей и отображении любых имен пользователей. При работе в качестве Сервера доменных имен (Domain Member Server) убедитесь в корректной работе *winbindd* для обеспечения правильного отображения идентификатора защиты (SID) Windows в UID UNIX. При сбое в работе этого компонента копирование настроек ACL на файлах станет невозможным, и при попытках создания файлов или каталогов могут даже иметь место ошибки доступа.

Во-первых, следует определить имена совместно используемых ресурсов на сервере Windows и создать эти ресурсы и каталоги на сервере Samba. Для получения списка совместных ресурсов на удаленном сервере можно воспользоваться командой *net rpc share*. Предположим, что сервер называется *ntserver* и пароль его администратора *admin*. Для получения списка существующих совместно используемых ресурсов можно использовать следующую команду:

```
net prc share -S ntserver -Uadministrator%admin
```

Введите надлежащие записи определения совместного ресурса в файл *smb.conf* и создайте необходимые каталоги. При этом может потребоваться перезапуск Samba или подача сигнала Hangup (HUP) процессам SMBD для того, чтобы новый совместно используемый ресурс стал видимым для клиента машины с Windows.

В Windows существуют два раздельных набора полномочий на использование коллективных ресурсов, которые, как правило, многих вводят в заблуждение. Существуют полномочия, применяемые к совместно используемым ресурсам (полномочия совместно используемых ресурсов), и полномочия, применяемые к файлам и каталогам. С машины-клиента Windows 2000 полномочия совместного доступа к разделяемым им папкам можно просмотреть нажатием правой кнопкой мыши на совместно используемой папке и выбором строки **properties** (свойства). Здесь имеется закладка «Sharing» — совместно используемые ресурсы и закладка «Security» (безопасность). На закладке «Sharing» есть кнопка «Permissions» (полномочия), после нажатия которой появляется закладка «Share Permissions», на которой можно задать три параметра на разрешение или запрет пользования полномочиями на совместные ресурса: *full control* (полный контроль), *change* (изменить) и *read* (чтение). В закладке «Security» можно задать полномочия на пользование конкретным каталогом. Для копирования файлов на сервер Samba и сохранения настроек ACL (как минимум в том объеме, в котором они необходимы для преобразования Samba этих записей ACL в POSIX ACL) из клиента Windows 2000 или более поздней версии можно воспользоваться командой *xcopy* с опцией */o*.

Также для просмотра ACL и для внесения в них изменений можно воспользоваться утилитой Samba под названием *smbcacls*. Если машина, с которой осуществляется перенос совместно используемых ресурсов, имеет систему, отличную от Windows 2000, то будет удобнее (хотя и дольше) смонтировать машину-источник и машину-назначение на машине с Windows 2000, после чего воспользоваться *xcopy* с нее.

Последняя версия Samba (v.3.0.7) имеет проблемы с установкой имен владельцев файлов, являющихся встроенными группами объединением в группы владельцев файлов (например, «Администраторы»); следовательно, при наличии файлов, владельцами которых являются группы (что возможно в Windows), во время копирования будут появляться сообщения *«доступ запрещен»*, и владелец записей ACL не будет настроен корректно. Есть надежда, что в последующих версиях эти недоработки будут устранены.

Перенос полномочий на использование файлов

Хотя *xcacls* может сослужить вам добрую службу, он не умеет совершать рекурсивный обход каталогов самостоятельно. W2k Resource Kit будет установлен в каталог *C:\Program Files\Resource Pro Kit\xcacls.exe*, а NT4 будет установлен в *C:\\NTreskit\xcacls.exe*.

Удостоверьтесь в том, что вы добавили строку PATH как в «User variables for Registered User» (пользовательские переменные для зарегистрированных пользователей), так и в «System Variables» (системные переменные). Для этого воспользуйтесь диалогом, доступным через «Пуск»/«Настройка»/«Панель управления»/«Система»/«Дополнительно»/«Переменные окружения». Эта команда помогает задать настройки, просмотр и сохранение полномочий на использование всех файлов и каталогов в разделе NTFS (с системой FAT не работает). Применение этой команды не совсем понятно, однако существует несколько полезных примеров использования:

Для вывода ACL для корневой файловой системы:

```
xcacls %systemroot%\*.* /T > C:\%1_acl.txt
```

Для просмотра полномочий на использование файла:

```
xcacls.exe c:\winnt
c:\WINNT BUILTIN\Users:R
   BUILTIN\Users: (OI) (CI) (IO) (special access:)
     GENERIC_READ
     GENERIC_EXECUTE
   BUILTIN\Power Users: C
   BUILTIN\Power Users: (OI) (CI) (IO) C
   BUILTIN\Administrators: F
   BUILTIN\ Administrators: (OI) (CI) (IO) F
   NT AUTHORITY\SYSTEM: F
   NT AUTHORITY\SYSTEM: (OI) (CI) (IO) F
   BUILTIN\Administrators: F
   CREATOR OWNER: (OI) (CI) (IO) F
```

- **Только наследование (IO)** ACE (адаптивная коммуникационная среда) не влияет на эту папку.
- **Наследование контейнером (CI)** ACE будет установлена на всех папках данного каталога.
- **Наследование объектом (OI)** ACE будет установлена на всех файлах данного каталога.
- **Без распространения (NP)** ACE не будет применяться к подпапкам или файлам в данном каталоге.
- **F** (Полное управление).
- **C** (Изменение).
- **W** (Запись).

Выведите все полномочия на пользования файлами и каталогами в файл файловой системы NTFS. В соответствии со статьей 245015 Базы знаний Microsoft (Microsoft Knowledge Base Article), «можно использовать утилиту *Xcacls.exe* для распечатки полномочий на пользование файлами и папками, содержащимися в других папках, однако нельзя распечатать полномочия на пользование папками и файлами, содержащимися в подпапках»:

```
XCACLS *.* > C:\filename.txt
```

Существуют бесплатные программные средства под названием FILEACL (*www.gbordier.com/gbtools/fileacl.htm*), которые можно использовать для простого вывода всех ACL для локальных и удаленных совместно используемых ресурсов сети:

```
setup samba as bdc with replication
setup samba to respect linux acl

dumping NTFS acl's

apply acl's to the shares
drag and drop files to samba share
```

С помощью утилиты Resource Kit под названием *srvcheck* (т. е., *srvcheck \\hostname*) можно получить список совместно используемых ресурсов и полномочий к ним в системе Windows и просмотреть полномочия на пользование файлами в утилите *perms* из состава Resource Kit (т. е., *perms C:\my_directory*).

Утилита showwaccs инструментальных средств поддержки

Инструмент SubInAcl представляет собой очень «разумное» и эффективное средство изменения полномочий совместно используемых ресурсов.

```
сохранить настройки:    SubInAcl /output=c:\subinacl_save.txt /noverbose
/display
```

```
    применить настройки:     SubInAcl /playfile c:\subinacl_save.txt
/subdirectories
SubInAcl /subdirec \\server\share\*.* /display /noverbose
модификация полномочий совместно используемых ресурсов из командной строки:
      хороший список инструментальных средств командной строки:
          http://www.ultratech_llc.com/KB/ASP/FileView.asp?File=/KB/Perms.TXT
```

Для задания совместно используемых ресурсов и полномочий к ним необходимо определить действующие полномочия для всех пользователей всех коллективных ресурсов. Процесс — следующий:

1. Проведите проверку на наличие сообщения «NO ACCESS».
2. Проверьте полномочия SHARE с самой высокой степенью разрешения доступа (они являются членами всех групп).
3. Проверьте полномочия FILE с самой высокой степенью разрешения доступа (они являются членами всех групп).
4. Действующим полномочием в сети будут самые «запрещающие» полномочия из FILE и SHARE.

Совет

Если Пользователь A создает файл Excel для редактирования Пользователем B, то, когда Пользователь B откроет этот файл, программа Excel создаст новый временный файл (владельцем которого будет Пользователь B). При сохранении изменений Excel присвоит временному файлу имя файла-оригинала так, что фактическим его создателем станет Пользователь B. Пользователь A по-прежнему остается владельцем файла на сервере W2K.

Краткое резюме по разделам

Понятие файловых систем Windows

- ☑ Несмотря на то, что Linux имеет доступ чтение/запись в файловые системы FAT, FAT/VFAT следует избегать, поскольку им не хватает ACL, они неэффективно используют дисковое пространство и легко фрагментируются.
- ☑ Файловая система NTFS управляет разделами намного больших размеров, поддерживает RAID, комплексные ACL, а также регистрационные журналы транзакций; при этом количество дополнительных функций постоянно растет. Недостатком является то, что ее совместимость с Linux ограничена драйвером ядра, предназна-

ченного только для чтения (за исключением проекта Captive), что делает ее непригодной для использования с операционными системами Microsoft не-NT версий.

- Самые распространенные файловые системы Windows (FAT/VFAT/NTFS) ограничены (намеренно или нет). Для Linux и других операционных систем *nix существуют более устойчивые варианты с более полным набором функций, поэтому при переходе на Linux следует учесть и возможную необходимость перехода на использование новой файловой системы.

Понятие файловых систем Linux

- В настоящее время EXT2, EXT3 и ReiserFS поддерживают POSIX ACL, RAID и доступ «чтение/запись» для операционных систем Windows и Linux. Это — основные файловые системы, используемые в Linux. Файловую систему ext2 можно преобразовать в ext3, и наоборот.
- Журналы ext2 и ReiserFS с разными уровнями ведения предлагают более надежную файловую систему уровня предприятия. На данный момент ReiserFS считается самой быстродействующей файловой системой.

Понятие управления полномочиями (управления доступом)

- Для поддержки POSIX ACL можно пользоваться файловыми системами Samba и Linux для создания полномочий с более разветвленной степенью детализации, подобных поддерживаемым NTFS, однако в данном случае усложняется поддержка ACL при резервировании либо перемещении данных с одного сервера на другой.
- Долгосрочной целью должно стать достижение необходимого уровня детализации управления доступом с использованием стандартного полномочия Unix на пользование файлом вместе с полномочиями совместных ресурсов Samba.

Понятие создания резервных копий файлов, их восстановления и возможностей репликации

- Файлы и серверы могут повреждаться или теряться, что обуславливает необходимость проектирования файловых служб с интегрированным планом создания резервных копий данных и их восстановления.
- Следует создавать резервные копии только нестандартных файлов (ради экономии времени и ресурсов); при этом должна быть создана структура одновременного резервирования нескольких файлов.
- Выбирайте способ резервирования и носитель, соответствующие размеру и сложности сети. При этом будет легче разработать окно планирования процесса резервирования.

- ☑ Регулярно планируйте процесс резервирования — полного или инкрементального — в соответствии с типом резервного носителя и временными ограничениями, а также с учетом возможности восстановления данных в рамках запланированного временного интервала.
- ☑ Тщательно планируйте архивирование, повторное использование и утилизацию носителей как созданных на устройствах хранения с автоматически устанавливаемыми носителями, так и при автономном сохранении, для обеспечения уровня надежности носителей резервирования и долгосрочного доступа к резервным копиям, избегая необходимости архивирования всех резервных копий.

AMANDA

- ☑ AMANDA — это расширяемое открытое решение резервирования по типу «клиент/сервер» для резервирования сетей клиентов Windows и *nix, выполняющегося на *nix, с интерфейсом командной строки, использующим стандартные утилиты *nix, включая rsync, dump, tar, либо cpio и mt.
- ☑ Процесс резервирования начинается при контакте сервера с демоном клиента. Клиент собирает данные, которые отправляются назад на сервер. Сервер сохраняет эти данные в области промежуточного хранения до их переноса на резервный носитель.
- ☑ С помощью нескольких файлов конфигурации можно создать надежное решение сетевого резервирования без приобретения коммерческих лицензий.

Проектирование файловых служб на базе Linux

- ☑ Установите в сети минимум 2 контроллера домена (с WINS) на каждый сетевой сегмент.
- ☑ В том, что касается аппаратных средств, планируйте скорость передачи данных в 100 Килобит в секунду на каждого пользователя по схеме «сеть-память-диск» и наоборот.
- ☑ Упростите сеть с точки зрения клиента, а также разгрузите трафик WAN с помощью утилиты rsync для синхронизации между сетевыми сегментами или серверами. Настройте DFS для каждого из совместно используемых ресурсов. Для поддержания одновременности изменений файлов, изменяемых в разных сетевых сегментах, необходим контроль за версиями.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом *www.syngress.com/solutions* (форма «**Ask the Author**»). Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: Может ли Samba заменить контроллер домена Windows NT4 или сервер Active Directory?

О: Samba может заменить контроллер домена Windows NT4, но пока не может заменить сервер Active Directory.

В: Каковы простейшие способы устранения наиболее распространенных неисправностей?

О: При настройке сервера Samba существует несколько операций устранения неисправностей:

'testparm' не обнаруживает ошибок в smb.conf

'lsof -i tcp ; lsof -i udp' показывает выполняющиеся демоны и порты: ldap, nmb, smb, windbind, cups.

'smbclient -L localhost -U%' показывает доступность Samba; хост MYSERVER является мастером для MYDOMAIN.

'net getlocalsid' и 'net getlocalsid MY DOMAIN' отображает тот же SID (идентификатор защиты), поэтому MYSERVER является MYDOMAIN.

'slapcat' выводит все объекты в базе данных ldap (даже когда ldap не запущен).

'ldapsearch -x -b "dc=myscompany,dc=com" " (ObjectClass=*)" ' доказывает, что slapd запущен и доступен (отвечает на запросы)

'getent passwd | grep Administrator' показывает, что файл nsswitch.conf сконфигурирован для отправки вас на сервер LDAP с помощью библиотеки nss_ldap.

'pdbedit -Lv Administrator' доказывает, что samba может получить информацию от ldap

'getend group' показывает все стандартные группы домена (а также группы unix).

Глава 6

Службы печати

Разделы:

- **Понятие служб печати Windows**
- **Понятие служб печати Linux**
- **Совместное использование печатающих устройств через Samba**
- **Понятие автоматической загрузки драйвера печатающего устройства**
- **Перенос служб печати Windows на CUPS/Samba**

☑ Резюме

☑ Краткое резюме по разделам

☑ Часто задаваемые вопросы

Введение

Процесс распечатки документов связан с соответствующими настройками машин клиентов и сервера. При некорректной конфигурации ничто не заставит сервер Samba (служащий только для объединения двух частей процесса) осуществить печать. В связи с этим в данной главе рассматриваются шаги настройки печати как на сервере, так и на клиентских машинах, а также особые, характерные для Samba, шаги настройки корректного взаимодействия двух сторон.

Данная глава предполагает наличие у читателя понимания базовых административных задач на машине-клиенте Windows, таких как использование Мастера печати (Add Printer Wizard) или обнаружение принтера в сетевом окружении. Также предполагается, что в системе Linux установлена и сконфигурирована система CUPS (Common Unix Printing System). Эти задачи описываются вкратце.

В главе представлен общий обзор служб печати Windows и Linux, за которым следует пошаговое описание процесса конфигурирования печатающих устройств для наиболее оптимального их использования клиентами Samba и Windows и, наконец, подробно рассматривается конфигурирование принтера для клиентов Windows для выполнения операций по типу *«укажи и печатай»*, а также способы устранения возможных неисправностей.

Понятие служб печати Windows

В подсистеме печати Windows используется Интерфейс графических устройств (Graphics Device System, GDI). Для преобразования выходных данных в стандартный язык, называемый расширенным метафайлом (Enhanced Meta File, EMF), для объектов, отображаемых на экране и посылаемых на печать, используется одна и та же библиотека процедур. После этого метафайл обрабатывается фактическим драйвером дисплея или принтера. Это значительно упрощает печать («что видишь, то и получишь», What You See is What You Get, WYSIWYG).

Когда клиент печати Windows подключается к серверу печати Windows, он может автоматически получить и установить нужный драйвер принтера. Среди компьютерщиков этот процесс называется *«укажи принтер и печатай»*. На сервере сохранены драйверы для разных принтеров и для разных версий Windows с тем, чтобы клиенты с системой Windows, отличающейся от системы, установленной на сервере, могли без проблем выбрать драйвер для принтера. После того, как драйвер установлен на машину-клиент, он может запустить код обновления настроек системного регистра для конфигурирования параметров печати по умолчанию для данного принтера. Для принтеров со шрифтами PostScript драйвер обычно состоит из файла PPD (PostScript Printer Description, файл описания принтеров в PostScript, поставляемый производителем), отображающего все поддерживаемые принтером функции на соответствующие команды PostScript, PCL (язык управления печатью) или PJL (язык процесса

печати). Графический интерфейс драйвера принтера использует этот файл для обеспечения пользователя необходимыми выбираемыми параметрами печати.

В среде Windows, когда программное приложение пытается распечатать документ, происходит следующее:

1. Приложение делает запрос Интерфейсу графических устройств на преобразование выходных данных в формат EMF.
2. Драйвер принтера преобразовывает формат EMF в формат, «понятный» для принтера.
3. Готовый к печати файл скачивается на компьютер, выполняющий роль сервера печати.
4. Файл отправляется на печать.

Возможно выполнение одних шагов на машине-клиенте, а других — на сервере. Клиент может предпочесть преобразование собственно данных EMF, используя драйвер принтера локально, либо может отправить данные EMF на сервер с тем, чтобы последний запустил драйвер принтера.

Сервер печати может задать ограничения доступа для каждого принтера с ограничением подключения для определенных клиентов, ограничением времени суток, в течение которых принтер использовать нельзя, либо ограничить число пользователей, которые могут управлять принтером и отправляемыми на него заданиями. Клиент или сервер могут пользоваться приложениями очереди задания на печать (вызываются нажатием на значок принтера) для просмотра состояния запросов на печать, прерывания, возобновления или отмены печати, если зарегистрированный пользователь обладает на это полномочиями.

Понятие служб печати Linux

Для систем UNIX не разработан общий интерфейс для отображения и печати, подобный GDI Windows. Следовательно, каждое приложение форматирует выходные данные для принтера так, как считает нужным. Файлы изображений обычно сохраняются в формате графического обмена (Graphics Interchange Format, GIF), JPEG (Joint Photographic Experts Group) (разработанный группой экспертов в области фотографии метод сжатия изображений и соответствующий графический формат, часто используемый в WWW. Характерен компактностью файлов и более быстрой передачей, чем GIF, но медленным декодированием и «потерей» деталей изображения. — *Примеч. пер.)* или в большинстве других файлов с выводом в PostScript. Многие принтеры, используемые с системами UNIX, содержат встроенный интерпретатор PostScript, преобразующий входные данные в формате PostScript в растровое изображение, необходимое печатающему устройству. Для принтеров другого типа программы фильтрации на сервере печати «занимаются» преобразованием формата PostScript или файлов изображений в подходящие данному принтеру форматы.

Если выражаться проще, то печать можно рассматривать как процесс, состоящий из трех этапов.

1. Файл сохраняется на сервере печати и помещается в так называемую очередь на печать. Данный этап называется *скачиванием* файла печати.
2. Файл преобразовывается (в случае необходимости) в форму, распознаваемую данным принтером. Данный этап называется *фильтрацией* файла печати.
3. Файл (в надлежащем формате) отправляется на принтер, который может быть подсоединен к компьютеру локально (через последовательный, параллельный порты, USB и т. д.) либо по сети. Система скачивания требует простых команд для того, чтобы любой пользователь мог просмотреть состояние печатающих устройств: задания на печать, приостановка или возобновление печати, а также отмена заданий на печать в очереди.

Системы UNIX именно в области печати демонстрируют существенные «отклонения». Существуют две основные «вотчины» систем UNIX: одна — на базе System V (SYSV), а другая — в Беркли (BSD). В каждом из этих типов UNIX используются разные способы скачивания и разные наборы команд управления спулом печати. Во многих современных версиях UNIX имеются оба набора команд, что позволяет пользователю выбрать наиболее подходящий способ печати. Кроме этого неудобства, не все поставщики систем UNIX используют одинаковые параметры командной строки для использования программ скачивания. Новые и усовершенствованные версии спулеров печати добавляют неразберихи. Новые функции, добавленные Common UNIX Print System (CUPS), подробно рассматриваются ниже. В табл. 6.1 перечислены команды, обычно имеющиеся в системе печати типа SYSV, с полным описанием опций каждой команды (см. оперативную страницу руководства для каждой команды).

Табл. 6.1. Команды печати Системы V

Команда SYSV	Описание
lpsched	Демон, планирующий задания на печать (как правило, запускается системой во время загрузки)
lpshut	Отключает демон планировщика заданий на печать
enable	Активизирует принтер для использования планировщиком и обеспечивает печать заданий
disable	Отключает принтер от использования планировщиком, а также отменяет печать заданий
reject	Предотвращает принятие заданий утилитой lp для указанного принтера
accept	Обеспечивает принятие утилитой lp заданий для указанного принтера
lpmove	Перемещает задания печати с одного принтера на другой
lp	Отправляет задание на печать в очередь
cancel	Отменяет задание на печать
lpstat	Отображает информацию о принтере и состоянии задания на печать

В табл. 6.2 приведены команды печати, обычно имеющиеся в системе печати типа BSD. Подробное описание доступных опций для каждой команды см. в оперативной странице руководства для данной команды.

Табл. 6.2. Команды печати BSD

Команда BSD	Описание
lpd	Демон, планирующий задания на печать (как правило, запускается системой во время загрузки)
lpc	Программа управления принтером, используемая для активизации/деактивизации принтера, перестраивания заданий в очереди и определения состояний принтеров и их очередей
lpr	Отправляет задание печати в очередь
Lprm	Удаляет задание печати из очереди
lpq	Отображает информацию о принтере и состоянии задания на печать

Конфигурирование печати на Linux с помощью BSD или SYSV

В данном разделе рассматривается активизация системы UNIX при распечатке документов на принтере, подключенном непосредственно к системе. Подробности различаются в зависимости от базового типа системы (BSD или SYSV), но сначала необходимо создать нужные каталоги и файлы фильтров печати, а также проинформировать систему о местоположении и возможностях принтера. В нижеприведенных примерах предполагается, что принтер имеет имя «*myprinter*».

В системах типа SYSV необходимо создать файл модели интерфейса либо использовать один из файлов модели, поставляющихся с системой, и **lpadmin** для установки принтера. При этом будет создан необходимый каталог спулинга, добавлен интерфейсный файл */var/spool/lp/interface/myprinter* и создан файл */var/spool/lp/member/myprinter*, указывающий на физическое устройство, к которому подключен принтер. Затем запускаются команды **enable myprinter** и **accept myprinter** для активизации принтера и обеспечения направления заданий на печать.

В системах типа BSD необходимо создать запись **/etc/printcap** и любые необходимые программы фильтрации, создать каталог подкачки (обычно */var/spool/lpd/myprinter*), после чего воспользоваться **lpc** для активизации принтера и его очереди документов на печать.

Большинство версий UNIX имеют графические инструменты или сценарии добавления принтеров в систему. Рекомендуется использование одного из этих инструментов для установки принтеров, если пользователь не является администратором со значительным опытом установки устройств печати. Создание записей **/etc/printcap** или фильтров принтеров может представлять определенную сложность, но обучение не входит в рамки данной книги.

После установки принтера в систему UNIX документ можно распечатывать. Для нижеприводимых примеров предполагается, что имя принтера *myprinter* и требуется распечатать текстовый файл с именем */tmp/myfile*.

Для выполнения печати в системе типа BSD следует подать команду:

```
lpr -Pmyprinter /tmp/myfile
```

При подаче этой команды программа lpr копирует файл */tmp/myfile* в каталог подкачки */var/spool/lpd/myprinter*. После этого программа-демон подкачки печати (lpd) взаимодействует с базой данных возможностей принтера /etc/printcap для определения способа обработки файла и местоположения отправки данных вывода.

Для осуществления печати в системе типа SYSV необходимо подать команду:

```
lp -dmyprinter /tmp/myfile
```

При этом команда lp сделает ссылку на файл */tmp/myfile* в каталоге подкачки */var/spool/lp/request/myprinter* (при необходимости создания копии вместо ссылки в вышеприведенную команду можно добавить опцию **-c**). Затем программа-демон подкачки печати (lpsched) обрабатывает этот файл и отправляет его в нужное место, исходя из информации, обнаруживаемой в программе-интерфейсе в каталоге */var/spool/lp/interface/myprinter*. Если для создания копии файла не задается опция -c, тогда необходимо убедиться в том, что файл-оригинал не будет удален до завершения печати.

Также необходимо убедиться в том, что файл можно распечатать в системе UNIX с помощью одной из вышеперечисленных команд, до попытки сделать этот принтер доступным через Samba. Большинство принтеров в системах UNIX могут печатать текстовые файлы (также известные как файлы ASCII) либо файлы на языке описания страницы PostScript (файлы, начинающиеся с символов %!).

Как только появится возможность корректной печати, необходимо убедиться в том, что пользователь, выбранный как учетная запись гостя (guest) для Samba, также может осуществлять корректную печать. Поскольку учетная запись пользователя-гостя не обязательно предоставляет возможность входа на машину UNIX, можно проверить возможность печати из этой учетной записи с первоначальным переходом к учетной записи root на машине с использованием команды **su** и последующим переходом в учетную запись пользователя Samba.

Иногда команды печати могут отсутствовать в пути поиска для пользователя. Для задания полного имени пути команды можно использовать команду **whereis**. Если предположить, что учетная запись гостя для Samba имеет имя **nobody**, то в системе UNIX типа BSD можно выполнить следующие команды:

```
[root@linuxbox /]# su - nobody
[nobody@linuxbox /]$ whereis lpr
lpr: /usr/bin/lpr /opt/../bin/lpr /usr/man/man1/lpr.1
[nobody@linuxbox /]$ /usr/bin/lpr -Pmyprinter /tmp/myfile
```

При этом сообщается, что команда **lpr** обнаруживается в **/usr/bin/lpr** в этой системе. После этого можно использовать полный путь для исполнения команды печати файла.

Конфигурирование печати на Linux с помощью CUPS

В отличие от традиционных, описанных выше, видов печати по типам BSD или SYSV, общая система печати UNIX — намного больше спулинговой системы печати. Это — полная система управления печатью, основанная на Протоколе печати Интернет (Internet Printing Protocol, IPP), которая обеспечивает локальное или удаленное управление сервером печати. Доступ ко многим функциям управления можно осуществить через web-браузер для получения независимого от платформы способа управления всеми службами печати. Он поддерживает интерфейсы командной строки BSD и SYSV, а также нескольких графических интерфейсов третьих сторон. В текущей версии CUPS применяется Ghostscript для преобразования файлов изображений и файлов растровых изображений формата PostScript для принтеров, не поддерживающих формат PostScript. Для получения списка устройств, поддерживаемых текущей версией Ghostscript, можно запустить команду **ghostscript -h**.

Как читатель помнит, в модели печати Windows сервер может получить задание на печать либо в формате, полностью готовом для печати, либо в формате, требующем преобразования (EMF). Система CUPS поддерживает создание так называемых заготовок принтеров, где не требуется преобразования выходного файла, либо «интеллектуальных» принтеров, где CUPS выполняет преобразование в формат, распознаваемый принтером. CUPS также использует файл Описания принтера в формате PostScript (PPD) для описания возможностей принтера. CUPS расширяет это понятие также до принтеров не-PostScript, для которых доступны многие файлы PPD (файлы описания принтеров в PostScript). При наличии файлов-PPD для всех типов принтеров CUPS может отобразить для клиентов все принтеры как принтеры PostScript и предоставить клиентам возможность выбора всех поддерживаемых опций печати. В CUPS разработан собственный драйвер PostScript для Windows NT/200x/XP, для более ранних версий Windows можно воспользоваться драйвером Adobe PostScript.

Подробное разъяснение принципов работы CUPS не входит в рамки данной главы (существует множество источников информации по данной теме). После установки CUPS доступной будет вся документация. Набор документации Samba HOWTO содержит очень хорошее описание работы и принципов CUPS. Изначально CUPS задает цепи фильтров входящих файлов для их преобразования в PostScript, после чего обрабатывает PostScript с помощью внешней программы GhostScript в нужный формат печати. После этого с помощью выходных буферов осуществляется преобразование для принтера, который может быть подключен локально (через параллельный, последовательный порт и т. д.) либо доступ к нему осуществляется через сеть TCP/IP (IPP, LPR/LPD, SMB и т.-д.).

Имея общий формат ввода (PostScript), CUPS может легко выполнять такие функции, как подсчет страниц, учет, печать нескольких страниц на листе (n-up) печать и т. д. Поскольку CUPS — это не просто полная система управления печатью и не просто спулер печати, то в ней имеются возможности настройки квот для ограничения передаваемых пользователем числа страниц или размера заданий, элементы управления доступом, аутентификация и даже возможности шифрования. Несколько принтеров можно даже объединить в класс для высокодоступной печати.

ПРИМЕЧАНИЕ Если принтер настраивается как «сырой» (raw printer — входные данные отправляются непосредственно), тогда функции учета игнорируются и задание рассматривается как одна страница.

Можно добавлять принтеры и управлять ими с помощью описанных выше стандартных команд BSD или SYSV, одного из нескольких графических пользовательских интерфейсов (GUI), например **kdeprint**, либо web-интерфейса, устанавливаемого с CUPS. Когда CUPS установлен и запущен, войдите в браузер и подключитесь к http://localhost:631 для доступа к оперативной документации либо для доступа ко всем функциям управления и администрирования, как показано на рис. 6.1.

ПРИМЕЧАНИЕ По умолчанию CUPS конфигурируются только для обеспечения доступа из локального хоста, однако также возможна конфигурация для обеспечения связей с другими машинами.

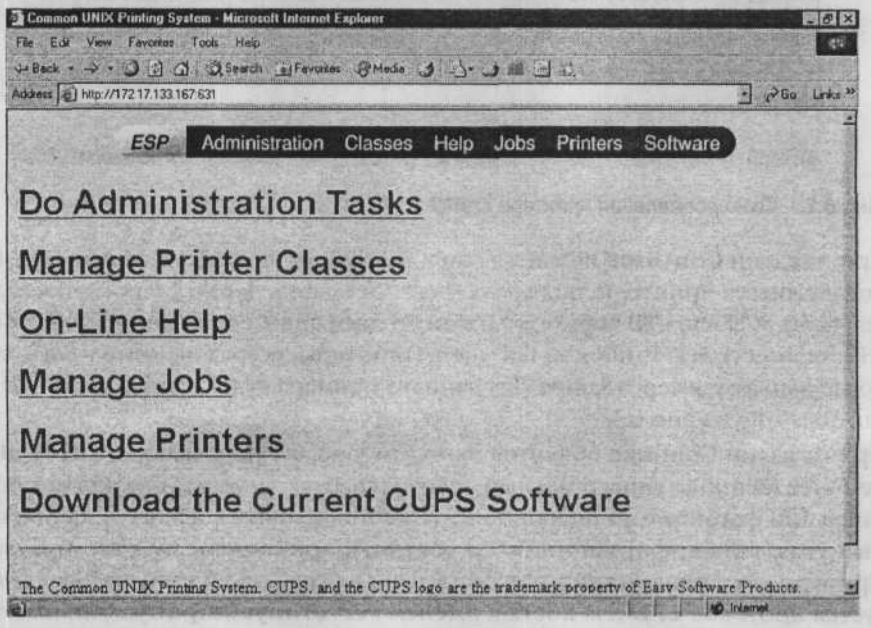

Рис. 6.1. Стартовая страница веб-интерфейса CUPS

6 Зак. 1269

1. При выборе закладки **Administration** появится подсказка для ввода имени пользователя и пароля.
2. Введите **root** в качестве имени пользователя и введите нужный пароль. Рассмотрим настройки принтера HP LaserJet с именем globe на удаленном сервере LPR/LPD с именем **server.mycompany.com**.
3. В окне Admin выберите **Add Printer**. Появится окно, показанное на рис. 6.2, позволяющее ввести имя, местоположение и описание данного принтера (необходимо только имя).

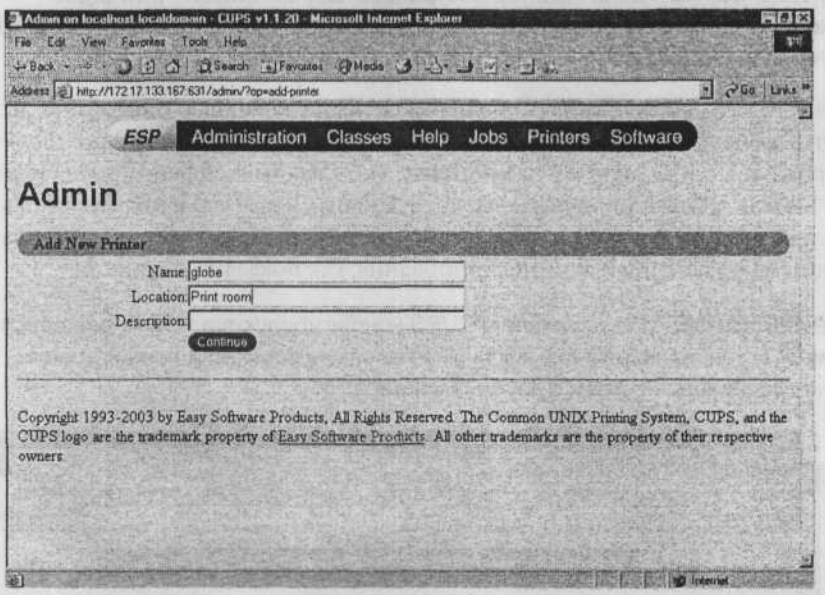

Рис. 6.2. Окно добавления принтера CUPS

4. При нажатии **Continue** появится окно для выбора устройства для печати. CUPS поддерживает принтеры, подключенные локально к параллельному, последовательному, SCSI или USB портам, а также к сетевым принтерам с помощью AppSocket (HP JetDirect), HTTP, IPP или LPD/LPR. Принтеры, подключенные к SMB, также поддерживаются через Samba. Для данного примера будет использован LPD/LPR, как показано на рис. 6.3.
5. При нажатии Continue появится окно (см. рис. 6.4) для выбора **URI** (Uniform Resource Identifier, универсальный идентификатор ресурса) устройства для принтера. URI формируется подобно URL (Uniform Resource Locator, унифицированный указатель информационного ресурса), применяемому в веб-браузерах. Примеры для различных типов представлены в окне. Для данного примера используется протокол **LPD** для хоста с именем **server.mycompany.com**, имеющем очередь на печать с именем **globe**.

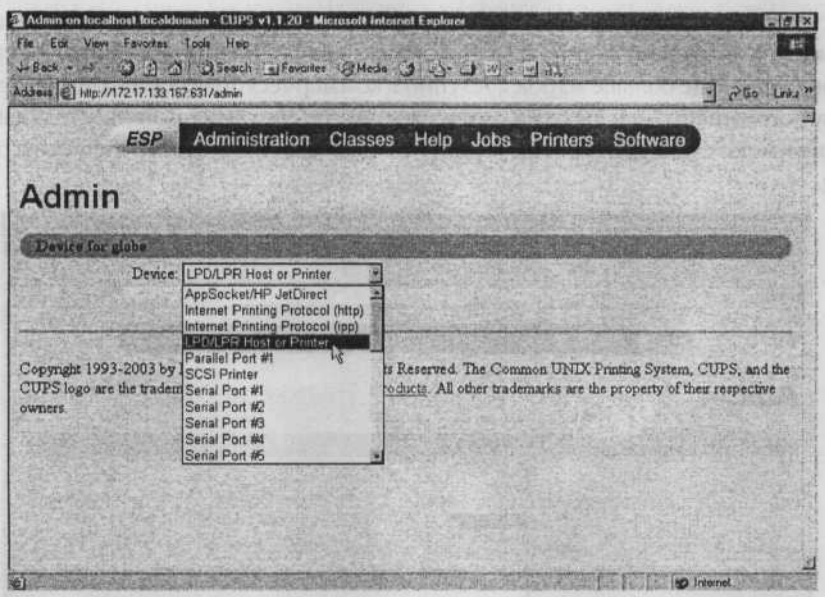

Рис. 6.3. Конфигурирование устройства принтера

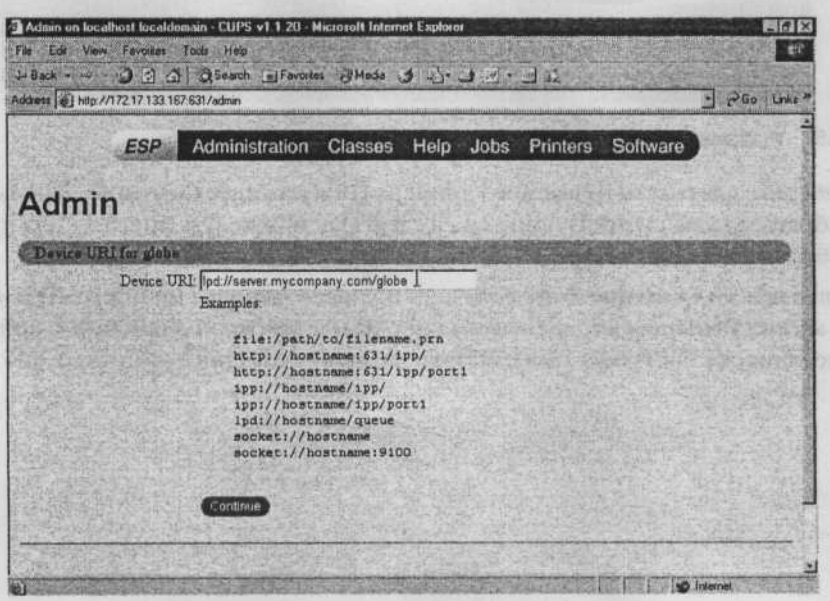

Рис. 6.4. Задание устройства URI

6. Введите URI и нажмите **Continue**. Теперь появляется возможность выбора марки (**Make**) принтера (см. рис. 6.5). В CUPS входят драйверы для нескольких марок принтеров; еще больше марок доступно в коммерческой версии CUPS от компании Easy Software Products на сайте www.easysw.com/printpro. Дополнительные драйверы имеются на сайтах http://gimp-print.sourceforge.net и www.linuxprinting.org.

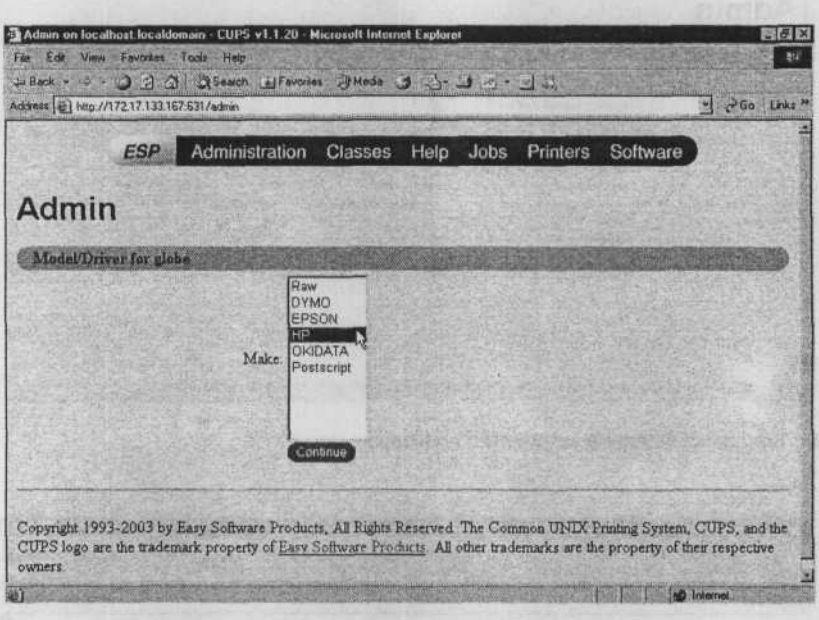

Рис. 6.5. Указание марки принтера

7. Выберите для рассматриваемого примера **HP** и нажмите **Continue**. Теперь можно выбрать модель (**Model**) принтера в следующем окне (см. рис. 6.6). Для примера выберем **LaserJet Series**.
8. При нажатии **Continue** будут получены полные настройки принтера. При нажатии на кнопку **Printers** в верхней части страницы появится информация о принтерах, имеющихся в системе, а также кнопки различных заданий (см. рис. 6.7).

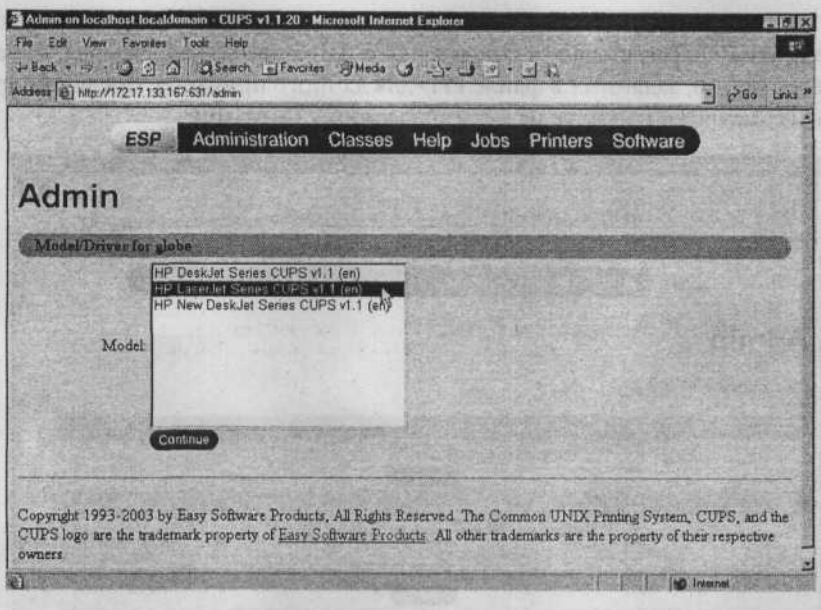

Рис. 6.6. Указание модели принтера

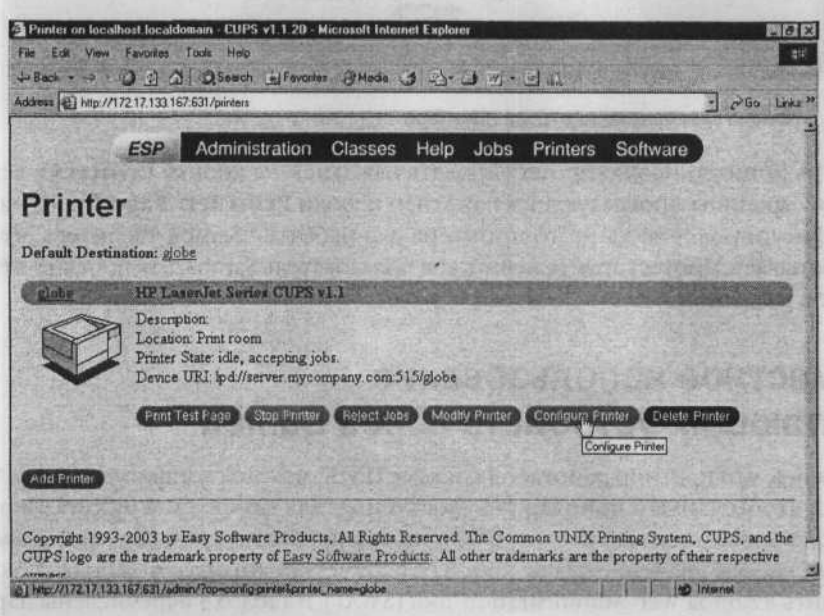

Рис. 6.7. Просмотр настроек принтеров

9. Для принтера потребуется сконфигурировать опции. Нажмите на кнопку **Configure Printer**; появится окно (см. рис. 6.8), позволяющее выбрать значения для всех опций, заданных в файле PPD для данного принтера. После выбора всех нужных значений нажмите на любую из кнопок **Continue**.

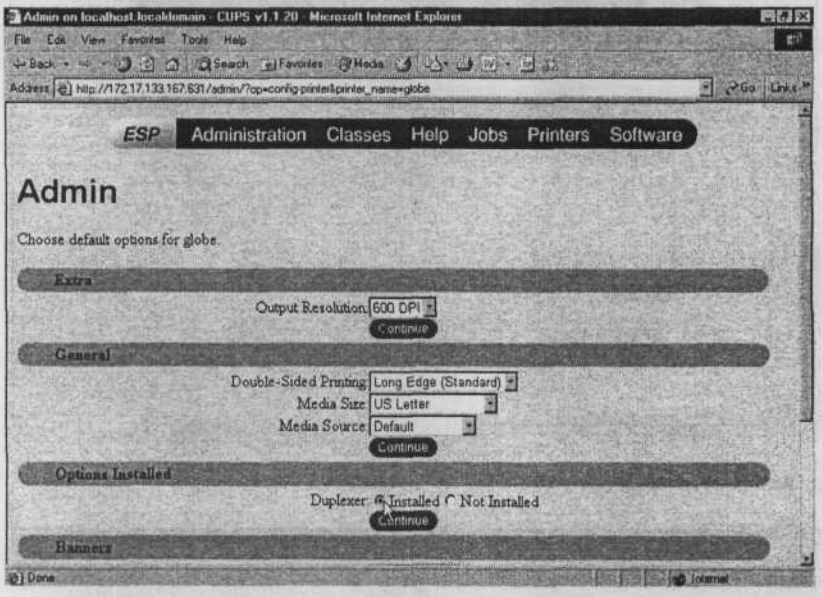

Рис. 6.8. Конфигурирование настроек принтера

10. Теперь принтер можно протестировать нажатием на кнопку **Printers** в верхней части страницы с последующим нажатием кнопки **Print Test Page**. Перед началом конфигурирования данного принтера для работы с Samba убедитесь, что тест срабатывает. Протестируйте печать как пользователь Samba, как описано в предыдущем разделе.

Совместное использование печатающих устройств через Samba

Убедившись, что принтер работает в системе UNIX, можно сконфигурировать Samba для того, чтобы данный принтер стал доступным для клиентов Windows. Перед настройкой возможности совместного использования рассмотрим параметры *smb.conf*, имеющие особое значение для печати. Это параметры, которые можно просмотреть и изменить в Samba Web Administration Tool (SWAT). В табл. 6.3 перечислены параметры печати, находящиеся в **smb.conf**. Некоторые параметры имеют псевдонимы, указанные в скобках после основного имени.

Табл. 6.3 Параметры печати smb.conf Samba

Имя параметра	Описание
printcap name (printcap)	Глобальный параметр, используемый для подмены скомпилированного внутри программы имени printcap, с помощью которого сервер получает список принтеров
load printers	Глобальный параметр, указывающий, все ли принтеры из printcap будут загружены для просмотра по умолчанию
printable (print ok)	Разрешает вывод файлов на печать
Printing	Задание стиля печати для системы; параметр определяет стиль интерпретирования информации о состоянии принтера. Он управляет параметрами по умолчанию для команд **print**, **lpq**, **lppause**, **lpresume** и **lprm**
print command	По окончании вывода задачи на обслуживание эта команда будет выполнена через вызов system() для обработки файла
lpq command	Используется для получения информации о состоянии очереди на печать
lprm command	Используется для удаления того или иного задания на печать
lppause command	Используется для остановки печати или вывода особого задания на печать
lpresume command	Используется для перезапуска или продолжения печати либо для вывода особого задания на печать
queuepause command	Используется для остановки подачи на принтер заданий на печать, находящихся в очереди на печать
queuresume command	Используется для возобновления отправки заданий на печать в очередь на печать
Comment	Текстовое поле, появляющееся в разделяемом ресурсе при запросе сервера клиентом списка доступных ресурсов коллективного использования
path (directory)	Каталог, в который будут скачиваться данные на печать до выполнения команды печати (print command)
printer (printer name)	Имя принтера, на который будут отправляться задания на печать
PostScript	При подаче данной команды принтер интерпретирует файл для печати как файл PostScript путем добавления символов «%!» в начало данных вывода на печать
lpq cache time	Глобальный параметр, управляющий временем кэширования информации, возвращенной командой, указанной в команде **lpq**, для предотвращения чересчур частого вызова этой команды
min print space	Задание минимального объема свободного дискового пространства, необходимого до вывода задания на печать
guest account	Имя пользователя UNIX, которое будет использоваться для доступа к службам, обозначенным как «guest ok»
guest ok (public)	Указывает, что для обращения к этой службе пароль не требуется. Доступ будет произведен от имени пользователя, указанного в параметре guest account

▶▶

Табл. 6.3. *(окончание)*

Имя параметра	Описание
hosts allow (allow hosts)	Список машин, которым будет разрешен доступ к данной службе. Может быть задан по имени или IP-адресу
hosts deny (deny hosts)	Список машин, доступ которым к данной службе будет особо ЗАПРЕЩЕН. Может быть задан по имени или IP-адресу. При наличии конфликтов приоритет имеет список hosts allow
browseable (browsable)	Управляет появлением или не появлением данной службы в списках просмотра клиентов
Available	Позволяет отключить службу. Все попытки подключения будут неудачными
Preexec (exec)	Задает выполнение команды при каждом подключении к службе
root preexec	Задает выполнение команды от имени root при каждом подключении к службе
Postexec root postexec	Задает выполнение команды при каждом отключении службы
	Задает выполнение команды в качестве корня при каждом отключении от службы

В дополнение к вышеперечисленным параметрам в службу печати можно включить большинство параметров на уровне службы. Существует семь переменных, специально предназначенных для печати, и несколько других, применяемых при создании различных команд, описанных выше. В общем виде эти переменные представлены в табл. 6.4.

Табл. 6.4. Переменные печати smb.conf

Имя переменной	Описание
%f или %s	Только имя файла для печати (без пути)
%p	Имя принтера UNIX для использования
%j	Номер задания на печать (для использования в командах управления очередью на печать)
%J	Имя задания, отправленного клиентом
%c	Количество печатаемых страниц (если известно)
%z	Размер скачиваемого файла (если известно)
%S	Имя текущей службы
%U	Имя сессии в сессии (имя пользователя, необходимое клиенту, не обязательно то же, что он имеет)
%m	Имя NetBIOS клиентской машины
%L	Имя NetBIOS сервера
%T	Текущая дата и время

Перед настройкой совместно используемого ресурса в Samba необходимо определить стиль печати, используемый в системе. Стиль печати, заданный по умолчанию, устанавливается во время компилирования Samba и является «вшитым» в его код. Значения по умолчанию **printcap name** и учетной записи гостя также задаются во время компилирования. Можно определить значения по умолчанию вашей версии Samba путем создания пустого файла конфигурации (или с помощью */dev/null*) и запуском **testparm** для этого файла. Для нахождения значений параметров **printing name**, **printcap name** и **guest account** по умолчанию запустите следующие команды:

```
[root@linuxbox /]# testparm -sv /dev/null | grep printing
printing = bsd
[root@linuxbox /]# testparm -sv /dev/null | grep printcap
printcap name = /etc/printcap
[root@linuxbox /]# testparm -sv /dev/null | grep guest account
guest account = nobody
```

Если значение по умолчанию некорректно, то его можно изменить добавлением записи **printing = <нужное значение>** и записи **printcap name = <путь к printcap>** в раздел **global** файла **smb.conf**. Неплохо размещать эти записи в файле **smb.conf** даже при корректных значениях по умолчанию. При этом становится абсолютно очевидно, какие значения будут использованы. Затем стиль печати определяет значения по умолчанию для других команд печати. В табл. 6.5 показаны команды печати по умолчанию, задаваемые для каждого стиля печати. Если эти команды не корректны для существующей системы, то их можно изменить в разделе **global** файла **smb.conf**.

Табл. 6.5. Значения по умолчанию стиля печати для разных систем печати

Стиль печати	Команды по умолчанию
BSD, AIX, NT, OS2	print command = lpr -r -P'%p'%s lpq command = lpq -P'%p' lprm command = lprm -P'%p'%j lppause command = lpresume command = queuepause command = queueresume command =
LPRNG, PLP	print command = lpr -r -P'%p'%s lpq command = lpq -P'%p' lprm command = lprm -P'%p'%j lppause command = lpc hold '%p'%j lpresume command = lpc release '%p' %j queuepause command = lpc stop '%p' queueresume command = lpc start '%p'

▶▶

▶▶ **Табл. 6.5.** *(окончание)*

Стиль печати	Команды по умолчанию
CUPS	print command = /usr/bin/lp -d '%p' %s; rm %s lpq command = /usr/bin/lpstat -o '%p' lprm command = /usr/bin/cancel '%p' -%j' lppause command = lp -I '%p-%' -H hold lpresume command = lp -I '%p-%' -H resume queuepause command = /usr/bin/disable '%p' queueresume command = /usr/bin/enable '%p' printcap name = lpstat
SYSV	print command = lp -c -d%p %s; rm %s lpq command = lpstat -o%p lprm command = cancel %p-%j lppause command = lp -i %p-%j -H hold lpresume command = lp -i %p-%j -H resume queuepause command = disable %p queueresume command = enable %p
HPUX	print command = lp -c -d%p %s; rm %s lpq command = lpstat -o%p lprm command = cancel %p-%j lppause command = lpresume command = queuepause command = disable %p queueresume command = enable %p
QNX	print command = lp -r -P%p %s lpq command = lpq -P%p lprm command = lprm -P%p %j lppause command = lpresume command = queuepause command = queueresume command =

В настоящее время Samba поддерживает следующие системы печати: SYSV, AIX, HPUX, BSD, QNX, PLP, LPRNG, CUPS, NT и OS2. Оба последних типа (NT и OS2) — LPR (удаленный линейный принтер) в соответствующей OS. Записи для CUPS — значения, которые будут получены, если Samba не была скомпилирована с поддержкой CUPS (библиотекой libcups). Если Samba была объединена с библиотеками, то она будет использовать CUPS API для отправки заданий на печать, управления принтером, очередью на печать, а все записи для команд по умолчанию будут игнорироваться.

При необходимости указания какой-то особой команды печати или одной из других команд при использовании печати CUPS в Samba с помощью libcups, можно задать стиль печати на **printing = sysv** в отдельном разделе принтера и перекрыть имеющуюся там команду. Это позволяет CUPS управлять всеми прочими принтерами и переопределит только настройки для одного, отдельно взятого принтера.

Затем, для возможности коллективного использования принтера создадим необходимые записи в **smb.conf**. Стиль печати будет CUPS, имя принтера в системе UNIX — **lp** и принтер будет использоваться коллективно под именем **myprinter** (любой пользователь сможет получить к нему доступ). Файлы будут помещены в каталог с именем ***/var/spool/samba*** с разрешениями **0700** до того, как они будут отправлены в спулер системы печати. В это время никакие другие принтеры в системе не будут доступны для коллективного использования. Следующие записи отражают все необходимое в **smb.conf**:

```
[global]
printing = cups
printcap name = cups
guest account = nobody
load printers = no
[myprinter]
printable = yes
writeable = no
path = /var/spool/samba
guest ok = yes
printer = lp
create mask = 0700
browseable = yes
```

Запись **printing = cups** в разделе global задает другие команды печати значениям, приведенным в таблице выше, либо использует CUPS API, если Samba скомпилирована на использование libcups. Запись **load printers = no** указывает на то, что все принтеры, управляемые CUPS, не будут автоматически настроены на коллективное использование. После этого задается совместный ресурс **myprinter** и объявляется как принтер с записью **printable = yes**. Ресурсы совместного использования принтеров всегда будут обеспечивать запись в каталог, указанный в параметре **path =** (права пользователя UNIX это позволяют), через спулер данных печати. Строка **writeable = no** указывает на то, что доступ к совместному ресурсу не с целью печати не будет позволять запись. Задание **ok = guest** задает совместный ресурс для обеспечения доступа всем пользователям от имени учетной записи, указанной в **guest account**.

По причине того, что имя принтера в UNIX не является именем, которое должно использоваться для клиентов Windows, имя UNIX задается явно параметром **printer = lp**. Если этот параметр не задан, то предполагается, что имя принтера UNIX будет тем же, что имя совместно используемого ресурса. Здесь важно помнить, что, несмотря на то, что для клиентов Windows имя совместно используемого ресурса

не зависит от регистра набора символов, имя, указанное в параметре **printer =** (либо имя совместно используемого ресурса, если этот параметр не указан), должно совпадать с именем принтера, определенного в системе.

Запись **create mask = 0700** снимает все разрешения группы владельца и прочих (other) с файла, отправляемого в совместно используемый ресурс.

Наконец, запись **browseable = yes** обеспечивает доступ к этому принтеру клиентам SMB, когда те просматривают информацию на сервере из диалогового окна Add Printer. Эту запись можно установить на **no** при необходимости сокрытия этого принтера от клиентов. Они по-прежнему смогут подключаться к принтеру при условии ввода корректного имени.

В случае, если к системе подключен только один принтер, то в файле **smb.conf** сравнительно просто создать определение для коллективного использования. При наличии нескольких принтеров Samba обладает механизмом, называемым разделом **printers**, который легко обеспечивает совместное использование всех принтеров, подключенных к системе, созданием только одной записи раздела в файле **smb.conf**. Ограничением на использование этого метода является то, что все принтеры должны иметь одинаковые установочные параметры (за исключением комментариев) и имя принтера должно быть тем же, что и имя совместно используемого ресурса.

Предположим, что к системе подключены три принтера с именами **hp**, **slides** и **color**. В файле **smb.conf** можно создать один раздел, который будет предоставлять в совместное использование все эти принтеры с одними и теми же параметрами. Следующие записи отражают то, что должно быть добавлено в файл **smb.conf**:

```
[global]
printing = cups
printcap name = cups
guest account = nobody
load printers = yes
[printers]
printable = yes
writeable = no
path = /var/spool/samba
guest ok = yes
create mask = 0700
browseable = no
```

ПРИМЕЧАНИЕ Не указывайте путь вывода файлов в том же каталоге, что использует спулер печати, иначе при распечатке на Samba результаты могут быть непредсказуемыми.

Рассмотрим отличия от предыдущего примера. В разделе **global** настройка параметра **load printers** изменена на **yes**. Он используется в связи с разделом **printers**. Когда клиент делает попытку подключения к совместно используемому ресурсу на

сервере, Samba сначала проверяет на совпадение все заданные разделы в **smb.conf**. При отсутствии совпадений Samba проверит, задан ли раздел **homes**, и, если — да, то попытается найти соответствие имени пользователя в локальном файле паролей. При отсутствии совпадений и при наличии раздела **printers** Samba будет искать совпадения в «файле», определенном **printcap name**. Обратите внимание на то, что в системе SYSV оно может быть определено как команда **lpstat**, в которой будет приведен список всех доступных принтеров.

При обнаружении совпадения (соответствия) создается новый раздел путем копирования информации в раздел **printers**, в котором имя совместно используемого ресурса совпадает с именем локального принтера. При отсутствии параметра **printer** задается имя принтера, совпадающее с именем совместно используемого ресурса. При недопущении «гостей» и если в запрос соединения не введено имя пользователя, то последнее также устанавливается равным имени принтера. Если не включен параметр **printable**, тогда в файле регистрации **smbd** появится предупреждающее сообщение, и Samba настроит данный раздел для возможности печати. Параметр **browseable** задает появление (или непоявление) имен принтеров в просмотровом списке принтеров. Поскольку данное имя совместно используемого принтера не является фактическим именем принтера, то, во избежание сбоев, лучше всего настроить параметр как **browseable = no**.

Разделом **printers** можно пользоваться даже в том случае, когда нет необходимости пользоваться всеми принтерами, подключенными к системе. Это можно сделать указанием псевдо-printcap, содержащим только имена принтеров, коллективное использование которых планируется. В каждой строке этого файла содержится имя принтера и все возможные псевдонимы в следующем формате:

имя | псевдоним | псевдоним | псевдоним с пробелами

Имена псевдонимов не требуются. Если псевдоним содержит пробелы, тогда этот псевдоним заменяется на параметр комментария в созданном совместном ресурсе.

Раздел **printers** также можно использовать в качестве шаблона для создания совместно используемого принтера, параметры которого будут отличаться от параметров остальных принтеров. Возможно, возникнет потребность ограничения числа людей, которые смогут пользоваться цветным принтером. В файл **smb.conf** можно добавить следующий раздел:

```
[color]
copy = printers
guest ok = no
browseable = yes
valid users = @sales
```

При этом совместно используемый принтер **color** будет определен со всеми параметрами, содержащимися в **printers**, после чего изменен для запрета доступа «гостей», для возможности просмотра совместно используемого принтера и доступа

только пользователей из отдела продаж. С помощью параметра **copy** в новое определение не потребуется включать все общие параметры, поэтому такие параметры, как **printable**, **path** и т. д. в определение включать не потребуется.

Понятие автоматической загрузки драйвера печатающего устройства

Систему Samba можно сконфигурировать на автоматическое скачивание драйверов принтеров для клиентов Windows, как это делается на сервере печати Windows NT (или более поздних версий). Сюда входит создание нового совместного ресурса под названием **print$**, где будут расположены файлы драйвера, установка драйверов в нужное место в совместном ресурсе **print$**, связывание драйвера с печатающим устройством совместного пользования, а также настройка опций принтера по умолчанию.

Создание совместно используемого ресурса **print$** включает в себя создание соответствующих каталогов на сервере Samba, а также настройку нужных записей файла **smb.conf**. Для поддержки скачивания драйверов для различных версий Windows в каталоге, созданном для совместного ресурса **print$**, потребуется создание различных подкаталогов. В табл. 6.6 перечислены подкаталоги, необходимые для каждой поддерживаемой архитектуры.

Табл. 6.6. Подкаталоги драйверов печати по архитектурам

Имя подкаталога	Архитектура драйвера
W32X86	Windows NT x86
WIN40	Windows 95/98
W32ALPHA	Windows NT Alpha_AXP
W32MIPS	Windows NT R4000
W32PPC	Windows NT PowerPC

На севере Samba можно создать группу для обозначения того, какие пользователи будут иметь право администрирования (возможность добавления новых драйверов и настройки свойств принтера). Если предположить, что имя созданной группы — **ntadmin**, в раздел **global** файла **smb.conf** можно добавить следующую запись:

```
printer admin = @ntadmin
```

Запись совместного ресурса **print$** может выглядеть следующим образом:

```
[print$]
comment = Download area for printer drivers (область скачивания для драйверов
принтера)
path = /var/samba/drivers
guest ok = yes
browseable = no
read only = yes
write list = @ntadmin, root
```

Если необходимо, чтобы к принтерам имели доступ только аутентифицированные пользователи, то параметр **guest ok = yes** можно удалить. При настройке параметра **browseable = no** совместный ресурс не проявляется в Сетевом соседстве (по умолчанию совместные ресурсы, имена которых заканчиваются на **$**, будут видны только администратору). Настройка параметра **read only = yes** запрещает загрузку файлов драйвера в этот совместный ресурс путем запрета на запись. Запись **write list = @ntadmin, root** предоставляет суперпользователю и пользователям в группе ntadmin UNIX разрешение на запись с тем, чтобы появилась возможность загрузки новых драйверов. Убедитесь также, что в каталогах совместного пользования предоставлено право записи для группы **ntadmin**, поскольку Samba не перекрывает разрешений нижележащей файловой системы.

Следующим шагом будет установка драйверов принтера на сервер Samba в надлежащий каталог совместно используемого ресурса **print$**. Это можно сделать с помощью команды **rpcclient** Samba либо с помощью Мастера добавления новых принтеров Windows (Windows Add Printer Wizard) от клиента NT/2000/XP. При желании использовать **rpcclient** обратитесь к документации Samba, потому что это может оказаться сложным, но здесь не описывается.

С помощью Windows Explorer войдите в Network Neighborhood и откройте хост Samba. Появится папка **Printers**, при открытии которой появится список всех принтеров, совместно используемых хостом Samba. На рис. 6.9 показано окно, появляющееся при нажатии правой кнопки мыши на ярлык принтера, с выбранной строкой **Properties** (свойства).

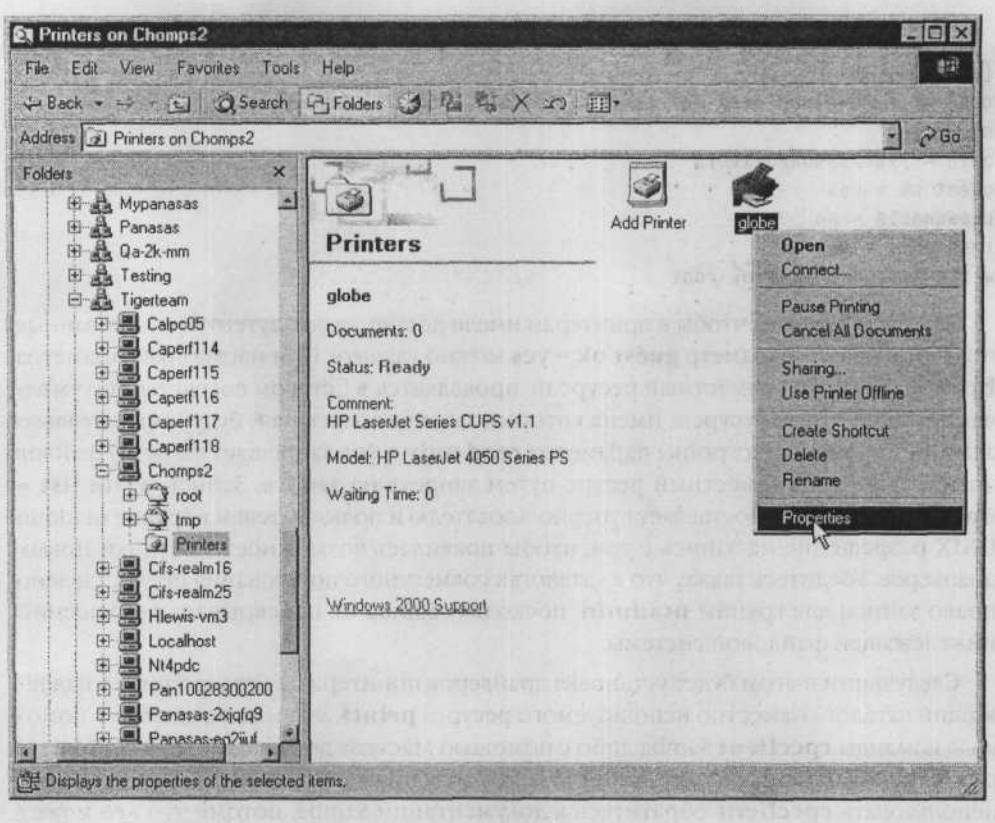

Рис. 6.9. Отображение свойств принтера системы Samba

Поскольку драйвера, относящегося к этому принтеру, нет, будет выдано сообщение об ошибке, подобное показанному на рис. 6.10. Формулировки варьируются в зависимости от версии Windows.

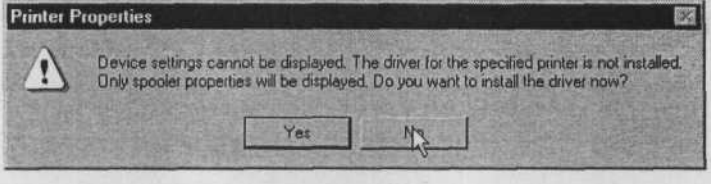

Рис. 6.10. Диалоговое окно запроса установки драйвера

Не нажимайте кнопку **Yes**, поскольку это действие устанавливает драйверы в локальную систему. При выборе **No** появится диалоговое окно **Printer Properties**. Выберите закладку **Advanced**, которая позволит выбрать строку **New Driver** (см. рис. 6.11) и установить драйвер на сервер Samba. Убедитесь в подключении в качестве пользователя с административной учетной записью, указанной в параметре **printer admin**, а также в наличии надлежащих каталогов, как указано в совместном ресурсе **print$**, и подкаталога, требуемого архитектурой клиента.

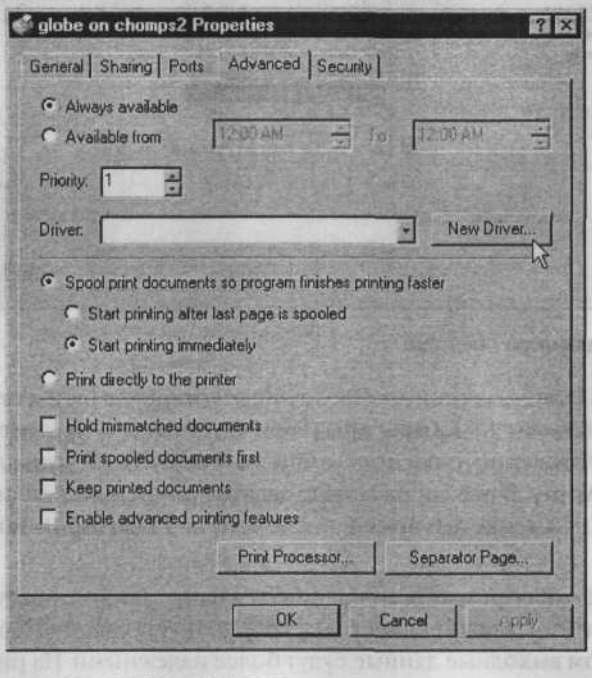

Рис. 6.11. Диалоговое окно свойств принтера

После нажатия на кнопку **New Driver** появится возможность выбора драйвера (см. рис. 6.12), файлы будут копироваться в надлежащий каталог на сервере Samba. После этого система (Samba) обновит файлы базы данных для указания того, какой из драйверов связан с этим принтером.

После установки файлов драйвера необходимо выполнить дополнительные действия. На сервере Windows установка драйверов может запустить программу на сервере для установки первоначальных режимов устройств. Поскольку программы не будут работать на сервере Samba, потребуется дополнительная работа по их настройке. Самый простой выход — это установка принтера на машине клиента, после чего следует открыть диалоговое окно значений печати по умолчанию (Printing Defaults) и скопировать настройки с машины клиента.

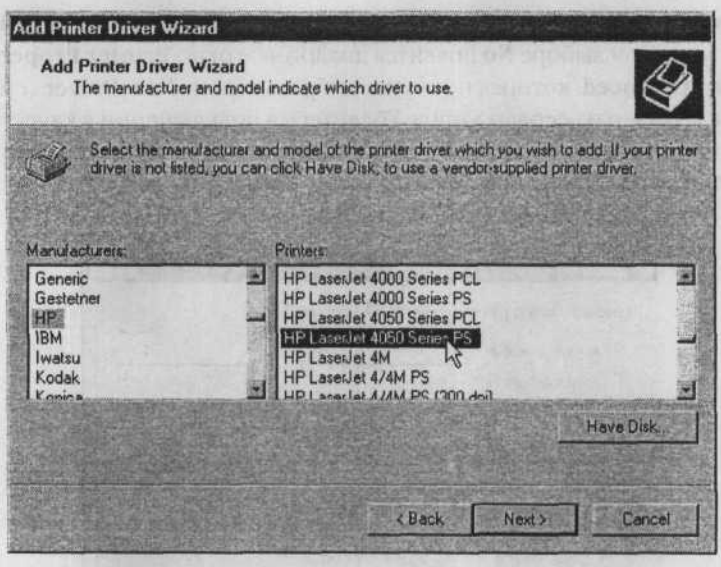

Рис. 6.12. Выбор драйвера принтера

Для настройки Режима устройств (Device Mode) откройте окно Printing Preferences, измените расположение на **Landscape** (Горизонтально) и нажмите кнопку **Apply** (Применить), потом верните расположение на **Portrait** (Вертикально) и еще раз нажмите кнопку **Apply**. В это время можно задать прочие настройки по умолчанию. Нажмите сначала на кнопку **Advanced**, после чего на **Printing Defaults**, как показано на рис. 6.13.

Для принтера PostScript может понадобиться настройка опции PostScript Output Option на Optimize for Portability, вместо настройки по умолчанию Optimize for Speed, поскольку при этом выходные данные будут более надежными. На рис. 6.14 показана эта настройка.

Теперь распечатайте тестовую страницу системы Windows и убедитесь в корректном выполнении процесса печати. Если страница не распечатается, то необходимо проверить, в какой части системы «клиент Windows — Samba — CUPS» возникла ошибка. Проверьте журналы регистрации ошибок Samba и CUPS на предмет наличия очевидных сообщений. Ключом к решению проблемы является проверка того, как работает каждое звено цепи.

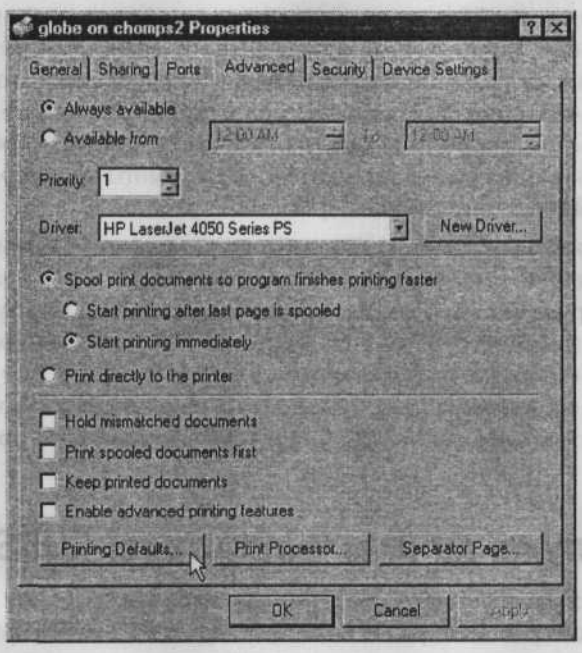

Рис. 6.13. Выбор настроек принтера по умолчанию

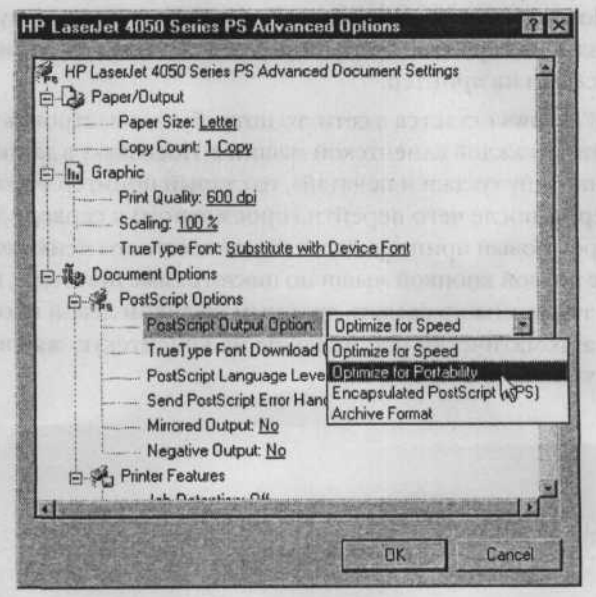

Рис. 6.14. Оптимизация портативности

Может возникнуть необходимость остановки принтера для того, чтобы проверить файл, отправленный Windows. При использовании CUPS нажмите на кнопку «Stop Printer» на странице настроек принтера CUPS (рис. 6.7) либо воспользуйтесь командой «disable». При этом задание будет скачано, но не будет распечатано. Попробуйте напечатать еще одну тестовую страницу из клиента Windows и проверьте загрузку файла нажатием кнопки «Jobs» в верхней части страницы принтера CUPS (рис. 6.7), либо запустите выполнение команды «lpstat -t».

Если задание не отображается, то проблема связана либо с клиентом Windows, с которого это задание отправляется, либо с Samba, передающей задание в системный спулер. Для обнаружения проблемы необходимо внимательно изучить системные журналы Samba (возможно, повысить уровень регистрирования). Если задание по-прежнему не отображается, просмотрите файл в каталоге /var/spool/cups (или в другом каталоге системного спулера) на предмет формата этого файла. Попытайтесь распечатать его с помощью команды lp. Если это не помогает, проверьте драйвер принтера.

Перенос служб печати Windows на CUPS/Samba

Теперь, когда принтер работает со стороны клиентов как Linux, так и Windows, можно начать процесс переноса служб печати с сервера Windows на сервер Linux. Так как Samba может объявить несколько имен *NetBIOS* через параметр **netbios aliases** в файле **smb.conf**, на одном сервере Samba можно консолидировать несколько серверов печати Windows. Если сервер Windows будет выведен из эксплуатации, то псевдоним можно задать на сервере Samba, и клиентам не нужно будет изменять используемое имя для ссылки на принтер.

Если сервер Windows остается в сети, то потребуется настроить (изменить) подключение к принтеру каждой клиентской машины. Поскольку в данном случае существует настройка по типу «укажи и печатай», то старый принтер можно легко удалить из папки принтеров, после чего перейти (просмотром) к серверу Samba и выбрать из папки принтеров новый принтер. Далее из контекстного меню, которое появится, если вы щелкнете правой кнопкой мыши по пиктограмме принтера, выберите команду **Connect** (это также можно сделать двойным щелчком левой кнопки), после чего драйверы будут автоматически установлены на клиентскую машину с заданными настройками по умолчанию.

Резюме

CUPS и Samba упрощают настройку принтеров на сервере Linux для их использования клиентами как Linux, так и Windows. CUPS упрощает добавление новых принтеров и администрирование сервера печати. Для принтеров PostScript можно использовать даже файлы PPD с драйверами Windows для того, чтобы функции, поддерживаемые Windows, были доступны для сервера CUPS.

Samba можно настроить для предоставления этих принтеров клиентам Windows, а также для автоматического скачивания нужных драйверов на клиентские машины. Для клиентов Windows эти принтеры выглядят и «ведут себя» так же, как принтеры, подключенные к серверу печати Windows. С помощью функции псевдонимов NetBIOS Samba можно сделать так, что один сервер Linux будет выдавать себя за несколько серверов Windows, что позволит создать столько серверов печати, сколько необходимо организации.

Краткое резюме по разделам

Понятие служб печати Windows

- ☑ Windows использует GDI в качестве обычного API для отображения данных и их печати.
- ☑ Драйверы принтера преобразуют выходные данные EMF через GDI в формат, распознаваемый принтером.
- ☑ Для описания возможностей принтеров PostScript используется файл PPD.
- ☑ Клиент Windows может автоматически скачать с сервера нужный драйвер принтера.

Понятие служб печати Linux

- ☑ Системы UNIX никогда не разрабатывали общего API для отображения и печати, как это делалось в Windows.
- ☑ Фильтры или интерфейсные сценарии выполняют функции драйвера печати Windows.
- ☑ Исторически, двумя основными подсистемами печати, используемыми на UNIX, является BSD и SYSV. В каждой системе для управления печатью используется собственный набор команд.
- ☑ Более новая система под названием CUPS — Общая система печати UNIX — обеспечивает управление множественными типами очереди на печать с помощью интерфейса веб-браузера.

Совместное использование печатающих устройств через Samba

- ☑ Необходимо настроить параметры файла **smb.conf** для используемой системы печати (BSD, SYSV или CUPS).
- ☑ Создайте разделы для отдельных принтеров или воспользуйтесь специальным разделом **Printers** в файле **smb.conf** для возможности распознавания принтеров клиентами Windows.
- ☑ Создайте каталог спулинга с необходимыми правами, чтобы пользователь, указанный Samba, мог создавать в нем файлы.

Понятие автоматической загрузки драйвера печатающего устройства

- ☑ Создайте в файле **smb.conf** запись для совместно используемого ресурса print$ и убедитесь в том, что она может записываться администраторами служб печати.
- ☑ Создайте нужный каталог и подкаталоги для поддерживаемых архитектур драйверов.
- ☑ Используйте Мастер добавления принтеров (Ad Printer Wizard) клиента Windows для загрузки драйверов на сервер и связывания с нужным принтером.
- ☑ Задайте для клиента Windows режимы устройств и печати по умолчанию.

Перенос служб печати Windows на CUPS/Samba

- ☑ Используйте псевдонимы NetBIOS для того, чтобы сервер Samba присвоил имя сервера Windows, который планируется к выведению из эксплуатации.
- ☑ Если старый сервер Windows останется в сети, но не будет являться сервером печати, то у клиентов можно удалить определения старого принтера. После этого используйте принцип «указал-распечатал» для подключения к местоположению нового принтера на сервере Samba.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма «Ask the Author»). Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: Как можно управлять сервером CUPS с другой системы с помощью браузера?

О: Встречаются два аспекта, которые могут сделать удаленное управление (администрирование) невозможным. В некоторых установках CUPS в файле **cupsd.conf** имеется директива **Listen**, которая обеспечивает подключения только с локального хоста. При получении с браузера сообщения «*Connection Refused*» (отказ в подключении) в эту строку потребуется внести изменения для считывания **Listen*:631** (либо удалить строку и убедиться в наличии строки **Port 631**). Получение сообщения «*Forbidden*» (запрещено) означает, что не было предоставлено право доступа. При этом потребуется модифицировать соответствующий раздел и внести изменения в директивы **Deny From** или **Allow From**. В Руководстве администратора программных средств CUPS этот процесс описан более подробно.

В: Почему мой принтер иногда печатает с остановками, за которыми следует нечто похожее на команды PostScript?

О: Скорее всего драйвер Windows вставляет какие-то команды PCL (язык управления печатью) в начало файла. При этом CUPS автоматически определяет тип файла и не распознает его как файл PostScript. Воспользуйтесь драйвером CUPS или Adobe PostScript клиента Windows.

В: Почему мой каталог спулинга Samba не может быть тем же, что и каталог спулинга CUPS?

О: Настройка в cupsd.conf для RequestRoot (каталог, в который скачиваются файлы) и запись в smb.conf для path= в разделе принтеров должны различаться. При перезагрузке системы cupsd будет изменять разрешения в каталоге спулинга. После этого разрешения будут такими, что Samba не сможет осуществлять запись в этот каталог.

В: Почему cupsaddsmb получает сообщения об ошибках на только что созданном принтере?

О: Может случиться так, что принтер еще не экспортирован Samba. Можно заставить Samba еще раз считать файл smb.conf отправкой сигнала HUP всем процессам smbd. Убедитесь, что Samba корректно настроена на совместное использование всех принтеров (load printers = yes), а также в корректной настройке совместно используемого ресурса print$.

Глава 7

Службы передачи сообщений

Разделы:

- Понятие служб передачи сообщений Microsoft
- Понятие служб передачи сообщений на базе Linux
- Проектирование служб передачи сообщений на базе Linux
- Интегрирование служб защиты от спама и вирусов
- Перенос информации из Exchange в Linux

☑ Резюме

☑ Краткое резюме по разделам

☑ Часто задаваемые вопросы

Введение

Службы передачи сообщений обеспечивают взаимодействие между персоналом компании и внешним миром. Для большинства предприятий наличие электронной почты — не роскошь, а необходимость. Отключение электронной почты на один рабочий день может грозить банкротством, пропущенной или полученной с опозданием информацией, снижением производительности, финансовыми потерями и разочарованиями как сотрудников компании, так и клиентов. Чем больше времени уделяется изучению и планированию работы служб передачи информации на базе Linux, тем меньше его будет тратиться на решение всевозможных проблем и объяснение причин простоев как начальству, так и коллегам.

Корпоративные службы передачи сообщений предлагают конечным пользователям множество разнообразных функций. В дополнение к банку сообщений IMAP (протокол интерактивного доступа к электронной почте), который «следует» за пользователем к любому настольному компьютеру (или ноутбуку) компании, каталог, обеспечивающий поиск электронных адресов (его настройка описана в предыдущих главах), а также фильтрация от спама и вирусов образуют ключевые подслужбы для обеспечения передачи корпоративной информации. Большинство из них также обеспечивают некий тип почтового web-клиента, а во многих присутствуют функции коллективного использования, такие как календари и совместно используемые папки. В настоящей главе представлен общий обзор упомянутых служб, описаны открытые решения и приведены руководства по проектированию и переносу служб передачи сообщений на базе Linux.

Основной упор в данной главе сделан на перенос информации из пакета Exchange (либо из любой другой системы передачи сообщений с интерфейсом IMAP/POP) на систему MTA-MDA-MAA-MUA на базе Linux. Несмотря на то, что большинство принципов применимы к системам, не имеющим отношения к системе Exchange, последняя будет использоваться в примерах, и сценарии будут тестироваться для работы на серверах Exchange. Несмотря на то, что ожидается абсолютно корректное выполнение сценариев с любым почтовым хранилищем, совместимым с IMAP, перед каждой компанией стоят свои задачи.

В первом разделе в общем виде рассматривается типичная система передачи сообщений Exchange. Эти же концепции применяются к другим системам передачи информации, однако в тексте упор делается на Exchange. Здесь рассматриваются основные функции и компоненты системы Exchange 5.5, а также обновления и новые функции, имеющиеся в Exchange 2000. Авторы также обсуждают различия в реализации каталогов в Exchange 5.5 и Exchange 2000.

Раздел «Понятие служб передачи сообщений на базе Linux» посвящен компонентам обычной системы передачи сообщений, а также взаимодействиям между различными компонентами. Помимо теоретических исследований системы передачи сообщений и ключевых концепций, будут рассматриваться агенты передачи почтовых сообщений

(MTA) Courier-MTA, postfix, exim и send-mail, а также агенты доступа к почте (MAA), включая Courier, Cyrus и серверы UW IMAP/POP. После этого рассматриваются варианты проектирования служб передачи информации в организации на базе Linux. Изучаются критерии проектирования, а также исследуются способы обмена сообщениями в компаниях Acme Widgets и Ballystyx Engineering.

После ознакомления с разделом о проектировании читатели научатся добавлять службы защиты от спама и вирусов. Рассматриваются решения этих проблем, включая выделенные шлюзы, серверы совместного использования, промышленные установки и возможность привлечения внешних ресурсов.

Наконец, подробно рассматривается собственно процесс переноса. Авторы дают рекомендации по подготовке Exchange к переносу информации, после чего переходят к использованию сценариев для переноса электронной почты с системы Exchange на почтовый сервер на базе Linux. Если следовать всем инструкциям настоящей главы, то в результате пользователи получат систему передачи сообщений на базе Linux с теми же функциями, что и в Exchange, но без затрат на лицензии или других недостатков патентованных программных средств.

Понятие служб передачи сообщений Microsoft

В 1996 году корпорация Microsoft представила на рынке корпоративных коллективно используемых систем и систем передачи информации пакет Exchange 4.0, который вытеснил MS-Mail, наиболее предпочитаемую крупными компаниями. MS-Mail была сложна в администрировании и подвержена частым сбоям. Выпуском Exchange Microsoft предложила корпорациям полнофункциональную многоабонентскую LDAP (облегченный протокол службы каталогов) службу, совмещенную со службой почтового хранилища базы данных уровня предприятия, унаследованной от JET. Серверы MS-Mail поддерживали от 100 пользователей, а серверы Exchange могли поддерживать тысячи пользователей с соответствующими аппаратными средствами.

Exchange является прямым конкурентом пакетов Novell Groupwise, Lotus Notes, Oracle Messaging и других патентованных средств передачи сообщений. На сегодняшний день Exchange и Notes доминируют на высокотехнологичном рынке средств передачи информации и коллективного использования среди первой сотни самых успешных компаний с изобилием открытых средств и патентованных решений, обслуживающих нишу мелких и средних предприятий.

Exchange предлагает пользовательские почтовые ящики, группы электронной почты, совместно используемые папки, интерфейсы IMAP и POP, составные контакты, пользовательские и групповые календари, гибкие механизмы хранения баз данных и практически любые функции, требуемые для передачи корпоративной информации, и системы коллективного пользования. Несмотря на то, что Exchange — это проверенная, полнофункциональная система передачи информации, ее недостатком явля-

ется слишком затратная интеграция в нее программ защиты от спама и вирусов. Ни одно открытое решение не может сравниться по функциональности с интегрированным пакетом Exchange 2000/Active Directory, но большая часть функций и возможностей Exchange доступны комбинации открытых программных средств передачи информации и сообщений.

Принципы передачи информации в Exchange 5.5

Сервер Microsoft Exchange 5.5 фактически представляет собой набор интегрированных служб. В табл. 7.1 перечислены компонентные службы Exchange 5.5 с кратким описанием.

Табл. 7.1. Компонентные службы Exchange 5.5

Служба	Функция
Администратор системы	Мониторинг всех прочих служб
Служба каталогов	Обеспечение служб каталогов Exchange
Хранилище информации	Управление базой данных, в которой сохранено содержимое папок коллективного использования и почтовые ящики пользователей
Агент передачи сообщений	Передача сообщений между серверами Exchange
Служба почты Интернет	Передача сообщений между хостами с помощью SMTP (простой протокол электронной почты)

Серверы Exchange 5.5 объединены в узлы. Серверы в рамках каждого узла взаимодействуют через всегда доступное подключение с высокой пропускной способностью, например серверы, объединенные в LAN (локальная сеть) и, возможно, в подсети WAN (глобальные сети). На языке Windows 2000 эти узлы являются наборами подсетей IP. В рамках Exchange каждый узел должен иметь уникальное имя и совместно использовать одно имя организации.

Соединительные блоки Exchange 5.5 (connectors) соединяют узлы Exchange с другими узлами либо с системами передачи третьих сторон — SMTP, Notes, MS-Mail, Fax или X.400. Эти соединители позволяют Exchange разделять службы по особым дополнительным адресным типам и переносить обработку этих типов на программные средства соединительного блока.

Один из самых распространенных соединительных блоков — Служба почты Интернет (включаемая в стандартную и корпоративную версии сервера Exchange) — предлагает значительное количество опций конфигурирования связей SMTP в обоих направлениях (прием входящих соединений из Интернета и установка исходящих соединений с серверами Интернет). На рис. 7.1 показана конфигурация Службы почты Интернет компании Acme Widget.

Рис. 7.1. *Конфигурация Службы почты Интернет компании Acme Widget*

При объединении двух узлов Exchange 5.5 с помощью другого узла или другого соединительного блока передачи информации, эти узлы могут обмениваться информацией репликации каталога. В рамках узла информация каталога дублируется через RPC (удаленный вызов процедуры). Между узлами информация каталога дублируется через электронные сообщения, передаваемые соединительными блоками дублирования каталога.

Exchange поддерживает определенное количество протоколов доступа к информации электронной почты и коллективного пользования. В табл. 7.2 перечислены эти протоколы и описано их использование.

Exchange 5.5 поддерживает *активно-пассивную* кластеризацию или то, что называется *отказоустойчивой* кластеризацией. Для того, чтобы воспользоваться преимуществами кластерных серверов Exchange 5.5, необходимо использовать форму сохранения с возможностью кластеризации, например SAN (архитектура «сервер-хранилище данных») или совместно используемую шину SCSI. Один из серверов Exchange должен быть обозначен как *пассивный* узел, который просто дожидается отказа другого сервера. *Активно-активная* кластеризация (или кластеризация *выравнивания нагрузки*), когда оба сервера работают в активном режиме, поддерживается в Exchange 2000, но не поддерживается в Exchange 5.5.

Табл. 7.2. Поддержка протоколов Exchange 5.5

Протокол	Описание
MAPI	Outlook использует Программный интерфейс приложения (API) передачи сообщений и предоставляет почтовый ящик и функции коллективного пользования
IMAP	IMAP — полнофункциональный межплатформенный протокол доступа к почтовому ящику
POP	POP — межплатформенный протокол доступа к почтовому ящику с ограниченными возможностями
HTTP	Протокол передачи гипертекстовых файлов (HTTP) обеспечивает доступ web-браузеров к сообщениям и календарю/средствам коллективного использования через OWA (Outlook Web Access)
LDAP	Обеспечивает межплатформенный доступ к информации каталога Exchange

Принципы передачи информации в Exchange 2000

Exchange 2000 предлагает те же основные функции, что и Exchange 5.5, только большинство из них усовершенствованы или обновлены. В Exchange не используется собственная служба каталогов, но здесь требуется Active Directory. Вся информация, которая сохранялась в каталоге Exchange 5.5, в Exchange 2000 сохраняется в Active Directory. При установке Exchange 2000 пакет просто обновляет схему Active Directory на каталогах объектов с активизированной электронной почтой и совместно используемых ресурсов и предоставляет интерфейсы для конфигурирования хранилища почты и передачи сообщений.

Хранилище почты в Exchange 2000 использует расширяемую архитектуру, где каждый сервер управляет группой (группами) сохранения вместо хранилища общественной папки/личного почтового ящика на каждом сервере, в случае с Exchange 5.5. При этом обеспечивается большая гибкость в том, что касается сохранения, резервирования, восстановления и кластеризации. Хранилище почтового ящика можно легко разбить по многочисленным базам данных меньшего размера, которые можно хранить на разных запоминающих устройствах, использовать разные схемы резервирования и восстанавливать быстрее, чем одну обширную базу данных.

Компонент OWA также значительно усовершенствован и дополнен функциями в большей степени, чем Outlook Web Access в Exchange 5.5, особенно если в качестве web-браузера используется Internet Explorer. В число дополнительных функций OWA 2000 входит поддержка drag-and-drop, построение сообщений по принципу WYSIWYG (что видно на экране, то и будет получено), а также расширенное отображение встроенных объектов.

В Exchange 5.5 схемой внутренней адресации прежде всего является соглашение X.400, когда все пользовательские почтовые ящики имеют адрес X.400. В Exchange 2000 основным механизмом адресации является SMTP, используемый как первичный механизм коммуникации.

Active Directory управляет дублированием (репликацией), доверительными отношениями, соединениями узлов и другими функциями, которые раньше управлялись службами каталогов Exchange 5.5. В Exchange 2000 узлы являются частью каталога Active Directory, где репликация управляется доменными контроллерами Windows 2000.

