



DominoTM

версий 5 и 6

Администрирование сервера

сканировал: Alex
вычитал: wector
благодарность: Роби :)
январь 2004

УДК 004.658
ББК 32.973.202-018.2
К43

К43 Кирклэнд Р.

Domino 5 & 6. Администрирование сервера: Пер. с англ. - М.: ДМК Пресс, 2003. - 832 с: ил. (Серия «Администрирование и защита»).

ISBN 5-94074-224-6

Книга посвящена вопросам использования сервера Domino и системы Notes в корпоративной среде. Здесь анализируются возможности системы Notes и делается особый акцент на новые функции, появившиеся в версиях R5 и R6. Подробно описываются методы администрирования сервера Domino, в частности методы управления почтовой службой, репликацией и обеспечением безопасности. Рассматриваются вопросы обслуживания клиентов Notes и соответствующих баз данных, причем представлена только необходимая информация и практические рекомендации. Также рассказывается о поиске оптимальных режимов работы сервера, обеспечении его более эффективного применения в различных ситуациях и о связи сервера с другими источниками данных.

Издание ориентировано на администраторов системы Notes/Domino, осуществляющих переход с версий R3/R4 на версии R5/R6, однако и начинающие администраторы систем смогут с помощью этой книги получить знания, необходимые для выполнения повседневной работы квалифицированно и в кратчайшие сроки.

ББК 32.973.202-018.2

Authorized translation from the English language edition, entitled Domino System Administration, 1st Edition by Kirkland, Rob, published by Pearson Education, Inc, publishing as New Riders.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc.

RUSSIAN language edition published by DMK Press, Copyright © 2003.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельца авторских прав.

Материал, изложенный в данной книге, многократно проверен. Но, поскольку вероятность технических ошибок все равно остается, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможный ущерб любого вида, связанный с применением содержащихся здесь сведений.

Все торговые знаки, упомянутые в настоящем издании, зарегистрированы. Случайное неправильное использование или пропуск торгового знака или названия его законного владельца не должно рассматриваться как нарушение прав собственности.

ISBN 1 -56205-948-3 (англ.)
ISBN 5-94074-224-6 (рус.)

Copyright © by New Riders Publishing
© Перевод на русский язык, оформление.
ДМК Пресс, 2003



Содержание

Предисловие.....	21
Введение.....	28

ЧАСТЬ I

Подготовка к использованию и установка версий 5 и 6.....	33

Глава 1

Характеристики сервера Lotus Domino версий 5 и 6.....	34

Характеристики сервера Domino и система Notes.....	34

Архитектура клиент/сервер.....	35

Архитектура баз данных.....	36

Обмен сообщениями, поддержка календаря и планирование.....	37

Службы каталога.....	39

Распределенная архитектура и репликация.....	40

Обеспечение безопасности.....	41

Поддержка мобильных пользователей.....	42

Поддержка нескольких компьютерных платформ.....	42

Обеспечение доступа к данным.....	43

Формирование интегральной среды проектирования.....	44

Расширения и надстройки.....	44

Web-сервер.....	44

Web-браузеры.....	45

Управляющие программные инструменты.....	46

Приложения системы Notes.....	47

Формирование и передача сообщений.....	47

Управление персональной информацией.....	48

Дискуссионные форумы.....	49

Информационные репозитории.....	49

Отслеживание приложений.....	50
Приложения для рабочих потоков.....	50
Web-приложения.....	51
Состав версий 5 и 6.....	51

Глава 2

Планирование и установка.....	54
Процедура развертывания сервера Domino.....	54
Технические требования.....	55
Подбор группы.....	56
Оценка необходимых ресурсов.....	57
План проекта.....	58
Пилотный проект.....	59
Встраивание сервера Domino в существующую инфраструктуру.....	59
Оценка будущего использования системы.....	60
Интеграция сервера Domino в сетевую инфраструктуру.....	60
Сетевые протоколы.....	69
Конфигурации аппаратных средств: требуемые модификации аппаратных и программных средств.....	71
Формирование внутренней инфраструктуры.....	76
Структура: домены, организации, именованные сети.....	77
Организации.....	81
Взаимосвязь между доменами и организациями.....	85
Именованные сети Domino.....	87
Проблемы обеспечения безопасности.....	89

Глава 3

Процедура установки и настройка первого сервера.....	91
Установка программного обеспечения сервера Domino.....	91
Конфигурирование первого сервера Domino.....	95
Задание организационных единиц для первого сервера.....	95
Конфигурирование первого сервера R5.....	103
Параметры конфигурирования сервера Domino, третий экран.....	106
Параметры конфигурирования сервера Domino, четвертый экран.....	108
Параметры конфигурирования сервера Domino, последний экран.....	112
Конфигурирование первого сервера R6.....	113
Запуск первого сервера.....	116

Установка учетной записи первого пользователя.....	117
Интерфейс программы Domino Administrator.....	120
Завершение процедуры конфигурирования первого сервера.....	121
Настройка портов.....	122
Настройка именованных сетей.....	123
Создание административных групп.....	124
Настройка службы Administration Process.....	126
Заполнение полей с параметрами доступа к серверу.....	130
Заполнение других серверных полей.....	133
Рекомендации по выполнению дополнительных операций.....	137
Прочие рекомендации.....	145

Глава 4

Установка дополнительных серверов.....	152
Установка других серверов.....	152
Регистрация идентификационных данных сервера.....	152
Процедуры установки.....	156
Установка модемных соединений.....	163
Настройка порта.....	166
Создание документа соединения.....	171
Установка сквозных серверов.....	176
Установка процедуры репликации.....	177
Установка процедуры маршрутизации почтовых сообщений.....	179
Установка процесса администрирования.....	180
Установка менеджера агентов.....	185
Настройка процедуры регистрации транзакций.....	186
Специальные серверы.....	187
Серверы почтовой службы.....	187
Серверы приложений.....	187
Серверы коммутируемого доступа и сквозные серверы.....	188
Концентраторы почтовой службы и репликации.....	188
Серверы с коллективным использованием браузера.....	189
Серверы сети Internet.....	190
Серверы-брандмауэры.....	191
Серверы каталога.....	191
Каталог домена и служба поиска.....	193

Глава 5

Процедура регистрации пользователей и настройки клиентов... 195

Создание профиля установки пользователей.....196

Создание профиля установки в версии R6.....201

Подготовка списка управления исполнением для режима
по умолчанию.....203

Сертификаторы для организационной единицы.....206

Альтернативные имена и языки.....206

Добавление альтернативного языка
в идентификационные данные сертификатора.....208События, связанные с добавлением нового языка
в идентификационные данные сертификатора.....209

Регистрация основных параметров пользователя.....210

Предварительные условия для регистрации.....211

Задание параметров по умолчанию для осуществления регистрации.....211

Заполнение регистрационной формы.....213

Поля диалогового окна регистрации сотрудника.....217

Добавление информации для восстановления
в идентификационные данные сертификатора.....223

Создание базы данных входящих почтовых сообщений.....225

Создание документа базы данных входящих почтовых сообщений.....227

Создание формы и вида.....227

Добавление информации о восстановлении
в идентификационные данные сертификатора.....231

Экспорт информации о восстановлении существующим пользователям ... 232