Понятие служб передачи сообщений на базе Linux

Большинство открытых систем передачи сообщений представляют собой интегрированную модульную систему, состоящую, в свою очередь, из многокомпонентных приложений. Эти компоненты передачи сообщений отвечают за передачу, прием, доставку электронных сообщений и обеспечение доступа к ним. В небольших компаниях эти компоненты, как правило, являются частью одного пакета передачи сообщений, например Courier-MTA. В крупных компаниях множественные компоненты часто «склеиваются» (объединяются) для формирования решения о передаче информации, настроенного под конкретные цели той или иной организации.

В данном разделе будет рассмотрен жизненный цикл электронной почты Интернет с последующим изучением отдельных компонентов систем передачи информации, обеспечивающих этот процесс. Авторы также перечисляют открытые серверные приложения, образующие основу служб передачи информации на базе Linux, и представляют краткий обзор каждого из этих приложений.

Отправка и получение электронной почты по Интернет

Для лучшего понимания принципов работы систем передачи информации рассмотрим отправку и получение электронной почты по Интернет. Другими словами, проследим жизненный цикл электронного сообщения в Интернет от момента, когда пользователь нажимает кнопку **Send** (Отправить), до момента поступления сообщения в раздел «Входящие» получателя.

Процесс отправки электронного сообщения по Интернет начинается с того, что MUA (пользовательский почтовый агент) передает электронное сообщение в MTA (почтовый агент). В примере, показанном на рис. 7.2, Джим Астер из компании Acme Widgets составил электронное сообщение с помощью программы Evolution и отправляет его Киму Чангу из компании Ballystyx Engineering. На этой иллюстрации компания Acme Widgets уже прошла процесс перехода и использует MTA и MUA на базе Linux. Ballystyx Engineering переход еще предстоит, поэтому в этой компании еще используется система Exchange/Outlook.

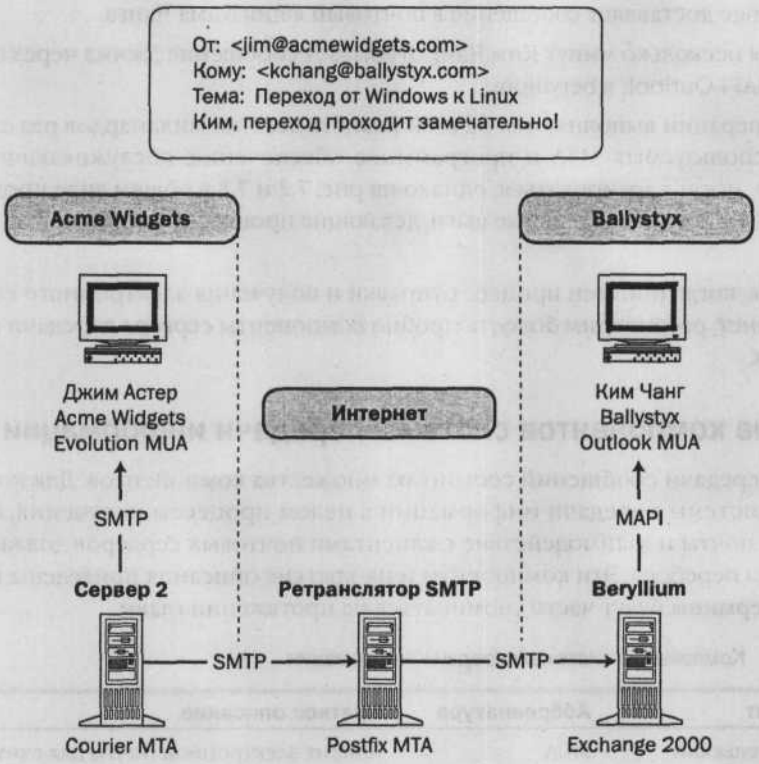

Рис. 7.2. Отправка и получение электронного сообщения по Интернет

Вышеуказанную процедуру можно разделить на семь основных шагов:

1. Джим Астер составляет сообщение и нажимает кнопку «Отправить».
2. Evolution пересылает сообщение на SERVER2.
3. Courier получает сообщение через SMTP.
4. Courier определяет, что сообщение предназначено для получателя с нелокальным SMTP, и отправляет сообщение на SMTP-Relay.acmeISP.net.
5. Машина-«ретранслятор» (relay) SMTP ISP компании Acme получает сообщение и ставит его в очередь на исходящую отправку.
   - MTA выбирает сообщение Джима из очереди на исходящую отправку.
   - MTA выполняет поиск DNS (служба имен доменов) на предмет записи MX (Mail Exchanger) в домене ballystyx.com и обнаруживает, что она соответствует beryllium.ballystyx.com.
   - MTA подключается к beryllium.ballystyx.com и через SMTP передает сообщение Джима на Exchange 2000.

6. Exchange доставляет сообщение в почтовый ящик Кима Чанга.
7. Спустя несколько минут Ким Чанг открывает сообщение Джима через подключение MAPI Outlook к beryllium.

Эти операции выполняются на всей планете десятки миллиардов раз ежедневно. Число используемых MTA и программное обеспечение, обслуживающее каждую функцию, могут варьироваться, однако на рис. 7.2 и 7.3 в общем виде представлены компоненты, связи и отдельные шаги, делающие процесс возможным от начала и до конца.

Теперь, когда понятен процесс отправки и получения электронного сообщения по Интернет, рассмотрим более подробно компоненты сервера передачи информации Linux.

Понятие компонентов системы передачи информации Linux

Сервер передачи сообщений состоит из множества компонентов. Для корректной работы системы передачи информации в целом процессы получения, отправки, доставки почты и взаимодействие с клиентами почтовых серверов должны выполняться без перебоев. Эти компоненты и их краткие описания приведены в табл. 7.3. Все эти термины будут часто упоминаться на протяжении главы.

Табл. 7.3. Компоненты системы передачи информации

Компонент	Аббревиатура	Краткое описание
Пользовательский почтовый посредник	MUA	Клиент электронной почты для считывания, отправки и удаления сообщений
Почтовый агент	MTA	Служба передачи сообщений от хоста к хосту
Агент доставки почты	MDA	Отправка сообщений в локальное хранилище почтовых сообщений
Агент доступа к почте	MAA	Ответ на запросы MUA для просмотра сообщений
Хранилище почтовых сообщений		Механизм сохранения сообщений и почтовых ящиков

На рис. 7.3 показана схема современного почтового сервера на базе Linux, MTA, MAA, MDA и входящие в него компоненты хранилища почтовых сообщений, также представлены действия MUA и другие (возможные) MTA.

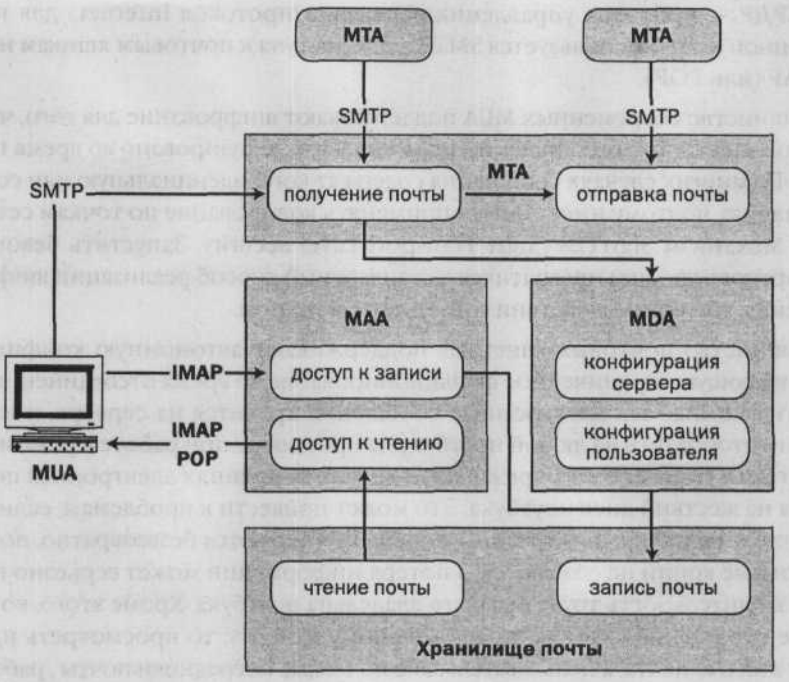

Рис. 7.3. Компоненты почтового сервера

В следующих разделах каждый из этих компонентов и протоколов будет рассмотрен более подробно.

Почтовый посредник пользователя (MUA)

Пользовательский почтовый посредник — это клиентский раздел системы передачи информации, который осуществляет взаимодействие с конечными пользователями. Во многих случаях он называется просто *почтовым клиентом* или *клиентом электронной почты*. По большей части эти термины взаимозаменяемы и широко используются при обращении к таким программным приложениям, как Evolution, Mozilla, Thunderbird, KMail, Outlook или Pine. Другим типом является почтовый клиент на базе web, обычно устанавливаемый как приложение cgi для Apache. Двумя популярными открытыми приложениями для работы с почтой через web являются SquirrelMail и SqWebMail (описываются далее). В двух словах можно сказать, что MUA отображает содержимое сообщений в почтовом ящике пользователя.

Для отправки сообщений MUA связывается с MTA, а для доступа к почтовому ящику — с MAA. В Linux (и практически во всех системах передачи сообщений по прото-

колу TCP/IP — протокол управления передачей/протокол Internet) для передачи электронной почты используется SMTP, а для доступа к почтовым ящикам используется IMAP (или POP).

Большинство современных MUA поддерживают шифрование для того, чтобы содержимое электронных сообщений не могло быть декодировано во время передачи по сети. Во многих случаях сообщения содержат конфиденциальную или секретную информацию, поэтому имеет смысл применять кодирование по точкам сетевой передачи. Механизм StartTLS (Start Transport Level Security, Запустить безопасность транспортного уровня) превратился в стандартный способ реализации шифрования соединения при взаимодействии с почтовым сервером.

Большинство почтовых клиентов поддерживают автономную конфигурацию, обеспечивающую ограниченное функционирование во время отсоединения от сети. Во многих компаниях электронные сообщения хранятся на сервере, и их можно зеркально отобразить на любой ноутбук для просмотра при работе в режиме отключения от сети (в автономном режиме). В других компаниях электронная почта скачивается на жесткий диск ноутбука. Это может привести к проблемам, если ноутбук утерян или поврежден. Электронные сообщения теряются безвозвратно, потому что их резервные копии не создаются, а потеря информации может серьезно повлиять на производительность труда бывшего владельца ноутбука. Кроме этого, когда электронные сообщения скачиваются локальному клиенту, то просмотреть их можно только с этого клиента, а пользовательские почтовые посредники почты , работающие через web, будут отображать пустой почтовый ящик.

Большинство MUA поддерживают адресные поиски через сервер каталогов (например, OpenLDAP). При этом значительно упрощается поиск персоналий, адресов электронной почты и контактной информации, особенно для сотрудников крупных компаний с большим количеством филиалов. Поскольку включенные в книгу сценарии перехода заполнили каталог OpenLDAP адресами электронной почты (см. главу 4), данная функция адресного поиска становится доступной для пользователей при их переходе к службам передачи информации на базе Linux.

Для Linux существует множество разнообразных открытых MUA; в табл. 7.4 представлены самые популярные почтовые посредники и их web-сайты.

Табл. 7.4. Популярные почтовые посредники Linux с web-сайтами

MUA	Web-сайт
Evolution	www.novell.com/products/evolution
Mozilla	www.mozilla.org/products/mozilla1.x/
Thunderbird	www.mozilla.org/products/thunderbird/
Kmail	kmail.kde.org/
Balsa	www.newton.cx/balsa/
Pine	www.cac.washington.edu/pine/

Более подробная информация о почтовых посредниках Linux представлена в главе 11 «Внутренняя структура настольной рабочей станции Linux». Полный список почтовых посредников Linux имеется на сайте www.linuxmafia.com/faq/Mail/muas.html.

Агент доступа к почте (MAA)

Почтовый посредник (MUA) должен иметь доступ к содержимому хранилища почтовых сообщений. Он осуществляется через MAA. Доступ может быть организован либо через совместное использование файла, либо через протокол — IMAP или POP. MUA указывает MAA операцию: получение, удаление, вставку и/или перемещение электронных сообщений, а MAA управляет операциями считывания и записи в хранилище сообщений.

Courier-IMAP, UW-IMAP и Cyrus-IMAP — три популярных открытых агента доступа к почте. Вообще, Courier-IMAP — рекомендуемый IMAP MAA, независимо от того, используются ли другие приложения в наборе Courier. UW-IMAP имеет дурную славу небезопасного продукта и не работает с почтовыми каталогами, а Cyrus-IMAP использует необычную методологию хранилища почтовых сообщений. Все эти MAA обслуживают клиентов с помощью IMAP и/или POP. В следующих разделах рассматриваются преимущества и характеристики IMAP и POP.

Понятие POP (почтовый протокол)

Почтовый протокол является предшественником IMAP и наиболее широко используемым сетевым протоколом для доступа к почтовым ящикам пользователей. В данной книге подразумевается версия 3 почтового протокола (POP3), определенная в RFC 1939. В большинстве окружений POP используется для скачивания электронной почты с сервера в локальное место сохранения, а также для удаления электронных сообщений с сервера после их успешного скачивания компьютером пользователя.

POP не обеспечивает поддержки серверных папок и ничего более сложного, чем получение и удаление электронных сообщений. Во многих случаях этих возможностей вполне достаточно для упрощенных служб передачи информации.

Понятие IMAP (протокол интерактивного доступа к электронной почте)

IMAP обеспечивает доступ к почтовому ящику на удаленном сервере. В данной книге подразумевается IMAP версии 4, описанный в RFC 3501. В то время, как POP обеспечивает только скачивание и удаление электронных сообщений, IMAP обеспечивает полное управление удаленными почтовыми ящиками и считается основным протоколом для доступа уровня предприятия к пользовательским почтовым ящикам. Он оптимален для сохранения электронных сообщений на сервере, организации иерархической структуры папок, для доступа с множества компьютеров, множества мест и для полного использования функций в автономном режиме.

Несмотря на то, что IMAP обладает бо́льшими возможностями, нежели POP, он более сложен для развертывания. Важно помнить, что POP и IMAP обслуживают несколько различные типы требований. Во многих случаях проще оперативно развернуть сервер POP и сконфигурировать клиенты на использование POP для скачивания электронных сообщений на локальный жесткий диск. На самом деле, некоторые устаревшие программные приложения не поддерживают IMAP.

Однако для полнофункционального доступа к почтовым ящикам, поддержки совместно используемых папок и работы в автономном режиме дополнительные усилия по развертыванию IMAP себя оправдывают, повышая ценность службы передачи информации. Сохранение данных хранилища электронных сообщений на почтовом сервере активизирует web-почту и упрощает процедуры создания резервных копий сообщений и их восстановления. Информация по установке и конфигурированию Courier-IMAP имеется на сайте www.courier-mta.org/imap/INSTALL.html.

Почтовый агент (MTA)

Почтовый агент прежде всего отвечает за передачу сообщений с одного хоста на другой, другими словами, за отправку и прием электронных сообщений в сети. В Интернет и практически в любой другой сети TCP/IP для этого существует протокол SMTP. SMTP и информация о форматировании электронной почты в Интернет описаны в RFC 821, 2821, 2822 и 2487.

Для отправки электронного сообщения с помощью SMTP хост инициирует передачу путем подключения к другому хосту через порт TCP 25. Если запущен сервер SMTP, то клиент и сервер вступают в диалог. Типичный диалог «MUA – MTA» в компании Acme Widgets между системой Evolution, работающей на WIDGET1, и системой Courier-MTA, работающей на SERVER2, показан на рис. 7.4. Текст, отправляемый клиентом (WIDGET1), изображен полужирным шрифтом.

Как видно в диалоге, команда StartTLS инициирует шифрование. Пакет Evolution был «осведомлен» о поддержке кодирования, потому что SERVER2 объявил эту возможность ответом:

```
250-STARTTLS
```

Большинство современных почтовых клиентов поддерживает шифрование. Однако активизация шифрования может быть как очень простой операцией (достаточно просто отметить опцию одним щелчком мыши), так и довольно трудоемкой (необходимо связаться с Бюро сертификации (CA). Для MUA кодирование обычно активизируется выбором опции **Use SSL/TLS**. Для MTA кодирование обычно требует установки сертификата сервера и переконфигурирования различных серверов для фактического использования сертификата и активизации функции кодирования. Управление сертификатами OpenSSL описано в главе 9.

```
SERVER2:    220 server2.acmewidgets.com ESMTP
WIDGET1:    EHLO widget1
SERVER2:    250-server2.acmewidgets.com Ok.
SERVER2:    250-STARTTLS
SERVER2:    250-PIPELINING
SERVER2:    250-8BITMIME
SERVER2:    250-SIZE
SERVER2:    250 DSN
WIDGET1:    STARTTLS
SERVER2:    220 Ok
      (Остальная часть диалога шифруется)
WIDGET1:    MAIL FROM: <sender@acmewidgets.com>
SERVER2:    250 Ok
WIDGET1:    RCPT TO: <recipient@ballystyx.com>
SERVER2:    250 Ok
WIDGET1:    DATA
SERVER2:    354 Ok
WIDGET1:    (содержимое почтового сообщения)
SERVER2:    250 Ok
WIDGET1:    QUIT
SERVER2:    250 Ok
```

Рис. 7.4. Диалог SMTP

Электронное сообщение имеет только одного отправителя, но может иметь несколько получателей. Если электронное сообщение адресовано нескольким получателем в одном и том же домене, то большинство МТА будут передавать только одно сообщение в домен. Например, если jim@somedomain.com отправил сообщение на адреса john@example.com и mary@example.com, то МТА на somedomain.com потребуется отправить только одну копию сообщения на систему обмена сообщениями для example.com, а принимающий МТА на example.com доставит копию сообщения на почтовые ящики Джона и Мэри.

Прикрепляемая к электронному сообщению информация управляется через MIME (многоцелевые расширения электронной почты в сети Internet). MIME разделяет электронное сообщение на несколько разделов. Каждый раздел может иметь разный тип формата содержимого. Более подробная информация о MIME имеется на сайте http://en.wikipedia.org/wiki/MIME и в RFC 2045, 2046, 2047, 2048 и 2049.

МТА работают с помощью множественных очередей для временного хранения сообщений. Все современные МТА, как минимум, используют исходящую, входящую и рабочую очереди. Большинство МТА также используют комбинацию очередей запаздывания, карантина, «мусора» и/или регистрации для расположения электронной почты по категориям для последующей обработки. Когда МТА получает электронное

сообщение, адресованное пользователю на локальном сервере, MTA передает сообщение Агенту доставки почты (MDA) для копирования в хранилище почтовых сообщений.

Агент доставки почты (MDA)

Агент доставки почты отвечает за передачу сообщений в хранилище. Иногда MDA называется агентом локальной доставки (LDA). В данной книге ссылки делаются на агент, доставляющий сообщение в хранилище, как MDA. Большинство MTA имеют свои собственные MDA, но при желании их можно легко сконфигурировать на использование другого MDA.

Многие MDA имеют основанный на правилах механизм фильтрации, который можно использовать в целой организации и/или по каждому почтовому ящику. Настройки конфигурации организации обычно хранятся в каталоге /etc/, тогда как настройки индивидуальных пользователей (например, перемещение определенных входящих сообщений в определенную папку) обычно хранятся в домашнем каталоге пользователя или в каталоге спулинга почты.

Procmail и maildrop — два популярных агента доставки почты. Оба обеспечивают фильтрацию электронной почты, несмотря на то, что язык для *рецептов* procmail считается замысловатым. Maildrop — MDA, используемый Courier-MTA, имеет более простой синтаксис, сходный с языками сценариев.

Fetchmail — это MDA с функциями, подобными MTA. Fetchmail получает электронное сообщение из почтовых ящиков POP или IMAP и переадресует его на MTA SMTP. Fetchmail имеет графический инструмент конфигурации — fetchmailconf, упрощающий использование многих возможностей конфигурации fetchmail. Fetchmail может управлять электронной почтой целого домена через один почтовый ящик, хотя это не обязательно самый лучший способ применения fetchmail. Более подробная информация о fetchmail имеется на сайте www.catb.org/~esr/fetchmail/, либо ее можно получить вводом строки **man fetchmail**.

Хранилище электронных сообщений

В дополнение к отправке, приему и доставке электронной почты следует рассмотреть важный аспект сохранения электронных сообщений на почтовом сервере Linux. На большинстве серверов Linux эта задача решается использованием сохранения на базе файлов, хотя в некоторых продуктах для сохранения электронной почты может применяться база данных. В то время как Exchange использует базу данных, унаследованную от JET, открытые приложения Linux для сохранения электронных сообщений используют два разных формата: maildir и mbox.

Формат сохранения сообщений Mbox/Mbx

Методология mbox — это исторический способ сохранения почтовых сообщений на почтовых серверах. Отдельные сообщения просто «склеиваются» в один файл с размещением маркера между сообщениями. В mbx эта строка содержит метаданные для повышения производительности индексирования. Такая упрощенная методология подходит для умеренного количества отдельных электронных сообщений на рабочей станции одного пользователя и может использоваться в качестве локального механизма сохранения несколькими почтовыми клиентами.

Будучи идеальными для клиентских сообщений, mbox и mbx не очень предпочтительны для устойчивого сохранения электронных сообщений, когда множественные процессы требуют параллельного доступа к чтению/записи в хранилище. Поскольку только один процесс может осуществлять запись в файл mbox, эта методология не очень хорошо масштабируется из-за проблем блокировки. Подобная потенциальная проблема становится особенно очевидной, когда данные почтового ящика размещаются в совместно используемых сетевых файлах (что может надлежащим образом активизировать правила блокировки, а может и не активизировать), и множественные процессы предпринимают попытку записи в один файл. Кроме этого, сбой подачи питания на сервер хранилища электронных сообщений во время операций записи на диск часто портит как минимум последнее сообщение в файле mbox, а иногда и весь файл mbox.

Формат сохранения сообщений Maildir

Формат сохранения почтовых сообщений maildir появился позже формата mbox. Maildir изобретен автором Qmail, и первая реализация maildir была представлена в Qmail. Одно из наиболее заметных отличий хранилища mbox от maildir заключается в том, что хранилище maildir сохраняет электронные сообщения как отдельные файлы. Блокировка здесь не требуется, что означает способность к работе этого формата доставки даже при дефектной активизации блокировки в нижележащих сетевых протоколах файла или в приложениях. Множественные процессы могут осуществлять запись в хранилища maildir одновременно, без блокирования элементов или утерянного/испорченного электронного сообщения.

Более подробная информация о доставке файлов и механизмах манипуляций, применяемых в maildir, содержится в оригинальной документации профессора Бернштейна (www.qmail.org/man/man5/maildir.html). Более полное обсуждение форматов maildir, включающее в себя квоты maildir, имеется на сайте www.courier-mta.org/maildir.html.

Формат сохранения сообщений Database

Сохранение почтовых сообщений по типу базы данных в основном используется в коммерческих патентованных продуктах, таких как Microsoft Exchange или Oracle Messaging. В большинстве открытых промышленных приложений передачи сообще-

ний используются форматы maildir или mbox, хотя Cyrus-IMAP использует собственное хранилище электронных сообщений по типу базы данных. Несмотря на то, что хранилище по типу базы данных предлагает набор потенциальных преимуществ, оно одновременно повышает сложность сохранения и имеет недостатки, отсутствующие в сравнительно простых механизмах хранения почтовых сообщений по типу «файл-и-каталог». На данном этапе maildir считается наиболее предпочтительным открытым форматом хранения сообщений для корпоративного обмена информацией.

Анализ открытых серверных программных средств передачи сообщений

История и разнообразие открытых серверных программных средств передачи сообщений начинается с пакета Sendmail, появившегося в 1980 году, за которым в 1990 году последовали Postfix, Exim, Qmail и Courier. В настоящее время существует множество открытых программных средств для передачи, приема, доставки электронной почты и доступа к ней с помощью открытых программных средств. В данном разделе будут рассмотрены наиболее популярные программные средства передачи информации.

Исторически сложилось много способов передачи электронных сообщений между хостами. Sendmail является первым групповым MTA. За этим пакетом последовало несколько других, которые, впрочем, не получили широкого распространения. Пакет Qmail сменил Sendmail как более безопасное и эффективное решение. В Qmail имел место более эффективный формат сохранения сообщений, решавший ряд проблем сохранения сообщений обычным способом. Однако Qmail — это очень простое решение, что называется, «чистый» MTA. Postfix был создан для решения проблемы так называемого «хлама» (результата не очень добросовестной программистской работы) — сложного синтаксиса конфигурации, а также других аспектов Sendmail, и с целью создания устойчивого MTA, который бы реализовывал самые современные функции, ожидаемые от почтового агента. Наконец, были объединены несколько проектов, связанных с передачей электронных сообщений, в результате чего было создано решение Courier MTA.

Sendmail

Обсуждение открытых программных серверных средств передачи сообщений стоит начать с рассмотрения пакета Sendmail, «предка» MTA. Первая версия Sendmail написана в 1980 году, задолго до того, как SMTP стал глобальным протоколом передачи электронных сообщений. В то время сообщения передавались по разным сетям в разных форматах. Революционным преимуществом пакета Sendmail явилась его способность передавать сообщения между разными сетями путем конвертирования сообщения для соответствия формату каждой сети.

Несмотря на то, что Sendmail по-прежнему широко используется, это происходит не из-за простоты использования. В Sendmail используется сложный, «страшный» конфигурационный файл. Его сложность обросла легендами, и далеко не каждый новичок сможет в нем разобраться. Конфигурационный файл Sendmail больше напоминает отдельный мини-язык программирования; это, по сути, низкоуровневый сценарий, по шагам описывающий обработку Sendmail электронных адресов и заголовков. Рекламный материал конференции Usenet в 1996 году показал, как можно использовать конфигурационный файл Sendmail для решения загадки Ханойских башен.

К счастью, в современные версии Sendmail входит макропрепроцессор. Вместо кодирования сценариев Sendmail вручную, конфигурация Sendmail описана с помощью набора директив конфигурации высокого уровня. Затем макропрепроцессор преобразует эту директиву в «родной» конфигурационный файл Sendmail.

Более того, Sendmail уже включен во все крупные дистрибутивы Linux в виде стандартной части. Sendmail обычно поставляется в достаточно общей конфигурации, поэтому во многих случаях практически никакой настройки не требуется. При этом, для небольших предприятий, переходящих на инфраструктуру Linux, выбор Sendmail, как правило, не рекомендуется. Можно выбрать более простой почтовый агент из числа включенных в большинство дистрибутивов Linux.

Для получения дополнительной информации по Sendmail посетите сайт www.sendmail.org. Информация по службам поддержки Sendmail и инструментам графической конфигурации имеется на сайте www.sendmail.com.

Qmail

Qmail — интересный почтовый агент. Используется он не очень широко из-за необычных условий лицензирования, однако этот пакет имеет репутацию очень надежного. Был случай, когда автор Qmail предлагал 500 долларов любому, кто выявит слабые места защиты, и эта премия осталась невостребованной.

Почтовый агент Qmail написан профессором Даниэлем Бернштейном в начале 90-х годов. Во многом Qmail является полной противоположностью Sendmail, который выполняется как единый монолитный процесс, реализующий все функции. Qmail представляет собой большой набор совместно работающих небольших модулей, каждый из которых предназначен для выполнения одной определенной задачи. В Sendmail используется один файл конфигурации с запутанным синтаксисом, а Qmail сохраняет данные конфигурации в виде отдельных текстовых файлов.

Главным вкладом Qmail в технологию почтовых агентов является разработка формата maildir для хранения электронных сообщений. Традиционно все сообщения в папке сохранялись как отдельный файл. На заре развития Интернет данного формата сохранения, называемого «mbox», было достаточно, однако по мере роста популярности электронной почты, все отчетливее стали заявлять о себе ограничения

mbox. В один момент времени папку обновить мог только один процесс, поэтому для координирования доступа к папке конкурирующих процессов возникла необходимость в функции блокировки, а традиционная блокировка файлов работала ненадежно с сетевыми файловыми системами. Для обновления папки процессу приходилось существенно переписывать заново весь файл либо его бóльшую часть. Если процесс прерывался до завершения, то результатом становилась испорченная почтовая папка.

Механизм maildirs, применяемый Qmail, помещает каждое сообщение в отдельный файл. Особым правилом именования определяется имя файла каждого сообщения, и существует определенный механизм для того, чтобы множественные процессы одновременно обновляли содержимое почтового ящика, «не наступая друг другу на пятки», и, соответственно, без блокировки.

Формат maildirs стал очень популярным и теперь поддерживается почтовыми агентами Courier, Postfix и Exim. При наличии взаимодействующего MDA (maildrop или procmail) система Sendmail также может осуществлять доставку почты в maildirs.

В качестве альтернативы SMTP профессор Бернштейн предложил новый протокол оперативной передачи почты — *QMTP*. Несмотря на то, что на сегодняшний день в большинстве MTA maildirs является основным форматом, QMTP не получил особого распространения и сегодня используется только в Qmail.

Qmail — очень маленький почтовый агент. Он реализует только самый необходимый минимум SMTP. За последние двадцать лет SMTP значительно усовершенствовался, расширил основные функции, но Qmail не следил за ними. Последняя версия Qmail — 1.03 была выпущена профессором Бернштейном в 1993 году. Qmail недостает ожидаемой от современных MTA функциональности SMTP, например шифрования и аутентификации SMTP.

Одним из основных недостатков использования Qmail в современной среде является то, что структура проекта требует приема всех сообщений, адресованных на локальный почтовый домен. Если почтового ящика назначения не существует, то сервер Qmail сделает попытку возврата сообщения отправителю с пометкой «Доставка невозможна» (*undeliverable*). Основной проблемой является спам. «Макулатурная» почта обычно содержит адреса, невозможные для возврата. Qmail не сможет вернуть сообщение отправителю, и оно останется в очереди Qmail, пока не истечет определенное время и сообщение не будет удалено. Большие объемы не возвращаемого почтового «мусора» могут серьезно повлиять на производительность Qmail.

Несмотря на то, что система Qmail давно не обновлялась, она имеет большую пользовательскую базу. Определенное число «заплаток» (патчей) и дополнений к Qmail третьих производителей устраняют некоторые недостатки системы. Qmail по-прежнему часто рассматривается в средах, где защита и безопасность имеет ключевое значение. По причине небольшого размера системы, при работе с Qmail меньше шансов столкнуться с ошибками. Вообще говоря, чем шире набор функций

программного приложения, тем выше вероятность наличия в нем критичных ошибок. Небольшой размер Qmail делает систему популярной в средах брандмауэров.

Более подробная информация о Qmail имеется на сайте www.qmail.org.

Postfix

Изначально система Postfix была разработана корпорацией IBM в 1997 году. Первым названием было «VMailer», следующим — «IBM Secure Mailer». С раннего этапа своего развития Postfix быстро «набирала обороты» и теперь существует независимо от IBM. Планировалось, что Postfix станет альтернативой Sendmail, однако система больше похожа на Sendmail, чем на Qmail. Postfix активно совершенствуется и по сей день и является MTA по умолчанию многих дистрибутивов Linux.

Postfix проектировалась с целью обеспечения живучести Sendmail с повышенной скоростью, упрощенной конфигурацией и высокой степенью защиты. Результатом стало то, что многие считают наиболее распространенным MTA, устанавливаемым в Linux.

В Postfix входят несколько опций фильтрации спама и множество возможностей реализации виртуальных почтовых ящиков. Поначалу почтовые ящики и системные записи UNIX были едиными: при наличии учетной записи UNIX имелся почтовый ящик и электронный адрес в формате *имяпользователя@домен*. Когда электронная почта стала отдельной службой, необходимость в системных записях для каждого почтового ящика отпала. Почтовый сервер превратился в отдельную систему с доступом к почтовым ящикам только через IMAP или POP3. В Qmail или Postfix почтовые ящики можно создавать без фактической системной записи путем простого добавления учетной информации в файл. После этого список учетных записей в файле компилируется в небольшой файл базы данных. Вместо файлов Postfix также предлагает вариант использования серверов LDAP, MySQL или PostgreSQL.

Более подробная информация о Postfix имеется на сайте www.postfix.org.

Exim

MTA Exim разработана в Университете Кембриджа. Система специализирована под фильтрацию почтовых сообщений и возможность их проверки с помощью собственного специального языка фильтрации почтовых сообщений. Подобно Postfix, Exim поддерживает базы данных LDAP, MySQL и PostgreSQL.

Одной из интересных особенностей фильтрации Exim (также доступной в Postfix) является возможность *идентификации* (обратного вызова). Перед приемом сообщения Exim может воспользоваться электронным адресом отправителя и попытаться связаться с почтовыми серверами отправителя для верификации существования адреса отправителя. При этом процесс доставки почты слегка замедляется, однако при этом удаляется большая часть спама с фальшивыми и несуществующими адресами.

Так же как и Postfix, Exim легко интегрируется с пакетом защиты от спама — SpamAssassin.

Другой интересной особенностью Exim является то, что для выполнения некоторых заданий система может использовать встроенные сценарии Perl. Exim можно описать как MTA для программистов, в том смысле, что навыки программирования позволяют администратору почтовых служб в полной мере использовать преимущества Exim.

Более подробная информация о Exim имеется на сайте www.exim.org.

Набор Courier

Courier — это полная модульная система передачи сообщений, включающая MTA (Courier-MTA), MUA web–почты (SqWebMail), MDA (maildrop), MAA (Courier-IMAP), администрирование на базе web (courierwebadmin), интегрирование LDAP, а также функции календаря и совместного использования ресурсов. Каждое приложение набора представляет собой отдельный продукт, однако они имеют общую кодовую базу и работают в интегрированной манере. Courier сконфигурирован для работы с хранилищем почтовых сообщений в формате maildir.

В табл. 7.5 перечислены компоненты набора Courier.

Табл. 7.5. Компоненты набора Courier

Компонент	Описание
Courier-MTA	MTA для передачи сообщений «хост-хост»
Maildrop	Локальный MDA, подобный procmail
Courier-IMAP	MAA для служб почтовых ящиков IMAP/POP
SqWebMail	MUA на базе web для доступа к электронной почте и календарю (требует cgi-bin Apache)
Webadmin	Модуль администрирования на базе web для Courier (требует cgi-bin Apache)
Courier-MLM	Менеджер списков рассылки
Courier-analog	Отчеты об использовании

Набор Courier включает в себя интегрированное решение для передачи, хранения электронной почты, для клиентского доступа, управления рассылкой почты, а также службы доступа на базе web. Набор имеет программу-календарь с доступом через web. В Courier также присутствует консоль управления на базе web для тех, кто предпочитает GUI (графический пользовательский интерфейс). Кроме всего перечисленного, защита всего пакета Courier легко обеспечивается с помощью кодирования SSL/TLS. Courier вполне соответствует текущим потребностям компании Acme Widgets и будет соответствовать прогнозируемым потребностям недалекого будущего. В будущем Acme Widgets может рассмотреть возможность развертывания факс-шлюза, имеющегося в Courier.

Набор необходимых функций и простота установки делает набор Courier вполне пригодным для использования в компании Acme Widgets. Поскольку требования к передаче почтовых сообщений в компании вполне умеренные (как и бюджет на развитие ИТ), то ее сотрудники получат всю необходимую функциональность без особых сложностей (и дополнительных трудозатрат) в получении MTA, MAA, MDA и пакетов обмена почтовой информацией почты через web.

Courier-MTA

Центральная часть Courier состоит из типичного почтового посредника (MTA). Courier-MTA принимает новые почтовые сообщения, размещает их во внутренней очереди на доставку, планирует доставку и изменяет очередность сообщений при невозможности их немедленной доставки.

Courier обеспечивает несколько элементов управления для выборочного приема и отказа в приеме сообщений. Существует несколько предварительно определенных фильтров, проверяющих сообщения на корректность. Также возможна установка сценария Perl или отдельной программы просмотра и «отсеивания» нежелательных электронных сообщений.

Подобно Exim и Postfix, Courier может использовать LDAP, MySQL или PostgreSQL. Общее введение в Courier см. на сайте www.courier-mta.org.

Maildrop

MDA maildrop поставляется вместе с Courier, однако Courier-MTA может использовать любой другой MDA. Maildrop сходен с procmail, но использует упрощенные команды фильтрации электронной почты в стиле Perl.

Maildrop можно установить либо как глобальный MDA, используемый Courier-MTA для доставки в каждую учетную запись, либо выборочно, исходя из каждой конкретной учетной записи. Courier-MTA может использовать maildrop непосредственно как элемент управления фильтрацией почты, однако это довольно сложная задача, требующая известного объема программирования. Для большинства ситуаций роли maildrop как обычного MDA будет достаточно.

Более подробную информацию по maildrop см. на сайте www.courier-mta.org/maildrop/.

Courier-IMAP

Сервер Courier-IMAP обеспечивает доступ IMAP и POP3 к локальным почтовым ящикам. Как и SMTP, IMAP совершенствовался в течение многих лет, и за это время базовая функциональность ядра IMAP была расширена. Courier-IMAP реализует большинство популярных расширений IMAP, таких как списки контроля доступа (ACL). В Courier-IMAP возможно установить совместно используемые почтовые папки, доступ к которым будет осуществляться множественными учетными записями, в соответствии с правилами, сконфигурированными ACL IMAP. Это можно использовать для реализации

базовых функций коллективного пользования, когда совместно используемые папки применяются для обмена служебными записками и файлами средних размеров.

Подобно другим приложениям Courier, Courier-IMAP можно установить независимо от набора Courier и использовать с любым хранилищем электронной почты maildir. В крупных компаниях принято использовать комбинацию Postfix для отправки/получения электронной почты и Courier-IMAP для обеспечения служб доступа к почте клиентов.

Более подробную информацию по Courier-IMAP см. на сайте www.courier-mta.org/imap/.

SqWebMail

Courier SqWebMail — полнофункциональный сервер web-почты с опцией ведения календаря и с программными средствами коллективного пользования. Интерфейс поддерживает папки пользовательских почтовых ящиков и коллективно используемые папки, а также составление адресных книг, проверку орфографии, календарь, фильтрацию почты и даже кодирование GnuPG. Все эти функции прекрасно отображаются в браузере и не требуют поддержки Javascript. На рис. 7.5 показано одно из диалоговых окон SqWebMail.

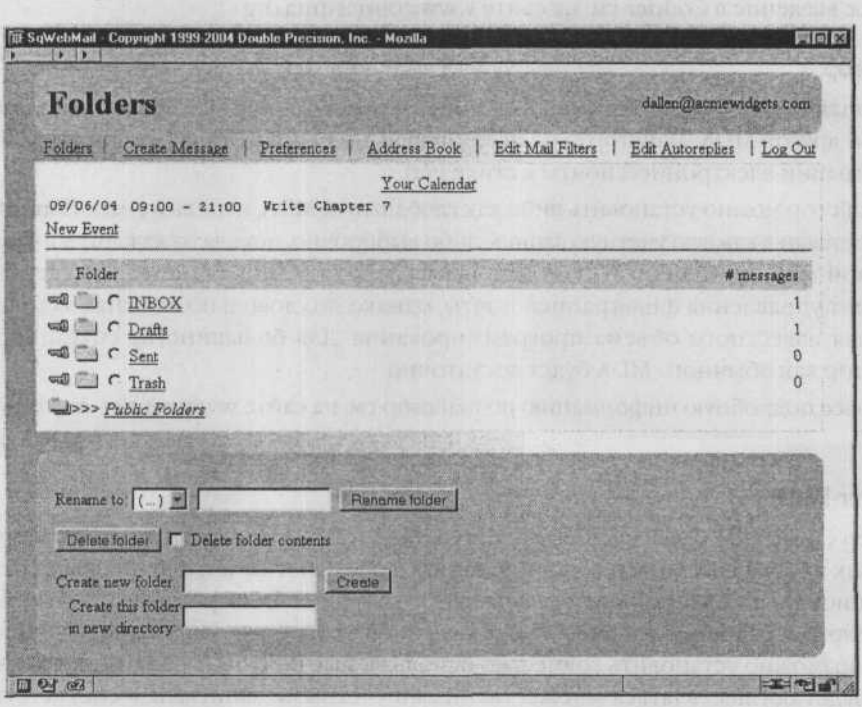

Рис. 7.5. Клиент Courier SqWebMail

SqWebMail работает очень быстро. Прочие серверы web-почты осуществляют доступ к сообщениям установлением фонового подключения к серверу IMAP и скачивают электронные сообщения с помощью IMAP до того, как они будут отформатированы для отображения. SqWebMail осуществляет доступ к maildirs напрямую, без использования IMAP.

SqWebMail также предлагает опцию создания базовых фильтров maildrop с помощью простого web-интерфейса. Этим обеспечивается создание базовых фильтров электронной почты даже без знания программирования.

SqWebMail и webadmin требуют наличие web-сервера с поддержкой cgi, например Apache. Более подробную информацию по SqWebMail см. на сайте www.courier-mta.org/sqwebmail/. На этом сайте представлено много экранных снимков.

Webadmin

Webadmin Courier — это интерфейс на базе web, обеспечивающий доступ к большинству настроек конфигурации. После внесения изменений в конфигурацию сервера webadmin автоматически перезапускает модуль (модули) Courier, на котором могут отразиться эти изменения. На рис. 7.6 показано диалоговое окно webadmin Courier.

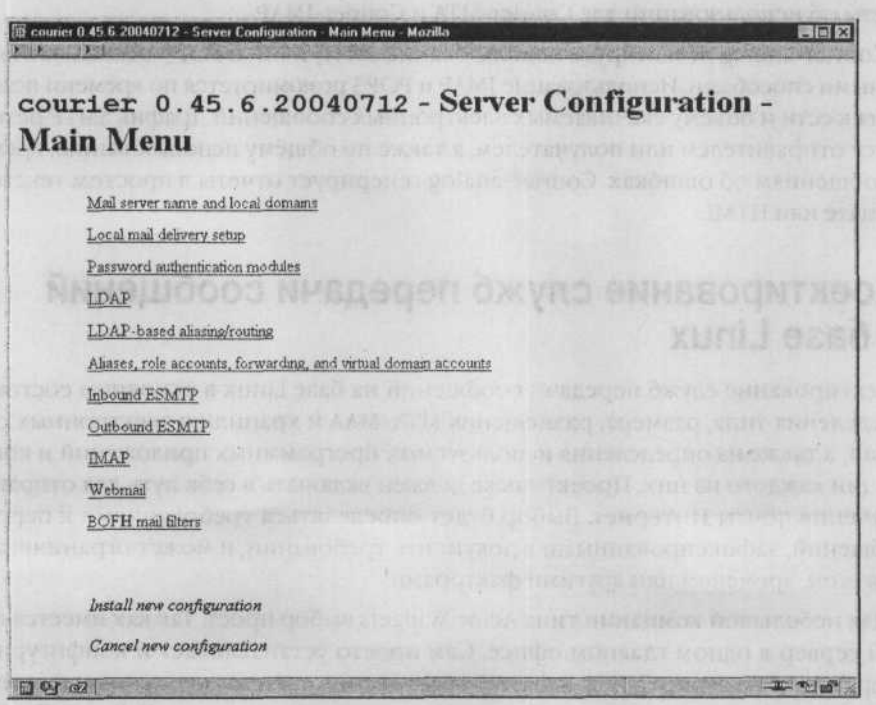

Рис. 7.6. GUI управления Courier Webadmin

Courier-MLM

Courier-MLM — базовый менеджер списков рассылок электронной почты. Для настройки списка адресатов (подписчиков) создайте на сервере Courier отдельную учетную запись с именем списка рассылки, затем установите Courier-MLM как MDA учетной записи, пользуясь указаниями в документации Courier-MLM. Результатом будет простой список рассылки.

Courier-MLM подойдет для создания большинства внутрикорпоративных списков адресатов. Ситуация, когда потребуется более совершенный обработчик списков рассылки, потребует использования вместе с Courier внешнего менеджера списка рассылок.

Courier-analog

Courier-analog — это анализатор регистрационного журнала Courier. Этот модуль не включен в основной дистрибутив Courier. В рамках обычного функционирования многие серверы Courier отправляют сообщения демону системного журнала (syslog), который сохраняет их в файл (обычно /var/log/messages или /var/log/maillog). Courier-analog — это сценарий Perl, считывающий системный журнал и генерирующий отчеты об использовании для Courier-MTA и Courier-IMAP.

Courier-analog резюмирует использование SMTP, IMAP и POP3 несколькими различными способами. Использование IMAP и POP3 резюмируется по времени подключения к сети и объему скачиваемых электронных сообщений. Трафик SMTP резюмируется отправителем или получателем, а также по общему использованию, времени и сообщениям об ошибках. Courier-analog генерирует отчеты в простом текстовом формате или HTML.

Проектирование служб передачи сообщений на базе Linux

Проектирование служб передачи сообщений на базе Linux в основном состоит из определения типа, размера, размещения MTA, MAA и хранилищ электронных сообщений, а также из определения используемых программных приложений и конфигурации каждого из них. Проект также должен включать в себя путь для отправки и получения почты Интернет. Выбор будет определяться требованиями к передаче сообщений, зафиксированными в документе требований, и может ограничиваться бюджетом, временем или другими факторами.

Для небольшой компании типа Acme Widgets выбор прост. Так как имеется всего один сервер в одном главном офисе, Сэм просто устанавливает и конфигурирует набор Courier на сервер Linux, и фаза развертывания системы передачи информации завершается за несколько минут. В крупных компаниях, таких как Ballystyx Engineering, ситуация не настолько проста. В таких компаниях много серверов, филиалов и

пользователей. Поскольку эффективность работы электронной почты критична для деятельности всего предприятия, то при наличии необходимого бюджета для учета различных аспектов проектирования имеет смысл внимательно изучить требования к системе передачи информации, чтобы проект в полной мере соответствовал текущим (и будущим) потребностям.

В том, что касается расширяемости, основной целью компании, проектирующей службы передачи сообщений на базе Linux должно стать проектирование системы передачи сообщений, способной обрабатывать существующие объемы электронной почты, а также быть способной управлять возрастающим за 2-3 года объемом электронной почты и ее хранилищем (включая неизбежный спам и вирусы). Система передачи информации должна обеспечивать пользователей необходимыми функциями, производительностью и быть максимально надежной в рамках бюджета.

Определение архитектуры электронной почты Интернет

Начинать проектирование инфраструктуры электронной почты лучше всего с определения потока электронной почты в Интернет и из него. Чтобы лучше проиллюстрировать этот процесс, рассмотрим архитектуры электронной почты Интернет компаний Acme Widgets и Ballystyx Engineering.

В Acme Widgets доступ в Интернет осуществляется через соединение DSL (цифровая абонентская линия). Такое подключение обеспечивает высокую скорость скачивания информации (около T1), а скорость загрузки только 128 килобит в секунду. Это означает, что получение информации из Интернет происходит очень быстро, а загрузка (включая отправку электронных сообщений) значительно медленнее. Для повышения производительности службы электронной почты (особенно при отправке сообщений больших размеров многим получателям) ISP Acme настроил машину с ретранслятором SMTP. Для ограничения исходящего спама и вирусов ISP Acme не дает клиентам DSL возможности отправлять электронную почту на почтовые серверы Интернет. Вся почта должна проходить через ретранслятор.

Способность ISP Acme к устранению спама и вирусов не ограничивается только исходящей электронной почтой. ISP Acme управляет входящей почтой для AcmeWidgets.com и использует MailScanner для удаления спама и вирусов до того, как почта будет получена сервером Exchange компании. Запись MX для acmewidgets.com указывает на MailScanner.AcmeISP.net. На рис. 7.7 показана текущая архитектура Интернет компании AcmeWidgets.

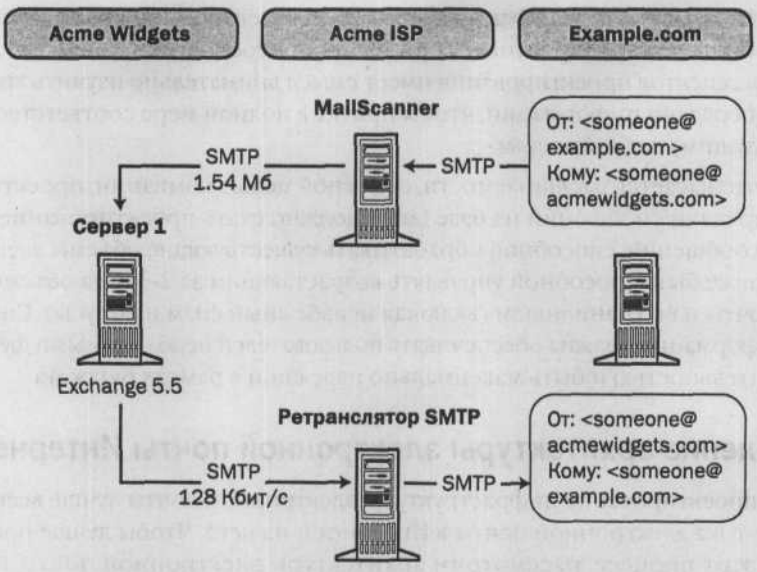

Рис. 7.7. Текущая архитектура электронной почты Интернет компании AcmeWidgets

Из-за ограничений архитектуры электронной почты Интернет, накладываемых провайдером услуги Интернет (ISP), для Acme Widgets можно спроектировать только один поток почты. После перехода Acme Widgets на Linux почтовая архитектура и поток будут выглядеть, как показано на рис. 7.8.

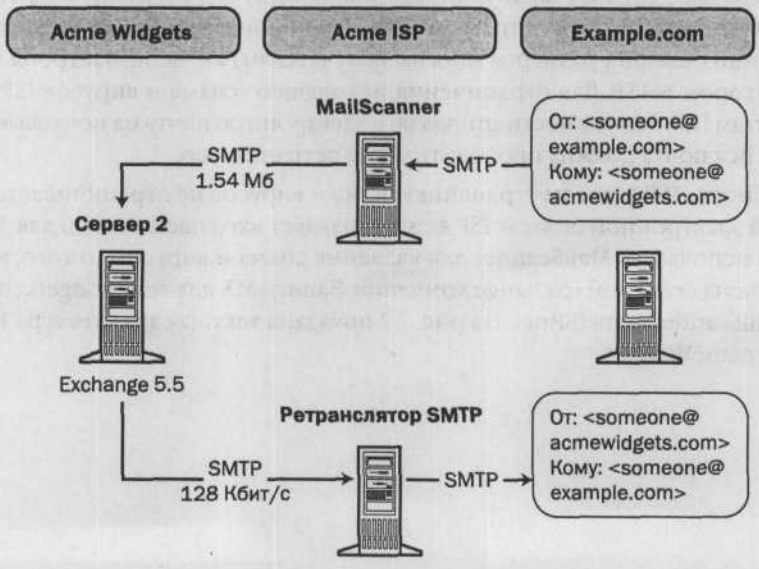

Рис. 7.8. Архитектура электронной почты Интернет компании AcmeWidgets после перехода

В компании Ballystyx Engineering доступ в Интернет осуществляется через подключение Т-1, обеспечивающее высокоскоростное скачивание и загрузку данных. Несмотря на то, что Т-1 обеспечивает значительную пропускную способность, этот канал как бы «забит» спамом и вирусами. ISP Ballystyx не фильтрует входящую почту и не ограничивает исходящую, поэтому компания отправляет и получает почту непосредственно на почтовые серверы Интернет. Запись MX для ballystyx.com указывает на beryllium.ballystyx.com. На рис. 7.9 показаны текущая архитектура Интернет и поток электронной почты компании Ballystyx Engineering.

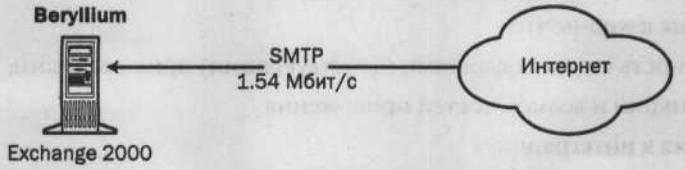

Рис. 7.9. Текущая архитектура электронной почты Интернет компании Ballystyx

Виджей планирует к развертыванию два новых сервера Linux — Boron и Nitrogen, как часть перехода с Windows на Linux. Boron заменит сервер Exchange компании Ballystyx на программные средства передачи сообщений на базе Linux и будет управлять отправкой и получением электронной почты по Интернет. Nitrogen будет развернут в офисе Ballystyx в Бангалоре при наличии времени и соответствующих финансовых средств. На рис. 7.10 показана архитектура электронной почты Интернет Ballystyx Engineering после перехода на Linux.

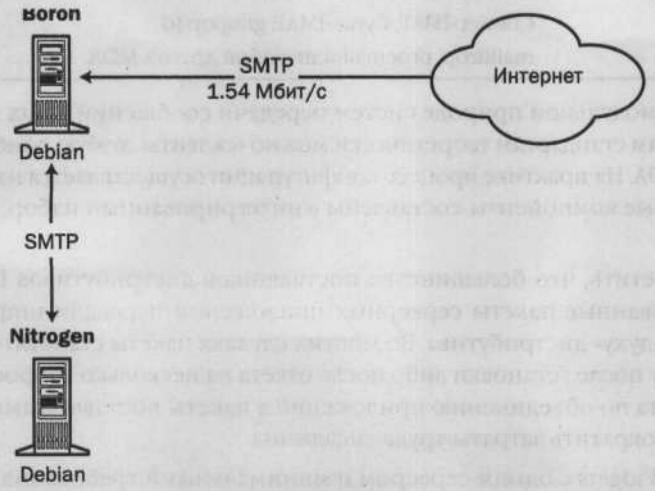

Рис. 7.10. Архитектура электронной почты Интернет компании Ballystyx после перехода на Linux

Выбор программных средств передачи сообщений

Теперь, когда определена архитектура электронной почты Интернет, обратим внимание на программные средства, которые завершат функциональность, определенную в документации с описанием требований передачи сообщений. Существует множество критериев, влияющих на выбор организацией программных средств, включая следующие:

- знание программных приложений ИТ-персоналом;
- аспекты расширения и производительности;
- требования к web-почте;
- совместимость с существующими (действующими) приложениями;
- набор функций и возможностей приложения;
- требования к интеграции;
- ограничения клиента электронной почты.

Для Linux существует большое разнообразие открытых программных средств передачи сообщений. В табл. 7.6 перечислены лишь некоторые открытые компоненты передачи сообщений, рекомендуемые для перехода от Windows к Linux. Более подробная информация об этих приложениях имеется на соответствующих сайтах.

Табл. 7.6. Рекомендуемые открытые серверные приложения передачи сообщения

MUA	SqWebMail, SquirrelMail, OpenWebmail
MTA	Courier-MTA, postfix, exim
MAA	Courier-IMAP, Cyrus-IMAP, gnupop3d
MDA	maildrop, procmail или любой другой MDA

Благодаря модульной природе систем передачи сообщений Linux и приверженности открытым стандартам теоретически можно «склеить» любую комбинацию MUA, MTA, MAA и MDA. На практике процесс конфигурации осуществляется намного проще, когда различные компоненты составлены в интегрированный набор, как в случае с Courier.

Важно отметить, что большинство поставщиков дистрибутивов Linux создают специализированные пакеты серверных приложений передачи информации для соответствия «духу» дистрибутива. Во многих случаях пакеты становятся работоспособными сразу после установки либо после ответа на несколько вопросов по конфигурации. Работа по объединению приложений в пакеты поставщиками Linux может значительно сократить затраты труда сисадмина.

Для Acme Widgets с одним сервером и минимальными требованиям Сэм выбрал набор Courier. Этим было обеспечено простое для развертывания интегрированное решение, соответствующее, а в некоторых случаях и превышающее потребности передачи сообщений компании. Пакет Courier привлек Сэма потому, что он смог за-

менить соответствующие функции Exchange и предложить простое решение перехода, требующее минимум времени на конфигурацию и запуск в работу. С помощью сценариев перехода перенос почтовых данных Acme Widgets на новый почтовый сервер Courier занимает меньше часа.

Из-за более сложных требований к передаче информации в компании Ballystyx Виджей выбрал пакет передачи сообщений, состоящий из нескольких оптимальных открытых приложений. Набор Courier казался привлекательным, но Виджей и другие сотрудники уже имели опыт администрирования postfix и функции и топология клиента web-почты SquirrelMail им нравились больше, чем клиента Courier SqWebMail. Виджей решил, что для Ballystyx предпочтительным MAA (агент доступа к почте) будет Courier-IMAP.

Определение способа хранения электронных сообщений

Одним из самых важных решений при проектировании системы электронной почты является определение способа хранения почты: централизованно, на почтовом сервере, на локальных жестких дисках клиентов. Существует много факторов, которые могут помочь сформировать это решение, включая следующие.

- Имеются ли ноутбуки, требующие функционирования электронной почты без подключения к корпоративной сети?
- Нужна ли пользователям возможность доступа к своим почтовым ящикам более чем с одного компьютера организации?
- Будет ли поддерживаться доступ (например, через Интернет) к почтовым ящикам? Какие протоколы будут поддерживаться локально?
- Будет ли необходим всем или некоторым пользователям доступ к web-почте?
- Сколько протоколов доступа к почте будет поддерживать ИТ-персонал: один или два?
- Будет ли у ИТ-персонала время на обслуживание пользователей настольных рабочих станций/ноутбуков, скачивающих всю свою почту на клиент POP, настроить конфигурацию которого «помог приятель»? В этих случаях почту придется загружать назад на почтовый сервер с помощью IMAP, а это сложный процесс, часто требующий много времени.

Локальное хранение электронной почты затрудняет доступ к хранилищу из нескольких мест и усложняет централизованное резервирование почты. Если организация хочет сделать web-почту доступной всем пользователям, тогда почту следует хранить на сервере. Кроме этого, при сохранении на сервере IMAP работает лучше всего.

Несмотря на то, что потребности в каждой организации разные и программные решения должны подготавливаться для решения конкретных задач, в большинстве

компаний, где предлагаются почтовые службы корпоративного класса (включая папки коллективного пользования) будет использоваться хранение почты на базе сервера с IMAP в качестве протокола MAA.

Проектирование и планирование

Резервирование и восстановление электронной почты

Для хранилищ почтовых сообщений Linux, которые используют @@file-based storage@@ (maildir, mbox), создать резервные копии и восстановить почтовые сообщения так же просто, как и скопировать файлы и каталоги на пленку с последующим восстановлением конкретных файлов и/или каталогов при случайном их удалении или отказе системы хранения на сервере.

Создание схемы почтового сервера Linux

Теперь, когда определены подробности проектирования служб передачи сообщений (не считая служб защиты от спама и вирусов), создадим схему, иллюстрирующую решения проектирования для каждого из компонентов системы передачи информации. Данная схема сходна с концептуальной схемой в разделе «Понятие служб передачи сообщений на базе Linux», но названия компонентов системы передачи сообщений изменены на названия программных приложений, предоставляющих эти службы.

Для обеспечения служб передачи сообщений в компании Acme Widgets используется набор Courier. На рис. 7.11 представлен проект компонентов сервера электронной почты для Сервер2.

В компании Ballystyx Engineering используются компоненты почтового сервера нескольких открытых проектов. На рис. 7.12 показано проектирование почтовых компонентов для Boron и Nitrogen.

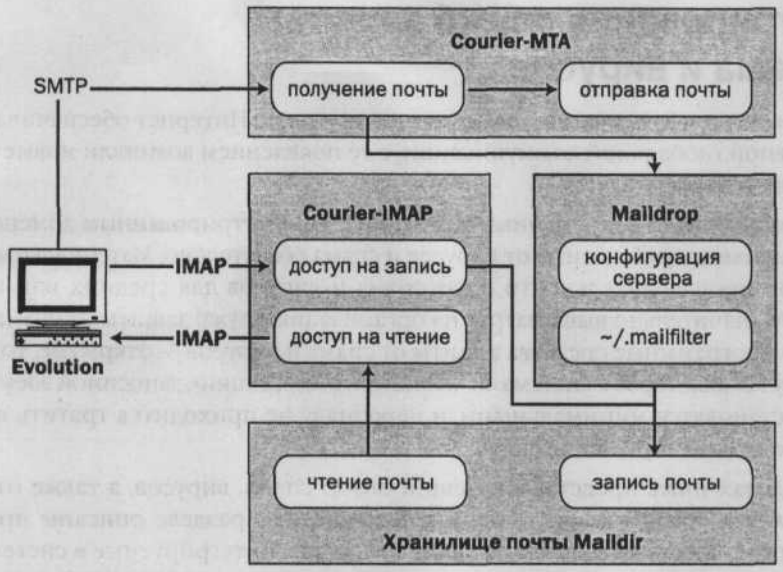

Рис. 7.11. Схема компонентов сервера электронной почты компании Acme Widgets

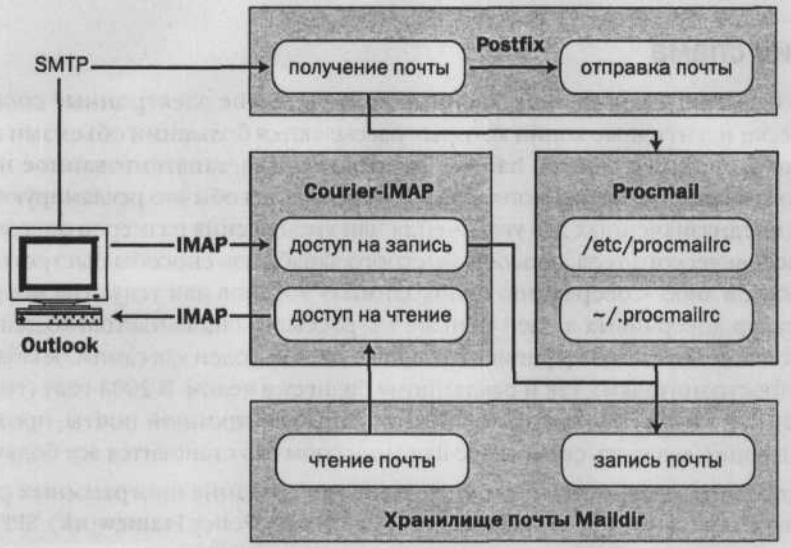

Рис. 7.12. Схема компонентов сервера электронной почты компании Ballystyx

Интегрирование служб защиты от спама и вирусов

Несмотря на то, что пересылка электронной почты по Интернет обеспечила выгоды оперативной глобальной коммуникации, с ее появлением возникли новые проблемы — спам и вирусы.

Для большинства современных компаний с зарегистрированным доменом в Интернет наличие служб защиты от вирусов и спама обязательно. Материальный ущерб от потери производительности из-за спама и вирусов для средних или крупных компаний значительно выше затрат на организацию служб защиты от спама и вирусов. Если программные средства защиты от спама и вирусов — открытые, то затраты на защиту компьютеров с системами Windows от «инфекции», заносимой электронной почтой, становятся минимальными, и персоналу не приходится тратить время на открытие, чтение и удаление спама.

В разделах ниже представлен общий обзор спама, вирусов, а также открытых программных средств защиты от них. В последнем разделе описаны принципы проектирования служб защиты от спама и вирусов, интегрируемые в систему передачи сообщений, а также рассматриваются преимущества и недостатки архитектуры одного сервера, нескольких серверов и аутсорсинга.

Понятие спама

Спамом называются антиобщественные коммерческие электронные сообщения, практически идентичные копии которых рассылаются большими объемами подобно Spam (сокращение от «spiced ham» — острая ветчина; запатентованное название колбасного фарша определенного вида). Эти сообщения обычно рекламируют партии товаров, предназначенных для увеличения или уменьшения размеров определенных частей человеческого тела, способы быстрого заработка, способы быстрого возвращения долгов либо «совершенно необходимых» товаров или услуг. Несмотря на то, что чересчур доверчивых людей меньше 1%, рассылка спама настолько дешева, что даже при таком низком коэффициенте отклика спам выгоден как самим «колбасникам» (его распространителям), так и рекламному бизнесу в целом. В 2004 году (год публикации данной книги) больше половины трафика электронной почты, проходящей через Интернет, являлось спамом, и с каждым годом его становится все больше.

Предпринимались многочисленные попытки создания программных решений защиты от спама, в число которых входит SPF (Sender Policy Framework). SPF работает с помощью записи DNS, указывающей, с каких компьютеров можно отправлять электронную почту от имени указанного домена. Несмотря на то, что на время написания книги SPF широко распространена не была, эта система все-таки применялась на самых известных доменах электронной почты, включая earthlink.net, gmail.com, mail.com и spamassassin.org.

Некоторые правительства принимают законы (например, американский акт U.S. CAN-SPAM), запрещающие рассылку инициативной рекламы. Но из-за трудности отслеживания и наказания нарушителей такие законы не очень эффективны и попросту вытесняют такие виды деятельности в страны с менее строгим законодательством. Так как рассылка спама продолжает оставаться прибыльной, в обозримом будущем борьба с ним будет продолжаться. К счастью, существуют эффективные открытые инструменты, блокирующие практически весь объем поступающего спама с низким коэффициентом ошибок.

Как определить спам?

Первым шагом в деле остановки спама на пути в сеть является определение того, является электронное сообщение спамом или нет. Существует много подходов к выявлению спама, и эффективное приложение защиты от спама так или иначе пользуется этими методиками в зависимости от целесообразности. Важно отметить, что каждый дополнительный тест повышает затраты на обработку каждого сообщения. Тесты по определению спама включают в себя следующее:

- сопоставление «*дактилоскопии*» спама;
- анализ заголовка сообщения;
- анализ тела текста сообщения;
- анализ на основе правил (эвристический);
- байсовский анализ.

Большинство систем защиты от спама присваивает каждому сообщению числовые очки, указывающие вероятность того, что сообщение является спамом. Для SpamAssassin диапазон такой шкалы варьируется от нуля (0% того, что сообщение является спамом) до 10 или более (100% вероятность спама). В хорошо спроектированных системах определения спама по очкам нет единого фактора, определяющего, что электронное сообщение является спамом. Вместо этого учитывается совокупный вес множества факторов, превышающий пороговое значение, заданное администратором системы электронной почты.

В большинстве систем защиты от спама так называемый «счет спама» электронного сообщения представляет собой критерий, определяющий действие (действия), которое будет предприниматься приложением защиты. Сообщения, почти наверняка являющиеся спамом, просто удаляются без доставки. Сообщения, которые, возможно, но не наверняка, являются спамом , могут размещаться в отдельную очередь на просмотр администратором системы электронной почты. Такой обзор может пригодиться при подготовке системы к выявлению спама и помочь ей точно классифицировать эти типы сообщений в будущем.

Другим способом обработки спама является пометка (и пересылка) сообщений, отнесенных к спаму, вводом в строку темы префикса вроде ****SPAM****. В этих случаях доставляться будут абсолютно все сообщения. При этом ни одно электронное сооб-

щение никогда не будет утеряно из-за ошибки классификации спама, но потребуется больше свободного пространства для сохранения и/или какие-то дополнительные усилия со стороны владельца почтового ящика. В большинстве случаев лучше всего останавливать сообщения с очень высоким коэффициентом спама и не тратить место на сохранение или время на обработку спама.

Дактилоскопия спама — один из самых эффективных способов его выявления. Этот метод представляет собой действие, основанное на предположении, что многие сообщения-спам имеют очень много общего. Когда адресат получает новое сообщение, рассчитываются его *«отпечатки пальцев»*, которые потом сличаются по базе отпечатков спама. Если совпадение есть, то это означает, что другой адресат уже сообщил о практически идентичном сообщении как о спаме. Если соответствия «отпечатков» нет, а позже выяснилось, что данное сообщение — спам, тогда адресат может закачать отпечатки нового спама в базу данных отпечатков спама.

DCC, Razor и Pyzor — три открытые службы защиты от спама, работающие как централизованные серверы сбора и распространения отпечатков спама и контрольных сумм. Можно использовать одну, две или все три службы для повышения эффективности выявления спама. В табл. 7.7 перечислены полные названия и адреса сайтов.

Табл. 7.7. Организации с сохраненными отпечатками спама

Полное название	Сайт
Distributed Checksum Clearinghouse	http://www.rhyolite.com/anti-spam/dcc/
Pyzor	http://www.pyzor.sourceforge.net/
Vipul's Razor	http://www.razor.sourceforge.net/

В дополнение к проверке отпечатков спама существует множество эвристических факторов, влияющих на повышение вероятности отнесения сообщения к спаму. Для начала, если электронное сообщение отправляется с IP-адреса, являющегося известным «колбасником», то числовой коэффициент спама значительно возрастает. Если тема сообщения или тело текста содержит определенные слова, (например, «Виагра») либо вариант этого слова с пробелами или в завуалированной форме (например, «В и.аг р_а), то счет спама возрастает. Если существуют проблемы с форматом электронной почты, включая недействительное кодирование MIME (многоцелевые расширения электронной почты в сети Интернет), поддельные строки заголовков или другие характеристики, нарушающие RFC (запросы на комментарии), то числовой коэффициент спама значительно возрастает. Если тело сообщения по большей части состоит из набора HTML-изображений либо содержит непонятный или недействительный HTML, то числовой коэффициент спама возрастает. Если электронные адреса отправителя или получателя (получателей) состоят из странных комбинаций букв и цифр либо имя домена отправителя — yahoo.com, а электронное сообщение отправляется IP-адресом из коммутируемого пула Earthlink.net, то числовой коэффициент спама

также возрастает. И, наконец, если электронное сообщение содержит URL «удалить из списка» (remove from list), предполагающий удовлетворение всех запросов на удаление, тогда числовой коэффициент спама возрастает очень сильно: хорошо известна уловка распространителей спама верифицировать владение электронными адресами существующих пользователей и массированно отправлять на эти адреса потоки спама!

Байсовский анализ представляет собой еще один эффективный метод борьбы со спамом. Он основан на базе данных слов или фраз (называемых *маркерами*), которые часто используются в «чистых» сообщениях, но почти никогда — в спаме, а также на второй базе данных маркеров, часто используемых в спаме, и почти никогда — в обычных сообщениях. Фильтры спама на основе байсовского анализа распространены не очень широко, потому что перед их использованием необходимо внести информацию о том, что есть спам, а что — нет. Чем больше спама и «чистых» сообщений анализируется байсовским механизмом, тем эффективнее он в борьбе со спамом.

Бороться со спамом сложно, потому что его природа постоянно изменяется. Непрерывное возрастание сложности спама и технологий защиты от него напоминает гонку вооружений, когда каждая из сторон делает все возможное, чтобы обогнать соперника. К счастью, сообществу программистов, работающих с открытыми средствами, и администраторов служб электронной почты удается справляться со спамом оперативной реакцией на появление новых «изобретений», обновлением эвристических фильтров и сообщениями о спаме организациям, занимающимся исследованием «отпечатков» спама.

«Белые» и «черные» списки

Составление «белых» и «черных» списков —метод разрешения или запрета доступа с использованием особых списков. По отношению к спаму это означает, что электронное сообщение можно классифицировать как спам на основе IP-адреса отправителя и/или электронного адреса/домена. «Белые» и «черные» списки могут быть очень эффективными и их можно использовать, чтобы избежать ошибочных выводов при выявлении спама. Составление «белых» списков имеет смысл, когда пользователи являются подписчиками списков электронной почты, получают сообщения как участники коммерческих проектов либо периодически сталкиваются с проблемами получения сообщений от хорошо известных отправителей/получателей по причине их задержки фильтром спама.

Одним из самых эффективных способов применения «черных» списков в борьбе со спамом является использование службы MAPS RBL («черный» список в режиме реального времени). RBL содержит тщательно поддерживаемый список IP-адресов, известных в качестве распространителей спама. Более подробная информация о MAPS RBL имеется на сайте www.mail-abuse.com/services/mds_rbl.html.

Несмотря на определенную дополнительную административную нагрузку, связанную с использованием «черного» и «белого» списков, они рекомендуются для повышения эффективности действий по борьбе со спамом.

Понятие вирусов

Помимо спама, еще одной проблемой, связанной с широким распространением электронной почты и компьютеров с системой Windows, являются вирусы, передаваемые вместе с сообщениями. При попытке инфицирования вирусом, передаваемым в электронном сообщении, пользователю обычно предлагается просмотреть (открыть) «зараженное» сообщение (или вложенную информацию) с провокационной темой (бесплатный приз, «интересная» картинка и т. д.). Такие типы атак называются «Троянским конем» по аналогии с историческим деревянным конем, с помощью которого грекам удалось проникнуть в город Трою и захватить его. При обсуждении вирусов в данной книге авторы имеют в виду собственно вирусы, «червей» и троянов.

Вирусы, передаваемые в электронных сообщениях, можно разделить на две категории.

- Вирусы, осуществляющие заражение с помощью уязвимых мест популярных почтовых клиентов, как правило, их частей, отвечающих за отображение HTML. Самые известные примеры: Outlook/Express и «движок» IE HTML (MSHTML.DLL).
- Вирусы, осуществляющие заражение, «замаскировавшись» под безопасное вложение. Когда пользователь открывает «троянское» вложение, запускается сценарий вируса или «нехороший» файл другого типа.

Воздействие вирусов, передаваемых по электронной почте, изменяется от плохого к очень плохому. В табл. 7.8 перечислены общие типы воздействия вирусов, передаваемых с электронными сообщениями.

Определенные виды файлов распространяют вирусы проще других. Файл должен иметь тип, который может быть выполнен базовыми операционными системами (обычно Windows), либо этот файл должен предоставлять возможности для написания сценариев или макросов.

Несмотря на то, что качественные программные решения контроля вирусов должны обращать особое внимание на ограничение их распространения, самым желательным антивирусным решением будет то, которое сможет предотвратить появление вирусов в корпоративной системе. Одним из самых простых способов защиты от вирусов такого типа является сканирование и/или блокирование некоторых или всех вложений, которые потенциально могут содержать вирусы. В табл. 7.9 представлен список типов файлов, которые можно использовать для выполнения злонамеренного кода на компьютере под Windows. Эти типы файлов не представляют такой угрозы для рабочих станций с Linux.

Табл. 7.8. Типы воздействия вирусов

Метод	Описание	Действие
Размножение по электронной почте	Вирус сообщения рассылает пользователям копии самого себя в Глобальном списке абонентов Exchange, в личной адресной книге или по электронным адресам, найденным в файлах на жестком диске. Когда пользователи открывают инфицированное сообщение или вложение, они автоматически рассылают его копии другим пользователям	Переполнение МТА и поглощение доступного пространства сохранения в хранилище почтовых сообщений
Размножение по сети	Вирус распространяется подключением к другим компьютерам и использованием «пробелов» защиты для инфицирования целевого хоста либо размещением копий самого себя в файлах коллективно используемых сетевых ресурсов. Затем вновь инфицированный хост делает попытку связи и инфицирования других хостов	Может «забить» пропускную полосу сети
Раздражение (annoying)	Вирус может многократно выводить какое-либо раздражающее или надоедливое сообщение, но, как правило, не распространяется на другие машины	Надоедает, но ничего не портит
«Черный ход» (backdoor)	Вирус электронного сообщения устанавливает программное обеспечение, позволяющее хакерам контролировать компьютер удаленным способом. Этот вирус может в обычном режиме связываться с сервером, поставляющим обновленные команды	Позже контролируемые хакерами компьютеры могут инициировать «нападения» и вызывать серьезные сбои в работе систем
Регистрация нажатий клавиш	Вирус регистрирует (записывает) все нажатия пользователем клавиш, включая имена пользователей и пароли. Эта информация может сохраняться локально или передаваться на компьютер хакера	Хакеры получают действующие имена пользователей и пароли, после чего используют их для совершения «нападений»
Разрушение (destructive)	Вирус осуществляет атаку на локальную машину и вложенные коллективно используемые файлы; при этом файлы могут стираться или изменяться. Вирус может поражать другие машины сети	Подобно стандартному проявлению вируса в настольной рабочей станции, очистка от вируса обычно включает в себя восстановление (перенос) резервных файлов с магнитного носителя
Гибрид	Гибридный вирус использует от двух до нескольких типов воздействия и/или маршрутов инфицирования, а также может объединять в себе усовершенствованные функции (например, полиморфизм), во избежание выявления программами защиты от вирусов	Может быть крайне разрушительным; трудно поддается «излечению» и преодолевает многие виды защиты

Табл. 7.9. Список блокирования вложений

Расширение	Тип файла
.PIF	Информационный файл программы
.BAT	Командный файл
.CMD	Командный файл
.COM	Исполняемый файл
.EXE	Исполняемый файл
.VBS	Язык сценариев, разработанный на основе языка Visual Basic
.SCR	Хранитель экрана Windows

Следует отметить, что причиной свыше 90% заражений вирусами, передаваемыми в электронных сообщениях, являются «дыры» Outlook/Express и IE (обычно MSHTML.DLL). Пройдет еще много времени, прежде чем пользователи откажутся от применения систем Exchange, Outlook/Express и Internet Explorer. Переход на системы передачи сообщений на базе Linux и Mozilla обеспечит повышение степени защиты от вирусов, а перевод настольных рабочих станций с Windows на Linux обеспечит еще большее повышение степени защиты.

Обзор открытых приложений защиты от спама и вирусов

Теперь, когда теоретически стала понятной подоплека служб защиты от спама и вирусов, рассмотрим открытые приложения, выполняющие эти важные задачи фактически. В данном разделе рассматриваются три самые популярные открытые приложения защиты от спама и вирусов:

- SpamAssassin;
- Clam AntiVirus;
- MailScanner.

Несмотря на разнообразие открытых приложений, выполняющих функции защиты от спама и вирусов, три указанных приложения очень широко используются для обеспечения этих служб и предоставляют простое для развертывания решение, соответствующее потребностям практически всех компаний.

SpamAssassin

SpamAssassin — это очень популярное открытое приложение защиты от спама. В данной книге, при упоминании SpamAssassin имеется в виду версия SpamAssassin 3.0.x. Будучи изначально закрытым продуктом компании Deersoft, который впоследствии был опубликован как open-source, SpamAssassin представлял собой набор сценариев Perl, выполняющих эвристический анализ текста заголовков и тел электронных сообщений. В число процедур входит нахождение соответствий слов и фраз, выявление попыток запутать сканер, анализ содержимого HTML, анализ электронного

сообщения и адреса, байсовский анализ, сопоставление «отпечатков» спама, а также использование «черных» и «белых» списков. Таким образом, можно сказать, что SpamAssassin — это зрелый продукт, имеющий практически все функции выявления спама, которые могут потребоваться в компании.

SpamAssassin легко интегрируется с Postfix, Exim, Sendmail и любым другим MTA и большинством открытых программных средств передачи сообщений. Функциональность SpamAssassin используется во многих открытых (и даже в некоторых коммерческих) продуктах. Для предоставления клиентам недорогих служб защиты от спама пакет SpamAssassin используется многими провайдерами услуг Интернет (ISP). Конфигурацию SpamAssassin легко настроить с помощью Webmin (www.webmin.com) или оперативного конфигуратора (www.yrex.com/spam/spam-config.php).

SpamAssassin может использовать все три бесплатные базы данных «отпечатков» спама. Документация по интегрированию этих услуг со SpamAssassin находится на следующих URL:

- http://wiki.apache.org/spamassassin/UsingDcc
- http://wiki.apache.org/spamassassin/UsingPyzor
- http://wiki.apache.org/spamassassin/UsingRazor
- http://spamassassin.apache.org

ClamAntiVirus

ClamAV — популярный вирусный сканер командной строки, распространяющийся по лицензии GPL. В данной книге имеется в виду версия ClamAV 0.80. ClamAV выявляет и изолирует свыше 20 000 известных вирусов и интегрируется практически с любым MTA или хранилищем почтовых данных. Система даже выявляет вирусы в системах архивирования zip, gzip, bzip2, rar и др. ClamAV включает в себя устройство автоматического обновления баз данных (freshclam) с поддержкой верификации цифровой подписи.

ClamAV используется многими провайдерами услуг Интернет и популярными открытыми доменами, такими как SourceForge.net и RoaringPenguin.com. База данных вирусов ClamAV обновляется несколько раз в неделю, и рабочая группа ClamAV по базам данных (virusdb) очень быстро реагирует на угрозы новых вирусов.

Более подробная информация о ClamAV имеется на сайте www.clamav.net.

MailScanner

MailScanner — это оригинальный продукт, объединяющий защиту от спама, вирусов и фильтрацию прочих вредоносных изобретений в единый пакет, работающий со SpamAssassin, ClamAV и другими сканерами вирусов. MailScanner — известное, проверенное и широко используемое интегрированное решение, работающее практически с любым открытым почтовым агентом или программой защиты от спама или ви-

русов. Для большинства компаний MailScanner будет прекрасным выбором в том, что касается набора функций и простоты развертывания. MailScanner сканирует электронное сообщение на наличие:

- вирусов с помощью сканеров вирусов (до 14), включая ClamAV;
- спама с помощью SpamAssassin и обычным коэффициентом выявления, равным 95% или выше;
- других видов атак, связанных с электронными сообщениями, и вредоносных разработок, созданных на основе известных (иногда и неизвестных!) слабых мест в системах защиты.

Помимо всего сказанного, система MailScanner сконфигурирована с определенной степенью защиты, во избежание отказа в обслуживании и исчерпания ресурсов. Она будет удалять подозрительные объекты при первой возможности и при необходимости обеспечивать «карантин» разделов. MailScanner используется тысячами организаций и сотнями тысяч пользователей, ежедневно защищая от спама и вирусов миллионы сообщений. MailScanner обладает высокой степенью конфигурируемости, но очень легко устанавливается с популярными MTA либо в режиме шлюза. Все практические рекомендации по установке описаны на сайте, рассказывающем, как интегрировать MailScanner в почтовый сервер, хотя самым простым способом выполнения этой задачи будет использование MailScanner в режиме шлюза.

Более подробная информация о MailScanner — на сайте www.mailscanner.info.

Проектирование служб защиты от спама и вирусов

Теперь, получив более-менее расширенную информацию о спаме, вирусах и открытых программных средствах защиты от них, пользователь сможет спроектировать программное решение защиты от спама/вирусов, соответствующее (или превышающее) требованиям его организации. Для служб защиты от спама/вирусов здесь рассмотрены четыре типа архитектурных решений: шлюз электронной почты, совместно используемый сервер, коммерческое устройство и аутсорсинг.

Для очень маленькой компании, такой как Acme Widgets, с ограниченным бюджетом и скромными ИТ-возможностями самым простым решением будет использование бесплатных служб защиты от спама и вирусов, предоставляемых по договору с провайдером услуг Интернет Acme (Acme ISP) о предоставлении служб домена для Acme-Widgets.com. В этом решении аутсорсинга Acme Widgets получит все преимущества служб защиты от спама и вирусов, без необходимости обращения к серверу или обслуживания программных средств.

Для Ballystyx Engineering Виджей выбрал выделенное решение шлюза электронной почты для защиты от спама и вирусов. При этом компания получила преимущество размещения служб защиты от спама и вирусов на отдельном сервере, что легко по-

зволило сисадмину усовершенствовать инфраструктуру защиты от спама и вирусов, не затрагивая внутреннюю службу электронной почты.

Коллективно используемый сервер электронной почты и защиты от спама и вирусов

В настоящее время широко распространена установка всего программного обеспечения защиты от спама и вирусов на одной машине, особенно в обстоятельствах ограниченного бюджета. Обычно это означает интегрирование SpamAssassin, ClamAV и/или MailScanner с MTA сервера. Описание тонкостей конфигурации такой установки не входит в задачи данной книги. Полностью эта тема описана в документации MaiScanner на сайте www.mailscanner.info.

Данное решение обладает преимуществом высокой конфигурируемости и возможности отбрасывания спама разных типов или вредоносных программ до их получения почтовым ящиком пользователя (но не до того, как спам войдет в корпоративную сеть). Установка, конфигурация, устранение неисправностей и настройка этой системы может занять очень много времени, однако она обеспечивает максимальный контроль за средой защиты от спама/вирусов/вредоносных программ. Если рассматривается возможность использования данного решения, следует помнить о том, что выполнение всех указанных процессов на одной машине может перегрузить ресурсы компьютера и что решение использования коллективного сервера может столкнуться со значительными сложностями в расширении (или настройки) по мере увеличения количества пользователей. Многие компании в начале своего развития принимают на вооружение коллективный сервер, но по мере роста переходят на выделенную систему шлюза электронной почты, описанную ниже.

Выделенный шлюз защиты от спама и вирусов

Другим подходом к защите от спама и вирусов является использование компьютера, специально выделенного для обработки электронных сообщений на предмет спама и вирусов. Такой шлюзовый компьютер принимает подключения SMTP из Интернет и выполняет проверку на спам, вирусы и наличие вредоносных программ до того, как электронное сообщение войдет в сеть внутренних почтовых серверов. Такой проект показан на рис. 7.13.

Проиллюстрированный вариант привлекателен по многим показателям. Аспекты технического обслуживания, интегрирования и расширяемости переносятся на одну машину, а аспекты производительности с почтовым шлюзом не снизят производительности почтового сервера для пользователей почтовых ящиков. Проблемы производительности со шлюзом могут немного замедлить доставку почты, но никак не повлияют на работу пользователей с электронной почтой. Если позволяет бюджет, то, как правило, функции защиты от вредоносного программного обеспечения целе-

8 Зак. 1269

Рис. 7.13. Шлюз электронной почты защиты от спама и вирусов

сообразно разместить на отдельной машине и убедиться в том, что для этих функций (служб) имеются вычислительные возможности даже при росте объема передаваемых сообщений.

Компании Ballystyx эта идея понравилась настолько, что Виджей принял решение немного опередить события. Из-за того, что провайдер услуг Интернет компании Ballystyx имел инвентарный излишек недорогих размещенных серверов, Виджей мог арендовать бывший в употреблении сервер за очень умеренную ежемесячную плату вместо приобретения нового сервера. Используя этот сервер для работы системы MailScanner, Виджей получил возможность обеспечить компании Ballystyx службы защиты от спама и вирусов, уменьшив нагрузку на линию Интернет, которая до этого была перегружена спамом, вирусами и вредоносными программами.

Машина (Mercury) физически была расположена в помещении, принадлежащем провайдеру, а не на территории Ballystyx, но для Виджея это не имело значения, потому что для безопасного обслуживания Mercury он мог использовать ssh (доступ предоставлялся только с IP-диапазона компании Ballystyx). Технические мощности провайдера были более совершенными, чем на Ballystyx, и это означало, что машина Mercury могла выдерживать более продолжительные перебои в подаче питания и была лучше защищена от землетрясений. У провайдера также был более защищенный почтовый шлюз, который мог принимать и обрабатывать электронную почту даже в случае отключенного питания в компьютерном зале Ballystyx. Такое решение было предпочтительнее по многим показателям, включая повышение скорости предоставления служб Интернет путем сокращения пропускной способности для потока электронной почты.

Если юридически требовалось архивирование или фильтрация типов электронных сообщений, то почтовый шлюз можно было сконфигурировать на обработку исходящей почты либо для упрощения решения этой задачи можно было добавить второй сервер. Данной функцией можно управлять с помощью одного из MTA, рассмотренных в книге.

Коммерческое устройство

В некоторых случаях бывает проще приобрести не очень дорогое устройство почтового шлюза для защиты от спама и вирусов. Развертывание его можно осуществить у провайдера услуг Интернет либо в компьютерном зале головного офиса компании. Существует очень много производителей, предлагающих разнообразные устройства, соответствующие потребностям компании любого размера или рода деятельности. На некоторых из этих шлюзовых устройств могут выполняться даже открытые программные средства. Практически у всех этих устройств имеется функция интерфейса конфигурации на базе web для упрощенного управления устройством.

Как правило, такие устройства продаются с соглашением о подписке и технической поддержке. В это соглашение обычно включается механизм получения программных средств, правила и обновления подписи. Следует помнить о том, что обновления прекращают поступать, если соглашение не оплачено или не обновлено, поэтому существует риск блокирования соглашения с поставщиком (производителем), если в устройстве не используются открытые программные средства, которые могут поддерживаться самим пользователем.

Даже с потенциальным риском зависимости от поставщика данное решение имеет преимущества освобождения организации от управленческих и административных требований, связанных со службами защиты от спама и вирусов. Для некоторых организаций, особенно тех, где сотрудникам недостает знания (или желания обучения) технологий защиты от спама и вирусов, данное решение может быть весьма привлекательным.

Аутсорсинг

Несмотря на то, что многосерверные решения и коммерческие устройства подходят для компаний с соответствующими бюджетами, временем и персоналом, предпочтение службам защиты от спама и вирусов, предоставляемым провайдером услуг Интернет (как в случае с Acme Widgets), избавляет компанию от задач (и возможных трудностей) управления этими услугами. При разумной цене выбор программного решения может быть еще и наименее затратным и сможет достаточно часто выступать как часть пакета услуг по поддержке домена.

Для компаний, которые хотят вообще избавить себя от сложностей управления электронной почтой, существует возможность заключения субдоговора на полную передачу управления провайдеру Интернет услуг (ISP), в этом случае последний занимается управлением электронными адресами домена Интернет (включая записи MX), службами входящей (и исходящей) почты (SMTP), хранением почтовых ящиков

и доступом к ним (POP и IMAP). Несмотря на то, что при этом с компании полностью снимаются издержки на хостинг почтовых служб домена Интернет, это ограничивает гибкость и может потребовать скачивания почтовых сообщений на локальные рабочие станции пользователей, что ограничит их работу с такими службами, как web-почта и электронная почта, доступными с любой рабочей станции компании. Подобное скачивание электронных сообщений добавляет клиенту сложности резервирования информации и связанные с ним хлопоты.

Перенос информации из Exchange в Linux

В данном разделе, посвященном собственно переходу, особое внимание уделено переносу электронной почты, сохраненной на серверах Exchange, на работающий экземпляр Courier IMAP. Сценарий, относящийся к данному примеру перехода, был написан для Courier, хотя может работать любой другой источник и целевые серверы IMAP. При ситуации, когда вся почта скачивается с сервера Exchange на локальный почтовый клиент (например, Outlook или Mozilla), информацию по переносу электронной почты см. в главе 11 «Внутренняя структура настольной рабочей станции Linux». Данный перенос обращает особое внимание на почтовые объекты, но не имеет дела с контактами, задачами, журналами и совместно используемыми папками. Функции коллективного использования Exchange описываются в следующей главе — «Службы коллективного использования и ведение календаря». Сценарии потребуют установки модулей Net::LDAP и Mail::IMAPClient языка Perl.

Подготовка Exchange к переносу

Для подготовки Exchange 5.5 или Exchange 2000 к переносу, нужно выполнить определенное количество шагов. Поскольку сценарии переноса электронной почты требуют служб IMAP, необходимо убедиться в активизации служб IMAP на сервере (серверах) Exchange (см. рис. 7.14).

- Активизируйте протокол IMAP почтового сервера.
- Создайте файл с расширением .csv, содержащий пользовательские почтовые ящики и пароли пользователей, которые необходимо перенести. Это необходимо, поскольку Exchange не обеспечивает административного доступа к почтовым ящикам через IMAP. В каждой строке файла должен содержаться набор <имя пользователя>, <пароль>.

При нормальной установке Exchange 2000 устанавливает службу IMAP4 по умолчанию. Необходимо просто войти в панель управления и убедиться в запуске IMAP4. На рис. 7.15 показана эта процедура.

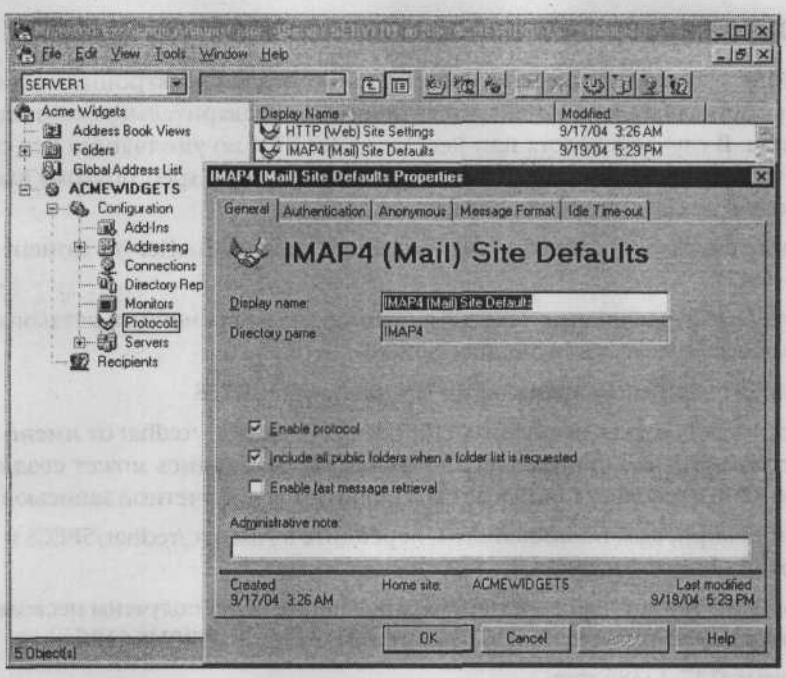

Рис. 7.14. Активизация служб IMAP (Exchange 5.5)

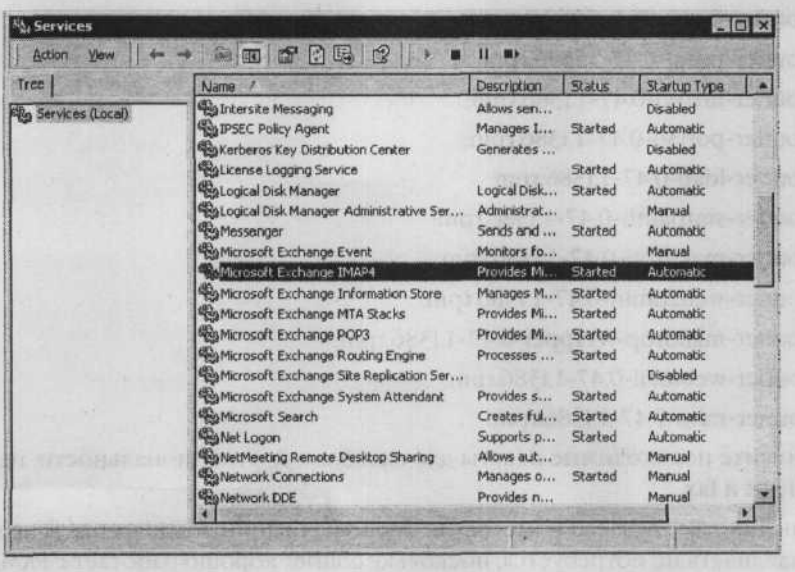

Рис. 7.15. Активизация служб IMAP (Exchange 2000)

Установка серверного набора Courier IMAP

Courier IMAP — это расширенный набор служб передачи электронных сообщений. Для дистрибутива Linux рекомендуется установка предварительно скомпилированного пакета. В случае с Fedora или RedHat AS 3.0 RPM по умолчанию нет, однако в архиве с исходными текстами Courier imap имеется файл .spec, поэтому для систем Redhat можно создавать пакеты. Вот как это делается:

- Скачайте самую последнюю архивированную версию Courier (на момент написания — 0.47).
- Разархивируйте исходные тексты (gunzip/untar) во временный каталог и скопируйте courier.spec в /usr/src/redhat/SPECS.
- Скопируйте оригинал архива в /usr/src/redhat/SOURCES.
- Может потребоваться выполнить chmod –R777 /usr/src/redhat от имени root для проверки того, что непривилегированная учетная запись может создать здесь файлы RPM, поскольку Courier не скомпилируется под учетной записью root.
- Будучи некорневым пользователем, перейдите в /usr/src/redhat/SPECS и введите rpm-build –bb courier.spec
- Компиляция займет некоторое время, в результате будут получены несколько RPM, созданных для версии Redhat в каталоге /usr/src/redhat/RPMS/i386:
  - courier-0.47-1.i386.rpm;
  - courier-mysql-0.47-1.i386.rpm;
  - courier-fax-0.47-1.i386.rpm;
  - courier-pgsql-0.47-1.i386.rpm;
  - courier-imapd-0.47-1.i386.rpm;
  - courier-pop3d-0.47-1.i386.rpm;
  - courier-ldap-0.47-1.i386.rpm;
  - courier-smtpauth-0.47-1.i386.rpm;
  - courier-maildrop-0.47-1.i386.rpm;
  - courier-webadmin-0.47-1.i386.rpm;
  - courier-maildrop-wrapper-0.47-1.i386.rpm;
  - courier-webmail-0.47-1.i386.rpm;
  - courier-mlm-0.47-1.i386.rpm.
- Установите необходимые пакеты для ожидаемой функциональности, например webclient и fax.
- В большинстве случаев такие модули аутентификации, как ldap, pgsql, mysql и т. д. устанавливать не потребуется, поскольку courier хорошо работает с PAM, что делает его наилучшим выбором.

Теперь, когда система Courier установлена, ее необходимо сконфигурировать. Описание всех доступных опций не входит в задачу данной книги, однако авторы рекомендуют обратиться к сопутствующей документации для выполнения настроек для конкретной организации. Примеры для Acme Widgets и Ballystyx приводятся на прилагаемом к книге компакт-диске.

Перевод службы электронной почты на систему Linux

Прилагаемый сценарий w2lmt-migrate-imap автоматизирует процесс переноса общедоступных папок объектов электронной почты с MS Exchange на действующий сервер Courier IMAP. Поскольку Courier требует использования Maildirs (описаны выше) и не создает эти папки для отдельных пользователей по умолчанию, сценарий переноса выполнит задачу автоматически, однако это потребует запуска сценария на сервере Linux, имеющем доступ к записи в домашний каталог пользователя. Сценарий разработан так, что лучше всего он работает с пустыми maildirs, однако он сделает попытку использования существующих экземпляров. Ниже представлен базовый принцип работы сценария (на примере Acme Widgets):

```
w2lmt-migrate-imap -f migrate-imap-acmewidgets.conf
```

- Убедитесь в том, что в наличии имеется все для продолжения.
- Укажите пароль администратора LDAP.
- Считайте список пользователей почтового ящика/пароли из файла csv, представленного в сценарии конфигурации.
- Для каждого пользователя:
  - считайте домашний каталог пользователя из LDAP;
  - сбросьте пароль пользователя Linux/Samba и установите пароль Exchange;
  - создайте нужные Maildirs в домашнем каталоге пользователя;
  - подключитесь к серверу Exchange через IMAP;
  - подключитесь к серверу Courier IMAP (необходимо использовать вновь созданные Maildirs);
  - просмотрите почтовый ящик exchange и скопируйте папки и объекты почтовых сообщений в нужное место на сервере Courier IMAP. (Обратите внимание на то, что поскольку Courier позволяет создавать папки только в папке INBOX, все переносимые папки и сообщения будут помещены в подпапки INBOX).

Важно отметить, что в результате этого процесса, пароль пользователя на PDC (главный контроллер домена) Linux/Samba будет настроен на соответствие паролю, указанному в файле csv. Поэтому из соображений безопасности следует убедиться в том, что пользователи сменили свои пароли с началом использования нового Samba PDC! Помимо этого, данный сценарий не имеет отношения к совместно используемым

папкам (Public). Обрабатывать их придется вручную, поскольку на Exchange они могут содержать различные объекты, не относящиеся к почте, а также особые разрешения.

Резюме

Предполагается, что после ознакомления с материалами данной главы читатель получил общее представление о процессах передачи почтовых сообщений, в частности о передаче сообщений на базе Linux, а также о MUA, MAA, MTA и MDA и процессах проектирования почтовых серверов и систем передачи сообщений, включая программы защиты от спама и вирусов.

При оптимальном использовании полученных знаний, создании прототипа среды передачи сообщений в лаборатории, полном тестировании, развертывании для пользователей и удачном переносе их электронных сообщений — Поздравляем! — теперь почтовые службы вашей компании не зависят от продукта Microsoft Exchange. Теперь осуществляется управление средой передачи информации, менее зависимой от ресурсов, где сообщения передаются, независимо от наличия лицензий, с надлежащей защитой от спама и вирусов.

По окончании ознакомления с материалами главы читатель должен иметь полностью функционирующую службу передачи сообщений. Это означает, что пользователи могут подключать клиентов IMAP (и/или POP) для получения своих сообщений, и организация может надлежащим образом отправлять и получать электронную почту по Интернет. Если применялся Exchange или другой агент доступа к почте (MAA) с возможностью IMAP, тогда все электронные сообщения почтового ящика важного клиента будут благополучно перенесены в почтовое хранилище Linux.

При добавлении в систему передачи сообщений открытых служб защиты от спама и вирусов будут сэкономлены сотни или тысячи долларов на лицензионные программы защиты от спама и вирусов, интегрированные в Exchange. По завершении этой работы от Microsoft Exchange можно отказаться, если нет необходимости переноса коллективно используемой информации / календаря (описывается в главе 8).

При «списании» Microsoft Exchange часто удаляется последнее приложение, зависящее от Active Directory. В этом случае можно списать Active Directory и службы MS-DNS/DHCP, зависящие от Active Directory, с удалением большей части инфраструктуры MS организации. Для большинства организаций это представляет собой основу инфраструктуры и значительную веху в процессе перевода сетевых служб с Windows на Linux.

Несмотря на определенные затраты труда при проектировании, развертывании и переходе на службы передачи сообщений на базе Linux, эти службы, как правило, работают очень надежно и требуют минимум технического обслуживания на протяжении довольно долгого времени.

Краткое резюме по разделам

Понятие служб передачи сообщений Microsoft

- ☑ Exchange 5.5/2000 — программное решение служб передачи сообщений компании Microsoft для Windows NT и Windows 2000 Server. Пакет Exchange предлагает пользовательские почтовые ящики с возможностью совместного пользования, группы электронной почты, совместно используемые папки, интерфейсы IMAP и POP, контакты коллективного пользования, календари для пользователей и групп пользователей, гибкие возможности хранения баз данных, а также почти любую функциональность, необходимую для службы передачи сообщений предприятия.
- ☑ Типичный сервер Exchange 5.5 состоит из пяти подкомпонентов: сопровождение мониторинга, сервер каталогов, хранилище электронной почты, MTA и шлюз SMTP. Exchange 5.5 поддерживает службы передачи сообщений и коллективно используемых средств с доступом к MAPI (интерфейс прикладного программирования для электронной почты), IMAP (протокол интерактивного доступа к электронной почте), POP (почтовый протокол) и HTTP (протокол передачи гипертекстовых файлов).
- ☑ Exchange 2000 предлагает те же (и/или усовершенствованные) возможности, что и Exchange 5.5. Однако Exchange 2000 не обеспечивает службы каталогов и требует Active Directory. При установке Exchange 2000 схема Active Directory обновляется для активизации электронной почты соответствующих объектов.

Понятие служб передачи сообщений на базе Linux

- ☑ Большинство систем передачи сообщений на базе Linux состоит из интегрированной, но все-таки модульной системы, состоящей из множества компонентов, отвечающих за передачу, прием, доставку электронных сообщений, а также за доступ к ним. В число этих компонентов входит почтовый агент (MTA), агент доставки почты (MDA), хранилище почты, агент доступа к почте (MAA) и пользовательский почтовый посредник (MUA).
- ☑ История популярных открытых серверных программных средств передачи сообщений началась с выпуском в 1980 году продукта Sendmail, за которым последовали Qmail, Postfix, Exim и Courier.
- ☑ Sendmail, Qmail, Postfix, Exim и Courier — широко применяемые агенты доставки почты с очень большими возможностями. Каждый из них имеет свои преимущества и недостатки. Courier отличается тем, что включает в себя практически все: MTA, MUA web-почты, MAA, функции календаря и коллективно используемых ресурсов, диспетчер списка рассылки и инструменты отчетности об использовании.

Проектирование служб передачи сообщений на базе Linux

- ☑ По большей части проектирование служб передачи сообщений на базе Linux состоит из определения пути отправки и получения почты по Интернет, а также из определения типа, размера, размещения и конфигурации каждого приложения компонента системы передачи сообщений. Первоочередными целями проектирования системы передачи сообщений должно стать проектирование системы, обеспечивающей пользователям надежное функционирование и возможность расширения на ближайшие 2-3 года, с учетом возможного увеличения объемов передачи электронной почты.
- ☑ На выбор компанией средств передачи информации влияют многие факторы, включая знание (или незнание) персоналом специфических приложений, аспекты расширяемости, совместимости с существующими (действующими) приложениями, требования интегрирования, а также ограничения почтовых клиентов.
- ☑ Для такой маленькой компании, как Acme Widgets, Courier является легким в развертывании решением, соответствующим и в некоторых случаях превышающим потребности компании в передаче информации. Для более крупных компаний, таких как Ballystyx Engineering, популярным выбором является комбинация систем Postfix, Courier-IMAP и SquirrelMail.
- ☑ Двумя важными аспектами проектирования являются вопросы о том, где хранить электронную почту и как осуществлять к ней доступ. Большинству организаций рекомендуется хранить электронные сообщения на сервере с IMAP-доступом к почтовым ящикам.

Интегрирование служб защиты от спама и вирусов

- ☑ Несмотря на то, что пересылка электронной почты по Интернет обеспечила преимущество оперативной глобальной коммуникации, с ее появлением возникли новые проблемы. Для большинства современных компаний с зарегистрированным доменом в Интернет наличие служб защиты от вирусов и спама является обязательным требованием.
- ☑ Спамом называются коммерческие электронные сообщения, отправляемые одновременно многим получателям в Интернет. Тесты по определению спама включают в себя сопоставление *«дактилоскопии»* спама, анализ заголовков сообщения, анализ тела текста сообщения и байсовский анализ. Каждому электронному сообщению присваиваются особые числовые очки, указывающие вероятность того, что сообщение является спамом.
- ☑ К вирусам относятся собственно вирусы, «черви», трояны и другие вредоносные программы, осуществляющие инфицирование и размножение. Воздействие вирусов может быть как неприятным, так и разрушительным. В стратегии защиты от вирусов входит блокирование типов вложений, которые могут содержать вирусы, а также сканирование электронной почты на предмет подписей вирусов.

- ☑ SpamAssassin, ClamAV и MailScanner — три рекомендуемых программных приложения защиты системы передачи сообщений от спама и вирусов. MailScanner объединяет в себе выявление спама и сканирование вирусов в одном интегрированном пакете.
- ☑ В книге рассматриваются четыре типа архитектурных решений защиты от спама и вирусов: шлюз электронной почты, совместно используемый сервер, коммерческое устройство и аутсорсинг.

Перенос информации из Exchange в Linux

- ☑ Методология перехода включает в себя копирование IMAP в почтовый ящик IMAP.
- ☑ Убедитесь, что в Exchange активизированы службы IMAP.
- ☑ Создайте файл csv, содержащий имя пользователя и пароль для каждого переносимого почтового ящика.
- ☑ Установите и сконфигурируйте серверный набор Courier IMAP.
- ☑ Запустите сценарий перехода на хосте Linux с WRITE-ACCESS для каждого пользовательского домашнего каталога.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма «**Ask the Author**»). Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: Как настроить хранение maildir?

О: Для конфигурирования каталога для хранения maildir можно использовать Maildirmake. Для получения более подробной информации введите **man maildirmake**.

В: Существует ли простой способ перехода от формата mbox к maildir?

О: Да. Эту задачу решают mbox2maildir и maildir2mbox. Для получения более подробной информации запустите дистрибутив Qmail и/или зайдите на сайт www.qmail.org.

В: После запуска сценария перехода я подключился к почтовому ящику Courier IMAP. Но в разделе «ВХОДЯЩИЕ» папок не было! Куда делась моя почта?

О: В зависимости от вашего почтового клиента, вам может потребоваться подписка к подпапкам, для того, чтобы они корректно отображались.

Глава 8

Службы коллективного пользования и ведение календаря

Разделы:

- **Понятие служб Exchange, служб коллективного пользования Outlook и календаря**
- **Понятие служб коллективного пользования и календаря на базе Linux**
- **Переход к службам коллективного пользования и календарю Linux**

☑ Резюме

☑ Краткое резюме по разделам

☑ Часто задаваемые вопросы

Введение

Для многих организаций (и поставщиков) программные средства коллективного пользования означают очень многое. Сюда, прежде всего, входит функция ведения календаря, а в контексте коллективного пользования это означает совместно используемые планы (расписания). Для некоторых — это просто доступный через web способ просмотра плана и внесения в него изменений. Для других — это наличие возможности, например, планирования совещания с доступом к свободному/рабочему времени всех участников, рассылки всем графически отформатированного приглашения и обеспечение для пользователей с различными платформами возможности принятия/отклонения приглашения к участию в совещании с обновлениями, предлагаемыми сервером календаря.

Другой формой коллективно используемых программных средств является система совместного управления/разработки содержания (Content Management System, CMS), например TWiki и прочие производные WikiWikiWeb. Sourceforge — еще один пример коллективной разработки расписания. Возможности Sourceforge для разработки программного обеспечения на базе CVS и web, а также функции распространения, позволяют ему поддерживать большую часть открытых проектов, существующих в мире.

Развертывание коллективных средств на базе Linux обычно требует среды LAMP (Linux-Apache-MySQL-PHP/Perl/Python). Подробное описание структуры LAMP не входит в цели данной книги, но является необходимым требованием некоторых средств коллективного пользования на базе web, описанных в этой главе.

Сложные коллективно используемые средства часто требуют развертывания специализированного сервера (например, сервера для работы календаря), а иногда связаны с интегрированием с сервером каталогов (обновление схемы), как в случае с eGroupware.

В данной главе достаточно подробно рассматриваются средства коллективного пользования, система календаря и программные решения для обеспечения совместной работы, соответствующие потребностям таких компаний, как Acme Widgets и Ballystyx Engineering.

Понятие служб Exchange, служб коллективного пользования Outlook и календаря

Возможности совместного использования и планирования комбинации пакетов Exchange / Outlook представляют собой очень привлекательные решения. Используя Outlook в качестве клиента, а Exchange — в качестве структуры связи / управления, корпоративные возможности коллективного пользования становятся доступными для всей организации.

Даже без Exchange клиент Outlook содержит определенное количество функций коллективного пользования или подобных им. В табл. 8.1 перечислены эти функции вместе с кратким описанием.

Табл. 8.1. Функции Outlook

Функция	Описание
Контакты	Имена, электронная почта/почтовые адреса, телефонные номера, место работы, дни рождения и т. д.
Календарь	Ежедневный/еженедельный/ежемесячный просмотр планов (расписаний), встречи, напоминания
Задачи	Состояние, уполномоченные, даты начала/окончания, состояние завершения в %, часы работы
Журнал	Тип работы, время начала/окончания, принадлежность, описание

Поддержка календаря Outlook является полнофункциональной при параллельном обслуживании организации встреч со многими участниками и поддержкой стандартов iCal и vCal (RFC 2445). При объединении Outlook с сервером Exchange функция календаря становится доступной для многих пользователей и добавляет возможности, перечисленные в табл. 8.2.

Табл. 8.2. Функции Outlook с сервером Exchange

Функция	Описание
Коллективно используемые календари	Exchange обеспечивает коллективное использование календарей отдельных пользователей и групп пользователей. Exchange активизирует ограничения защиты списков контроля доступа (ACL)
Планирование совещаний	Outlook дает пользователям возможность планировать совещания и приглашать на них многочисленных участников. В паре с Exchange Outlook показывает свободное/рабочее время каждого участника, а также автоматический выбор времени, когда все участники совещаний (собраний) будут свободны
Учетные записи ресурсов	Обеспечивают планирование ресурсов (залы для совещаний, питание, проекторы или другое специальное оборудование)
Обработка автоматизированных запросов	Активизирует автоматизацию особых функций планирования, так, учетную запись ресурсов (например, зал для совещаний, который используется не очень часто) можно сконфигурировать на автоматический прием приглашений на участие в совещаниях от любого человека

В следующем разделе описываются открытые эквиваленты большинства из этих функций.

Понятие служб коллективного пользования и календаря на базе Linux

Несмотря на то, что в настоящее время не существует прямой открытой замены функциям поддержки календаря Exchange, имеются программные решения, соответствующие требованиям к средствам коллективного пользования и ведению календаря практически в любой области деятельности. Если эти решения не удовлетворяют каким-то требованиям, то можно рассмотреть возможность использования патентованных программ, даже несмотря на их стандартные недостатки.

В разделах ниже рассматриваются eGroupware и Horde — два наиболее широко используемых, проверенных открытых программных приложений коллективного пользования/планирования с полным набором возможностей. Здесь также вкратце упоминается пакет OPEN-XCHANGE, ставший открытым приложением за несколько недель до даты публикации этой книги (имеется в виду английский вариант. — *Примеч. науч. ред.*).

Понятие eGroupware

Существуют многочисленные примеры открытых программных средств коллективного пользования; самым популярным из них является eGroupware — программный набор на базе web, выполняющийся на архитектуре LAMP. eGroupware требует Apache, MySQL или PostgreSQL и PHP.

Набор функций eGroupware — практически полный, он включает в себя такие функции коллективного использования, как поддержка календаря, а также неколлективные функции (например, комиксы). Неполный список многих функций eGroupware приведен ниже:

- календарь с функциями составления индивидуальных и групповых планов, «аварийных» извещений и уведомлений;
- web-почта (требует сервера IMAP (протокол доступа к сообщениям в Интернет));
- адресная книга;
- система отслеживания и учета дефектов;
- портал Intranet (называется Site Mgr);
- управление проектами;
- управление закладками Интернет-сайтов;
- комиксы.

eGroupware — проверенное программное решение, в августе 2004 года вышла версия 1.0. Распространено оно очень широко; модульная структура обеспечивает

возможность легко удовлетворить требования заказчика. eGroupware отличается привлекательным интерфейсом, поддержкой многих языков и активной группы разработчиков.

Более подробная информация о eGroupware имеется на сайте www.egroupware.org. Рабочая демо-версия находится на сайте www.egroupware.org/demo.

Понятие Horde

Среда Horde Application Framework — это структура коллективного пользования на базе web, выполняющаяся на архитектуре LAMP. Horde требует Apache, MySQL или PostgreSQL, а также PHP / PEAR (PHP Extension and Application Repository). Среда Horde обеспечивает стандартные средства для межпроцессных коммуникаций, учета пользовательских предпочтений, выявления версий браузеров, контроль доступа, пользовательскую справку и т. д.

Существует определенное количество приложений коллективного пользования и созданных по типу коллективного пользования, в которых применяется среда Horde. В табл. 8.3 перечислены некоторые приложения проекта Horde вместе с краткими описаниями.

Табл. 8.3. Приложения проекта Horde

Приложение Horde	Описание
IMP	Доступ web-почты к почтовым ящикам IMAP или POP3 (почтовый протокол, версия 3)
MIMP	Мини-версия IMP для мобильных телефонов/PDA («карманный» компьютер)
Ingo	Диспетчер фильтров электронной почты для procmail/Sieve
Forwards	Конфигурирование переадресации электронной почты
Vacation	Автоответчик электронной почты для уведомлений о временном отсутствии
Turba	Управление адресной книгой / контактами
Kronolith	Просмотр календаря
Hermes	Система отслеживания по времени
Whups	Отслеживание и учет дефектов (Web Horde User Problem Solver)
Rakim	Web-чат
Nag	Диспетчер списка задач
Team	Диспетчер закладок
Chora	Web-доступ к репозитариям CVS
Gollem	Диспетчер файлов на базе web

Эти приложения обеспечивают значительную функциональность в рамках единой среды. Несмотря на то, что в организациях абсолютно необходимо наличие не всех этих приложений, многие из них легко устанавливаются/интегрируются с другими компонентами структуры.

Более подробная информация о среде Horde и приложений проекта Horde (Horde Project) имеется на сайте www.horde.org. Демо-версия популярных приложений Horde Project находится на сайте www.horde.org/demo/.

Конфигурирование и реализация

Создание программных решений коллективного пользования по требованиям заказчика

Большинство открытых программных решений коллективного пользования и поддержки календаря (включая Horde и eGroupware) состоят из каркаса приложений и раздельных модулей, реализующих функции системы коллективного пользования. Преимущество данного подхода заключается в том, что модули достаточно легко компоновать, модифицировать, устанавливать и удалять. Это значительно упрощает процесс настройки решения коллективного пользования непосредственно под требования организации.

Обзор OPEN-XCHANGE (OX)

К сожалению, из-за того, что перед датой официальной публикации данной книги система OPEN-XCHANGE была поставлена в условия открытого лицензирования, у авторов книги просто не хватило времени на изучение и тестирование новой открытой версии этого сервера коллективного пользования. Поэтому полный анализ данного продукта в книгу не включен, и авторы предлагают всего лишь краткий обзор OX.

OX — это открытая версия коммерческого сервера Openexchange от Suse. OX поддерживает множественные языки и предоставляет следующие функции:

- web-портал;
- службы поддержки календаря;
- управление контактами;
- управление задачами;
- управление проектами;
- управление закладками;
- web-форумы;
- web-почта.

В соответствии с документацией, OX работает с любым браузером, клиентом iCal, электронной почты или WebDAV. Из-за того, что в OX используется Java и серверы Java, компилирование OX требует Java SDK (набор инструментальных средств разработки программного обеспечения, включающий библиотеки, заголовочные файлы, help-файлы, документацию и т. п.), компилятор Java Apache ANT и определенное количество общих библиотек Perl и Java.

Из-за сравнительной новизны этого открытого продукта на данном этапе довольно сложно прогнозировать его коммерческую и производственную успешность. Если OX будет решением, достойным своего набора функций, тогда эта система сможет стать лучшим открытым продуктом-заменой Exchange. Openexchange — испытанный продукт, поэтому предполагается, что OPEN-XCHANGE также будет надежным.

Более подробная информация об OX имеется на сайте www.open-xchange.org.

Понятие программного пакета коллективного пользования TWiki

До сих пор в основном рассматривались программные решения поддержки функций календаря и планирования. Существуют и другие типы программных пакетов коллективного пользования, называемые *системами управления и распоряжения знаниями*. Коллективные средства такого типа обеспечивают совместное создание и администрирование содержимого, как правило, структурированным способом, учитывая определенный вид технологического процесса. Они также могут упростить создание, распространение и использование определенных знаний.

WikiWikiWebs (сокращенно Wiki) представляет собой популярный способ коллективного создания и поддержки программного содержания и знаний группой людей. Wiki — это сеть с возможностью записи, набор объединенных между собой web-страниц, изменяющихся и расширяющихся «органично». В большинстве случаев имеется возможность редактирования любой страницы (и это поощряется), даже если пользователь не является ее владельцем. В Wiki применяется простой синтаксис, намного проще, чем в HTML (язык гипертекстовой разметки), хотя некоторые реализации Wiki позволяют использовать теги HTML. Как правило, редактирование основано на тексте, но в некоторых реализациях используется редактирование по принципу WYSIWIG (что видно на экране, то и получится на печати).

Одной из самых известных Wiks является Wikipedia (www.wikipedia.org) — бесплатная энциклопедия, где тысячи пользователей, желающих внести свой вклад в развитие ресурса, работают свыше чем над миллионом статей на множестве разных языков. Любому пользователю Интернет (можно анонимно) предлагается отредактировать любую статью в Wikipedia либо написать свою. Очевидно, что о сколько-нибудь надежной защите и безопасности речи идти не может, поэтому все предприятие внешне выглядит как приглашение к решению потенциальных проблем. Изредка появляются «граффити», но удаляются они обычно за считанные минуты, потому

что содержимое просматривается многими. Такая «мягкая» защита основана на содержимом с поддержкой версионности, и экспертная оценка работает достаточно эффективно, даже на таком обширном уровне, как всемирная информационная сеть Интернет. Более подробная информация о том, почему система Wikis настолько эффективна, имеется на сайте http://c2.com/cgi/wiki?WhyWikiWorks.

Одной из самых полезных вариаций Wiki в корпорациях является система TWiki за авторством Питера Тоуни (Peter Thoeny). TWiki обладает большим уклоном в сторону делового взаимодействия, нежели другие разновидности Wiki, что особенно подходит типам представленных в книге компаний. Прежде всего, систему можно использовать, как и любую систему Wiki для поддержки содержимого в свободной неструктурированной форме. TWiki обладает большинством нужных в этой среде функций: аутентификацией, контролем доступа, полным контрольным отслеживанием, управлением документацией, интегрированной электронной почтой (и другими системами управления предприятием), а также подключаемыми модулями. Это позволяет рабочим группам осуществлять обслуживание содержимого структурированным способом. TWiki отличается поддержкой функций, необходимых при проведении деловых встреч:

- совместно используемый блокнот для ведения проектов: хранилище, планирование, встречи;
- инструмент взаимодействия подразделений предприятия: обработка документации, обзоры проектов, отслеживание вопросов и ответов;
- инструмент публикации Intranet: ИТ, HR, стандарты компании, стратегии и процедуры;
- система управления информационным содержимым с особым учетом свободного рабочего взаимодействия: охват требований;
- база знаний: пара «проблема/решение» с подключаемыми вставками;
- инструмент создания книг коллективного авторства: авторы, обзоры и редактирование глав книги. В частности, данная книга написана несколькими авторами с помощью Twiki;
- платформа для создания программных приложений на базе web: порталов новостей для сотрудников, систем инвентаризации, а также систем отслеживания информационных элементов.

Организации используют TWiki в разных целях; это подтверждают «истории успеха» таких компаний, как Disney, Motorola, SAP, Yahoo и др., приведенные на сайте www.twiki.org. Более подробная информация о Wikis и TWiki имеется на сайтах www.wikipedia.org/wiki/Wiki и Twiki.org.

Переход к службам коллективного пользования и календарю Linux

Теперь, когда службы коллективного пользования благополучно протестированы и развернуты, пользователи получают преимущества переноса информации с Exchange на новую систему коллективного пользования и поддержки календаря. В зависимости от возможностей импорта/экспорта программного решения коллективного пользования это может быть, а может и не быть целесообразным.

При небольшом количестве пользователей самым простым способом будет выполнение переноса вручную, особенно если службы поддержки календаря и коллективные программные средства используются не очень интенсивно. Несмотря на то, что такой простой в техническом отношении подход не является показательным для поведения сисадмина, иногда самое простое решение является и самым лучшим. Перенос многих средств коллективного пользования и поддержки календаря даже в компаниях со 100 или более сотрудниками можно легко выполнить с помощью ручного ввода данных, особенно если группа, использующая эти функции, небольшая.

Существует несколько стандартов, типов файлов и RFC (запросы на комментарии), описывающих некоторые из аспектов средств коллективного пользования, а именно, для служб контактов и календаря. В эти стандарты входят iCal/vCal (RFC 2445) и vCard (RFC 2426). iCal и vCal — это файловые представления календарных записей, а файл vCard — представление визитной карточки. Файлы iCal обычно используют расширение ics, а файлы vCal — .vcs. Файлы vCard имеют расширение .vcf.

Понятие Outport

Outport — одно из самых полезных программных приложений для переноса списков контактов, календаря и информации о заданиях из системы Outlook. Данными могут быть экспортированные форматы файлов Evolution или другие клиенты календаря/средств коллективного пользования. Слово *Outport* представляет собой производное из двух слов *Out*look E*xport*, что точно объясняет выполняемые этой программой задачи.

Система Outport очень простая, и пользоваться ею легко. В левой части окна представлено дерево каталогов Outlook с возможностью выбора папки. В правой части — осуществляется управление конфигурацией экспорта. На рис. 8.1 показано окно программы Outport, подготовленное для переноса почтового ящика.

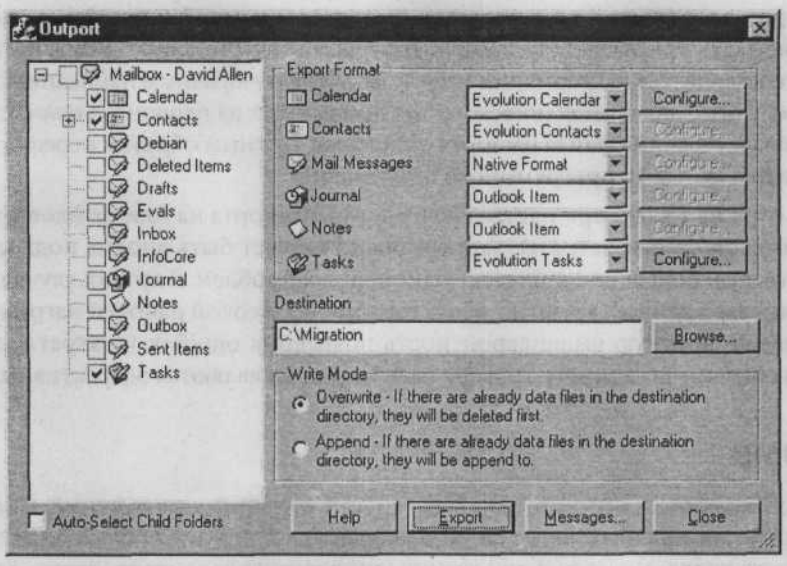

Рис. 8.1. Экспорт данных с помощью системы Outport

При показанной конфигурации будет осуществляться перенос списка контактных лиц, календаря и задач для почтового ящика Дэвида Аллена в формат, распознаваемый Evolution. Файлы копируются в каталог, в котором сохраняются данные Evolution, и перенос завершается.

Другие способы переноса информации

При выполнении переноса из клиента электронной почты/PIM (личная информационная система), отличного от Outlook, Outport работать не будет. Но при этом не все потеряно, потому что существуют еще несколько возможностей выбора, если нет желания выполнять перенос вводом данных вручную.

Одним из самых эффективных подходов к переносу служб ежедневника, контактов и других данных коллективного пользования является использование промежуточного формата файлов, распознаваемого приложениями как Windows, так и Linux. Для службы ежедневника (календаря) использование файлового формата iCal/vCal (.ics/ .vcs) работает практически со всеми клиентами ежедневника. Большинство клиентов, управляющих контактной информацией, могут использовать файлы в формате vCard (.vcf).

Для объектов, не имеющих стандартного типа файла для обмена информацией, часто допускается использование представления в виде текстового файла для переноса данных из одного программного приложения в другое. Если приложение его поддерживает, то данные можно вывести в файл .csv (значения с разделяющими запятыми) либо в файл с расширением .txt, разделенный символом табуляции. Этот тип

файла предварительно форматируется по строкам и столбцам, и его можно легко импортировать в структуру, подобную базе данных. При необходимости переноса большого количества информации может быть целесообразным написание сценария Perl (или Python) для синтаксического анализа данных из первоначального экспортного файла и создания файла импорта с данными, нужным образом переформатированными для целевого программного приложения.

Несмотря на то, что при настройке импорта/экспорта на базе файлов требуются авансовые временные затраты, данный подход может быть вполне подходящим, в частности, при большом количестве однородных проблем. В других случаях можно применять ввод данных вручную, особенно при невысокой рабочей нагрузке. Однако при вводе вручную выше вероятность появления ошибок и затраты рабочего времени системного администратора на эти цели не являются эффективными.

Резюме

Для Linux существует огромное множество программных приложений; в основном все они работают на платформе LAMP. Эти решения дублируют большую часть функций средств коллективного пользования и поддержки календаря «дуэта» Exchange-Outlook, хотя и не всегда в той же интегрированной манере, как это происходит в Exchange.

eGroupware и Horde — два очень популярных набора средств коллективного пользования; оба представляют большое разнообразие функций и возможностей, и каждый имеет свои преимущества и слабые места. OPEN-XCHANGE — открытая версия Openexchange, была передана в открытое лицензирование незадолго до даты публикации данной книги. Система OPEN-XCHANGE выглядит многообещающе, но не рассматривается подробно.

При переходе с Outlook / Exchange к открытым серверам передачи сообщений и таким клиентам, как Evolution, для упрощения процесса перехода можно использовать пакет Outport (http://outport.sourceforge.net). Outport поддерживает много типов форматов файлов, и с его помощью данные можно экспортировать практически в любой почтовый клиент / PIM.

Другой способ перехода заключается в ручном вводе данных в новую систему ежедневника / коллективного пользования. Это способ обладает тем преимуществом, что он является потенциальным выбором «на все случаи жизни», но он действен только при невысокой рабочей нагрузке. Кроме этого, при применении этого способа велика вероятность ошибок при наборе и неэффективно используется рабочее время сисадмина.

По завершении переноса средств коллективного пользования и поддержки календаря из системы организации можно устранить ее зависимость от Exchange, и от данной рабочей среды (Exchange) можно отказаться.

Краткое резюме по разделам

Понятие служб Exchange, служб коллективного пользования Outlook и календаря

- ☑ Outlook предоставляет определенное количество функций коллективного пользования, включая поддержку календаря, списка контактов, списков заданий и журнал.
- ☑ В паре с сервером Exchange Outlook предоставляет коллективно используемые ежедневники, функции планирования встреч, отчеты о ресурсах и автоматическую обработку запросов.
- ☑ Большинство функций Outlook / Exchange обеспечивается открытыми программными средствами.

Понятие служб коллективного пользования и календаря на базе Linux

- ☑ eGroupware — это программное решение коллективного пользования и поддержки календаря, написанное на PHP. eGroupware выполняется на архитектуре LAMP и интегрируется с OpenLDAP. Более подробная информация имеется на сайте www.egroupware.org.
- ☑ Horde — структура средств коллективного пользования PHP/PEAR. Horde Project содержит несколько программных приложений, предоставляющих функции коллективного пользования и им подобные. Более подробная информация имеется на сайте www.horde.org.
- ☑ OPEN-XCHANGE (OX) — открытое производное сервера Openexchange Suse. Подробности см. на сайте www.open-xchange.org.
- ☑ TWiki — система рабочего взаимодействия Wiki, которую можно применять для управления знаниями и содержимым. Подробная информация о TWiki имеется на сайте www.twiki.org.

Переход к службам коллективного пользования и календарю Linux

- ☑ При использовании Outlook лучшим способом переноса календаря, контактов, журнала, заданий и информации памяток является использование пакета Outport (http://outport.sf.net).
- ☑ При использовании клиента PIM, отличного от Outlook для переноса информации календаря и контактных данных можно применять файлы с расширениями .ics, .vcs и .vcf, если исходное и целевое программное приложение поддерживает эти форматы. В других случаях можно использовать текстовые файлы или ввод данных вручную.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма «**Ask the Author**»). Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: Я не могу найти открытое программное приложение, предоставляющее именно ту функцию коллективного пользования, которая мне нужна. Что следует делать?

О: В некоторых случаях нужные функции можно найти в патентованных решениях (например, Bynari или Skalix).

В: Я хочу запустить сервер коллективного пользования, который бы гладко интегрировался с Outlook. Что следует делать?

О: Рассмотрите возможность использования коллективного решения, имеющего подключаемый модуль для Outlook и/или Evolution.

В: Где можно получить информацию о настройке архитектуры LAMP?

О: Пошаговые инструкции содержатся в материале «Организация сервера LAMP» (www.brtnet.org/linux/lamp.htm).

Глава 9

Web-службы. Сравнительный анализ Информационного сервера Интернет и Apache

Разделы:

- Предыстория: Протокол передачи гипертекстовых документов
- Информационный сервер Интернет
- Web-сервер Apache
- Перенос статичных сайтов с IIS на Apache

☑ Резюме

☑ Краткое резюме по разделам

☑ Часто задаваемые вопросы

Введение

С самого начала развития всемирной сети Интернет ни один протокол не получил такого широкого распространения, как Протокол передачи гипертекстовых документов (HTTP). В августе 1991 года Тим Бернерс-Ли (Tim Berners-Lee) представил первый web-сервер, обслуживающий файлы Европейской лаборатории физики элементарных частиц (The European Laboratory for Particle Physics, CERN). Спустя год в активном режиме уже функционировали 50 web-серверов. К 1999 году в мире насчитывалось уже 720 000 web-северов общего пользования. В августе 2004 года, по данным самого последнего исследования Netcraft, запросы получали уже более 54 миллионов web-серверов и ежемесячно эта цифра увеличивается на 1 миллион. Почти на 70% из них работает Apache. Простота языка HTML, объединенная с простотой администрирования сервера HTTP, позволяет разместить информацию для открытого доступа во всемирной сети (World Wide Web, WWW); возможно, что наступит день, когда такой сервер будет работать у каждого пользователя.

Люди разворачивают web-серверы в разных ситуациях и по многим причинам. Многие корпорации, независимые консультанты, а также конечные пользователи, самостоятельно занимающиеся сборкой компьютеров, имеют возможность заниматься весьма доходным бизнесом, при условии наличия технического ноу-хау. Плоды их труда можно обнаружить на больших установочных серверах, на небольших сетевых программно-аппаратных средствах и даже в таких невероятных местах, как насосы для очистки нефтезаводских ловушек. В то время как одни компании вкладывают миллионы долларов в разработку своих сетевых программных приложений, а другие просто обновляют существующие системы для работы с web-службами, не удивительно, что идея получения в собственное распоряжение web-сервера является неотъемлемой частью бизнес-плана любой компании, претендующей на звание технологически передовой. Затраты на развертывание и обслуживание web-сервера сравнительно невысоки по сравнению с другими средствами рекламы: объявлениями в газетах, журналах, брошюрах или местных справочниках «Желтые страницы»; люди могут легко опубликовать информацию о бизнесе и продукции своих компаний без особых предварительных знаний о web-службах всего лишь за часть затрат на рекламу в печатных СМИ. Действительно, любая компания, намеренная связать свой бизнес со всемирной сетью, осознает потенциальную выгоду подобного предприятия. С точки зрения деловой активности такой подход может представлять собой дальновидное и перспективное вложение капитала.

Для технологически «подкованных», «ушлых» и инициативных личностей web-сервер с устойчивой операционной системой (ОС) представляют собой кладезь потенциальных возможностей. Языки серверных сценариев, программы-оболочки и стандартные утилиты на базе UNIX могут превратить web-сервер в станцию прогнозирования погоды, корпоративную доску объявлений либо службу знакомств.

Данная глава посвящена процессу переноса web-служб с Информационного сервера Интернет (Internet Information Server, IIS) на web-сервер Apache; здесь также дается обзор web-служб Linux. В ориентированных на серверы дистрибутивах Linux с Apache объединено великое множество различных утилит; авторы предполагают осознание читателем многочисленных выгод перехода от Windows к Linux: свободный доступ к операционной системе, сопутствующим службам, неограниченное количество документации по любой теме, практические способы решения проблем и ответы на наиболее часто задаваемые вопросы, широкое пользовательское признание — все это лишь малая часть преимуществ. После ознакомления с материалами главы читателям станет понятно, что научиться администрировать свой собственный web-сервер может практически любой пользователь.

Авторы не планируют вдаваться в подробности программирования службы web-хостинга, однако вкратце обозначат направления, в которые можно направить процесс дальнейших исследований. Основной упор в главе сделан на администрирование и хостинг статичного содержимого в качестве толчка администратору к скорейшему развертыванию Apache. Без сомнения, многие читатели попросту пропустили это введение, поэтому не будем задерживаться и пойдем дальше, но для начала — еще немного истории.

Предыстория: Протокол передачи гипертекстовых документов

Еще в 1989 году Бернерс-Ли составил предложение для CERN (Европейская организация по ядерным исследованиям) по управлению ее информационными ресурсами. Данное предложение объединяло в себе более ранние идеи Gopher (*распределенная запросно-поисковая система, обеспечивающая доступ к иерархическим информационным хранилищам в сети Internet через сервер Gopher посредством простого протокола*) о дереве связанных объектов с возможностью навигации по нему, идею Теда Нельсона (Ted Nelson) о «гипертексте» из его работы с Xanadu, а также включало три новых важных составных части: протокол передачи документов по соединениям TCP/IP (Протокол управления передачей/протокол Internet), язык разметки под названием HTML (Язык разметки гипертекстовых файлов) и клиентские программные средства для просмотра содержимого, написанного на HTML. Ставилась цель исключения избыточной информации из CERN путем «гиперсвязывания» с другими необходимыми документами, во избежание повторения информации.

Материал с круговыми перекрестными ссылками образовал нелинейный путь исследований. Исследователь мог перемещаться с помощью гиперссылок с одного текста на другой, пока не возвращался в то место, с которого все началось. Данная функция позволяла членам CERN сделать вывод о том, что представляемая ими информация уже не была сохранена в каком-либо архиве ранее.

Вскоре после этих событий, в 1993 году Марк Андрисон (Marc Andreeson) возглавлял рабочую группу, занимающуюся проектом для Национального центра по использованию суперкомпьютеров (National Center for Supercomputing Applications, NCSA), создавшую первый графический WWW-браузер, названный Mosaic. Затем эта рабочая группа создала свой собственный web-сервер — демон NCSA HTTP (httpd). Позже Андрисон ушел из компании и в 1994 году вместе с Джимом Кларком (Jim Clark) основал Netscape Communications Corporation.

Идея навигации через сотни документов простым нажатием кнопки мыши оказалась очень привлекательной и быстро укоренилась. Система Netscape вышла со своим собственным сервером — Netscape Communication Server, и так появилось новое рыночное направление.

Корпорация Microsoft, разумеется, не могла проигнорировать зарождающуюся технологию, теперь известную как Web, и разработала свой собственный web-браузер под названием Internet Explorer. Поскольку HTTP — стандарт открытый, и авторские права на этот протокол не принадлежали никому, Microsoft приступила к созданию собственной версии web-сервера под названием IIS.

Информационный сервер Интернет

Информационный сервер Интернет корпорации Microsoft (Microsoft Internet Information Service, IIS) объединяет в себе несколько служб Интернет в один пакет. Вместе с web-сервером IIS также включает в себя исходящую почту или сервер SMTP (Simple Mail Transfer Protocol, простой протокол электронной почты), а также файловый сервер (FTP — протокол передачи файлов). В данном разделе представлен обзор и некоторая терминология запуска web-служб с IIS 5.0. с использованием Windows 2000 Server. Описываются виртуальные каталоги, защита и аутентификация, а также настраиваются статичные web-страницы с IIS до начала процесса переноса сайтов на Apache и Linux. Перед началом следует знать, что Информационный сервер Интернет доступен во всех продуктах NT, 2000, 2003 и XP корпорации Microsoft, однако в несерверных разновидностях этих операционных систем некоторые функции отключены. В частности, в не-серверных версиях Windows возможность создания множественных web-сайтов и метод аутентификации Digest Authentication отключены. Поддержка SSL (Secure Sockets Layer, протокол защищенных сокетов) доступна во всех версиях, но ее нельзя сконфигурировать без предварительного приобретения подписи для запроса сертификата от Бюро сертификации (Certificate Authority, CA) (см. раздел по созданию самостоятельно подписанных сертификатов для их использования с Apache).

Перед началом работы

Администрирование web-сервера IIS осуществляется через диалоговое окно **Internet Information Services** (Информационные службы Интернет). Для доступа к этому

диалоговому окну щелкните мышью по пунктам **Control Panel** (Панель управления) / **Administrative Tasks** (Задачи администрирования) / **Internet Service Manager** (Диспетчер служб Интернет). Это позволит сконфигурировать серверы FTP, Web, SMTP, как показано на рис. 9.1. После установки через функцию **Add/Remove Programs** (Установка/удаление программ) IIS находится в рабочем состоянии и ожидает запросы к порту 80. При условии отсутствия брандмауэра, блокирующего порт 80, в наличии должна быть возможность запуска web-браузера и просмотра страницы «Добро пожаловать в службы Интернет 2000» по адресу http://localhost. При просмотре этой страницы с локального компьютера будет выдан запрос регистрационного имени Windows. Введите учетную запись пользователя, пароль и браузер будут перенаправлены на страницу «Перед началом работы». При просмотре с другого компьютера эта страница просто выдаст сообщение о том, что находится в процессе создания (Under Construction).

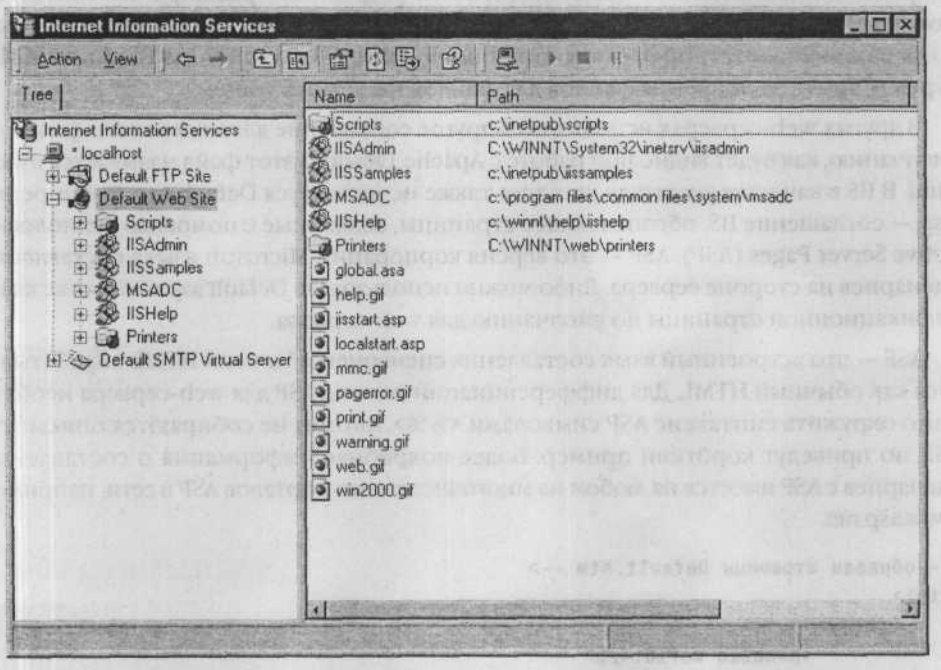

Рис. 9.1. Диалоговое окно информационных служб Интернет

Создание индексной страницы по умолчанию

Чтобы показать пользователям что-нибудь более интересное, чем страница «Under Construction», следует просто создать файл HTML с именем Default.htm и переместить его в домашний каталог web-сервера (c:\Inetpub\www-root). Для создания файла Default.htm можно воспользоваться любым текстовым редактором или редактором

WYSIWYG (что отображается на экране, то и получается на печати). После сохранения файла Default.htm скопируйте домашний каталог web-сервера и перезагрузите web-браузер:

```
<!-образец страницы Default.htm -->
<html>
     <body>
          <p>Hello world.</p>
</body>
</html>
 [warning]
```

Убедитесь, что файл имеет имя Default.htm, а не Default.htm.txt из-за используемого текстового редактора. Активизация показа расширений файлов в настройках операционной системы поможет защититься от двойного расширения. Войдите в **Control Panel / Folder Options** (Опции папки) / **View Tab** (Просмотреть закладку) и для изменения настройки отключите опцию **Hide file extensions for known file types** (Скрыть расширения файлов для файлов известных типов).

В других web-серверах используется другое соглашение для индексного файла по умолчанию, как будет видно при работе с Apache. Обычно этот файл называется index.html. В IIS в качестве указателя каталога также используется Default.asp. Расширение .asp — соглашение IIS, обозначающее страницы, созданные с помощью технологии Active Server Pages (ASP). ASP — это версия корпорации Microsoft языка составления сценариев на стороне сервера. Либо можно использовать Default.asp в качестве классификационной страницы по умолчанию для web-сервера.

ASP — это встроенный язык составления сценариев; обычный HTML обрабатывается как обычный HTML. Для дифференциации команд ASP для web-сервера необходимо окружить синтаксис ASP символами <% %>. Авторы не собираются описывать ASP, но приведут короткий пример. Более подробная информация о составлении сценариев с ASP имеется на любом из многочисленных порталов ASP в сети, например www.asp.net.

```
<!--образец страницы Default.htm -->
<html>
     <body>
          <p>Hello world.</p>
          <p> Время: <%response.write(time())%> </p>
</body>
</html>
```

Теперь скопируйте Default.asp в c:\Inetpub\wwwroot и удалите Default.htm. На рис. 9.2 иллюстрируется этот процесс в web-браузере.

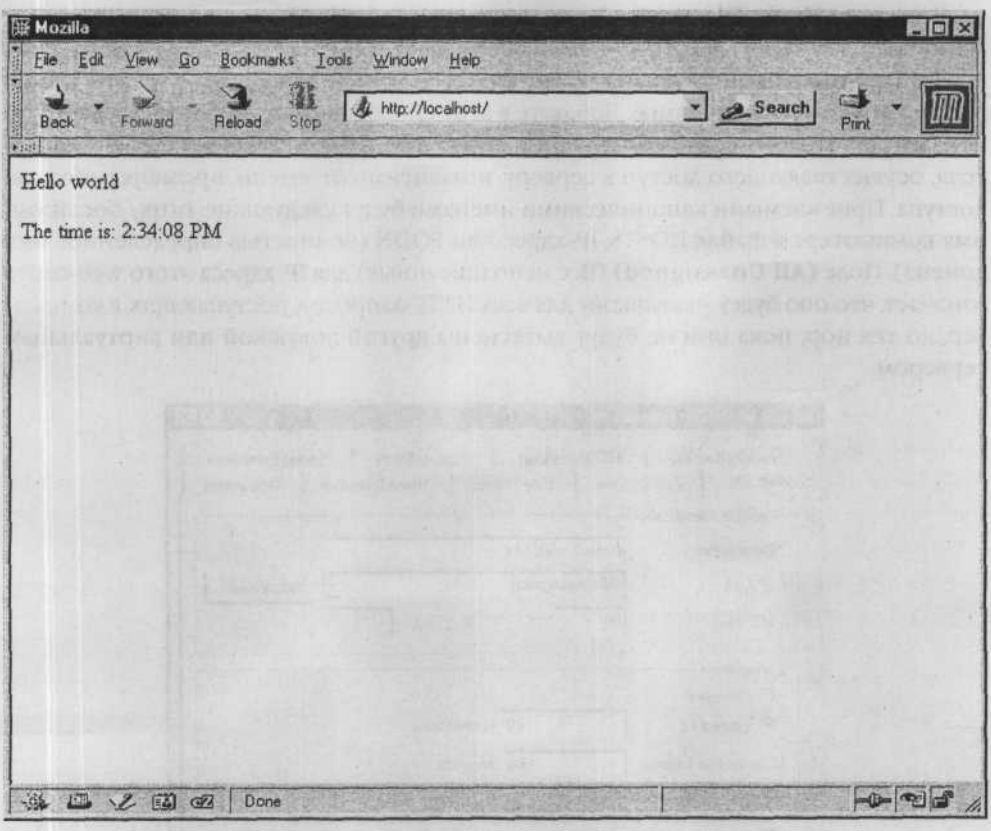

Рис. 9.2. Страница Default.asp, просматриваемая в web-браузере

Создание Web-сайта по умолчанию

При возвращении в диалоговое окно Информационных служб Интернет и нажатии кнопки мыши на **Default Web Site** (Web-сайт по умолчанию) в левой части будет видно, что теперь страница Default.asp появляется в списке справа. При щелчке правой кнопкой мыши в правой части или нажатии правой кнопкой мыши на ветви **Default Web Site** в левой части можно получить доступ к **Properties** (Свойства) web-сервера по умолчанию (см. рис. 9.3). Данное диалоговое окно зависит от контекста, оно разное для каждого виртуального каталога и виртуального сервера. Это окно позволяет определить домашний каталог, индексную страницу (страницы) по умолчанию, а также настройки защиты каталогов и разрешения. Обратите внимание на эти свойства и сделайте нужные доступными.

В закладке **Home Directory** (Домашний каталог) будет показан домашний каталог (c:\Inetpub\wwwroot), в который были скопированы страницы по умолчанию. В закладке **Documents** (Документы) можно указать документ, который будет отображен в этом каталоге по умолчанию. Добавьте в этот список index.html. Закладка **Web Site** показывает, что web-сайт по умолчанию будет отображаться для всякого пользователя, осуществляющего доступ к серверу, независимо от имени, применяемого для доступа. Приемлемыми каноническими именами будут следующие: http://localhost, имя компьютера в файле HOSTS, IP-адрес или FQDN (полностью определенное имя домена). Поле **(All Unassigned)** (Все неподписанные) для IP-адреса этого web-сайта означает, что оно будет «ловушкой» для всех HTTP-запросов, поступающих в компьютер, до тех пор, пока они не будут вытеснены другой ловушкой или виртуальным сервером.

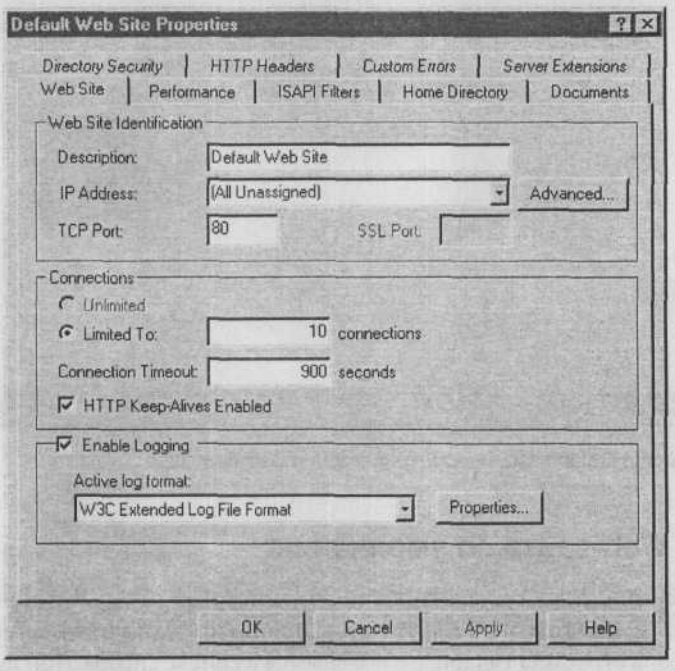

Рис. 9.3. Свойства web-сайта по умолчанию

Виртуальные каталоги

Виртуальные каталоги в IIS представляют собой реальные, но особые каталоги файловой системы. В Apache они называются *псевдонимами*. Используются эти каталоги для отображения части URL (Uniform Resource Locator, унифицированный указатель информационного ресурса) каталога в специальный каталог в файловой системе сервера, за пределами домашнего каталога web-сервера. Последний знает, где искать

файлы, относящиеся к конкретному виртуальному каталогу, — в конце запрошенного URL (минус имя файла). Если представленный каталог не является подкаталогом c:\Inetpub\wwwroot, тогда web-сервер будет осуществлять проверку на предмет соответствия одному из отображений виртуального каталога. Если соответствие обнаруживается, то в этом каталоге осуществляется поиск файла.

Виртуальные каталоги полезны для выделения информации из домашнего каталога web-сервера. Их также можно использовать, если каталог, предназначенный для коллективного пользования, находится в другой файловой системе или на другой машине. Выполните следующие шаги для создания виртуального каталога для хранения сценариев вне домашнего каталога web-сервера.

1. Создайте каталог c:\Inetpub\cgi-bin.
2. В диалоговом окне информационных служб Интернет щелкните правой кнопкой мыши строку **Default Web Site** (web-сайт по умолчанию) и выберите **New/Virtual Directory** (Новое/Виртуальный каталог).
3. Появится подсказка-«мастер», запрашивающая псевдоним для этого каталога (часть URL, отвечающая каталогу) и реальный каталог в файловой системе (только что созданный вручную). Также будет запрос на задание разрешений доступа. Единственным разрешением, которое может не иметь очевидного значения, является разрешение **Browse** (Просматривать). Если эту опцию активизировать, то web-сервер создаст листинг каталога, если в нем отсутствует индексная страница по умолчанию. В противном случае пользователю выдается страница с сообщением «Directory Listing Denied» («просмотр каталога запрещен»). Выберите разрешения **Read** (Читать), **Script** (Сценарий) и **Execute** (Выполнить), поскольку известно, что создается каталог сценариев не для просмотра другими пользователями. Теперь все настроено для использования сценариев Perl CGI (общие шлюзовые интерфейсы) или механизма Вставок на стороне сервера (SSI) за пределами домашнего каталога web-сайта: достаточно просто перенести все CGI в каталог c:\Inetpub\cgi-bin, и к ним можно будет осуществлять доступ через URL, например http://example.com/cgi-bin/Default.pl или http://example.com/cgi-bin/Default.cgi. Разумеется, эти имена файлов нужно будет добавить в список индексных файлов по умолчанию, если не используются абсолютные URL.

Защита

Защита в IIS конфигурируется для всего web-сервера, для виртуального сервера, для каталога или для файла. Для каждого из перечисленных элементов можно настроить *анонимный доступ, базовую аутентификацию, дайджест-аутентификацию* (или базовую аутентификацию с хэшированием) либо *аутентификацию на базе Windows*. Ни один из перечисленных видов аутентификации не защищен сам по себе, однако они защищаются при использовании их поверх SSL. Ниже приведены различия указанных видов аутентификации:

- **Анонимный доступ** — полный открытый доступ к ресурсу.
- **Базовая аутентификация** — стандартный метод аутентификации HTTP Internet, поддерживаемый многими web-браузерами. Он защищает ресурсы, основанные на *областях* (по серверу, по каталогу, по файлу и т. д.) При базовой аутентификации применяется процесс «отклик-отзыв» для определения корректности пользовательских мандатов доступа и, следовательно, доступности ресурса для данных пользователей. Однако базовая аутентификация обеспечивает весьма ограниченную защиту, поскольку пароли передаются по сети открытым текстом.
- Предполагается, что **Дайджестная аутентификация** вытеснит базовую, однако ее защита не намного надежнее. При использовании данного вида аутентификации сервер отправляет контрольную сумму клиенту, работающему с браузером. После этого браузер использует эту контрольную сумму и md5sum для вычисления хеша имени пользователя, пароля и URI (универсальный идентификатор ресурса) и отправляет их назад на сервер. Сервер может использовать эту информацию для обращения процесса и проверки действительности мандатов. Это очень упрощенный взгляд на процесс (более подробную информацию см. RFC 2616 и RFC 2617). Поскольку процесс — известный и обратимый, его защита считается немного надежнее защиты базовой аутентификации. Дайджестная аутентификация — это стандарт Интернет, поддерживаемый большинством web-браузеров.
- **Аутентификация на базе Windows** очень похожа на дайджестную аутентификацию, но представляет собой стандарт Windows и поддерживается в основном в Internet Explorer. Некоторые последние версии Netscape и Mozilla также поддерживают аутентификацию на базе Windows.

Вообще говоря, перечисленные методы аутентификации следует использовать только во внутренних сетях, поскольку они не обеспечивают надежной защиты. Эти способы аутентификации никогда не следует применять в ненадежных сетях без шифрования с помощью SSL.

Для настройки базовой аутентификации web-сервера по умолчанию:

1. Войдите в диалоговое окно Информационных служб Internet.
2. Щелкните правой кнопкой мыши строку **Default Web Server** (Web-сервер по умолчанию).
3. Выберите **Properties** (Свойства) и закладку **Directory Security** (Защита каталога).
4. В режиме **Anonymous access and authentication control** (Анонимный доступ и контроль аутентификации) нажмите **Edit** (Редактировать).
5. Отмените выбор **Anonymous access** (Анонимный доступ) и активизируйте **Basic authentication**.
6. Выберите **Edit** и введите имя домена или имя машины для сервера.

7. Перезапустите web-сервер и перезагрузите web-браузер. Появится запрос о вводе имени пользователя и пароля. Имя пользователя и пароль соответствуют непосредственно фактическому пользователю системы и конфигурируются через **Control Panel / Users and Passwords**.

Для активизации дайджестной аутентификации просто активизируйте одноименную опцию. Других настроек не требуется.

Активизация аутентификации Windows практически идентична двум вышеописанным методам. При этом используется *криптографический обмен* с браузером Internet Explorer, и такой вид аутентификации стоит рассматривать только при работе с изученной, однородной сетью компьютеров Windows либо со сравнительно новыми браузерами, поддерживающими данный способ аутентификации. Для активизации аутентификации Windows просто активизируйте опцию. Пользователи конфигурируются в **Control Panel** в **Users and Passwords**.

Одним из значительных ограничений перечисленных способов аутентификации является то, что здесь не существует разделения между пользователем системы и пользователем HTTP; применение любого из указанных способов аутентификации для тысяч пользователей web-портала попросту будет трудно контролировать. Указанные способы аутентификации должны работать быстро и просто. Используйте их в проверенных или домашних сетях. Для создания более совершенных и устойчивых способов аутентификации обратитесь к любой методологии на базе сценариев (PERL, PHP, ASP), осуществляющей доступ к базе данных для получения информации о пользователе. Эти способы имеют высокую степень расширяемости и легко объединяются с SSL.

SSL/TLS

Протокол защищенных сокетов (SSL) и *Безопасность транспортного уровня* (TLS) — это стандарты Интернет для зашифрованных подключений HTTP (или HTTPS). Несмотря на то, что это два разных способа кодирования по HTTP, они применяются совместно, и большинство пользователей просто называют закодированный HTTP как «SSL». Корпорация Netscape Communications разработала первый Протокол защищенных сокетов в 1996 году, а IETF дополнила его протоколом TLS. Более подробную информацию о TLS см. на web-сайте Проблемной группы проектирования Интернет — www.ietf.org (особенно RFC 2817 и RFC 2818), а подробности о SSL — Проект Интернет «Протокол SSL» — http://www.netscape.com/eng/ssl3/draft302.txt.

Поддержка SSL не-серверными разновидностями IIS сконфигурировать нельзя, не имея подписи от Бюро подписки сертификатов (Certificate Signing Authority, CSA). Впрочем, с помощью IIS можно создавать запросы на подпись сертификатов (CSR). При необходимости работы с IIS вместе с SSL этот CSR можно создать в подсказке-«мастере» (щелчок правой кнопкой мыши на **Default Web Browser** (Web-браузер по умолчанию), выбор **Properties** (Свойства), закладка **Directory Security** (Защита каталога), **Server Certificates** (Сертификаты сервера)). Затем скопируйте полученный

текстовый файл в web-форму на сайте выбранного бюро сертификации. Оно также предоставит вам дополнительную информацию о подключении поддержки SSL в IIS после приобретения подписанного сертификата.

При использовании серверного варианта Windows для получения сертификатов Бюро сертификации можно воспользоваться сервером сертификатов, создать новые запросы на подписку сертификата либо просмотреть уже имеющиеся. Это — рекомендуемый способ работы с сертификатами сервера IIS, однако IIS не поддерживает самостоятельно подписываемые сертификаты для тестирования SSL-подключений на сервере. Для доступа к серверу сертификатов выберите в Панели управления программу **Add/Remove Programs** (Установка и удаление программ), нажмите строку **Add/Remove Windows Components** (Установка и удаление компонентов Windows) и убедитесь в том, что на компьютере установлена служба сертификатов — **Certificate Services**. Затем откройте браузер и войдите на сайт http://localhost/certsrv. Появится управляемая ASP web-подсказка-«мастер», в которой осуществляется обработка запросов на сертификацию (см. рис. 9.4).

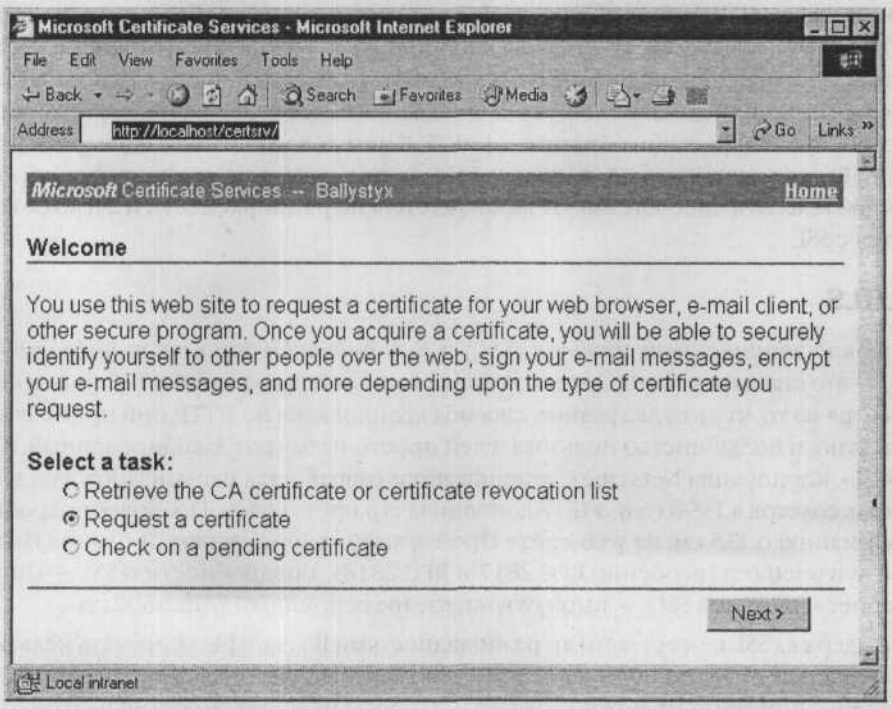

Рис. 9.4. Окно входа в службы сертификации Microsoft

Виртуальные серверы

Если после выполнения указанных операций по установке web-служб на NT Workstation, 2000 Professional, XP или XP Pro необходимо создать другой web-сайт (или виртуальный сервер), то — извините, — это невозможно, да, в общем, и не нужно. В указанных продуктах возможность создания второго сайта отключена и имеется только в версии Windows NT/2000/2003.

При работе с серверным вариантом операционной системы Windows новые сайты создаются посредством другой подсказки-«мастера» в диалоговом окне **Internet Information Services**. Однако перед добавлением нового сайта следует определиться, с настройкой какого виртуального сервера придется иметь дело: на базе имени или IP. Настройка на базе имени означает, что несколько доменов будут указывать на один IP-адрес; при настройке на базе IP несколько IP-адресов указывают на один компьютер. Виртуальные серверы на базе имени не требуют особого рассмотрения, а на базе IP потребуется сконфигурировать сетевой интерфейс (интерфейсы) для каждого IP, контролируемого компьютером. Чтобы настроить конфигурацию интерфейсов для нескольких IP-адресов, войдите в **TCP/IP Properties** для интерфейса (интерфейсов) компьютера и нажмите **Advanced** для добавления большего количества IP. Далее предполагается, что от ISP (провайдер услуг Интернет) получен хотя бы один общедоступный IP-адрес, уже сконфигурирован DNS (служба разрешения имен доменов) либо отредактирован файл HOSTS для указания на этот IP для каждого домена, который предполагается обслуживать.

Конфигурирование IIS для распознания домена и переадресации запросов в надлежащий каталог выполняется в диалоговом окне **Internet Information Services**. Щелкните правой кнопкой мыши ветвь главного сервера и выберите **New / Web Site** (Новое / Web-сайт). Появится программа-«мастер» с запросом о вводе имени (**Name**) сайта, которым может быть любое идентификационное имя (просто для организационного использования в IIS), IP-адреса компьютера, номер порта, с которого будет работать виртуальный сервер, и имя Заголовка хоста (Host Header name), представляющее собой имя обслуживаемого домена. В рассматриваемой системе созданы два домена — internal.ballystyx.com и www.ballystyx.com, и задано одно и то же имя для полей **Name** и **Host Header**. После этого домен был связан с каталогом файловой системы. Подобно виртуальным каталогам, данный каталог (см. рис. 9.5) может быть размещен в любом месте; для размещения каталогов домена в рассматриваемой системе создан каталог **c:\Inetpub\vhosts**.

Теперь создайте web-страницы и скопируйте созданные по умолчанию индексные файлы в каталоги нового виртуального сервера. После этого убедитесь, что ни один шаг не пропущен. В данном случае созданы две страницы: одна — для internal.ballystyx.com внутреннего пользования, а другая — для www.ballystyx.com открытого пользо-

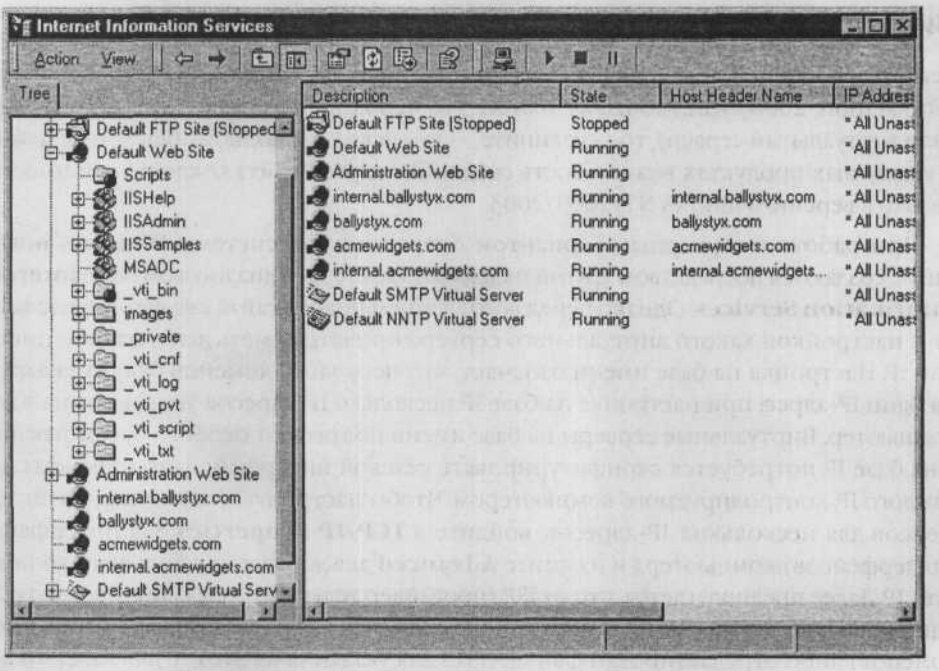

Рис. 9.5. Каталог Информационных систем Интернет

вания, после чего эти страницы скопированы в c:\Inetpub\vhosts\internal.ballystyx.com и в c:\Inetpub\vhosts\www.ballystyx.com, соответственно. На рис. 9.6 и 9.7 представлены эти страницы.

```
<! - - Пример Default.htm для internal.ballystyx.com - ->
<html> <head> <title> - - - - - Ballystyx Internal - - - - -</title> </head>
<body bgcolor= #FFFFFF>
<center>
      <img src=Ballystyx_rocket.gif border=0 alt=logo>
 <h1> Greetings Programs< /h1>
      <p>Здесь будут обнаружены ресурсы для упрощения работы. </p>
      <br>
      <br>
</center>
</body>
</html>
```

Рис. 9.6. Внутренние индексные файлы, созданные по умолчанию для internal.Ballystyx.com

```
<! - - Пример Default.htm для www.ballystyx.com - ->
<html> <head> <title> Ballystyx Global Semiconductor Engineering </title>
</head>
<body bgcolor= #FFFFFF>
<center>
      <img src=ballystyx_rocket.gif border=0 alt=logo>
 <h1> Добро пожаловать в Ballystyx Semiconductor Engineering < /h1>
      <p>Приглашаем посетить наш новый web-сайт. </p>
      <br>
      <br>
</center>
</body>
</html>
```

Рис. 9.7. Внутренние индексные файлы, созданные по умолчанию для www.ballystyx.com

ПРИМЕЧАНИЕ

- **Индексная страница** Страница по умолчанию, которую вызывает web-сервер, если URL не предоставляет абсолютной страницы.
- **Виртуальный сервер** Один из потенциально многих доменов, обслуживаемых на одном web-сервере.
- **Виртуальный сервер на базе имени** Несколько доменов, отвечающих по одному IP-адресу.
- **Виртуальный сервер на базе IP** Несколько IP-адресов, обращающихся к одному компьютеру.
- **Виртуальный каталог** Псевдоним URL. Отображает особый путь, необходимый в URL, к каталогу в файловой системе.
- **SSL/TLS** Стандарт Интернет для зашифрованного HTTP.

Web-сервер Apache

По сравнению с IIS процесс конфигурирования Apache намного прозрачнее. Его можно установить и запустить на Windows и UNIX/Linux, а также множестве других операционных систем, включая встроенные. Сервер поддерживает множественные виртуальные серверы, называемые в терминах Apache *виртуальными хостами*; в нем легко настраиваются такие важные опции конфигурации, как аутентификация и SSL. Конфигурация традиционно выполняется через текстовые файлы. Однако здесь будут

упомянуты некоторые полезные инструментальные средства графического администрирования; как локальные, которые сисадмин получает в свое распоряжение вместе с дистрибутивом, так и web-инструменты администрирования (например, WebMin).

Сообщество пользователей Linux имеет свою историю так называемых «войн дистрибутивов». Поскольку исходный код доступен для тысяч программных приложений, лицензированных по GPL (Общественная Лицензия GNU), то за годы разработок появилась масса конкурирующих дистрибутивов. Не вдаваясь в подробности войн дистрибутивов, в качестве примера для данного раздела авторы выбрали Fedora Core (http://fedora.redhat.com).

Fedora Project — это открытый проект, спонсируемый RedHat и поддерживаемый сообществом. Он также служит испытательным полигоном новой технологии, которая в скором времени может быть представлена в продуктах Red Hat. Официально продукт Fedora не поддерживается компанией Red Hat, Inc. Несмотря на это, многие функции были предоставлены конечным пользователям, что дало им возможность *поучаствовать* в развитии дистрибутива. Проект Fedora во многом похож на проект Debian (http://debian.org); результаты разработок — общедоступны, однако сам дистрибутив основан на RedHat Package Manager (rpm), а не на пакетах Debian (dpkg).

Предыстория Apache

Apache Web Server — наиболее распространенный сервер во Всемирной сети, который еще очень долго не сойдет с коммерческой сцены. По последним статистическим данным NetCraft, Apache применяется почти на 70% всех web-серверов Интернет. IIS занимает второе место (немногим более 21%); оставшиеся 10% приходятся на долю серверов Sun, iPlanet и httpd. Для администраторов Apache текущая ситуация имеет особое значение. В паре с тем фактом, что в настоящее время Apache разрабатывается и обслуживается в качестве открытого продукта организацией Apache Software Foundation, он является проектом, поддерживаемым сообществом и представляющим общественный интерес, можно сказать, что это — прекрасный и реальный пример того, как открытое решение может превзойти патентованные модели разработок.

Система Apache выросла из продукта httpd NCSA в форме патчей к коду. В феврале 1995 года httpd NCSA был самым популярным web-сервером в Интернет, однако с уходом главного разработчика — Роба МакКула (Rob McCool) дальнейшая работа прекратилась. Небольшая группа разработчиков, включая Брайана Белендорфа (Brian Behlendorf) и Клиффа Скольника (Cliff Skolnik), собрали патчи к оригинальному коду httpd и в апреле 1995 года выпустили первую версию Apache версии 0.6.2. Название представляет собой игру слов: конечный продукт рассматривался как web-сервер, собранный «по кусочкам» (a-patch). С тех пор код полностью переписан, и в настоящее время имеются восемь основных разработчиков и группа содействующих авторов, которые образовали Apache Group, позже превратившуюся в Apache Software Foundation.

Установка

Установить Apache на системы Linux очень легко. Некоторые дистрибутивы содержат пакет. Если нет, проверьте наличие предварительно подготовленного пакета специально для имеющегося дистрибутива. В данном разделе описывается установка и конфигурирование самой последней (на момент написания книги) версии Apache — 2.0.

Для проверки того, установлен ли Apache в Debian, перейдите к командной строке, введите команду **dpkg -1 / grep apache**. В системах, подобных Fedora и RedHat, воспользуйтесь командой **rpm -qa / grep apache** или **rpm -qa / grep httpd** (в некоторых системах пакет имеет название «httpd», а не «apache»). В других системах попробуйте использовать команду locate apache, если на экране появляется большой список файлов, то можно быть уверенным, что пакет установлен. Дополнительную информацию по перечислению пакетов и определению установленных программ см. в документации к вашему пакету.

Если пакет Apache не установлен, определите нужный пакет для имеющегося дистрибутива и установите его. RPM-пакеты для RedHat находятся на http://rpmfind.net и http://freshrpms.net, а пакеты Debian доступны в хранилищах Debian, которые обычно заранее конфигурируются под операционную систему, и доступ к ним осуществляется через утилиты *apt*. При наличии в системе утилиты *apt-get* можно ввести команду **apt-get install apache** или **apt-get install httpd**, и apt-get загрузит и установит пакет. Также можно зайти на страницу загрузки Apache Server и скачать исходный код (http://httpd.apache.org/download.cgi). Компиляция Apache из исходного кода в данном разделе не рассматривается: в Интернет предостаточно материалов на эту тему. По возможности, всегда рекомендуется пользоваться готовыми пакетами. Если пакет для системы имеется, запустите пакетный менеджер для его установки. В системах Debian это выглядит примерно как **dpkg -i apache-2.0.x.dpk**, а в системах RedHat — **rpm -i httpd-2.0.x.rpm**. Фактическое название пакета будет варьироваться и, несмотря на то, что многие пакеты могут работать с разными дистрибутивами, рекомендуется подбирать пакет, специально подготовленный для вашей системы.

Запуск, остановка и проверка состояния

Запуск Apache осуществляется через сценарии инициализации стиля rc системы, расположенные в /etc/init.d. Для запуска Apache в командной строке от имени root введите команду: **/etc/init.d/httpd start** или **/etc/init.d/apache start**. Для остановки Apache введите **/etc/init.d/httpd stop** или **/etc/init.d/apache stop**. Название сценария — httpd или apache — зависит от дистрибутива. Данный сценарий также примет другие команды, например **status, reload, help** и **configtest**. Запустите сценарий сам по себе, без аргументов, для проверки того, какие команды поддерживаются.

Apache также имеет свой собственный сценарий администрирования — *apachectl*. Он принимает такие команды, как **start, stop, restart** и другие. Запустите сценарий /usr/sbin/apachectl самостоятельно либо обратитесь к странице руководства пользователя.

Конфигурация

Перечисление и описание каждой опции конфигурирования Apache (а их очень много) заняло бы слишком много времени и места, поэтому рассмотрим самые основные. Опишем компоненты основного файла конфигурации — *httpd.conf* — и принципы конфигурирования уже рассмотренных опций. Обсуждение также включит в себя другие файлы конфигурации и модули Apache вместе с возможностью добавления в пакет новых модулей. По ходу описания авторы обращают внимание читателя на определенные графические инструменты для упрощения задачи администрирования, упоминают другие опции конфигурации и их применение.

Конфигурирование сервера Apache выполняется через файл с именем httpd.conf, однако перед тем, как рассмотреть его подробно, обратим внимание на структуру каталогов, предполагаемую файлом. В зависимости от опций времени компиляции, этот файл можно расположить в разных местах. Чаще обычного он размещен в каталоге /etc/httpd/conf. Для достижения целей данного раздела предположим установку на базе RedHat, размещающую ServerRoot в /etc/httpd, а DocumentRoot — в /var/www; подробнее эти термины объяснены ниже. В системе Fedora Core 2 после установки пакета httpd каталог /etc/httpd содержит пять элементов. Из этих элементов два — каталоги конфигурации: conf и conf.d, а три — символические ссылки, указывающие на другие пути в файловой системе сервера: logs, modules и run.

Опишем эти каталоги: /conf содержит *httpd.conf* — основной файл конфигурации для Apache; *magic* — файл, помогающий Apache определить типы файлов; несколько каталогов /ssl.* для сертификатов, ключей и запросов и *Makefile*, который можно использовать для генерирования запросов на подпись сертификатов и самостоятельной подписи сертификатов для использования сервером. Каталог /conf.d содержит отдельные файлы конфигурации, которые можно разделить для логической организации, но которые с тем же успехом могут быть частью основного файла конфигурации. Файлы включаются в файл httpd.conf директивой *Include*. Модули и другие пакеты, требующие специальной опции конфигурации Apache, напишут свои собственные файлы конфигурации conf.d. Каталог /logs содержит регистрационные журналы сервера, /modules — это каталог модулей, а /run — символическая ссылка на каталог эквивалента /var/run вашего дистрибутива — места, где многие программы записывают идентификатор процесса (PID).

Как уже упоминалось, разные дистрибутивы Linux разместят эти каталоги в разных местах, и при установке из исходных текстов имеется возможность выбора места расположения этих каталогов вводом опции **-f** в строку **./configure**. Подробности см.

в документации, поставляемой вместе с исходными текстами. Обратите внимание, что если пакет Apache установлен из исходных текстов и место установки не указано явно, то пакет будет помещен в каталог /usr/local/apache.

Теперь, когда в общих чертах идея ясна, перейдем к синтаксису конфигурационного файла.

Файл httpd.conf имеет два основных раздела: Раздел *Main* (Главный) и раздел (разделы) *Virtual Host* (Виртуальный хост). Раздел Main — это все, что находится за пределами контейнера **<Virtual Host>**. С этого момента будем пользоваться этими терминами. Раздел Main поглощает любые разделы виртуального хоста методом вложения. Таким образом, при определенных условиях виртуальный хост может подменить опцию конфигурации Main, однако, если в рамках данного контейнера VirtualHost данной настройки нет, настройки этой опции будут настройками по умолчанию для раздела Main. Любой раздел может иметь любое количество *директив* и *контейнеров*, и последние могут быть вложены позже.

- На каждую строку может приходиться одна **директива**. Можно использовать символ обратной косой — «\» для переноса директивы на другую строку. Директивы имеют форму **Directive Argument1 Argument2 [...]**. Аргументы зависят от регистра набора, а сами директивы — нет.
- **Контейнеры** напоминают язык HTML тем, что здесь также имеются открывающий и закрывающий теги, определяющие начало и конец контейнера с аргументом контейнера, размещенным в открывающем теге. Они разделены на два разных типа: Filesystem (файловая система) и Webspace (web-пространство) (эти термины используются в документации к Apache для описания различий между наиболее распространенными типами контейнеров, которые будут обнаружены в файле конфигурации). Контейнеры *Filesystem*, такие как **<Directory>** и **<Files>**, функционируют в локальной файловой системе и управляют разрешениями и опциями каталогов, подкаталогов или конкретного файла. Если контейнер **<Files>** находится в разделе Main файла конфигурации, тогда эти разрешения будут применимы к любому файлу с таким именем, независимо от того, в каком каталоге он размещен. Однако, если вложить контейнер **<Files>** в контейнер **<Directory>**, эти разрешения будут применяться к любому файлу с таким именем, размещенном в этом каталоге и под ним. С другой стороны, контейнер *Webspace*, например **<Location>**, функционирует на запрошенном URL, присваивая разрешения или действия на основании пути в URL. При этом местоположение не обязательно должно представлять собой каталог в файловой системе.

  Другим типом контейнера является контейнер **<VirtualHost>**. Он используется для разграничения сервера Main (или web-страницы по умолчанию) и виртуальных хостов (или виртуальных серверов, как упоминалось в предыдущем разделе). Контейнер **<VirtualHost>** может содержать любое количество директив, контейнеров файлов и web-пространства, однако некоторые комбинации не имеют

логического смысла. Apache обладает очень хорошей системой предупреждения администратора о конфликтах директив. Для проверки синтаксиса конфигурации в apachectl можно ввести опцию **-t**.

ПРИМЕЧАНИЕ Многие контейнеры имеют эквиваленты, использующие регулярные выражения, например **<DirectoryMatch>** или **<FilesMatch>**, позволяющие осуществить поиск по регулярному выражению, а не по строковым литералам.

Для подкрепления изложенного обратимся к нескольким примерам, но перед этим вспомним о комментариях и пробельных символах. В рамках файла httpd.conf знак «#» в начале строки является комментарием, и его нельзя поставить в конец предыдущей строки. Пробелы игнорируются даже в начале строки, поэтому нет ничего страшного в отступах директив: это делает файл удобочитаемым и структурированным.

Опции базовой конфигурации для сервера Main (главного)

Теперь, имея в наличии основы файла конфигурации Apache, рассмотрим минимальный файл httpd.conf и применим изложенные принципы. Полный файл содержит свыше 100 строк, но авторы удалили комментарии и оставили только необходимое для работы сервера. По большей части, при работе с этим файлом применяется эвристическое правило, гласящее, что если пользователь не знает функций той или иной опции, то он имеет право применить значения по умолчанию: возможно, они окажутся тем, что нужно. Раньше пакет Apache вынуждал администратора редактировать этот файл, т. к. программа не работала без внесения необходимых изменений. Сегодня установка Apache по умолчанию запускается на локальном хосте, прислушивается к порту 80 и получает документацию с /var/www/html. После примера значение этих опций описывается более подробно:

```
### Раздел сервера Main
#
ServerName www.acmewidgets.com
ServerRoot "/etc/httpd"
ServerAdmin root@acmewidgets.com
DocumentRoot "/var/www/html"
User apache
Group apache
Listen 80

DirectoryIndex index.htm index.html index.php Default.htm index.cgi

### Контейнер Directory для всей файловой системы
#
```

```
<Directory />
      Options None
      AllowOverride None
      Order deny, allow
      Deny from all
<Directory />

### Контейнер Directory для всей DocumentRoot
#
<Directory "var/www/html" >
      Options Indexes
      AllowOverride None
      Order deny, allow
      Allow from all
</Directory>
```

Предупреждение

При использовании вышеприведенного файла конфигурации сервер работать не будет. Этот файл призван проиллюстрировать, на какие опции прежде всего следует обращать внимание, чтобы web-сервер сразу начал работать. Оставьте все прочие опции файла без изменений.

- **ServerName** — имя по умолчанию для данного сервера. Это полностью квалифицированное имя домена, и оно может отличаться от имени машины. Так Apache идентифицируется для посетителей.
- Как упоминалось выше, **ServerRoot** — это (по мнению Apache) местоположение, в котором он установлен в системе. Большинство пакетов для Linux устанавливают Apache в каталог /etc/httpd, так что файлы конфигурации и регистрационные журналы расположены в этом каталоге.
- **ServerAdmin** — почтовый адрес администратора, отображаемый на страницах ошибок и в переменных окружения для сценариев.
- **DocumentRoot** — эквивалент домашнего каталога по умолчанию (в терминах IIS). Отсюда сервер извлекает документы в отсутствие заданного виртуального хоста.

В вышеприведенной конфигурации пользователь и группа, в качестве которой работает web-сервер, — apache. Директива *listen* может быть парой IP:порт или просто номером порта. Если IP не задан, Apache прослушивает этот порт на всех сконфигурированных интерфейсах. Множественные директивы listen могут быть размещены в одном файле конфигурации. В Apache 2.0 должна присутствовать по крайней мере

одна директива listen, иначе сервер не запустится. В разделе «Виртуальный хостинг» рассматривается более подробный пример директивы listen.

DirectoryIndex задает по умолчанию индексную страницу для вывода на случай, если в URL не будет задано имя файла.

Остаток файла — это контейнеры, задающие разрешения и поведение корневой файловой системы и DocumentRoot. Это самые распространенные строки, которые должны входить в контейнеры. Среди опций имеются ExecCGI, FollowSymLinks, Includes или Indexes (есть еще пара, но они — более эзотерические). Если в контейнере опускается Options, то подразумевается All. ExecCGI указывает на то, что данный каталог является каталогом для сценариев CGI. FollowSymLinks означает, что в данном каталоге сервер будет следовать символическим ссылкам. Includes обеспечивает вставки на стороне сервера. Indexes генерирует листинг данного каталога, если индексная страница не найдена.

Директива *AllowOverride* сообщает пакету Apache, какая из этих опций может быть перезаписана (подменена) позже в файле конфигурации или в файле .htaccess. Директивы *Allow* и *Deny* (не показаны) определяют хосты, имеющие возможность доступа к данному каталогу или ресурсу. Они могут быть перечислены по имени хоста, IP, диапазону IP либо даже по переменным окружения, полученным от клиента, работающего с браузером. Директива Order определяет порядок применения директив Allow и Deny.

Теперь web-сервер можно запустить с помощью следующей команды и протестировать его работу на используемом браузере:

```
/etc/init.d/apache start
```

Web-страница по умолчанию

Браузер должен отображать тестовую страницу (Test Page) или страницу «It worked!» (сработало!). Процесс изменения web-страницы по умолчанию — такой же, как и в IIS. Просто скопируйте индексную страницу по умолчанию в каталог DocumentRoot. В рассматриваемом файле конфигурации DocumentRoot определен как /var/www/html, поэтому скопируйте его в этот каталог и смените название страницы на название, определенное директивой *DirectoryIndex*. В следующем примере создается страница index.html для www.acmewidgets.com и копируется в каталог DocumentRoot (см. рис. 9.8).

```
<! - - Пример index.html для www.acmewidgets.com - ->
<html> <head> <title> AcmeWidgets</title> </head>
<body bgcolor= #FFFFFF>
<center>
      <img src=acme_anvil.gif border=0 alt=logo>
 <h1> Добро пожаловать в Acme Widgets в Сети < /h1>
      <p>Приглашаем посетить нашу новую домашнюю страницу в Сети.
      Мы подключились к новому провайдеру хостинга,
      использующему на 100% открытый продукт!</p>
      <br>
      <br>
 </center>
 </body>
 </html>
```

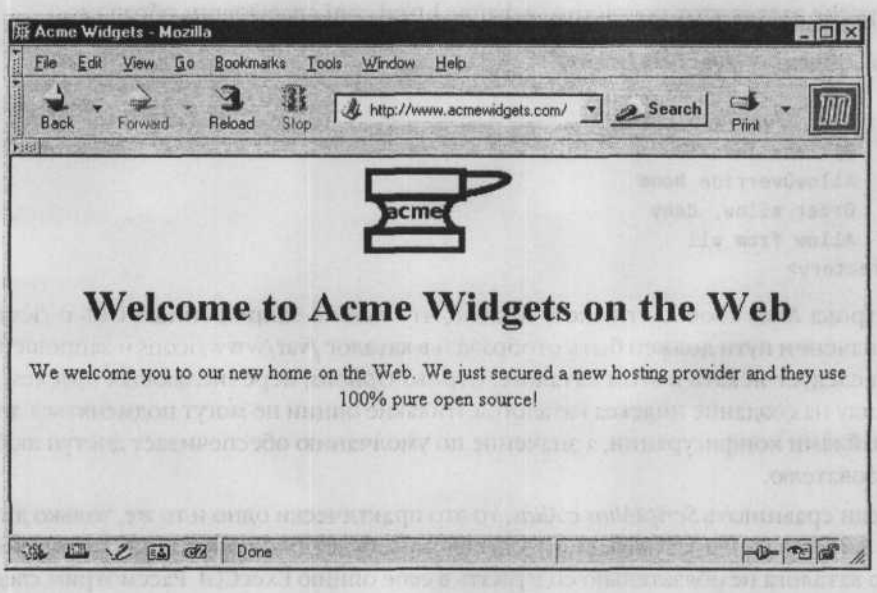

Рис. 9.8. Каталог DocumentRoot для www.acmewidgets.com

Псевдонимы и псевдонимы сценариев

Идентично виртуальным каталогам IIS, пакет Apache обеспечивает способ отображения запрошенного пути URL в другую часть файловой системы. Конфигурация в Apache осуществляется с помощью директивы *Alias* (псевдоним). Самый распространенный псевдоним, который должен присутствовать в конфигурации Apache, — каталог /icons/(пиктограммы, значки). Это — феномен, уходящий в историю развития вычислительных технологий, когда сисадмины старались избежать хранения множества копий одних и тех же изображений по всей файловой системе. Сисадмин использует каталог пиктограмм как единое хранилище изображений, после чего, независимо от обеспечиваемого web-пространства, теги <img> HTML можно записать, как показано в нижеприведенном примере, и Apache будет знать, где искать это изображение:

```
<img src=/icons/blank.gif>
```

Apache задает этот псевдоним в файле httpd.conf следующим образом:

```
Alias /icons/ " /var/www/icons/"

<Directory "/var/www/icons/"
      Options Indexes
      AllowOverride None
      Order allow, deny
      Allow from all
</Directory>
```

Строка Alias сообщает пакету Apache, что любой запрошенный URL с /icons/ в обозначении пути должен быть отображен в каталог /var/www/icons и запрошенный файл следует искать в этом каталоге. Строка *Options*, перечисляющая Indexes, дает команду на создание индекса каталогов. Никакие опции не могут подменяться другими файлами конфигурации, а значение по умолчанию обеспечивает доступ любому пользователю.

Если сравнивать *ScriptAlias* с *Alias*, то это практически одно и то же, только директива ScriptAlias подразумевает, что псевдоним будет обслуживать CGI. Контейнеру этого каталога не обязательно содержать в себе опцию ExecCGI. Рассмотрим следующий пример:

```
ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"

<Directory "/var/www/cgi-bin">
      Options None
      AllowOverride None
      Order allow, deny
      Allow from all
</Directory>
```

Защита и разрешения

Механизмы управления защитой сервера пакета Apache обладают такой же (если не большей) гранулярностью, как и в IIS. Apache обладает возможностью разрешения (allow) и запрета (deny) хостов, управления правами доступа к файлам, а также базовой и дайджестной аутентификацией для управления доступом.

Как уже отмечалось, директивы allow и deny позволяют обеспечивать явный контроль за отдельными хостами или даже целыми сетями, имеющими доступ к сайту. Формат — **Allow host1 host2 [...]**. Хостом может быть точный IP-адрес, частичный IP-адрес, сетевой сегмент или адрес CIDR (бесклассовая междоменная маршрутизация), адрес IPV6 или значение переменной, заданное сценарием в среде web-браузера, например:

```
## Доступ к файлам с именем admin.html разрешен только локальному хосту
#
<Files "admin.html">
      Options None
      AllowOverride None
      Order allow, deny
      Allow from 127.0.0.1
</Files>

## Доступ к файлам с именем admin.html разрешен только внутренней сети и
## локальному #узлу
# admin.html
#
<Files "admin.html">
      Options None
      AllowOverride None
      Order allow, deny
      Allow from 192.168.0.0/24 127.0.0.1
</files>
```

Директива Deny имеет тот же синтаксис, но отказывает любому совпадающему хосту.

Разрешения файловой системы применяются к *User* (пользователь) и *Group* (группа), от имени которых работает web-север. В данном случае они определены как **apache**. Обратите внимание, что это может быть фактический пользователь и группа в системе. В большинстве случаев дистрибутив самостоятельно определяет эти параметры. Если возникают сомнения, то в файле конфигурации лучше оставить значения по умолчанию. Что касается разрешений файлов, если apache не имеет в каталоге, например, разрешений на считывание, запись или исполнение (read, write, execute), то Apache не сможет перечислять ветви дерева каталога, осуществлять в них запись или просто проходить по ним.

Вообще, разрешения файлов для ServerRoot принадлежат пользователю root. Владельцем каталогов DocumentRoot обычно является *apache* или пользователь web-сервера. При запуске его пакетом Apache запускается один материнский процесс от имени root, после чего запускается до 10 порожденных процессов (заданных в файле конфигурации), выполняющихся как пользователь web-сервера. Регистрационные журналы и другая информация о процессах управляются материнским процессом, а «дети» контролируют запросы. Таким образом, разрешения должны быть настроены в соответствии с выполняющимися программными приложениями. Если не используется ничего, кроме статичного содержимого из каталога DirectoryRoot, тогда ничего особенного не требуется: разрешений по умолчанию — 755 /var/www/html и владельца root должно быть достаточно:

```
drwxr-xr-x  2 root      root 4096 Sep 10 14:36 html
```

Однако при необходимости выполнения сценариев, осуществляющих запись в файловую систему, либо при наличии каталога CGI, содержащего файлы исполнения, необходимо убедиться, что Apache имеет доступ к записи в этот каталог либо бит исполнения настроен на сценарии в каталоге cgi-bin.

Apache так же, как и IIS, обладает способами базовой и дайджестной аутентификации. Эти способы можно определить в рамках контейнеров и использовать в разделе Main файла конфигурации, в каталоге, в файлах и в контейнерах VirtualHost. Для настройки базовой аутентификации в одну из областей потребуется добавить следующие строки:

```
AuthType Basic
AuthName "Acme Widgets Internal Area"
AutheUserFile /etc/httpd/passwd/acme_internal
Require valid-user
```

AuthType может иметь тип либо **Basic** (Базовая), либо **Digest** (Специализированная). Различия между данными типами аутентификации описаны в разделах выше. *AuthName* — название защищенной области. Это имя появится во всплывающем окне с подсказкой пользователю о вводе регистрационных параметров, поэтому лучше всего в качестве имени выбирать значащее слово, чтобы пользователи понимали, где им регистрироваться. *AuthUserFile* определяет место хранения паролей. В отличие от IIS пользователи HTTP не являются пользователями системы; файлов htpasswd может быть сколько угодно. Создаются новые пользователи, и пароли изменяются с помощью команды **htpasswd**. Этот аспект рассматривается ниже. Строка *Require* определяет, какие пользователи могут получить доступ к этой области. При установке на **valid-user** любому действительному пользователю в этом файле пароля будет предоставлен доступ. Это также может быть разделенный пробелами список имен пользователей в файле.

Администрирование многих HTTP-пользователей — задача не из трудных. Эта функция не задумана как масштабируемая, но она подходит для добавления пары учетных записей администратора в конкретную область или файл. Для создания

файла пароля создайте каталог в любом месте системы для хранения файлов htpasswd. С этой целью был создан файл /etc/httpd/passwd. Затем создайте файл (от имени root) с добавлением в него нового пользователя с помощью следующей команды:

```
$ htpasswd -c /etc/httpd/passwd/passwords admin
```

Опция **-c** создает новый файл, и имя пользователя admin будет единственной в нем записью. Эта команда — сама по себе интерактивна, и она будет спрашивать пароль администратора. Пароль будет сохранен в специальном файле, закодированном по умолчанию алгоритмом md5. Если необходимо создать другой пользователь, просто подайте следующую команду:

```
$ htpasswd -c /etc/httpd/passwd/passwords acme
```

При этом будет добавлен пользователь **acme**. Если пароль нужно задать неинтерактивно, то его можно добавить в конец команды:

```
$ htpasswd -c /etc/httpd/passwd/passwords acmeadmin new_password
```

Файлов паролей можно иметь сколько угодно и/или хранить их в разных местах, в зависимости от потребностей. Например, при выполнении хостинга домена, возможно, потребуется создание файла пароля для каждого конкретного хоста, его размещение в домашнем каталоге каждого хоста и возможность читать его только данным пользователем и пользователем web-сервером.

Файлы .htaccess

Apache дает возможность пользователям и администраторам сайтов на сервере подменять настройки конфигурации для отдельных каталогов. Преимущество этого заключается в том, что web-программист может получить разрешение на конфигурирование определенных опций сервера для своего сайта без доступа к файлу httpd.conf. Для настройки главный файл конфигурации — httpd.conf — должен иметь директиву *AllowOverride*, определенную для **<Directory>**, и в данном каталоге должен быть файл .htaccess. *AllowOverride* принимает разделенный пробелами список групп опций, которые будет разрешено подменять. Названия групповых опций могут быть следующие: *AuthConfig, FileInfo, Indexes, Limit, Options, All* и *None*. Файл .htaccess — это текстовый файл, содержащий опции конфигурации для данного каталога. Web-сервер должен иметь возможность его считывания. Обратите внимание на точку, с которой начинается имя файла. *AllowOverride* работает только в контейнерах **<Directory>**, однако .htaccess не должен содержать в себе другой контейнер <Directory>. Он должен лишь размещать опции, относящиеся к каталогу, в котором находится файл .htaccess:

```
#httpd.conf
<Directory  /var/www/html/internal/>
      AllowOverride Indexes AuthConfig
</Directory>
```

В вышеприведенном примере web-программисту, работающему над созданием внутреннего web-сайта, дается возможность подмены директив *Indexes* и *AuthConfig*. Разрешение *Indexes* означает, что web-программист может подменять опции, имеющие отношение к индексированию каталога в каталоге, в котором находится файл .htaccess. Разрешение *AuthConfig* означает, что пользователи могут пользоваться директивами, применяемыми для настройки Базовой и Дайджестной аутентификации этого каталога.

Следующий пример иллюстрирует то, как может выглядеть соответствующий файл .htaccess:

```
# /var/www/html/internal/.htaccess
Options Indexes
AuthType Basic
AuthName "Internal Use Only"
AuthUserFile /etc/httpd/passwd/internal.passwords
Require valid-user
```

Если web-программист имеет доступ к оболочке на сервере и может осуществлять запись в каталог /etc/httpd/passwd, то создание нового файла пароля и заполнения его пользователями выполняется так, как описано выше. Однако, если web-программист не имеет права доступа к записи в данный каталог, он может принять решение о размещении файла пароля в своем собственном каталоге или в другом месте, созданном сисадмином вне каталогов web-сервера. Поскольку опция *Indexes* задана, индексы каталогов будут сгенерированы для любого каталога в каталоге /var/www/html/internal, не имеющего страницы index.html.

При необходимости изменения имени файла .htaccess можно использовать директиву *AccessFileName* в файле httpd.conf.

Виртуальный хостинг

Apache стал первым web-сервером, поддерживающим виртуальный хостинг. Подобно виртуальным серверам в IIS, эта функция позволяет подключать множественные домены к одному web-серверу. Виртуальный хостинг Apache настраивается через файл httpd.conf и его можно сконфигурировать под любую комбинацию хостов на базе имени, IP либо обоих типов. Виртуальный хостинг на базе имени конфигурируется с помощью директивы *NameVirtualHost* и контейнеров VirtualHosts. Хостинг на базе IP нуждается в директиве *Listen*, которая «подскажет» Apache, какие IP-адреса прослушивать и какие контейнеры VirtualHosts использовать. Рассмотрим вкратце пару различных примеров.

Для активизации виртуального хостинга на базе имени, помимо директивы NameVirtualHost в разделе Main файла httpd.conf, как минимум еще требуется директива *ServerName* внутри каждого контейнера VirtualHost для того, чтобы Apache обрабатывал запросы для домена с таким именем.

```
NameVirtualHost *:80
<VirtualHost *:80>
      ServerName internal.acmewidgets.com
      DocumentRoot /var/www/vhosts/internal
</VirtualHost>
<VirtualHost *:80>
      ServerName billing.acmewidgets.com
      DocumentRoot /var/www/vhosts/billing_dept
</VirtualHost>
```

В данном примере Apache обслуживает запросы на internal.acmewidgets.com или billing.acmewidgets.com из DocumentsRoots /var/www/vhosts/internal и /var/www/vhosts/billing_dept, соответственно. Запросы могут поступать на любой IP на сервере через порт 80. Apache обрабатывает эти запросы путем поиска совпадений директивы *ServerName* в контейнере VirtualHost с запрошенным именем сервера в URL. Данный пример предполагает, что DNS сконфигурирован на указание на IP-адрес сервера для этих субдоменов acmewidgets.com. Можно иметь сколько угодно доменов или субдоменов, если DNS (сервер доменных имен) сконфигурирован соответствующим образом. Контейнер VirtualHost может содержать почти все, что содержит раздел Main файла конфигурации, поэтому имеет смысл настраивать такие аспекты, как разрешения каталогов, аутентификация, системные журналы и администраторы сервера так же, как настраивался бы раздел Main.

Для конфигурирования виртуального хостинга на базе IP сначала на компьютере необходимо настроить множественные IP-адреса. Простейшим способом добавления нового IP-адреса в системах типа Fedora или RedHat будет копирование файла /etc/sysconfig/network-scripts/ifcfg-eth0 в /etc/sysconfig/network-scripts/ifcfg-eth0:0 и изменение переменной DEVICE для соответствия в новом файле:

```
$     cd    /etc/sysconfig/network-scripts/
$     cp    ifcfg-eth0  ifcfg-eth0:0
$     cp    ifcfg-eth0:0 ifcfg-eth0:1
$     vi    ifcfg-eth0:0
# Sample    ifcfg-eth0:0 file
DEVICE=eth0:0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.0.53
NETMASK=255.255.255.0
GATEWAY=192.168.0.1
# Sample    ifcfg-eth0:1 file
DEVICE=eth0:1
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.0.54
NETMASK=255.255.255.0
GATEWAY=192.168.0.1
```

Устройству eth0 можно добавить сколько угодно IP-адресов путем прибавления числа после двоеточия для каждого IP-адреса и присвоения нового IP-адреса переменной IPADDR. В вышеприведенном примере использовалось адресное пространство класса С (внутренние адреса). Другим интерфейсам также можно добавить дополнительное количество IP-адресов путем повторения указанных шагов для eth1, eth2 до ethN интерфейсов.

Теперь, когда IP-адреса сконфигурированы, в Apache можно настроить виртуальный хостинг на базе IP путем добавления директивы *Listen* в раздел Main файла httpd.conf. Как указывалось выше, Apache будет прослушивать все интерфейсы, если IP не указан, однако явное его указание увеличивает предсказуемость и улучшает контроль функций сервера. В следующем примере настроим два виртуальных хоста на базе IP, один — с порта 80 (по умолчанию), а другой — с порта 8080:

```
# Раздел Main httpd.conf
Listen 192.168.0.53:80
Listen 192.168.0.54:8080
<VirtualHost 192.168.0.53:80>
      ServerName sales.acmewidgets.com
      DocumentRoot /var/www/vhosts/sales_dept
</VirtualHost>
<VirtualHost 192.168.0.54:8080>
      ServerName internal2.acmewidgets.com
      DocumentRoot /var/www/vhosts/internal2
</VirtualHost>
```

Apache поддерживает кодирование SSL/TLS через модуль SSL *mod_ssl*. В большинстве дистрибутивов модуль mod_ssl предлагается как отдельный пакет. Например, в Fedora Core этот пакет просто называется mod_ssl и зависит от пакета openssl. В зависимости от разновидности Linux, лучше всего искать пакет, специально подготовленный под используемый дистрибутив. При работе с Suse следует просмотреть установочные диски, с Debian — хранилища (с помощью утилиты *apt*), с RedHat/Fedora — обратиться к сайту http://rpmfind.net или http://freshprms.net. Mandrake может иметь нужный пакет на установочных дисках либо следует зайти на сайт http://rpmfind.net.

После установки пакет mod_ssl установит в каталог *ServerRoot* разделяемую библиотеку mod_ssl и несколько файлов конфигурации. В библиотеке имеются функции, нужные Apache для выполнения подключений SSL, а файлы конфигурации управляют поддержкой SSL. Также имеется сертификат сервера по умолчанию и *Makefile* для генерирования новых сертификатов, но в данном случае используется openssl. Однако для начала протестируем web-сервер с активизированным протоколом защищенных сокетов (SSL) путем перезапуска Apache и попытки подключения к https://localhost.

От браузера должно поступить предупреждающее сообщение (см. рис. 9.9) о том, что он не смог проверить «личность» сервера. Нажав кнопку **Examine Certificate** (Изучить сертификат), пользователь увидит серверный сертификат по умолчанию (см. рис. 9.10).

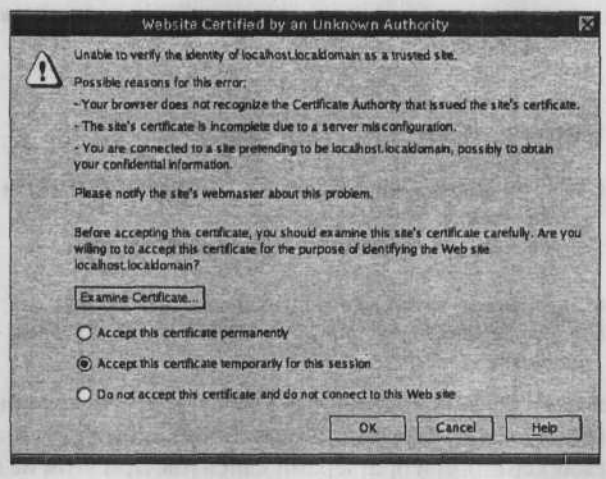

Рис. 9.9. Предупреждающее сообщение о неподтвержденной «личности» сервера и сопутствующие опции

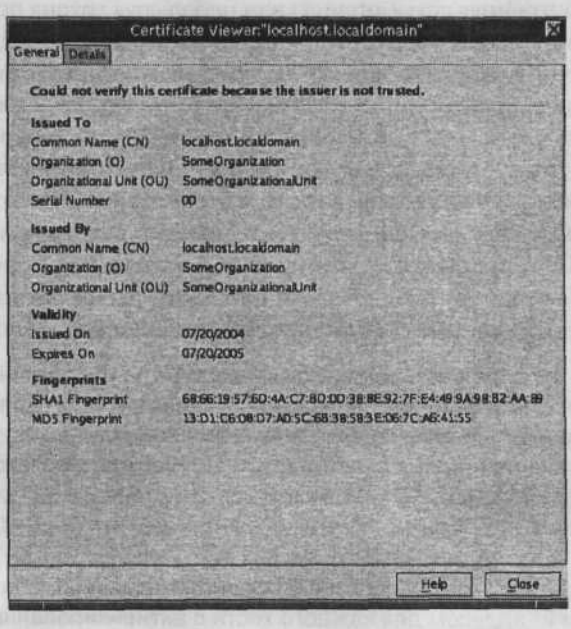

Рис. 9.10. Сертификат сервера по умолчанию

Если предупреждение появляется, значит web-сервер с активизированным SSL функционирует. Установленный Apache сертификат по умолчанию выдается на имя «SomeOrganization» (некая организация). Для создания запроса на новый сертификат введите следующие команды. Для этого должен быть установлен пакет openssl.

```
$     #     создайте резервную копию оригинала личного ключа и сертификата
$     cd    /etc/httpd/conf
$     mkdir ssl_bak
$     cp ssl.key/server.key ssl_bak/
$     cp ssl.crt/server.crt ssl_bak/
$
$     # создание нового Запроса на подписание сертификата (CSR) и личного ключа
$     openssl     req -new > acmewidgets.csr
$     openssl     rsa -in privkey.pem -out acmewidgets.key
$
$     # альтернатива: самостоятельное подписание сертификата
$     openssl x509 -in acmewidgets.csr -out acmewidgets.crt -req -signkey \
acmewidgets.key -days 999
```

При этом создается новый CSR и личный ключ. В качестве альтернативы сертификат можно подписать самостоятельно и использовать его для шифрования HTTP-подключений между сервером и браузерами клиентов. При этом не следует забывать о том, что данный сертификат не является официальным. Это «самоподписанный» сертификат, который объявлен действительным самим пользователем. Если вы сами, корпоративная внутренняя сеть (intranet) или небольшая группа пользователей будут единственными, кто увидит этот сертификат, то их можно попросить о подтверждении предупреждений с последующим продолжением регистрации или выполнения необходимых задач переадресации HTTPS. С другой стороны, при организации Интернет-магазина и необходимости шифрованного HTTP для интерактивного приема оплаты по кредитным картам, может возникнуть необходимость в приобретении подлинной подписи третьей стороны от одного или нескольких Бюро сертификации в Интернет. Эти бюро сертификации зарегистрированы в популярных web-браузерах, и их сертификаты распространяются вместе с браузерами. При этом, если сертификат подписывается одним из бюро сертификации, распознанным браузером, то сертификат сервера будет принят с установлением зашифрованного подключения.

Примечание Использовать виртуальный хостинг на базе имени с отдельными сертификатами SSL нельзя. Таково ограничение протокола SSL. Причина заключается в том, что SSL-подключение устанавливается до HTTP. Поскольку ссылка на машину до установки HTTP осуществляется только по IP-адресу, то не существует заголовка хоста, который сервер мог бы идентифицировать с помощью отдельного виртуального хоста. При необходимости запуска с одной машины нескольких виртуальных хостов с отдельными SSL-сертификатами следует пользоваться виртуальным хостингом на базе IP с отдельным IP-адресом для каждого хоста с активизированным SSL.

Установка mod_ssl добавила в файл /etc/httpd/conf.d/ssl.conf все необходимые опции конфигурации, которые активизируют SSL в Apache. Просто скопируйте его в места, указанные в файле ssl.conf, и перезапустите Apache для активизации нового сертификата:

```
$     # перезаписать ключ сервера по умолчанию
$     cp acmewidgets.key ssl.key/server.key
$     # перезаписать crt сервера по умолчанию
$     cp acmewidgets.crt ssl.crt/server.key
$     /etc/init.d/httpd restart
```

Новый сертификат сервера должен быть активен с возможностью просмотра с любого https:// URL на сервере.

Apache обеспечит поддержку SSL в конфигурации сервера Main, вне ее или VirtualHosts путем добавления директивы *SSLEngine*, но позволит использовать только один сертификат на каждый IP-адрес (см. Примечание выше). Потребуется также добавить директиву *Listen* для того, чтобы Apache прослушивал зарегистрированный порт для HTTPS-подключения. Все это должен добавить файл ssl.conf. Рассмотрим данный аспект. Приведенный ниже пример взят из ssl.conf, удалены комментарии и директивы, которые уже описаны:

```
# загрузка модуля, прослушивание порта 443 и регистрация типов MIME
LoadModule ssl_module modules/mod_ssl.so
Listen 443
AddType application/x-x509-cf-cert .crt
AddType application/x-pkcs7-crl .crt
# опции управления SSL
SSLPassPhraseDialog        builtin
SSLSessionCache            shmcb:/var/cache/mod_ssl/scache (512000)
SSLSessionCacheTimeout     300
SSLMutex                   default
SSLRandomSeed              startup file:/dev/urandom 256
SSLRandomSeed connect builtin
SSLCryptoDevice builtin
<VurtualHost _default_:443>
ErrorLog     logs/ssl_error_log
TransferLog  logd/ssl_access_log
LogLevel     warn
SSLEngine    on
SSLCipherSuite All:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP
SSLCertificateFile /etc/httpd/conf/ssl.crt/server.crt
SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key
</VirtualHost>
```

Это — минимальная конфигурация для SSL на Apache. Если после установки сертификата в файл ssl.conf не вносить никаких изменений, Apache будет ожидать

запросы на порт 80 и порт 443. При необходимости добавления другого виртуального хоста HTTPS, это можно сделать здесь. В начале приведенного выше примера конфигурации представлено несколько конфигураций раздела Main, которые будут определять некоторые опции управления SSL пакетом Apache, — этот модуль загружается, и Apache получает сообщение о прослушивании порта 443 на предмет запросов. Имеются зарегистрированные типы MIME, поэтому Apache знает, как обслуживать файлы .crt и .crl. Также заданы опции кэширования и другие значения по умолчанию. В организационных целях разработчики mod_ssl активизировали SSL в VirtualHost, но SSL с тем же успехом можно поместить в файл конфигурации раздела Main. Поскольку теперь данный VirtualHost имеет *DocumentRoot*, виртуальный хост будет наследоваться из основного файла конфигурации, и все файлы в web-пространстве будут обслуживаться идентично, как и ранее, но будут закодированы, если доступ к ним осуществляется по схеме https:// URL.

Модули

При необходимости модули Apache можно подключать и отключать в файле httpd.conf. По умолчанию Apache поставляется со многими модулями — базовый набор включает в себя практически все, что нужно, для выполнения всех описанных до сих пор операций. Однако если попытаться настроить какую-либо особую службу, например поддержку WebDav или LDAP (облегченный протокол службы каталогов), то, возможно, потребуется «раскомментировать» этот модуль и настроить предоставляемые им опции конфигурации.

При установке пакета mod_ssl он добавляет новый файл конфигурации, который загружает модуль mod_ssl. При загрузке этого модуля все вышеперечисленные директивы SSL_... становятся доступными для использования в конфигурации после вставки этого модуля. Настройка прочих модулей во многом такая же, но с каждым используются разные наборы новых директив. Например, для настройки интерфейса LDAP на сервере в файл конфигурации добавляется следующее:

```
# загрузка mod_ldap и mod_auth_ldap
LoadModule ldap_module modules/mod_ldap.so
LoadModule auth_ldap_module modules/mod_auth_ldap.so

LDAPSharedCacheSize 200000
LDAPCacheEntries 1024
LDAPCacheTTL 600
LDAPOpCacheEntries 1024
LDAPOpCacheTTL 600

<Location /ldap-status>
      SetHandler ldap-status
      Order deny, allow
      Deny from all
```

```
      Allow from acmewidgets.com
      AuthLDAPEnabled on
      AuthLDAPURL ldap://127.0.0.1/dc=acmewidgets, dc=com?uid?one
      AuthLDAPAuthoritative on
      Require valid-user
</Location>
```

Аналогично, при необходимости активизации поддержки WebDAV для DocumentRoot с модулями mod_dav и mod_dav_fs, в файл конфигурации понадобится добавить что-то, похожее на следующее:

```
LoadModule dav_module modules/mod_dav.so
LoadModule dav_fs_module modules/mod_dav_fs.so
DavLockDB /var/lock/DavLock
<Location /var/www/html>
      Dav On
      AuthType Basic
      AuthName DAV
      AuthUserFile user.passwd
<LimitExcept GET OPTIONS
      require valid-suer
</LimitExcept>
</Location>
```

Графические инструменты

В дистрибутивах RedHat версий 7.3 и выше имеется полный набор графических инструментальных средств администрирования сервера. Все эти инструментальные средства имеют названия, составленные по схеме *redhat-config-«что-то»*, где *«что-то»* — название конкретной службы, которую приходится конфигурировать. Вот некоторые примеры: *redhat-config-network*, *redhat-config-bind* и *redhat-config-httpd*. В рамках рабочего стола GNOME эти инструментальные средства интегрированы с оконным менеджером, и доступ к ним осуществляется через меню **System Settings** (системные настройки). В системах Fedora Core эти утилиты конфигурации меняют названия на *system-config-«что-то»*. Примеры: *system-config-network*, *system-config-bind* и *system-config-httpd*. Независимо от оконного менеджера эти инструменты можно запускать в X-Window через терминал путем ввода от имени root названия команды. На рис. 9.11 показано окно инструмента конфигурации HTTPD.

Рис. 9.11. Инструмент конфигурации HTTPD

Несмотря на несколько обманчивый внешний вид, утилита конфигурации HTTP, предоставляемая системами Fedora и доступная через команду *system-config-httpd*, — весьма неплохо разработанное программное приложение. Оно обладает во много раз большей ступенчатостью, чем диалоговое окно системы IIS. Каждая закладка имеет собственные подменю, и некоторые из этих подменю также имеют подменю со своими закладками. Таким образом, при навигации по всем подменю можно управлять практически любой опцией из рассмотренных в данной главе без обращения к командной строке.

Еще одной утилитой, упрощающей администрирование Apache, является пакет WebMin (www.webmin.com/). Эта программа превращает сервер Linux или UNIX в сетевое устройство, полностью управлять которым можно из web-браузера. В ней не только имеется поддержка конфигурации Apache из браузера, но и поддержка конфигурирования всех серверных демонов, типичных для таких Интернет-серверов, как Postfix, Bind/Named, MySQL, PostgreSQL, Sendmail, Procmail, SpamAssassin (перечислены далеко не все). Программа также имеет множество меню конфигурации, с помощью которых можно настраивать сетевое поведение, ограничение пропускной способности и фильтрацию TCP/IP с Netfilter на уровне ядра (брандмауэр). Этот программный набор можно сравнить с большим перочинным ножом известной швейцарской марки с десятком разных инструментов, а также с Linuxconf для всемирной сети. Но это еще не все. Пакет WebMin помогает в администрировании базовой операционной системы, позволяя управлять группами и пользователями, менять пароли, управлять файловыми системами, а также просматривать регистрационные журналы, редактировать файлы конфигурации и управлять опциями времени загрузки. WebMin превратился в очень мощную и надежную утилиту для сисадмина. Это настоятельно рекомендуемое к использованию инструментальное средство показано на рис. 9.12.

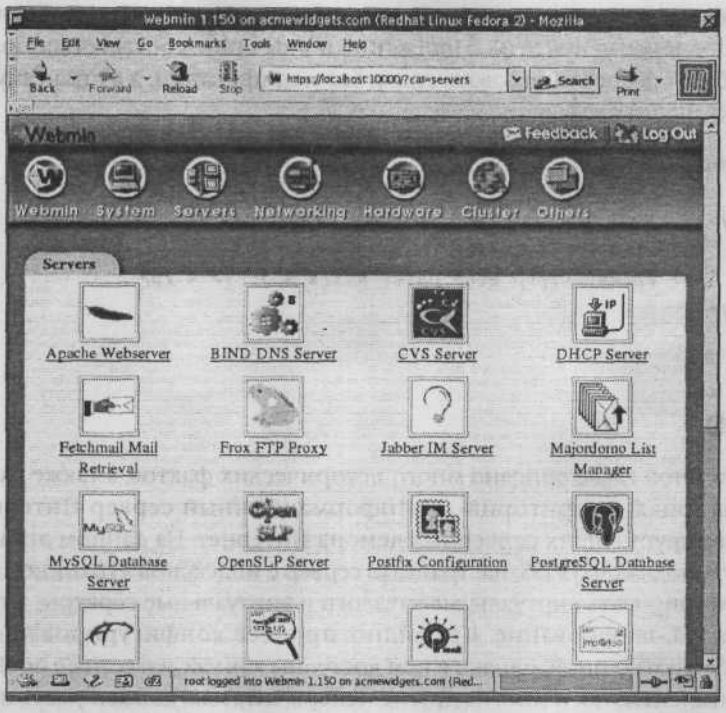

Рис. 9.12. Инструментальное средство администрирования WebMin

Перенос статичных сайтов с IIS на Apache

Теперь, когда два рабочих web-сервера настроены и отвечают на запросы, переход от IIS к Apache — всего лишь вопрос копирования документов с одного на другой и переименование индексных страниц по умолчанию. В настоящее время сайт еще не динамичен, за исключением ASP «Hello world!», но даже это можно преобразовать в эквивалентный код PHP. Для переноса файлов можно пользоваться любым протоколом передачи файлов. Поскольку авторы всегда предпочитают (и предлагают) по возможности избегать протоколов передачи открытым текстом, используем OpenSSH и клиент WinSCP для переноса файлов с Windows в Linux. WinSCP — прекрасная, открытая графического программа для защищенного копирования с поведением, сходным с любой другой программой FTP, которая взаимодействует с серверами SSH или SFTP. Более подробная информация о WinSCP и ее загрузке имеется на сайте http://winwcp.sourceforge.net/eng.

После копирования страниц Default.htm и Default.asp в каталог DocumentRoot сервера Linux переименуйте их в index.html и index.php, соответственно. Страница index.html будет функционировать сразу, без модификации, а в страницу index.php необходимо внести следующие изменения:

```
<! - - пример index.php - ->
<html>
      <body>
            <p>Hello world. </p>
            <p> Время: <?php echo date("h:i:s A"); ?> < /p>
      <body>
</html>
```

Резюме

В представленной главе описано много исторических фактов, а также охвачена довольно обширная «территория» — Информационный сервер Интернет (IIS) и Apache — два крупнейших серверных демона Интернет. На данном этапе читатель должен уметь подключать ISS, настраивать сервер с индексной страницей по умолчанию, конфигурировать виртуальные каталоги и виртуальные серверы, а также активизировать SSL-шифрование. Как видно, процесс конфигурирования сервера Apache — абсолютно иной, однако в нем доступны как уже известные по IIS функции или их эквиваленты, так и многие другие. Теперь читатель должен уметь подключать пакет Apache Web Server, конфигурировать его индексную страницу по умолчанию, сервер Main, псевдонимы и псевдонимы сценариев (ScriptAliases), виртуальные хосты и поддержку SSL. Обладая этими знаниями, читатель сможет установить любое количество модулей, в соответствии с потребностями его компании. Кроме этого, способ переноса web-сайта с одного сервера на другой должен быть простым и понятным: все, что нужно, — это хороший клиент переноса файлов.

Краткое резюме по разделам

Предыстория: Протокол передачи гипертекстовых документов

- ☑ Тим Бернерс-Ли спроектировал протокол HTTP в 1990 году во время работы в CERN.
- ☑ При разработке протокола HTTP была позаимствована концепция «гипертекста» Gopher и Теда Нельсона, который работал над проектом Xanadu.

- ☑ HTTP и World Wide Web имели ошеломительный успех. В начале 90-х годов корпорации Microsoft и Netscape Communications начали разработку собственных web-серверов и web-браузеров.

Информационный сервер Интернет

- ☑ IIS доступен в линии продуктов NT от Microsoft, однако некоторые функции отключены в не-серверных вариантах операционных систем. Конфигурирование и администрирование IIS осуществляется через диалоговое окно Информационных служб Интернет.
- ☑ IIS поддерживает виртуальные каталоги, виртуальные серверы и аутентификацию, но, при необходимости запуска SSL, сначала необходимо приобрести подпись Бюро сертификации.

Web-сервер Apache

- ☑ Apache создан из серии патчей к старой программе httpd CERN.
- ☑ Традиционно конфигурирование Apache выполняется в текстовом файле httpd.conf, однако в распоряжении сисадмина имеются инструментальные средства GUI и web-приложения.
- ☑ Apache поддерживает псевдонимы, виртуальные хосты, аутентификацию и SSL, однако из-за ограничений протокола SSL нельзя запустить более одного виртуального хоста SSL с виртуальным хостингом на базе имени; необходимо применить хостинг на базе IP для получения нескольких SSL-сертификатов для работы на одном сервере.
- ☑ Apache имеет много модулей для расширения функций пакета, предоставленных по умолчанию.

Перенос статичных сайтов с IIS на Apache

- ☑ Скопируйте файлы с сервера Windows на сервер Linux с помощью протокола переноса файлов.
- ☑ Разместите файлы в каталоге DocumentRoot.
- ☑ Переименуйте файл Default.htm в index.html.
- ☑ Простой функциональности ASP можно добиться с помощью свободно доступного языка PHP.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма «**Ask the Author**»). Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: Где в IIS по умолчанию размещен каталог Web?

О: c:\Inetpub\wwwroot.

В: Где в Apache размещен DocumentRoot (каталог Web по умолчанию)?

О: /var/www/html.

В: Где размещены журналы регистрации для Apache?

О: /var/log/httpd **или** /etc/httpd/logs.

В: Как проще всего проверить функционирование web-сервера?

О: В командной строке осуществите подключение telnet к порту 80 на локальной машине, затем введите **GET / HTTP/1.0**.

В: Как проще всего проверить действенность SSL-сертификата?

О: Аналогично telnet на порту 80 можно воспользоваться openssl для проверки корректной работы порта 443:

```
$ openssl s_client -connect localhost:443 -state -debug

GET / HTTP/1.0.
```

В: Как протестировать функционирование PHP?

О: В DocumentRoot создайте файл с именем info.php и добавьте в него следующее:

```
<?php phpinfo ( ); ?>.
```

Затем откройте http://localhost/info.php в web-браузере.

В: Что такое RFC?

О: Аббревиатура RFC расшифровывается как Запрос на комментарии (Request for Comments). RFC — это открытые стандарты Интернет, определяющие принципы работы всех протоколов TCP/IP. Они представляют собой так называемые «белые книги», в которых для разработчиков изложены лучшие стратегии реализации того или иного протокола. Они открыты для комментариев, внесения изменений и обновлений со стороны любых пользователей. Например, HTTP RFC много раз переписывался с целью реализации новых функций. RFC имеются как для каждого популярного Интернет-протокола, так и для не очень популярных, например HTCPCP 1.0 (Hyper Text Coffee Pot Control Protocol, Гипертекстовый протокол уп-

равления кофеваркой. (В среде компьютерных специалистов нередка фраза «XXX умеет делать все, кроме приготовления кофе», означающая, что продукт XXX обладает очень богатой функциональностью. Это является благодатной почвой для различных шуток на «кофейные» темы, например документов, описывающих способы подключения кофеварки к последовательному порту компьютера и управления им с Linux-машины. Как пишет автор данного изобретения: «Мне надоело слышать, что Linux может все, КРОМЕ приготовления кофе, и я решил научить его». Стандарт HTCPCP является одним из них. — *Примеч. науч. ред.*). Для получения более подробной информации о RFC рекомендуется посетить сайт http://ietf.org. Проблемной группы проектирования Internet (IETF).

В: Где найти более подробную информации о Протоколе защищенных сокетов (SSL)?

О: Теоретическое описание принципов работы SSL находится на web-странице OpenSSL www.openssl.org/; для Apache SSL/TSL Encryption — http://httpd.apache.org/docs-2.0/ssl/.

В: К кому обратиться, если никакие средства не помогают?

О: Наиболее распространенные дистрибутивы имеют свои центры технической поддержки, куда и можно обратиться. Как правило, техническое обслуживание осуществляется не бесплатно, но оно того стоит. Большинство специалистов по Linux готовы помочь в достижении поставленной цели, если им подробно ее объяснить. Можно поискать независимых консультантов в Интернет, которые будут рады оказать помощь за умеренную плату. Можно сказать, что эти службы — как раз и есть то место, где Linux начинает стоить денег, однако авторы не раз убеждались на собственном опыте, что это лучше, чем в самых тяжелых ситуациях замыкаться на поставщиках, и такие связи помогают выстроить профессиональные взаимоотношения с теми специалистами, кому небезразлично расширение вашего бизнеса.

Интернет — прекрасная среда для поиска и нахождения подходящих методов и ответов на интересующие вопросы по Linux и, поскольку движение по распространению бесплатных программных средств имеет большее отношение к культуре, нежели к свободе, Группы пользователей Linux (LUG) — замечательное место, где можно получить помощь и узнать больше об администрировании сервера. Ищите нужную вам область, пользуйтесь перекрестными ссылками, и успех *не заставит* себя ждать. При неудаче, попробуйте открыть свою страницу по техническому обслуживанию. Проект документации Linux имеет полную информацию о группах пользователей Linux: www.tldp.org/HOWTO/User-Group-HOWTO-3.html#ss3.1.

10 Зак. 1269

Глава 10

Порядок миграции настольных систем

Разделы:

- Оценка текущего рабочего окружения
- Проектирование настольной системы Linux
- Тестирование настольной системы Linux
- Перенос данных программных приложений и профилей
- Обучение пользователей настольных систем
- Развертывание настольных систем Linux

☑ Резюме

☑ Краткое резюме по разделам

☑ Часто задаваемые вопросы

Введение

Процесс перехода (миграции) пользователей настольных систем Windows на Linux похож на процесс перехода с серверов Windows на Linux, описанный в главе 1, однако следует обратить особое внимание на системные настройки каждого из пользователей и необходимость обучения для облегчения перехода. Процесс аналогичен описанному в главе 1 в отношении этапов сбора информации, проектирования и развертывания, однако, поскольку уже известно, в каком месте общей сетевой топологии будут расположены настольные рабочие станции, этот аспект проектирования можно пропустить. В данной главе авторы анализируют среду настольных рабочих станций компании Acme Widgets и определяют схему перевода пользователей на Linux, используя дистрибутив Fedora Core.

Предполагается, что описанный процесс станет общим обзором миграции настольных систем. Будет рассмотрена сравнительно небольшая корпоративная сеть Acme Widgets, хотя процесс можно расширить, в зависимости от необходимого количества пользователей и систем. Будут даны советы по формированию схемы переноса, подходящей каждой конкретной компании.

Для успешного перехода на Linux необходимо планирование, наличие нескольких дополнительных компьютеров и определенная помощь. Оценка существующих программных и аппаратных средств, а также проектирование новой среды являются предпосылками перехода. Собранная информация позволит определить лучшее решение для каждого типа пользователей в компании и составить план реализации решений. Именно поэтому авторы разделили процесс перехода на следующие этапы: оценка, проектирование, испытание, переход, обучение и развертывание. Эти этапы должны быть выполнены, хотя и не обязательно в указанном порядке. Рассмотрим каждый из этих этапов.

Оценка включает в себя изучение различных настольных систем и подготовку справочной документации. Для этого составляется список программных приложений, аппаратных средств и лицензий для каждой машины. Он называется *списком активов*, с помощью которого можно определить типы пользовательских профилей и создать *спецификацию функциональных требований* к замене настольных рабочих систем. Спецификация функциональных требований обычно готовится в виде электронной таблицы ресурсов программных приложений, необходимых каждому пользователю. Оценка заканчивается после составления этих двух документов.

На этапе проектирования по списку активов и спецификации функциональных требований из первого этапа составляется *спецификация функциональной замены* для каждого типа пользовательского профиля. Спецификацию замены также можно рассматривать как назначение профиля Linux пользовательским профилям, перечисленным в списке активов. Эта спецификация используется для сборки машин, которые будут использоваться позже для тестирования и обучения.

Этапом испытаний подтверждается, что замена тестовой операционной системы «дотягивает» до спецификации функциональной замены и будет соответствовать спецификации требований (техническому заданию) из предыдущего этапа. Чтобы убедиться в том, что пользователь впоследствии не столкнется с легко выявляемыми ошибками, следует протестировать несколько элементов контрольной таблицы.

При наличии свободного ИТ-персонала одновременно с этапом перехода можно выполнять этап обучения. В то время, как один сотрудник будет обучать пользователей основам работы с Linux, другие смогут резервировать данные на компьютерах пользователей и устанавливать на них новые профили указанной операционной системы. Для резервирования понадобится сетевой файловый сервер или пишущий CD-ROM. Установку можно осуществить несколькими способами: сетевая установка, клонирование жестких дисков, методы Kickstart либо установка с CD-ROM — весьма популярные и несложные способы.

Для обучения, как правило, необходимо дополнительное оборудование. В зависимости от размеров компании ресурсы будут варьироваться, однако определенное количество дополнительных машин следует зарезервировать для обучения. Самый простой метод изучения Linux заключается в обычной практической работе. Наличие компьютеров для обучения не только обеспечит пользователям возможность потренироваться работе с Linux, но и позволит протестировать операционную среду в реальных условиях. Понятно, что чем больше компьютеров имеется для обучения, тем лучше, но обычно достаточно 7-14 машин для компании среднего размера с 50-100 сотрудниками. В маленькой компании, такой как Acme Widgets, обучение можно осуществлять на личной машине каждого пользователя с миграцией каждого компьютера в нерабочее время. Обучение занимает от одного дня до недели и больше и должно проводиться очень тщательно, потому что многие операции на настольной рабочей станции Linux сходны с операциями в Windows. Во время обучения следует рассмотреть файловую систему, запуск программных приложений, а также настройку электронной почты и индивидуальных параметров.

В последний этап — развертывание — входят ответы на вопросы и помощь пользователям в привыкании к новой среде по мере возникновения трудностей. Составление документации с короткими пояснениями по настройке обычных программных приложений и опций — прекрасное средство как обучения, так и развертывания систем. Частью развертывания является помощь пользователям в настройке электронной почты, служб мгновенного обмена сообщениями и средств коллективного пользования, а также в управлении каталогами резервных файлов на сервере файлов и импортировании, например закладок из настроек старого браузера.

Все перечисленное подразумевает наличие в компании квалифицированных ИТ-кадров, но может быть выполнено и неспециалистом, если потратить немного больше времени.

Оценка текущей настольной среды

Перед тем, как определить способ перехода, необходимо знать, с чем придется работать. Составьте так называемую опись типов пользователей, аппаратных и программных средств, а также используемых лицензированных программных приложений. С помощью этой информации можно определить возможное наличие программного решения Linux, совместимость аппаратных средств с Linux, а также особые пожелания, которые могут предъявлять пользователи настольных рабочих станций. В следующих двух разделах описываются различные типы пользователей, а также аспекты их настольных сред, на которые следует обращать особое внимание. На основании этой информации будет составлена *спецификация функциональных требований*, определяющая возможные требования пользователей к программным приложениям и аппаратным средствам.

Типы пользователей

В компьютерной среде любого офиса пользователи обычно делятся на несколько категорий. В небольших организациях подобное разделение может не иметь особой важности, если использование сотрудниками компьютеров обобщено. В крупных организациях с узкоспециализированными сотрудниками полезно определить число и типы пользователей, чтобы спроектировать для них замещающую операционную систему. Общие категории — следующие.

Киоск

Киосками называются простые рабочие станции с очень ограниченным набором программных приложений. Многие киоски имеют нестандартный форм-фактор, например являются встроенной системой или приставкой. Киоски часто используются как кассовые терминалы, для информационных презентаций, поиска данных в Интернет через браузер и для работы с пользовательскими приложениями. В некоторых случаях киосками пользуются сотрудники, в других — бизнес-клиенты или руководители. Системы развлечений Интернет и системы информационных презентаций также являются примерами киосков.

Специалист «базовых знаний»

Специалисты «базовых знаний» в основном пользуются офисными программными приложениями. Сюда, как правило, входит web-браузер, почтовый/PIM клиент и стандартный офисный набор: текстовый редактор, электронные таблицы, презентации, программа для рисования и, возможно, СУБД. Специалисты «базовых знаний», как правило, не пользуются специальными приложениями, но могут выполнять

определенные транзактные операции. Типичные должности, подпадающие под категорию «базовых знаний» — это служащие по вводу данных (клерки), фонотипистыи помощники по административной работе.

Специалист по обработке транзакций

Это довольно обобщенная категория, включающая в себя несколько подтипов. Специалист по обработке транзакций прежде всего решает практически идентичные и хорошо определенные задачи, иногда используя для этого специализированные программные приложения. Обычно это должности работников справочных служб, сотрудников отделов заказов, служб поставок и приемок либо центра технической поддержки.

Технический работник

Технические работники — разработчики программного обеспечения, разработчики аппаратных средств CAD/AM/CAE, системные и сетевые администраторы — как правило, используют свои настольные рабочие станции для проектирования, разработки или работы со специализированными приложениями проектирования, например с Интегрированной средой разработки (Integrated Development Environment, IDE). Обычно им нужны те же приложения, что специалистам «базовых знаний» — электронная почта, web-браузер и офисные программы.

Опытный специалист

Это — продвинутые пользователи, обладающие глубоким знанием офисных приложений, умеющие работать с их «замысловатыми» особенностями и функциями. Скорее всего, эти искушенные пользователи работают с множеством подключаемых устройств, а также с дополнительными программными средствами, повышающими эффективность работы. Опытных специалистов можно встретить в разных должностях — от исполнительных помощников до «технарей», следящих за компьютерами для отдыха. В маленьких компаниях опытные специалисты могут осуществлять системное администрирование или решать другие ИТ-задачи.

Составление списка активов настольной системы

Проведение надлежащей оценки текущей настольной среды — самый критичный аспект миграции. К информации, собранной на данном этапе, придется обращаться не один раз на всем протяжении процесса перехода. Список *активов настольной системы* можно подготовить в помощь анализу требований пользователя. Этот документ представляет собой опись аппаратных и программных средств настольной системы. Оценка аппаратных средств заключается в проверке скорости, емкости и компонентов/периферии настольных машин. В оценку программной среды пользо-

вателя входит опись используемого программного обеспечения, лицензий, а иногда и конфигурации. Последний аспект подробно рассматривается в главе 11.

В большинстве организаций уже имеется нечто похожее на список активов — опись, предоставленная поставщиками аппаратных средств. Если нет, то составить этот документ достаточно просто. Все, что нужно знать, это — серийный номер; название компьютера, марка и модель; марка CPU, модель и скорость работы процессора (МГц); объем оперативной памяти (RAM) и объем жесткого диска. Придется выяснить всю информацию об основных компонентах компьютера, а также подсоединенной периферии, включая съемные платы, их марки и номера моделей. Сбор этой информации в одном месте значительно ускорит процесс определения совместимости с аппаратными средствами, требуемыми Linux, и сформирует основу спецификации замены. В табл. 10.1 показано, как может выглядеть самый обычный список активов аппаратных/программных средств/лицензий.

Как будет видно далее, чем подробнее собранная информация об аппаратных средствах, тем легче определить совместимость с Linux. Большая часть представленной выше информации получена с помощью Диспетчера установленных устройств в Windows, однако рекомендуется фактически просмотреть аппаратуру, потому что названия в Диспетчере устройств часто отличаются от фактической модели платы. Если возможно, откройте корпус компьютера и спишите марку и номер модели (если он есть) съемных плат и материнской платы. Эта информация может быть указана в документации или товарных чеках. Все это поможет избежать разночтений, потому что под одной торговой маркой могут выпускаться разные типы моделей.

Далее выясните, какие программные приложения используются в организации и какую они обеспечивают функциональность. Попытайтесь составить максимально ясную картину того, какие именно задачи решают сотрудники на своих настольных системах. Эта информация поможет впоследствии сформировать требования к рабочим станциям.

Пользователи киосков, специалисты «базовых знаний» и специалисты по обработке транзакций обычно пользуются офисным пакетом, клиентом электронной почты, web-браузером и, возможно, некоторыми специализированными программами, например графическим редактором. Все эти потребности легко удовлетворяются с помощью открытых приложений, многие из которых работают как под Windows, так и под Linux. Для запуска офисных приложений воспользуйтесь OpenOffice.org, для работы в Интернет и с электронной почтой — Mozilla, для редактирования графики — GIMP. Сегодня эти альтернативные решения представляют собой законченные программные приложения: они имеют интуитивный графический пользовательский интерфейс (GUI), многофункциональны и интегрируются с оконным менеджером. Известно, что проект OpenOffice.org (http://openoffce.org) бесплатно распространяет открытый офисный пакет. Система может обрабатывать .doc файлы Word/Office XP/2000, электронные таблицы, презентации, рисунки, HTML (Hypertext Markup Language, язык обработки гипертекстовых файлов) и т. д. Mozilla (http://mozilla.org) —

Табл. 10.1. Примерный список активов компании Acme Widgets

Серийный номер, название компьютера, марка, модель	Марка CPU, модель, быстродействие, RAM, жесткий диск, CD	Сетевая, звуковая, видео карта, модем, WiFi, прочее	Принтер, сканер, внешние устройства USB	Операционная система, программное обеспечение	Лицензионные программные приложения
1001 LPTP_1001 HP Omnibook 6000	Intel PIII, 850 МГц, 256 М, 20 Гб, DVD/CD-RW	3com 10/100 «mini PCI» NIC и модем 56K, ATI Rage 8Мб, ESS Meastro, Orinoco 11 Мб/с WiFi PCMCIA	HP Photosmart 1 200 USB, Generic USB, диск 20 Гб, 256 Мб, плеер MP3 (сохранение USB)	Windows 2000 Pro, Graphic Design, Office App, Email, Web, Web Development	Windows 2000 Pro, Office 2000, Photoshop 5, Ultimate FTP, Dreamweaver
1002 LPTP_1002 Panasonic Toughbook CF-71	Intel PII, 300 МГц, 192М, 200 Гб, CD-ROM	Neomagic Gen. SB, Neomagic 2 Мб видео, Aironet 11 Мб/с WiFi PCMCIA	Kodak DC 240 USB-камера	Windows 98 SE, Graphic Design, Word Processing, Email, Web	Windows 98 SE, Photoshop 5, Word 6
1003 DKTP_1003 PC Compatible Desktop, Поставщик неизвестен	Dual PIII 700 МГц, 512 Мб, 60 Гб + 40 Гб внешний, CD-RW	2 Lite-on 10/100 NIC, NVIDIA Riva TNT 2, Trident SCSI	Внешний шлюз, 40 Гб SCSI, жесткий диск, USB, мышь/клавиатура	Windows 2000 Pro, Graphic Design, Office App, Email, Web, Web Development	Windows 2000 Pro, Office 2000, Photoshop 5, Ultimate FTP, Dreamweaver

надежный web-браузер, клиент электронной почты, новостей, IRC (Internet Relay Chat) и много что еще, собранное в одном наборе инструментальных средств. Известно, что GIMP — программа обработки графических изображений GNU (Graphics Image Manipulation Program) (http://gimp.org) — является open-source и предоставляет любые функции обработки фотографий, которые только могут потребоваться.

Опытные пользователи и технические служащие часто работают с патентованным программным обеспечением. Определение подходящих решений Linux для таких настольных станций займет больше времени. В некоторых случаях может понадобиться эмулятор для обеспечения на Linux функциональности, аналогичной настольной станции Windows. Впрочем, одно из преимуществ переноса таких пользователей заключается в их готовности к изменениям, некоторые из них, возможно, уже экспериментируют с альтернативными решениями.

Из списка активов для Acme Widgets видно, что пользователи в основном являются опытными техническими работниками.

Каталогизация форматов файлов

Полезно знать также форматы файлов, необходимые пользователям. Определите форматы файлов, используемые в организации, открытием приложений на рабочих станциях и считыванием файлов или их записью. Большинство программ имеют выпадающее меню в диалоговых окнах **Open File** (Открыть файл) и **Save File** (Сохранить), в которых видно, какие форматы файлов поддерживает программа. Многие из широко распространенных типов файлов (.doc, .xls, .ppt и .html) легко принимаются в Linux такими открытыми приложениями, как OpenOffice.org и Mozilla. Составьте список всех форматов файлов, относящихся к различным приложениям организации в помощь при поисках приложения-замены. В табл. 10.2 перечислены некоторые распространенные форматы файлов с соответствующими программными приложениями Windows и Linux, осуществляющими считывание этих форматов и запись в них.

Табл. 10.2. Распространенные форматы файлов

Тип файла	Расширение	Приложения Windows	Приложения Linux
Гипертекст	.htm, .html	Internet Explorer	Mozilla, Firefox, Konquerer
Документ	.doc, .rtf	MS-Word	OpenOffice.org, Writer, Abiword
Таблица	.xls	MS-Excel	OpenOffice.org, Calc, Gnumeric
Презентация	.ppt	MS-PowerPoint	OpenOffice.org, Impress
Персональное хранилище	.pst	MS-Outlook	Ничего, что работало бы непосредственно с .pst
Изображения .jpg, .gif, .bmp, .png	Photoshop	Gimp	
Audio/Video	.wav, .mp3, .mpg	Windows Media Player	X Multi-Media System (XMMS)

Спецификация функциональных требований

Документ функциональных требований сформирует базу для выбора программных приложений для Linux. Этот документ повторяет список активов, но в нем нет приложений, необходимости в которых не будет. Как правило, этот документ готовит руководитель проекта или ИТ-менеджер с правом принятия исполнительных решений, и он составляет основу для Заявок на предложения (Reques For Proposal, RFP) при поиске решений во внешних источниках. Документ функциональных требований также послужит основанием для закупок, одобряемых заинтересованными пользователями, с учетом того, что их потребности будут удовлетворены. Просмотрите этот документ вместе с сотрудниками во время их работы на компьютерах, чтобы убедиться в том, что ничего не упущено: простой операции — **Start Menu / Programs** — недостаточно. Если позволяет время, просмотрите содержимое жесткого диска и убедитесь, что нет никаких необычных программ. Оценка и документирование всей информации на данном этапе являются основой успешного перехода. В табл. 10.3 приведен пример упрощенного документа функциональных требований для компании Acme Widgets.

Для компьютеров головного офиса Acme Widgets требуется следующая функциональность, определенная по списку активов и с учетом форматов файлов из предыдущего раздела.

Табл. 10.3. Документ функциональных требований

Приложение	Функция
Набор для офиса	Должно поддерживать MS Document, расширенный текстовый формат (RTF), электронные таблицы и презентации
Работа с Web	Должно поддерживать HTML 4.0, CSS 2.0, Frames, Javascript
Разработка Web	Визуальный (WYSIWYG) HTML-редактор
Электронная почта	Должно поддерживать зашифрованные протоколы IMAP, POP и news. Должно управлять папками, обладать функциями ежедневника и уметь просматривать почтовые сообщения в формате HTML
Графика	Должно поддерживать форматы изображений TIF, PNG, GIF, JPEG, Postscript, Bitmap и PSD
Мультимедиа	Должно поддерживать форматы файлов мультимедиа WAV, MPG, MP3 и OGG

Проектирование настольной системы Linux

По завершении оценки настольных систем Windows можно приступать к проектированию замены настольного решения на базе Linux. Проект будет в очень большой степени зависеть от функциональных требований и, следовательно, создаваемый в данном разделе *документ функциональной замены* обеспечивает решения для требований, обозначенных на этапе оценки. Затем этот документ может быть перерабо-

тан, например в заказ на поставку (после выбора программных решений третьих сторон), или возвращен ИТ-персоналом руководителю проекта. Используя документ функциональных требований в качестве руководства, определите подходящее программное приложение Linux, которое бы удовлетворяло каждое требование каждого типа сотрудников организации. Эта информация будет включена в спецификацию функциональной замены.

Проектирование и планирование

Списки активов

Некоторые аспекты миграции могут потребовать определенного порядка следования; другие же смогут быть простыми и прозрачными. Подготовка списка активов поможет определить порядок задач для решения во время миграции.

Что касается основных приложений в приведенном примере требований, то тут уже известно, какие программные средства будут использованы в качестве замены обычных программ, однако в случае с патентованными приложениями может возникнуть необходимость поиска подходящей замены в Интернет. Freshmeat.net (http://freshmeat.net) — принятое компьютерным сообществом хранилище открытых и бесплатных программных продуктов. Если провести поиск в этом портале, то можно с удивлением обнаружить, что открытое сообщество уже давно предлагает именно то решение, без которого не обойтись при переходе с Windows на Linux.

Иногда, если кто-либо из сотрудников прошел специальное обучение работе с конкретной частью программного продукта, имеет смысл продолжать использовать патентованные приложения. Эти программы часто можно запускать в средах эмуляторов Win32 в рамках Linux. Сложность и цены подобных альтернативных «Виндусоидов» варьируются. Некоторые из них просто предоставляют библиотеки, необходимые для запуска приложений Windows из Linux; другие же создают *виртуальные машины*, позволяющие установить лицензионную копию операционной системы Windows. Если обнаружится, что требуется решение такого рода, обратитесь к CrossOver Office, WINE, VMWare или Bochs. Поиск на Google или Freshmeat также может дать положительные результаты.

Особо упрямых пользователей, не желающих менять операционные системы, можно убедить предоставлением им альтернативных программных решений, пока они продолжают работать на Windows. На сегодняшний день OpenOffice.org, Mozilla и GIMP бесплатно доступны в Windows. Такой тип промежуточного решения надлежащим образом обеспечит упорядоченный переход и упростит процесс обучения, поскольку пользователь уже будет знаком с некоторыми приложениями до фактического перехода на Linux.

Инструментальные средства и ловушки

Терминальные службы Linux

Другой возможностью для настольных рабочих станций Linux, подходящей для установки крупных сетей с большим количеством киосков и сотрудников, обрабатывающих транзакции, является переход к модели Терминальных служб Linux. Терминальные службы Linux — это способ экспорта настольных сред с центрального сервера в «тонкие» клиенты внутренней сети. Эта методология очень легко расширяется, и управлять ею проще, чем отдельными настольными станциями. Недостаток заключается в том, что они не вполне пригодны для мелких сетей, и их реализация достаточно сложна.

Если все-таки принимается решение о развертывании Терминальных служб Linux, то весьма неплохой идеей будет добавление резервного оборудования на терминальном сервере путем объединения его с отказоустойчивой машиной и регулярного создания резервных копий документов. Модель Терминальных служб Linux обходится намного дешевле с каждой вновь добавляемой системой в том, что касается оборудования, требуемого каждой рабочей станцией, и технического обслуживания. Эта модель хорошо подвергается расширению, поскольку добавление в сеть очередного пользователя заключается в простом создании на терминальном сервере очередной учетной записи и подключении к сети очередного «тонкого» клиента. Впрочем, не следует забывать о том, что проектирование Терминальных служб Linux требует довольно много времени на планирование и тестирование. Однако выгода видна сразу: администрирование сосредотачивается всего на одном компьютере. Терминальные службы Linux — лучший выбор в плане управляемости, но их невозможно (или нежелательно) устанавливать во всех случаях без исключения; мелкие, специально сконфигурированные сети — яркий тому пример. Более подробная информация о Терминальных службах Linux размещена на домашней странице проекта (http://ltsp.org).

Некоторые поставщики также предлагают Linux-версии своих программных продуктов для Windows. Если компания приобрела лицензию на приложение, поддерживаемое поставщиком в Linux, возможно, что поставщик согласится перевести лицензию. В некоторых случаях бинарные файлы Linux могут уже быть включены в установочный диск.

Для всех прочих приложений Windows, которые желательно сохранить, придется воспользоваться уже упомянутыми решениями, работающими «как Windows». Вообще говоря, простые программные приложения, работающие на более старых версиях Windows (например, Windows 98), как правило, прекрасно работают с WINE, бесплатно предоставляющим «родные» библиотеки для приложений Windows в Linux. Достаточно ввести в Linux команду **wine some.exe**. Более крупные приложения, требующие тщательно продуманной локальной установки, например MS Office 2000, потребуют CrossOver Office либо установки в виртуальную машину. Поскольку потребности компании Acme Widgets легко удовлетворяются обычными пакетами Linux, то здесь авторы больше не будут упоминать гибридные решения. Подробности о настольных средах Linux и обычных программных приложениях см. в главе 11 «Внутренняя структура настольной рабочей станции Linux».

Пользовательские профили Acme Widgets потребуют установки двух разных операционных систем Linux. Для сотрудников с «базовыми знаниями» потребуется базовая установка настольной системы Linux, подготовленная для комфортной работы на старом оборудовании. Для опытных пользователей потребуется установка Linux «для разработчиков», предоставляющая пользователю библиотеки и инструментальные средства разработки, такие как IDE. Программа установки Linux, поставляющаяся вместе с дистрибутивом, обеспечивает опции для выбора этих типов профилей операционных систем, а также более «ступенчатые» окна настройки предпочтений. Установить операционную систему Linux на компьютер, соответствующий всем указанным описаниям, сможет любой обученный сотрудник службы технической поддержки. Эти профили операционных систем будут использоваться для создания спецификации функциональной замены.

Спецификация функциональной замены

Приступим к созданию спецификации функциональной замены и документа функциональных требований. Последний, по существу, приводит программу Linux обратно к функциональности, которую нужно заменить. В крупных установках можно создать документ замены для каждого пользовательского профиля, однако для рассматриваемых здесь целей достаточно сказать, что опытные специалисты имеют ту же конфигурацию, что и специалисты с «базовыми» знаниями, плюс дополнительные инструментальные средства разработки. Пример такого документа показан в табл. 10.4.

Табл. 10.4. Документ функциональной замены

Тип пользователя/ Профиль операционной системы	Программное приложение	Программа Linux
Сотрудник с «базовыми знаниями»/ Настольная система	Офисный пакет	OpenOffice.org
Сотрудник с «базовыми знаниями»/ Настольная система	Работа в Интернет	Mozilla
Сотрудник с «базовыми знаниями»/ Настольная система	Электронная почта	Mozilla
Сотрудник с «базовыми знаниями»/ Настольная система	Графика	The GIMP
Сотрудник с «базовыми знаниями»/ Настольная система	Мультимедиа	XMMS
Опытный сотрудник/Разработка	Web-разработка	Quanta, Scream

Поскольку дистрибутив Linux обязательно должен быть завершенным, то все программы замены уже включены в популярные дистрибутивы, включая Интегрированные среды разработки Web-приложений. Предоставление их пользователям заключается лишь в выборе их во время установки.

Компоновка компьютеров для обучения

Если в вашей маленькой компании всего несколько сотрудников и компьютеров, то этот раздел можно пропустить. Для крупных организаций, стоящих перед необходимостью развертывания десятков настольных рабочих станций, потребуется создание прототипов профилей операционной системы на нескольких дополнительных компьютерах, предназначенных для обучения персонала. При этом появляется возможность «убить сразу трех зайцев»: ИТ-менеджер сможет разработать методологию установки для наблюдения за этими машинами; появятся рабочие станции, на которых можно протестировать эти системные профили; появится «песочница», в которой пользователи смогут благополучно «играть». Зеркалирование жестких дисков, создание установочных профилей с помощью Kickstart от Red Hat, сетевые установки и установки с CD-ROM — опции, доступные в любом широко распространенном дистрибутиве Linux. Обратитесь к этим опциям, если необходимо обеспечить полдюжины и больше настольных рабочих станций. Для Acme Widgets воспользуемся только методом установки с CD-ROM и после установки создадим диск Kickstart, на случай, если в будущем для компании придется создать схожую машину. Google предлагает много примеров установки Kickstart.

Тестирование настольной системы Linux

После компоновки компьютеров для обучения их можно испытать (протестировать) путем разработки плана проведения испытаний, подобного описанному в главе 1. План испытаний должен проверить соответствие системных профилей спецификации замены. План испытаний должен подтвердить, что все необходимое для данного пользовательского профиля программное обеспечение установлено и работает без дополнительных (не установленных) библиотек или программных пакетов. План должен проверить интуитивность и простоту использования оконного менеджера по умолчанию: эту программу можно настроить специально под нужды профиля конкретного пользователя, например путем доступности в панели инструментов самых популярных программ и приложений. В следующей главе этот вопрос будет рассматриваться более подробно.

Убедившись, что установка соответствует требованиям системных профилей, запишите шаги, которые были для этого сделаны, и повторите процесс на оставшихся системах. Это — самый простой способ, если речь идет о нескольких компьютерах. Если же машин очень много, то можно, как уже отмечалось, воспользоваться методом Kickstart либо методом зеркального отображения диска на другие компьютеры. В маленькой сети, подобно рассматриваемой, повторить одну и ту же установку три раза не составит труда.

После переноса данных пользователей на новые машины Linux авторы намерены рассмотреть испытания и план их проведения более подробно.

Перенос данных программных приложений и профилей

На данном этапе миграция фактически заключается только в экспортировании и резервировании пользовательских данных, в установке Linux с последующим импортированием и копированием пользовательских данных в новую систему Linux. После оценки, проектирования и испытаний проекта должно быть ясно, что требует резервирования и какие программные приложения должны быть доступными на настольной рабочей станции Linux. Профили операционной системы Linux испытаны, и теперь приблизительно известно, сколько времени занимает их установка на машину. Переход к следующему этапу — вопрос согласования времени с пользователями.

Время на установку Linux на пользовательские машины будет варьироваться, в зависимости от профессионализма технического работника, но, как правило, на современном оборудовании (процессор порядка 1 ГГц и 256 Мб оперативной памяти) установка займет от 2 до 4 часов на каждый компьютер. При добавлении большего количества машин это время будет сокращаться, поскольку можно осуществлять параллельную установку с нескольких наборов CD-ROM дистрибутива. Время установки также сокращается при переходе на другие установочные среды, например

сетевую установку или Kickstart. Поскольку автоматизированных программ для переноса межплатформенных приложений не существует, то большую часть всего процесса приходится выполнять вручную. Именно поэтому некоторые ИТ-менеджеры предпочитают, чтобы техники осуществляли перевод пользовательских компьютеров на Linux в нерабочее время.

Резервирование данных с настольных рабочих станций

Простыми вариантами резервирования, доступными для мелких и средних размеров сетей, являются сетевое резервирование, резервирование на жесткий диск USB либо резервирование через CD-ROM (если на машине установлен пишущий CD-ROM). Каждый способ имеет свои преимущества, в зависимости от размеров сети и имеющихся ресурсов. При достаточной емкости запоминающего устройства на файловом сервере для охвата данных всех пользователей сразу сетевое резервирование будет самым оперативным способом. Резервирование на внешнем жестком диске USB, возможно, самый простой способ, поскольку оно не задействует никаких других служб. Резервирование через CD-ROM, пожалуй, самый дешевый способ в том, что касается носителей, однако объем одного диска не более 650 Мб и для резервирования даже одной машины может понадобиться несколько дисков. Еще существует вариант резервирования через DVD, но в этом случае понадобится устройство DVD-RAM и носитель, который может дорого стоить и работает медленно. При существующих емкостях и ценах жестких дисков сетевое резервирование или использование жестких дисков USB, вероятно, является наиболее приемлемым решением. Для крупных сетей с большим количеством настольных рабочих станций файловый сервер не только рекомендуется, но и является необходимым.

Несмотря на то, что резервирование пользовательской почты, адресной книги и закладок для каждого приложения будет варьироваться, все пользовательские данные, а также версии этих ресурсов для пользователя, отформатированные под Windows, будут сохранены в пользовательском каталоге в C:\Documents and Settings. Следовательно, как правило, достаточно резервирования домашних каталогов для восстановления из них данных при необходимости возврата в систему Windows. Перед выполнением резервирования откройте каждое приложение на рабочей станции пользователя и экспортируйте почту, адресную книгу и закладки в текстовый формат с помощью функции экспорта, имеющейся в программе. Сохраните экспортированные файлы на рабочем столе машины пользователя. Можно попросить пользователей сделать это самим, предварительно представив короткие инструкции в виде памятки.

Папка Documents and Settings содержит подпапку для каждого пользователя системы. В свойствах каждой подпапки указан ее размер. Сохраните папки на резервном носителе. Как обсуждалось выше, возможностей резервирования очень много, и они зависят от настроек и ресурсов. Также зарезервируйте каталог All Users. В более старых системах (Windows 95/98) в дополнение к резервированию пользовательских каталогов потребуется проверить диск C: и любые физические дисководы или разделы на

предмет блуждающих папок конфигурации. В системах NT и более современных их быть не должно, поскольку это — многопользовательская платформа, однако на компьютерах с системами Windows 95/98, не являющихся многопользовательскими, программы обычно сохраняют данные в каталоги программ — C:\Program Files.

Теперь, в каждой зарезервированной пользовательской папке должна находиться электронная почта, закладки, адресные книги, настройки профилей и пользовательские данные, необходимые для перевода пользователя на платформу Linux и обратно.

Установка Linux

Как упоминалось выше, процесс установки Linux довольно прост. Можно выполнить сетевую установку, установку с CD-ROM либо зеркально отобразить жесткие диски с компьютеров для тестирования. Для компьютеров Acme Widgets установка осуществляется напрямую с CD-ROM с Fedora Core Linux. Дистрибутив Fedora Core можно скачать с сайта http://fedora.redhat.com. Две системы будут установлены в режиме «для разработчиков» (Development), а третья — в «настольном» (Desktop). После установки на каждую систему будет установлена утилита apt for rpm, доступная с http://freshrpms.net/apt, и запуск apt-get update; apt-get-upgrade; apt-get dist-upgrade обновит пакеты под их самые последние версии.

Импортирование профилей пользователей и предпочтений

По завершении установки создайте учетные записи пользователей и зарегистрируйтесь как пользователь. Смонтируйте коллективно используемый сетевой ресурс, носитель USB или носитель CD-ROM и запустите копирование файлов пользователей в их пользовательский каталог Linux. Откройте каждое приложение и выполните процедуру импортирования. Например, для импортирования экспортированного файла mbox в Mozilla закройте Mozilla и скопируйте файл в <mozilla_userdir>/Mail/Local Folders. После этого он будет доступен в Local Folders в рамках Mozilla Mail. В следующей главе эта тема описана более подробно; сейчас дано только общее представление.

Обучение пользователей настольных систем

В обучение должны входить такие темы, как навигация по рабочему столу, открытие программных приложений и монтирование CD-ROM. Современные настольные рабочие станции, работающие под Linux, — очень устойчивые и интуитивно понятные. Переход на них — все равно что переход на любую другую ОС. Открытие командной строки и обучение пользователя работе с несколькими базовыми командами UNIX (**cd**, **pwd**, **ls**, **cp**, **mkdir** и **rm**) — возможно, самый быстрый способ его обучения

работе с файловой системой. Затем откройте Nautilus и покажите пользователям графический способ навигации в файловой системе.

Обучающие руководства

Как такового, набора обучающих руководств не существует. Все зависит от способностей самих пользователей. Поощряйте их делать записи и задавать вопросы. Покажите им, как находить ответы в документации, поставляемой с дистрибутивом, в электронных поисковых системах, например http://google.com/linux, и хранилищах, подобных Linux Documentation Project (http:///linuxdoc.org).

Базовое обучение работе с Linux группы пользователей можно осуществить за один день, а инструктор, нанятый в консалтинговой обучающей компании, либо технический работник, выполняющий установку, могут потратить несколько часов на эффективное обучение отдельных пользователей с целью ускорения понимания ими материала. Если сеть небольшая, то целесообразно обучение «один на один». В более крупных сетях, возможно, потребуется спланировать групповые занятия с инструктором, в то время как ИТ-персонал будет заниматься резервированием и подготовкой компьютеров. Занятия можно запланировать на любую пятницу с тем, чтобы в выходные дни технические работники могли отладить все обнаруженные ошибки, обеспечив пользователей к понедельнику новыми системами. При этом время простоя будет минимальным. Возможностей много, но основной задачей является обеспечение пользователей возможностью самим находить ответы на интересующие вопросы. Определенное поощрение и поддержка на данном этапе играют очень важную роль, и пользователи очень скоро безболезненно перейдут на систему Linux.

В каких-то случаях обучение будет необходимо, в каких-то оно не потребуется вообще. Процесс миграции можно растянуть на продолжительное время, если того требует производственная необходимость. В сравнительно небольшой компании специалиста можно пригласить в день установки новых программных приложений. Все это должно быть отражено в плане перехода и будет зависеть от спецификации функциональной замены. Ниже приводится еще несколько полезных советов.

Воспользуйтесь списком программных приложений Linux, планируемых к развертыванию, и, исходя из функциональности, составьте сравнительную таблицу эквивалентов Windows приложениям Linux. Определите сходства и различия. В результате этого процесса можно составить документы качества и одновременно начать подготовку материалов для будущих курсов обучения. Для начала выполните большое количество простых заданий, а оставшееся время отведите на составление точных описаний того, как осуществлялось выполнение того или иного процесса, задокументированного на этапе оценки настольной системы; в качестве иллюстраций полезно включать снятые с экрана изображения различных диалоговых окон программ.

Помните о том, что пользователей нужно постоянно «подталкивать» к изменениям (так как люди обычно избегают перемен), но здесь важно не переусердствовать.

Эту задачу можно решить с помощью оценок, планирования и донесения своих целей до нужных адресатов. Задавайте вопросы, особенно когда они касаются производственного процесса. Не бойтесь потратить время на нахождение лучшего способа поддержания бесперебойного и беспроблемного хода работы при использовании разных программных приложений.

Если что-то из перечисленного не получается или не выполнимо, то в Интернет можно найти локальные Группы пользователей Linux (Linux Users Groups, LUG) и форумы. Центры образования/обучения также могут иметь специализированные материалы по различным программным приложениям, планируемым к развертыванию. В Группах пользователей Linux можно найти даже инструкторов, главное — не останавливаться на достигнутом и искать то, что необходимо.

Отличия настольных рабочих станций Linux от Windows

Большинство отличий настольных рабочих систем Windows от Linux имеют отношение к среде. То есть, они (различия) — фундаментальные и, как правило, не видны «невооруженным» глазом. Подробно они рассматриваются в следующей главе. Впрочем, большинство различий, что называется, косметические. В двух наиболее распространенных настольных системах для Linux — GNOME и KDE — имеется навигационная панель с конфигурируемым меню пуска, панелью задач и панелью инструментов, которую можно настроить на использование кнопок быстрого запуска приложений и утилит; многие из них поставляются в дистрибутиве по умолчанию, и в панели Preferences (предпочтения) их можно активизировать или отключать. Поведение таких настольных систем по большей части аналогично поведению настольных систем под Windows. Уже говорилось о том, что файловая система отличается от имеющейся в Windows, и ее придется рассматривать особо.

В Windows домашние каталоги хранятся в C:\Documents and Settings, а в Linux эквивалентный каталог — /home. Поскольку щелчок кнопки мыши на любом приложении в диспетчере файлов в системе Linux отправляет пользователя в его домашний каталог, то в этом случае каталог /home/<username>/ — хорошее место для копирования оставшихся резервных данных. Скрытые файлы, начинающиеся с точки, по-прежнему останутся скрытыми: большинство из них представляет собой каталоги конфигурации. Их можно внимательно изучить и, возможно, импортировать дополнительные настройки из других приложений. Примером может служить настройка клиентов мгновенного обмена сообщениями.

Перенос данных сотрудников компании, обрабатывающих транзакции, и их обучение работе с новыми программными приложениями, вероятно, будут самыми простыми задачами, потому что в течение рабочего дня они используют меньшее количество программ, и, как правило, ограниченный набор функций этих программ. Труднее всего перевести на новую систему опытных работников, не только из-за более широкого спектра приложений, с которыми они работают, но и из-за обширного

набора используемых функций в этих приложениях. Впрочем, «продвинутые», как правило, всегда готовы узнавать что-то новое.

Внимание ко всем деталям и подробностям, опять же, стимулируется спецификацией технических требований (техническим заданием), спецификацией функциональных требований и тем, насколько они соответствуют новым программным приложениям. В некоторых случаях различия могут быть принципиальными, а иногда — даже не заслуживающими внимания. К каждому переходу предъявляются свои особые требования.

Чем обширнее развертывание, тем более целесообразно осуществлять все поэтапно. В небольшом офисе установить и настроить каждую систему под требования конкретного пользователя легко, но когда настольных станций больше 15, документация, описанная выше, придется очень кстати.

Различия файловых систем

В Windows «C:» — самый верхний каталог первого раздела жесткого диска. В Linux он представлен левой косой чертой «/» и обычно называется *корневым* каталогом; *все остальное* в Linux выходит именно отсюда. *Все* в Linux — это файл. Существует семь типов файлов, однако пользователям целесообразно иметь представление только о файлах устройств, регулярных (обычных) файлах и каталогах. Первый уровень под «/» содержит системные папки, с которыми работает администратор. Как упоминалось ранее, в каталоге /home хранятся домашние каталоги. Каталог /dev содержит файлы устройств для всего оборудования и устройств системы. В каталоге /usr сохранены файлы коллективного пользования, а множество доступных пользователям бинарных файлов командной строки хранятся в каталоге /bin. Для работы с CD-ROM или USB в Linux их необходимо *смонтировать* в определенном месте файловой системы. В настоящее время имеются утилиты автоматического монтирования, устанавливающие съемные носители в каталог /mnt. В Windows доступ к CD-ROM осуществляется через каталог D:, а в Linux — через /mnt/cdrom.

Для пользователей процесс перехода можно упростить присвоением знакомых имен папок и создания на рабочем столе «быстрых клавиш» для их открытия, например «Быстрая клавиша для Мои документы», а также созданием символических ссылок на часто используемые элементы.

Прочие различия

Другие аспекты Linux объяснить не совсем просто, поскольку в Windows им нет эквивалентов. Примерами могут служить виртуальные рабочие столы, виртуальные консоли и различия в менеджере окон. Изменить разрешение монитора в Linux можно одним движением; также имеются «горячие» клавиши для перезапуска сеанса X-Windows. Использование устройств — понятие, к которому тоже нужно привыкнуть, особенно к устройствам USB. К примеру, если пользователи предполагают работать со съемными носителями, то в этом случае необходимо настроить autofs или утили-

ты автоматического монтирования и разместить на рабочем столе быструю клавишу, чтобы вся задача заключалась в подключении и просмотре. Многое здесь зависит от того, как люди работают со своими системами. Разные отделы компании имеют разные потребности. Для определения необходимости создания быстрой клавиши для выхода на внешнее USB-устройство в системе того или иного пользователя следует в очередной раз проконсультироваться со спецификацией функциональных требований.

Подсказки

Сбор и анализ трафика DHCP

- **Оконные менеджеры (Window Manager)** — в Linux система X Window обеспечивает оконную среду, а диспетчеры окон представляют собой уровень абстракции между пользователем и оконной средой. Для Linux существует множество программ-оконных менеджеров. Иногда оконные менеджеры называют также «диспетчерами окон».
- **Виртуальная рабочая станция (Virtual Desktop)** — Большинство оконных менеджеров в Linux имеют множественные рабочие столы. Переходить от одного к другому можно с помощью апплета в панели меню рабочего стола.
- **Виртуальная консоль (Virtual Console)** — Нажатием **Ctrl+Alt+F2** можно перейти к виртуальной консоли от диспетчера окон и зарегистрироваться в командной строке. Выход к другим консолям осуществляется нажатием той же комбинации клавиш с **F3** по **F6**. Нажатие комбинации **Alt+F7** возвращает пользователя назад в диспетчер окон.

Эквиваленты альтернативным программным приложениям

Пользователи Windows привыкнут к определенному набору приложений для выполнения различных необходимых функций. В Linux эти функции могут называться иначе. Новое правило присвоения имен — одна из самых сложных тем. Чем больше программных приложений добавляется, тем ближе к переполнению «банк имен». Для приложений, замещающих программы Windows, можно использовать пиктограммы Windows для упрощения ассоциаций новых имен со старыми. Для крупных компаний безусловно полезным будет создание таблицы приложений и ее сохранение в корпоративной сети. Простую таблицу эквивалентов можно держать в совместно используемом ресурсе и связываться с ним через рабочий стол пользователя либо разместить в каталоге /etc/skel, похожем на каталог All Users в Windows. Размещение файлов в /etc/skel распространит обычные файлы настройки пользователей для всех новых пользователей.

Огромное множество программных приложений, у каждого из которых свое имя, — одно из самых сложных препятствий для всех, кто осуществляет переход с Windows на Linux. В Linux программ и утилит устанавливается больше, чем в Windows. В главном меню можно сделать выбор из большего количества вариантов.

Как уже отмечалось, существует много полнофункциональных программных приложений, и для решения самых обычных задач (составление документа, работа с электронной почтой, поиск в Интернете или работа с графикой/разработка программ) существует очень много разнообразных опций.

Также можно говорить о бесчисленных играх, инструментальных средствах конфигурирования и мониторинга, научных программах и средствах построения диаграмм. Если установлена утилита apt, можно запустить **apt-get install synaptic** и дать пользователям возможность выбора из огромного хранилища программных приложений.

Каждый дистрибутив Linux можно настроить с помощью инструментов, аналогичных apt-get, что позволит устанавливать новые приложения простым вводом короткой команды от имени root в окне консоли. Существует несколько вариантов apt-get, например urpmi от Mandrake и yum от Red Hat. Эти утилиты значительно облегчают рутину настройки, администрирования и обеспечения пользователей новыми программами; в Windows они не имеют эквивалентов.

Получение справок

Несмотря на наличие крупных коммерческих организаций технической поддержки, вряд ли люди будут к ним обращаться, если речь не идет о работе на уровне крупного производства. Ответы практически на все возникающие вопросы можно найти в документации, прилагаемой к дистрибутиву, в Интернет или из других источников (LUG или независимые консультанты). В пакете с каждым дистрибутивом имеются опции «Справка» (Help) с документацией по многим аспектам GUI (графический пользовательский интерфейс). Кроме этого каждый добавляемый в систему пакет устанавливает свою собственную документацию на страницы **/usr/share/doc** или **man** (руководство пользователя). Например, в командной строке можно ввести **man bash** для выхода на страницу руководства для оболочки BASH. Дополнительная информация о BASH имеется в каталоге /usr/share/doc/bash/some_version.

В Интернет поиск можно осуществлять в рассылках, группах новостей, досках объявлений и в соответствующих статьях. Часто решение проблемы заключается только в нахождении уже кем-то предложенного решения. Если задача сравнительно простая, то для экономии времени достаточно просто заглянуть в Интернет и найти нужное решение. Точно так же можно искать Группы пользователей Linux и консультантов простым поиском по своей географической области и LUG в Google. Либо сама сфера деятельности и консультант по Linux предложит вам помощников. Выйти из затруднительного положения можно всегда.

Развертывание настольных систем Linux

В небольших организациях развертывание — это описанный выше процесс резервирования компьютера пользователя, установка Linux и возврат данных пользователя в новую настольную систему. В крупных организациях, где обслуживание «один на один» не приемлемо, очень важно документировать все процессы. При этом желательно уметь прогнозировать многие из распространенных проблем, с которыми придется столкнуться пользователям.

При переходе на новые системы вся функциональность старых должна быть сохранена, но она будет иначе структурирована, иначе именована, и на привыкание к новой среде, несомненно, потребуется определенное время. Возможно, что в течение какого-то периода за пользователями придется «понаблюдать», и хотя бы на первую неделю после начального развертывания технический работник всегда должен быть доступен по телефону, на случай возникновения вопросов. Не исключено, что возникнет необходимость в рекомендациях по работе с принтерами и настройке старых учетных записей в системах мгновенной передачи сообщений. В этом смысле было бы полезно спрогнозировать возможные вопросы.

Документация

Записывайте все возникающие вопросы. В данной главе о документации было сказано немного, потому что любая созданная спецификация функциональных требований, спецификация функциональной замены, список активов или таблица регистрации приложений служат прекрасным материалом для справок. Для пользователей можно составить краткие тематические пояснения, например по настройке учетных записей электронной почты или учетных записей сетей мгновенного обмена сообщениями, и разместить их в общедоступном месте сети. Таким образом, нагрузка на службу технической поддержки будет радикально сокращена. Обученный приглашенный консультант (наученный опытом) обязательно об этом позаботится.

Резюме

В данной главе представлен общий обзор и введение в некоторые «непонятности», вероятность столкновения с которыми на пути перевода настольных рабочих станций Windows на платформу Linux велика. Представлены стратегии, которые авторы сочли наилучшими для облегчения процесса перехода. В главе описана оценка существующей настольной среды, проектирование и тестирование новой среды, перевод в нее пользователей, их обучение и, наконец, использование новых компьютеров и пользователей Linux в обычной работе. Конечно, в отличие от традиционных рекомендаций и способов, данную стратегию можно изменить под потребности каждой конкретной организации; она больше напоминает сборник практических «рецептов». Если следовать предложенным шагам, то переход с одной платформы на другую будет

осуществлен с минимальными потерями; можно сказать, что любое изменение предполагает рост числа проблем, но при грамотном и заблаговременном планировании их всегда можно избежать. Теперь пользовательский интерфейс вполне подготовлен и можно начинать...

Данная глава послужила руководством по миграции. Следующая посвящена подробностям настройки настольной системы Linux.

Краткое резюме по разделам

Оценка текущей настольной среды

- ☑ Составьте списки активов аппаратных/программных средств/лицензий.
- ☑ Разработайте спецификацию функциональных требований для определения цели, к которой следует двигаться.
- ☑ Для облегчения задачи проектирования определите типы пользователей и форматы файлов.

Проектирование настольной системы Linux

- ☑ Учитывайте сетевую топологию и потребности пользователей.
- ☑ Идентифицируйте сопоставимые решения в Linux.
- ☑ Разработайте спецификацию функциональных замен.
- ☑ Создайте профили операционной системы и, учитывая их, соберите компьютеры для обучения/тестирования.

Тестирование настольной системы Linux

- ☑ Следуйте плану проведения испытаний для того, чтобы профили операционной системы в полной мере соответствовали требованиям.
- ☑ Протестируйте вручную часто используемые программные приложения.

Перенос данных программных приложений и профилей

- ☑ Согласуйте время работы на компьютерах пользователей.
- ☑ Зарезервируйте пользовательские данные, установите Linux и скопируйте данные в новую систему.

Обучение пользователей настольных систем

- ☑ Спланируйте обучение пользователей.
- ☑ Рассмотрите системные различия, различия интерфейсов, часто используемые программные приложения и основные функции командной строки.
- ☑ Проинструктируйте пользователей о способах получения справок и помощи.

Развертывание настольных систем Linux

- ☑ Документируйте все.
- ☑ В течение первой недели после развертывания подготовьтесь к потоку вопросов к службе технической поддержки.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма «**Ask the Author**»). Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: Где взять программное приложение?

О: Для Linux существуют тысячи программных приложений и столько же мест, откуда их можно взять. Попробуйте поискать готовое к установке программное обеспечение в Интернет.

В: Откуда можно скачать новые приложения?

О: Freshmeat (www.freshmeat.net) и SourceForge (www.sf.net) — два замечательных портала, откуда можно скачать новые открытые приложения.

В: Стоит ли пытаться осуществить перевод настольной рабочей станции с одной платформы на другую за один день?

О: Для пользователей переход за один день может оказаться затруднительным. В принципе — возможно, но далеко не все и не всегда идет по запланированному сценарию. В большинстве случаев лучше всего распределить сбои между пользователями и дать им время на устранение неожиданных проблем.

В: Как связан Коэффициент окупаемости инвестиций (КОИ или ROI в англоязычной терминологии, Return On Investment) с переводом настольных рабочих станций с платформы Windows на Linux?

О: Трудно ответить на этот вопрос, потому что существует очень много способов расчета КОИ. И некоторые преимущества Linux не так просто выразить в долларах. Любая миграция изначально стоит времени и денег, но успешные миграции со временем окупаются и экономят средства в том, что касается приобретения лицензий и технического обслуживания. Для организаций, рассматривающих варианты приобретения дорогостоящих лицензий на патентованное программное обеспечение, переход на Linux и открытые программные средства практически всегда означает денежную экономию.

Глава 11

Внутренняя структура настольной рабочей станции Linux

Темы главы:

- Традиционные настольные среды
- Серверы X Window и Диспетчеры управления окнами
- Клиенты электронной почты и управления персональной информацией
- Web-браузеры
- Офисные пакеты
- Запуск приложений Windows на Linux

☑ Резюме

☑ Краткое резюме по разделам

☑ Часто задаваемые вопросы

Введение

Всякий раз, когда начинаются дискуссии на тему Linux, многие консультанты и поставщики делают упор на преимущества. Техники упирают на привлекательные с точки зрения продаж аспекты, такие как общая устойчивость системы, возможности расширения средств защиты, а также на тот факт, что Linux помогает компаниям экономить деньги на лицензиях.

Большинству же конечных пользователей все это не очень интересно; их волнует лишь процесс работы с настольными рабочими станциями. По словам самих пользователей, им нужна настольная система, которая бы была «интуитивной» и одновременно «незамысловатой». То есть, по сути, им нужна система, подобная той, с которой они уже давно знакомы. Microsoft и Apple в этом смысле преуспели: им удалось убедить пользователей в том, что их интерфейсы — *всегда* интуитивны и просты в работе, даже несмотря на то, что за последнее десятилетие они радикально изменили интерфейсы своих продуктов.

Помните о том, что работа заключается в удовлетворении запросов «среднестатистического конечного пользователя». Такие пользователи захотят узнать, как получить доступ к производительным и эффективным программным приложениям после регистрации в системе, как размещать файлы на жестком диске и как их открывать с помощью соответствующих программ. И все. Кроме этого их мало что интересует...

Поэтому в данной главе авторы намерены рассказать о том, как выбрать подходящую настольную среду и диспетчер окон для клиентов. Ознакомившись с материалами главы читатели смогут рекомендовать программы электронной почты, управления персональной информацией (Personal Information Management, PIM) и web-браузеры с тем, чтобы пользователи могли осуществить перенос информации с таких приложений, как Outlook, Outlook Express и Internet Explorer. Пользователи, несомненно, намерены работать с файлами Word, PowerPoint и Excel, поэтому им будет нужно порекомендовать идеальный во всех отношениях офисный пакет для Linux, а также дополнительные открытые решения. К концу главы сисадмины должны быть уверены в том, что производительность их сотрудников на рабочих местах не снизится.

Традиционные настольные среды

«Итак, Linux работает в командной строке, правильно? Ну, то есть, здесь нет графической среды как в Windows, да?» Любой человек, мало-мальски знакомый с Linux, сочтет такой вопрос глупым. Однако такие вопросы периодически поступают от заинтересованных в переходе на Linux. Одна из причин того, что вопрос еще жив, заключается в том, что одно время версии UNIX (как и любая другая операционная система на тот момент) не имели графического интерфейса пользователя (GUI). В то время, когда появились Macintosh и Windows, системы UNIX для среднестатистического пользователя казались чем-то очень далеким.

С ростом популярности Linux подобных вопросов постепенно становится меньше. Однако по-прежнему одной из первых проблем, с которой придется столкнуться, является выбор для пользователей подходящей настольной среды.

Итак, требуется настольная станция, о которой заказчики думают, что она:

- проста в использовании (и обучении);
- легко настраивается под конкретного пользователя;
- легко расширяется и обновляется.

Конечно, слово «легко» в данном случае весьма относительно, но как консультанту вам придется рассказать про сравнительные преимущества и недостатки наиболее распространенных настольных сред. Следует помнить о том, что в любой операционной системе UNIX всегда существует более одного способа выполнения любой операции. И вам предстоит предоставить клиенту управляемый набор вариантов. Вы также должны быть готовы скорректировать свои рекомендации (в соответствии с требованиями заказчика).

Самыми распространенными настольными средами являются Gnome (www.gnome.org) и KDE (www.kde.org). Существуют и другие среды, в число которых входит Common Desktop Environment (Общая рабочая среда, CDE) и Xfce. Ниже подробно рассматривается каждая из этих сред. Однако хотим предупредить: не стоит думать, что к каким-то из этих настольных сред отношение будет предвзятое. Авторы предпочитают среду, предоставляемую диспетчером окон Blackbox, в основном потому, что их интерфейс «чище» и не пытается имитировать Windows. «Правильный» выбор настольной среды зависит от разных факторов, большинство из которых могут описать только пользователи.

Рекомендуя настольную среду, избегайте рассуждений на тему «Gnome против KDE». Просто найдите время продемонстрировать пользователям обе среды. Предоставьте им право, так сказать, «пробной поездки». Ведь, только тогда клиенты смогут сделать сравнительно осознанный выбор. Поэтому, при ознакомлении с главой, учитывайте слабые и сильные места каждой настольной среды.

Gnome

Настольная система Gnome разработана проектом GNU Project (www.gnu.org), создавшим большое количество программного обеспечения для различных платформ, включая Windows, Linux и Macintosh. На рис. 11.1 показан рабочий стол Gnome в системе Red Hat Linux.

При этом следует учитывать, что показанный на рис. 11.1 рабочий стол имеет настройки по умолчанию. Его можно настроить так, что вид будет во многом другим. Рекомендуя Gnome, делайте упор на следующее:

- Система ассоциируется с GNU Project (www.gnu.org). Следовательно, Gnome лицензирован по Общедоступной Лицензии GNU (General Public License, GPL), а это значит, что код разработан по открытой и свободно доступной технологии.

- Многие приложения написаны под Gnome и используют библиотеки Gnome. Gnome гордится тем, что является настольной средой, открытой для различных сред разработки, включая C, C++, Tcl/Tk и Python. Использование Gnome GPL — также «плюс» большому разнообразию программных приложений, поддерживаемых Gnome.
- Код редактировался рабочей группой, участвовавшей в создании GnuPG (по сути, открытый PGP) и многих других приложений.
- Разработчики настольной среды Gnome предприняли специальные шаги по выяснению того, что Gnome доступен для людей с ограниченными физическими возможностями.
- Если клиенты хотят пользоваться такими программами, как Galeon, Evolution и GnomeMeeting, то Gnome можно порекомендовать в качестве настольной системы по умолчанию.
- Gnome чаще других программ считается «чище», потому что по умолчанию эта система предоставляет меньше функций.

Настольная среда Gnome кажется не настолько интегрированной, как KDE. Более того, традиционно приложения Gnome создавались медленнее, нежели приложения KDE. Однако многие поставщики приняли систему Gnome из-за ее ассоциаций с GNU, и это означает, что данное программное средство останется открытым. Более подробная информация о Gnome содержится на сайте www.gnome.org.

KDE

Для многих KDE кажется системой, максимально похожей на Windows. На рис. 11.2 показана среда KDE в системе Red Hat Linux.

Сравните рис. 11.2 с рис. 11.1. Как видно, компания Red Hat предприняла массу усилий, чтобы оба интерфейса выглядели максимально похожими друг на друга. Но дело не в этом. Рекомендуя KDE, учитывайте следующие положения:

- Все приложения тесно интегрированы между собой. Можно сказать, что люди, спроектировавшие KDE, начали с разработки настольной станции с логическим потоком и когерентной организацией. Конечные пользователи чувствуют, что система KDE обеспечивает более оперативный доступ к большему количеству программных приложений.
- Настольная система KDE предоставляет тщательно разработанные программные приложения и упрощает процесс конфигурирования сети.
- Если клиентам нравятся такие программные приложения, как KMail и Konqueror, то KDE можно сделать настольной станцией по умолчанию.

Один из недостатков среды KDE заключается в том, что она не призывает к «всеобщей разработке», как это делает Gnome. Именно поэтому попросту можно не найти такого же количества приложений, совместимых с KDE, как с Gnome. Система

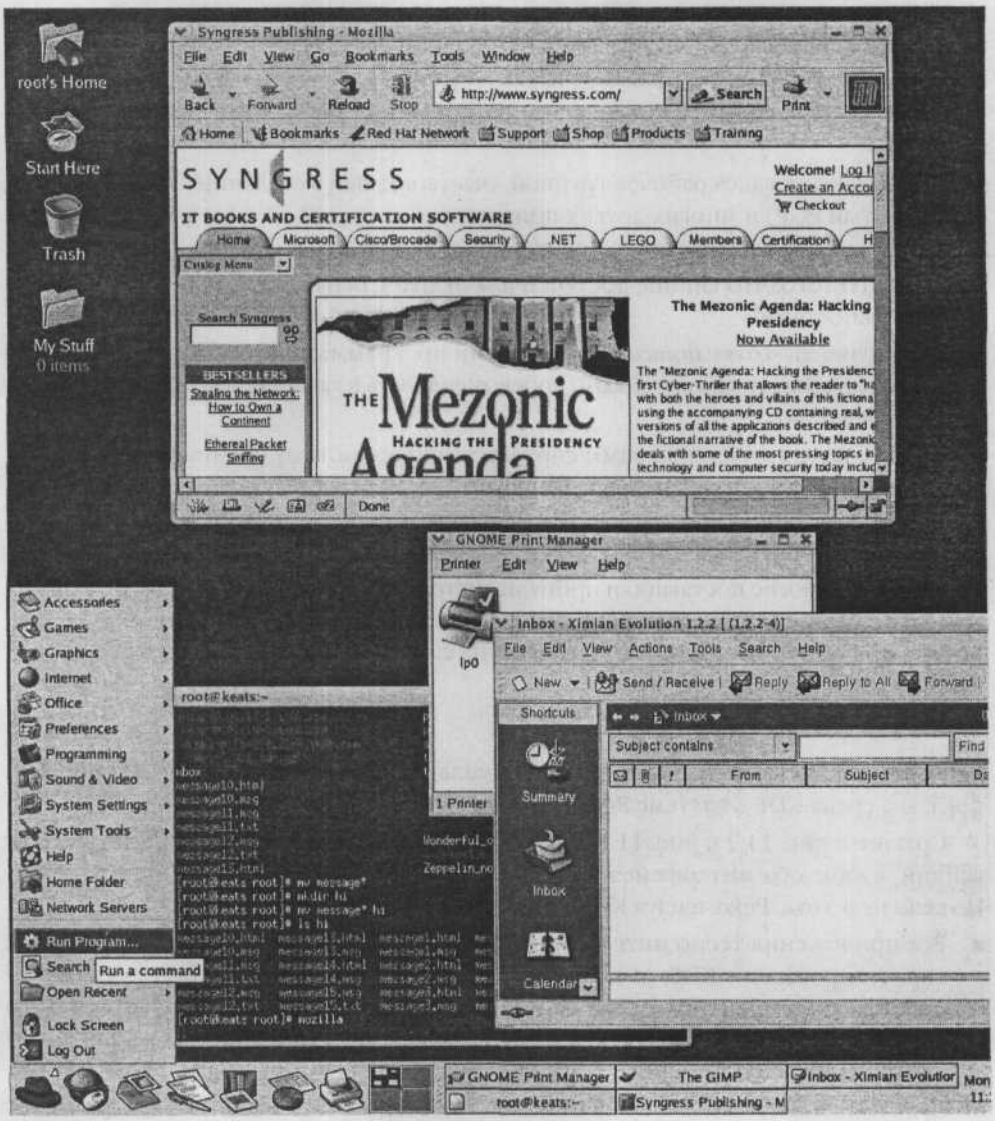

Рис. 11.1. Настольная среда Gnome

KDE базируется на инструментарии Qt GUI и в результате этого не базируется на GPL GNU. Впрочем, это уже не так. Лицензия Qt, не совместимая с GPL, была предметом активных обсуждений в конце девяностых годов. К настоящему моменту этот вопрос урегулирован — Qt распространяется по дуальной лицензии. (GPL для использования

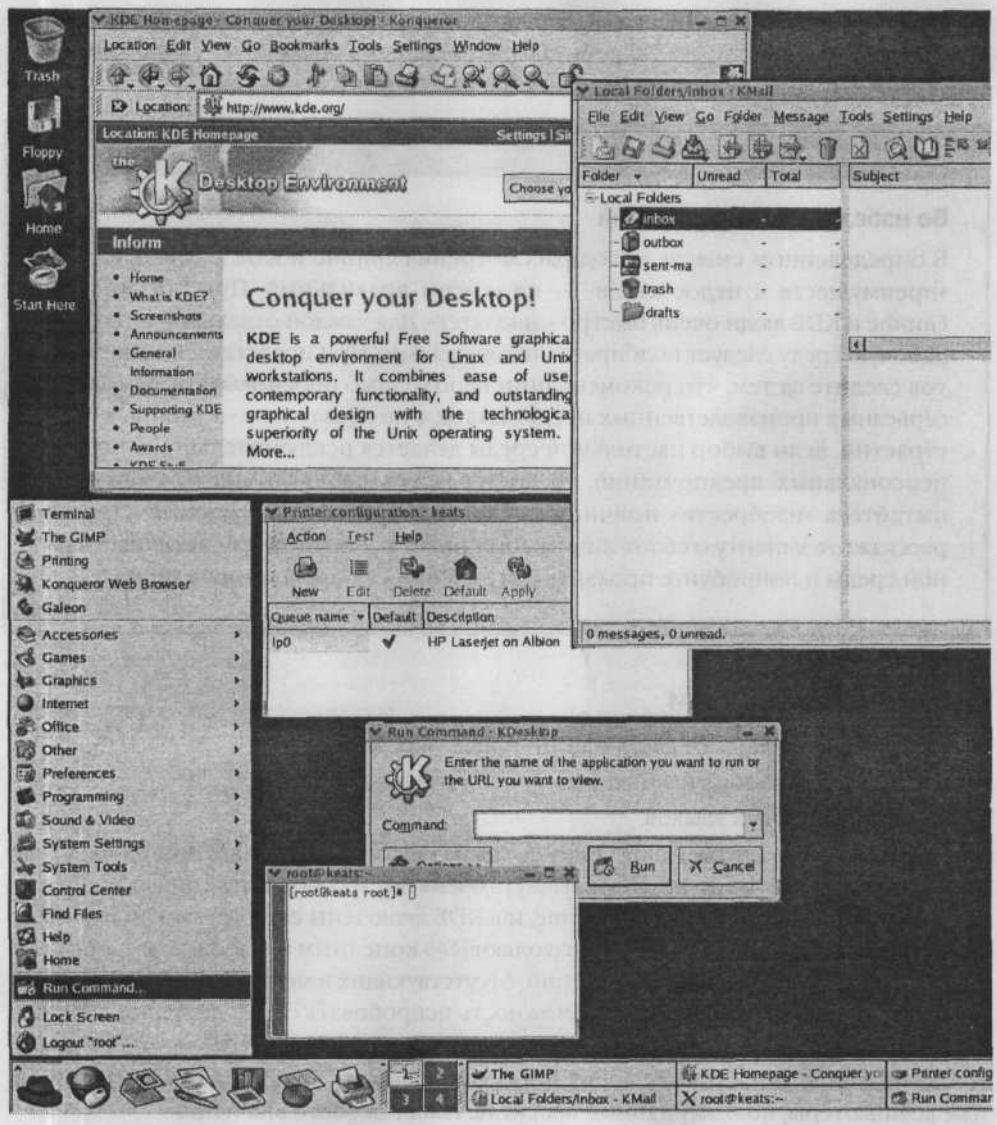

Рис. 11.2. Настольная среда KDE

в открытых приложениях и коммерческой для использования в закрытых. Разработки проекта KDE изначально использовали GPL, LGPL или совместимые лицензии. — *Примеч. науч. ред.)*. Но, несмотря на это, история вынудила многих разработчиков принять на вооружение Gnome, по крайней мере в 1990-х годах. Кроме того, суще-

ствует общее предубеждение, что KDE работает медленнее, чем Gnome. Авторы лично выяснили, что и Gnome, и KDE работают медленно, по сравнению с другими «спартанскими» средами, например Blackbox (рассматривается далее).

Мысли вслух...

Во избежание противоречий

В определенном смысле метод рассмотрения Gnome и KDE с точки зрения «преимуществ и недостатков» — не совсем правильный. При обсуждении Gnome и KDE люди очень быстро «заводятся». Для каждой отдельной ситуации рабочую среду следует подбирать индивидуально. При представлении вариантов следите за тем, что рекомендации необходимо обосновывать, исходя из серьезных производственных предпосылок, а не обязательно из личных пристрастий. Если выбор настольной среды делается исключительно на основе персональных предпочтений, то постарайтесь избежать предвзятости. Не пытайтесь «изобрести» причину, внешне кажущуюся приемлемой. Просто расскажите клиенту о своих личных причинах выбора той или иной настольной среды и попробуйте проявить в этом вопросе определенную гибкость.

Общие особенности

И Gnome, и KDE обладают следующими преимуществами:

- простота использования и настройки под нужды клиента;
- поддержка многих языков.

Gnome и KDE поддерживают меню, похожие на применяемые в Windows. Опытные пользователи Windows должны привыкнуть очень быстро, поскольку они уже знакомы с нужными приложениями. И в Gnome, и в KDE включены свои версии диалогового окна приложения запуска «Start», позволяющего конечным пользователям осуществлять запуск программных приложений, отсутствующих в меню. Но в этом случае все равно стоит дать пользователям возможность испробовать обе настольные среды.

Из-за наличия завершенной графической среды Gnome и KDE работают достаточно медленно. В настоящее время многие используют мощные и самые современные компьютеры, поэтому данный аспект не имеет особого значения.

Установка обеих настольных сред, одной — по умолчанию

При наличии достаточного объема дискового пространства установите и Gnome, и KDE. После этого клиент может выбрать любую среду для ее применения по умолчанию. Это означает, что пользователи получают доступ к программным приложени-

ям Gnome и KDE из любой среды. Не каждое приложение Gnome совместимо с KDE, и наоборот. Впрочем, проблемы совместимости достаточно редки.

После этого пользователям следует предоставить информацию о дополнительных настольных средах и критериях их выбора. Таким образом, клиенты получают возможность выбора настольной среды и ее настройки под свои потребности.

Альтернативные диспетчеры окон

Настольная система Xfce спроектирована для работы на любой системе UNIX, включая Linux. Данный проект также совместим с Gnome и KDE. Одной из отличительных особенностей Xfce является более полная поддержка ею принципа управления файлами «drag and drop», чем конкурентами. Более подробная информация о Xfce имеется на сайте www.xfce.org.

Другой альтернативной настольной средой является Общая настольная среда (CDE), разработанная рабочей группой, в которую входили специалисты из HP, Novell, Sun и IBM. Системы Sun Solaris традиционно поставлялись с CDE. Это — не совсем обычный диспетчер окон. Подробности о CDE — на сайте www.sun.com/software/solaris/cde/.

Серверы X Window и диспетчеры управления окнами

Система X Window (постарайтесь удержаться от соблазна назвать эту систему X WindowS. Такая ошибка сделает вашу речь неграмотной и вынудит специалиста с опаской относиться ко всему, что вы скажете после. — *Примеч. науч. ред.)* спроектирована для предоставления среды GUI на базе общих стандартов. Это означает, что разработчику, желающему создать сервер X Window, просто следует ознакомиться с общими стандартами. После этого он может создавать программные приложения, соответствующие этим стандартам.

С самого начала разработки планировалось, что среда X будет совместима с сетевыми средами; это означает, что выполнение сеанса X Window станет возможным по сети. Следовательно, с помощью среды X Window можно подключиться к серверу X Window удаленной системы так, будто пользователь работает непосредственно с удаленной машиной.

Сервер X Window отвечает за обеспечение среды GUI. Чаще всего эта среда доступна для локальной системы, но она может быть доступной и для удаленных систем. Таким образом, всякий раз при регистрации в среде Gnome или KDE, вы работаете с X Window. Среда Gnome или KDE просто будет играть роль клиентов для локальной системы.

11 Зак. 1269

Существуют две основные реализации среды X Window:

- **X.org** — Сервер X Window, используемый в большинстве дистрибутивов Linux из-за его совместимости с GNU GPL.
- **XFree86** — приблизительно до 2002 года — программное обеспечение X Window по умолчанию для большинства платформ. Однако XFree86 принял новую лицензию, отказавшись от совместимости с GNU GPL, в результате чего многие поставщики и разработчики перешли на поддержку сервера X.org (см. рис. 11.3).

Рис. 11.3. Web-сайт X.org

Сравнительный анализ серверов X Window и диспетчеров управления окнами

Диспетчер управления окнами — это промежуточное звено между сервером и настольной рабочей средой. Он отвечает за управление панелями инструментов окон и их меню. Также среда определяет положение программных приложений при их

запуске. Наиболее распространенные диспетчеры управления окнами включают в себя следующее:

- **Metacity** Диспетчер управления окнами по умолчанию для настольных систем Gnome, от версии 8.0.
- **Sawfish** Диспетчер управления окнами по умолчанию для настольных систем Gnome версии 8.0 и более старых.
- **Kwin** Диспетчер управления окнами по умолчанию для KDE.
- **Tab Window Manager (TWM)** Немного устаревший диспетчер управления окнами, рассчитанный только на предоставление необходимых элементов рабочего стола. Часто используется во время удаленных сеансов X для обеспечения максимальной совместимости с системами, не имеющими более совершенных диспетчеров управления окнами.
- **Enlightenment** Было время, когда система Enlightenment считалась обновлением FVWM. Теперь она является независимым проектом. Подробности об Enlightenment — на сайте www. enlightenment.org.
- **FVWM** Последняя версия FVWM — FVWM2 (доступна на www.fvwm.org).
- **AfterSTEP** Подробности см. на сайте www.afterstep.org.
- **WindowMaker** Подробности см. на сайте www.windowmaker.org.
- **Blackbox** Некоторые версии поддерживают KDE, но официально не поддерживают Gnome. Система Blackbox доступна на сайте http://blackboxwm.sourceforge.net.

Инструментальные средства и «ловушки»

Настольная среда, сервер X Window, диспетчер управление окнами... Чем они различаются?

Клиентам могут быть не совсем понятны различия между понятиями: настольные системы, серверы X Window и диспетчеры управления окнами. Ниже кратко описано каждое из них.

Настольная рабочая среда (например, Gnome) — не то же самое, что диспетчер управления окнами. Настольная среда включает в себя множество функций, например приложения для конфигурирования (yast/yast2 для SuSE Linux или draconf для Mandrake Linux) и приложения по умолчанию (текстовые редакторы, клиенты FTP и калькуляторы). В настольную рабочую среду входит диспетчер управления окнами. Без настольной среды пользователи получат только «скелет» графической среды, который отпугнет большинство тех, кто привык к Windows.

▶▶

Сервер X Window выполняет роль фундамента для GUI в Linux. Он отвечает за предоставление шрифтов и сетевые возможности системы. Без сервера X Window GUI невозможен.

Диспетчер управления окнами — это клиент сервера X Window (например, реализации X.org или XFree86). Он работает как бы «за сценой» и отвечает за внешний вид окон рабочего стола, включая панели инструментов и меню. Диспетчер управления окнами также управляет внешним видом меню на рабочем столе. При наличии доступа к системе Linux войдите в сеанс X Window, после чего можно запускать любое приложение. Обратите внимание на панель заголовка приложения. Посмотрите, как приложение запускается в разных частях экрана (например, в центре или слева). Пользуйтесь левой и правой кнопками мыши. Все эти элементы управляются диспетчером окон. Без него содержимое, представляемое сервером X Window, будет некогерентным (бессвязным) и не будет иметь общей темы.

Вообще, существует с десяток диспетчеров управления окнами. При рекомендации настольной среды целью должен стать выбор такого диспетчера управления окнами, который был бы по-настоящему полезным клиенту. Если последний ожидает полную среду KDE, наиболее похожую на Windows, тогда возможным выбором может стать KWin. Если нужно что-либо попроще, тогда можно остановиться на WindowMaker или Blackbox. При необходимости настольной среды, внешне в точности напоминающей систему Macintosh, выбирайте Metacity. Более подробную информацию о диспетчерах управления окнами см. сайт www.xwinman.org.

Диспетчеры управления окнами как альтернатива настольным рабочим средам

Gnome, KDE, CDE и XFCE — не единственные настольные рабочие среды. Альтернатива диспетчеру управления Blackbox показана на рис. 11.4. Система Blackbox сильно отличается от Gnome и KDE. Например, в ней нет меню или панелей задач, как в Windows. Кроме этого, Blackbox — это диспетчер управления окнами, а не настольная рабочая среда.

Для вызова меню достаточно щелкнуть правой кнопкой мыши на рабочем столе. После этого можно выбирать программные приложения для открытия. Одним из преимуществ такой среды, как Blackbox, является ее меньшая зависимость от ресурсов, вследствие чего она быстрее загружается. Скорость предпочтительна в любом случае, в основном из-за отсутствия средств на приобретение новой системы всякий раз, когда разработчики Gnome или KDE выпускают на рынок новую жадную до ресурсов функцию GUI.

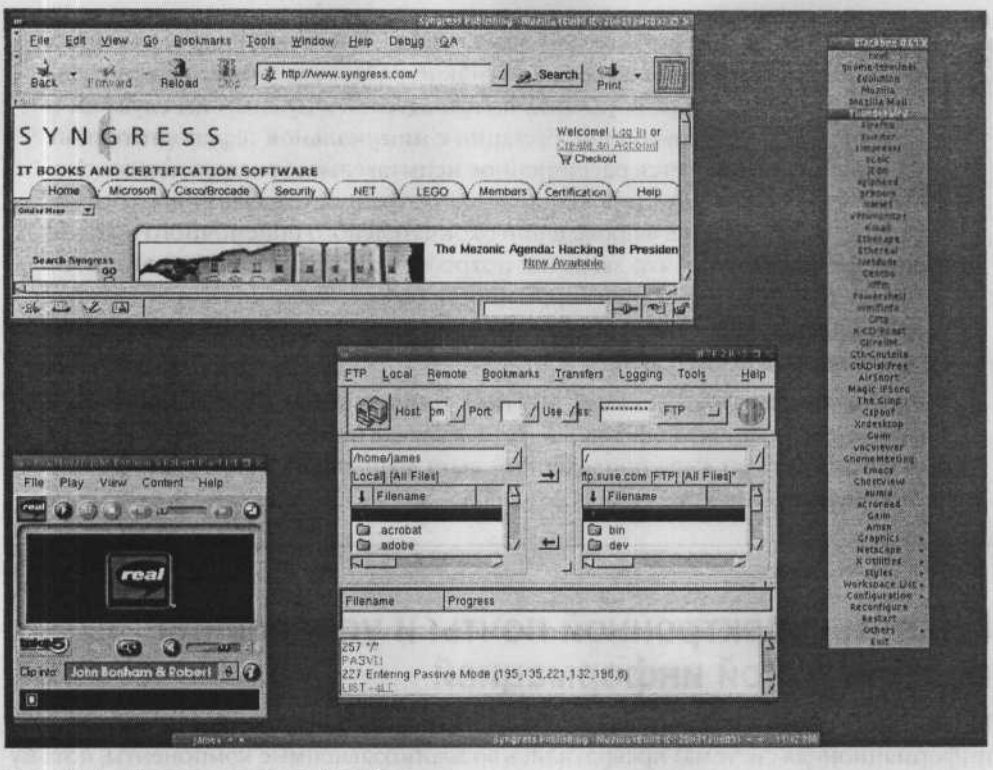

Рис. 11.4. Настольная среда Blackbox

Мысли вслух...

Что нужно заказчику?

В задачи консультанта, дающего клиентам рекомендации по переходу с Windows на Linux, входит следующее:

1. **Определение потребностей клиента** Определите набор служб, необходимых заказчику. Составьте подробный список потребностей. Сразу же определите наличие альтернативного открытого решения. Если Linux в него не входит, не пытайтесь навязывать систему. А то к вам больше не обратятся, и у вас появится недовольный клиент.
2. **Определение решений** Цель консультанта — понимание существующих открытых программных средств. Изучите последние решения, появившиеся на рынке. Почаще заходите на такие сайты, как Freshmeat (www.freshmeat.net), SourceForge (www.sourceforge.net) и даже на Slashdot (www.slashdot.org), чтобы быть в курсе последних программных разработок.

▶▶

3. **Выполнение потребностей заказчика** С помощью программных приложений на базе Linux создайте гибкие, работоспособные решения для возможности доступа конечных пользователей к нужным им службам и получения необходимой информации с минимальной переподготовкой. Для начала потребуется расширенное испытательное развертывание системы с целью проверки удовлетворения потребностей заказчика. Следующий шаг заключается в проведении окончательного приемочного испытания. Не исключено, что заказчик потребует так называемого «льготного периода» с целью проверки корректности работы созданного программного решения. И, наконец, необходимо обучить пользователей тонкостям работы с новой системой.

Часто бывает так, что даже самые опытные консультанты не всегда могут удовлетворить пожелания клиентов. Поэтому, в случае неудач можно быть уверенным в том, что три вышеприведенные шага выполнялись некорректно или не учитывались вообще.

Клиенты электронной почты и управления персональной информацией

В настоящее время электронная почта и PIM (Personal Information Manager, личная информационная система) превратились во взаимозависимые компоненты, потому что большинство людей пользуется e-mail для передачи информации о себе и о своем бизнесе. В данном разделе рассматриваются программные средства электронной передачи сообщений и PIM, помогающие пользователям организовать свою работу даже в отсутствие Outlook.

По опыту авторов известно, что большинство пользователей считают, что Outlook — и *есть* система передачи электронной почты. Многие даже не подозревают, что они просто пользуются программой для отправки и получения почты. При работе с клиентами не пожалейте времени, чтобы выяснить, понимают ли они разницу. Проблема в том, что многие из этих конечных пользователей часто управляют целыми компаниями, нанимают (и увольняют) сотрудников и принимают решения о закупках. Задача консультанта заключается в информировании пользователей о том, что они могут работать с электронной почтой даже без таких программ, как Outlook или Outlook Express.

Поэтому тем, кто не уверен, что система передачи электронных сообщений существует и вне Outlook или Outlook Express, можно предложить ознакомиться с данным разделом, потому что в среде Linux явно нет недостатка в приложениях

передачи и приема электронных сообщений. В число наиболее широко распространенных программных средств работы с электронной почтой входят следующие:

- Evolution;
- KDE Suite/Kmail;
- Mozilla mail/Thunderbird;
- Aethera;
- Sylpheed.

Evolution

Evolution — это почтовый и PIM-клиент по умолчанию для Gnome. Kmail и Evolution будут работать в любом выбранном диспетчере управления окнами. Они также совместимы со средами KDE, Gnome или Blackbox. На рис. 11.5 показан почтовый интерфейс Evolution, из которого можно отправлять и принимать электронную почту.

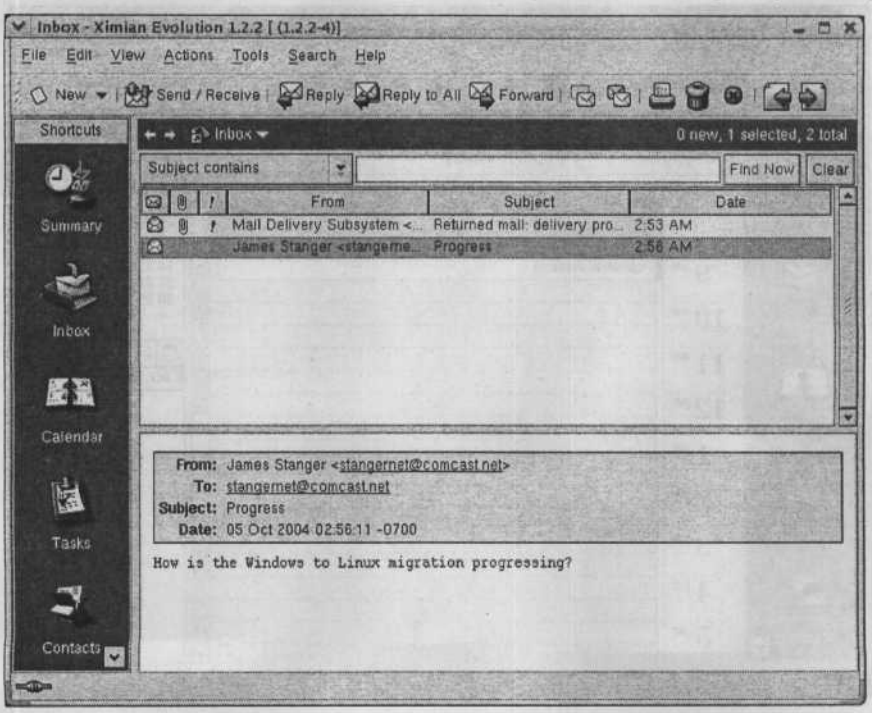

Рис. 11.5. Почтовый интерфейс Evolution

Evolution сохраняет файлы в формате mbox. Если имя пользователя — «james», то почту следует искать в каталоге /home/james/evolution/local, содержащем каталоги для всех почтовых папок. В каждой папке имеется файл с именем mbox, являющийся почтовым сообщением в формате mbox.

Evolution также имеет функции PIM (персональный органайзер), включая функцию ежедневника (календаря), показанную на рис. 11.6.

Преимущества использования Evolution — следующие:

- Система разработана Novell — известной компанией с историей разработки и формирования постоянного контингента заказчиков. (Данное утверждение не вполне корректно. Фактически, Novell приобрела Evolution вместе с компанией Ximian в 2003 году и с тех пор Evolution действительно разрабатывается Novell. Однако на более ранних этапах своего развития Evolution не имел к Novell никакого отношения. — *Примеч. науч. ред.).*
- Работает на любом распространенном диспетчере управления окнами (например, KDE или Gnome).
- Спроектирована для работы с традиционными серверами коллективного пользования, например Microsoft Exchange.

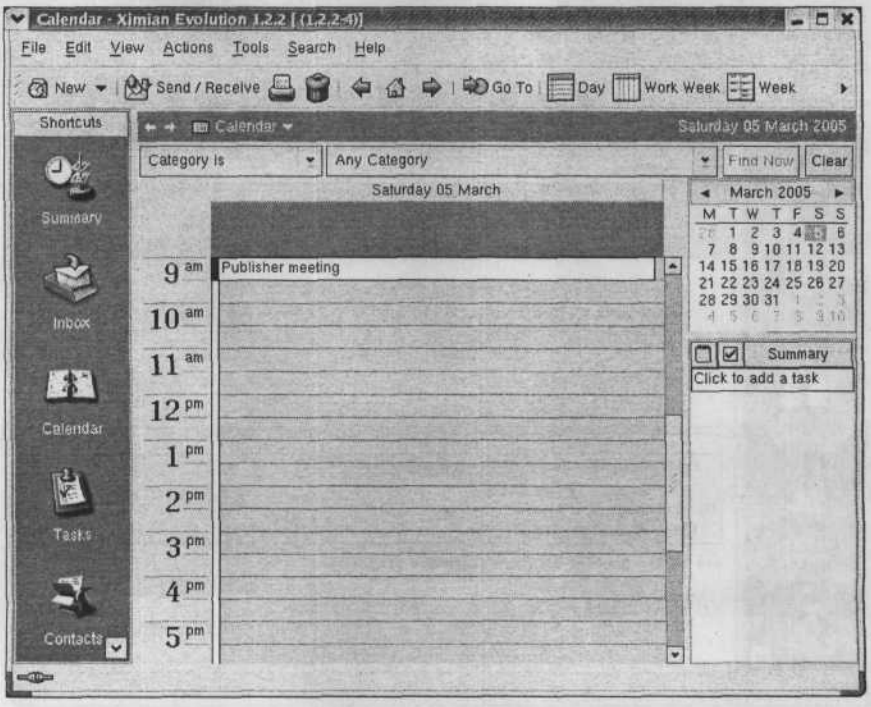

Рис. 11.6. Интерфейс ежедневника Evolution

Evolution, Microsoft Exchange, Novell GroupWise и OpenExchange

Уникальность Evolution заключается в том, что система хорошо работает с серверами, созданными третьими производителями. Например, Evolution Connector для Microsoft

Exchange позволяет пользоваться всеми функциями, предоставляемыми Exchange. Аналогично, подключаемые модули для Evolution обеспечивают работу системы в качестве клиента для серверов Novell GroupWise и OpenExchange от Novell. Подробности об Evolution — на сайте www.novell.com/products/evolution.

KDE Suite/KMail

Почтовый клиент KDE по умолчанию называется KMail. Программа может работать как сама по себе, так и встраиваться в Kontact, что делает ее внешне похожей на Outlook. В KMail и большинстве других почтовых клиентах все электронные сообщения сохраняются в домашнем каталоге в папке с именем Mail, если только не используется IMAP. В папке /home/user_name/Mail хранятся все файлы электронной почты: inbox (входящие), trash (мусорная корзина), sent (отправленные), drafts (черновики) и так далее. Скопируйте файлы и убедитесь в том, что разрешения заданы корректно, что пользователь единственный, кто имеет право чтения и записи разрешений. Папка Mail должна иметь приблизительно следующий вид:

```
ls -lh /home/james/Mail
total 11M
-rw - - - - - - - 1 james james 0 Aug 20 19:51 drafts
-rw - - - - - - - 1 james james 11M Aug 20 19:51 inbox
-rw - - - - - - - 1 james james 0 Aug 20 19:51 outbox
-rw - - - - - - - 1 james james 26K Aug 13 19:04 sent-mail
-rw - - - - - - - 1 james james 0 May 17 18:32 trash
```

Kontact

По своей сути Kontact — это KMail «на стероидах». Система обеспечивает подключение к следующим серверам коллективного использования:

- **Microsoft Exchange** В настоящее время Kontact поддерживает только Microsoft Exchange 2000. Подробности — на сайте www.microsoft.com.
- **Novell GroupWise** В настоящее время Kontact поддерживает только версию 6.5. Подробности — на сайте www.novell.com.
- **eGroupWare** Приложение коллективного пользования на базе PHP, спроектированное сообществом открытых программных средств для внутреннего пользования. Работает на серверах Linux. Подробности — на сайте www.egroupware.org.
- **The Kolab project** Сервер коллективного пользования, разработанный правительством Германии. Подробности — на сайте www.bsi.bund.de.

Таким образом, KMail является конкурентом Evolution. Более подробная информация о Kontact имеется на сайте www.kontact.org.

Aethera

Подобно Evolution, Aethera — это программное приложение для работы с электронной почтой со стандартными средствами PIM, распространяющееся по лицензии GPL. Однако на время написания книги система Aethera была спроектирована для поддержки только коллективного сервера Kolab. На рис. 11.7 показана функция ежедневника Aethera.

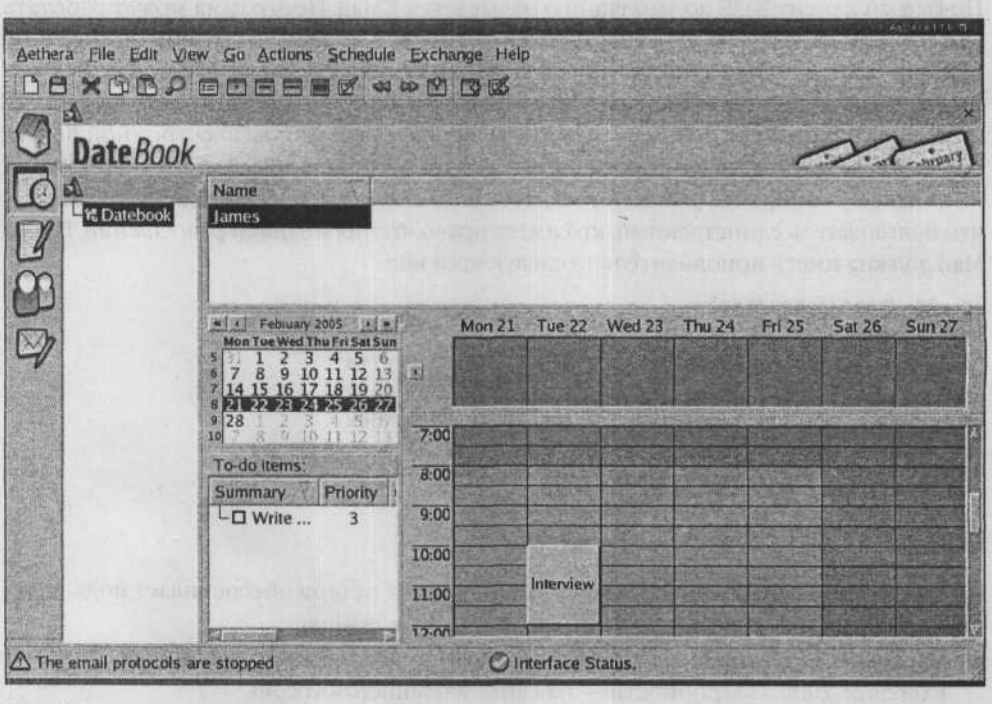

Рис. 11.7. Функция ежедневника Aethera

Aethera — приложение с общедоступной лицензией, считающееся достаточно надежным. Однако его ограниченная поддержка серверов коллективного пользования может представлять проблему для компаний, не желающих переходить на сервер Kolab. Более подробная информация об Aethera имеется на сайте www.thekompany.com/projects/aethera/index.php3.

Mozilla Mail/Thunderbird

Система Mozilla Mail (см. рис. 11.8) объединена с web-браузером Mozilla и с Composer — визуальным редактором HTML. Mozilla Mail — устойчивый почтовый клиент, поддерживающий SMTP, POP3 и IMAP.

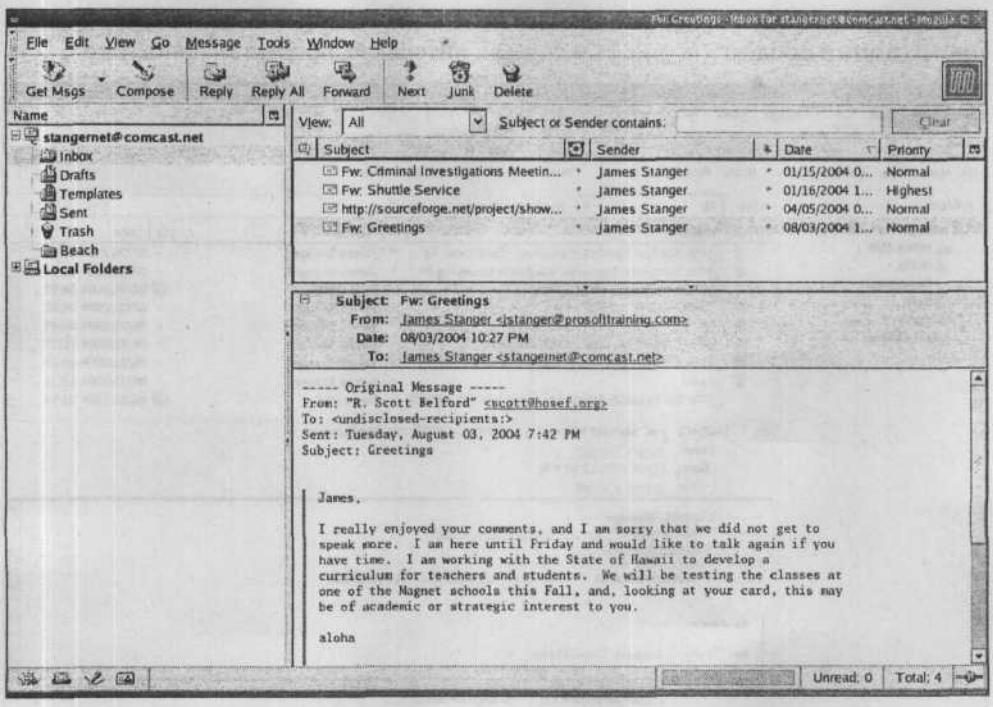

Рис. 11.8. Mozilla Mail

Почтовый клиент Mozilla Mail распространен чрезвычайно широко, это весьма надежный продукт. Впрочем, на время написания книги, он не поддерживал системы коллективного пользования. По причине объединения с редактором HTML и браузером Mozilla Mail можно рассматривать как прекрасное приложение для компаний, не применяющих средств коллективного пользования. Многие компании обнаружат, что конечные пользователи могут пользоваться преимуществами редактора HTML и web-браузера. Более подробная информация о Mozilla Mail имеется на сайте www.mozilla.org, а также в разделе — «Перенос электронной почты».

Thunderbird

Несмотря на то, что продукт Thunderbird также разработан на Mozilla.org, в нем применен другой код, нежели в Mozilla Mail. (Не совсем так. Thunderbird базируется на Mozilla Mail, но преследует иные цели. Thunderbird — самостоятельный продукт, в то время как Mozilla Mail — часть пакета Mozilla. В связи с тем, что фонд Mozilla Foundation принял решение развивать именно самостоятельные приложения: web-браузер Firefox, клиент электронной почты Thunderbird, а не цельный пакет, Thunderbitrd в настоящее время приобретает первостепенное значение. — *Примеч.*

науч. ред.). Именно поэтому Thunderbird можно рассматривать как абсолютно иной программный продукт. На рис. 11.9 показан интерфейс продукта Thunderbird.

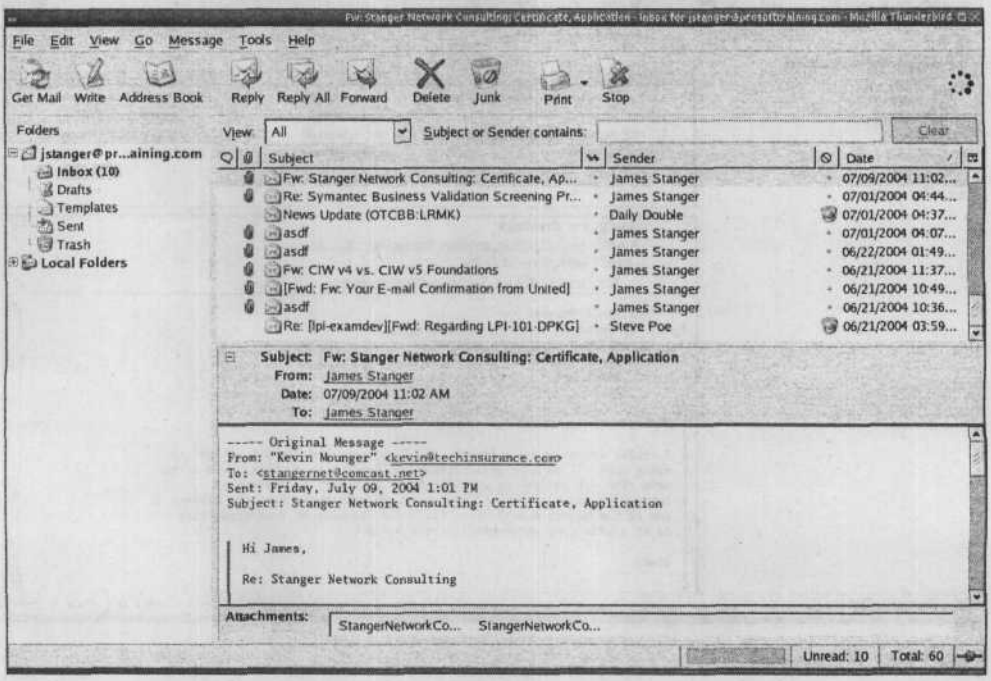

Рис. 11.9. Программное приложение Thunderbird

Подобно Mozilla Mail, на время написания данной книги Thunderbird не поддерживал групповые серверы. Однако загружается оно достаточно оперативно, имеет небольшой размер, что делает его идеальным для тех, кто нуждается в автономном приложении для работы с электронной почтой. Подробности о Thunderbird см. на сайте www.mozilla.org.

Sylpheed

Продукт Sylpheed (см. рис. 11.10) — одно из многих почтовых программных приложений, существующих на компьютерном рынке. Оно не имеет функций поддержки групповых средств или планирования. Однако в одном этот продукт показал себя с очень хорошей стороны: он поддерживает системы PGP *(набор алгоритмов и программ для высоконадежного шифрования сообщений с использованием открытых ключей)* и GPG. Несмотря на то, что многие почтовые клиенты утверждают о своей поддержке PGP и GPG, мало кто из них делает это настолько же хорошо, как Sylpheed.

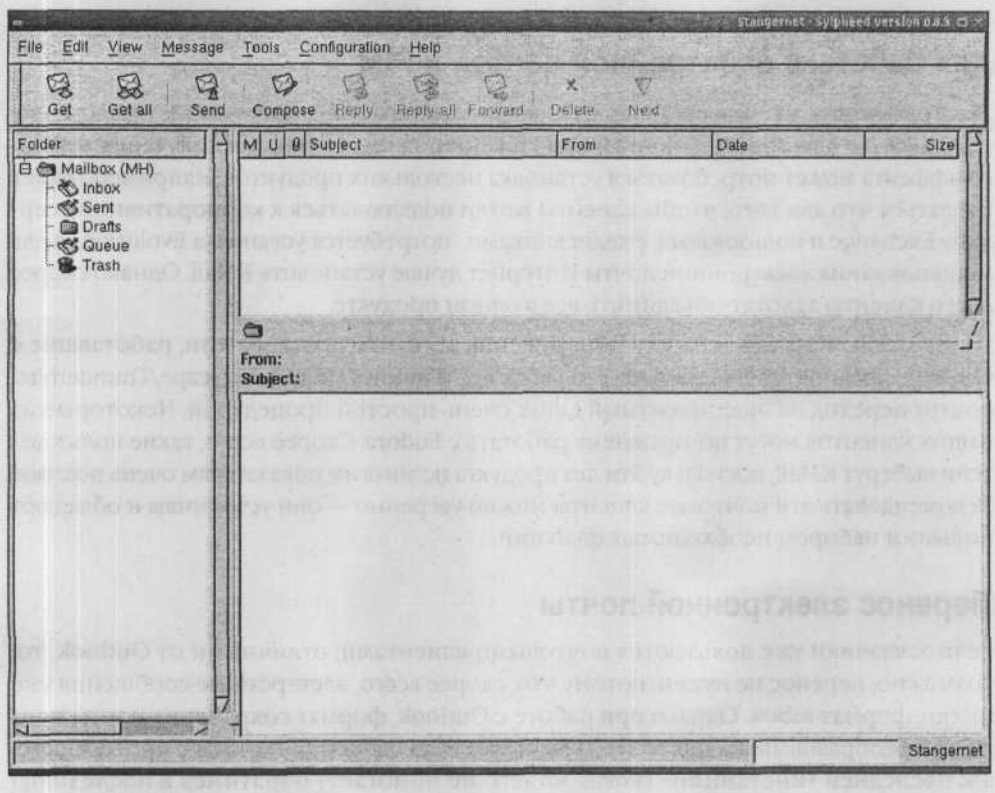

Рис. 11.10. Sylpheed

Таким образом, если клиентам необходима поддержка PGP или GPG, рассмотрите возможность рекомендации Sylpheed. Подробности о продукте имеются на сайте http://sylpheed.good-day.net. Создатели Sylpheed сделали упор на поддержку продуктом IPv6 — новой версии IP, рассчитанной на повышение безопасности.

Существенная информация

Независимо от того, какой почтовый клиент планируется к использованию, следующая информация будет необходимой:

- имя сервера SMTP или IP-адрес;
- имя сервера POP3 или IMAP или IP-адрес;
- информация аутентификации пользователя (например, имя пользователя и пароль).

Спишите эти данные, чтобы они всегда были под рукой. При осуществлении миграции их придется многократно сообщать тем, кто непосредственно занимается процессом.

Рекомендуемые программные средства для работы с электронной почтой и PIM

Не стоит думать, что порекомендовать можно только одно программное приложение для работы с электронной почтой или PIM. Во многих случаях для получения нужного эффекта может потребоваться установка нескольких продуктов. Например, может оказаться что для того, чтобы клиенты могли подключаться к корпоративному серверу Exchange и пользоваться ежедневниками, потребуется установка Evolution, а для использования электронной почты Интернет лучше установить KMail. Однако скорее всего клиенты захотят объединить все в одном продукте.

Не исключена вероятность обнаружения того, что пользователи, работавшие с Outlook, предпочтут Evolution. Те, кто работал с Windows Mozilla/Netscape/Thunderbird, сочтут переход на эквивалентный Linux очень простой процедурой. Некоторые из ваших клиентов могут по-прежнему работать с Eudora. Скорее всего, такие пользователи выберут KMail, поскольку эти два продукта по многим показателям очень похожи. Рекомендовать эти почтовые клиенты можно уверенно — они устойчивы и обладают большим набором необходимых функций.

Перенос электронной почты

Если заказчики уже пользуются почтовыми клиентами, отличными от Outlook, то, возможно, перенос не нужен, потому что, скорее всего, электронные сообщения уже имеют формат mbox. Однако при работе с Outlook, формат сохранения почты придется преобразовывать. Для этого существует пять способов. Начнем с простейшего, а к последней «инстанции» (когда ничего не помогает) обратимся в последнюю очередь. В зависимости от версии используемого клиента, до переноса почты, возможно, потребуется обновление. Если для каждого клиента необходимо перенести несколько тысяч электронных писем, то данная часть процесса переноса может занять очень много времени.

Одним из лучших способов убедиться в том, что времени на надлежащий перенос достаточно, является планирование поэтапного переноса, куда входит использование большого количества программных приложений для преобразования электронных писем. Может случиться так, что экспортировать почту напрямую из программы электронной почты Windows с последующим импортированием в программу Linux будет невозможно. Обнаружится, что для начала придется экспортировать почту в промежуточный почтовый клиент, который затем сможет экспортировать материалы в формат, требуемый приложением, планируемым к использованию.

Рассмотрим процесс переноса электронной почты из Outlook и Outlook Express.

Перенос из Outlook или Outlook Express

Первым шагом является создание резервных копий на случай возникновения проблем. В Outlook нужно экспортировать электронные сообщения в один файл с расширением .pst. Выберите **File** (Файл) / **Import and Export** (Импорт и экспорт) для открытия диалогового окна Мастера экспортирования и импортирования. После этого выберите строку **Export to a file** (Экспортировать в файл) (см. рис. 11.11).

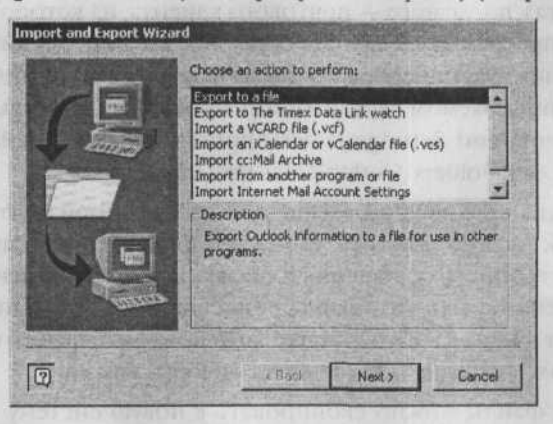

Рис. 11.11. Окно Мастера импортирования и экспортирования Microsoft Outlook

После нажатия кнопки **Next** (Далее) выберите **Personal Folder File (.pst)** (Файл .pst личной папки). Затем откройте верхнюю часть дерева нажатием на **Personal Folder** (Личная папка) и активизируйте опцию **Include all subfolders** (Включить все подпапки). Не забудьте запомнить место сохранения резервного файла .pst. При сохранении файла не экспортируйте резервную копию с шифрованием, архивированием или защитой паролем. В противном случае процесс импортирования не состоится. Теперь файл можно импортировать в Mozilla.

Импортирование Outlook Mail в Mozilla

Теперь установите Mozilla в настольную систему Windows. Убедитесь, что для этого шага выбран продукт Mozilla, а не Firefox или Thunderbird, даже если в конце процесса Mozilla не планируется к использованию.

Прежде всего установите Mozilla и при запросе компонентов к установке выберите **Complete** (Полностью). Системе не следует указывать, чтобы она сделала продукт Mozilla браузером или почтовым клиентом по умолчанию. После установки запустите Mozilla и выберите **Windows>Mail & Newsgroups** (Группы новостей). В открывающемся мастере ввода учетной записи указывать настройки не нужно. Если есть желание, то их можно импортировать в Mozilla из Outlook; они появятся как вторая учетная запись.

После настройки учетной записи необходимо импортировать старые почтовые сообщения из Outlook в Mozilla. Теперь выполните то же самое для настроек и адресной книги. Адресную книгу можно просто экспортировать в формате .csv из Outlook или Outlook Express и импортировать в Mozila тем же способом, что и почтовые сообщения.

Для этого выберите в окне импорта **Tools>Import** (Инструменты>Импорт), выберите **Mail** (Почта), после чего — почтового клиента, из которого осуществляется импортирование; программа сделает все остальное. По выполнении указанных шагов почтовые сообщения будут преобразованы из формата .pst в стандартный почтовый формат mbox. В описываемом случае импортированные почтовые папки размещаются в C:\Documents and Settings\james\Application\Data\Mozilla\Profiles\default\033c70c1.slt\Mail\Local Folders\Outlook Mail.sbd\Inbox.sbd.

Внутри этой папки размещены все папки с электронной почтой, перенесенные из клиента Outlook. Можно заметить, что в каждой папке существует два файла: собственно файл электронного сообщения и указатель того, что именно в нем находится. Если попытаться открыть этот файл без расширения .msf, например в Блокноте (Notepad), то будет видно, что это стандартный почтовый файл в формате mbox. По некоторым отзывам Mozilla не осуществляет преобразования.

Теперь все эти файлы можно скопировать в новую систему любым способом: сбросить на CD, отправить по FTP на сервер либо воспользоваться winscp для копирования в новую систему.

LibPST

LibPST — программное приложение Linux, преобразующее файлы PST в файлы формата mbox, совместимые с Mozilla. Таким образом, после создания файла PST LibPST просто устанавливается в систему Linux и используется для подготовки содержимого файла PST для работы с Mozilla. LibPST можно скачать с сайта http://sourceforge.net/projects/ol2mbox. Эта программа — идеальный выбор, если файлы PST для преобразования большого объема. Во многих случаях Mozilla не сумеет преобразовать их с помощью собственной соответствующей утилиты.

Импортирование Outlook Mail в Evolution

Один из способов импортирования Outlook Mail в Evolution — применение программы под названием Outport, которую можно скачать с сайта http://outport.sourceforge.net. Предположим, к примеру, что клиент имеет в Outlook Express набор электронных сообщений под названием Syngress, напоминающий показанный на рис. 11.12.

Все, что требуется, — это скачать из Интернета программу Outport и дважды щелкнуть кнопкой мыши на файле outport.exe. Откроется главный интерфейс Outport (см. рис. 11.13).

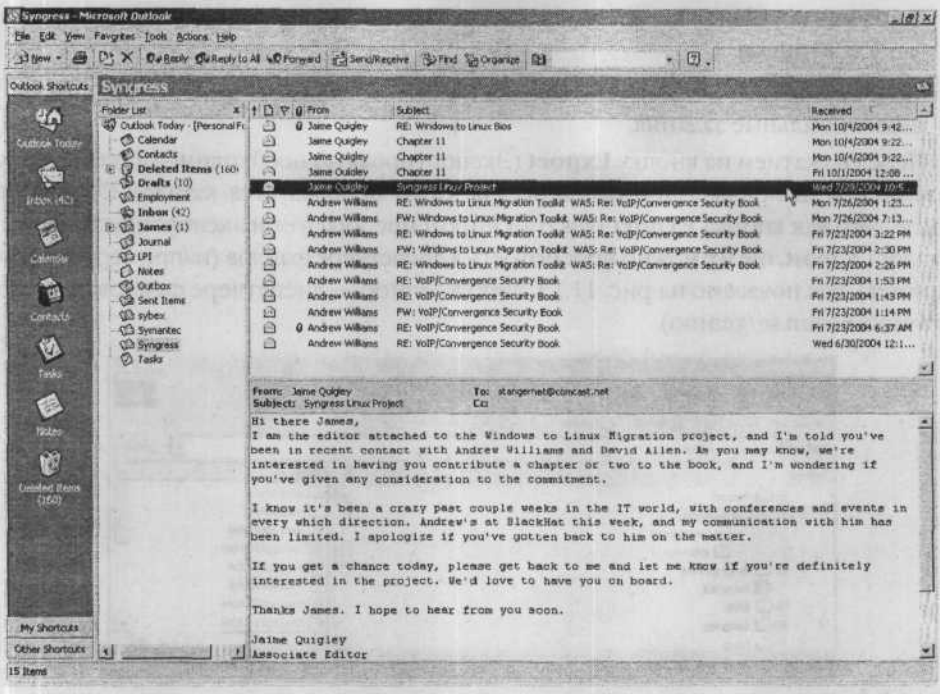

Рис. 11.12. Электронные сообщения в Outlook

После появления Outport для экспортирования можно выбрать различные элементы Outlook:

- записи Outlook Calendar;
- контакты;

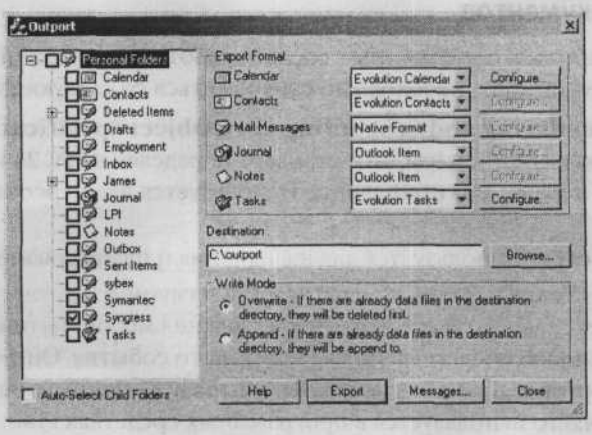

Рис. 11.13. Использование Outport для экспортирования сообщений из Outlook

- почтовые сообщения;
- записи журнала;
- примечания;
- индивидуальные задания.

Перед нажатием на кнопку **Export** (Экспортировать) необходимо указать каталог назначения. В предыдущем примере для этого используется каталог C:\outport/. После того как кнопка **Export** нажата, Outport преобразует и экспортирует файлы в каталог Outport, где их можно просмотреть в диспетчере файлов (например, Windows Explorer), как показано на рис. 11.14, либо в Gentoo — диспетчере файлов для Linux (www.obsession.se/gentoo).

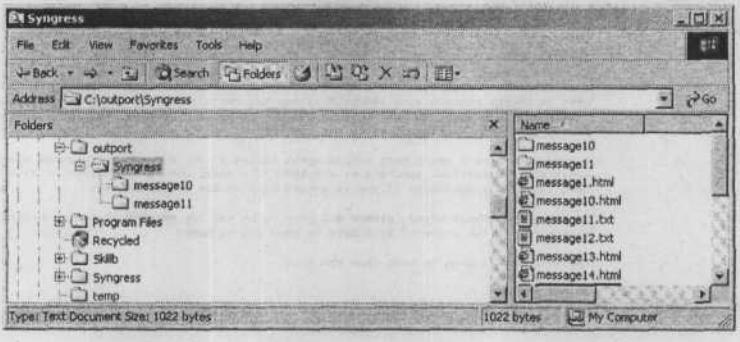

Рис. 11.14. Просмотр экспортированных сообщений в Windows Explorer

После экспортирования этих файлов их можно импортировать в Evolution или другую программу для упрощения их преобразования в файлы формата, распознаваемого Evolution.

Стандарты документов

При переносе настроек программных средств работы с электронной почтой и PIM из систем Windows в Linux, необходимо ознакомиться со следующими стандартами:

- **Internet Calendaring and Scheduling Core Object Specification (iCalendar)** Известный под названием Ical, этот стандарт определен в RFC 2445. Машины Apple были в числе первых, его принявших. Используется для персональных ежедневников.
- **Vcalendar (Vcal)** Используется для назначения и планирования встреч.
- **Virtual Card (Vcard)** Формат электронной визитной карточки, предназначенный для универсального текстового представления мероприятий. Это — межплатформенный способ представления календарного события. Outport может осуществлять экспортирование в эти форматы (см. главу 8). Данный стандарт определен в RFC 2426 и часто используется в программных средствах PIM.

Сложный способ

Наименее «удобным» способом экспортирования является простая переадресация электронных сообщений из клиента Windows в новую систему Linux. Если приходится прибегать к этому способу, то, возможно, простейшим путем будет переадресации папки с почтой целиком. Впрочем, при такой переадресации большого количества сообщений в виде одного существует риск того, что пользователи смогут найти свои электронные сообщения, только просмотрев все сообщения, сохраненные в папке. Поэтому при переадресации электронной почты выбирайте наименее болезненный способ.

Web-браузеры

Web-браузеры предназначены не только для «серфинга по волнам Интернет»; их можно использовать для запуска встроенных приложений, проверять электронную почту, а также просматривать ежедневники коллективного пользования. По этой причине web-браузеры — очень замысловатые программы, которые должны поддерживать различные схемы аутентификации и шифрования. В данном разделе рассматриваются принципы выбора надлежащего браузера (браузеров) для клиента.

Конечные пользователи будут ожидать от систем Linux наличия одного (и только одного) браузера. В Windows практически повсеместно используется Internet Explorer. Этот браузер установлен на каждом компьютере со времени выхода системы Windows 98; многие пользователи привыкли к Internet Explorer еще с Windows 95.

В Linux же возможностей выбора несколько:

- Mozilla;
- Forefox;
- Galeon;
- Konqueror;
- Opera.

Вероятно, ни один web-браузер Linux не удовлетворит абсолютно всех потребностей пользователей. Придется ознакомиться с большим количеством браузеров, прежде чем будет выбран наиболее подходящий. Ниже рассматриваются наиболее важные браузеры на базе GUI.

Mozilla

Mozilla (см. рис. 11.15) фактически представляет собой группу приложений, включающую в себя браузер Mozilla, Mozilla Mail и Composer.

В числе преимуществ Mozilla следующие:

- **«Вкладки» (Tabs)** Возможность просмотра множественных страниц в одном окне повышает эффективность работы.

Рис. 11.15. Mozilla

- **«Движок» Gecko** Библиотека для быстрой и эффективной визуализации web-страниц.
- **Быстродействие** Браузер оперативно визуализирует и легко загружает в память страницы.
- **Устойчивость** Код многократно просмотрен и может быть устойчивее многих браузеров других производителей.
- **Встроенная блокировка всплывающих страниц** При работе с Mozilla для блокирования всплывающих рекламных материалов нет необходимости загружать программные средства третьих сторон.
- **Встроенные программные приложения** Возможность просмотра групп новостей и использования клиента IRC (Internet Relay Chat, Интернет-чат).

Если заказчикам нужен полнофункциональный пакет «в одном флаконе», рекомендуется Mozilla.

Mozilla и Microsoft CHAP

В web-сервере IIS (Информационный сервер Интернет) применяется специальная форма Протокола аутентификации с предварительным согласованием вызова (Challenge Handshake Authentication Protocol, CHAP), называемого MS-CHAP. Так

Microsoft спроектировал IIS. Цель заключалась в том, что если администратор IIS активизировал MS-CHAP, то безопасная аутентификация должна быть доступна только пользователям Internet Explorer.

Однако Mozilla.org удалось реализовать MS-CHAP версии 1.6. Это очень важная разработка, потому что она устраняет еще одну из причин, по которой следует отказаться от браузера Internet Explorer, который испытывал серьезные проблемы с защитой.

Firefox

Firefox — это автономный браузер на базе «движка» Gecko, как и Mozilla (см. рис. 11.16).

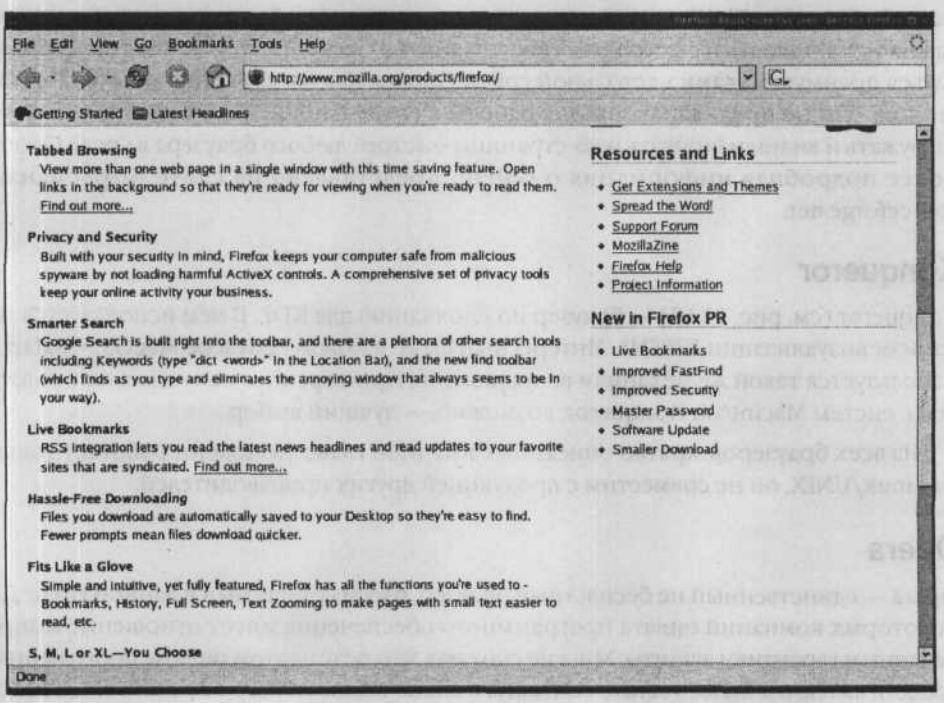

Рис. 11.16. Firefox

Однако Firefox — не просто разновидность Mozilla. Firefox обладает следующими особенностями:

- **Усовершенствованное обеспечение соответствия требованиям заказчика** Firefox обеспечивает очень широкие возможности настройки под требования пользователя — от выбора гарнитуры шрифта до определения отображаемых виртуальных кнопок.

- **Ускоренная визуализация (представление) страниц** В Firefox включена более современная версия Gecko.
- **Меньший размер** Разработчики Firefox сделали все возможное для уменьшения размера приложения приблизительно до 4 Мб.

Если заказчики не возражают против использования отдельных приложений (например, отдельных web-браузеров и клиентов электронной почты), тогда рекомендуется Firefox. И, наконец, Firefox выигрывает от совместимости с MS-CHAP. Более подробная информация о Firefox имеется на сайте www.mozilla.org.

Galeon

Galeon специально разработан для настольной системы Gnome, но использует «движок» Gecko от Mozilla. Следовательно — это подходящий выбор для клиентов, которым важна устойчивость и быстродействие механизма Gecko и которые хотят воспользоваться преимуществами настольной среды Gnome. Как бы хороши ни были Mozilla и Firefox, они не предназначены для работы в среде Gnome. Поэтому Galeon может загружать и визуализировать web-страницы быстрее любого браузера в среде Gnome. Более подробная информация о Galeon представлена на сайте http://galeon.sourceforge.net.

Konqueror

Konqueror (см. рис. 11.17) — браузер по умолчанию для KDE. В нем используется механизм визуализации KHTML. Интересный факт: в новом браузере MacOS — Safari — используется такой же механизм визуализации. При переносе конечных пользователей с систем Macintosh Konqueror, возможно, — лучший выбор.

Из всех браузеров, кратко описанных в данной главе, Konqueror работает только на Linux/UNIX; он не совместим с продукцией других производителей.

Opera

Opera — единственный не бесплатный браузер, рассматриваемый в данной главе. Для некоторых компаний оплата программного обеспечения имеет отношение к определенным гарантиям защиты. Многие считают, что результатом оплаты программных средств являются более тесные контакты в плане технического обслуживания. Разработчики Opera утверждают, что их продукт имеет следующие преимущества:

- самая быстрая визуализация web-страниц из всех web-браузеров;
- просмотр с использованием «вкладок»;
- возможность фокусирования и визуального «увеличения» содержимого;
- совместимость с IRC.

Во многом Opera предлагает те же функции, что и Mozilla.

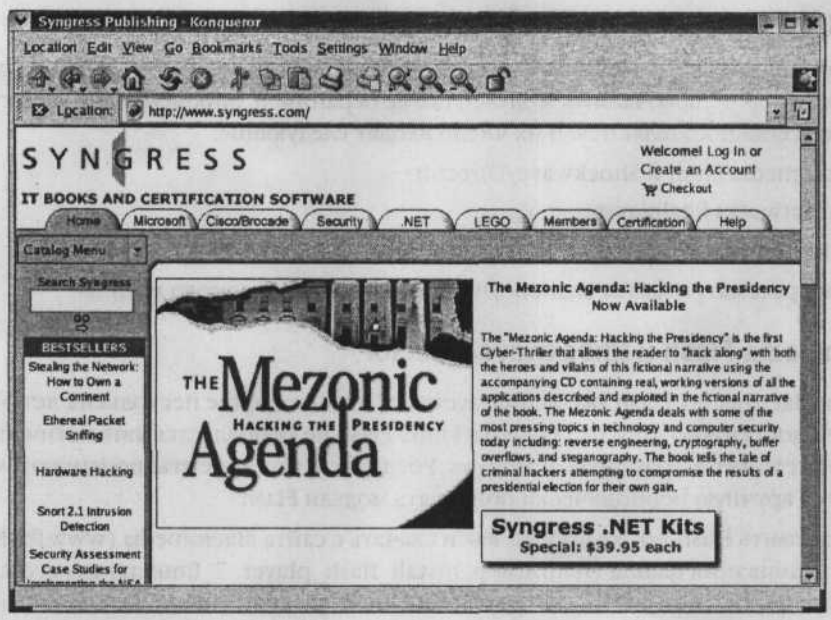

Рис. 11.17. Web-браузер Konqueror

Перенос закладок

Понятно, что перевод конечных пользователей на браузер Linux — процедура сравнительно простая, потому что практически каждый браузер, работающий под Linux, автоматически импортирует закладки, экспортированные из Internet Explorer. Данные экспортированной закладки легко обнаруживаются. Однако в последних версиях Internet Explorer эти данные сохраняются в каталоге. В описываемой системе закладки Internet Explorer размещены в каталоге C:\Documents and Settings\james\Favorites.

После установки Mozilla, Firefox или Opera доступ к этим данным упрощается, потому что они сохраняются в отдельном файле. Этот файл может иметь имя bookmark.htm, bookmarks.htm, bookmark.html или bookmarks.html в зависимости от версии браузера. Все, что следует сделать, — скопировать этот файл в новую систему Linux при переносе операционной системы. После этого достаточно найти функцию работы с закладками. К примеру, в Firefox нужно выбрать **Bookmarks** (Закладки) / **Manage Bookmarks** (Управление закладками). Когда открывается окно Bookmarks Manager (Диспетчер закладок) войдите в **File** (Файл) / **Import** (Импорт) и выберите опцию **From File** (Из файла). Затем можно выбрать файл закладки, экспортированный из Internet Explorer.

Подключаемые модули браузера

Вероятно, пользователи Windows знают десятки подключаемых модулей браузеров. В Linux набор подключаемых модулей более ограничен; впрочем, наиболее существенные всегда поставляются. В их число входят следующие:

- Macromedia Flash и Shockwave/Director;
- RealNetworks Realplayer;
- Adobe Acrobat Reader.

Ниже рассматривается технология каждого подключаемого модуля.

Macromedia Flash и Shockwave/Director

Модуль Macromedia Flash уже используется с Linux в течение нескольких лет. Установить его достаточно просто. Однако в Linux Flash не обновляется автоматически, как это происходит в браузерах Windows. Убедитесь, что клиенты понимают, что им придется вручную периодически обновлять модули Flash.

Установить Flash так же просто, как и скачать с сайта Macromedia (www.flash.com). После скачивания файла (например, install_flash_player_7_linux.tar.gz) его следует разархивировать и перейти в каталог install_flash_player_7_linux/. После этого следует запустить сценарий установочной программы flash-player (например, flashplayer-installer) и следовать инструкциям на экране.

На время написания книги Shockwave/Director от Macromedia можно было установить в Linux только с помощью набора CrossOver Office Plugins (рассматривается далее). Впрочем, ситуация может измениться, поскольку Macromedia проявляет все больший интерес к Linux и доля рынка этой корпорации расширяется. Однако особой производственной оправданности продукт не имеет, и его функциями мало кто пользуется, исключая, возможно, компьютерных художников и домашних пользователей. Одним словом, если нужен Shockwave/Director, рекомендуем установить набор CrossOver Office Plugins.

RealPlayer

RealPlayer (см. рис. 11.18) — один из наиболее значимых подключаемых модулей, потому что он обеспечивает просмотр потокового вещания. Его можно использовать как для потокового аудио, так и видео.

Запустить RealPlayer можно из любого web-браузера, описанного в данной главе. Например, в Konqueror появится запрос о том, какое программное приложение следует запустить. Достаточно просто ввести название исполняемого файла RealPlayer (например, realplay), и пользователь сразу сможет просматривать или прослушивать выбранный носитель. Базовую версию RealPlayer можно скачать бесплатно с сайта www.realplay.com. Относительно используемой версии следует проконсультироваться с заказчиками.

Рис. 11.18. RealPlayer

RealPlayer можно определить как «вспомогательное приложение» для надлежащего проигрывания потокового видео. Для этого в любом браузере откройте **Preferences** (Предпочтения) и осуществите доступ к соответствующему окну, в котором можно задать файловые ассоциации. Например, в Konqueror придется войти в **Settings** (Настройки) / **Configure Konqueror** (Сконфигурировать Konqueror), после чего выбрать окно **File Associations** (Ассоциация файла). В Mozilla нужно войти в меню **Edit** (Правка) / **Preferences** (Предпочтения), выбрать **Helper Application** (Вспомогательное приложение), после чего задать соответствующий тип MIME. В число обычных типов MIME для потоковых сред (носителей) входят следующие:

- application/x-pn-realaudio (для файлов rm и ram);
- audio/x-realaudio (для файлов ra);
- audio/x-wav (для файлов wav).

Adobe Acrobat Reader

Другим важным модулем является Adobe Acrobat Reader (см. рис. 11.19).

На определенных браузерах может потребоваться задание типа MIME для PDF. Типы MIME — следующие:

- application/pdf;
- application/x-pdf;
- application/acrobat;
- text/pdf;
- text/x-psdf.

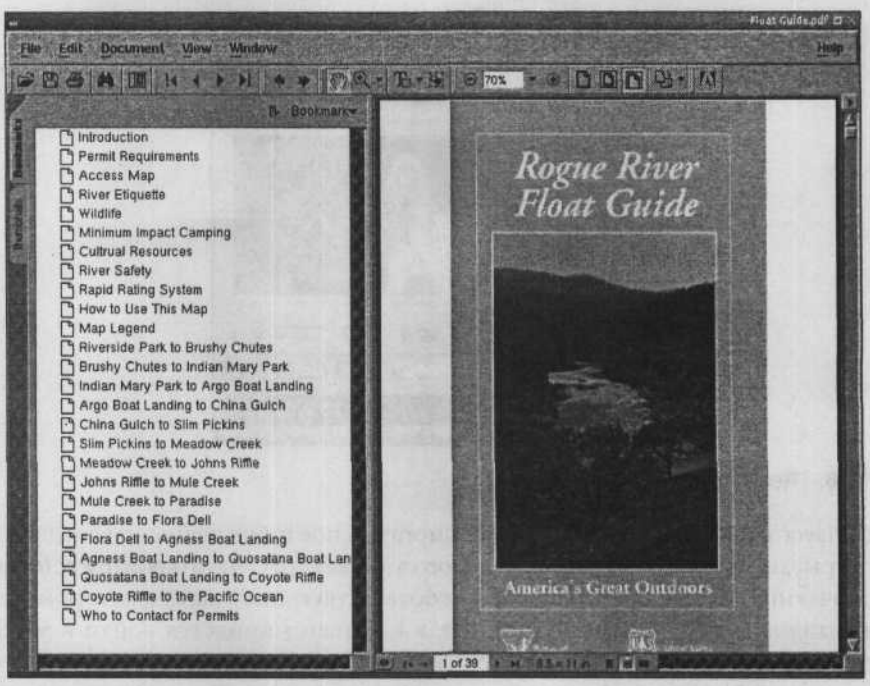

Рис. 11.19. Acrobat Reader

Типа application/pdf, как правило, достаточно. Acrobat Reader можно скачать бесплатно на сайте www.adobe.com.

Офисные пакеты

Итак, перевод рабочих станций на почтовые/PIM клиенты и web-браузеры на базе Linux рассмотрен. Консультанты наверняка найдут способ удовлетворить потребности клиентов при работе с электронной почтой и приложениями на основе браузеров. Однако конечные пользователи не только целыми днями пользуются электронной почтой и web-браузерами, они также создают документы и презентации. Они спросят: «Где Microsoft Word?». Тот же вопрос будет относиться к Excel и PowerPoint. Другими словами, людям будет интересно знать, смогут ли они работать со своими файлами.

Всем нужно делать свою работу, и пользователям не очень понравится, если операционная система станет «преградой» на этом пути. Руководители озаботятся спадом производительности. Перед консультантом встанет непростая задача убедить и тех, и других в том, что даже при отходе от Microsoft Office производительность сохранится. Ему придется доказать, что пользователи:

- по-прежнему смогут работать с файлами типов .doc, .rtf, .xls и .ppt;
- достаточно быстро привыкнут к новым программам;
- смогут обмениваться файлами с пользователями, по-прежнему работающими с программными средствами Microsoft.

Наиболее распространенное программное обеспечение для работы в офисе включает в себя следующие продукты:

- OpenOffice.org;
- StarOffice;
- KOffice;
- Hancom Office.

Далее описывается каждый из этих продуктов .

OpenOffice.org

Продукт OpenOffice.org очень быстро стал стандартным для офисного набора Linux, после представления корпорацией Sun в 1999 году. OpenOffice включает в себя несколько программных приложений:

- **StarWriter (swriter)** Текстовый редактор; эквивалент Microsoft Word.
- **Star Impress (simpress)** Продукт для демонстрации слайдов; эквивалент Microsoft PowerPoint.
- **Star Calc (scalc)** Продукт для создания электронных таблиц; эквивалент Microsoft Excel.
- **Star Web (sweb)** Продукт для создания web-страниц; эквивалент продукта Microsoft FrontPage Express.

В принципе, после установки OpenOffice делать ничего не приходится. Если происходит обмен документами за пределами компании (как чаще всего и происходит), то решение этой задачи для пользователей можно упростить настройкой OpenOffice для сохранения файлов в форматах .doc, .xls или .ppt. Делается это выбором меню **Tools>Options>Load&Save>General** (Сервис>Настройки>Загрузка и сохранение>Общие) и в разделе стандартного формата файла выбором опции **Always save as Microsoft Word 97/2000/XP for Document type, text document** (всегда сохранять текстовые документы в формате Microsoft Word 97/2000/XP). Выполните то же самое для опции **Spreadsheet and Presentations** (Электронные таблицы и презентации). Убедитесь, что шаблоны не выбраны, потому что это делается по-другому. Более подробная информация об OpenOffice имеется на сайте www.openoffice.org.

В OpenOffice.org можно открыть любой документ, созданный в Microsoft Office 2000. Например, документ, показанный на рис. 11.20, был создан в Microsoft Office 2000.

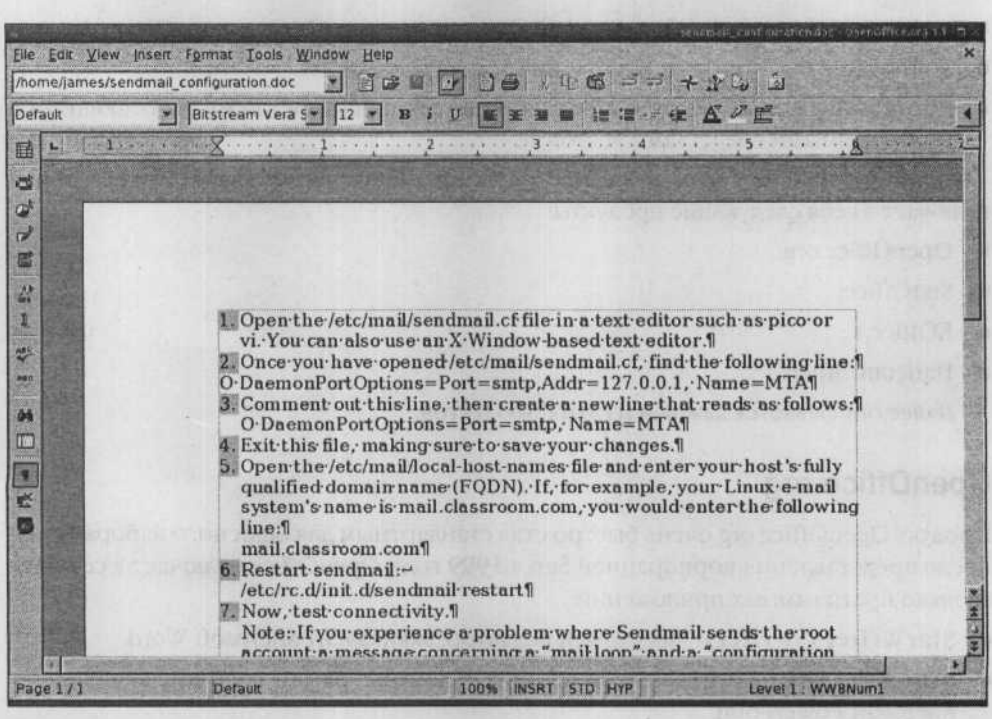

Рис. 11.20. Star Writer

В документ, показанный на рис. 11.21, также были внесены изменения в Office 2003. На рис. 11.21 показана программа Star Impress. Видно, что интерфейс очень напоминает PowerPoint.

Документ, показанный на рис. 11.21, был создан в PowerPoint, после чего открыт в программе Star Impress. На самом деле большинство слайдов для данной презентации были созданы в Star Impress. Затем презентация была отправлена нескольким лицам, которые работали только с Microsoft Power Point. Было совершенно неочевидно, что некоторые слайды создавались в Linux.

На рис. 11.22 показана программа Star Calc с обычной электронной таблицей.

Таблица на рис. 11.22 достаточно проста. Впрочем, мало кто выполняет какие-либо иные операции в электронных таблицах, кроме создания строк и столбцов с последующим подсчетом сумм. Обратите внимание, что данная таблица поддерживает таблицы с «вкладками».

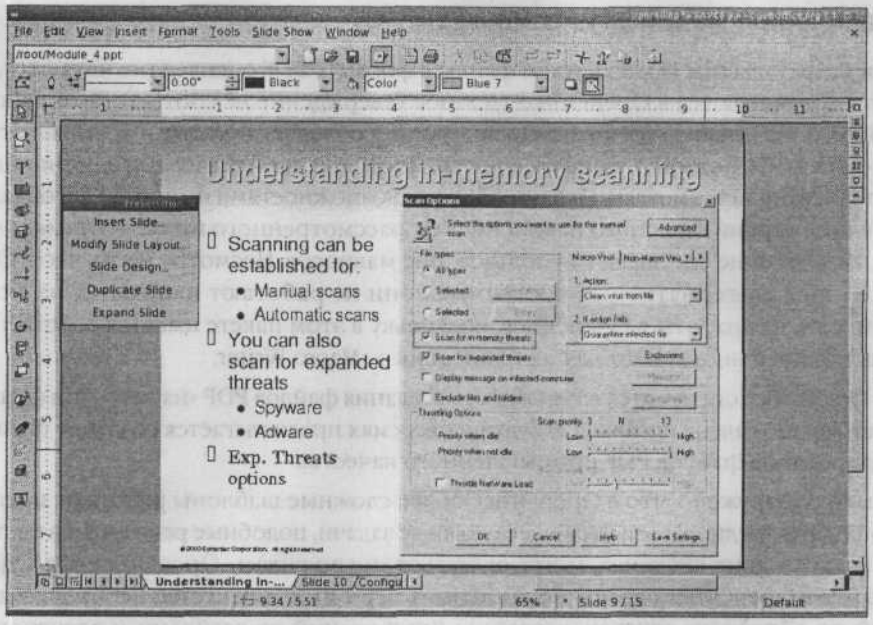

Рис. 11.21. Star Impress

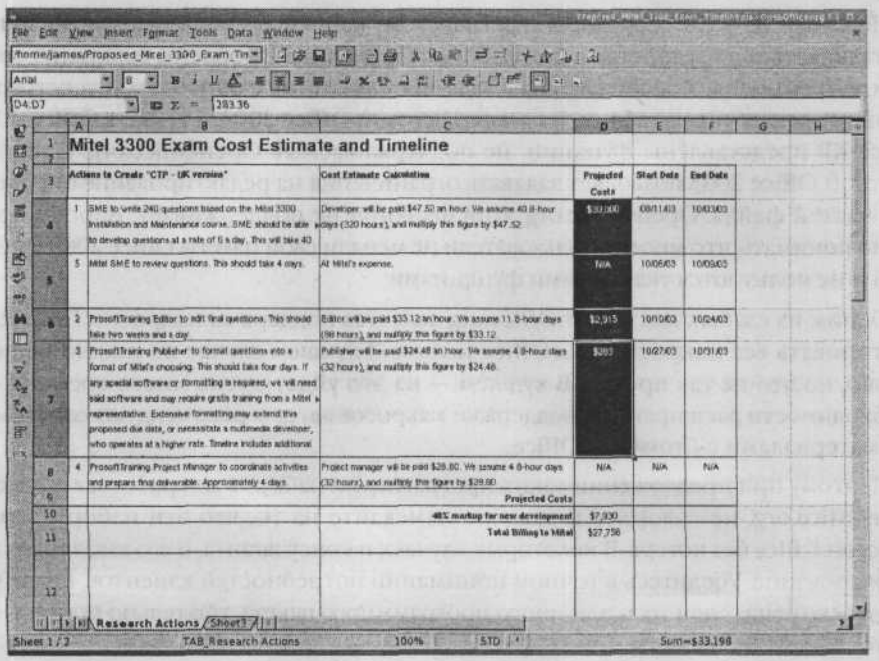

Рис. 11.22. Star Calc

Ограничения: макросы и файлы PDF

За очень небольшим исключением файлы в формате PDF очень легко читаются, создаются и изменяются в OpenOffice. (Данное утверждение не соответствует действительности. Начиная с версии 1.1 OpenOffice.org обладает богатыми возможностями экспорта в PDF, однако импорт этих файлов, т. е. их чтение и модификация в OpenOffice.org невозможны. Ограниченными возможностями импорта PDF обладают последние версии офисного пакета KOffice, рассмотренного ниже. — *Примеч. науч. ред.)*. Исключение составляет использование макросов. Несмотря на то, что в OpenOffice или в альтернативных программах они не работают напрямую, их можно переписать для работы в OpenOffice, поскольку в этом пакете имеется собственный очень мощный инструмент для их написания — Macro Writer.

В OpenOffice.org имеется возможность создания файлов PDF «на лету». Эта функция впечатляет, но она не идеальна. В будущих версиях предполагается создание функции генерирования файлов PDF промышленного качества.

Было обнаружено, что в OpenOffice более сложные шаблоны работают не очень хорошо. Это предполагает, что более сложные задачи, подобные решаемым в настольных издательских системах, могут оказаться «не по силам» OpenOffice.org. Однако при этом в OpenOffice.org можно выполнять огромное множество необходимых заданий по обработке текстов, созданию презентаций со слайдами и электронных таблиц.

Несмотря на все это, среднестатистическому конечному пользователю не придется сталкиваться с трудностями при работе с OpenOffice. Проблемы возникнут только у тех, кто выполняет особо сложные задания, связанные с обработкой текстов и созданием электронных таблиц. В пакете Microsoft Office 2003, а также в Office 2000 и Office XP представлены функции, не поддерживаемые OpenOffice.org. Например, Microsoft Office 2003 позволяет задавать ограничения на редактирование определенных частей файла. OpenOffice.org этой функции не поддерживает. Впрочем, здесь важно понимать, что многие пользователи не меняли свои пакеты Office 2000 на Office 2003 и не пользуются указанными функциями.

Одним из слабых мест OpenOffice.org является поддержка макросов. Просто импортировать все макросы в StarOffice нельзя. В лучшем случае их можно написать заново, но это не так просто. В худшем — на это уйдет очень много времени. При необходимости расширенной поддержки макросов авторы рекомендуют ознакомиться с материалами о CrossOver Office.

Поэтому при предложении таких программных наборов для работы в офисе, как OpenOffice.org, не говорите и даже не намекайте на то, что эти наборы заменят Microsoft Office без потерь. В некоторых случаях и консультанта, и его заказчиков ждет разочарование. Убедитесь в точном понимании потребностей клиентов, после чего, перед рекомендацией того или иного программного пакета, тщательно протестируйте его.

Планы на будущее

Вероятно, в будущем пакет OpenOffice.org сможет создавать файлы Shockwave Flash (SWF) «на лету». (В настоящий момент возможность экспорта презентации в формат SWF присутствует в OpenOffice.org Impress 1.1. — *Примеч. науч. ред.)*. До сих пор ни один офисный набор не имеет этих функций. OpenOffice.org уже использует XML в качестве основы для своих файлов. Следовательно, этот набор может обрабатывать сложные задания. Для проекта OpenOffice.org создание таких продуктов, как Microsoft Office — вопрос времени.

StarOffice

StarOffice — по сути устойчивая версия OpenOffice.org с обеспечением технического обслуживания заказчиков. Вероятно, здесь поможет сравнительная аналогия: StarOffice для OpenOffice.org — все равно что Netscape Navigator для Mozilla. Подобно тому, как Netscape берет надежную версию Mozilla и продает ее, Sun берет OpenOffice.org и продает ее как StarOffice.

Корпоративное доверие к StarOffice постепенно растет, потому что компании одновременно приобретают гарантию на техническое обслуживание на случай появления проблемы или ошибки. За номинальную плату можно получить техническое обслуживание, хранилище файлов на базе Интернет, а также расширенную поддержку макросов. Более подробная информация о StarOffice — на сайте www.staroffice.com.

KOffice

Проект рабочей группы KDE — KOffice — это полнофункциональная замена Microsoft Office. На рис. 11.23 показано программное приложение KWrite — текстовый редактор по умолчанию для KDE. Будучи более мощным, нежели такой простой текстовый редактор, как Wordpad или Notepad, он все-таки уступает по мощности редактору Star Writer. (К этому заявлению авторов можно относиться разве что, как к неуместной шутке. KWrite не входит в пакет KOffice и является устаревшей заменой Блокнота Windows в KDE (сейчас предполагается использовать Kate вместо KWrite). Текстовый процессор KOffice называется KWord и имеет очень развитые возможности, в том числе поддержку концепции «кадров» — frames, что делает его похожим на настольную издательскую систему. Однако существующие на момент подготовки к печати русскоязычной версии книги редакции KOffice очень плохо поддерживают форматы Microsoft Office, что является их главным недостатком с точки зрения конечного пользователя. — *Примеч. науч. ред.)*.

Hancom Office

Продукт Hancom Office продается корейской компанией; цели его следующие:

- создание дружественного пользователю программного набора, совместимого с Microsoft Office;
- поддержка большого количества языков. Расширенная поддержка Unicode означает, что Hancom Office — идеальный продукт на случай, если в компании приходится работать с текстами на китайском (упрощенном и традиционном), корейском и арабском языках.

Подробности о Hancom Office доступны на сайте www.hancom.com. Один из способов, посредством которого Hancom Office делает попытки обеспечения совместимости с документами Microsoft Office, — это функция автоматического обновления. Эта функция обеспечивает оперативное получение самых последних фильтров и механизмов визуализации (представления).

Одним из ограничений Hancom Office является отсутствие поддержки макросов, написанных в Visual Basic. Hancom Office в этом смысле не лучше OpenOffice.org или StarOffice.

Запуск приложений Windows на Linux

Легко понять, что в любое время перевести любого пользователя на платформу Linux будет невозможно. Вместо того, чтобы мириться с поражением, можно воспользоваться двумя вариантами:

- **Эмулятор** Установите программное обеспечение, позволяющее системе Linux, так сказать, имитировать систему Windows. После корректной установки эмулятора остается только установить в систему Linux программное приложение Windows. После этого эмулятор позволит работать с этой программой из среды Linux.
- **Программные средства удаленного управления рабочим столом** Достаточно просто установить сервер, обеспечивающий непосредственный доступ к рабочему столу через web-браузер или специализированное приложение.

Каждая из представленных опций описывается ниже.

Программные средства уровня совместимости

Во многом рассматриваемые программные средства не являются эмуляторами. Строго говоря, программы-эмуляторы восстанавливают программные интерфейсы приложений (API) и фактические функции CPU (например, процессор класса Pentium). Wine, CrossOver Office и Win 4 Lin Workstation не восстанавливают архитектуру CPU. Следовательно, в техническом смысле они не являются эмуляторами.

Несмотря на это, распространенной практикой по-прежнему является выделение этих программных средств в категорию эмуляторов, потому что при использовании таких приложений, как Wine, систему Linux можно заставить «вести себя» как система Windows. На самом деле, при надлежащей конфигурации этих приложений определенные «родные» приложения Windows будут работать, ошибочно предполагая, что они работают в среде Windows. Эти приложения используют наборы API, целью которых является «убеждение» программных приложений Windows в том, что они действительно работают в этой среде.

Поэтому во избежание противоречий авторы не будут называть эти приложения «эмуляторами», даже несмотря на то, что, в принципе, они таковыми и являются. С легкой руки разработчиков Wine называем их «программными средствами уровня совместимости», потому что все они создают уровень (прослойку) между операционной системой Linux и приложением Windows.

Преимуществом данного типа эмуляторов — нет, программного обеспечения — является то, что с «родными» программами Windows можно работать непосредственно на рабочей станции с системой Linux. При этом нет необходимости полагаться на сетевое подключение к другой системе. Впрочем, иногда настройка конфигурации эмуляторов превращается в довольно тонкую операцию, и малейшее изменение конфигурации приложения может «сломать» конфигурацию пользователя, в резуль-

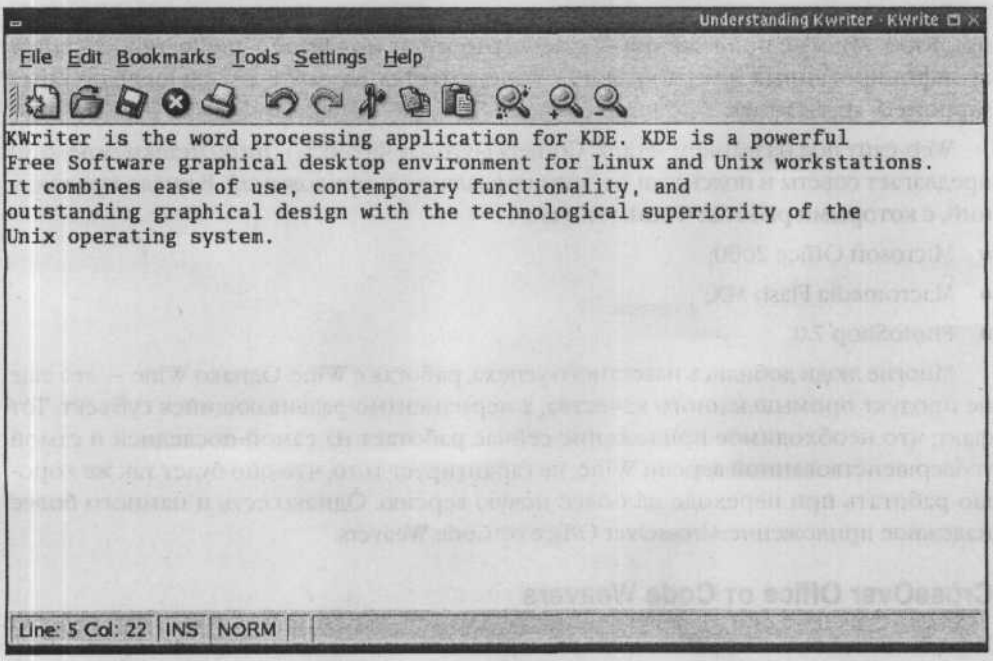

Рис. 11.23. KWriter

тате чего масса времени и, возможно, денег будет потрачена на вызов технической службы.

При подготовке к использованию эмулятора задайте себе следующие вопросы:

- Какую версию операционной системы Windows требует программное приложение?
- Требуется ли доступ к необработанным данным из системы Linux?
- Скольким пользователям необходим одновременный доступ к этим приложениям и данным в них? То есть, какова ожидаемая нагрузка на подобную систему?

Эти вопросы помогут точно определить размер аппаратных средств, а также нужное программное обеспечение. Теперь рассмотрим некоторые из наиболее распространенных эмуляторов.

Wine

«Wine» — это акроним английской фразы «Wine Is Not an Emulator» («Wine — это не эмулятор»). Изначально предполагалось, что Wine заменит Windows; для его работы Windows не требуется. Следовательно, для работы с программным приложением Windows лицензия на Windows также не требуется. Однако, лицензия все равно понадобится. Например, предположим, что удалось запустить Microsoft Word на Wine. Лицензия на Windows в этом случае не нужна, но нужна на Microsoft Word.

Важно понимать, что в течение многих лет Wine имеет статус развивающегося продукта. Многие приложения Windows работают под Wine. Список приложений, верифицированных для работы под Wine, имеется на сайте www.winehq.org/site/supported_applications.

Web-сайт под названием «Frank' Corner» («уголок Фрэнка») (http://frankscorner.org) предлагает советы и подсказки по запуску различных приложений. В число приложений, с которыми работал Фрэнк, входят:

- Microsoft Office 2000;
- Macromedia Flash MX;
- PhotoShop 7.0.

Многие люди добились известного успеха, работая с Wine. Однако Wine — это еще не продукт промышленного качества, а перманентно развивающийся субъект. Тот факт, что необходимое приложение сейчас работает на самой последней и самой усовершенствованной версии Wine, не гарантирует того, что оно будет так же хорошо работать при переходе на более новую версию. Однако есть и намного более надежное приложение: CrossOver Office от Code Weavers.

CrossOver Office от Code Weavers

По сути дела, CrossOver Office — это усовершенствованная коммерческая версия Wine. CrossOver Office обеспечивает бесперебойную работу любого (Это не так. Разработ-

чики CrossOver Office гарантируют бесперебойную работу избранных, наиболее популярных приложений, в числе которых Microsoft Office, Internet Explorer и некоторые другие. Работа других приложений в CrossOVer Office не гарантируется. — *Примеч. науч. ред.)* приложения Windows («бесперебойную» настолько, насколько это определение уместно при обсуждении совместимости программных средств). Так же, как и в случае с Wine, при работе с CrossOver Office лицензия на Windows не нужна. Пользователи обнаружат, что при работе с CrossOver Office обновления не вызовут сбоя существующей конфигурации. Кроме того, CrossOver Office обеспечивает запуск любых макросов, написанных на Visual Basic, на которые рассчитывают многие пользователи Microsoft Office.

Установка CrossOver Office и запуск приложения Windows под Linux — операции сравнительно простые. Однако и здесь не обошлось без определенных недостатков. Во-первых, CrossOver Office требует большого объема памяти. Помимо этого, не все функции приложений Windows будут доступны. Поэтому, даже если и удастся запустить копию Macromedia Flash MX, то некоторые возможности будут отсутствовать.

Несмотря на эти недостатки, возможно, пользователи поймут, что при работе с альтернативными программами, рассмотренными выше, и такими приложениями, как CrossOver Office, перевести на Linux можно любого пользователя. Подробности о CrossOver Office выложены на сайте www.codeweavers.com/site/products.

Резюме

Выбор надлежащей настольной рабочей среды требует определенных навыков. Во-первых, необходимо знать возможности. Во-вторых, необходимо знать потребности заказчиков и то, в какой мере существующие технологии могут их удовлетворить. В данной главе описаны доступные технологии и их потенциальное соответствие потребностям заказчиков.

Начиная такими распространенными настольными средами, как Gnome и KDE, и заканчивая программными приложениями для работы с электронной почтой и web-браузерами, читатели научились давать рекомендации, экономящие время и деньги конечных пользователей. Они также научились переносить настройки и устанавливать «родные» Windows-приложения на Linux, которые, по каким-то причинам, не могут быть замещены эквивалентами этой операционной системы.

Материал главы помог выявлению проблем, возможностей и решений. Теперь, когда читатели имеют более широкое представление о программных решениях настольной рабочей среды Linux, они имеют возможность продолжить процесс обучения, попробовав установить какое-либо программное обеспечение, описанное в данной главе. Единственным способом движения вперед в развитии и навыках решения проблем является самостоятельное прохождение процесса установки программных средств.

Краткое резюме по разделам

Традиционные настольные среды

- ☑ Две наиболее популярные настольные рабочие среды — Gnome и KDE.
- ☑ Системы Gnome и KDE очень похожи друг на друга.
- ☑ Задачей консультанта является оценка сравнительных преимуществ каждой системы.
- ☑ Клиентам необходимо предоставить возможность подробного рассмотрения существующих настольных сред для осознанного выбора между ними.

Серверы X Window и Диспетчеры управления окнами

- ☑ Сервер X Window отвечает за обеспечение ресурсами диспетчера управления окнами, выступающего в качестве клиента.
- ☑ Можно сделать выбор из нескольких диспетчеров управления окнами.
- ☑ Диспетчер управления окнами — не то же самое, что настольная рабочая среда; диспетчер окон входит в настольную среду.
- ☑ Диспетчеры управления окнами помогают определить внешний вид элементов, предоставляемых настольной средой, ощущение от них, включая то, как они расположены на рабочем столе, как выглядят панели инструментов и гарнитуры шрифтов.

Клиенты электронной почты и управления персональной информацией

- ☑ Существует очень много программ-клиентов электронной почты. Одни представляют собой простые почтовые клиенты, другие имеют доступ к функциям коллективного пользования, включая ежедневники и планирование.
- ☑ Перенос настроек электронной почты требует принятия промежуточной стратегии, когда настройки сначала переносятся в один браузер, а затем — в другой. Данная стратегия помогает в переводе информации в формат, распознаваемый почтовым браузером назначения.
- ☑ Если больше ничего не срабатывает, почтовые сообщения можно перенести простой переадресацией с одной машины на другую.

Web-браузеры

- ☑ Вполне вероятно, что ни один web-браузер не удовлетворит потребностей всех пользователей.
- ☑ В настоящее время браузеры используются для доступа к информации всех типов.
- ☑ Последние версии Mozilla имеют возможность выполнения сеансов на базе Microsoft CHAP.

Офисные пакеты

- ☑ Для поддержания производительности труда пользователи должны работать с программными приложениями, помогающими им выполнять свои обязанности.
- ☑ В сферу ответственности консультанта входит обеспечение максимальной прямолинейности и правдивости относительно возможностей и функций наборов для работы в офисе, доступных в Linux. Не преувеличивайте. Предоставьте пользователям возможность «пробного запуска» для того, чтобы они точно знали, что их ждет в будущем.
- ☑ Может показаться, что программное средство OpenOffice.org — самое лучшее, *потому что, во-первых, в нем много функций, а во-вторых, оно бесплатное*. Однако в некоторых случаях OpenOffice.org и даже StarOffice недостаточно. Тогда, возможно, придется приобрести продукт Hancom Office и даже изучить процесс запуска «родных» приложений Windows в среде Linux.

Запуск приложений Windows на Linux

- ☑ Такие приложения, как Wine (www.winehq.org) не являются строго эмуляционными программными средствами. Настоящие эмуляторы имитируют запуск библиотек необходимых средств и фактического CPU (например, процессора Pentium). Wine просто содержит средства программного интерфейса приложения (API), необходимые для того, чтобы заставить родные приложения Windows думать, что они в самом деле работают под Windows (а не в Linux).
- ☑ При работе с эмуляторами следует задать себе как минимум три вопроса: первый: «какую версию операционной системы Windows требует программное приложение?»; второй: «требуется ли доступ к необработанным данным из системы Linux?»; третий вопрос определяет ожидания от системы: «скольким пользователям необходим одновременный доступ к этим приложениям и данным в них? То есть, какова ожидаемая нагрузка на подобную систему?»
- ☑ Система CrossOver Office от Code Weavers представляет собой коммерческую версию Wine. Поэтому она намного более надежна. При этом следует помнить о том, что CrossOver Office имеет ограничения. Например, несмотря на то, что приложение Windows может работать, не все его функции будут доступны.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма «**Ask the Author**»). Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: Что лучше: KDE или Gnome?

О: Для ответа на этот вопрос следует изучить оба интерфейса и потребности конкретных заказчиков. Обратите внимание на такие аспекты, как производительность, гибкость и доступность приложения. Можно сделать так, что интерфейсы будут напоминать друг друга. Но эти среды можно настроить под требования заказчиков так, что они будут радикально различаться.

В: Могут ли приложения Gnome работать в средах KDE и Blackbox?

О: По большей части — да. Могут быть исключения, но, например, Evolution будет работать одинаково хорошо как под KDE, так и под Gnome. Kmail работает одинаково хорошо в Gnome и Blackbox.

В: Я принял решение о том, чтобы мои сотрудники пользовались тремя web-браузерами. Нужно ли устанавливать RealPlayer три раза?

О: Нет. Просто войдите в нужные меню для направления браузера на поиск двоичного кода RealPlayer (realplay). Возможно, потребуется задать тип MIME.

В: Я получаю запросы от руководителей разных отделов, которые хотят, чтобы их сотрудники имели необходимые программные средства для создания PDF. Они не хотят покупать Adobe Acrobat. Какие альтернативные программные приложения можно использовать для создания файлов PDF?

О: Их несколько: OpenOffice.org, StarOffice, Hancom Office и CrossOver Office.

В: Почему продукт CrossOver Office от Code Weavers устойчивее, чем Wine? Я думал, что они одинаковы.

О: CrossOver Office от Code Weavers — коммерческий продукт, над ежедневным совершенствованием которого работает специальная рабочая группа. Разработчики Wine не имеют столько времени.

ПРИЛОЖЕНИЯ
ПО ВОПРОСАМ ЗАЩИТЫ

В первых одиннадцати главах книги описаны инструментальные средства осуществления перевода сети с операционной системы Windows в среду Linux. В Приложениях по вопросам защиты предлагается наиболее важная информация по открытым инструментальным средствам мониторинга и обеспечения защиты сети. Более подробная информация о рассматриваемых программных средствах представлена в следующих источниках:

Анжела Орбау (Angela Orebaugh) и Гилберт Рамирес (Gilbert Ramirez) — ***«Ethereal Packet Sniffing»*** (Syngress ISBN: 1-932266-82-8).

Брайан Кэсуэлл (Brian Caswell) и Джей Били (Jay Beale) — ***«Snort 2.1 Intrusion Detection, Second Edition»*** (Syngress ISBN: 1-931836-04-3).

Рено Дересон (Renaud Deraison), Эйч-Ди Мур (HD Moore) и Джей Били (Jay Beale) — ***«Nessus Network Auditing»*** (Syngress ISBN: 1-931836-08-6).

Приложение А

Введение в сетевой анализ и Ethereal

Разделы:

- Понятие сетевого анализа и анализа пакетов
- Кому нужен сетевой анализ?
- Принципы работы сетевого анализатора
- Обнаружение сетевых анализаторов пакетов
- Защита от сетевых анализаторов пакетов
- Сетевой анализ и корпоративная политика

☑ Резюме

☑ Краткое резюме по разделам

☑ Часто задаваемые вопросы

Введение

«Почему сеть работает так медленно?», «Почему я не могу просмотреть свою почту?», «Почему невозможен доступ к совместно используемому ресурсу?», «Почему мой компьютер выполняет какие-то странные операции?». Наверняка, сисадмины, инженеры-сетевики или специалисты по обеспечению сетевой защиты слышали эти вопросы не раз. С этого начинается утомительный и иногда болезненный процесс устранения неисправностей. Прежде всего, проблема воспроизводится на компьютере сисадмина. Совершенно очевидно, что ни в локальной сети, ни в Интернет никаких решений не обнаруживается. Что делать? Проверять каждый сервер на предмет работоспособности? Проверять свой маршрутизатор? Проверять возможные неисправности сетевых карт каждого компьютера?

А как насчет следующего сценария: вы идете к главному концентратору или граничному маршрутизатору и конфигурируете один из неиспользуемых портов на предмет зеркального отображения портов. Подключаете свой ноутбук, запускаете сетевой анализатор и просматриваете тысячи пакетов Пользовательских протоколов данных (User Datagram Protocol, UDP) с назначением на порт 1434 с разными, возможно, произвольными, IP-адресами. Тут же применяются фильтры доступа для блокирования входа в сеть или выхода из нее этих пакетов до проведения более подробного изучения. После оперативного поиска в Интернет находится ответ. Дата — 25 января 2003 года, оказалась, что сеть поражена «червем» SQL Slammer. Проблема оказалась решенной сравнительно быстро благодаря профессионализму сисадмина и использованию системного анализатора.

Понятие сетевого анализа и анализа пакетов

Сетевой анализ — это перехват сетевого трафика и внимательное его изучение на предмет выявления проблем в сети. Сетевой анализатор декодирует или разбивает пакеты данных обычных протоколов и отображает сетевой трафик в формате, понятном человеку. Существуют другие обозначения сетевого анализа, вот некоторые из них: анализ трафика, анализ протоколов, анализ пакетов, «прослушка» и т. д. На сегодняшний день наиболее часто употребляемым обозначением сетевого анализа является «анализ пакетов» (Англ. sniffing. — *Примеч. науч. ред.)*. Впрочем, и это будет отмечено в настоящем приложении; из-за некоторых зловредных пользователей это словосочетание в прошлом имело отрицательный подтекст.

Сетевой анализатор может быть автономным аппаратным устройством со специализированным программным обеспечением либо просто программным продуктом, устанавливаемым на настольную рабочую станцию или ноутбук. Сетевые анализаторы доступны как бесплатно, так и за деньги. Различия сетевых анализаторов в основном зависят от таких функций, как, например, количество поддерживаемых декодеров протоколов, пользовательского интерфейса, а также графических и статистических возможностей. Другие различия связаны с возможностями выводов, например, функ-

ций экспертного анализа и качества декодирования протоколов. Несмотря на то, что несколько сетевых анализаторов дешифрируют одни и те же протоколы, некоторые из них делают это лучше других.

ПРИМЕЧАНИЕ «Sniffer» (с прописной буквы) — это торговая марка Network Associates, обозначающая серию продуктов Sniffer (анализатор пакетов). В промышленности это название стало нарицательным — «sniffer» (со строчной буквы) обозначает программу перехвата и анализа сетевого трафика.

На рис. А. 1 показано окно отображения сетевого анализатора Ethereal. Обычный сетевой анализатор отображает перехваченный трафик в трех панелях:

- **Резюме** В этой панели отображается одна строка резюме перехвата. Поля: дата, время, исходный адрес, адрес назначения, а также имя и информация о протоколе самого высокого уровня.
- **Описание** В данной панели в виде структуры дерева отображаются описания каждого из уровней, содержащихся внутри перехваченного пакета.
- **Данные** Здесь отображаются необработанные перехваченные данные в шестнадцатеричном формате и в формате ASCII.

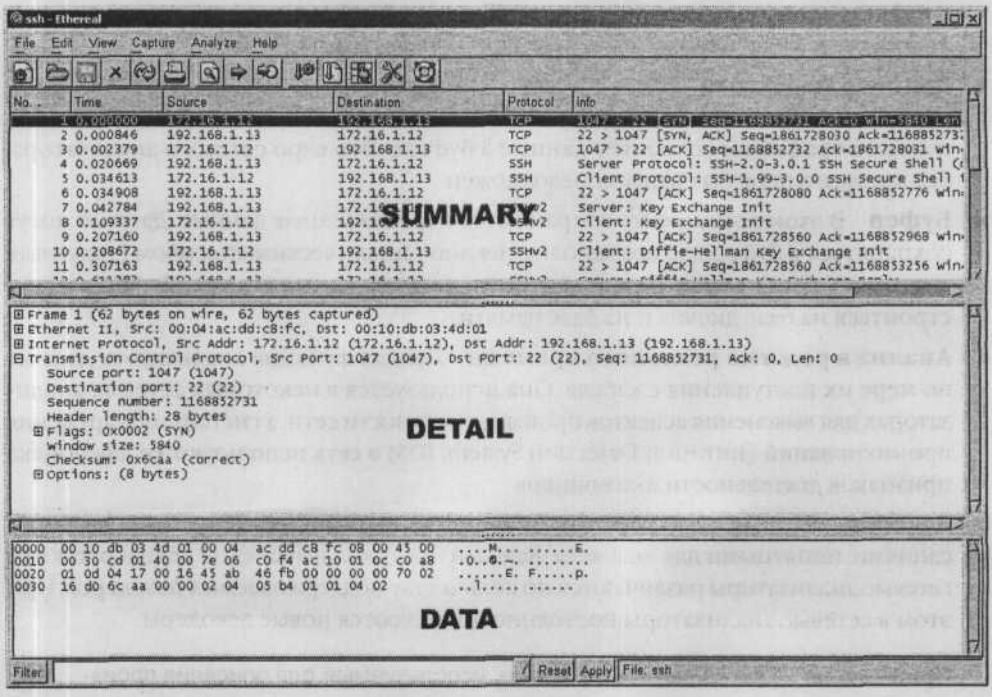

Рис. А. 1. Пример окна отображения сетевого анализатора Ethereal

Сетевой анализатор представляет собой комбинацию аппаратных средств и программного обеспечения. Хотя в различных продуктах сетевые анализаторы разные, любой из них состоит из пяти основных частей:

- **Аппаратные средства** Большинство сетевых анализаторов основано на программных средствах и работают в стандартных операционных системах и с сетевыми интерфейсными платами (сетевые адаптеры — NIC). Однако существуют и сетевые анализаторы со специализированными аппаратными средствами, предлагающими дополнительные преимущества, например анализ аппаратных сбоев, включая: контроль за ошибками при помощи циклического избыточного кода (CRC) (Схема определения ошибок при передаче данных: на основе полиномиального алгоритма вычисляется контрольная сумма передаваемого модуля данных и передается вместе с данными; получившее пакет устройство заново вычисляет контрольную сумму по тому же алгоритму и сравнивает ее с принятым значением; отсутствие расхождений говорит о высокой вероятности безошибочной передачи. — *Примеч. науч. ред.),* проблемы с питанием, кабелями, неустойчивую синхронизацию (дрожание), всевозможные сбои, ошибки согласования и т. д. Некоторые сетевые анализаторы поддерживают только Ethernet или беспроводные адаптеры; другие же поддерживают множественные адаптеры и позволяют пользователям конфигурировать систему под свои требования. Иногда для подключения к существующему кабелю необходим концентратор или отвод кабеля.
- **Драйвер перехвата** Часть сетевого анализатора, отвечающая за фактический перехват необработанного трафика с кабеля. Он также осуществляет фильтрацию нужного трафика и сохраняет данные в буфере. Это ядро сетевого анализатора, без которого перехват данных невозможен.
- **Буфер** В этом компоненте сохраняются перехваченные данные. Данные могут сохраняться в буфере до его заполнения либо циклическим способом («круговая система»), когда самые новые данные замещают самые старые. Буферы могут строиться на базе дисков и на базе памяти.
- **Анализ в режиме реального времени** Данная функция анализирует данные по мере их поступления с кабеля. Она используется в некоторых сетевых анализаторах для выяснения аспектов производительности сети, а системы обнаружения проникновений (Intrusion Detection System, IDS) в сеть используют ее для поиска признаков деятельности взломщиков.
- **Декодер** Данный компонент отображает содержимое сетевого трафика с описаниями, понятными для человека. Каждый протокол имеет свой декодер, так что сетевые анализаторы различаются по количеству поддерживаемых декодеров. При этом в сетевые анализаторы постоянно добавляются новые декодеры.

Примечание *Дрожание* — это термин, используемый для описания произвольных колебаний синхронизации сигнала. Дрожание может быть вызвано электромагнитными помехами и перекрестными помехам других сигналов.

Сбой происходит тогда, когда какое-то устройство некорректно обрабатывает электрические сигналы, что влияет на остальные устройства сети. Неисправные сетевые интерфейсные платы могут вызвать сбой.

Кому нужен сетевой анализ?

Сисадмины, инженеры сетей, инженеры по безопасности, системные операторы и даже программисты применяют в своей работе сетевой анализ. Сетевые анализаторы представляют собой уникальные инструменты для диагностики и устранения сетевых проблем. Сетевые анализаторы всегда были выделенными устройствами и всегда стоили очень дорого. Новые шаги в технологии обеспечили развитие программных сетевых анализаторов. При этом задачи администраторов по эффективному устранению сетевых проблем значительно упростились. Сетевые администраторы также обеспечивают возможность сетевого анализа всем, кто в этом заинтересован.

Мастерство сетевого анализа — это «палка о двух концах». В то время как специалисты по сетям, защите и системам применяют его для устранения неисправностей и мониторинга сети, так называемые «взломщики» могут применять сетевой анализ в злонамеренных целях. Сетевой анализатор — это инструмент, и, как любой инструмент, его можно использовать как для пользы, так и для вреда.

В нижеприведенном списке перечислены некоторые причины применения администраторами сетевого анализа:

- преобразование двоичных данных в пакетах в формат, распознаваемый человеком;
- поиск и устранение сетевых неполадок;
- анализ производительности сети для обнаружения «узких мест»;
- обнаружение несанкционированного проникновения в сеть;
- регистрирование сетевого трафика для судебных разбирательств и сбора доказательств;
- анализ операций, выполняемых программными приложениями;
- выявление неисправных сетевых плат;
- выявление источников атак типа «Отказ в обслуживании» (DoS);
- обнаружение шпионских программ;
- сетевое программирование для исправления ошибок на этапе разработки;
- обнаружение дискредитированного компьютера;
- подтверждение соблюдения корпоративной политики;
- использование в качестве обучающего ресурса при изучении протоколов;
- инженерный анализ протоколов для написания клиентов и поддерживающих их программ.

Как взломщики сетей используют анализаторы пакетов?

Когда анализаторы пакетов используются злоумышленниками, они могут представлять значительную угрозу безопасности сети. Взломщики сетей часто используют сетевой анализ пакетов с целью похищения ценной конфиденциальной информации. С этой практикой часто связывают жаргонные термины «вынюхивание» (одно из значений слова «sniffing») и «прослушка». Впрочем, теперь слово sniffing уже практически потеряло свой отрицательный оттенок, и для большинства людей термины «анализ пакетов» и «сетевой анализ» взаимозаменяемы.

Использование сетевого анализатора в незаконных целях рассматривается как пассивная атака. Он не подключается и не связывается ни с какими другими системами в сети. Однако компьютер, на который установлен анализатор пакетов, может быть поврежден в результате активной атаки. Именно пассивная природа анализаторов пакетов чрезвычайно осложняет их обнаружение. Далее в приложении будут рассмотрены способы обнаружения сетевых анализаторов пакетов.

В нижеприведенном списке представлены несколько причин использования сетевых анализаторов взломщиками сетей:

- перехват имен пользователей и паролей, передающихся открытым текстом;
- похищение закрытой информации;
- перехват и воспроизведение телефонных разговоров, переданных по системе Voice over IP (VoIP);
- построение карты сети;
- пассивное снятие «отпечатков» операционной системы.

Очевидно, что все перечисленное в отношении сетевых анализаторов пакетов — незаконно, если человек не является тестером несанкционированного проникновения в сеть, в задачи которого входит обнаружение указанных видов слабых мест и сообщение о них заинтересованным лицам организации.

Для того, чтобы анализ пакетов состоялся, злоумышленник, прежде всего должен получить доступ к кабелю связи интересующих его систем. Это означает его нахождение в том же сегменте коллективного пользования сети либо создание ответвления от кабеля в каком-либо месте между каналами связи. Если злоумышленник не присутствует в нужной ему системе или точке доступа к кабелю связи физически, у него все равно есть возможности прослушивания сетевого кабеля. В их числе — следующие:

- взлом интересующего компьютера и установка на него удаленно управляемой программы анализа сетевых пакетов;
- врезка в точку доступа к кабелю связи, например к ISP (Internet Service Provider, провайдер услуг Интернет);
- обнаружение/нахождение у ISP системы, на которой уже установлены программные средства сетевого прослушивания;
- использование социотехники для получения физического доступа к ISP для установки анализатора пакетов (Имеется в виду комплекс социально-психоло-

гических действий, направленных на сотрудника провайдера и имеющих целью «выпросить» (путем обмана, угроз и т. п.) доступ к необходимым ресурсам. — *Примеч. науч. ред.)*;

- наличие сообщника в целевой организации или в ISP для установки анализатора;
- переадресация связи с выбором пути через компьютер злоумышленника.

Программы анализаторов сетей входят практически во все «руткиты» (Англ. rootkit — набор программ шпионского характера, скрытно устанавливаемый на компьютере жертвы в ходе активной атаки. — *Примеч. науч. ред.)*, которые обычно устанавливаются на дискредитированные системы. Руткиты используются для охвата каналов злоумышленника путем подмены команд и утилит и стирания записей журналов. Они также устанавливают другие программы: сетевые анализаторы, регистраторы нажатых клавиш и программы секретного доступа. Прослушка Windows может быть осуществлена как часть какого-либо RAT (Remote Admin Trojan), например SubSeven или Back Orifice. Злоумышленники часто применяют программы прослушки, сконфигурированные на выяснение конкретных вещей, например паролей, после чего в электронном виде отправляют их получателю (либо сохраняют до последующего скачивания злоумышленником). Для подобного рода деятельности уязвимы такие протоколы, как Telnet, FTP, POP3, IMAP, SMTP, HTTP, rlogin и SNMP (Все они передают пароли в открытом или слабозашифрованном виде. — *Примеч. науч. ред.)*.

Одним из примеров руткита является T0rnKit, работающий под Solaris и Linux. Анализатор пакетов, включенный в этот руткит, называется t0rns и установлен в скрытый каталог /usr/srec/.puta. Другой пример руткита — Lrk5 (Linux Rootkit 5), который устанавливается с анализатором linsniff.

Злоумышленники обычно используют программы анализаторов для управления так называемыми «лазейками». Один из способов — установка в целевую систему анализатора, который прослушивает нужную информацию. После этого информация, управляемая лазейкой, может отправляться в соседнюю систему. Анализатор собирает ее и совершает соответствующие действия в целевой системе. Часто такой тип управления лазейками очень трудно обнаружить, поскольку он выглядит так, что «невинная» соседняя система и является дискредитированной целью.

Cd00r — пример лазейки-анализатора, работающей в упорядоченном режиме, что еще более усложняет ее обнаружение. Использование продукта, подобного Nmap, для отправки серии TCP (Transmission Control Protocol) SYN пакетов на несколько предварительно заданных портов открывает лазейку на предварительно заданном порту. Более подробная информация о Cdoor выложена на сайте www.phenoelit.de/stuff/cd00r.c.

ПРИМЕЧАНИЕ *Руткит* — это набор программ-троянов, используемых для подмены настоящих программ в дискредитированной системе, во избежание обнаружения. В число некоторых программ, которые могут быть подменены, входят *ps*, *ifconfig* и *ls*. Корневые наборы также устанавливают дополнительные программные средства, например анализаторы пакетов.

ПРИМЕЧАНИЕ Nmap — инструмент сканирования сети для ее исследования и аудита. Может отправлять необработанные пакеты IP на порты назначения целевых систем.

Как выглядят «прослушанные» данные?

Уже много сказано о программах-анализаторах пакетов, о том, для чего они нужны, однако простейшим способом более точного понимания описанных положений будет наблюдение анализаторов пакетов в действии. На рис. А. 2 показан перехват простого сеанса FTP с ноутбука на систему Sun Solaris. Два выделенных пакета показывают, насколько просто «просканировать» имя пользователя и пароль. В данном случае имя пользователя — «root», а пароль — «password». Конечно, допуск суперпользователя по FTP в систему — очень ненадежная практика защиты, но здесь она представлена только для наглядности!

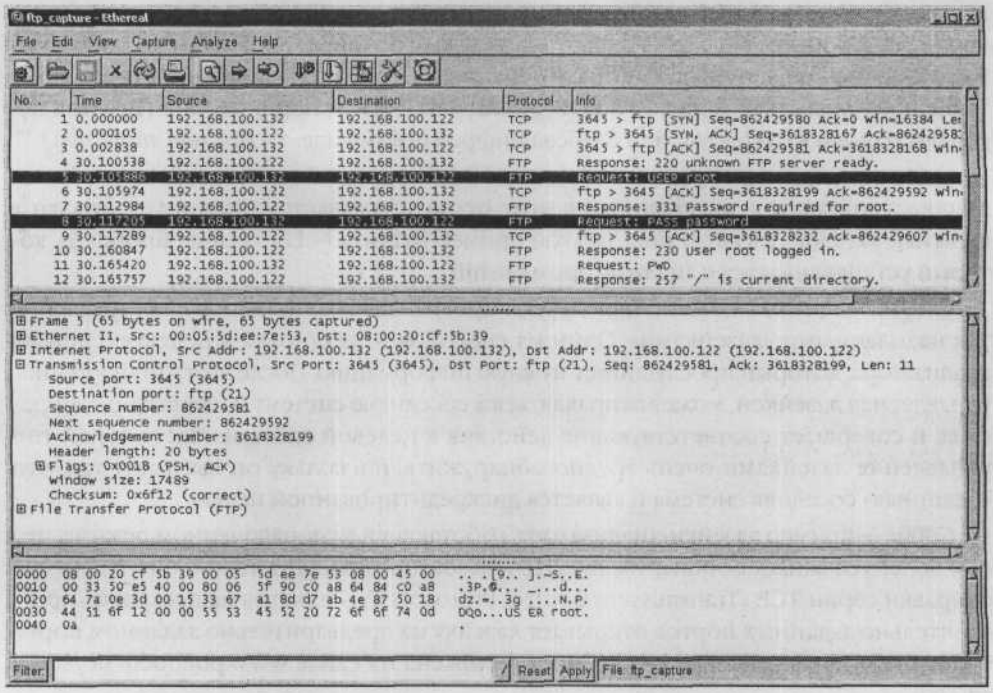

Рис. А. 2. Пример прослушивания подключения

Обычные сетевые анализаторы

Поиск на сайте SecurityFocus (www.securityfocus.org/tools/category/4) демонстрирует разнообразие и количество имеющихся анализаторов пакетов. Наиболее известные из них — следующие:

- **Ethereal** Разумеется, это одна из тем данной книги! Ethereal — один из самых лучших анализаторов. Разработан как бесплатный анализатор коммерческого качества. Имеет множество функций, прекрасный пользовательский графический интерфейс (GUI), декодирует свыше 400 протоколов и постоянно совершенствуется и дорабатывается. Работает в системах на базе UNIX и Windows. Очень хорош для использования даже в промышленной среде. Имеется на сайте www.ethereal.com.
- **WinDump** Версия tcpdump для Windows; имеется на сайте http://windump.polito.it. Использует библиотеку WinPcap и работает на Windows 95/98/ME/NT/2000/XP.
- **Network Associates Sniffer** Один из самых популярных коммерческих продуктов. Распространяемый через McAfee Network Protection Solutions, Network Associates имеет полную производственную линию Sniffer, доступную на сайте www.nai.com.
- **Windows 2000/NT Server Network Monitor** Windows 2000 Server и NT Server имеют встроенную программу для выполнения сетевого анализа. Она расположена в папке Administrative tools (Инструменты администрирования), но не устанавливается по умолчанию; при необходимости ее можно найти на установочном диске.
- **EtherPeek** Коммерческий сетевой анализатор от компании WildPackets. Существуют версии для платформ Windows и Mac, а также другие продукты сетевого анализа (см. www.wildpackets.com).
- **Tcpdump** старейший и самый распространенный сетевой анализатор. Разработан Группой сетевых исследований (Network Reseach Group, NRG) Отдела информационных и вычислительных технологий (Information and Computing Sciences Division, ICSD) в Национальной лаборатории Лоренс Беркли (Lawrence Berkeley National Laboratory, LBNL). Работает в командной строке и запускается на системах на базе UNIX. Активно дорабатывается и совершенствуется на www.tcpdump.org.
- **Snoop** Сетевой анализатор командной строки включен в операционную систему Sun Solaris. Особо полезен при декодировании протоколов, относящихся к системам Sun.
- **Sniffit** Данный сетевой анализатор работает под Linux, SunOS, Solaris, FreeBSD и IRIX. Доступен на http://reptile.rug.ac.be/~coder/sniffit/sniffit.html.

- **Snort** Система обнаружения несанкционированного проникновения в систему, использующая сетевой анализатор пакетов. Активно совершенствуется на www.snort.org. Более подробную информацию см. в *Snort 2.0: Intrusion Detection* (Syngress Publishing, ISBN: 1-931836-74-4).
- **Dsniff** Очень популярный пакет сетевого анализа пакетов. Представляет собой набор программ для анализа таких «интересных» данных, как пароли, а также для упрощения процесса анализа, например для уклонения от коммутаторов. Активно совершенствуется на www.monkey.org/~dugsong/dsniff.
- **Ettercap** Данный анализатор пакетов разработан специально для анализа коммутируемой сети. Имеет встроенные функции: сбор паролей, снятие «отпечатков» операционной системы и инжекция символов. Работает на нескольких платформах, включая Linux, Windows и Solaris. Активно совершенствуется на http://ettercap.sourceforge.net.
- **Analyzer** Бесплатный анализатор пакетов для Windows OS, активно совершенствуемый производителями WinPcap и WinDump в Politecnico di Torino (Политехнический университет г. Турина). Имеется на http://analyzer.polito.it.
- **Packetyzer** Бесплатный анализатор пакетов для Windows OS, использующий логические схемы Ethereal. Отстает на одну или две версии от текущего выпуска Ethereal. Активно совершенствуется Network Chemistry (www.networkchemistry.com/products/packetyzer/index.html).

Мысли вслух...

Carnivore или вегетарианец?

Обсуждение сетевых анализаторов было бы неполным без упоминания продукта под названием Carnivore (*англ.* — плотоядное животное). Используемый весьма редко, он вызвал много кривотолков как в сообществе создателей систем сетевой защиты, так и в СМИ. Carnivore — это кодовое название сетевого анализатора, применяемого ФБР (Федеральное бюро расследований). Он используется для мониторинга важных коммуникаций между избранными лицами как часть криминальных расследований. С целью сокрытия самого образа и во избежание некорректного толкования общественностью термина название было изменено на DCS100. При необходимости агенты федеральной службы входили в ISP подозреваемого субъекта с помощью «черного ящика» — обыкновенного выделенного сервера с системой Windows 2000 или NT с предварительно установленным программным продуктом ФБР — Carnivore. Сервер размещается в транке ISP (провайдер услуг Интернет) для считывания информации заголовков любого трафика, поступающего к подозреваемому или исходящего от него. После событий 11 сентября 2001 года такая практика стала обычной на многих ISP.

▶▶

Из соображений неприкосновенности приватной информации многие пользователи были озабочены применением Carnivore и способностью программы перехватывать весь трафик. В основном озабоченность касалась принципов работы анализатора Carnivore, того, насколько высока вероятность его неправомерного применения, а также общих рассуждений о сохранении конфиденциальности при наличии отводов в каналах связи.

Carnivore — это продукт для перехвата и прослушивания сообщений в Интернет, разработанный (ФБР). Первоначальной целью было обоснование особых потребностей применения закона. Например, одни постановления суда разрешают автоматическую регистрацию и мониторинг только входящих и исходящих адресов, а другие постановления суда санкционируют полный перехват электронной почты. Общий обзор функций Carnivore представлен в программе конфигурации на рис. А. 3.

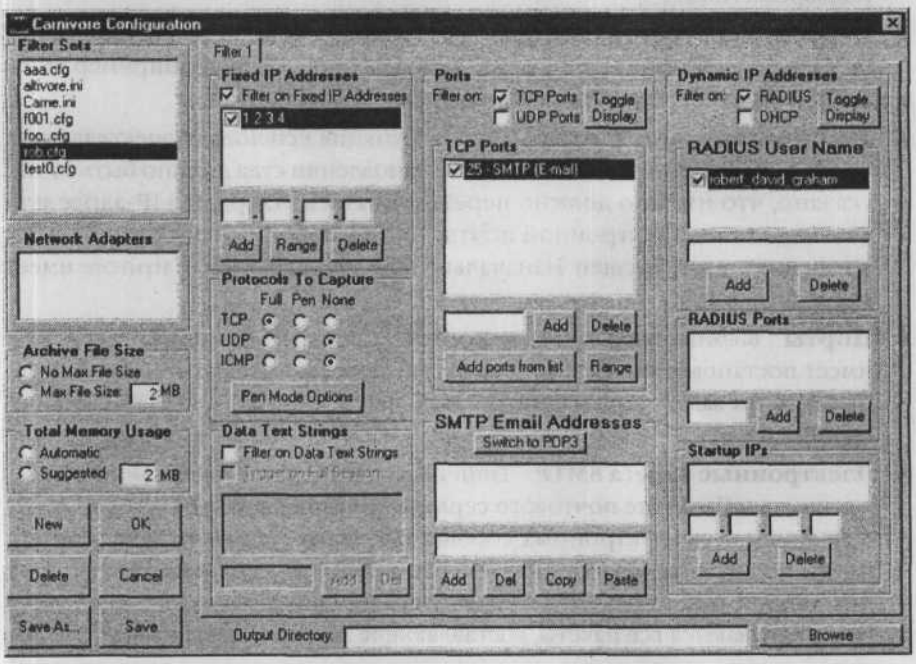

Рис. А. 3. Программа конфигурации Carnivore

Функции — следующие:

- **Наборы фильтров** Настройки сохраняются в файлах конфигурации; пользователь может оперативно изменить мониторинг выбором иного набора фильтров.

- **Сетевые адаптеры** Система может иметь несколько сетевых адаптеров; для анализа пакетов за один раз выбрать можно только один сетевой адаптер.
- **Размер файла архива** Можно установить предел объема перехватываемых данных; по умолчанию диск заполняется полностью.
- **Общее использование памяти** Сетевой трафик может поступать пакетами, быстрее, чем осуществляется запись на диск; память резервируется для буферизации поступающих данных.
- **Фиксированный IP-адрес** Фильтроваться может весь входящий и исходящий трафик целого диапазона IP-адресов. Например, подозреваемый может иметь фиксированный IP-адрес 1.2.3.4, присвоенный кабельному модему. ФБР может добиться постановления суда на анализ всего трафика подозреваемого.
- **Перехватываемые протоколы** Как правило, суд выносит постановление на разрешение мониторинга только особых протоколов, например SMTP по TCP. В режиме Pen перехватываются только заголовки.
- **Текстовые строки данных** Это — функция Echelon, осуществляющая поиск в трафике ключевых слов. В постановлении суда должно быть точно указано, что именно должно перехватываться, например IP-адрес или учетная запись электронной почты. В США подобный открытый поиск ключевых слов запрещен. Изначально ФБР отрицало, что Carnivore имеет такую функцию.
- **Порты** Можно задать список портов TCP и UDP. Например, если ФБР имеет постановление суда, разрешающее перехват электронной почты, то Бюро может задать порты электронной почты: 25 (SMTP), 110 (POP3) и 143 (IMAP).
- **Электронные адреса SMTP** Типичным сценарием является мониторинг с помощью Carnivore почтового сервера провайдера услуг Интернет с отсеиванием всех электронных сообщений, за исключением электронной почты подозреваемого. Сеанс электронной почты прослеживается до тех пор, пока не будет получен электронный адрес подозреваемого, после чего перехватываются все пакеты, составляющие электронную почту.
- **Динамические IP-адреса** Когда пользователи подключаются к Интернет по коммутируемому каналу, они регистрируются по протоколу RADIUS, который присваивает пользователю IP-адрес. Как правило, ФБР делает запрос ISP на переконфигурирование их серверов RADIUS с тем, чтобы всегда присваивать подозреваемому один и тот же IP-адрес, после чего осуществлять мониторинг всего входящего и исходящего трафика на этом IP-адресе.

Обратите внимание: если вы входите в Интернет по коммутируемому каналу и подозреваете, что за вами «охотится» ФБР, проверьте, не одинаковый ли IP-адрес всякий раз при наборе телефонного номера. Иногда это сделать невозможно. Carnivore можно сконфигурировать так, что программа будет осуществлять мониторинг протокола RADIUS и динамически распознавать новый IP-адрес, присвоенный подозреваемому. Мониторинг начинается с присвоением IP-адреса и прекращается, когда он не присвоен.

ФБР разработало Carnivore, потому что другие существующие утилиты не соответствовали потребностям применения закона. При отправке электронной почты по кабелю она разбивается на множество пакетов. Утилита, подобная mailsnarf, «соберет» почтовое сообщение в первоначальную форму. В этом нет ничего хорошего, потому что адвокаты подозреваемого подвергнут сомнению логическое соответствие: Не мог ли пакет «выпасть» где-нибудь «по пути», что изменило смысл электронного сообщения? Не мог ли пакет из другого сообщения случайно попасть в рассматриваемое сообщение? Путем перехвата необработанных пакетов вместо их повторной компоновки Carnivore поддерживает первоначальную последовательность чисел, портов и временных меток. Любые недостающие или лишние пакеты сразу видны, что позволяет ФБР защищать соответствие и точность системы.

Другая проблема, с которой сталкивается ФБР, — это минимизация анализируемых пакетов данных. Когда Бюро прослушивает линию, для этой задачи должен быть выделен сотрудник. Если подозреваемый — не единственный, кто пользуется телефоном (например, есть еще жена и дети), то сотрудник должен отключать записывающие устройства. Примерно по такому же принципу спроектирован продукт Carnivore, во избежание перехвата информации, не имеющей отношения к подозреваемому. Типичным примером будет использование Carnivore для мониторинга деятельности коммутируемого (dial-up) пользователя. В Carnivore имеется модуль для мониторинга трафика RADIUS, используемого большинством провайдеров сетевых услуг, для аутентификации пользователя и присвоения IP-адреса. Это позволяет Carnivore следить только за данным пользователем, без перехвата других трафиков (Отрывок из главы книги Роберта Грэма «Защита сети от несанкционированного проникновения» 2-е издание. Syngress Publishing 1-928994-70-9).

Ниже перечислены web-сайты с дополнительной информацией о Carnivore:

- www.fbi.gov;
- www.robergraham.com/pubs/carnivore-faq.html;
- www.stopcarnivore.org.

Принципы работы сетевого анализатора

В данном разделе представлен общий обзор процесса сетевого анализа пакетов вместе с базовой информацией о работе сетей и протоколов; впрочем, ресурсов по этим темам столько, что из них можно составить отдельную книгу! Самым популярным и, несомненно, лучшим ресурсом является «TCP/IP Illustrated, Vol. 1-3» Ричарда Стивенса (Richard Stevens).

Понятие Ethernet

Ethernet — самый популярный протокол, используемый для связи компьютеров между собой. Условно говоря, «протокол» — общение на определенном языке. Ethernet строился вокруг принципа среды коллективного пользования, где все компьютеры в сегменте локальной сети совместно используют один кабель. Он называется протоколом *широковещательной адресации*, потому что, когда на компьютере имеется информация для отправки, он передает данные на все компьютеры, находящиеся в том же сетевом сегменте. Эта информация делится на управляемые порции, называемые пакетами (Строго говоря, в Ethernet для них используется другой термин — кадры. — *Примеч. науч. ред.)*. Каждый пакет имеет заголовок, напоминающий конверт с указанным адресом отправителя (компьютера) и адресата. Несмотря на то, что информация передается на все компьютеры в сегменте, ответит на нее только компьютер с совпадающим адресом назначения. Все остальные компьютеры в сети будут «видеть» этот пакет, но, если он им не предназначен, то они его проигнорируют, если на каком-либо из них не запущен анализатор пакетов. При запущенном анализаторе упоминавшийся выше драйвер перехвата пакетов переведет сетевую интерфейсную плату (NIC) этого компьютера в беспорядочный режим (Состояние, в котором сетевой адаптер обнаруживает в сети все фреймы, вне зависимости от их конечного адреса. — *Примеч. науч. ред.)*. Это означает, что анализирующий пакеты компьютер будет способен просматривать весь трафик сегмента, независимо от того, кому он предназначался. Обычно компьютеры работают в упорядоченном режиме, прослушивая информацию, предназначенную только для них. Однако при работе NIC в беспорядочном режиме она может следить за переговорами всех соседей.

Адреса Ethernet называются адресами MAC (Media Access Control, контролер доступа к среде), аппаратными адресами, а иногда просто адресами Ethernet. Поскольку один сегмент Ethernet может коллективно использоваться множеством компьютеров, каждый из них должен иметь индивидуальный идентификатор. Эти идентификаторы жестко запрограммированы на сетевой карте. MAC-адрес — это 48-битовое число, также выражаемое 12-символьным шестнадцатеричным числом. Это число разбивается на две половины: первые 24 бита обозначают производителя платы Ethernet, а вторые 24 бита — серийный номер, присваиваемый производителем.

Перечисленные ниже шаги позволяют просмотреть MAC-адрес NIC:

- **Windows 9x** Войдите в **Start/Run** (Начать / Запустить) и введите **winipcfg.exe**. MAC-адрес будет обозначен как «Adapter Address» (адрес адаптера).
- **Windows NT/2000/XP** Войдите в командную строку и введите **ipconfig/all**. MAC-адрес будет обозначен как «Physical Address» (физический адрес).
- **Linux и Solaris** Введите в командной строке **ifconfig -a**. MAC-адрес будет обозначен как «HWaddr» в Linux и «ether» — в Solaris.

MAC-адреса компьютеров, с которыми недавно осуществлялась связь, также можно просмотреть с помощью команды **arp -a**. Более подробно данная тема рассматривается в разделе «Разгром коммутаторов».

MAC-адреса — уникальны, и, например, они никогда не могут быть одинаковыми на двух компьютерах. Впрочем, дело даже не в этом. Иногда имеют место технологические ошибки, когда несколько сетевых интерфейсных плат имеют один и тот же MAC-адрес, но, по большей части, пользователи намеренно меняют свои MAC-адреса. Это можно сделать с помощью программы (например, ifconfig), которая поможет «подделать» MAC-адрес. Подделка MAC-адреса еще называется спуфингом (*англ. — spoofing*). Также некоторые адаптеры позволяют применять программу для переконфигурирования MAC-адреса во время работы. И, наконец, имея в наличии нужный инструментарий и определенные профессиональные навыки адрес можно физически ввести повторно в сетевую интерфейсную плату.

ПРИМЕЧАНИЕ Спуфингом (spoofing) называется изменение реквизитов сетевого пакета, например исходного IP-адреса, MAC-адреса или даже адреса электронной почты. Это часто делается для «мимикрирования» под другое устройство с целью использования доверительных отношений либо для усложнения обнаружения источника атак. Спуфинг адресов также используется при атаках DoS (отказ в обслуживании), например в Smurf, где адрес возврата сетевых запросов ложно считается IP-адресом жертвы.

Понятие модели OSI

В начале 80-х годов Международная организация по стандартизации (International Standards Organization, ISO) разработала модель Взаимодействия открытых систем (Open System Interconnection, OSI) для описания совместной работы сетевых протоколов и компонентов. Данная модель делит сетевые функции на семь уровней, каждый из которых представляет группу взаимозависимых спецификаций, функций и операций.

Уровни модели OSI — следующие:

- **Уровень программного приложения (или Прикладной Уровень)** Самый верхний уровень модели OSI, отвечающий за управление связью между сетевыми приложениями. Сам по себе этот уровень не является приложением, хотя некоторые приложения могут иметь возможность и базовые протоколы для выполнения

функций уровня приложения. Например, web-браузер является программным приложением, однако именно базовый протокол HTTP (Hypertext Transfer Protocol, протокол передачи гипертекстовых файлов) обеспечивает функциональность уровня приложения. В число примеров протоколов уровня приложения входят Протокол передачи файлов (File Transfer Protocol, FTP), Простой протокол сетевого управления (Simple Network Management Protocol, SNMP), Простой протокол электронной почты (Simple Mail Transfer Protocol, SMTP) и Telnet.

- **Уровень представления** Данный уровень отвечает за представление данных, шифрование и сжатие.
- **Сеансовый уровень** Сеансовый уровень отвечает за создание и управление сеансами между оконечными системами. Протокол сеансового уровня во многих протоколах часто не используется. Примеры протоколов на сеансовом уровне: NetBIOS и Удаленный вызов процедуры (Remote Procedure Call, RPC).
- **Транспортный уровень** Данный уровень отвечает за связь между программами или процессами. Номера порта или сокета используются для идентификации этих уникальных процессов. Примеры протоколов транспортного уровня: TCP, UDP и Последовательный обмен пакетами (Sequenced Packet Exchange, SPX).
- **Сетевой уровень** Отвечает за адресацию и доставку пакетов от компьютера-отправителя компьютеру-адресату. Сетевой уровень принимает данные с транспортного уровня и заключает их в пакет или дейтаграмму. Логические сетевые адреса обычно присваиваются компьютерам на этом уровне. Примеры сетевых протоколов: IP и Межсетевой пакетный обмен (Internetwork Packet Exchange, IPX). На этом уровне работают такие устройства, как маршрутизаторы и коммутаторы Уровня 3.
- **Канальный уровень** Этот уровень отвечает за обмен фреймами между NIC в одном физическом сегменте. Связь на канальном уровне, как правило, основана на MAC-адресах. Канальный уровень заключает данные из сетевого уровня во фрейме. Примеры протоколов канального уровня: Ethernet, Token Ring и Протокол соединения типа «точка-точка» (Point-to-Point Protocol, PPP). На этом уровне работают мосты и коммутаторы.
- **Физический уровень** Этот уровень определяет соединители, проводку и спецификации того, как напряжение и биты проходят по кабельной или беспроводной среде. В число устройств на данном уровне входят повторители (репитеры), концентраторы, «хабы» (hub) и кабельные отводы. Устройства, работающие на физическом уровне, не распознают сетевых путей.

ПРИМЕЧАНИЕ При обсуждении сетевого трафика термины *фрейм* и *пакет* взаимозаменяемы. Однако различие кроется в различных уровнях модели OSI. Фрейм — это единица передачи на канальном уровне. Пакет — единица передачи на сетевом уровне, хотя многие используют термин «пакет» для обозначения данных на любом уровне.

По своей сути модель OSI имеет групповую природу, и ее можно использовать для описания практически любого сетевого протокола. С этой целью различные наборы протоколов часто отображаются на модели OSI. Доскональное понимание модели OSI очень помогает при сетевом анализе, сравнении и устранении неисправностей. Однако также важно помнить о том, что не все протоколы свободно отображаются в модели OSI. Например, TCP/IP разработан для отображения в модели DoD (U. S. Department of Defense, Министерство обороны США). В 70-х годах МО США разработало собственную модель DoD, состоящую из четырех уровней. Этой модели придерживаются основные протоколы Интернет.

Модель DoD — просто сокращенная версия модели OSI. Ее четыре уровня — следующие:

- **Уровень процесса** Данный уровень определяет протоколы, реализующие программные приложения на пользовательском уровне: доставка почты, удаленная регистрация и передача файлов.
- **Уровень «хост-хост»** Управляет связью, потоком данных и повторной передачей утерянных данных.
- **Уровень Интернет** Уровень отвечает за доставку данных от хоста-отправителя хосту-адресату через сеть разных физических сетей, посредством которых две машины соединяются между собой.
- **Уровень доступа к сети** Управляет доставкой данных по конкретной аппаратной среде.

Мысли вслух...

Протоколы TCP/IP

В данной книге делается много ссылок на TCP/IP и связанные с ним протоколы, особенно IP, TCP и UDP. TCP/IP (разработан Управлением перспективных исследовательских программ (Defense Advanced Research Projects Agency, DARPA)) — на сегодняшний день наиболее широко используемый протокол. IP — это протокол Уровня 3, содержащий информацию адресации и управления, обеспечивающую маршрутизацию пакетов. IP — это протокол без установления соединения, поэтому он обеспечивает ненадежную службу доставки пакетов данных по принципу «как получится». Именно поэтому во время передачи пакет может быть потерян. Все IP-пакеты состоят из заголовка и полезной нагрузки (данные верхних уровней).

На транспортном уровне TCP/IP стека обычно используются два протокола — TCP и UDP. В заголовки обоих протоколов входят номера исходного порта и порта назначения, используемые для определения программного приложения или процесса, из которых выходят или направляются сегмент

▶▶

TCP или дейтаграмма UDP. TCP — протокол с установкой соединения, а UDP — без установки соединения. В заголовок TCP входят номер последовательности и подтверждения для бесперебойной доставки данных. IP необходима надежная, гарантированная передача, обеспечение данной функциональности IP зависит от TCP.

Поскольку TCP ориентирован на установление соединения, он создает диалог между двумя взаимодействующими хостами с целью установления соединения. Это называется трехходовым квитированием (three-way handshake). Оно начинается, когда Хост А отправляет пакет *SYN* (синхронизация) на Хост В, предлагая выйти на связь. Хост В отвечает отправкой *SYN/ACK* (синхронизация/уведомление), подтверждая готовность к взаимодействию. После этого Хост А заканчивает соединение отправкой *ACK*.

Также TCP использует принцип «подвижного окна». Алгоритм с таким названием позволяет разместить буфер между программным приложением и потоком сетевых данных. Получаемые по сети данные помещаются в этот буфер до тех пор, пока приложение не будет готово к их считыванию. Окном называется объем данных, который можно поместить в буфер, до того, как должно быть отправлено уведомление. В число приложений, использующих TCP, входят FTP, Telnet, Сетевая файловая система (Network File System, NFS), SMTP, HTTP, Служба имен доменов (Domain Name System, DNS) и Сетевой протокол передачи новостей (Network News Transfer Protocol, NNTP). В число приложений, использующих UDP, входят DNS, Протокол маршрутной информации (Routing Information Protocol, RIP), NFS, SNMP и Протокол динамической конфигурации хоста/протокол BOOTP (Dynamic Host Configuration Protocol/Boot Protocol, DHCP/BOOTP). Как видно, некоторые приложения (например, DNS и NFS) могут использовать оба протокола.

Написание собственного сетевого анализатора

Есть прекрасная работа Чеда Ренфро (Chad Renfro) под названием «Построение сетевого анализатора пакетов от начала до конца», размещенная на сайте www.unixgeeks.org/security/newbie/security/sniffer/sniffer_construction.txt. В этом документе автор представил простейший 28-строчный анализатор пакетов, написанный на С и названный sniff.c. Очень прозрачным языком, понятным даже непрограммистам, Чед описывает программу построчно. Она демонстрирует применение устройства RAW_SOCKET для считывания пакетов TCP с сети и стандартного вывода основной информации заголовка (на экран). Для пущей простоты программа работает в упорядоченном режиме, так что для начала потребуется привести интерфейс в беспорядочный режим вводом команды **ifconfig eth0 promisc**.

Еще имеется заголовочный файл, который также придется скопировать в тот же каталог, в котором размещен sniff.c. При этом будут обеспечены стандартные структуры для доступа к полям IP и TCP. Эти структуры идентифицируют каждое поле в заголовке IP и TCP. Заголовок содержит больше информации, чем фактически используется sniff.c, но, по крайней мере, построение нужно начинать с этого места.

Для запуска программы скопируйте sniff.c и headers.h в один каталог и введите команду **gcc –o sniff sniff.c**. При этом программа скомпилируется, и будет создан исполняемый файл с именем sniff, который можно запустить вводом **./sniff**. Нижеприведенный текст показывает программу sniff на выходе при попытке создать подключение TELNET и FTP:

```
Bytes received (получено байт) : : :    48
Source address (исходный адрес) : : :    192.168.1.1
IP header length (длина заголовка IP) : : :    5
Protocol (протокол) : : :    6
Source port (исходный порт) : : :    1372
Dest port (порт назначения) : : :    23
Bytes received (получено байт) : : :    48
Source address (исходный адрес) : : :    192.168.1.1
IP header length (длина заголовка IP) : : :    5
Protocol (протокол) : : :    6
Source port (исходный порт) : : :    1374
Dest port (порт назначения) : : :    21
```

После перехвата данных программу можно завершить вводом **CTRL-C**. Также можно перевести интерфейс из беспорядочного режима путем ввода команды **ifconfig eth0 -promisc**.

CSMA/CD

Ethernet использует протокол Множественного доступа с контролем несущей/обнаружения столкновений (Carrier Sense Multiple Access/Collision Detection, CSMA/CD) для устройств в сети, предназначенных для обмена данными. Термин «множественный доступ» относится к тому факту, что многие сетевые устройства, подключенные к одному сегменту, имеют возможность передачи. Каждому устройству предоставлены равные возможности: ни одно не имеет приоритета над другим. *Контроль несущей* описывает то, как интерфейс Ethernet в сетевом устройстве прослушивает кабель

перед передачей. Сетевой интерфейс проверяет отсутствие каких бы то ни было посторонних сигналов в кабеле перед передачей. Во время передачи интерфейс Ethernet также осуществляет прослушивание на предмет того, что никакое другое сетевое устройство не передает данные в то же самое время. При одновременной передаче данных двумя сетевыми устройствами возникает *столкновение* (конфликт). Поскольку интерфейсы Ethernet прослушивают среду во время передачи, они могут идентифицировать наличие других сигналов посредством метода *обнаружения столкновений*. При возникновении столкновения передающее устройство войдет в режим ожидания на неопределенное время до того, как возобновить передачу. Данная функция называется *произвольной отсрочкой*.

Работа Ethernet традиционно была *полудуплексной*. Это значит, что интерфейс может либо передавать, либо принимать данные, но не может осуществлять то и другое одновременно. Если в сегменте более одного сетевого интерфейса пытаются осуществить передачу, то возникает столкновение по CSMA/CD. При использовании для соединения двух устройств переходного (crossover) кабеля или при подключении одного устройства к порту коммутатора, только двум интерфейсам в сегменте нужно передавать или принимать данные, и столкновение не происходит. Происходит это потому, что гнездо передачи (TX) устройства A подключено к гнезду приема (RX) устройства B, а TX устройства B подключено к RX устройства A. Таким образом, необходимость в методе обнаружения столкновений отпадает, поэтому интерфейсы можно ввести в *полнодуплексный* режим функционирования. Данный режим позволяет сетевым устройствам осуществлять передачу и прием данных одновременно, что значительно повышает производительность.

Аппаратные средства: отводы, концентраторы, коммутаторы

Кабельные отводы — это аппаратные устройства, помогающие подключению к сетевому кабелю. В данном случае по-английски термин «отвод» обозначается словом «tap» (Test Access Point), что в переводе означает «порт доступа к средствам тестирования» или «тест-порт», и это устройство можно использовать для доступа к любому кабелю, соединяющему компьютеры, концентраторы, коммутаторы, маршрутизаторы и прочие устройства. Существуют полу- и полнодуплексные отводы для каналов Ethernet на 10, 100 и 1000 Мбит/с. Они также доступны для разных размеров множественных портов. Ниже приведен список некоторых распространенных продуктов кабельных отводов:

- Net Optics имеет несколько типов сетевых отводов для медных и волоконно-оптических кабелей. Их можно увидеть на сайте www.netoptics.com.
- Семейство Century Tap доступно от Shomiti на сайте www.shomiti.net/shomiti/century-tap.html. Они предлагают большое разнообразие отводов как для медных, так и волоконно-оптических кабелей.

Концентратор — это устройство, позволяющее соединить друг с другом несколько хост-машин в совместно используемой среде, например в Ethernet. Когда компьютер отправляет информацию, она проходит через концентратор, который «вслепую» направляет ее на все подключенные к нему компьютеры. Как уже описывалось выше в разделе об Ethernet, компьютер, для которого предназначалась информация, распознает в заголовке пакета свой MAC-адрес и примет данные. Область рассылки концентратором всей поступающей информации называется *коллизионным (или широковещательным) доменом*. Концентратор имеет только один коллизионный домен для всего коллективно используемого трафика. На рис. А. 4 показана сетевая архитектура с коллизионными доменами, относящимися к концентраторам. Крупные коллизионные домены не только упрощают сетевой анализ пакетов, но также создают определенные аспекты производительности, а именно — уменьшение полосы пропускания или чрезмерный трафик на концентраторе.

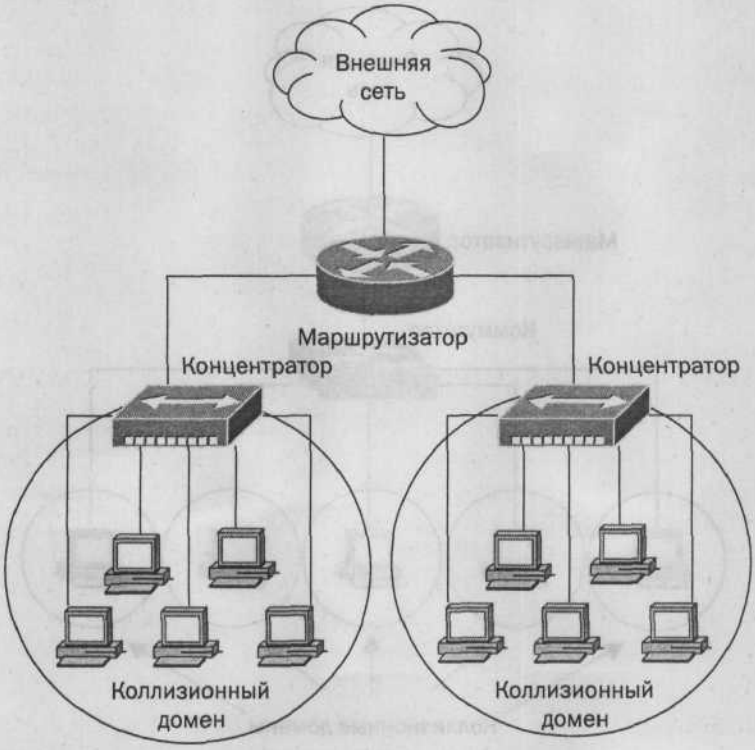

Рис. А. 4. Коллизионные домены концентратора

Коммутатор работает совсем иначе, нежели концентратор. Он также используется для соединения компьютеров в совместно используемой среде; однако, когда информация поступает от компьютера на коммутатор, последний направляет ее на

другие компьютеры не «вслепую». Коммутатор обратит внимание на заголовок пакета для определения местоположения MAC-адреса. Коммутатор поддерживает список всех MAC-адресов и соответствующих портов на коммутаторе, к которым подключены компьютеры. После этого он отправляет пакет на нужный порт. При этом коллизионный домен или широковещательный домен сужается до одного порта, как показано на рис. А. 5. Такой тип коллизионного домена также обеспечит определенную пропускную полосу для каждого подключения на концентраторе, вместо совместно используемого трафика. В связи с тем, что за последние несколько лет цена на коммутаторы резко упала, нет особого смысла не менять концентраторы на коммутаторы или предпочитать концентраторы при закупке нового оборудования. Также некоторые из сравнительно дорогостоящих коммутаторов часто включают в себя усовершенствованные технологии, делающие их более защищенными от атак анализаторов пакетов.

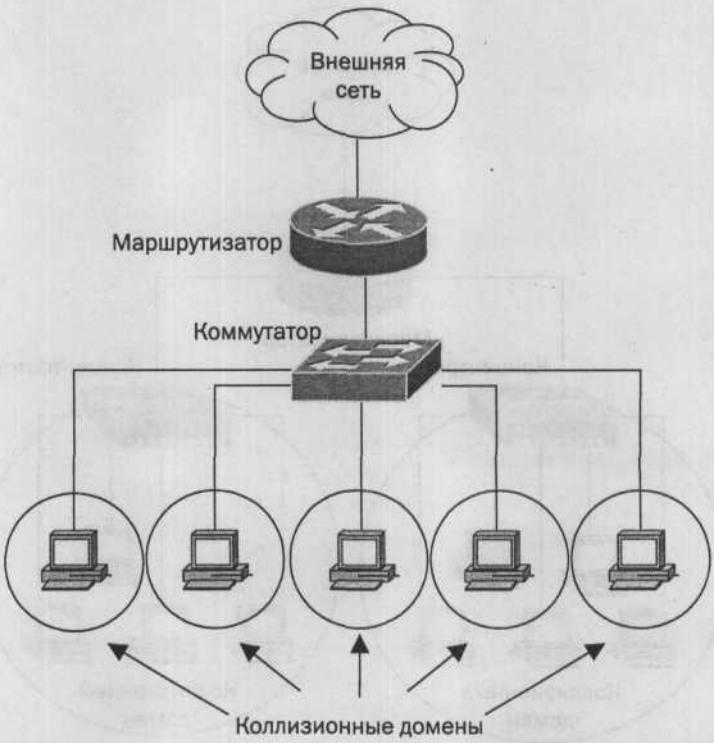

Рис. А. 5. Коллизионные домены коммутатора

Как видно в схемах, концентраторы упрощают анализ пакетов, а коммутаторы — усложняют. Впрочем, как видно из раздела «Разгром» коммутаторов», коммутаторы тоже можно обмануть.

Зеркальное отражение портов

Что делать, если работа ведется в сети с коммутаторами, но при этом необходимо провести легальный сетевой анализ? Ничего страшного, потому что большинство коммутаторов и маршрутизаторов поставляются с функцией *зеркального отражения портов* или *охвата портов*. Для зеркального отображения портов коммутатор необходимо сконфигурировать на дублирование трафика с порта мониторинга на порт, к которому подключен сетевой анализатор. Данная функция была разработана именно для этой цели — анализа сетевого трафика с целью обнаружения и устранения неполадок.

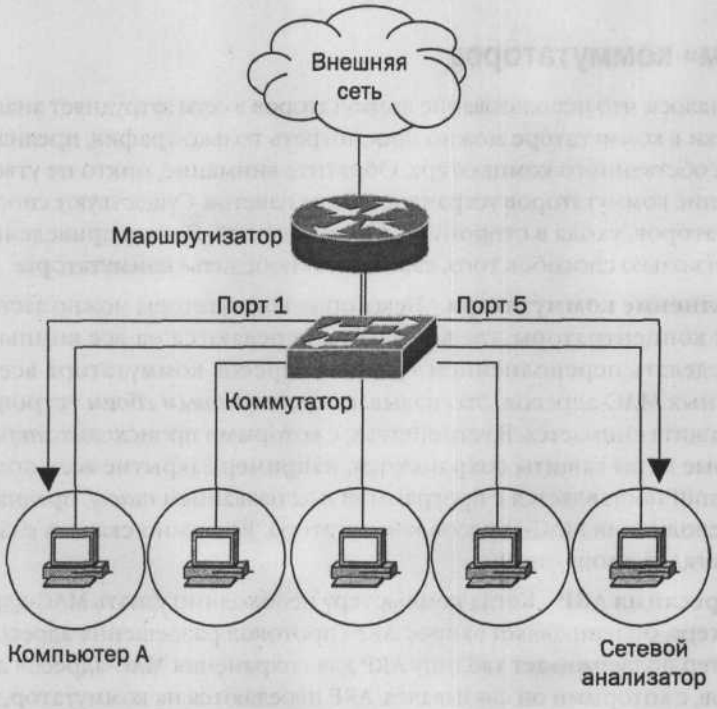

Рис. А. 6. Зеркальное отражение порта

Применение охвата портов не мешает нормальному функционированию коммутаторов, однако всегда необходимо сверяться с документацией конфигурируемого коммутатора и периодически проверять журнальные записи устройства. На коммутатор это не повлияет, однако объем трафика на определенном порту назначения будет увеличен, поэтому следует проверять корректность конфигурации сетевого анализатора на порту назначения. Для активизации зеркального отражения порта обратитесь к документации нужного коммутатора для выяснения точной команды. На рис. А. 6 представлен процесс зеркального отражения порта. Коммутатор сконфи-

гурирован для отражения всего трафика порта 1 на порт 5. Сетевой анализатор увидит весь трафик, входящий на Компьютер А и исходящий из него. Иногда администраторы отражают на коммутатор порт входящего (uplink) канала связи; таким образом, они могут следить за всем трафиком, входящим на коммутатор и исходящим из него, а также за всеми портами коммутатора.

ПРИМЕЧАНИЕ Английское слово «Span» (зд. — охват) составлено из Switched Port Analyzer (анализатор коммутированного порта). Cisco использует слово «span» для описания понятия зеркального отражения портов. На языке Cisco охват порта — то же самое, что и его зеркальное отображение.

«Разгром» коммутаторов

Ранее отмечалось, что использование коммутаторов в сети затрудняет анализ пакетов. Теоретически в коммутаторе можно просмотреть только трафик, предназначенный для своего собственного компьютера. Обратите внимание, никто не утверждал, что использование коммутаторов устраняет анализ пакетов. Существуют способы «обмана» коммутаторов, ухода в сторону от их технологий. В нижеприведенном списке описаны несколько способов того, как можно «победить» коммутаторы:

- **Переполнение коммутатора** Некоторые коммутаторы можно заставить работать как концентраторы, где все пакеты передаются на все компьютеры. Это можно сделать переполнением таблицы адресов коммутатора всеми видами поддельных MAC-адресов. Это называется *открытым сбоем* устройства, когда всякая защита снимается. В устройствах, с которыми происходит *закрытый сбой*, некоторые меры защиты сохраняются, например закрытие всех подключений. Пакет Dsniff поставляется с программой под названием *macof*, предназначенной для переполнения MAC-адресов коммутатора. Ее можно скачать с сайта http://monkey.org/~dugsong/dsniff.
- **Переадресация ARP** Когда компьютеру необходимо узнать MAC-адрес другого компьютера, он направляет запрос ARP (протокол разрешения адресов). Каждый компьютер поддерживает таблицу ARP для сохранения MAC-адресов других компьютеров, с которыми он связывался. ARP передаются на коммутатор, так, что все компьютеры, подключенные к этому коммутатору, увидят запрос и ответ. С применением ARP существует несколько способов «заставить» коммутатор отправлять трафик туда, куда не следует. Во-первых, злоумышленник может «ввести коммутатор в заблуждение», направив ARP с чужим MAC-адресом. Злоумышленник также может отправить ARP с заявлением о том, что он является маршрутизатором, и тогда компьютеры будут пересылать свои пакеты данных через машину взломщика сети. Либо запрос ARP может поступить одной «жертве» с указанием на то, что это и есть маршрутизатор, и в этом случае «пострадавший» начнет переадресовывать пакеты своих данных злодею. Все эти уловки позволяют взломщику просматривать не предназначенную ему информацию.

- **Переадресация ICMP** Иногда компьютеры находятся в одном физическом сегменте, подключены к одному и тому же коммутатору, но в разных логических сегментах. Это означает, что они находятся в разных подсетях IP. Когда Компьютер А хочет выйти на связь с Компьютером В, он направляет запрос через маршрутизатор. Последний «знает», что обе машины находятся в одном и том же физическом сегменте, поэтому отправляет переадресацию ICMP (протокол управляющих сообщений в Интернет) на Компьютер А, сообщая, что он может отправлять свои пакеты данных напрямую на Компьютер В. Злоумышленник — Компьютер X — может отправить ложную переадресацию ICMP на Компьютер А, сообщая, что ему следует отправлять пакеты данных Компьютера В на Компьютер X.
- **Объявления маршрутизатора ICMP** Эти объявления информируют компьютеры о том, кто является маршрутизатором. Злоумышленник может рассылать такие объявления с заявлениями о том, что именно он является маршрутизатором, и все компьютеры будут отправлять свои пакеты данных через машину злоумышленника.
- **Спуфинг MAC-адреса** Незваный гость может притвориться, что он использует другой компьютер, путем спуфинга MAC-адреса. Отправка пакетов с исходным адресом жертвы может ввести коммутатор в заблуждение. Коммутатор введет «спуфированную» информацию в свою таблицу и начнет рассылку пакетов злоумышленнику. А как быть с жертвой, которая по-прежнему остается на коммутаторе и продолжает рассылать обновления, заставляя коммутатор возвращать таблицу в первоначальное состояние? Эта задача решается выводом компьютера-жертвы из строя с помощью какого-либо вида DoS-атаки с последующей переадресацией коммутатора и продолжением сеанса связи. Злоумышленник также может разослать получаемый им трафик, чтобы убедиться, что компьютер-жертва по-прежнему получает пакеты данных. Некоторые коммутаторы обладают «противоядием», позволяющим статически присваивать порту MAC-адреса. Если сеть обширная, то управлять этой функцией достаточно сложно, но при этом спуфинг MAC-адреса будет устранен.

  Для спуфинга MAC на Linux или Solaris при локальном подключении ifconfig можно использовать следующим образом:

  ```
  ifconfig eth0 down
  ifconfig eth0 hw ether 00:02:b3:00:00:AA
  ifconfig eth0 up
  ```

  Зарегистрируйте MAC на всех хостах путем рассылки ping (и воспользуйтесь комбинацией клавиш CTRL-C для закрытия ping): **ping –c 1 –и 192.168.1.255**.

  Теперь можно осуществить анализ пакетов всего трафика к компьютеру, имеющему данный MAC-адрес.
- **Переконфигурирование зеркального отражения портов на коммутаторе** Как упоминалось выше, порты коммутатора можно сконфигурировать для про-

смотра трафика, предназначенного для других портов. Злоумышленник может сделать это путем подключения к коммутатору через Telnet или какую-либо другую «лазейку» по умолчанию. Можно воспользоваться протоколом SNMP, если он не защищен.

- **Отводы кабеля** Как упоминалось выше, отводы кабелей можно использовать для физической «врезки» в кабель. Врезкой во входящий кабель (uplink) на коммутаторе можно просматривать весь трафик, входящий на данный коммутатор и исходящий из него.

Существует много способов «обмана» коммутаторов, но это зависит от того, как коммутатор функционирует. Не все из рассмотренных способов сработают, особенно при наличии новейших, технологически изощренных коммутаторов. Dsniff FAQ содержит полезную информацию об анализе пакетов в коммутируемой среде. Эта информация может быть размещена на сайте http://monkey.org/~dugsong/dsniff/faq.html.

Обнаружение сетевых анализаторов пакетов

Вспомните о том, что сетевые анализаторы пакетов представляют собой разновидность пассивной атаки. Они не взаимодействуют ни с какими устройствами и не передают никакой информации, поэтому их трудно обнаружить. Впрочем, обнаружить несанкционированные анализаторы пакетов можно, хотя и непросто. Самый простой способ — проверка сетевых интерфейсов на предмет их функционирования в беспорядочном режиме. В системах на базе UNIX команда **ifconfig –a** выведет список сетевых адаптеров системы. Найдите флажок PROMISC на выходе, как в следующем примере:

```
[root@localhost root]# ifconfig -a
eth0  Link encap:Ethernet HWaddr 00:02:B3:06:5F:5A
      inet addr:192.168.1.2 Bcast:192.168.1.255 Mask:255.255.255.0
      UP BROADCAST RUNNING PROMISC MULTICAST MTU:1500 Metric:1
      RX packets:204 errors:0 dropped:0 overruns:0 frame:0
      TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 exqueuelen:100
      RX bytes:46113 (45.0 Kb) TX bytes:5836 (5.6 Kb)
      Interrupt:11 Base address:0x1800 Memory:e8120000-e8120038
```

Если ifconfig не обнаруживает анализатор пакетов, о котором известно, что он установлен и работает в беспорядочном режиме, тогда можно попробовать воспользоваться командой **ip link** — удобной утилитой конфигурирования и маршрутизации TCP/IP. Приведенный ниже пример показывает выход после использования команды ip:

```
[root@localhost root]# ip link
1:    lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
      link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
```

```
2:    eth0: <BROADCAST,MULTICAST,PROMISC,UP> mtu 1500 qdisk pfifo_fast qlen 100
      link/ether 00:02:b3:06:5f:5a brd ff:ff:ff:ff:ff:ff
```

Обнаружить беспорядочный режим в системах Windows — сложнее, потому что не существует стандартных команд, которые перечисляют этот тип информации. Впрочем, имеется бесплатное инструментальное средство под названием PromiscDetect, разработанное Арне Видстрёмом (Arne Vidstrom), которое помогает обнаружить сетевые адаптеры беспорядочного режима для Windows NT, 2000 и XP. Этот продукт можно скачать с сайта http://ntsecurity.nu/toolbox/promiscdetect. Нижеприведенный пример показывает выход PromiscDetect; адаптер D-link — в нормальном рабочем режиме, а на адаптере Intel запущен Ethereal:

```
C:\>promiscdetect
PromiscDetect 1.0 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
                  - http://ntsecurity.nu/toolbox/promiscdetect/

Adapter Name (Название адаптера):
- D-Link DWL-650 11 Mbps WLAN Card
Active filter for the adapter (Активный фильтр адаптера):
- Directed (перехват пакетов, направленных на данный компьютер)
- Multicast (перехват многоадресных пакетов для групп, членом которых является
компьютер)
- Broadcast (перехват широковещательных пакетов)
Adapter Name (Название адаптера):
- Intel ® PRO/100 SP Mobile Combo Adapter
Active filter for the adapter (Активный фильтр адаптера):
- Directed (перехват пакетов, направленных на данный компьютер)
- Multicast (перехват многоадресных пакетов для групп, членом которых является
компьютер)
- Broadcast (перехват широковещательных пакетов)
- Promiscuous (перехват всех пакетов в сети)
ПРЕДУПРЕЖДЕНИЕ: Поскольку адаптер работает в беспорядочном режиме, на компьютере
может быть установлен несанкционированный анализатор пакетов!
```

К сожалению, некоторые анализаторы могут «заметать следы» путем сокрытия флажков беспорядочного режима. Также, если анализатор был установлен на дискредитированной системе с помощью руткита, тогда, скорее всего, злоумышленник заменил команды, подобные ifconfig. В списке ниже представлено несколько других способов, которые можно использовать для обнаружения анализаторов в сетях.

- Мониторинг обратного поиска DNS. Некоторые анализаторы пакетов будут выполнять запросы DNS для разрешения IP-адресов в имена хост-машин. Эту операцию можно активизировать выполнением сетевого PING-сканирования или тестовым опросом (pinging) адресного пространства всей сети.
- Отправка пакетов TCP/IP на все адреса одного сегмента Ethernet, но с ложными MAC-адресами. Обычно сетевой адаптер сбрасывает пакеты с некорректными

MAC-адресами. Однако некоторые системы, работающие в беспорядочном режиме, отвечают пакетом сброса (reset packet, RST). То же самое может сработать в коммутируемой среде, поскольку коммутаторы отправляют широковещательные пакеты, для которых они не имеют зарегистрированных MAC-адресов. Многие новейшие коммутаторы имеют встроенную защиту от этой методики, работающую изменением способа обработки MAC-адресов.

- Внимательный мониторинг портов концентраторов. В идеале, в наличии должна быть сетевая диаграмма и кабели должны быть маркированы. В этом случае, при появлении чего-либо необычного, например нового устройства или вновь активизированного порта концентратора, их можно будет легко идентифицировать. Впрочем, в реальной жизни специальные шкафы с проводкой и короба с кабелями могут превратиться в настоящий кошмар. Если мониторинг концентраторов осуществляется через систему управления сетью по протоколу SNMP, то эту информацию можно использовать для обнаружения нетипичных подключений и отключений.
- Следует вспомнить, как используется ARP для связи IP-адресов с MAC-адресами. Обычно ARP широковещательно отправляется всем участникам сети. Однако ARP можно отправить и не на широковещательный адрес, за которым следует широковещательный отправитель пакетов (ping). Никто не должен получать информацию таблицы ARP, кроме анализатора пакетов, потому что он прослушивает весь трафик, даже не широковещательный. Поэтому ответит компьютер с установленным сетевым анализатором пакетов.
- Использование так называемой «приманки» (honeypot). Так называется сервер, настроенный на мониторинг действий специалистов по несанкционированному проникновению в сеть. На нем хранятся ложные данные и службы. В этом случае на этом сервере можно создать ложные учетные записи администратора или пользователя, после чего создать в сети подключения к нему с помощью открытых протоколов типа Telnet или FTP. Если некто охотится за именами пользователей и паролями, то он наткнется на «приманку» и так или иначе попытается войти в нее. На таких серверах установлены программные средства обнаружения и мониторинга проникновений в сеть; при использовании ложных учетных записей в триггерные системы тревожного оповещения можно добавить специальные подписи.
- Следует внимательно наблюдать за хост-машинами. Это относится к дисковому пространству, использованию CPU и времени отклика. Анализаторы пакетов постепенно поглощают пространство на диске, по мере ежедневного накопления трафика, и иногда накладывают заметную нагрузку на центральный процессор. При чрезмерном поглощении ресурсов инфицированного компьютера его время отклика значительно снижается.

Существует несколько специальных инструментов для обнаружения анализаторов в сети. Многие из них уже устарели и обслуживаются не так активно, как раньше (иногда их даже трудно найти). При этом хакеры постоянно переписывают свои сетевые анализаторы, во избежание обнаружения. Приведем некоторые инструментальные средства обнаружения несанкционированных сетевых анализаторов.

- **PromiScan Ver 0.27** Бесплатная, вполне современная и активно поддерживаемая программа, разработанная Security Friday. Работает на Windows 2000, XP и требует наличие драйвера WinPcap. С помощью пакетов ARP может сканировать локальные сети на предмет удаленных адаптеров беспорядочного режима. Имеется на сайте www.securityfriday.com/ToolDownload/PromiScan/promiscan_doc.html.
- **AntiSniff** Данная программа изначально написана L0pht; в настоящее время не поддерживается и не обновляется. Архивные версии для Windows и UNIX имеются на сайте http://packetstormsecurity.nl/sniffers/antisniff.
- **Sentinel** Данная бесплатная программа осуществляет обнаружение удаленных беспорядочных режимов и работает на разных версиях BSD и Linux. Для работы требует библиотеки libpcap и libnet. Имеется на сайте www.packetfactory.net/projects/sentinel.
- **Neped** Network Promiscuous Ethernet Detector — бесплатная программа на базе UNIX, изначально разработанная Apostols Group для удаленного обнаружения сетевых адаптеров беспорядочного режима на компьютерах с системами Linux. Обнаружение осуществляется только на подмножестве систем Linux с ядрами «без заплат» до версии 2.0.36. Web-сайта компании Apostols уже не существует, и поэтому найти программу Neped достаточно сложно. В настоящее время имеется версия на www.dsnet.org/tools/network-sniffers/neped.c.
- **Check Promiscuous Mode (CPM)** Бесплатная программа для UNIX, изначально разработанная CERT/CC в ответ на участившиеся случаи незаконного сканирования сетей. Дополнительная информация, включая саму программу, имеется на сайте www.cert.org/advisories/CA-1994-01.html.
- **Ifstatus** Бесплатная программа для UNIX, предназначенная для обнаружения интерфейсов, работающих в беспорядочном режиме на системах Solaris и AIX. Имеется на ftp://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/ifstatus.
- **Promisc.c** Бесплатная программа для UNIX, предназначенная для обнаружения интерфейсов, работающих в беспорядочном режиме на системах Linux и некоторых системах SunOS. Имеется на сайте www.dsinet.org/tools/network-sniffers/promisc.c.

Защита от сетевых анализаторов пакетов

До сих пор речь шла о том, что собой представляет сетевой анализ пакетов и о принципах его работы. Читатели также познакомились с некоторыми методами и ухищрениями «специалистов» по незаконному проникновению в сети, а также с некоторыми не очень «дуракоустойчивыми» способами обнаружения несанкционированных анализаторов. Впрочем, ничто из описанного не дает конкретных положительных рекомендаций по решению довольно трудной задачи защиты сети и данных. К счастью, существуют способы, которые можно использовать при работе в сетях, предлагающие защиту от пассивного нападения, называемого незаконным сканированием (анализом) пакетов данных.

Выше обсуждалось использование в сетях коммутаторов вместо концентраторов. Однако также рассматривались способы «обмана» коммутаторов. Использование коммутаторов до сих пор считается лучшей практикой в сетевых разработках, помогающей повысить производительность и защиту, и которую следует применять, независимо от существующих способов ее обхода. Несмотря на то, что коммутаторы представляют собой барьер для случайного прослушивания сети, лучшим способом ее защиты является шифрование. Последнее — лучшая форма защиты от перехвата трафика как в сетях общего доступа, так и в корпоративных. Злоумышленники все равно будут просматривать трафик, однако данные в нем будут нечитаемыми; расшифровать и прочитать их сможет только предполагаемый получатель. При некоторых способах шифрования заголовок все равно передается открытым текстом, поэтому хакер увидит адрес отправителя и адрес назначения и, возможно, сумеет построить карту сети, однако данные останутся зашифрованными. При других способах шифрования закодированными передаются даже заголовки.

В виртуальной частной сети (virtual private network, VPN) шифрование и аутентификация используются для обеспечения защиты коммуникаций с другими незащищенными сетями. VPN защищают передачу данных по Интернет и даже по внутренней сети. Однако, если злоумышленник дискредитирует какой-либо конечный узел VPN, то защита окажется бесполезной. В нижеприведенном списке представлено несколько используемых в настоящее время методов VPN для защиты данных от прослушивания:

- **Secure Shell (SSH)** SSH — это VPN на уровне приложения, работающая по TCP для обеспечения защиты транзакций «клиент-сервер». Часто используется для общей регистрации, а также для удаленного администрирования серверов. Обычно применяется для замены Telnet, FTP и команд «r» Berkley Services. Однако по причине того, что любой произвольный протокол TCP можно провести через подключение SSH, последнюю можно использовать для множества других целей. SSH обеспечивает аутентификацию по парам несимметричных ключей RSA или DSA. Заголовки в сеансе SSH не шифруются, поэтому злоумышленник сможет просматривать исходный адрес и адрес назначения.

- **Secure Sockets Layer (SSL) / Transport Layer Security (TLS)** Изначально SSL (протокол защищенных сокетов) разработан Netscape Communications для обеспечения защиты и конфиденциальности сеансов Интернет. Как отмечается в RFC 2246, этот протокол был заменен на TLS (протокол защиты транспортного уровня). TLS обеспечивает защиту на транспортном уровне и по некоторым показателям превосходит аспекты защиты SSL. TLS используется для инкапсулирования сетевого трафика приложений более высокого уровня, таких как LDAP, HTTP, FTP, NNTP, POP3 и IMAP. Обеспечивает аутентификацию и целостность посредством цифровых сертификатов и цифровых подписей.
- **IP Security (IPSec)** IPSec — это протокол на сетевом уровне, объединяющий защиту в протоколы IPv4 и IPv6 непосредственно на уровне пакета путем расширения заголовка IP-пакета. Это позволяет зашифровывать любой протокол более высокого уровня. В настоящее время включается в устройства маршрутизации, брандмауэры и клиенты для защиты доверяемых сетей. IPSEC предоставляет возможности аутентификации и шифрования с поддержкой довольно большого количества аутентификационных шифров открытых ключей и шифров с использованием симметричных ключей. Может работать в туннельном режиме для создания нового IP-заголовка, который будет скрывать исходный адрес и адрес назначения.

Применение одноразовых паролей (One-time Pasword, OTP) — еще один способ защиты от несанкционированного анализа пакетов данных. S/key, OPIE (One-time Pasword In Everything, одноразовые пароли для всех данных) и другие методики использования одноразовых паролей защищают от сбора паролей и повторного их использования. Работают по принципу «отклик-отзыв», всякий раз при необходимости аутентификации передается новый пароль. Пароли, собранные хакерами, будут бесполезными, поскольку они используются только один раз. Смарт-карты — также популярная методика реализации одноразовых паролей.

Защита электронной почты — весьма актуальная проблема как для отдельных пользователей, так и для компаний. Двумя способами защиты почтовых сообщений путем их шифрования во время передачи и хранения являются Pretty Good Privacy (PGP) и Secure Multipurpose Internet Mail Extensions (S/MIME). Каждый из них обеспечивает аутентификацию и целостность с помощью цифровых сертификатов и цифровых подписей.

Сетевой анализ и корпоративная политика

Есть еще один важный аспект, на который авторы хотели бы обратить внимание читателей. Перед тем, как запускать в работу вновь установленный сетевой анализатор, пожалуйста, ознакомьтесь сначала с политикой своей компании! В продуманной и грамотно составленной политике работы с сетями («Правила безопасной работы») наверняка будет присутствовать пункт, запрещающий использование сетевых анали-

заторов. Как правило, исключением является случай, когда сетевой анализ входит в описание обязанностей сотрудника. При этом, даже предоставление консультаций клиентам по вопросам сетевой защиты не означает, что сотрудник может использовать анализатор пакетов в корпоративной сети. Впрочем, если это сисадмин, которому разрешено использовать сетевой анализатор, то это можно делать для соблюдения политики сетевой защиты компании. Если последняя запрещает использование программ коллективной работы с файлами (KaZaA, Morpheus) или таких служб, как Интернет-чат (Internet Relay Chat, IRC) или сетей мгновенного обмена сообщениями (например, ICQ), то анализатор можно использовать для выявления подобного рода нарушений.

Также, при предоставлении клиентам услуг сетевой защиты, например так называемого обслуживания «доброжелательным хакером» с осуществлением проникновения в сеть, убедитесь в том, что применение сетевого анализатора оговорено в Правилах. Следует соблюдать предельную корректность в отношении того, как, где и когда будет применяться анализатор. В своде корпоративной политики должны иметь место такие пункты, как «Договор о неразглашении», запрещающие просмотр конфиденциальной информации.

И еще два слова предупреждения: в «Правилах безопасной работы» многих провайдеров Интернет-услуг применение сетевых анализаторов запрещено. Если обнаружится, что при подключении к их сети использовался сетевой анализатор, то они могут отказать компании в предоставлении услуг. Эксперименты с анализаторами безопаснее всего проводить в домашней сети, не подключенной к Интернет. Все, что понадобится, — это пара компьютеров, соединенных кабелем crossover. Один можно использовать в качестве клиента, а на другой установить серверные службы — Telnet, FTP, Web и электронную почту. Установите сетевой анализатор на одну или обе машины и — вперед!

ПРИМЕЧАНИЕ С многочисленных web-сайтов можно скачать базы пакетов и считывать их с помощью своего сетевого анализатора для того, чтобы привыкнуть к анализу и интерпретации программных пакетов. На HoneyNet Project (*http://project.honeynet.org*) данные для анализа обновляются ежемесячно.

Резюме

Сетевой анализ является ключевой стратегией обслуживания оптимизированной сети и выявления различных аспектов защиты и безопасности. Упреждающее администрирование помогает обнаружить те или иные аспекты до того, как они превратятся в серьезные проблемы, спровоцируют сбой в сети или дискредитируют конфиденциальную информацию. Помимо выявления возможных атак и подозрительной деятельности данные, полученные с помощью сетевого анализатора, можно исполь-

зовать для обнаружения слабых мест сетевой защиты с последующим приведением в действие соответствующей корпоративной политики. Регистрацию анализаторов можно соотносить с IDS, брандмауэром и регистрационным журналом маршрутизатора для сбора доказательств на случай судебных разбирательств и при рассмотрении различных инцидентов. Сетевой анализатор позволяет перехватывать данные сети по пакетам, расшифровывать информацию и просматривать ее в удобочитаемом формате. Найти сетевые анализаторы достаточно просто, часто они распространяются бесплатно; они просты в использовании и являются одним из основных инструментов любого сисадмина.

В данном приложении изложены основы организации сетей, Ethernet, модель OSI, а также описаны аппаратные средства, используемые в сетевой архитектуре. На самом деле, все описанное — это лишь надводная часть огромного айсберга. Подробные материалы по организации и обслуживанию сетей и протоколов должны стоять на книжной полке каждого администратора. Они очень пригодятся, когда в сети вдруг обнаружится неизвестный или нетипичный трафик.

Сисадминам важно уметь отслеживать использование сетевых анализаторов желающими незаконно проникнуть в сеть. Нужно постоянно быть в курсе всех новейших хакерских ухищрений, направленных на обход мер защиты. При этом в обычном порядке необходимо следить за тем, чтобы компьютерные системы компании всегда обновлялись соответствующими модулями защиты от руткитов и других небезопасных «лазеек».

Авторы описали разнообразные способы защиты данных от прослушивания. Необходимо постоянно следить за появлением новейших технологий сетевой защиты, алгоритмов шифрования и процессов аутентификации. «Взломщики» сетей непрестанно находят новые способы обхода существующих средств защиты, поэтому и разрабатываются все более изощренные технологии. Хорошим примером в этом смысле может служить взлом схемы шифрования DES с ее последующей заменой на Тройной стандарт шифрования данных (Triple Data Encryption Standard, 3DES).

И, наконец, не стоит забывать о правиле сетевого анализа: проводите его только при наличии разрешения. Энергичного, любознательного и напористого сисадмина могут запросто принять за взломщика сетей. Получите официальное разрешение на сетевой анализ либо экспериментируйте на домашней сети.

Краткое резюме по разделам

Понятие сетевого анализа и анализа пакетов

- ☑ Сетевым анализом называется перехват и декодирование передаваемой по сети информации.
- ☑ Сетевыми анализаторами могут быть как аппаратные, так и программные средства, доступные бесплатно или за плату.
- ☑ Обычно интерфейсы сетевых анализаторов имеют три панели (подокна): «Резюме», «Описание» и «Данные».
- ☑ Сетевой анализатор состоит из пяти компонентов: аппаратные средства, драйвер перехвата, буфер, анализ в режиме реального времени и декодер.

Кому нужен сетевой анализ?

- ☑ Сисадмины используют сетевой анализ для устранения неисправностей и проблем в сетях, анализа производительности сети и для обнаружения несанкционированного проникновения.
- ☑ Когда злоумышленники используют сетевые анализаторы, это рассматривается как пассивная атака.
- ☑ Злоумышленники используют анализаторы в основном для перехвата имен пользователей и паролей, для сбора конфиденциальных данных и для построения карты сети.
- ☑ Сетевые анализаторы — это типичный компонент руткитов.
- ☑ Взломщики сетей используют анализаторы для управления программами незаконного проникновения в сеть («лазейками»).

Принципы работы сетевого анализатора

- ☑ Ethernet — среда коллективного пользования, в которой используются MAC-адреса или аппаратные адреса.
- ☑ Модель OSI имеет семь уровней и является стандартом сетевого взаимодействия.
- ☑ Концентраторы рассылают информацию на все хосты сегмента с созданием коллективно используемого коллизионного домена.
- ☑ Коммутаторы имеют по одному коллизионному домену на каждый порт и поддерживают адресную таблицу MAC-адресов, относящихся к каждому порту.
- ☑ Зеркальное отражение портов — функция, позволяющая осуществлять сетевой анализ на коммутаторах.

- ☑ Коммутаторы затрудняют сетевой анализ, однако меры защиты в архитектурах коммутаторов можно «обойти» с помощью определенных способов, позволяющих перехватывать трафик, предназначенный для других компьютеров.

Обнаружение сетевых анализаторов пакетов

- ☑ Иногда анализаторы можно обнаружить в локальных системах по беспорядочному режиму работы.
- ☑ Существует несколько инструментальных средств, с помощью которых несколькими способами можно обнаружить беспорядочный режим.
- ☑ Следует проводить тщательный мониторинг хостов, концентраторов и портов коммутаторов; обратный поиск DNS помогает в обнаружении сетевых анализаторов.
- ☑ «Приманки» — хороший способ выявления в сети «непрошеных гостей», пытающихся воспользоваться скомпрометированными паролями.
- ☑ Новейшие анализаторы спроектированы достаточно хорошо, чтобы «уходить» от традиционных методик обнаружения.

Защита от сетевых анализаторов пакетов

- ☑ Коммутаторы предлагают далеко не полную защиту от сетевых анализаторов.
- ☑ Шифрование — лучший способ защиты информации от перехвата сетевыми анализаторами.
- ☑ SSH, SSL/TLS и IPSEC — формы VPN, функционирующие на разных уровнях модели OSI.
- ☑ Туннельный режим IPSec может защитить исходный адрес и адрес назначения в заголовке IP путем добавления нового заголовка.

Сетевой анализ и корпоративная политика

- ☑ Убедитесь в наличии разрешения на работу с сетевым анализатором в чужой сети.
- ☑ Перед использованием сетевого анализатора ознакомьтесь с соответствующими правилами провайдера Интернет-услуг.
- ☑ Если нанятый для оценки сети администратор планирует использовать сетевой анализатор, ему следует убедиться в наличии договоров о неразглашении, потому что он может иметь доступ к конфиденциальным данным.
- ☑ Одноразовые пароли делают дискредитированные пароли недействительными.
- ☑ Защиту электронной почты необходимо осуществлять во время передачи и хранения с помощью метода шифрования данных.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма «**Ask the Author**»). Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: Я запустил программу переполнения коммутатора, но ничего не произошло. Почему?

О: Некоторые новые разновидности коммутаторов неуязвимы для устаревших инструментов переполнения.

В: Мои концентраторы соединены между собой шлейфом через полы здания офиса компании. Образуют ли все они один коллизионный домен?

О: Да! Концентраторы не имеют никаких логических устройств для определения того, куда отправлять данные, поэтому они отправляют их на все подключенные машины «вслепую». Поэтому каждый из подключенных цепью концентраторов просматривает трафик всех портов.

В: Когда я запускаю Ethereal на своей системе Linux я не вижу на выходе ifconfig – а флажка PROMISC.

О: Для перехвата и фильтрации пакета Ethereal использует программу libpcap. Некоторые более современные версии if libpcap применяют другой способ перевода интерфейса в беспорядочный режим, который ifconfig не может обнаружить.

В: Понизит ли производительность сети добавление шифрования?

О: Да, шифрование и декодирование данных могут требовать дополнительных ресурсов системы, в зависимости от нескольких факторов, включая алгоритм шифрования и длину ключа. Впрочем, в зависимости от архитектуры сети, конечные пользователи могут не заметить изменения производительности.

В: Что будет, если хакер дискредитирует хост-машину, на которой я запускаю клиент VPN?

О: Изначально VPN предложит злоумышленнику безопасную и защищенную среду, в которой он может творить все, что хочет! Например, вы подключаете свой рабочий ноутбук дома к Интернет через коммутируемую линию или по выделенной линии, и систему поражает троян. Подключение в офисе защищено подключением VPN, которая активизируется сразу при вашем подключении к почтовому серверу или к другим защищенным ресурсам. Хакер может получить доступ к этим ресурсам, которые иначе были бы защищены VPN.

В: Я все-таки не понимаю, как работают одноразовые пароли.

О: Рассмотрим один пример. У вас имеется аппаратный маркер RSA Secure ID. Это — небольшое устройство с экраном, цифры на котором меняются каждые 60 секунд. Эти цифры — ваш ответ на запросы сервера RSA, т. е. ваш пароль. Маркер и сервер синхронизированы, поэтому, когда вы регистрируетесь, сервер запрашивает пароль, и вы вводите число, которое в данный момент высвечивается на экране маркера Secure ID. Вы будете аутентифицированы только для данного сеанса, однако при следующем входе цифры будут другие: вот вам и одноразовый пароль.

Приложение В

Введение в системы обнаружения несанкционированного вторжения в сеть и Snort

Разделы:

- **Введение в системы обнаружения несанкционированного вторжения в сеть**
- **Ответы на общие вопросы по IDS**
- **Ввод Snort в архитектуру сетевой защиты**
- **Определение аспектов проектирования и конфигурирования IDS**
- **Терминология IDS**

☑ Резюме

☑ Краткое резюме по разделам

☑ Часто задаваемые вопросы

Введение в системы обнаружения несанкционированного вторжения в сеть

На часах — три ночи, а Энди Этакер (Andy Attacker — вымышленное собирательное имя хакера) уже весь в работе. С результатами последнего сканирования портов в руках Энди нацелился на кажущиеся уязвимыми серверы. Он прилагает героические усилия, стараясь переполнить буферы и переписать указатели с целью взлома чужих серверов. Кое-что ему удается. Воодушевленный успехом, Энди быстренько устанавливает на «убитые» машины руткиты, попутно открывая механизмы доступа через черные ходы, слегка блокируя машины от доступа других негодяев и усиливая контроль. Покончив с этим, Энди приступает к очередному раунду операции «смотри и пользуйся» на свежевзломанных компьютерах.

На часах — три ночи, а Дженнифер Сисадмин (Jennifer Sysadmin — вымышленное имя системного администратора) просыпается от пронзительного и настойчивого пиканья пейджера. Она сонно находит его и пытается рассмотреть сообщение. Это предупреждение о попытке переполнения Secure Shell... исходящее с одного из ее серверов. Дженнифер вздрагивает и окончательно просыпается. Сбрасывая одеяло, она недовольно ворчит что-то о подлой манере взломщиков заниматься своим черным делом, когда самый сон, хватает мобильный и со знанием дела направляется к ближайшему компьютеру.

Три часа утра. На другом конце города мирно похрапывает Боб Сисадмин. Ничто не тревожит его сон — ни пейджер, ни мобильный.....

Неужели защита сети Боба настолько лучше, чем у Дженнифер, что он может спокойно спать, когда она, проклиная все на свете, занимается «ремонтно-восстановительными работами»? Или, может быть, его систему тоже «кракнули», только он об этом еще не знает? Мы тоже не знаем. IDS (Intrusion Detection System) — это оружие в арсенале системных администраторов, администраторов сетей и специалистов по безопасности, обеспечивающее сообщения в реальном времени о любой подозрительной деятельности в сети и предупреждающее о наличии в ней небезопасных систем. Несмотря на свое несовершенство и невозможность предупреждения обо всех «нападениях», IDS обладают уровнем машинного интеллекта, столь необходимого для понимания администратором того, что на самом деле происходит на его хост-машинах и в сети в целом.

Что такое несанкционированное вторжение?

Чтобы понять, что такое «обнаружение вторжений», надо знать, что такое «вторжение». Словарь Вебстера определяет слово «вторжение» как «акт проникновения или входа в место или состояние без приглашения, права или должного приема». В данном случае вторжением называется деятельность несанкционированной системы или сети на одном компьютере или в целой сети. Вторжение может принимать форму

законного пользователя системы, пытающегося получить больше прав доступа к системе, чем ему предоставлено, удаленного, неавторизованного пользователя, пытающегося дискредитировать работающую службу для создания в системе учетной записи, вируса, безумствующего в системе электронной почты, и многого чего еще... Вторжения могут поступать от злонамеренных энди этакеров либо от чудовищно легкомысленных арчибальдов энд'юзеров (Archibald Enduser — вымышленное имя конечного пользователя), которые открывают все приходящие им сообщения с вложениями, несмотря на многочисленные увещевания не делать этого. Вторжения могут поступать от абсолютно незнакомых людей из-за трех континентов, от разозленного недавно уволенного сотрудника из другого района города и даже от тех коллег, которым вы всегда доверяли...

ПРИМЕЧАНИЕ Выявление злонамеренной деятельности своих собственных коллег — одна из важнейших целей IDS во многих средах. В принципе, корректно реализованная IDS, контролируемая кем-то, помимо сисадмина, может быть одним из способов, с помощью которого сисадмина можно «поймать» на неблаговидной для компании деятельности. Это одна из главных причин того, почему персонал, занимающийся сетевой защитой, должен анализировать события IDS, а сисадмины — управлять системами.

Юридические определения

Прозрачных и универсальных юридических стандартов того, что называется несанкционированным вторжением, нет. Во многих странах, например в США и Австралии, существуют федеральные законы о преступлениях в области информационных технологий, но есть страны, в которых таких законов нет. Существуют различные государственные законы и региональные юридические акты на местах, но далеко не везде. Юрисдикция за преступления в области информационных технологий часто весьма размыта, особенно когда законы в местоположении компьютерного злоумышленника сильно отличаются от региональных законов местоположения дискредитированной системы. К тому же, даже если вторжение четко укладывается в рамки закона, мало какие юридические консалтинговые органы будут тратить время на его рассмотрение без гарантий определенной оплаты. Некоторые оценивают свои услуги в 10 000 USD, другие — до 100 000 USD; цифры варьируются в зависимости от региона.

Другим юридическим вопросом использования IDS является конфиденциальность. В техническом смысле IDS — это полнофункциональная система прослушивания. В США применение таких устройств регулируется федеральным законодательством, включая Титул III Свода законов по контролю за преступностью и безопасностью дорожного движения (Omnibus Crime Control and Safe Streets Act) 1968 г. (Титул III), 18 U.S.C §§ 2510-2522 и Закона о конфиденциальности электронной связи (Electronic Communications Privacy Act) от 1986 года. Эти законы подчиняются менее строгим

законам, регулирующим ситуации, когда необходимо прослушивать и перехватывать телефонные переговоры, например Статут о прослушивании телефонных переговоров и слежения «Поправка о провайдерах» (Pen Registers, Trap and Trace Statue «Provider Exception»), 18 U.S.C, § 2511(2)(h). Сюда, как правило, входит перехват характеристик и моделей трафика без анализа собственно данных. В соответствии с этими юридическими актами, перехват сетевых данных может быть незаконным, особенно если он осуществляется не оператором сети при выполнении им своих обычных служебных обязанностей либо не в целях непосредственной помощи проводящемуся расследованию преступной деятельности компьютерного нарушителя. Авторы настоятельно рекомендуют проконсультироваться с юристом компании на предмет конкретной юрисдикции данного вопроса, а также возможной интенсивности развертывания IDS в корпоративной сети.

Некоторые компании полагаются на статус своих данных как «защищенной коммерческой тайны», находящихся под защитой местных универсальных положений о коммерческой тайне. Обычно такие законы требуют, чтобы информация не была доступна широкой общественности и чтобы предпринимались определенные действия по их защите. Поэтому, если компания полагается на такие законы при похищении у нее информации, то для нее может оказаться неприятным потрясением тот факт, что суд сочтет меры защиты недостаточными. Впрочем, Закон об экономическом шпионаже США (U. S. Economic Espionage Act) от 1996 года (см. www.cybercrime.gov/eea.html) может поставить подобную деятельность в ранг федерального преступления.

На это также может повлиять тип и размах деятельности. На форумах по компьютерной безопасности часто поднимается вопрос о том, законно ли сканирование портов. Ответ зависит от конкретной юрисдикции. В 1998 г. в Норвегии вышло постановление о том, что сканирование портов не является незаконным. Однако закон штата Мичиган гласит, что несанкционированный доступ к компьютеру является незаконным, если не было повода предположить, что система предназначена для всеобщего пользования. Юристы по сей день спорят о том, является ли сканирование портов «несанкционированным использованием» (unauthorized use). Некоторые законодательства требуют размещения специальных сообщений, открыто запрещающих доступ, чтобы показать, что использование той или иной системы не санкционировано. При этом ожидания конфиденциальности могут превратиться в своего рода уравнение: если пользователь считает, что работа его системы может быть конфиденциальной, то преследование его за пользование ею может быть затруднено, даже если такое использование заведомо злонамеренно.

Лучшим способом распутывания этого юридического клубка, как правило, является максимальная защита всех систем, четкая маркировка всех доступных служб регистрационными сообщениями с указанием условий использования, а также доскональное знание местных и федеральных законов, если таковые имеются. Это поможет защитить системы и определить, что именно по данной юрисдикции считается несанкционированным вторжением.

Сравнительный анализ понятий сканирования и дискредитации

При мониторинге сетевой деятельности первым, что бросается в глаза, является процесс сканирования, особенно если оно осуществляется в больших объемах. Независимо от того, проводится сканирование на предмет выявления слабых мест системы или это обычное сканирование открытых портов, подобного рода деятельность является вполне обычной как в не фильтрованной среде Интернет, так и во многих частных сетях. Многие IDS сконфигурированы на запрет операций сканирования, и, как правило, при любой форме сканирования на экране появляется множество предупреждающих сообщений. Само по себе сканирование — не обязательно всегда злонамеренная операция, оно может иметь юридические основания (например, перед наложением заплат (патчей) администратор локальной системы проверяет свою сеть на наличие уязвимых мест или компания нанимает специалиста для проведения аудита защиты своих систем), но довольно часто сканирование является прелюдией к намеренной атаке. По сути дела, многие администраторы хотят получать предупреждающие сообщения о том, что их систему сканируют. Сканирование со слежением также может быть полезно в целях сопоставления на случай последующей атаки злоумышленников.

Большинство широко распространенных программных продуктов для сканирования распространяется бесплатно, и они вполне доступны. Быстрый поиск в системе Google выдаст результаты от ping и FTP (File Transfer Protocol) «Grim's Ping» до полнофункционального сканера портов Nmap, от коммерческого сканера SolarWinds до сканера слабозащищенных мест Nessus. Поскольку инструменты сканирования — легкодоступны, не удивительно, что они так широко используются.

При этом важно понимать, что само по себе сканирование еще не есть попытка дискредитации системы, и к этому процессу не стоит относиться с той же степенью активности реагирования, какой заслуживают попытки фактической атаки на систему. Некоторые люди проводят сканирование из чистого любопытства, без всяких намерений взлома. Однажды на конференции по компьютерной защите авторам довелось встретиться с молодым человеком, который признался в том, что перед заключением с кем-либо финансовых сделок через Интернет, он сканировал все машины компании-партнера, какие только мог. Таков был его метод определения степени надежности защиты систем будущих партнеров до того, как он доверит им свои деньги.

Еще важно отметить, что операции сканирования проводятся почти постоянно. На «Диком Западе» все виды автоматизированных программ постоянно сканируют огромное количество адресов. Некоторые из них могут быть вашими. Инструменты мониторинга сетей, черви и вирусы, автоматизированные приложения оптимизации, специализированные сценарии (script kiddies) и много что еще постоянно пытаются прозондировать ваши компьютеры и сеть. Если не будут предприняты попытки их фильтрации, то этот трафик станет жизненным фактом вашей работы в Интернете.

ПРИМЕЧАНИЕ Несмотря на всю важность осведомленности о том, когда сеть сканируют, очевидно, что никому не захочется терять драгоценного времени на отслеживание каждого идиота, который «сидит» в сети и как будто бы сканирует ее. Лучший способ получения информации о сканировании — это отслеживание исходных IP, осуществляющих сканирование, с последующим соотнесением их со случаями высокоприоритетных предупреждений либо поиск повторяющихся сканеров.

Вирусы и черви — SQL Slammer

Итак, теперь, когда процесс сканирования в общих чертах рассмотрен, перейдем к более подробному обсуждению некоторых фактических попыток дискредитации систем. Еще одним очень распространенным типом трафика, который будет вызывать срабатывание установленных IDS, являются автоматизированные черви. Черви и вирусы — весьма неплохие кандидаты на отслеживание IDS, потому что их поведение повторяется и постоянно идентифицируется. Даже полиморфные компьютерные черви и вирусы, делающие попытки многовекторных атак, имеют общее сетевое поведение, определенную модель трафика, которые IDS может сопоставить и обнаружить. В качестве примера рассмотрим червя SQL Slammer.

25 января 2003 года червь SQL Slammer был выпущен на волю. Еще известный как Sapphire, этот червь пользуется слабостями Microsoft SQL Server. Он отправляет 376-байтовый пакет UDP (User Datagram Protocol, пользовательский протокол данных) на порт 1434, переполняет буфер на сервере SQL и получает привилегии SYSTEM — высший уровень дискредитации в операционной системе Windows. Единожды «заразив» хотя бы один хост, он начинает сканировать IP-адреса для дальнейшего распространения.

ПРИМЕЧАНИЕ Черви, использующие множественные пути атак, представляют собой прекрасный пример ценности процесса сопоставления. Отдельные предупреждения от CodeRed или Nimda — достаточно распространены, но когда они вместе (как и будет от CodeRed или Nimda), тогда они являются явным следом червя.
Также следует отметить, что SQL Slammer — замечательный пример ситуации, когда IDS «активного реагирования» не сможет предотвратить заражения, а встроенная IDS — сможет.

Распространение по всему миру с момента появления у этого червя заняло порядка 10 минут. Огромные объемы сетевой пропускной способности были забиты попытками сканирования и дальнейшего распространения червя. Очень много систем было дискредитировано. Он вывел из строя пять из 13 корневых серверов доменных имен, предоставлявших службы имен в Интернет. С заключением корпорации Microsoft по поводу этого червя можно ознакомиться на сайте www.microsoft.com/technet/treeview/default.asp?url=/technet/security/alerts/slammer.asp, а Координацион-

ного центра группы компьютерной «скорой помощи» (Computer Emergancy Response Team Coordination Center's, CERT-CC) — на сайте www.cert.org/advisories/CA-2003-04.html.

ПРИМЕЧАНИЕ CERT-CC — экспертный центр по вопросам защиты Интернет, расположенный в Институте программотехники (Software Engineering Institute), финансируемом правительством научно-исследовательского центра, руководимого Университетом Карнеги-Меллона (Carnegie-Mellon University).

Так, как же лучше поймать этого червя с помощью IDS? Очевидно, что это — именно тот вид деятельности, которую необходимо выявлять в сети. Все хосты, зараженные червем Slammer, объединяет эксплуатационная нагрузка, которую он рассылает. И это — именно то, против чего выступает соответствующая этой деятельности подпись Snort IDS, которая приведена ниже:

```
alert udp $EXTERNAL_NET any -> $HOME_NET 1434 (msg: "MS-SQL Worm propagation
attempt"; content: " |04|"; depth:1; content: "|81 F1 03 01 04 9B 91 F1 01 |";
content:"sock"; content: "send"; reference:bugtraq,5310; classtype:misc-attack;
reference bugtraq,5311;
reference:url,vil.nai.com/vil/content/v_99992.htm; sid:2003; rev:2;)
```

Здесь видно, что предупреждение помечено как попытка распространения червя (worm propagation) и что оно совпадает с трафиком UDP, входящим в сеть $HOME_NET на порту 1434 со специфической полезной нагрузкой. С помощью этой подписи можно обнаружить и пронумеровать увиденные попытки атаки, а также, на какие хосты они были направлены. Массивные автоматические атаки, подобные этой, обычно порождают скоординированную реакцию со стороны сообщества сетевой защиты: IDS-программисты пишут новые подписи, разработчики антивирусных программ пишут диагностику и исправления, провайдеры магистральных сетей отслеживают трафик и ослабляют воздействие путем фильтрации по запросам и по необходимости. Эта подпись помогает отследить попытки заражения сети червем, а также обеспечить защиту сети от последующих нападений.

Скоординированные действия компаний и разработчиков средств защиты — один из способов, с помощью которых можно «идти в ногу» со злоумышленниками. Очень большое число компаний специально занимается оказанием помощи пострадавшим от последствий вирусных атак, в том числе в обмене информацией.

ПРИМЕЧАНИЕ Ниже перечислены некоторые из многих организаций, чья деятельность связана со смягчением последствий вирусных нападений:

- Forum of Incident Response and Security Teams (Forum of Incident Response), также известная под аббревиатурой FIRST, — это сообщество профессионалов в области сетевой защиты в различных организациях. Членство ограничено приемлемыми рабочими группами с четкой регистрационной и организационной структурой, спонсируемыми существую-

щей рабочей группой и способными установлению защищенных коммуникаций через PGP.

- Центры совместного использования информации и анализа (Information Sharing and Analysis Centers, ISAC), зарегистрированные в США в 1998 году под эгидой PDD 63 — Политика защиты критичной инфраструктуры Америки. ISAC охватывают такие сферы деятельности, как энергетика, финансовые операции, контроль за запасами питьевой воды, наземный транспорт, но самым уместным ISAC для защиты электронных сетей является ISAC информационных технологий (Information Technology ISAC) (www.it-isac.org/).
- Distributed Intrusion Detection System Dschield занимается сопоставлением записей журналов брандмауэров и сообщениями о вирусных атаках в сети по всему миру. В эту организацию каждый может вступить либо представить для анализа свои системные журналы анонимно. Вступление в члены — бесплатно.
- Для обеспечения сетевой защиты, администрирования брандмауэров и IDS, анализа системных журналов и сопоставления вирусных атак любой компании существует огромное множество коммерческих предложений. Одни провайдеры сопоставляют данные, полученные от разных клиентов, для повышения вероятности выявления наиболее активных злоумышленников, другие — нет. Специфика предлагаемых услуг зависит от того, кто их предоставляет.

Живые атаки — переполнение буфера электронной почты

Выше уже рассматривались действия IDS по извещению о том, что имела место автоматическая атака на сеть. Однако как быть с атаками, управляемыми человеком, с единичными попытками переполнения сетевой службы, а не с виртуальным потоком информационных пакетов? В решении этой проблемы может помочь Snort. Рассмотрим наиболее часто поражаемое слабое место — переполнение буфера Wingate POP3.

Уязвимость — удаленное переполнение буфера в реализации Wingate демона POP3. После отправки команды USER достаточно большой объем данных, следующих за «USER», переполнит буфер, что может привести к исполнению произвольного кода. При нормальном использовании POP3 демон просто передаст после команды «USER» имя пользователя, а обычное имя пользователя редко когда бывает очень длинным. Рассмотрим правило Snort, выявляющее попытку использования (эксплуатации):

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 110 (msg: "POP3 USER overflow attempt";
flow:to_server, established; content: "USER"; nocase; isdataat: 50, relative;
pcre: "/^USER\s[^\n] {50, }/smi"; reference:bugtraq, 789; reference:cve, CVE-
1999-0494; reference:nessus, 10311; classtype:attempted-admin; sid:1866; rev:7;)
```

Данное правило осуществляет поиск данных с содержимым USER, за которыми следует более 50 байтов данных, где эти 50 байтов данных после USER не содержат символа новой строки. Это должно соответствовать модели данных, которая будет видна при реальной попытке переполнения данного буфера, и не должно соответствовать регистрационным записям авторизованных пользователей.

Принципы работы IDS

Теперь, когда рассмотрены некоторые из возможностей IDS, относящиеся к предупреждениям о появлении опасного трафика, настало время обсудить подробнее, на что конкретно IDS прежде всего должна обращать внимание, какие источники данных используются для подобного мониторинга, как IDS отличает трафик атакующего от обычного трафика, а также некоторые возможные ответные действия для обнаружения опасных трафиков.

Что отслеживает IDS?

Начнем с того, что вообще может отслеживать IDS. Это в большой степени зависит от типа IDS и ее местоположения в сети. IDS классифицируются по их функциональности и не очень строго разделены на три следующие категории:

- NIDS (Network-Based IDS, IDS на базе сети);
- HIDS (Host-Based IDS, IDS на базе хоста);
- DIDS (Distributed IDS, распределенные IDS).

Сетевые IDS

NIDS получили свое название потому, что выполняют мониторинг всего сетевого сегмента или подсети. Это осуществляется изменением режима сетевого адаптера (network interface card, NIC) NIDS. Обычно сетевой адаптер работает в упорядоченном режиме, прослушивая только пакеты данных, предназначенные для его адреса протокола управления доступом (media access control address, MAC-адреса). Все прочие пакеты не отправляются в стек для анализа: они игнорируются. Для мониторинга всего трафика подсети NIDS должна принимать все пакеты (не только предназначенные для машины NIDS) и отправлять их в стек. Этот процесс называется беспорядочным режимом.

В этом режиме NIDS может перехватывать все подключения к сетевому сегменту. Однако этого недостаточно для того, чтобы NIDS прослушивала весь трафик подсети. Сетевое устройство, расположенное непосредственно выше NIDS, также должно быть сконфигурировано на отправку всех пакетов в подсеть NIDS. Если это концентратор, тогда все пакеты будут отправляться автоматически, потому что все порты концентратора принимают весь трафик, проходящий через него. Однако если устройство — коммутатор, то может потребоваться перевести порт на нем в режим монито-

ринга, превратив его в отраженный порт. После настройки NIDS в интерфейсе рекомендуется запустить инструмент сетевого анализа для подтверждения того, что в подсети просматривается весь трафик целиком.

Преимущество NIDS заключается в том, что она никак не влияет на системы или сети, мониторинг которых осуществляет. Она не добавляет никакой нагрузки на хосты, и злоумышленник, которому удалось «запортить» одну из контролируемых им систем, не может прикоснуться к NIDS; он может даже не подозревать о ее наличии. Одним из недостатков такого мониторинга является то, что выделенные для данной сети зеркально отраженные порты минимизируются, а также минимизируется пропускная способность самого отражения. Если 20 портов по 100 Мб отражаются на один порт, начинается заполнение системной платы... как только объем превысит 5 Гб или 11 Гб системной платы, начинаются проблемы.

Инструментальные средства и «ловушки»

Инструментальные средства сетевого анализа

При настройке или отладке NIDS очень важно убедиться в том, что просматривается весь трафик подсети, к которой осуществлено подключение. Snort может прекрасно выполнять роль пакета сетевого анализа. После вызова в командной строке ключом **-i** Snort прослушивает заданный интерфейс. Убедитесь в том, что просматривается входящий и исходящий трафик других машин в сети, а не только широковещательный трафик и трафик локальной машины.

Помимо Snort еще несколько программ являются замечательными средствами сетевого анализа. Ethereal (www.ethereal.com) — межплатформенный пакет сетевого анализа. Tcpdump (www.tcpdump.com) уже имеется на многих системах Unix, а Windump (http://windump.polito.it) выполняет те же функции для Windows, хотя его, как правило, приходится устанавливать в систему отдельно.

В свете соблюдения правил конфиденциальности мониторинг сетевых связей заслуживает особого внимания. До проведения подобных операций ознакомьтесь с местными положениями законодательства по данному вопросу.

На рис. B.1 показана сеть с тремя NIDS. Узлы размещены в стратегических сетевых сегментах и могут просматривать сетевой трафик всех устройств сегмента. Такая конфигурация представляет собой стандартную топологию сетевой защиты по периметру, когда экранированные подсети, обслуживающие общедоступные серверы, защищены NIDS. При дискредитации общедоступного сервера в экранированной подсети этот сервер может превратиться в платформу для запуска дополнительных

задач. Для предотвращения еще больших проблем следует осуществлять тщательный мониторинг.

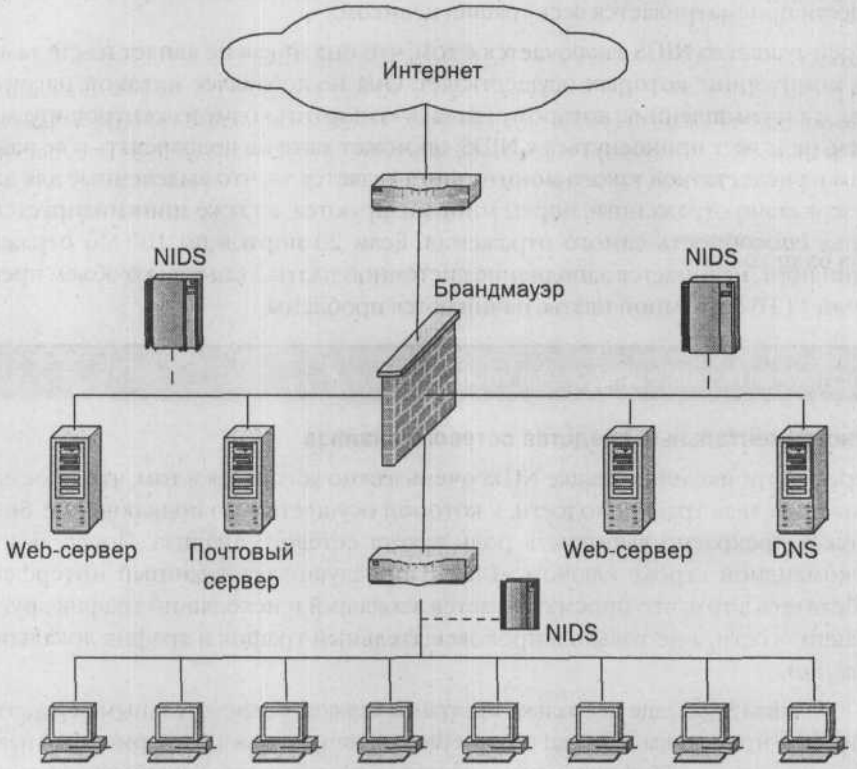

Рис. В.1. Сеть NIDS

Внутренние базисные системы защищены дополнительной NIDS для уменьшения подверженности внутренней дискредитации. Использование множественных NIDS в рамках сети — пример глубоко эшелонированной архитектуры защиты.

ПРИМЕЧАНИЕ В качестве дополнительного напоминания: правила конфиденциальности могут оказаться опасной ловушкой. Даже если пользователи расписались в том, что они ознакомлены с разделом «Порядок работы» в своде правил корпоративной политики, что дает вам право просматривать их трафик, все равно могут возникнуть ситуации, когда они могут потребовать презумпции конфиденциальности. Обязательно заручитесь одобрением руководства (если вам поручено развертывание IDS) или отдела кадров (при наличии его в компании). Последней инстанцией может стать юрист компании; обратитесь к нему за подтверждением того, что никакие законы не нарушаются. Если не соблюдать корректность, то в конечном итоге винова-

тыми окажетесь вы, а не человек, трафик которого подвергался мониторингу! Акт PATRIOT, несмотря на все его несовершенство, все-таки гарантирует провайдеру услуг и сисадмину право следить за использованием сети и систем с целью выявления нарушений.

Особое внимание следует обращать на то, кто просматривает данные, а также на процесс обеспечения их защиты. И, наконец, помните о том, что все юридические советы, описанные в данной книге, не являются консультацией профессионального юриста; перед тем как воспользоваться ими, следует проконсультироваться у профессионала.

IDS на базе хоста

IDS на базе хоста (Host-based IDS, HIDS) отличаются от NIDS по двум признакам. Во-первых, установленная HIDS защищает только свою систему, а не всю подсеть и, во-вторых, сетевая плата системы, на которой установлена HIDS, как правило, функционирует в упорядоченном режиме. Иногда это является преимуществом: не все сетевые адаптеры способны работать в беспорядочном режиме, хотя большинство новейших функционирует именно так. Кроме того, беспорядочный режим значительно повышает нагрузку на CPU не очень быстродействующей хост-машины.

Еще одним преимуществом HIDS является способность «подгонять» набор правил индивидуально под конкретную базисную систему. Например, нет необходимости конфигурировать множественные правила, предназначенные для обнаружения использования сетевой файловой системы (Network File System, NFS) на хосте, на котором NFS не используется. Возможность точной настройки набора правил повысит производительность сети и снизит вероятность ошибочных результатов (или верных результатов, которые не имеют значения). Основное же преимущество HIDS заключается в способности обнаружения особых изменений файлов и операционной системы хоста. HIDS может осуществлять мониторинг размеров файлов и контрольных сумм для того, чтобы ни одно злонамеренное изменение критичных системных файлов не осталось незамеченным. Система может перехватывать нестандартные системные вызовы, которые могут оказаться попыткой эксплуатации локальной уязвимости. Более того, HIDS может просматривать трафик внутри системы, который никогда не пересекается с сетью и, следовательно, никогда не может быть просмотрен с помощью сетевой IDS.

При всем этом существуют и обратные стороны выбора HIDS. Во-первых, придется выбрать систему, которая специально приспособлена под нужную операционную систему. Если в сети несколько операционных систем, а администратор хочет воспользоваться услугами одного поставщика HIDS, тогда производителя, продукция которого поддерживала бы все необходимые операционные системы, еще придется поискать. HIDS добавляет нагрузку на хост, на котором она сконфигурирована, поскольку процессы HIDS довольно ресурсоемкие. На отдельной рабочей станции это,

как правило, не представляет проблемы, однако не все так благополучно с постоянно загруженным сетевым сервером. Убедитесь, что вам известны все тонкости функционирования выбранной HIDS: одни могут следить за доступами к файлам, временем использования, технологической нагрузкой и/или системными вызовами, а другие при этом еще отслеживать сетевую деятельность с точки зрения хост-машины. Определитесь с тем, чего вы хотите от HIDS и убедитесь в том, что выбранная система поддерживает эти функции на необходимых платформах.

Кроме того, техническое обслуживание сети с несколькими развернутыми HIDS может оказаться довольно сложной задачей. Отдельное решение HIDS не всегда легко поддается расширению, и в отсутствие централизованного управления сисадмин может попросту физически не успевать следить за всеми поступающими сигналами предупреждения.

На рис. В.2 показана сеть, использующая HIDS на специализированных серверах и хост-машинах. Как упоминалось выше, набор правил для HIDS на почтовом сервере настроен на его защиту от несанкционированных использований, тогда как правила для web-сервера составлены для использования Web. Во время установки отдельные хост-машины можно сконфигурировать с обычным набором правил. Периодически можно загружать новые правила для учета новых слабых мест.

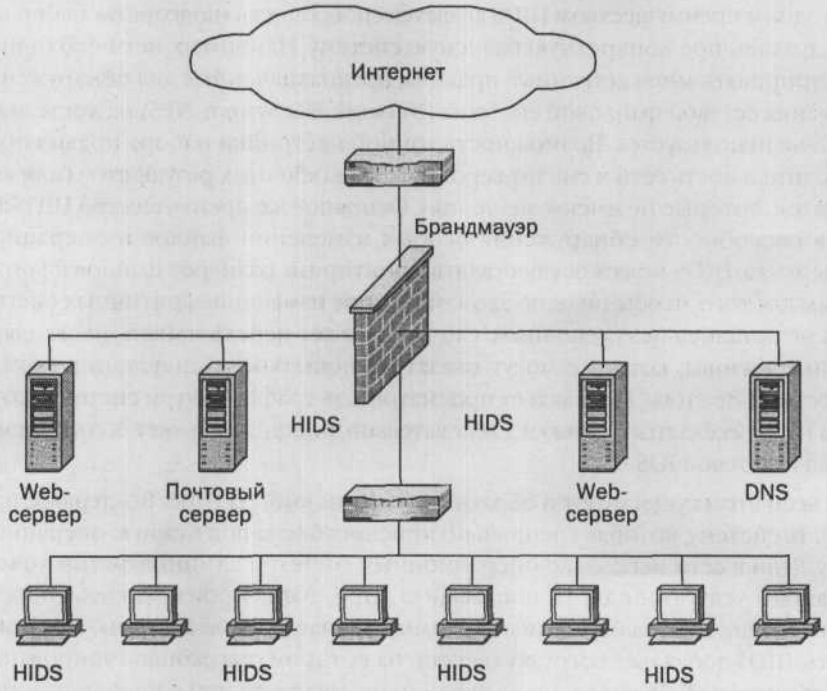

Рис. В.2. Сеть HIDS

Распределенные IDS

Распределенные системы обнаружения несанкционированного вторжения (Distributed, DIDS) — это комбинация сенсоров NIDS, сенсоров HIDS либо тех и других, распределенная по всему предприятию, где каждый «отчитывается» перед центральной системой сопоставления информации. Системные записи атак генерируются на сенсорах и загружаются (периодически или непрерывно) в центральный сервер, где хранятся в центральной базе данных. По мере поступления новых подписей атак они создаются или скачиваются на станцию управления, после чего пересылаются на сенсоры по мере необходимости. Разными типами сенсоров может управлять один сервер (а может и не управлять), а серверы управления часто отделены от серверов, собирающих системные записи. Правила для каждого сенсора можно настроить под его индивидуальные потребности сети или хоста, мониторинг которых осуществляет каждый сенсор. Предупреждающие сигналы могут отсылаться в систему передачи сообщений, расположенную на рабочей станции системы сопоставления, и использоваться для уведомления администратора IDS.

На рис. B.3 показана система DIDS, состоящая из четырех сенсоров и станции централизованного управления. Сенсоры NIDS1 и NIDS2 функционируют в неви-

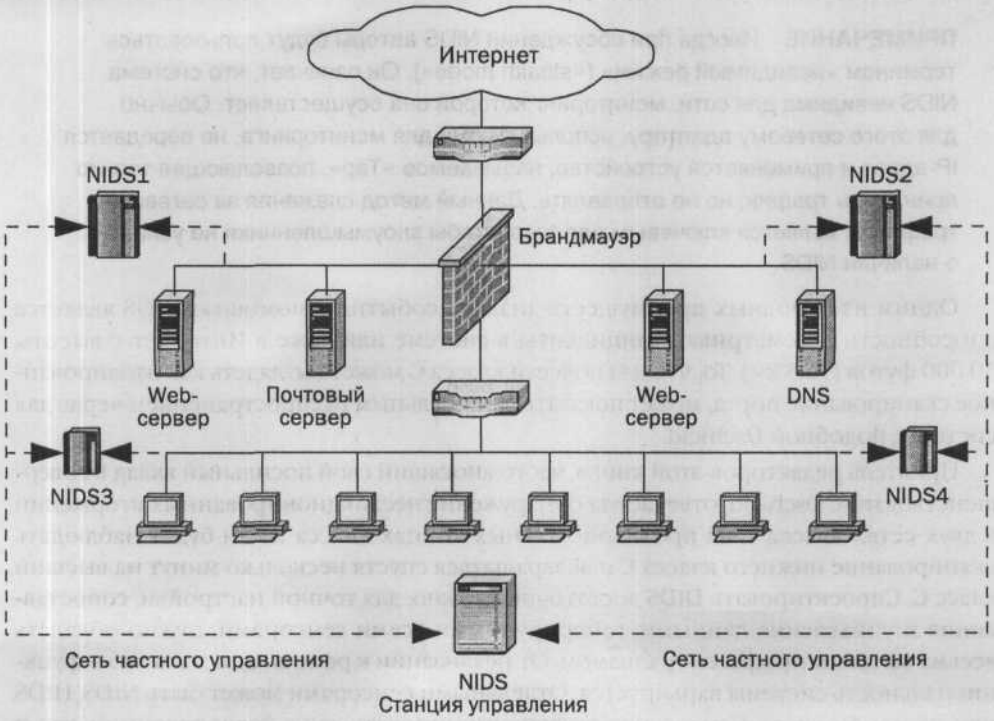

Рис. B.3. Сеть DIDS

димом беспорядочном режиме и защищают общедоступные серверы. Сенсоры NIDS3 и NIDS4 защищают базисные (централизованные) системы в надежной базовой системе.

Сетевые транзакции между сенсором и менеджером (системой управления) могут осуществляться в частной сети, либо сетевой трафик может использовать существующую инфраструктуру. При использовании для управленческой информации существующей сети настоятельно рекомендуется применение дополнительной защиты (шифрование или технология VPN). Рассылка всей информации о защите по сети открытым текстом равносильна обращению к смекалистым хакерам с просьбой о ее перехвате. В лучшем для вас случае они узнают, когда будет запущена IDS, и смогут хорошо подготовиться, чтобы избежать обнаружения. В худшем — информация будет перехвачена, и настройки механизма предупреждения будут изменены: данные будут испорчены и на них нельзя будет полагаться при анализе и/или судебном преследовании. Другой аспект, который следует учитывать при принятии решения о связи DIDS по обычной сети, — если корпоративная сеть когда-либо будет переполнена или выведена из строя «злобным» трафиком (как произошло со многими сетями, «благодаря» SQL Slammer), то сенсоры IDS не смогут осуществлять взаимодействие с серверами сопоставления или управления, что значительно снизит их полезность.

ПРИМЕЧАНИЕ Иногда при обсуждении NIDS авторы будут пользоваться термином «невидимый режим» («stealth mode»). Он означает, что система NIDS невидима для сети, мониторинг которой она осуществляет. Обычно для этого сетевому адаптеру, используемому для мониторинга, не передается IP-адрес и применяется устройство, называемое «Tap», позволяющее только принимать трафик, но не отправлять. Данный метод слежения за сетевым трафиком является ключевым для того, чтобы злоумышленники не узнали о наличии NIDS.

Одним из основных преимуществ анализа событий с помощью DIDS является способность рассматривать инциденты в системе или даже в Интернет с высоты 50 000 футов (16,5 км). То, что для подсети класса С может выглядеть как изолированное сканирование порта, может показаться глобальным распространением червя для системы, подобной Dschield.

Приятель редакторов этой книги, часто вносящий свой посильный вклад в совершенствование Dschield, отвечает за обнаружение несанкционированных вторжений в двух сетях класса С на противоположных концах класса В. Он будет наблюдать сканирование нижнего класса С и возвращаться спустя несколько минут на высший класс С. Спроектировать DIDS достаточно сложно; для точной настройки, сопоставления и управления данными, генерируемыми всеми сенсорами, нужно обладать весьма высоким профессионализмом. От реализации к реализации масштаб и функциональность системы варьируется. Отдельными сенсорами может быть NIDS, HIDS или их комбинация. Сенсор может функционировать как в беспорядочном, так и упорядоченном режимах.

Теперь, ознакомившись с методами развертывания разных типов IDS, рассмотрим информацию, которые они могут собирать.

Информация приложений

Все три типа IDS могут контролировать определенную часть информации, имеющей отношение к программным приложениям. Это зависит от трафика, поступающего на web-сервер, и поступающих из него на внутренние структуры данных заказных приложений (разумеется, для таких приложений необходимо настроить правила IDS для проверки трафика). По мере прохождения трафика приложения по сети он обнаруживается NIDS. Если трафик отправлен открытым текстом (Telnet или по протоколу передачи гипертекстовых файлов (HTTP)), то у NIDS не должно возникать проблем соответствия. В качестве примера рассмотрим следующую сигнатуру поиска доступа к уязвимому PHP-приложению «Proxy2.de Advanced Poll 2.0.2.».

Инструментальные средства и «ловушки»

PHP и изменение акронимов

Изначально аббревиатура «PHP» расшифровывалась как «Personal Home Page» (личная домашняя страница). В соответствии с историей происхождения PHP (www.cknow.com/ckinfor/acro_p/php_1.shtml), она обозначала «обертку» для web-страниц над Perl. По мере смещения функциональности PHP в сторону полностью сформировавшегося серверного языка сценариев для web-серверов, этот акроним потерял свое значение и впоследствии превратился в рекурсивный акроним «PHP: Hypertext Preprocessor» (гипертекстовый препроцессор) (см. www.php.net/manual/en/faq.general.php).

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg: "WEB-PHP Advanced
Poll admin_tpl_misc_new.php access"; flow:to_server, established; uricontent: "/
admin_tpl_misc_new.php"; nocase; reference:bugtraq,8890; classtype:web-
application-activity; sid:2299; rev:2;)
```

Даже если трафик передается в двоичном формате, то при наличии известной полезной нагрузки или постоянной части пакета (уникальной для того, чтобы избежать ошибочных результатов), с которым NIDS может осуществлять сопоставление, возможно сопоставление правил на основе подписи. Однако зашифрованный трафик приложения, отправляемый со сравнительно хорошей криптографией, может выходить за рамки того, что обнаруживает большинство NIDS. Написать хорошее правило NIDS для трафика, зашифрованного с помощью хорошего начального произвольного числа (например, одинаковые результаты строки ввода в разном выводе всякий раз при шифровании), — задача достаточно сложная.

Зашифрованный трафик — это та область, где особенно выделяются IDS на базе хоста. Трафик программного приложения, проходящий по сети в зашифрованном формате, обычно декодируется в каждой конечной точке. Следовательно, трафик, который ранее представлял собой случайную ненужную информацию, превращается в уязвимые комбинации на хосте, и сопоставление с ним можно осуществлять по сигнатурам.

Что представляет интерес в информации, связанной с приложениями? Попытки использования полей ввода путем ввода слишком большого количества данных, известные переполнения или опустошения, использующие недостаток проверки ввода, а также инжекция SQL (язык структурированных запросов) — всего лишь несколько примеров. Разумеется, подписи очень разнятся в зависимости от защищаемого программного приложения.

ПРИМЕЧАНИЕ Замечание о том, что HIDS очень хорошо себя проявляют, когда дело доходит до просмотра зашифрованных данных, потому что они находятся на хосте, отправляющем или принимающем данные (и, следовательно, возникает большая вероятность того, что HIDS просмотрит информацию до того, как она будет зашифрована или расшифрована), не совсем верно. Важно помнить, что система HIDS по-настоящему хороша только при фактическом просмотре незашифрованных данных. Это означает, что если шифрование происходит на уровне приложения (например, выполняется web-браузером, клиентом SSH или почтовым клиентом) и HIDS просматривает сетевой трафик во время его выхода из системы или входа в нее после шифрования или до дешифрования, то HIDS бесполезна; система по-прежнему не сможет осуществить дешифрование и будет такой же «слепой», как и любая система NIDS.

Информация хоста

В то время как большинство HIDS на самом деле не видят всего, что происходит на хост-машине, эти системы могут наблюдать за поведением отдельно взятого хоста — от создания файлов и доступа к системным вызовам до сетевой деятельности на интерфейсе-заглушке (loopback). Для HIDS при их установке обычной практикой является создание базы данных состояния системы (размеры файлов, разрешения, значения времени доступа), после чего осуществляется мониторинг отклонений от этого эталонного уровня. На самом деле, для многих типов HIDS процесс настройки требует установки программного обеспечения HIDS с последующей обработкой при нормальном функционировании системы для задания эталонного уровня того, что изменяется, когда и кем.

Информация подсети

Большинство сетей имеет общие модели потоков трафика. Если известно, что одна машина в сети — почтовый сервер, то нет ничего удивительного в том, что все в него

поступающее и из него выходящее использует Простой протокол электронной почты (Simple Mail Transfer Protocol, SMTP). Если администратор привык к тому, что устройство сетевого мониторинга перебрасывает информацию на каждое сетевое устройство каждые пять минут, то данный трафик будет приемлем, даже несмотря на то, что точно такое же поведение другого устройства сети будет вызывать определенное опасение. Со временем любая усовершенствованная система NIDS должна быть настроена на распознавание ожидаемого поведения подсети, на которой она установлена, с обеспечением ожидаемого и приемлемого трафика и отправкой предупреждающих сигналов при поступлении сходного трафика с неавторизованных хостов. Рабочая станция авторизованного тестера может просканировать сеть, тогда как рабочая станция нового сотрудника — нет.

ПРИМЕЧАНИЕ Развертывание NIDS, описанное в предыдущем параграфе, часто называют IDS, основанной на корпоративной политике. Применение подобного рода систем наиболее эффективно в сферах со строгим контролем над тем, какой тип трафика наиболее приемлем. Поэтому такие системы весьма распространены в военных организациях или в компаниях с чрезвычайно строгим контролем за состоянием сетей и всех систем в целом. Если сфера деятельности предприятия очень динамичная или комплексная, то внедрить строгий принцип IDS на базе корпоративной политики будет сложнее.

Другим заслуживающим внимание и часто недооцениваемым компонентом трафика подсети является отображение протокола Уровня 2. Большинство IDS не придают особого значения трафику Протокола разрешения адресов (Address Resolution Protocol, ARP), применяемого для отображения MAC-адресов на IP-адреса в локальной сети. Злоумышленники могут сымитировать трафик путем изменения своих MAC-адресов или фальсификацией IP-адреса, им не принадлежащего, после чего попытаются перехватить обратный трафик. Такие ухищрения можно наблюдать на уровне подсети, в зависимости от сетевой топологии. Если NIDS размещена в другой локальной подсети, нежели та, в которой бывают атаки Уровня 2, то NIDS не сможет их обнаружить надлежащим образом. Когда сетевой трафик проходит маршрутизатор, MAC-адрес изменяется. Поскольку проверяются порты и местоположения MAC-адресов, то изменять их до проверки нельзя, поскольку в этом случае данные потеряют свою достоверность.

Таким образом, при необходимости перехвата данных Уровня 2 с помощью NIDS, следует убедиться в том, что система NIDS размещена в той же локальной подсети, что и наблюдаемые компьютеры, до того, как в передаче потока данных начнут участвовать маршрутизаторы.

Распределенные IDS (DIDS)

С помощью DIDS можно собрать и сопоставить всю необходимую информацию, однако масштаб охвата в данном случае гораздо шире. Вместо локального контроля

подсети и подключенных к ней машин можно получить общий обзор функционирования сети целого предприятия. Можно выборочно отбирать модели данных, которые в более мелком масштабе будут неблагоприятными или непоследовательными, и то, что казалось автоматически созданной резервной копией, на поверку оказывается скоординированной (злонамеренной) репликацией данных, распространенных по всей сети при их общем рассмотрении. Наблюдение за трафиком на уровне DIDS позволяет более прозрачно видеть крупномасштабные потоки данных и общие тенденции сетевого функционирования. Недостатком является то, что для эффективного осмысления объема собираемых данных требуются специальные инструментальные средства, иначе «незначительные» атаки, на выявление которых рассчитывал администратор, попросту затеряются в общем шуме рабочей среды.

Механизм наблюдения IDS за сетью

Если нет эффективного способа сбора данных для анализа, то наличие систем IDS не имеет смысла. К счастью, существует несколько возможных способов сбора данных IDS. Ниже описаны наиболее распространенные способы сбора данных для анализа IDS. Каждый имеет свои сильные и слабые стороны, и каждый по-своему хорош для решения различных задач. Для IDS существует несколько возможных источников данных.

Анализ пакетов

Любая система IDS, просматривающая сетевой трафик, выполняет анализ пакетов данных. Как уже отмечалось, NIDS переводит интерфейс в беспорядочный режим работы и осуществляет на этом интерфейсе пакетный анализ. При этом перехватывается каждый пакет, проходящий по кабелю локальной подсети. IDS не видят пакеты, проходящие через внутренний стек TCP/IP для машины, но потенциально просматривают все, что происходит в локальном кабеле. Однако многие HIDS, выполняющие анализ сетевого трафика, также используют сходные методики без применения беспорядочного режима для сбора трафика, относящегося к хостам, на котором они установлены. Пакетный анализ — классический способ обнаружения несанкционированных проникновений в сеть; в то же время существуют классические способы уклонения от пакетного анализа IDS, например атаки фрагментации, при которых нагрузка атаки разбивается по нескольким пакетам. Способы обхода защиты, а также основные рекомендации по его предотвращению рассматриваются в настоящем приложении ниже. Авторы настоятельно рекомендуют читателям ознакомиться с ними и иметь их в виду, когда производитель будет рассказывать о том, что их система не пропускает ни одного несанкционированного вторжения. Ответом IDS стало создание функции перекомпоновки пакетов с последующим их сопоставлением со вновь скомпонованным пакетом данных. В ответ злоумышленники изменили способ фрагментации пакетов, в результате чего определенные данные наложились

друг на друга (переписались). Были разработаны способы устранения подобного рода неприятностей, и т. д. Если читатели еще не догадались, то можно сказать, что пакетный анализ применяется в Snort.

Анализ системного журнала

Еще одним замечательным источником данных для проверки безопасности являются системные журналы. Многие системы IDS могут извлекать данные из системных журналов и «бить тревогу» при обнаружении каких-либо аномалий. На самом деле, в некоторых из первоначальных реализаций IDS мониторинг системных журналов использовался как способ сбора данных. Некоторые хакерские нападения — слишком вопиющие, судя по следам, которые они оставляют в системных журналах. Например, переполнение Secure Shell CRC32 может оставлять в системных журналах:

```
sshd [3698]: fatal: Local: crc32 compensation attack: network attack detected
```

ПРИМЕЧАНИЕ Доктор Тина Берд (Tina Bird) много занималась анализом несанкционированных вторжений по системным журналам. Ознакомиться с результатами ее исследований можно на сайте www.loganalysis.org.

Мониторинг системных вызовов

HIDS могут настраиваться в качестве резидента в ядре операционной системы и отслеживать (в некоторых случаях перехватывать) потенциальные злонамеренные системные вызовы. Системным вызовом называется запрос от программы к ядру операционной системы. Если HIDS считает, что какой-то вызов может быть опасным для системы, например запрос об изменении ID пользователя на ID привилегированного пользователя, то система может подать предупреждающий сигнал, либо, как в случае с некоторыми HIDS, например LIDS (Linux IDS), отклонить системный вызов при отсутствии особых указаний.

Слежение за файловой системой

Другой распространенной тактикой HIDS является наблюдение за размерами и атрибутами критичных файлов файловой системы. Если размер ядра операционной системы внезапно изменяется и никто из сисадминов не знает причины, то имеет смысл провести проверку. При обнаружении каталогов с возможностью записи в них любым внешним пользователем или изменений обычных системных бинарных файлов не исключено, что они поражены вирусами-троянами. Наблюдение за файловыми системами в этом смысле помогает администраторам отслеживать возможную злонамеренную деятельность; если ее не удалось предотвратить, то меры необходимо принять сразу же по обнаружении вторжения. Пожалуй, Tripwire — лучший из известных инструментов мониторинга файлов на предмет изменений, но есть и другие, выполняющие ту же функцию, включая открытое инструментальное средство под названием Advanced Intrusion Detection Environment (AIDE).

14 Зак. 1269

Механизм обнаружения попыток вторжения по собранным данным

Любая система IDS собирает очень большие объемы данных: сеть активна, серверы работают непрерывно, происходит постоянный обмен данными, постоянно запускаются различные процессы, слышен непрекращающийся электронный гул. Для эффективного функционирования IDS должна иметь как минимум один (если возможно, несколько) алгоритмов определения того, какой трафик заслуживает особого внимания администраторов. Существует несколько стратегий, но в основном на базовом уровне используются два тактических варианта.

Принципы «заведомо свой» и «заведомо чужой»

Идентифицировать и классифицировать сетевой трафик можно несколькими способами. Трафик можно рассматривать с точки зрения его соответствия установленной корпоративной политике защиты, диктуемой потребностями бизнеса или сети. Некоторые администраторы предпочитают допускать в сеть только тот трафик, о котором заведомо известно, что он не причинит ей вреда, другие же — наоборот: отсеивают только заведомо злонамеренные. Чаще всего политика компании следует принципу «заведомо свой». Для выбора наилучшего решения для своей компании проанализируйте типы трафиков, чаще всего поступающих в сеть, количество персонала, задействованного в обработке предупреждающих сигналов, а также целесообразность «дуть на воду, обжегшись на молоке».

Здесь важно определиться с потребностями: идентифицировать только приемлемый трафик в сети и блокировать все прочие либо идентифицировать известные виды атак, пропуская все остальное. Это — основная дилемма стратегии IDS, и администраторы брандмауэров знакомы с ней не понаслышке. Следование принципу «заведомо свой» потребует гораздо больших затрат труда, поскольку сортировать придется весь сетевой трафик с целью определения того, что может произойти и что потенциально рискованно. Администратор незамедлительно столкнется с огромным количеством ошибочных результатов, которые вывалит на него дымящаяся от нагрузки IDS, и ему придется медленно просеивать их до управляемого уровня для определения заведомо «чистого» трафика. Помимо этого, если в сети никогда ничего не менялось, все равно IDS придется постоянно подстраивать и перестраивать под штатные изменения, происходящие практически в каждой среде. Существуют автоматизированные инструментальные средства, определяющие «нормальность» происходящих процессов — допустимое приближение понятия «хорошо». Однако такие инструменты страдают от ошибочных результатов в комплексных или высокодинамичных средах. При этом они могут ошибочно принимать за «нормальный» какой-либо новый небольшой процесс, происходящий в течение достаточно долгого времени. (Вспомните историю про варку лягушки: если лягушку бросить в кипящую воду, то она выпрыгнет. Если же положить ее в холодную воду и постепенно нагревать, то лягушка ничего не заметит и просто сварится).

Однако, если следовать стратегии подачи тревожных сигналов только при обнаружении известного «чужого» (или подозреваемого таковым) трафика, то этим можно значительно сократить количество подаваемых тревожных сигналов. Правила, определяющие, что «хорошо», а что «плохо», могут быть весьма и весьма специфическими, поэтому при получении тревожного сигнала (при условии тщательно продуманных правил) можно быть вполне уверенным в том, что система IDS действительно столкнулась с «нехорошей» деятельностью в сети. Это означает, что сотруднику, контролирующему IDS, не обязательно быть «семи пядей во лбу» (ему не придется устранять неполадки IDS). Однако при данном подходе велика вероятность того, что атакующий трафик будет упущен, а это не соответствует установленным корпоративным правилам. Если же попробовать составить более гибкие правила, то количество ошибочных решений может возрасти. В некоторых сценариях, например в случае с домашней системой Арчибальда Энд'юзера, когда тот мало что понимает в механизме обнаружения вторжений и не имеет времени или желания научиться, это может оказаться наиболее оптимальным решением. Однако при желании повысить вероятность перехвата атаки и при наличии ресурсов для мониторинга и обслуживания IDS, можно рассмотреть другой подход. На выбор стратегии влияет анализ затрат/прибыли; следует оценить время и ресурсы, которые можно выделить на IDS, и важность и необходимость перехвата максимального количества атак.

ПРИМЕЧАНИЕ В реальной жизни в наиболее качественно спланированных реализациях IDS применяется комбинация обоих принципов. Там, где можно точно определить разрешенный трафик, пользуйтесь принципом «заведомо свой». Там, где приходится идти на компромисс или часто происходят изменения рабочей среды, следуйте принципу «заведомо чужой». Подход должен определяться обстоятельствами и соображениями целесообразности; только так администратор сможет повысить свои профессиональные навыки как аналитик несанкционированных вторжений.

Технологии реализации выбранной стратегии

IDS дифференцируют атакующий трафик от безопасной сетевой и системной деятельности несколькими способами. В некоторых изначально используется методика, называемая *анализом на основе правил* (также известная как *«анализ на основе подписи/сигнатур»*), при которой известная модель сопоставляется с тем, что видно в системе или сети. Мы уже рассматривали примеры правил Snort с поиском в сети содержимого пакета и его сопоставлением с набором заранее установленных правил. То же самое можно сделать при просмотре записей в системных журналах или наборах системных вызовов. Это очень похоже на то, как используют подписи вирусов многие программы-антивирусы для распознавания и блокирования от попадания в компьютерную систему инфицированных файлов, программ или активного web-содержимого (именно поэтому антивирусные средства необходимо регулярно обновлять). В современной коммерческой технологии IDS обнаружение подписей —

наиболее широко распространенный метод, поскольку его легко демонстрировать, он эффективен и доступен для настройки под конкретного пользователя; требует минимального обучения или опыта. По мере активной разработки новых способов несанкционированного внедрения можно писать новые подписи для сопоставления с новыми формами атак и принятия соответствующих мер.

Более сложной версией анализа на основе правил является анализ протоколов. Вместо составления сравнительно простого правила, определяющего аспекты события (хорошего или плохого), при анализе протоколов делается попытка определения любого мало-мальски допустимого поведения того или иного вида деятельности. Например, когда компьютеру нужно установить TCP-подключение, он отсылает пакет SYN. Допустимыми ответами будут либо RST/ACK, либо SYN/ACK. Что-либо иное будет рассматриваться как нарушение протокола. Данный подход обеспечивает немного больше гибкости в определении того, что есть «плохо». Вместо того, чтобы говорить: «Если вы видите строку длиной больше 500 байтов, заполненную специальным символом, это — атака данного типа», можно сказать: «В данной точке подключения не должно быть строки длиной, превышающей 500 байтов. Если она присутствует, то это означает атаку. Если более 500 байтов встречается где-либо в другом месте, то в этом нет ничего страшного». Проблема заключается в том, что, несмотря на четкое и краткое определение протоколов, не все производители обращают в этом определении внимание на все, что необходимо. В результате этого можно обнаружить, что протокол IDS на основе анализа справедливо «жалуется» на то, что не оговорено в RFC (Request For Comments, Запросы на комментарии: документы, используемые для определения большинства протоколов Интернет. Полный список представлен на сайте www.rdc-editor.org), но совершенно нормально для того или иного производителя. Кроме того, написание хорошей модели протокола требует чрезвычайно много времени, и сделать это довольно сложно, не говоря уже об эффективном внедрении с тем, чтобы его можно было использовать для мониторинга высокоскоростных сетей. Для этого требуются годы. Это означает, что большинство производителей очень неохотно распространяют свои модели протоколов открытым способом, даже при работе с собственными заказчиками. Следовательно, самостоятельное исправление ошибочных решений IDS анализа протоколов или ожидание, пока их исправит производитель, может занять очень много времени. Другой подход называется *обнаружением аномалий*. В нем используются полученные опытным путем или предварительно заданные концепции о «нормальном» и «ненормальном» поведении системы (называется *эвристикой*) для выявления отклонений системы от нормального поведения и мониторинга, создания отчетов или блокирования аномалий по мере их возникновения. Некоторые IDS обнаружения аномалий поставляются уже с заданными стандартами того, как должен выглядеть нормальный сетевой трафик, другие же отслеживают трафик сети (или функционирование систем) и используют алгоритм обучения для разработки на его основе базового профиля. Эти профили являются так называемыми «базовыми линиями» нормального функционирования, и их можно

построить с помощью статистической выборки, подхода на основе правил или с помощью нейтральных сетей (перечислено всего лишь три способа).

Буквально сотни производителей предлагают различные разновидности коммерческих IDS. Из-за простоты реализаций большинство изначально построены на основе подписи с меньшим количеством решений анализа протоколов и с ограниченным числом функций обнаружения на основе аномалий, имеющихся в некоторых специализированных продуктах или программных решениях.

ПРИМЕЧАНИЕ Наиболее эффективные развернутые проекты IDS объединяют в себе реализации на основе сети и хоста, но очень мало производителей смогли с успехом предложить оба типа IDS либо IDS, которая объединяла бы в себе множественные технологические подходы. Все заканчивается тем, что программные продукты выполняют все необходимое, но не делают ничего выдающегося. Возможно, ситуация изменится из-за большого числа приобретений в сфере IDS, свидетелями которых мы были в последние годы. Оставшиеся производители или разрабатывают отдельную проблемную область или делают что-то незначительное во всех областях.

Действия IDS при обнаружении попытки атаки на сеть

В большинство современных IDS включены определенные ограниченные возможности автоматического срабатывания, но, как правило, они направлены на автоматическую фильтрацию трафика, блокирование или, как последнее средство, отключение. Несмотря на то, что некоторые системы заявляют о своей способности запуска «противоядия» от атак, практика показывает, что наиболее полезными являются функции автоматической идентификации и отслеживания (при наименьшей вероятности судебного преследования за их использование); поэтому, они, скорее всего, и будут применяться.

Существуют разные мнения и решения с очень гибкой конфигурацией, определяющие, как себя ведет IDS при обнаружении попытки атаки. В этом смысле полезно вкратце обсудить преимущества активного реагирования систем IDS (иногда ошибочно называемых IPS (Intrusion Preventio System, Система предотвращения несанкционированных вторжений)) и сравнить их с более традиционным пассивным обнаружением и предупреждением.

Пассивное реагирование

Традиционно IDS наблюдают за функционированием сети; их можно сконфигурировать на регистрацию в файле и/или отправку предупреждающих сигналов сисадмину (администраторам). Предупреждения могут иметь разные формы: ловушки Простого протокола сетевого управления (Simple Network Management Protocol, SNMP), исходящая электронная почта, сообщения на пейджер или текстовые сообщения сисадмину, даже автоматические телефонные звонки. Большинство администраторов

настраивают IDS по-разному, в зависимости от опасности перехваченной атаки и частоты ее повторения. Понятно, что никому не захочется получать сообщения по пейджеру по 10 раз в час о том, что поначалу может показаться катастрофой, но при внимательном рассмотрении окажется ложным вызовом. При этом важно, чтобы тревожный сигнал предупреждал именно о серьезной дискредитации, особенно если по-настоящему ложные вызовы происходят не очень часто.

Традиционные IDS на этом заканчиваются. Как правило, они настраиваются с интерфейсом управления, абсолютно отделенным от отвода прослушивания, так что они не обнаруживают своего присутствия на отводе постоянной отправкой тревожных сигналов. Очень часто прослушивающий отвод не имеет даже IP-адреса и представляет собой невидимый интерфейс, сконфигурированный так, чтобы не отвечать ни на один трафик.

Активное реагирование

IDS с функцией активного реагирования и IPS моделируют поведение традиционных пассивных IDS в том, что касается обнаружения. Однако при отслеживании попытки атаки активные IDS можно настроить на принятие упреждающих мер защиты, вместо простого предупреждения администратора и ожидания, пока он предпримет соответствующие действия. Такие IDS можно разместить в оперативном режиме для прекращения потенциально опасных трафиков, они могут имитировать обрыв соединения TCP (Transmission Control Protocol) для исходной системы или системы назначения (или для обеих) для резкого прерывания сеанса TCP, через который проходит атакующий трафик, либо отправлять «недоставляемые» сообщения Интернет-протокола управляющих сообщений (Internet Control Message Protocol, ICMP) в исходную систему, чтобы убедить злонамеренный трафик в том, что целевая система недоступна; некоторые меняют конфигурацию брандмауэров или маршрутизаторов между целевой системой и хакерами с целью блокирования трафика. Некоторые системы осуществляют поиск серверов доменных имен или маршрутов слежения в атакующей системе, пытаясь собрать о ней информацию. Некоторые системы даже ответно сканируют порты атакующей системы и предоставляют администратору отчет о ее потенциально слабых местах.

Привлекательность активного реагирования заключается в том, что у сисадмина нет необходимости следить за трафиком в реальном времени. Опасность — в том, что последствия некорректной конфигурации могут быть очень неприятными. Ранее авторам доводилось настраивать абсолютно новую систему IDS с функциями предотвращения только для наблюдения за прослушиванием ею сетевого трафика, за сканированием сервером DNS портов сети и блокированием доступа к ней. Без службы имен многие сетевые приложения останавливаются «с визгом тормозов». Во избежание такого поворота дел, прежде всего IDS необходимо проверить на наличие в ней функций «белого списка». Также рекомендуется справиться о законности и юрисдикции, если в планах стоит автоматическое отслеживание или сканирование «атакующей» системы.

Встроенные (Inline) IDS

В настоящее время много спорят о конфигурации IDS: система должна быть подключена отводом к коммутатору или установлена где-то на линии между пользователем и сетью Интернет. У обеих конфигураций есть свои преимущества и недостатки. Если администратор планирует использовать IDS как IPS, то следует внимательно рассмотреть вариант ее встроенной установки (inline setup). Предотвращение намного более эффективный метод, когда система IDS просто перекрывает трафик, считая, что пропускать его нельзя. Если IDS не встроена в систему, то можно отправлять сообщения ICMP «узел недоступен» или обрыв соединения TCP в исходную систему и систему назначения, но при этом нужно быть уверенным, что поведение этих устройств будет корректным. Сетевой сегмент между ними не контролируется, поэтому ничего больше сделать нельзя. Если IDS встроена, то администратор имеет гораздо больше механизмов управления.

Впрочем, при использовании такого типа конфигурации существуют два «момента озабоченности»: ошибочные решения имеют намного более катастрофические последствия, нежели при работе с обычными IDS, и особенно актуальным становится вопрос производительности. Поскольку весь сетевой график проходит через данный блок, то одна точка сбоя часто доставляет неприятности с точки зрения избыточности и производительности.

Ответы на общие вопросы по IDS

Рассмотрим основные вопросы, возникающие при рассмотрении возможности установки IDS в сеть. Здесь очень важно четко себе представлять функции IDS в рамках общего проекта системы защиты, различия между разными системами IDS и прочими устройствами защиты, а также то, чем IDS может помочь, а чем — нет в плане повышения защиты сети.

Обоснование необходимости систем обнаружения несанкционированных вторжений

IDS обеспечивают внутренний компонент аудита устойчивости проекта и политики защиты. Они извещают администраторов о фактах сканирования их систем и нападения на них. Они предоставляют более подробную информацию, чем можно получить в результате обычных проверок системных журналов серверов и брандмауэров. С помощью IDS можно видеть как несостоявшиеся, так и успешные атаки на систему, а также получать уведомления о попытках атак в режиме реального времени. Администратор может просматривать трафик своей сети, находить области неправильной конфигурации и злонамеренные «поползновения» на сеть раньше, чем без системы IDS. При этом они не «альфа и омега» любой проблемы, связанной с защитой, но очень ценный инструмент в руках опытного администратора по сетевой безопасности.

Почему брандмауэр не может выполнять функции IDS?

Несмотря на то, что производители некоторых интегрированных систем заявляют, что их продукты могут служить как брандмауэрами, так и IDS (вероятно, в будущем подобных систем будет еще больше), функцией брандмауэра является только фильтрация пакетов данных, но никак не предупреждение о появлении злонамеренного трафика. Брандмауэры изначально спроектированы на допуск (или не допуск) трафика в сеть, но не на предупреждение администраторов о «нехорошей» активности в ней. Многие брандмауэры представляют собой фильтры пакетов данных с допуском или отказом в допуске трафикам исключительно на основе исходного IP-адреса, IP-адреса назначения и порта. При этом о сложности анализа трафика (выполняемого IDS) речи не идет. Если никому не приходит в голову считать, что дверные замки должны одновременно выполнять функции камер слежения; почему же тогда замки компьютерной сети (брандмауэры) должны еще работать как упомянутые камеры (IDS)?

Чем я так заинтересовал хакеров?

Да ничем особенным... просто потому, что вы есть. Разумеется, они ищут выгодные цели, но потенциальной целью в Интернет сегодня может стать любая система. Кто-то из злоумышленников пытается добраться до «фрукта, висящего на вершине дерева», кто-то довольствуется тем, что попроще, однако тот факт, что ваша система — «невкусная», не означает, что она в безопасности. В современной среде цифровых технологий вам не хочется быть немного в большей безопасности, чем... вон тот парень; вам хочется быть защищенным по-настоящему. Многие руководители ошибочно полагают, что хакер охотится за корпоративной информацией. В большинстве случаев ему нужен канал доступа, а не какие-то коммерческие тайны.

Автоматическому сканированию/вторжению не важно, кто вы

Многие злоумышленники сканируют (или даже атакуют без сканирования) подсети всего класса В одновременно. Для тех, кто не привык выполнять экспоненциальные вычисления в уме, это 65 536 машин сразу. Многие сценарии вторжения даже не ищут какую-то конкретную машину, им просто нужно как можно больше дискредитированных машин-«зомби». Поэтому, они будут запускать свои автоматизированные устройства сканирования и попытаются воспользоваться всеми машинами, которые кажутся уязвимыми, независимо от того, кем они являются. You@example.com рассматривается так же, как you@whitehouse.gov или you@google.com. Вы будете пользоваться еще большим вниманием со стороны автоматизированных червей и вирусов, которые будут благополучно сканировать произвольные подсети и машины в них, не отдавая себе отчета в том, что за машины установлены в этих сетях и будут ли они сканироваться в будущем.

Так почему же злоумышленников интересует такое большое количество машин, которые могут быть, а могут и не быть им полезными? Им просто нужно все, что можно похитить: каналы доступа, циклы синхронизации CPU или данные.

Нужные ресурсы превращают компьютер в цель

Чем больше различных устройств или программ установлено на компьютере, тем больше шансов, что кто-то попытается ими воспользоваться. Если даже Арчибальд Энд'юзер может стать целью атаки, то что говорить о более мощных компьютерах и корпоративных сетях! Что же, все-таки, хакеры планируют сделать с компьютером?

Канал доступа

Использование злоумышленниками корректно соединенных между собой компьютеров преследует несколько целей. Самая популярная — это запуск распределенных атак отказа в обслуживании (Distributed Denial-of-Servise, DDoS) с использованием канала доступа вашего компьютера для отправки атакующего трафика тем, кто «не понравился» хакерам. Конечно, при этом законное использование компьютера и сети сильно замедлится, но это никого не беспокоит. Каналом также можно пользоваться для рассылки коммерческого спама, для нападений на компьютер с целью автоматического создания рекламных объявлений, например «Виагры» и пластической хирургии, либо для обслуживания пользующихся популярностью (и генерирующих большой трафик) торговых серверов с пиратским программным обеспечением, фильмами, порнопродукцией и музыкой.

Дисковое пространство

Дисковое пространство обычно интересует злоумышленников в плане хостинга торговых серверов для распространения пиратских программных продуктов, кинофильмов, порнографии и музыки. Чем больше дискового пространства имеется на компьютере, тем привлекательнее он будет для взломщиков.

Ценная информация

Если на машине имеется какая-либо секретная информация, то, возможно, за ней и охотятся злоумышленники. Корпоративный шпионаж или продажа информации вполне вероятны, независимо от того, что это: намеренная попытка атаки с целью похищения секретных планов компании по созданию Isengard 2.0 или просто повезло хакеру-одиночке. В качестве примера можно вспомнить скандал с похищением информации по выборам в Конгресс США в 2004 году.

ПРИМЕЧАНИЕ Именно по причине того, что на похищении информации можно нажиться, для любой компании злоумышленники такого рода чаще всего представляют собой угрозу, которая очень хорошо финансируется и обладает профессионально подготовленными специалистами.

Рассматриваемый вопрос: за шесть месяцев до появления вируса Slammer был еще один компьютерный червь, пользовавшийся слабостями сервера SQL Microsoft. Известный как SQL Snake, этот вирус пользовался тем, что многие установки сервера SQL имели пароль сисадмина (SA), заданный по умолчанию, поле которого было пустым. Говорят, что создатели этого червя похитили сотни баз данных и предлагали их для продажи.

Политическая или эмоциональная мотивация

Некоторые злоумышленники руководствуются соображениями накопления политического капитала или чувством мести. Примерами подобной деятельности можно назвать атаки (DDoS), генерируемые разновидностями червя MyDoom в начале 2004 года. Целью тогда были порталы sco.com и Microsoft.com, также часто сообщалось о его появлении на google.com и Berkeley.edu. В сообществе разработчиков средств защиты известно, что серверы Интернет-чата (Internet Relay Chat, IRC) часто являются целями атак DDoS, когда в сети начинается «большой базар» (обмен язвительными или оскорбительными посланиями). Например, все знают о большой нелюбви друг к другу индийских и пакистанских хакеров; в той среде вирусы так и летают от одного к другому вместе с прокламациями, излагающими политические цели или объявляющими превосходство одной национальности над другой. После террористической атаки на США 11 сентября были приняты акты так называемого технического джихада, когда американские хакеры нападали на Интернет-сайты, подозреваемые в связи с Аль Каидой, и наоборот.

Как IDS соответствует общему плану сетевой защиты?

Наряду с тщательно разработанной политикой безопасности, планом реагирования на инциденты, архитектурой брандмауэров, средствами защиты от вирусов и другими особенностями современного плана защиты корпоративных сетей, IDS может сыграть жизненно важную роль в защите предприятия. IDS может стать средством раннего оповещения о проблемах в сети, часто обнаруживающим злонамеренную деятельность «на дальних подходах» к любому из уровней защиты. IDS может генерировать необходимые системные записи и доказательства подрывной деятельности на случай, если по поводу несанкционированного вторжения в сеть придется обращаться в суд. IDS заблаговременно предупреждает сисадминов и персонал, связанный с системной защитой, для того, чтобы были предприняты своевременные меры защиты, а также может стать полезным инструментом приведения в действие ИТ-политики компании и маркировки нарушений. И последней, но ни в коем случае не менее важной функцией является то, что IDS предупреждает администратора о сбоях других средств защиты, обеспечивая своевременное устранение неполадок. Во многих компаниях и организациях на каждую сторону брандмауэров устанавливается сенсор NIDS для отправки высокоприоритетных сигналов тревоги при обнаружении трафика, который не должен проходить через стену защиты.

Где искать несанкционированные вторжения?

Хорошо разработанная политика защиты различными способами учитывает множественные уровни защиты активов предприятия. Эта концепция называется «глубоко эшелонированной защитой» и является центральной при проектировании эффективных средств защиты от многочисленных угроз, с которыми сталкиваются современные предприятия и компании. Если злоумышленники не могут проникнуть за брандмауэр, они могут обратиться в «справочный стол» и обманом «выудить» мандаты учетных записей (аккаунтов). При невозможности физического появления в головном офисе злоумышленники могут отправить вице-президенту электронное сообщение с «лазейкой», замаскированной под поздравительную открытку. Изобретательность хакеров в проникновении в сети ограничивается только их воображением.

К сожалению, это означает, что самым правильным ответом на этот вопрос будет следующий: «Ищите везде!». Впрочем, если говорить серьезно о размещении IDS, то следует принять во внимание все точки, где корпоративная сеть подключается к другим сетям (Интернет, DMZ, модемные пулы, шлюзы VPN и так далее), а также все мало-мальски важные серверы, дискредитация которых может обернуться крупными неприятностями. Более подробная информация об альтернативных хакерских способах проникновения в корпоративные сети содержится в последней книге Кевина Митника «Искусство обмана» («*The Art of Deception*» Kevin Mitnick, Wiley Publishing Inc., 2002, ISBN 0-471-23712-4), где описаны некоторые нетрадиционные методы обхода систем сетевой защиты.

Защита операционной системы — лазейки и трояны

Классическими объектами рассмотрения при планировании сетевой защиты являются Трояны, лазейки (черные ходы), дискредитация отдельных машин, использующая слабые места программного обеспечения или конфигураций. В дополнение к продуманной практике системного администрирования — отключению ненужных служб и наложению программных заплат, следует проводить регулярное сканирование сети или оценку ее уязвимых мест. Это поможет обнаружить неизвестные службы прослушивания или неутвержденную конфигурацию. Необходимо иметь стандартные, задокументированные, проверенные шаблоны конфигурации, чтобы при подключении к сети новой машины она не стала шлюзом, через который в сеть хлынет поток предотвратимых нарушений. При отслеживании таких трафиков IDS может оказать неоценимую помощь.

ПРИМЕЧАНИЕ Пара компаний-производителей (на данный момент, действительно, только две) предложили интересную разработку, которая, якобы, обнаруживает слабые места систем путем пассивного наблюдения за сетевым трафиком. Если это действительно так, то сенсор-IDS получает фактическую возможность выполнения определенного мониторинга и анализа

слабых мест. Одной из самых распространенных жалоб компаний, связанных со сканированием слабых мест, является риск того, что в результате сканирования сервер в сети будет аварийно остановлен либо повысится общая нагрузка. Данный принцип имеет то преимущество, что он никогда не касается серверов и не повышает нагрузку в сети. На время публикации данной книги двумя известными производителями были Tenable Security и Sourcefire.

Физическая безопасность

Применение хороших стратегий защиты — это не просто слежение за подключениями к сети. Физические методы атаки живы и здоровы. Может ли кто-нибудь зайти в ваш офис, взять ноутбук с ценной информацией и выйти незамеченным? Не надо смеха! Такое случается гораздо чаще, чем можно предположить. Недавно подобный случай имел место в одной авиакомпании: два человека в спецовках прошли в офис и вышли с двумя основными компьютерами компании. Можно только предполагать, что они сделали с похищенной информацией, поскольку их не поймали. Значит, наряду с сетевой защитой также следует подумать о разработке модели физической защиты. Где расположены серверы: в отдельном помещении с контролем доступа персонала? Любой специалист по сетевой защите скажет, что физический доступ к устройству крайне опасен. В большинстве случаев, все, что требуется, — перезагрузить машину и настроить BIOS на загрузку с CD-ROM. Существуют достаточно небольшие инструментальные наборы защиты, помещающиеся на CD-ROM размером с визитную карточку, содержащие все инструменты для обнаружения практически любого типа информации о жестких дисках серверов и данных, а также инструменты для внесения произвольных изменений. Такие инструментальные наборы агностичны по отношению к операционной системе; например, загружаемый CD Linux может сбросить пароль администратора для машины с системой Windows. Еще более опасно то, что в последнее время широкое распространение получили носители USB, успешно обходящие защиту методом удаления из компьютера всех дисков и носителей CD-ROM.

Впрочем, физическая защита не ограничивается простым оберегением серверов от непрошенных гостей и злоумышленников. Важными сторонами физической безопасности являются слежение за тем, чтобы кто-нибудь не стащил ноутбук с секретной информацией, обеспечение наличия резервных копий всей важной информации в другом месте на случай неожиданного «пожара» в хранилище основных данных, а также обучение персонала распознаванию попыток применения социотехники и действиям при обнаружении попыток взлома системы защиты.

Инструментальные средства и ловушки...

Инструментальные наборы загрузочных CD

- **FIRE** Дистрибутив Linux на базе CD-ROM со 196 инструментами защиты и анализа на время написания книги (версия 4.0). FIRE спроектирован для проведения с загружаемого CD-ROM оценки слабых мест системы, анализа, сканирования вирусов и реагирования на инциденты вторжений. Чрезвычайно полезный для администратора системной защиты, пакет FIRE также незаменим для людей с неустойчивыми моральными принципами в сценариях оценки физической уязвимости. Все, что можно сделать с помощью этого инструмента, также доступно и для злоумышленника. В активном режиме доступен на http://fire.dmzs.com/.
- **Knoppix** Полнофункциональная среда Linux, включающая графический пользовательский интерфейс (GUI), OpenOffice, Gimp, Abiword и Mozilla. Данный пакет менее полезен для злоумышленника или администратора сетевой защиты, чем FIRE, однако он предлагает функцию просмотра офисных документов на локальной машине непосредственно из собственной операционной системы, их редактирования и выхода без необходимости регистрации или доступа к системе законным путем. Доступен на www.knoppix.net.
- **Linux-BBC** Хорошо известная в сообществе пользователей Linux Загружаемая визитная карточка Linux (Bootable Business Card, BBC) — это дистрибутив Linux на CD-ROM, по форме напоминающий миниатюрную визитную карточку. Достаточно компактный для того, чтобы поместиться в любом бумажнике, Linux-BBC поддерживает высокообъемные диски IDE, BitTorrent и Coroner's Toolkit — пакет программного обеспечения для анализа. Имеется на сайте www.lnx-bbc.org.
- **Offline NT Password & Registry Editor, Bootdisk/CD** Необходимо изменить пароль администратора (или любой другой) в системе Windows? Нет текущего регистрационного имени? Войдите на сайт http://home.eunet.no/~pnordah/bootsidk.html и загрузите этот инструментальный пакет. Менее чем через 10 минут вы сможете изменить пароль, загрузиться в Windows и зарегистрироваться с новым паролем.

Защита программных приложений и целостности данных

Уверены ли вы в том, что ваши данные не подделаны? Уверены ли вы в том, что исходный код в центральном хранилище CVS — тот же самый, что был вчера вечером? Как доказать, что цифры в банковской базе данных — верны и точны, а не подделаны? Доказуемая аутентификация целостности данных является критичной для современной компании, а хорошо мотивированные злоумышленники только и ждут момента, чтобы «запустить лапу» в чужие ресурсы. Со случая несостоявшегося проникновения в дерево исходного кода Linux в ноябре 2003 года до беспроводного взлома сети израильского почтового ведомства, приведшего к похищению 80 000 номеров кредитных карт, становится понятно, почему у злоумышленников есть все основания использовать в качестве жертв программные приложения с неразвитой системой защиты. В отсутствие способа подтверждения того, что данные не изменялись незаконно или что все транзакции надежно защищены, можно нарваться на большие неприятности в случае успешного или даже потенциально успешного несанкционированного проникновения в сеть. Вряд ли заказчики будут удовлетворены ответом: «Не знаю» на вопрос о целостности и неприкосновенности данных.

Сопоставление информации всех источников

Стоит отметить, что сопоставление информации о защите, полученной из многих источников, наилучшим образом поможет реконструировать прошедшие события при анализе попыток несанкционированного вторжения. Данные брандмауэров и маршрутизаторов могут содержать резервные копии тревожных сигналов, зарегистрированных IDS. Пересекающиеся источники могут поддерживать друг друга в случае отказа одной из систем; при наличии же возможности сопоставлять предупреждающие сигналы из множества источников можно быть в большей степени уверенным в том, что не приходится иметь дело с ошибочными показаниями. Системные записи фактов считывания карточки-ключа помогают определить того (или, по крайней мере, мандаты доступа этого лица), кто был в конкретном месте в конкретное время, мандаты сетевого доступа помогают определить зарегистрированных в системе лиц, а камеры защиты подскажут, действительно ли человек, сидевший за клавиатурой был тем лицом, чей пароль занесен в системный журнал.

В чем заключается помощь IDS?

IDS может быть весьма ценным дополнением к существующей системе сетевой защиты. Система обнаружения несанкционированного вторжения предлагает беспрецедентную возможность наблюдения за тем, что в действительности происходит в сети, и предупредить о новых проблемах или о попытках атак до того, как они будут иметь место. IDS помогает в мониторинге и приведении в действие корпоративной политики безопасности, в получении более прозрачной картины тенденций использования системы и сети, а также в планировании будущего бюджета и закупок путем определения «мертвых зон» и существующих проблем. IDS уведомляет администраторов

о вероятной дискредитации системы и даже о неудавшихся попытках несанкционированного вторжения. При этом система никогда не устает, ей не нужны перерывы, чтобы выпить кофе, и она никогда не требует прибавки к жалованью, когда вы срываетесь на крик...

Необходимость непрерывного мониторинга и анализа пакетов данных сети

Еще предстоит поискать сисадмина или инженера по сетевой безопасности, способных на решение этой задачи более, чем за пять минут, и то на сравнительно медленной сети, и считывая шестнадцатеричные, а не двоичные коды. IDS вполне способна на неустанное сличение одного пакета данных за другим по их известным сигнатурам и на сравнение полезной нагрузки без необходимости их перевода в формат, понятный человеку. Как правило, системы работают на несколько порядков быстрее, чем человек, выполняющий ту же самую работу, и вероятность допуска ошибки машиной намного ниже.

Ежедневное считывание сотен мегабайтов системных журналов и поиск специфических аспектов

IDS может в значительной степени ускорить обработку количества системных журналов, которое живой человек способен проанализировать за один день. Когда администратор несет ответственность за защиту и безопасность обширной рабочей среды, то объем накапливающихся системных журналов поражает (в случае с большой группой систем и активной высокоскоростной сетью речь идет о терабайтах данных). Сортировка их вручную превращается в неразрешимую проблему, особенно при расширении сети. IDS с возможностью структурного анализа системных журналов обеспечивают осмысленный способ поиска нужных аспектов и подписей в системных журналах, в результате чего проявляется четкая картина происходящего со всеми сетевыми устройствами.

Создание как можно большего объема данных, независимо от их настройки

Даже максимально тщательно настроенная IDS будет иметь на выходе колоссальное количество данных. Аномальные события в сетях и системах происходят постоянно. Пользователи становятся привилегированными. Команды отправляются по web-интерфейсам. Изменяются пароли администраторов, передаются пакеты с некорректными комбинациями флажков TCP, программные приложения эксплуатируют протоколы с такими нарушениями установленных режимов, до которых могут додуматься только крайне извращенные умы, и автоматизированные компьютерные черви и вирусы продолжают свои слепые поиски возможностей самораспространения. Каждое из этих событий может стать причиной предупреждающего сигнала IDS, а когда в день их поступают тысячи, то обработка их всех может стать поистине неразрешимой проблемой.

Очень часто администраторы IDS сталкиваются с ежедневной перспективой сортировки нескольких тысяч (или нескольких сотен тысяч) сигналов тревоги, многие из которых не представляют никакой опасности, но попросту не настроены должным образом. Некоторые настроить сложно исключительно из-за их происхождения: многие операционные системы и приложения отправляют пакеты данных, которых быть не должно в принципе! Однако нельзя же постоянно тратить время на настройку каждой отдельно взятой системы в Интернет, которая работает на одной из указанных операционных систем, а также отправлять подпись в мусорную корзину исключительно из боязни фактических невидимых сканирований портов, которые могут быть разведкой сети. Принимая решение об установке IDS, следует быть готовым к ситуациям, подобным только что описанной. Независимо от качества настройки, данные будут поступать, и в очень больших объемах. Часть их, несомненно, будет ошибочной. Продуманное составление правил и сопоставление данных может уменьшить вероятность появления ошибочных результатов и даже число положительных результатов, требующих индивидуального рассмотрения, но данных все равно будет очень много.

Создание настолько большого объема данных, что недостаток их настройки равносилен их отсутствию

Иногда компания, «не считая», вкладывает безумные деньги в приобретение новейших, самых современных IDS, после чего нанимает для их мониторинга и администрирования человека, не имеющего даже базового представления о вопросах системной защиты и безопасности. Неквалифицированный администратор ничего не смыслит в настройке IDS и еще меньше понятия имеет о том, как обрабатывать вал тревожных сигналов, поступающих практически непрерывно. «Проницательный» шеф при подобном положении дел решит, что все IDS бесполезны. Все-таки, деньги заплачены за самые лучшие системы, так?

Выделение ошибочных результатов из IDS — критичная задача. Очень важно привлекать знающих и высокопрофессиональных администраторов к проектированию и размещению сенсоров с последующей настройкой набора правил. Если администратор знает собственную сеть не достаточно хорошо для того, чтобы отслеживать и отделять корректные действия от ошибочных, то очень скоро он будет погребен под шквалом фактов сканирования портов и информационных предупреждающих сигналов без надежды на обработку полученных данных с целью обнаружения сравнительно небольшого количества откровенных вторжений и/или незначительных моментов дискредитации системы. Каждая новая IDS будет генерировать огромные объемы ошибочных результатов, а не очень квалифицированный специалист по системной защите может не получить ни одного.

Выявление мелких тенденций в больших объемах данных, которые можно не заметить

Одним из преимуществ наличия массивной базы данных является возможность выявления тенденций в сигналах тревоги или в потоке пакетов. Сегодня фактов сканирования необычного порта было больше чем вчера? Просматривается ли с некоторого времени устойчивый рост их числа? Не исключено, что на данный порт нацелено какое-либо новое инструментальное средство или программа-«эксплоит». Не увеличилось ли количество фактов неудачной регистрации в серверах сети? Может быть, кто-то пытается подобрать (вычислить) пароль? Возможность увидеть общую картину в огромном количестве данных обеспечивают IDS, особенно имеющие функции сопоставления.

Внедрение других механизмов защиты

IDS может служить подтверждением или резервной поддержкой других систем сетевой защиты. Это восходит к принципу «защиты в глубину». Если обнаружен трафик, нацеленный на web-агент, но администратор не уверен, что программа-агент «очистит» этот трафик перед передачей его конечному пользователю, следует проверить информацию IDS. Проверьте наличие сигналов тревоги до прохождения трафиком программы-агента и после нее. Если известно, что некто с доступом администратора использовал вчера удаленное подключение Remote Desktop для подключения к серверу Exchange непосредственно перед тем, как он вышел из строя, обратитесь к системным журналам IDS, в которых зафиксировано лицо, осуществлявшее доступ к серверу, местоположение доступа, а также тип отправленного трафика (при наличии HIDS и NIDS). Отсутствие сигнала тревоги с IDS не должно рассматриваться как доказательство того, что все в порядке. Как уже отмечалось, ISD не отслеживает каждую атаку. Даже при наличии сигнатуры атаки достаточно интенсивный трафик вынудит IDS на сброс пакетов данных. Однако наличие сигнала тревоги можно использовать как резерв для поддержки других систем сетевой защиты и системных журналов.

Мыслящая система — множитель результатов усилий или просто системный администратор?

С помощью IDS квалифицированные специалисты по системной защите имеют возможность обрабатывать намного большее количество системных журналов и сетевых данных, чем в отсутствие IDS. Хотя системы обнаружения несанкционированных вторжений не заменят помощи «разумного» администратора по системной защите, они повысят эффективность его работы. При рассмотрении той или иной попытки вторжения в сеть обычно стоит задать вопросы: «А какие еще предупреждающие сигналы может породить этот исходный IP или пользователь?», «Какие еще сигналы имели отношение к этому IP назначения?». Оперативный автоматический

доступ к прочим необходимым данным намного быстрее поможет администраторам понять тип и масштаб рассматриваемого вопроса, чем если бы они анализировали и искали нужные системные журналы вручную.

ПРИМЕЧАНИЕ Что такое Множитель усилий (Force Multiplier)? Это — нечто, что повышает полезную «отдачу» на каждую единицу вложенных сил. Примеры имеются в любой книге по машиностроению (вполне подойдет «Как оно работает?» (*The Way Things Work*)).

Уведомления о возможных атаках

В большинстве IDS существует масса путей уведомления сисадминов о возможных атаках. Сэкономленное время может стать ценным «капиталом» для группы реагирования на инциденты. Оно имеет значение для вывода одной дискредитированной системы из сети до того, как она успеет распространить «заразу» по другим системам, либо при обработке массивной «бреши» защиты на уровне целого предприятия, требующей очень больших затрат как труда, так и времени.

В чем бессильны IDS?

Системы IDS не являются панацеей для лечения всех проблем безопасности. Они не заменят сисадмина, не заставят уйти с IRC «того парня», которому не понравились вы, не ответят на электронное письмо, на которое отвечать не хочется. Они не обезопасят физического периметра сайта, не будут каким-то волшебным образом отслеживать каждый потенциально «зараженный» бит в сети или сообщать о том, что один из сотрудников имеет намерение «сдать» корпоративные секреты конкурентам. Для использования IDS «по максимуму» важно осознавать границы их возможностей, в соответствии с чем и должна строиться политика системной защиты.

Замена профессионалов по сетевой защите

Даже самые лучшие системы IDS хороши на уровне их программирования. Они подскажут, что нужно делать, если правильно сформулировать «заказ», они подадут сигнал тревоги так, как это запрограммировано и, если это IPS, то она будет реагировать так, как этого хочет пользователь. Но они не «ориентируются» в новых ситуациях. Они не пишут собственных сигнатур для новых попыток атак и не могут соперничать с проницательным, гибким и адаптивным злоумышленником, выбравшим способ нападения, выходящий за рамки спецификаций системы обнаружения. IDS не может определить политику защиты. Она не может давать информационные рекомендации для сети, исходя из последних промышленных разработок. Одним словом, ни одна система не заменит способного и профессионального специалиста по сетевой защите.

Необходимость перехвата любой атаки

Новые виды сетевых атак разрабатываются постоянно. Даже во время написания этого текста, даже во время его чтения злоумышленники разрабатывают новые способы проникновения в системы. Иногда возникают новые способы использования уже известных слабых мест, а порой — совершенно новые. IDS не может быть настроена на обработку всех возможных атак просто потому, что все еще не изобретены. Защититься можно только от того, что известно, и даже от известных атак защищают не все IDS. Они всего лишь отслеживают потенциальные попытки проникновения в сети, но не предотвращают их всех.

Взломы и защита от них

fragroute и документ Newsham/Ptacek

В 1998 году Тим Ньюшэм (Tim Newsham) и Том Птацек (Tom Ptacek) составили документ под названием «Вставка, уклонение и отказ от оказания услуг: как избежать обнаружения проникновения в сеть», в котором описываются способы уклонения от обнаружения проникновения, применяемые в большинстве имеющихся на тот момент IDS (www.insecure.org/stf/secnet_ids/secnet_ids.pdf). В число рассматриваемых методик входило тестирование времени простоя на IDS, проверка компоновки фрагментированных пакетов (с перезаписью одних и тех же данных с разным содержимым), моделирование задержек и потерь пакетов в сетевых программах, а также задание IP-параметров случайным образом с целью противоборства снятию «отпечатков» с системы. Многим специалистам по обнаружению несанкционированных проникновений в сеть это прибавило работы, но это было ничто по сравнению с шумом, поднятым в связи с выпуском Dug Song программ fragrouter, реализующих большую часть из упомянутых атак (www.monkey.org/~dugsong/fragroute/). Теория превратилась в реальность. Многие из этих атак обнаруживаются Snort, начиная с версии 1.9, однако по-прежнему многие IDS их пропускают, а некоторые просто не поддаются обработке с сетевой точки зрения. В настоящее время существует один подход, привлекающий к себе особое внимание, это — IDS на основе целевой системы, объединяющие знание сети, операционных систем и конфигурации с обнаружением атак «вживую». Целью IDS на базе целевых систем является представление администратору более «сфокусированных» сигналов тревоги, что намного сокращает количество ложных сигналов и делает упор на анализ наиболее вероятных реальных атак. Более подробная информация о IDS на основе целевых систем имеется в Information Security Magazine (http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss306_art540,00.html; общие обзоры IDS на основе целевых систем демонстрировались на обложках журнала в январе 2004 года.

Предотвращение атак

Никакая система IDS не защитит систему от попыток атаковать ее злоумышленниками. Средства защиты могут свести на нет эти попытки, однако это не остановит хакеров от стремления «пробить виртуальную стену». Независимо от качества IDS они не смогут изменить человеческую натуру или стремление зловредных хакеров завладеть сетевой информацией.

При выборе и установке IDS важно учитывать, что с ее помощью можно будет отслеживать, а чего — нельзя. Если трафик зашифрован, то IP-заголовки и заголовки протокола транспортного слоя будут по-прежнему видны, но декодировать содержимое пакета будет нельзя без взлома шифра. Можно отслеживать объем отправляемого трафика, от кого — кому и как часто, однако понять, что именно отправлено — невозможно. Тип развернутого NIDS ограничивает стиль реакции. IDS на базе подписей, зависящие от отправляемого открытым текстом трафика, могут не подавать сигналов тревоги, если этот трафик зашифрован. Анализ протоколов может срабатывать для зашифрованного трафика, но может выйти из строя, если трафик отправлен на неожиданный порт. При декодировании анализ модели трафика может оказаться наилучшим средством.

ПРИМЕЧАНИЕ Очевидно, что NIDS не сможет просматривать сетевой трафик, если он зашифрован (при отсутствии специальных инструментальных средств и изменении схемы кодирования). Не так очевидно то, что даже большинство просматривающих сетевой трафик HIDS (также называемых IDS сетевых узлов или NNIDS), не смогут просматривать зашифрованный трафик. Причиной этого является то, что почти все HIDS просматривают сетевой трафик по мере его вхождения в систему или выхождения из нее в области Уровня 2 на сетевом стеке (непосредственно перед тем, как трафик поступает на аппаратное обеспечение из операционной системы). В настоящее время большая часть кодирования осуществляется на уровне приложения (Уровень 7) такими программными приложениями, как Web-браузер или SSH. Это означает, что трафик по-прежнему остается зашифрованным, в то время, когда IDS отслеживает его вхождение в систему или выхождение из нее. К сожалению, это то, о чем производители забывают сообщить, говоря о преимуществах их программных продуктов.
Все это постепенно превращается в проблему, по мере увеличения числа рабочих сред (и сетевых связей), использующих шифрование. Хорошо, что поставщики IDS осведомлены об этих проблемах и работают над их решением. Надеемся, что решения будут качественными.

Предотвращение автоматического прохождения сетевых атак (в большинстве случаев)

За исключением некоторых IPS, в большинстве случаев, когда IDS обнаруживает попытку сетевой атаки, она уже состоялась. Например, в случае с электронным сообщением, в котором передается вирус, возможно, что IPS «включится» на строке «Тема» и успеет запустить режим «сброс-отмена» и завершить передачу всего «зараженного» сообщения до его прохода в систему. Впрочем, во многих других случаях атака и успех срабатывания программы-«эксплоита» идут непосредственно друг за другом, и IDS или IPS попросту не успевают отправить команду отмены последней операции до исполнения shell-кода.

Замена прочих механизмов защиты

Несмотря на обилие комплексных программных продуктов сетевой защиты, не стоит думать, что один продукт защиты будет выполнять работу другого. Наличие в системе IDS не означает, что о брандмауэре можно забыть. Наличие VPN также не означает, что на системы не нужно накладывать исправления. Процесс сетевой защиты дополняется резервированием и уровнями повышенной защиты. Сама по себе система IDS — не единственное устройство безопасности, которое потребуется.

Дополнительные преимущества обнаружения несанкционированных вторжений

Выше перечислены только некоторые возможные способы использования IDS. Многие HIDS позволяют осуществлять аудит и мониторинг коллективно используемых ресурсов. Они обеспечивают расширенные возможности определения того, кто работает с сетевыми ресурсами коллективного пользования, разметку и статистику использования ресурсов для мониторинга функций сервера, а также могут сопоставлять строки «Тема» или содержание электронного сообщения для оповещения и/или сброса почтовых сообщений с заведомо злонамеренным содержанием. Возможностей очень много, и они настолько же гибкие, как и набор установленных правил и реализация IDS.

Ввод Snort в архитектуру сетевой защиты

Поскольку читатель держит в руках эту книгу, авторы предполагают, что он заинтересован в установке в свою в сеть пакета Snort. Это очень гибкая IDS, предлагающая множество авторских правил и возможность написания каждым администратором своих собственных. Существует несколько списков рассылки, в которые вносятся новые правила Snort, написанные в ответ на самые последние атаки, а также коммен-

тарии к правилам и новые комментарии к правилам вместе с новыми попытками проникновения, которые пользователи обнаруживают в сети. Snort обладает полным набором функций с множеством предварительных процессоров для обработки разных типов данных, комплексом паролей, позволяющих сопоставлять содержимое, порт, протокол и т. д., функцией обнаружения сканирования портов, длиной буфера и другими функциями; поскольку пакет — открытый, добавлять можно любую функциональность. Также существует множество приставок для поддержки сигналов тревоги при регистрации в форматах баз данных, программ управления и автоматической загрузки новых правил, функция распределения правил по сенсорам без затирания наборов локальных правил, web-интерфейс для управления сенсором Snort и много другого. Рассмотрим вкратце полезные функции Snort в производственной компьютерной сети.

Вирусы, черви и Snort

В течение дней, а то и часов с момента выпуска нового компьютерного червя для него пишутся сигнатуры Snort. Часто они интегрируются в основной набор правил Snort так, что все пользователи Snort могут пользоваться их преимуществами. Подписи для SQL Slammer появились в списке рассылки NANOG в течение несколько часов после первого обнаружения этого червя (www.merit.edu/mail.archives/nanog/2003-01/msg00775.html). Подписи для червя MyDoom.A были выпущены в течение одного дня после его обнаружения лабораториями по созданию антивирусных программ. Такой тип активности дает пользователям Snort возможность обновлять наборы правил при появлении новой атаки и начать скорейшее обнаружение и исправление слабых мест. Фактически, при использовании каких-либо приставок, имеющихся для Snort, можно обнаруживать признаки распространения компьютерных червей до того, как для них будут доступны подписи.

Известные инструменты сетевого нападения и Snort

Многие подписи Snort специально созданы для того, чтобы сообщать администратору об использовании известного инструмента сетевого нападения. Некоторые из этих инструментов сами проявляются в полезной нагрузке пакетов, например, такие как SolarWinds ICMP и сканер SNMP. Ниже приведена подпись Snort (www.snort.org|snort-db/sid.html?sid=1918):

```
alert icmp $EXTERNAL_NET any - > $HOME_NET any (msg: "SCAN SolarWinds IP scan
attempt"; content: "SolarWinds.Net"; itype:8; icode:0 classtype:networkscan;
sid:1918; rev:3;)
```

Отметьте содержимое «SolarWinds.Net» в эхо-пакете ICMP. В этом случае оно является «отпечатком» данного инструмента. Однако не все известные инструменты нападения на сети проявляют сами себя. Рассмотрим следующую подпись для клиента

атаки Trin00, который пытается подключиться к главному серверу Trin00 на порту по умолчанию с паролем по умолчанию:

```
alert tcp $EXTERNAL_NET any _> $HOME_NET 27665 (msg: "DDOS Trin00 Attacker to
Master default startup password"; flow:established, to_server; content:
"betaalmostdone"; reference:arachnids,197; classtype:attempted-dos; sid233;
rev:3;)
```

Несмотря на то, что многие подписи Snort написаны максимально обобщенно для обнаружения атаки, независимо от того, какой инструмент используется для ее генерирования, авторы правил также сразу напишут правило для конкретного инструмента, если он явно себя проявляет.

Написание авторских подписей с помощью Snort

Теперь становится очевидно, что одной из наиболее сильных сторон Snort является способность пакета к написанию сетевых правил под каждую конкретную сеть и для каждого наблюдаемого трафика. Синтаксис здесь — очень точный и гибкий, что позволяет сопоставлять все виды различных сетевых трафиков. Дополнительная информация имеется на сайте www.snort.org/.

Использование IDS для мониторинга корпоративной политики

Специальные правила Snort обычно используются для наблюдения за трафиком, который, не будучи активно зловредным, ограничен корпоративной политикой либо его прохождение по сети настоятельно не рекомендуется ею. В некоторых компаниях составляются правила для подачи сигналов тревоги при доступе пользователей к web-страницам с содержимым, сличающим конкретные пароли, либо к сайтам с нелицензионным программным обеспечением или при других нарушениях корпоративной политики. В частности, в Snort имеется набор правил для трафиков, которые предположительно являются порнографическими. Можно написать собственные правила Snort для сличения любого типа сетевого трафика, например для обнаружения закрытия каким-либо пользователем сетевого сервера и запуска сервера Quake.

Определение аспектов проектирования и конфигурирования IDS

Определив тип (типы) IDS и места их установки в сети, администратор должен обратить особое внимание на возможности усовершенствования проекта. Существует ли вероятность того, что ложных сигналов тревоги будет слишком много либо будут пропущены полезные сигналы? Может ли реальная атака «проскользнуть» сквозь сплошной поток ошибочных сигналов?

Ложные и полезные сигналы тревоги

При определении политики IDS можно предполагать наличие очень большого количества ложных сигналов тревоги, по крайней мере до настройки IDS на сокращение их числа до управляемого потока. В этом смысле большую важность имеет возможность появления полезных сигналов об атаках, которые IDS пропускает. Существует опасность ложного чувства защищенности: ежедневное получение большого числа сигналов тревоги создает ощущение того, что, система отслеживает их все. Впрочем, профессиональные хакеры могут сканировать и писать коды инструментов нападения, обнаружить которые будет практически невозможно. Для этого существует достаточно много разных методов, которые вкратце будут рассмотрены.

«Обман» IDS

В упоминавшемся выше документе Птацека и Ньюшэма описано множество отдельных способов «одурачивания» NIDS, но, в принципе, основных подходов — два. Первый — это передача настолько больших объемов данных, что система может упустить часть пакетов, либо подача такого большого числа сигналов тревоги, что администратор никогда не обнаружит настоящего нападения на его сеть. Другой общий подход заключается в том, что атака структурируется так, что она не соответствует подписям или алгоритмам, используемым IDS для выделения фактов нападений из общего сетевого шума. Такие инструменты, как Stick и Snot, а также сканирование ложных трафиков от Nmap, основаны на первом подходе. Второй подход — это невидимое сканирование Nmap и такие инструменты, как fragrouter от Dug Song или Rain Forest Puppy's Whiskeruse.

Методы обхода IDS

Сначала рассмотрим так называемый шумовой метод. Stick и Snot (см. врезку) — инструментальные средства, предназначенные для генерирования как можно большего количества тревожных сигналов на IDS. Это делается путем генерирования сигналов тревоги из набора правил, сходного с набором правил, используемого IDS для сличения трафика. Некоторые злоумышленники надеются проникнуть в сеть по атакующему трафику в то время, как администратор отвлекается на отслеживание полезных сигналов тревоги, либо во время сброса пакетов IDS. Другим просто нравится сама идея уничтожения IDS.

Если для сокрытия своих каналов злоумышленник использовал Stick или Snot, после чего запустил атаку на TCP, тогда ее можно легко предотвратить подачей сигналов тревоги Snort на установленных сеансах TCP. Однако для злоумышленника появится идеальная возможность для запуска атаки на базе UDP — Удаленного вызова процедуры (Remote Procedure Call, RPC), DNS или что-нибудь в этом роде.

Для максимальной невидимости злоумышленник может даже сымитировать источник; в беспроводных UDP (пользовательский протокол данных) это не срабатывает. Существует определенная вероятность того, что атакующие пакеты будут сброшены, если сетевые каналы переполнены выходными данными Stick/Snot, однако при этом атакующие пакеты не будут отслежены IDS либо потому, что система отслеживает только установленные сеансы TCP, а атака — UDP или ICMP, либо потому, что IDS отслеживает все подключения, но переполнена ложными сигналами тревоги.

Мысли вслух...

Stick, Snot и Snort

Stick, Snot и Snort — инструментальные средства, позиционируемые как «Подавители IDS», спроектированные на перегрузку IDS до тех пор, пока систему слежения попросту нельзя будет использовать.

- **Stick** (www.eurocompton.net/stick/projects8.html) — это программа языка C на базе старой версии набора правил Snort, предназначенная для распространения такого большого количества пакетов, активизирующих сигналы тревоги в секунду, что в работе IDS происходит серьезный сбой. Для своего времени программа была чрезвычайно эффективной, однако теперь Snort обладает «противоядием» для компенсирования данного типа атак.
- **Snot** — сходный с предыдущим инструмент (www.stolenshoes.net/sniph/index.html), принимающий наборы правил Snort в качестве аргумента и генерирующий серию пакетов, запускающих данный набор правил. Будучи достаточно гибким продуктом, работающим на многих платформах, Snot способен распространять поддельные сценарии по всем мировым компьютерным сетям, заметно прибавляя работы администраторам IDS.

Если установка Snort подверглась нападению этих или аналогичных программных инструментов, то ограничить количество тревожных сигналов Snort можно путем пометки установленных сеансов TCP только аргументами *snort –z est*. Однако, чтобы этот способ сработал, для начала необходимо сконфигурировать предварительный процессор stream4. Также следует помнить, что при этом не будут видны все прочие не меняющие своего состояния тревожные сигналы TCP: UDP, ICMP и атаки на базе ARP. Однако при этом работа IDS не прекращается.

Nmap обеспечивает шумовое сканирование, генерирующее целую связку поддельных пакетов в качестве альтернативных «источников» с помощью опции –D «при-

манка». Для целевой системы это выглядит так, словно все эти пакеты сканируются всеми машинами-«приманками» сразу, а реальное сканирование замаскировано среди поддельных.

Теперь рассмотрим бесшумный способ. Существуют злоумышленники, которых следует опасаться всерьез. При описании документа Ньюшэма-Птацека авторы уже рассматривали способы обхода fragroute и Dug Song, однако Nmap также обладает опциями, позволяющими оставаться невидимым. Имеют место свободное сканирование, атака рикошета FTP, временные атаки, например очень медленное сканирование, растягивающееся на многие дни, атаки на основе фрагментации и перекомпоновки, атаки комбинации флажков TCP и даже сканирование ничего не подозревающих зомби-хостов. Подробности о компоновке пакетов при появлении всех этих атак доступны на странице оперативных руководств Nmap www.insecure.org/nmap/data/nmap_manpage.html.

Прибыль на инвестиции: стоит ли игра свеч?

И самым последним определяющим фактором для многих компаний является ожидаемый возврат прибыли на инвестиции. Действительно ли установка, конфигурирование и техническое обслуживание IDS помогут в достаточной степени укрепить сетевую защиту предприятия? Защита и безопасность часто рассматриваются как финансовая «яма»: компании тратят на нее деньги, но не видят отдачи, если не происходит никаких инцидентов. Однако прибыль выражается не в произведенной продукции, а в экономии затрат. По этой причине, многие руководители высшего звена весьма неохотно тратят средства на дорогостоящие системы или решения, особенно если на IDS уже были произведены затраты, но число обнаруженных попыток несанкционированного проникновения в сеть намного меньше ложных тревожных сигналов.

При обсуждении вариантов установки в сеть IDS их следует рассматривать как бизнес-задачу. Каковы будут потери компании, если корпоративная сеть будет «взломана»? Каков будет перевес в пользу вторжения? В какую сумму обойдется установка и обслуживание IDS? Насколько IDS отодвинет или снизит риск вторжения? Каково юридическое воздействие IDS на компанию. Выше в данном приложении уже рассматривались последствия влияния законов о прослушивании и нарушении конфиденциальности при использовании компанией IDS. Однако система поможет в соблюдении законов корпоративной отчетности, например требований Сарбанеза-Оксли (Sarbanes-Oxley requirements), а также при установлении контрольных следов в случае дискредитации. В разделах 302 и 304 требований Сарбанеза-Оксли ответственность за организацию внутреннего управления сетью возлагается на корпорацию. Любая IDS с возможностью демонстрации может стать частью этой структуры управления. При объединении испытания на проникнове-

ние третьих производителей обоснование (и подтверждение действительности) данных в отношении внешнего аудита с отслеживанием может занять достаточно много времени. В некоторых регионах, например в штате Калифорния, на сегодняшний день от компаний требуется уведомление клиентов о случаях дискредитации их данных. Наличие IDS дает возможность более надежного выявления попыток проникновения в сети. Появление в офисе генерального директора с точным цифрами, юридическими подтверждениями будет гораздо более впечатляющим прецедентом, чем простое замечание о том, что, дескать, «а не пора ли нам тоже установить то-то и то-то, потому что у всех это уже есть...»

Терминология IDS

Понимание различий между типами IDS и работы их функций — принципиально при попытках проектирования архитектуры безопасности. Рассмотрим некоторые из наиболее распространенных терминов в области IDS и убедимся, что все опции доступны.

Системы предотвращения незаконного проникновения (HIPS и NIPS)

Система IDS, которая не только обнаруживает возможные атаки, но и реагирует на них, предотвращая успешность попыток. Таким реагированием может быть все, что угодно: от составления особых правил для брандмауэра до полного уничтожения системы злоумышленника, от уничтожения злонамеренного процесса (при работе с Системой обработки информации (IPS) хоста) до сброса атакующего трафика (при работе с сетевыми IPS).

IDS-шлюз

IDS, расположенная в «узком месте» между сетью и Интернет (или любым равноправным входным потоком, к которому осуществлено подключение), также известная как «inline-IDS», для того, чтобы выйти из локальной сети, весь трафик целиком должен пройти через данный шлюз. IDS-шлюз может работать как IPS при наличии функции принятия решений о том, стоит ли допускать этот трафик в сеть вообще.

IDS главного узла

Метод выявления несанкционированного проникновения в сеть, если устанавливается базовая линия для «нормального сетевого трафика, после чего осуществляется поиск отклонений от заданной нормы, которые отмечаются (маркируются) как возможный атакующий трафик.

Анализ протоколов

Метод выявления несанкционированного проникновения в сеть, если просмотр потока данных осуществляется в рамках спецификаций каждого протокола с поиском аномалий и возможных опасных трафиков на основе ожидаемого поведения протокола.

IDS на базе целевой системы

Новая разновидность IDS, нацеленная специально на то, что находится в сети. Спроектированы на получение меньшего количества ложных тревожных сигналов, а в основном на получение сигналов об атаках, имеющих реальное отношение к сети, а также к выполняющимся на ней специализированным службам.

Резюме

IDS служат множеству целей при работе в архитектурах, спроектированных на «глубоко эшелонированную защиту». Помимо идентификации несанкционированных проникновений (атак) в сеть и любой подозрительной деятельности, данные IDS можно использовать для выявления уязвимых и слабых мест сетевой защиты.

IDS могут осуществлять аудит и стимулировать соблюдение корпоративной политики. Например, если последняя запрещает использование таких программных приложений коллективного использования, как Kazaa, Gnutella, либо таких служб передачи электронных сообщений, как IRC (Интернет-чат) или Instant Messenger, то IDS можно сконфигурировать на обнаружение и оповещение о подобных нарушениях корпоративной политики.

IDS представляют собой ценный источник свидетельских показаний. Системные записи IDS могут стать важной частью доказательств при судебных разбирательствах и преследованиях, а также при попытках обработки инцидентов. Системы обнаружения используются для выявления атак внутри компании путем мониторинга трафика от «троянских коней» или опасного кода, а также могут применяться как инструментальные средства обработки инцидентов при отслеживании атак.

Сопоставление данных (с HIDS, NIDS или DIDS) — возможно, лучший способ подхода к обнаружению данных незаконного проникновения. Несмотря на то, что IDS могут превратиться в ценного помощника в организации безопасности архитектуры, сами по себе, «в одиночку» эти системы ни в коем случае не могут полностью обезопасить и защитить компьютерную сеть.

NIDS можно использовать для фиксирования и корреляции злонамеренной сетевой деятельности. NIDS невидимы, и их можно реализовать для пассивного мониторинга либо сконфигурировать на реагирование на несанкционированные проник-

новения. HIDS играют жизненно важную роль при организации «защиты в глубину»; они представляют собой последний оплот защиты при атаках. Если хакер проходит все предварительные уровни защиты, то HIDS может стать единственным устройством, предотвращающим полную дискредитацию системы. HIDS установлены на хост-машине и несут ответственность за просмотр пакетов данных, поступающих на этот хост и исходящих из него. На уровне хоста HIDS имеет возможность осуществления мониторинга зашифрованного трафика, а также полезен при сопоставлении атак, обнаруженных другими сетевыми сенсорами. Используемая таким образом, HIDS может определить успешность атаки. Системные записи превращаются в основной и чрезвычайно важный ресурс реконструкции процесса атаки или определения серьезности инцидента несанкционированного проникновения.

Краткое резюме по разделам

Введение в системы обнаружения несанкционированного вторжения в сеть

- ☑ Вторжением называется несанкционированный доступ, использование или атаки на сеть или компьютеры.
- ☑ IDS работают по принципу наблюдения за деятельностью, происходящей в сети или системе, с последующим сравнением их с известными сигнатурами или алгоритмами для отделения законной деятельности от подозрительной.
- ☑ IDS регистрируют факты несанкционированного проникновения в системном журнале и реагируют на них различными способами. Самым распространенным является подача сисадминам сигналов тревоги через ловушки SNMP, в виде текстовых сообщений, телефонных звонков или по пейджеру.

Ответы на общие вопросы по IDS

- ☑ Злоумышленники заинтересованы в любом пользователе, подключенном к Интернет; это совсем необязательно связано с личной неприязнью.
- ☑ IDS может поставить сисадмина в известность о сетевом трафике и системной деятельности, о которой он может не иметь представления. IDS повышает эффективность работы высокопрофессионального сисадмина, обеспечивая его дополнительными данными.
- ☑ IDS не заменит живого персонала по безопасности и не остановит хакеров от желания «взломать» сеть.

Ввод Snort в архитектуру сетевой защиты

- ☑ Snort — сетевая IDS со сложными функциями сопоставления моделей, используемая для индивидуального описания атакующего трафика.
- ☑ Как правило, подписи Snort для самых современных вирусов, компьютерных червей и других новых уязвимых мест создаются в течение нескольких часов или дней с момента первого случая той или иной атаки на сеть.
- ☑ Для отслеживания нарушений корпоративной политики, какого-либо уникального трафика и т. д. в Snort можно создавать авторские подписи.

Определение аспектов проектирования и конфигурирования IDS

- ☑ IDS можно сконфигурировать на обнаружение, предупреждение атак, а также на реагирование.
- ☑ В число возможной реакции входят сброс трафика, имитация ICMP или пакеты сброса TCP либо идентификация и обратное отслеживание в сторону источника атаки.
- ☑ IDS не являются системами абсолютной защиты или «защиты от дурака»; их можно «обойти» или «обмануть». Они являются ценными помощниками поддержания и соблюдения политики сетевой защиты, но только их для системы недостаточно.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма «**Ask the Author**»). Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: Почему мой брандмауэр не работает как IDS?

О: Брандмауэры спроектированы преимущественно для пропуска, отброса трафика или отказа от него, но не для предупреждения об опасном трафике. IDS спроектированы на предупреждение о том, что в сети имеет место подозрительная деятельность.

В: Что может сделать IDS из того, чего не может сисадмин?

О: Обрабатывать несколько сотен миллионов (или больше) пакетов системных записей в день в двоичном коде. Мало кто из администраторов на такое способен.

В: Что может сделать сисадмин из того, чего не может IDS?

О: Привнести в работу творческое мышление и понимание значимости анализа этой сетевой деятельности.

В: Придется ли тратить время на настройку IDS?

О: Да. Если администратор не хочет погрязнуть в огромном количестве ошибочных результатов, IDS рекомендуется подстроить под окружающую среду.

В: Имеет ли значение физическая защита, даже если у меня лучшая сетевая защита?

О: Разумеется. Если любой может зайти в офис и уйти с сервером, то это равносильно электронному проникновению в сеть.

В: Зачем писать авторские подписи, когда их и так очень много в Snort?

О: В этом нет необходимости, однако администратору может понадобиться добавление функциональности, отсутствующей в существующем наборе правил, например правил, специально «подогнанных» под требования корпоративной политики, либо для обнаружения атак, нацеленных на конкретное закрытое программное обеспечение.

Приложение С

Понятие оценки уязвимости систем и Nessus

Темы приложения:

- **Что такое оценка уязвимости системы?**
- **Автоматические системы оценки**
- **Два подхода**
- **Реалистические виды на будущее**

☑ Резюме

☑ Краткое резюме по разделам

☑ Часто задаваемые вопросы

Введение

В современном Интернете, анализ каждой сетевой структуры вручную на предмет слабых мест защиты просто не реален. За последнее десятилетие операционные системы, программные приложения и сетевые протоколы настолько усложнились, что для обеспечения защиты от несанкционированных проникновений даже сравнительно небольшой сети потребуется специально приставленный к ней администратор.

Каждое техническое новшество влечет за собой волну новых слабых мест защиты. Результатом нового протокола могут стать десятки фактических реализаций, каждая из которых может содержать ошибки программирования, которые могут быть использованы хакерами. Логические ошибки, установленные производителями «лазейки» и конфигурации, заданные по умолчанию, затрагивают все — от современных операционных систем до самых простых серверов печати. Вчерашние вирусы кажутся «укрощенными зверьками» по сравнению с высокооптимизированными Интернет-червями, постоянно нападающими на каждую систему, подключенную к глобальной сети.

Для борьбы с этими сетевыми атаками сетевому администратору, наряду с профессиональными знаниями, необходимы соответствующие инструментальные средства для обнаружения уязвимых систем и их защиты до того, как возникнут проблемы. Одним из наиболее мощных на сегодняшний день инструментальных программных средств является оценка уязвимости, и в данном приложении описывается ее понятие, функции и то, почему ее необходимо проводить как можно чаще. Далее представлен анализ различных типов программных решений, преимущества каждого из них, а также фактические шаги, предпринимаемые большинством инструментов во время процесса оценки. В следующем разделе описываются два четких подхода, применяемые текущим поколением программ оценки, и то, как выбор подходящей программы может оказать значительное воздействие на защиту сети. И, наконец, завершается приложение аспектами и ограничениями, которые можно ожидать при использовании любых доступных средств оценки.

Что такое оценка уязвимости системы?

Для раскрытия понятия оценки уязвимости систем прежде всего необходимо определить, что такое «уязвимость». Для целей данной книги *уязвимостью* называется любая ошибка программирования или конфигурации, которая может дать взломщику сети возможность получения несанкционированного доступа к ней. В это понятие входит все: от предсказуемого пароля на маршрутизаторе до неисправленных дефектов программирования открытой сетевой службы. Факты уязвимости больше не являются прерогативой системных хакеров или консультантов по сетевой защите; они превращаются в отпирающий фактор, лежащий в основе большинства сетевых червей, шпионских программ и вирусов электронной почты.

15 Зак. 1269

«Спамеры» все чаще учитывают слабости защиты программного обеспечения для сокрытия своих каналов; ретрансляторы открытых электронных сообщений 90-х годов заменены на современные дискредитированные «зомби»-посредники, созданные с помощью массовой эксплуатации распространенных слабых мест программных приложений. Часто можно услышать вопрос: «Зачем кому-то нужна моя система?» Ответ заключается в том, что большинство эксплуатированных систем не являлось целью само по себе, они просто оказались очередным адресом в сетевом диапазоне, сканированном хакером. Это — цели вероятности, а не выбора. Распространителям спама все равно, принадлежит система международному банку или вашей бабушке; для них это не имеет значения до тех пор, пока они могут устанавливать программы-ретрансляторы.

Оценка уязвимости — это просто процесс определения ее местоположения и информации о ней. Такая оценка обеспечивает администраторов методами обнаружения и решения проблем сетевой защиты до того, как злоумышленники смогут ими воспользоваться. Одной из наиболее распространенных областей использования оценки уязвимости является их возможность подтверждения правильности мер защиты. Если недавно была установлена система выявления несанкционированных проникновений (intrusion detection system, IDS), то оценка уязвимости позволяет определить, насколько хорошо работает эта система. Если по завершении оценки IDS не выдала ни единого предупреждающего сигнала, то, возможно, настало время переговоров с производителем.

Процесс идентификации уязвимости использует разные способы, однако целью их всех является одно— отчет обо всех выявленных слабых местах сети в данный момент времени. Отчет обычно содержит список обнаруженных слабых мест с подробным описанием каждого, места их обнаружения, связанные с ними потенциальные риски и методы их решения. На рис. С.1 представлен образец отчета сканера защиты Nessus для сети, состоящей всего из пяти систем; количество слабых мест превышает цифру 100!

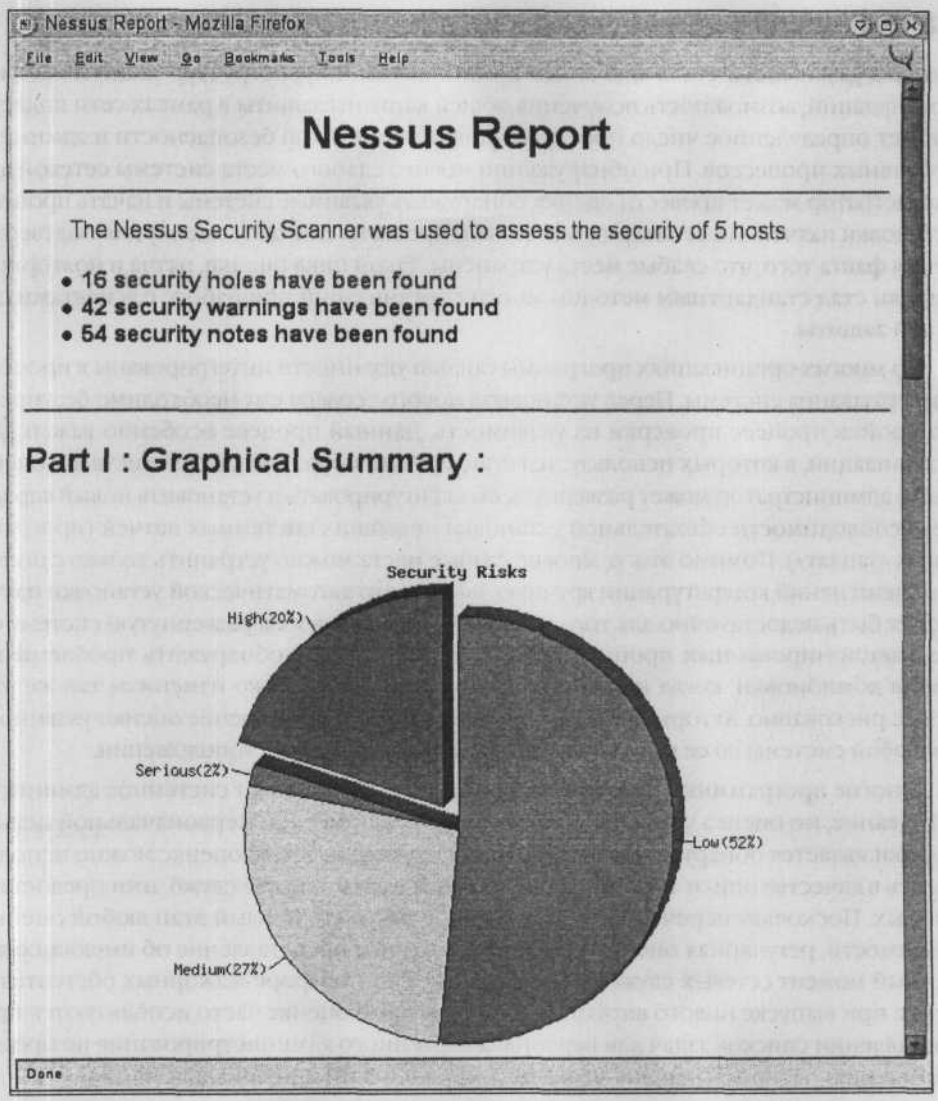

Рис. С. 1. Образец отчета Nessus

Зачем нужна оценка уязвимости?

Оценка уязвимости стала ключевым компонентом инфраструктур защиты многих организаций; возможность получения общей картины защиты в рамках сети поддерживает определенное число процессов информационной безопасности и административных процессов. При обнаружении нового слабого места системы сетевой администратор может провести оценку, обнаружить уязвимые системы и начать процесс установки патчей. По ее завершении можно провести еще одну оценку для подтверждения факта того, что слабые места устранены. Такой цикл оценки, патча и повторной оценки стал стандартным методом многих организаций при работе с аспектами сетевой защиты.

Во многих организациях программы оценки уязвимости интегрированы в процесс развертывания системы. Перед установкой нового сервера ему необходимо безупречно пройти процесс проверки на уязвимость. Данный процесс особенно важен для организаций, в которых используется стандартный образ для каждой системы; очень часто администратор может развернуть, сконфигурировать и установить новый сервер без необходимости обязательной установки новейших системных патчей (программных «заплат»). Помимо этого, многие слабые места можно устранить только с помощью изменений конфигурации вручную, потому что автоматической установки патча может быть недостаточно для того, чтобы обезопасить вновь развернутую систему от несанкционированных проникновений. Гораздо проще обнаружить проблемы во время компоновки, когда конфигурацию можно очень легко изменить; так же это менее рискованно. Авторы настоятельно рекомендуют выполнение оценки уязвимости любой системы *до* ее развертывания в окончательном местоположении.

Многие программные решения сетевой защиты усложняют системное администрирование, но оценка уязвимости фактически ей помогает. Первоначальной целью оценки является обнаружение слабых мест системы; отчет об оценке можно использовать в качестве описи систем, установленных в сети, а также служб, ими предоставляемых. Поскольку перечисление хостов и служб — это первый этап любой оценки уязвимости, регулярная оценка дает очень полезное представление об имеющихся в данный момент сетевых службах. Оценка помогает при форс-мажорных обстоятельствах: при выпуске нового вируса (червя) отчеты об оценке часто используются при составлении списков задач для персонала системного администрирования по предотвращению распространения червя до достижения им критической массы.

Классификация основных средств — одна из наиболее общих областей применения программ оценки уязвимости, не связанная с системной защитой. Осведомленность о количестве и типах используемых принтеров помогает при планировании ресурсов. Определение количества систем Windows 95, подлежащих обновлению, ограничится простым просмотром последнего отчета. При планировании сетевой

топологии чрезвычайно полезна возможность простого просмотра документации, чтобы сказать, какие из сетевых ресурсов могут быть перегружены или использованы не с полной нагрузкой.

Программные средства оценки также могут обнаруживать факты нарушения корпоративной политики; многие инструменты имеют возможность сообщать о пиринговых (peer-to-peer services, P2P) службах, о коллективно используемых каталогах, заполненных незаконно используемыми материалами и неправомочными инструментами удаленного доступа. Если из компании уходит сисадмин, довольно долго проработавший на этой должности, то инструмент оценки можно использовать для обнаружения возможного оставления им «лазейки» в брандмауэре. Если в канале доступа к сети появляются внезапные помехи, то оценку уязвимости можно использовать для определения местоположения рабочих станций с установленным программным обеспечением коллективного использования файлов.

Одной из наиболее важных областей использования данных оценки уязвимости является корреляция событий; если имеет место несанкционированное проникновение в сеть, самый последний отчет оценки позволяет администратору сетевой защиты определить, как он произошел и какие другие устройства были дискредитированы. Если взломщик получил доступ к сети, содержащей web-серверы без последних патчей, то можно предположить, что он также получил доступ и к этим системам.

Мысли вслух...

Системы обнаружения несанкционированных проникновений (IDS)

Различие между оценками уязвимости и IDS не всегда очевидно. Чтобы понять различия между этими надежными системами защиты для начала следует понять принципы работы IDS. Говоря о последних, люди часто имеют в виду то, что на профессиональном языке называется сетевыми системами обнаружения несанкционированных проникновений (network intrusion detection system, NIDS). Роль NIDS состоит в мониторинге сетевого трафика, «отсеивании» опасных атак от полезных данных и подаче сигнала тревоги при обнаружении попыток несанкционированного проникновения в сеть. Такой тип защиты называется *реактивной мерой безопасности*, поскольку информация о несанкционированном проникновении поступает администратору уже после того, как оно произойдет. При оценке же уязвимости администратор получает информацию о слабом месте до того, как оно будет использовано для дискредитации системы, что позволяет своевременно устранить проблему и избежать злонамеренного проникновения. По этой причине оценки уязвимости считаются *упреждающей мерой безопасности*.

Типы оценок

Термин *«оценка уязвимости»* используется для обозначения различных типов и уровней сетевых служб. Оценка хоста, как правило, относится к анализу защиты одной системы, часто с помощью специализированных инструментальных средств и учетной записи администратора. И наоборот, сетевая оценка применяется для тестирования одновременно всей сети систем.

Оценка хостов

Инструменты оценки хостов были в числе первых упреждающих средств защиты, доступных для сисадминов, и используются до сих пор. Эти инструменты требуют установки программных средств оценки на каждую систему, к которой необходимо осуществить доступ. Эти программные средства могут работать как в автономном режиме, так и быть подключенными к центральной системе сети. При оценке хостов осуществляется поиск слабых мест на системном уровне: небезопасных разрешений на использование файлов, недостающих патчей программного обеспечения, несоответствий требований корпоративной политики и неприкрытых «лазеек» и установок «Троянских коней».

Глубина проверки, выполняемой инструментами оценки хостов, делает ее предпочтительным способом мониторинга защиты критичных систем. Недостаток ее заключается в том, что, помимо административного доступа к каждой тестируемой системе, такая оценка требует набора специализированных инструментов для операционной системы и используемых программных пакетов. Вкупе со значительными временными затратами, связанными с тестированием, и ограниченной расширяемостью, оценка хостов часто используется только для нескольких наиболее критичных систем.

За последние несколько лет количество доступных и современных программных решений оценки хостов сократилось. Такие инструменты, как COPS и Tiger, на которые сисадмины «молились» всего несколько лет тому назад, теперь уже считаются практически бесполезными. Многие независимые (автономные) инструменты заменены на агентские системы, в которых применяются средства централизованной отчетности и управления. Подобный переход «подогревался» необходимостью расширяемых систем, которые можно было бы развертывать в более крупных серверных «фермах» с минимумом усилий администрирования. На время публикации книги единственные более-менее часто используемые автономные инструменты оценки хостов были предназначены для «нетехнических» домашних пользователей и администраторов, работающих по совместительству в компаниях с небольшими системами.

Несмотря на спад использования автономных инструментальных средств, число систем «управления корпоративной безопасностью», включающих компонент оценки хостов, по-прежнему активно растет. Результатом двойственных требований расширяемости и простоты использования стало то, что оценка хостов превращает-

ся в компонент более крупных систем управления. Многие компании-производители программных средств предлагают коммерческие продукты в этой сфере, включая (но не ограничиваясь) производственную линию Internet Security System's System Scanner, Computer Associates eTrust Access Control, а также продукт BindView's bvControl.

Сетевая оценка

Методы сетевой оценки применяются почти так же долго, как и оценка хостов, начиная с пакета SATAN (Security Administrator Tool for Analyzing Networks), выпущенного в 1995 году Дэном Фармером (Dan Farmer) и Вьетце Венема (Wietse Venema). Продукт SATAN обеспечивал новую перспективу администраторам, привыкшим к методам оценки хостов и устойчивым инструментальным средствам. Вместо проведения анализа локальных систем на предмет наличия проблем, он позволял рассматривать общие проблемы любой системы, подключенной к сети. Это открывало путь непрерывно развивающемуся рынку как открытых, так и коммерческих сетевых систем оценки.

Оценка сетевой уязвимости размещает все работающие системы в сети, определяет используемые сетевые службы, после чего анализирует их на предмет потенциального наличия слабых мест. В отличие от программных решений оценки хостов, данный процесс не требует изменений конфигурации оцениваемых систем. Методы сетевой оценки могут быть расширяемыми и эффективными в том, что касается административных требований, и они являются единственным гибким путем измерения степени защиты крупных, сложных сетей разнородных систем.

Несмотря на очевидную эффективность использования сетевых оценок для выявления слабых мест систем, они демонстрируют ряд ограничений, в число которых входят следующие: неспособность обнаружения определенного типа «лазеек», сложности с брандмауэрами и невозможности тестирования определенных типов уязвимости из-за опасности самого процесса тестирования. Сетевая оценка может сбить нормальное функционирование служб, препятствовать работе многих устройств (особенно принтеров), занимать слишком большой объем пропускной способности и создавать на оцениваемых системах переполненные диски с системными журналами. Кроме того, многие уязвимости могут эксплуатироваться с помощью учетной записи авторизованного, но непривилегированного пользователя, и их нельзя обнаружить путем сетевой оценки.

Автоматические системы оценки

Столкнувшись с методами оценок уязвимости, можно получить опыт использования услуг консалтинговой компании по системам безопасности, обеспечивающей сетевой аудит. Такой тип аудита, как правило, состоит как из ручных, так и автоматизированных компонентов; аудиторы будут использовать автоматические инструменты для предварительной работы, завершая ее инспекцией системы вручную. Несмотря на то,

что этот процесс может дать исчерпывающие результаты, он часто намного более дорогостоящий, по сравнению с простым использованием автоматизированного инструмента оценки для ее выполнения внутри компании.

Результатом необходимости автоматизированных инструментов оценки стала разработка определенного числа самых современных программных решений в диапазоне от продуктов с простыми графическими пользовательскими интерфейсами (graphical user interface, GUI) до автономных устройств с возможностью интеграции в массивные распределенные архитектуры для оценки. Из-за огромного количества испытаний на уязвимость, необходимых для создания даже простейшего инструмента оценки, коммерческий рынок легко разделился на две части: на определенное количество хорошо финансируемых независимых программных продуктов и буквально сотни решений, созданных на открытом сканере системной защиты Nessus (Nessus Security Scanner). Эти автоматизированные инструменты можно разделить также на два типа продуктов: приобретаемые фактически (покупкой или скачиванием из Интернет) и получаемые по подписке.

Сравнение автономных программных продуктов и полученных по подписке

В автономную категорию продуктов входит большинство открытых проектов и порядка половины серьезных коммерческих предложений. Примерами могут служить Nessus Security Scanner, Retina от eEye, Lightning Proxy от Tenable Security и Security Baseline Scanner от Microsoft. Эти продукты поставляются либо как программные пакеты, устанавливаемые на рабочую станцию, либо как аппаратное средство для простого подключения и выхода в сеть.

Решения, получаемые по службе подписки, придерживаются несколько иного подхода; вместо того, чтобы требовать от пользователя выполнение фактической установки и развертывание системы, производитель самостоятельно задает базовую конфигурацию и предоставляет клиенту web-интерфейс. В основном это используется для обеспечения методов оценки уязвимости для устройств, связанных с Интернет (внешняя оценка), но может и быть объединено с устройством предоставленных методов оценки для внутренней сети организации. В число примеров продуктов, поставляемых по подписке, входят QualysGuard от Qualys, Automated Scan от BeyondSecurity, а также продукт Frontline от компании Digital Defense.

Преимущества использования автономных продуктов очевидны: никакие данные не выходят за пределы компании и администраторы всегда знают, когда, где и как используется тот или иной продукт. Недостаток, впрочем, заключается в том, что такие продукты требуют от пользователя обновления перед каждым использованием, во избежание работы с просроченным набором проверки уязвимости, когда потенциально можно пропустить вновь обнаружившиеся слабые места. Преимущества модели службы подписки: обновления осуществляются без участия пользователя,

а, поскольку внешняя оценка происходит из сети производителя, администратор получает реальную картину того, как его сеть выглядит из Интернет.

Недостатки подписного решения: неполный контроль над конфигурацией устройства и сохранение уязвимости на системах производителя. Появились некоторые смешанные (гибридные) подписные программные решения, обрабатывающие оба этих аспекта посредством арендованных устройств, совместно с предоставленными пользователями носителями для хранения данных оценки. Одним из продуктов, реализующих данный подход, является система IP360 от nCircles, в которой применяются множественные выделенные устройства, сохраняющие все уязвимые данные на съемном flash-устройстве.

Процесс оценки

Независимо от того, какое используется программное решение автоматизированной оценки, оно, более чем вероятно, будет придерживаться одного общего процесса. Каждая оценка начинается с того, что пользователь указывает адрес или диапазон адресов для тестирования. Это часто реализуется в виде выпадающего списка предварительно заданных диапазонов или текстового элемента управления, куда можно ввести сетевой адрес и маску. После того, как заданы адреса, интерфейс часто представляет пользователю набор опций конфигурации для проведения оценки; сюда могут входить списки портов для сканирования, настройки ширины канала либо другие особенности, имеющие отношение к данному продукту. После ввода всей этой информации начинается фаза фактической оценки. На рис. С. 2 показано окно конфигурации оценки на Nessus Security Scanner.

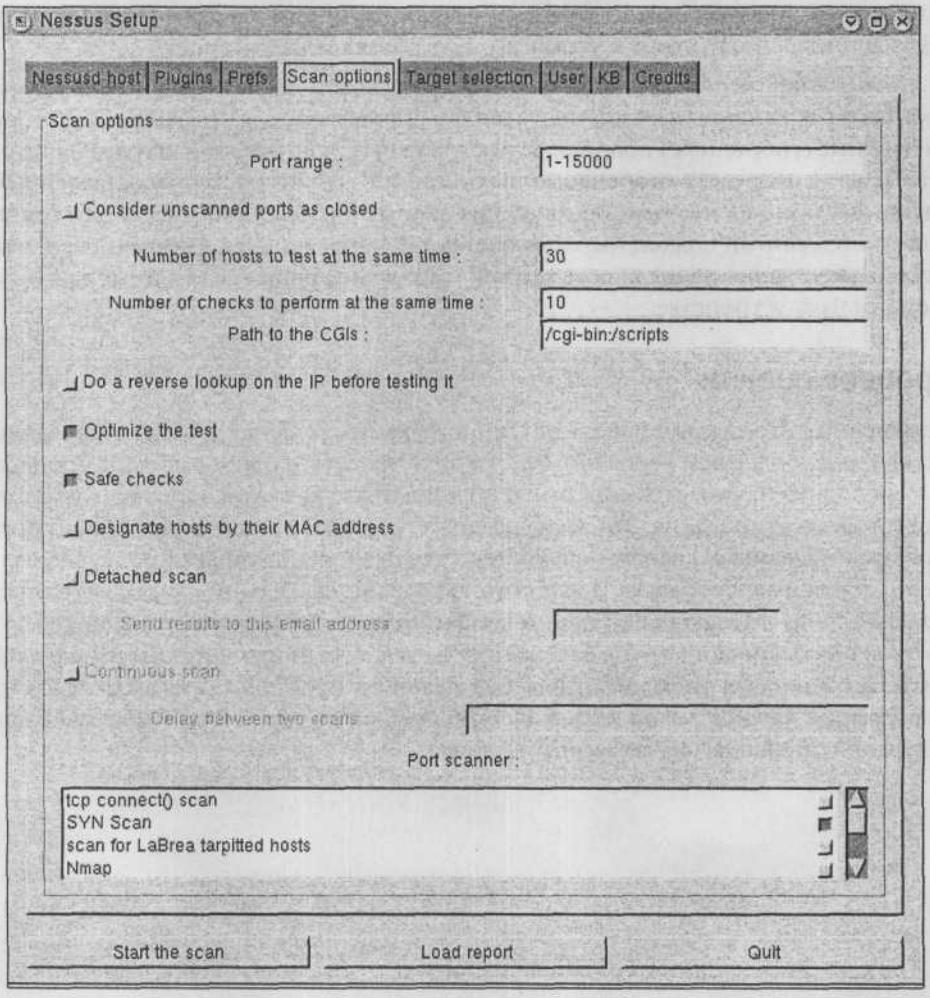

Рис. С. 2. Опции Nessus Scan

Обнаружение активных систем

Первый этап оценки сетевой уязвимости определяет, какие IP-адреса (Internet Protocol addresses) в целевом диапазоне фактически соответствуют системам, работающим в активном режиме, к которым может быть осуществлен доступ. Для каждого указанного пользователем адреса отправляются один или два пробных запроса с целью получения ответа. При получении ответа система разместит этот адрес в списке действу-

ющих хостов. В случае с сетями с большим количеством надежных брандмауэров большинство продуктов имеет возможность принудительного сканирования всех адресов, независимо от того, получен ли на данном этапе ответ.

Типы отправляемых на данном этапе пробных запросов варьируются в зависимости от инструмента оценки; несмотря на то, что все пользуются ping-запросами протокола ICMP (Internet Control Message Protocol), выходящие за эти рамки способы редко похожи друг на друга в двух разных программных продуктах. Nessus Security Scanner обладает возможностью применения серии запросов TCP-подключения к набору обычных портов для идентификации систем, которые, возможно, блокируют сообщения ICMP. Это позволяет сканеру идентифицировать системы, расположенные позади брандмауэров либо специально сконфигурированные на игнорирование трафика ICMP. После отправки запроса на подключение любой ответ, полученный с данной системы, добавит ее в список тестируемых хостов. Многие коммерческие продукты, помимо стандартных тестов ICMP и TCP, включают в себя возможность апробирования особых служб пользовательского протокола данных (User Datagram Protocol, UDP). Данная методика полезна для обнаружения систем, пропускающих только особые запросы приложений UDP, как обычно случается с внешними серверами DNS и RADIUS.

Идентификация активных систем

По завершении первоначальной фазы обнаружения хоста многие программные продукты будут использовать различные методики «снятия отпечатков» для определения типа обнаруженной системы в каждом адресе в списке активных систем. Эти методики варьируются от запросов Простого протокола сетевого управления (Simple Network Management Protocol, SNMP) до идентификации операционной системы на основе особенностей стека TCP/IP.

Данный этап может быть критичным для предотвращения столкновения процесса оценки с нормальным функционированием сети; достаточно много серверов печати, «пожилых» систем UNIX и программных приложений сетевого пользования демонстрируют сбои при проведении оценки их уязвимости. В самом деле, самая большая проблема, с которой сталкиваются очень многие администраторы инструментов автоматизированной оценки заключается в том, что они могут нарушить нормальный ход сетевых операций. Довольно часто администратору приходится тратить время на перезагрузку устройств, извлечение «мусорных» распечаток из сетевых принтеров печати и отладку пользовательских проблем в работе с сетевыми приложениями. Данный этап идентификации часто можно использовать для обнаружения и «излечения» проблематичных систем до того, как последующие этапы вызовут реальные проблемы.

Перечисление служб

После обнаружения и идентификации хоста следующим шагом, как правило, является сканирование портов. Сканирование портов — это процесс определения того, какие службы TCP и UDP открыты на рассматриваемой системе. Сканирование портов TCP выполняется отправкой запросов о подключении в сконфигурированный список номеров портов в каждой системе. Если система отвечает сообщением, указывающим, что порт открыт, то номер порта записывается и сохраняется для последующего использования. При сканировании портов UDP результаты часто противоречивы, поскольку сама природа этого протокола затрудняет во многих сетях получение непротиворечивых результатов.

Существует 65 536 доступных портов TCP, однако большинство инструментов оценки выполняет сканирование только ограниченного их числа. Ограничение сканирования поднабором доступных портов сокращает время выполнения оценки и ширину канала, требуемую процессом оценки (в том, что касается передачи пакетов данных в секунду, а не общего числа байтов). Недостатком того, что сканируются не все порты, является то, что службы, не придерживающиеся принятых стандартов, использующих большие номера портов (например, ничто не мешает запустить web-сервер на порту 8088, а не 80.— *Примеч. науч. ред.*), часто полностью игнорируются процессом оценки. Nessus Security Scanner предоставляет опцию, дающую пользователям возможность задания того, как рассматривать эти порты. Установка по умолчанию — считать все не сканированные порты TCP открытыми, что во время проведения оценки может занять довольно много времени, особенно в случаях с плотными фильтрами пакетов данных или брандмауэрами. На рис. С. 3 показан Nessus Security Scanner, выполняющий фазу перечисления служб.

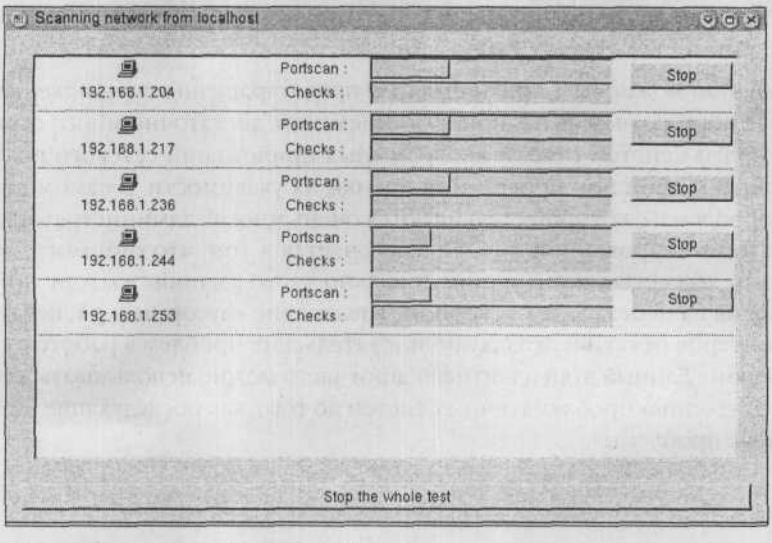

Рис. С. 3. Перечисление служб сканером Nessus

Идентификация служб

После фазы сканирования портов многие инструменты оценки переходят к идентификации служб на каждом открытом порту. Данный процесс начинается с отправки определенных общих запросов приложений и анализа ответов в соответствии с набором подписей. Когда подпись находит соответствие с известным программным приложением, эта информация сохраняется для последующего использования, и тестируется следующая служба. Несмотря на то, что данный этап выполняется не всеми инструментами оценки, те, которыми он выполняется, выдают намного более точные результаты, просто обладая информацией о том, какие слабые места и на каких портах искать.

Nessus Security Scanner включает в себя мощный механизм идентификации служб, способный к обнаружению более 90 различных протоколов приложений. В этом механизме используется набор пробных запросов приложений для получения ответа (реагирования) от каждой службы. После отправки каждого пробного запроса результат сравнивается со списком подписей известных приложений. При нахождении совпадающей подписи номер порта и протокол сохраняются для последующего использования, и механизм переходит к следующей службе. При обнаружении транспортного протокола защищенных сокетов (Secure Sockets Layer, SSL) механизм автоматически переходит в режим SSL до отправки пробных запросов приложения. Такая *комбинация идентификации на транспортном уровне и уровне службы позволяет* системе точно выявлять слабые места, даже когда пораженная служба находится на нестандартном порту.

Протокол передачи гипертекстовых файлов (HyperText Transfer Protocol, HTTP) — прекрасный пример службы, часто обнаруживаемой на порту, отличном от заданного по умолчанию. Несмотря на то, что практически все стандартные web-серверы используют порт TCP 80, буквально тысячи программных приложений устанавливают службу HTTP на порт, отличный от 80-го. Интерфейсы web-конфигурации для многих серверов web-приложений, аппаратные средства и инструменты защиты будут использовать нестандартные порты. Протоколы передачи электронных сообщений, такие, как Простой протокол электронной почты (Simple Mail Transfer Protocol, SMTP), Почтовый протокол 3 (Post Office Protocol 3, POP3) и Протокол доступа к сообщениям в Интернет (Internet Message Access Protocol, IMAP) часто конфигурируются с транспортным протоколом SSL и также устанавливаются на нестандартные порты. Обычной ошибкой конфигурации является блокирование спама на основной службе SMTP, но безоговорочный прием всех сообщений, полученных через службу SMTP в оболочке SSL на другом порту. В дополнение к сказанному, данная фаза предохраняет приложение, выполняющееся на порту, обычно зарезервированном для другого протокола, от полного игнорирования процессом сканирования или передачи ошибочных результатов.

Идентификация программных приложений

После завершения фазы обнаружения служб следующий шаг — выявление фактически используемого приложения для каждой обнаруженной службы. Цель данного этапа — идентификация поставщика, типа и версии каждой службы, обнаруженной на предыдущем этапе. Данная информация критична, поскольку тесты на уязвимость для одного приложения могут вызвать сбой другого приложения. Примером этому может служить уязвимость web-сервера к переполнению буфера длинным именем пути. Если любые другие тесты на уязвимость отправляют запрос длиннее, чем эта система ожидает, тогда программное приложение переживет аварийный отказ. Чтобы не подводить под сбой web-сервер, для аккуратного выявления на нем этого слабого места система должна сначала идентифицировать именно это приложение, после чего запретить выполнение на нем «проблематичных» тестов.

Одной из самых распространенных проблем большинства инструментов оценки является *ошибка*, когда инструмент сообщает о слабом месте, которого на самом деле на тестируемых системах не существует. Ошибки являются причиной очень большого объема работы по верификации для инженера-оценщика. При отсутствии информации об идентификации приложения или при ее недостаточности результаты тестирования всегда включают в себя ошибки. Когда разработчики таких инструментов оценки пишут тесты уязвимости, часто предполагается, что система, с которой они взаимодействуют, всегда будет продуктом, в котором обнаруживаются слабые места. Другие программные приложения, предлагающие те же службы, часто будут реагировать на пробные запросы так, что логика теста уязвимости регистрирует слабое место. По этой причине идентификация программного приложения часто превращается в один из наиболее критичных компонентов современных инструментальных средств оценки.

Идентификация слабых мест

После идентификации каждого работающего хоста, сопоставления каждого открытого порта на известную службу и отображения известных служб на конкретные программные приложения, система готова к проведению теста на уязвимость. Данный процесс часто начинается с базовых методик сбора информации, за которыми следуют пробы активной конфигурации и, наконец, набор обычных атак, определяющих наличие тех или иных слабых мест в тестируемой системе.

Процесс идентификации слабых мест может варьироваться от простого сопоставления баннеров и тестирования версий до полной эксплуатации тестируемого дефекта. При использовании для идентификации уязвимости процессов обнаружения версий и сопоставления баннеров, результатом часто бывают ошибки из-за того, что производители программных средств предоставляют обновленные версии, в которых по-прежнему отображен баннер уязвимой версии. (Кроме того, многие администраторы сознательно изменяют баннеры, выдавая одни службы за другие с тем, чтобы

сбить с толку потенциального злоумышленника. — *примеч. науч. ред.*). По этой причине сверка с номерами версий производится только в отсутствие другого способа надежной верификации наличия в системе слабых мест.

Многие из известных слабых мест можно идентифицировать только попыткой эксплуатации дефекта. Это часто означает использование слабого места для выполнения команды, отображения системного файла или подтверждения иным способом, что система действительно уязвима для несанкционированных проникновений со стороны удаленных злоумышленников. Многие из слабых мест — переполнение буфера, манипуляции с данными ввода — можно выявить запуском дефекта в объеме, достаточном, чтобы понять, что система без патчей, но недостаточном для фактического сбоя сетевой службы. Инструмент оценки должен проходить «по грани» между уверенной идентификацией уязвимости и разрушительными побочными эффектами.

Тестирование на уязвимость, при котором применяется проверка баннеров, сталкивается с проблемами, когда на сетевую службу компанией-производителем или сисадмином «накладываются заплаты» , а отображаемый в сети номер версии не обновляется, либо когда он не обновляется так, как этого ожидает тест на уязвимость. Такие случаи весьма распространены при работе с открытыми платформами на базе UNIX и некоторыми дистрибутивами Linux.

Отчеты о слабых местах системы

По завершении анализа последним этапом процесса оценки является составление отчетности. Каждый программный продукт имеет свои «представления» о том, как должны генерироваться отчеты, что в них должно входить и в каких форматах. Независимо от марки продукта в отчете будут перечислены системы, обнаруженные во время оценки, и любые идентифицированные в них слабые места. Разные продукты обеспечивают разные уровни отчетности в зависимости от того, кто их будет читать; полезно составлять резюме высокого уровня для руководства с отчетом сисадмину о том, что систему необходимо отлаживать и как это лучше всего сделать. Одной из популярных функций многих инструментов оценки является возможность составления отчетов об общих тенденциях того, как сеть будет функционировать в будущем. На рис. С. 4 показано резюме отчета HTML Nessus Security Scanner.

Nessus Scan Report - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

Nessus Scan Report

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan Details	
Hosts which were alive and responding during test	5
Number of security holes found	16
Number of security warnings found	42

Host List	
Host(s)	**Possible Issue**
192.168.1.2	Security hole(s) found
192.168.1.204	Security warning(s) found
192.168.1.217	Security hole(s) found
192.168.1.236	Security hole(s) found
192.168.1.253	Security warning(s) found

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
192.168.1.2	ssh (22/tcp)	Security warning(s) found
192.168.1.2	netbios-ssn (139/tcp)	Security hole found
192.168.1.2	general/tcp	Security warning(s) found
192.168.1.2	netbios-ns (137/udp)	Security warning(s) found
192.168.1.2	general/udp	Security notes found
192.168.1.2	general/icmp	Security warning(s) found

Done

Рис. С. 4. Резюме отчета Nessus

Два подхода

При выполнении автоматизированной оценки уязвимости тестирование может радикально повлиять на подробность и качество результатов. В принципе, существуют два разных подхода к проверке на уязвимость: административный и внешний. Каждый подход имеет свои ярко выраженные преимущества и недостатки, связанные с тем, что многие из наиболее совершенных инструментов оценки превратились в смешанную модель, объединяющую все самое лучшее двух подходов. Ознакомление с ними обеспечит более глубокое понимание того, почему два разных инструмента оценки могут дать принципиально разные результаты при тестировании одной и той же сети.

Административный подход

При административном подходе оценка осуществляется с точки зрения обычного аутентифицированного сисадмина. Запуск инструмента оценки может производиться аутентифицированным административным пользователем либо осуществляться с помощью учетной записи пользователя и пароля. Эти мандаты можно использовать для выявления недостающих программных патчей, небезопасных настроек конфигурации и потенциально уязвимого клиентского программного обеспечения (например, клиентов электронной почты и web-браузеров).

Это — весьма мощный подход для оценки сетей, состоящих в основном из систем на базе Windows, авторизованных в одном домене. Он объединяет большую часть глубокого анализа оценки хостов с преимуществами расширяемости сетевой оценки. Поскольку все тесты на уязвимость выполняются либо с помощью удаленного регистра, либо с помощью удаленного доступа к файловой системе, то вероятность того, что инструмент оценки, использующий этот метод, может отрицательно повлиять на тестируемые системы, — чрезвычайно мала. Это позволяет проводить оценку в течение дня на фактически работающих системах, без боязни навредить производственному процессу.

Административный подход особенно хорош при попытках обнаружения и устранения слабых мест на стороне клиента сети рабочих станций. Многие компьютерные черви, Трояны и вирусы распространяются, используя слабые места клиентов передачи электронных сообщений и программы web-браузеров. Инструмент оценки, использующий данный подход, может осуществлять доступ к реестру каждой системы и определять, установлены ли самые последние патчи, применены ли нужные настройки сетевой защиты, а также то, имели ли место успешные атаки на данную систему. Системы защиты на стороне клиента — одна из наиболее часто игнорируемых точек входа в большинстве корпоративных сетей; имели место многочисленные случаи в сетях, когда хорошо защищенный периметр захватывался только потому, что пользователь ошибся web-сайтом, войдя на него с помощью устаревшего web-браузера.

К сожалению, эти программные продукты также часто имеют серьезные ограничения. Поскольку процесс тестирования использует стандартные административные каналы Windows, а именно службы NetBIOS и учетную запись административного пользователя, то результатом всего, что препятствует доступу к этому каналу, будут неточные результаты сканирования. Доступ к любой системе сети, сконфигурированной с другим источником аутентификации (работающей в автономном режиме, в другом домене либо авторизованной на сервере Novell), будет некорректным. Кроме этого, в этих программных продуктах могут присутствовать проблемы, схожие с проблемами инструментов оценки на базе хостов, — сетевые устройства, серверы на базе UNIX и телефонные системы, работающие поверх IP, могут полностью отсутствовать либо возвращать неполные результаты.

Брандмауэры на базе сети и хоста также могут препятствовать проведению оценки. Это препятствие обычно имеет место при проведении оценок по системе, расположенной в другом сетевом сегменте, например в демилитаризованной зоне (demilitarized zone, DMZ) или во внешнем сегменте позади выделенного брандмауэра. Помимо этого, сетевые устройства, серверы на базе UNIX и телефонные системы, работающие поверх IP, также могут полностью отсутствовать или давать минимальные результаты. Примером этого может быть определенный коммерческий инструмент оценки на базе Windows, который будет выдавать отчет об отсутствующих патчах IIS (Internet Information Server, информационный сервер Интернет), даже если web-сервер не активизирован или не сконфигурирован.

Данный тип тестирования очень полезен для верификации развертывания патчей в сети, но на него не следует полагаться как на единственный метод тестирования защиты. Программный пакет Security Baseline Scanner от Microsoft — лучший пример инструмента оценки, в котором применяется только этот подход. Многие из функций и предложений коммерческих инструментов оценки изначально базировались на данном подходе, и только с недавнего времени в процесс тестирования на уязвимость началось интегрирование других методик. Более подробно различия между административным и смешанным решениями рассматриваются в разделе «Смешанный подход».

Внешний подход

При внешнем подходе оценка рассматривается с точки зрения злонамеренного хакера, не имеющего аутентификации, пытающегося несанкционированно проникнуть в сеть. В процессе оценки могут приниматься решения о защите системы только через комбинацию «отпечатков» программных приложений, идентификации версий и фактических попыток эксплуатации. Оценочные инструменты, базирующиеся на этом подходе, часто имеют возможность обнаружения слабых мест системы в гораздо большем количестве операционных систем и устройств, чем при административном подходе.

При проведении крупномасштабной оценки сети, в которую входят рабочие станции с разными операционными системами и сетевыми устройствами, внешний подход — единственная методика, имеющая шанс возврата точных и непротиворечивых результатов о каждой обнаруженной системе. Если система защищена брандмауэром, то тестироваться будут только уязвимые службы с предоставлением той же информации, которую будет видеть взломщик при реальной атаке. Отчеты, генерируемые инструментами, работающими на данном смешанном подходе, нацелены на предотвращение общих атак, в отличие от средств, использующих административный подход, где упор сделан на отсутствующие патчи и незащищенные настройки конфигурации. По сути дела, внешний подход представляет более конкретный список проблем для устранения, что позволяет администратору сосредоточиться на аспектах, которые станут первоочередной целью потенциального взломщика.

Несмотря на то, что данный подход — единственный убедительный способ проведения оценки уязвимости разнородной сети, он также не лишен значительного количества недостатков. Наличие многих слабых мест проверить просто невозможно без вызова отказа программного приложения, устройства или операционной системы. В результате любые инструменты, проверяющие наличие данных типов слабых мест, либо обеспечивают возможность «шпионской» проверки, либо всегда подают сигнал тревоги при обнаружении потенциально уязвимой сетевой службы. Поскольку внешний подход обнаруживает только то, что видно из точки сети, в которой оценка была запущена, то ни одна уязвимая служба, связанная с другим интерфейсом той же системы, обнаружена не будет. Это относится к отчетности в большей степени, чем что-либо другое, потому что человек, просматривающий такой отчет, может не рассмотреть сеть в перспективе при составлении списка задач исправления для такой системы.

Смешанный подход

В последние годы все больше инструментов переходят на смешанный подход оценки уязвимости сетей. Там, где возможно, применяется административный подход, однако при недоступности учетной записи или ее непринятии тестируемой системой, приходится обращаться к методам удаленного снятия отпечатков. Качество смешанных программных решений очень сильно варьируется; продукты, изначально спроектированные на применение только административного подхода, переживают не лучшие времена при недоступности административных мандатов, а продукты, основанные на внешнем подходе, часто сбоят при использовании во время тестирования административной учетной записи. По всей видимости, второй вариант имеет больше шансов преодоления подобных барьеров без необходимости переписывания. Вообще говоря, все эти программные продукты выдают на порядок более точные результаты, чем системы, использующие какой-либо один подход. Nessus Security Scanner и пакет Retina от eEye — примеры использования смешанного подхода.

Одним из самых больших преимуществ инструментальных средств с применением внешнего подхода является то, что они часто могут определять наличие того или иного слабого места, независимо от применения патча. Как известно многим администраторам сетей Windows, установка патча операционной системы не гарантирует устранения слабого места. Недавно обнаруженный недостаток Microsoft Windows Network Messenger позволил удаленному хакеру выполнить произвольный код на уязвимой системе. Началась повсеместная эксплуатация этой уязвимости, и компании лихорадочно бросились устанавливать патч на все внутренние рабочие станции. «Недосмотр» заключался в том, что для того, чтобы «заплата» заработала, систему после ее наложения следовало перезагрузить. Многие сайты использовали инструменты автоматической установки патча для обновления уязвимых систем, но напрочь забыли о требовании перезагрузки.

В результате этого, при запуске инструмента оценки с административным подходом в отчете указывалось, что системы — «залатаны». Однако при проведении оценки с помощью Nessus Security Scanner отчеты показали, что на самом деле системы были уязвимы для несанкционированного проникновения. Инструмент с административным подходом просто проверил реестр каждой системы для определения применения патча, тогда как сканер Nessus фактически опробовал данное слабое место на предмет его действительной слабости. Без такой повторной проверки организация потеряла бы сотни «беззащитных» рабочих станций, несмотря на наложенные «заплаты». Анализ системного реестра, проводимый большинством инструментов с административным подходом, может пропускать слабые места по многим другим причинам. Чаще всего случается так, что для «лечения» одной уязвимости применяется экстренное исправление (hotfix), после чего ко всей системе применяется устаревший пакет исправлений (service pack). Изменения, внесенные hotfix'ом, перезаписываются, а запись системного регистра о применении патча по-прежнему существует. Данная проблема в основном касается операционных систем Windows, хотя многие производители коммерческих систем UNIX также сталкивались с подобной проблемой отслеживания установленных патчей и определения того, какие из них еще предстоит применить.

С недавнего времени во многих инструментах административного и смешанного типа разрабатываются новые методики верификации наличия установленного патча. Пакет HFNetChk Pro от Shavlik Technology проверяет фактическое время последней перезагрузки и сравнивает его с датой установки экстренного исправления. Nessus Security Scanner же фактически оценивает нужные исполняемые файлы в сети и верифицирует интегрированные номера версий.

Недостатки смешанного подхода, как правило, незаметны до просмотра результатов достаточно большого количества обширных областей сканирования; по причине того, что административный подход применяется в нужное время и в нужном месте, факт наличия слабых мест, передаваемый на систему, принимающую предоставленную учетную запись пользователя, может не передаваться на сходную систему, использующую иную область аутентификации. Если администратор не отдает себе отчета в том, что уязвимой может быть и другая система, то это может привести к возникновению ложного ощущения защищенности. Пропущенные слабые места может быть очень сложно отследить автоматически, и они могут попасться администратору. Возможно, к этим системам не были применены патчи, поэтому результатом использования смешанного подхода могут стать большие потери при несанкционированном вторжении или появлении в системе компьютерного червя. Несмотря на то, что административный подход «страдает» от такой же проблемы, использование административного подхода гарантированно не будут проверять системы, находящиеся за пределами области аутентификации.

Реалистические виды на будущее

Первые коммерческие инструменты оценки уязвимости компьютерных систем рекламировались как способные магическим образом идентифицировать любую «брешь» в защите сети. Еще несколько лет назад это утверждение могло казаться близким к истине. Количество описанных слабых мест еще было небольшим, и отслеживание информации об уязвимости систем могло рассматриваться как не совсем понятное хобби. На сегодняшний же день картина во многом иная; если ранее было описано несколько сотен слабых мест, то сегодня — тысячи, а о количестве системных дефектов, которые можно использовать для проникновения в корпоративную сеть, не стоит даже говорить.

Помимо наступления «уязвимостей» резко подскочило число и количество типов устройств, обнаруживаемых в средней корпоративной сети. Какие-то из них выходят из строя, какие-то демонстрируют неадекватное поведение либо начинают работать крайне медленно во время проведения оценки уязвимости сети. Тест на уязвимость, спроектированный для одной системы, может полностью вывести из строя какое-либо другое программное приложение или аппаратное устройство, что может прерывать нормальный ход работы. Инструменты оценки выполняют сложную работу; им приходится идентифицировать в системах максимально возможное количество слабых мест, которые тут же необходимо анализировать и распределять по категориям, не включая в отчеты ложные сигналы, и одновременно избегать выхода из строя устройств и программ, которые изначально не были рассчитаны на какую бы то ни было защиту. Одни инструменты демонстрируют большую эффективность, другие — меньшую, хотя все доступные в настоящее время инструменты, так или иначе, сталкиваются с этой проблемой.

Когда человек впервые начинает пользоваться системой оценки уязвимости, он часто замечает, что результаты между последовательными сканированиями могут значительно различаться. Этот момент чаще встречается в обширных сетях, подключения в которых осуществлены через менее быстродействующие каналы связи. Причины этого могут быть разными, однако основная в том, что, в отличие от большинства процессов, происходящих в программном обеспечении, удаленное тестирование на уязвимость имеет больше отношения к искусству, нежели к науке. Многие инструменты оценки задают жесткие рамки времени простоя для установки подключения к сетевой службе или получения результата запроса. Если в сети имеет место задержка срабатывания на секунду-другую, то тест может пропустить действительный системный ответ. Такие тонкости, связанные со временем, — весьма распространены в среде инструментов оценки, однако при определении непротиворечивости результатов сканирования большое значение имеет множество других факторов.

Во многих сетевых устройствах имеется консоль Telnet, позволяющая администратору удаленно изменить конфигурацию системы. Такие устройства часто налагают жесткие ограничения на число параллельных сетевых подключений, допустимых для

данной службы. Процесс оценки уязвимости может выполнить одновременно несколько тестов на одном порту; при этом одна проверка получит действительный ответ, а другая — сообщение об ошибке, указывающее, что используются все доступные подключения. Если второй тест «отвечал» за проверку пароля по умолчанию на данном конкретном устройстве, то он вполне может пропустить слабое место. Если то же самое сканирование запустить позже, когда тест на пароль по умолчанию уже проведен, то слабое место будет обнаружено за счет других тестов. Такой тип временной проблемы шире распространен на сетевых устройствах и устаревших системах UNIX, нежели на более современных рабочих станциях и серверах, однако в конечном итоге он может привести к противоречивым результатам оценки.

Инструменты и ловушки...

Оценка серверов печати

Практически все инструментальные средства оценки систем на уязвимость имеют одно общее свойство: они могут «сожрать живьем» сервер печати. Источником данной проблемы является тот факт, что серверы печати предлагают пользователям множество сетевых служб, используемых для сброса документов непосредственно на подключенный принтер. Самой проблематичной из этих служб является Протокол прямой печати (Direct Print Protocol), являющийся службой TCP. При работе с этим протоколом могут возникнуть проблемы с автоматизированными инструментами оценки, поскольку на этапе идентификации службы принтер выдает кучу бумаги, заполненной непонятными символами. Другая общая проблема относится к обычной службе FTP, к которой подключено много принтеров. Данная служба обеспечивает аутентификацию с помощью комбинации имени пользователя и пароля и просто распечатывает загруженные файлы. Если инструмент оценки осуществляет поиск уязвимых мест конфигурации FTP, то вся печать может закончиться выводом тестового файла сервера печати. В довершение ко всему, достаточно много серверов печати обладают настолько убогой реализацией TCP/IP, что обычное сканирование портов может вывести их из строя, и, чтобы вернуть их к жизни, требуется повторение полного энергетического цикла.

Динамические системы — «гроза» инструментов оценки уязвимости. Если процесс оценки — в полном разгаре, а пользователю приходит в голову мысль о перезагрузке компьютера, то программа оценки начнет получать извещения о задержке подключения проверок. Как только система вернется в рабочий режим, все последующие тестирования будут проходить нормально, однако результатами всех тестов, запущенных в период простоя, станут упущенные слабые места. Вычислить подобную проблему невероятно сложно при просмотре объемного отчета оценки, и в этот момент

только набор коммерческих систем может предложить возможность обнаружения и повторного сканирования систем, которые перезагружаются во время процесса оценки на уязвимость.

Несмотря на огромное количество уточнений и тестирований, которым подвергалось большинство программ оценки, ошибочные результаты продолжают досаждать администраторам сетей и консультантам по сетевой защите. Как уже обсуждалось выше, так называемая «ошибка» — это просто слабое место, о котором сообщается в отчете, но которого на самом деле не существует в тестируемой системе. Эти неприятности требуют достаточно большого объема работы по верификации: перед тем, как отказаться от Nessus или от любого программного приложения оценки уязвимости из-за нагрузки ошибочных результатов, рекомендуется потратить время на их настройку. Нестандартные web-серверы, портированные пакеты программного обеспечения и разрешительные строки сопоставления в рамках сценариев тестов на уязвимость — основные причины ошибочных результатов.

Программное обеспечение web-сервера, обеспечивающее консоль конфигурации для многих сетевых устройств — печально известная причина ошибочных результатов; вместо возврата стандартного сообщения об ошибке о несуществующих файлах «404» эти системы часто возвращают успешное сообщение для любого файла, запрашиваемого у системы. В ответ на это почти во всех инструментах оценки была разработана определенная форма «снятия отпечатков» web-сервера, позволяющих системе «обходить» эти web-серверы. Спектр таких программных решений простирается от весьма устойчивых (например, имеющихся в последних версиях Nessus Security Scanner) до не заслуживающих особого внимания, имеющихся в определенных коммерческих программных продуктах.

Ограничения автоматизации

Программные инструментальные средства оценки уязвимости систем не заменят аудита защиты, выполняемого рабочей группой профессиональных специалистов по системной защите. Несмотря на то, что многие инструменты оценки делают все возможное для обнаружения распространенных слабых мест во всех открытых службах, сравнительно несложные для обнаружения слабые места часто пропускаются. Пользовательские web-приложения, написанные в рамках жестких сроков для небольших пользовательских баз, часто выполняют неадекватные проверки защиты пользовательских данных, однако автоматизированные системы оценки могут не обнаружить этих недостатков. Несмотря на то, что шансы на обнаружение слабых мест в таком программном обеспечении со стороны автоматизированных средств очень малы, аналитик по системной защите, имеющий опыт тестирования web-приложений, может за короткое время точно определить аспекты защиты. Тот факт, что при автоматизированной оценке не обнаруживаются слабые места защиты, не означает, что их не существует.

Резюме

Число выявляемых слабых мест с каждым днем увеличивается, и поддерживать сетевую защиту становится сложнее. Для многих организаций оценка уязвимости становится предпочтительным способом обработки упущений сетевой защиты. Возможность оперативной идентификации неправильно сконфигурированных систем, а также простота использования и точность многих инструментов оценки изменили методику работы многих сисадминов. Оценка сетевой уязвимости обеспечивает широкий обзор слабостей защиты той или иной сети, дополняемый программными решениями оценки хостов, обеспечивающими шаги по упрочению защиты критичных систем.

Традиционный процесс упрочения систем и применения патчей ушел в прошлое, поскольку количество слабых мест превышает количество, которое может обработать большинство администраторов, особенно в разнородных сетях. На помощь пришли автоматизированные системы оценки, как автономные, так и получаемые по подписке. Администратору средней руки теперь не нужно быть «докой» в вопросах защиты для поддержания безопасности своей системы. Тот же повторяемый процесс позволяет администраторам отслеживать, устранять и верифицировать слабые места.

Хотя все инструменты оценки заявляют о своей способности обнаруживать и документировать все критичные слабые места, проекты этих систем и методики, используемые при тестировании на уязвимость, очень разнообразны. Не все программы оценки спроектированы одинаково; инструменты, в которых используется административный подход, — полезны, когда речь идет об идентификации слабых мест в сетевых устройствах и в крупных сетях. В то же время, инструменты, использующие внешний подход, ограничены техническими пределами самих слабых мест системы и часто игнорируют слабые места, которые не могут протестировать. К счастью, многие из более популярных программных решений консолидировались вокруг смешанного подхода к тестированию слабых мест систем, что обеспечило беспрецедентные уровни точности и проверки «в глубину».

Методы оценки уязвимости — не панацея защиты; несмотря на то, что они демонстрируют великолепное обнаружение слабых мест в многочисленных программных продуктах, пропущенными могут быть и сравнительно несложные для обнаружения дефекты. Существующий рынок инструментов оценки часто сталкивается с проблемами сетевых устройств, с медленнодействующими каналами связи Интернет и пользовательскими приложениями. Независимо от того, какой инструмент используется, ошибочные результаты всегда будут представлять собой серьезную проблему. Хотя многие программные решения и достигли значительных успехов в ее устранении, обратно портированные патчи и идентификаторы неизвестных версий гарантируют, что она никогда не исчезнет бесследно. Глубина и гибкость оценки уязвимости вручную всегда будет лучше любого автоматизированного решения: ни одна программа не заменит опытного аналитика, вручную осуществляющего мониторинг систем, сетевой архитектуры и корпоративных программных приложений.

Краткое резюме по разделам

Что такое оценка уязвимости системы?

- ☑ Уязвимостью называется любой недостаток системы, который злоумышленники могут использовать для получения доступа к ней или к сети.
- ☑ Методы оценки уязвимости обеспечивают снимок состояния защиты сети.
- ☑ Оценка хостов предоставляет подробную информацию о слабостях системы.
- ☑ При сетевой оценке обнаруживаются дефекты, которые могут быть использованы злоумышленниками для проникновения в сеть.

Автоматические системы оценки

- ☑ На сегодняшний день методы оценки вручную не целесообразны для крупных сетей из-за огромного количества существующих слабых мест защиты систем.
- ☑ Автономные и подписные модели оценки имеют ярко выраженные преимущества.
- ☑ Автоматизированные оценки уязвимости стремятся придерживаться одного и того же процесса, независимо от используемого инструментального средства.
- ☑ Процесс оценки представляет собой пошаговый сбор информации.

Два подхода

- ☑ Два разных инструмента оценки уязвимости дают совершенно разные результаты в зависимости от используемого подхода.
- ☑ Административный подход — наиболее безопасный, но не всегда самый надежный.
- ☑ Внешний подход обеспечивает администратора той же информацией, которую может получить злоумышленник.
- ☑ Для максимального охвата всех возможных слабых мест устойчивые инструменты оценки используют смешанный (или гибридный) подход.

Реалистические виды на будущее

- ☑ В корпоративной сети среднего размера оценка уязвимости может вызвать массу побочных эффектов.
- ☑ Последствия оценок часто не идеальны.
- ☑ Ошибочные результаты всегда будут представлять проблему, однако более современные инструментальные средства делают успехи в ее решении.

- ☑ Аудит сетевой защиты вручную дает лучшие результаты, нежели с помощью любых программных средств оценки.
- ☑ Испытания на проникновения обеспечивают более глубокий и широкий взгляд на сеть с точки зрения злоумышленников.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма «**Ask the Author**»). Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: *Я планирую использовать в своей организации программу оценки системной защиты. Есть ли смысл в доступе к внутренним сетям так же, как и к внешним?*

О: Несмотря на то, что системы, подключенные к Интернет, всегда должны быть включены в план оценки уязвимости, внутренняя оценка может фактически снизить риск для организации. При появлении нового компьютерного червя, который эксплуатирует одно или несколько слабых мест системы, первое, что необходимо сделать в организации, — это защитить все внешние и внутренние системы. Внутреннюю оценку можно использовать для верификации того, что ни одно из внутренних устройств не подвержено риску нападения. Внутренние сети чувствительны к заражению со стороны пользователей, дискредитированных через их почтовых клиентов и web-браузеры; результатом заражения сегмента внутренней сети может стать полная остановка деятельности компании. Кроме этого, неэтичные консультанты, раздраженные сотрудники и посетители сети могут использовать незащищенные системы для получения доступа к информации.

В: Чем различаются оценка уязвимости и испытание на проникновение?

О: Одной из самых серьезных проблем сферы безопасности является последовательное именование сетевых служб. Дело в том, что многие, не совсем честные компании, занимающиеся вопросами системной защиты, продают «тесты на проникновение», которые на самом деле не являются ничем иным, как оценкой уязвимости с помощью автоматизированных инструментов. Оценка уязвимости сети — это процесс идентификации ее слабых мест, а испытание на проникновение направлено на фактическое получение несанкционированного доступа к тестируемым системам и использование этого доступа к сетевым данным так, как нужно клиенту. Испытание на проникновение — замечательный способ определения того, насколько хорошо меры системной защиты реагируют на реальную атаку, а также того, что именно злоумышленник может дискредитировать, однако оно не проводит подробного анализа каждой системы в сети.

В: Можно ли при оценке на уязвимость обнаружить пользователей со слабыми паролями?

О: Несмотря на то, что методы оценки на уязвимость могут включать в себя аудит паролей, автоматизированные инструменты оценки редко выявляют расхожие или слабые пароли. Причиной этого является не то, что эти инструменты плохо разработаны в техническом плане для выполнения проверки, а в том, что результатом процесса тестирования каждого пользователя может стать блокирование учетной записи. Как правило, это происходит с доменами Windows, но может применяться и ко многим коммерческим системам UNIX. Тогда как некоторые автоматизированные инструменты будут тестировать учетные записи с паролем по умолчанию или без пароля, они не смогут обнаружить учетные записи с простым паролем, состоящим из одного символа. Наконец, автоматизированные инструменты могут замедлить работу тестируемого приложения или сети. Это та часть процесса оценки защиты, которую необходимо очень тщательно координировать с администраторами для достижения максимального успеха с минимальными негативными последствиями для пользователей.

В: В моей организации используется система предупреждения несанкционированного проникновения (IPS). Какие сложности она может вызвать при оценке на уязвимость?

О: Цель IPS — заблокировать «нехороший» трафик до того, как он достигнет потенциально незащищенной системы. Многие средства автоматизированной оценки зависят от способности отправки специально разработанной пробной атаки и определения уязвимости системы путем анализа полученного ответа. Если IPS блокирует первоначальный пробный запрос, то оценка уязвимости не сможет с точностью определить слабое место. Эту проблему можно решить либо специальным конфигурированием IPS на игнорирование трафика, исходящего из инструмента оценки, либо запуском инструмента с защищенной части IPS. Большинство инструментов оценки не приспособлены к обходу этих систем, однако квалифицированный взломщик может легко обнаружить IPS и найти способ эксплуатации слабого места в обход блокировки IPS. О том, как можно избежать обнаружения проникновения и предупреждения атаки, можно написать отдельную книгу; здесь же достаточно сказать: то, что обнаруживает IPS, может не быть тем, чем пользуется злоумышленник для успешной эксплуатации слабых мест сетевой защиты.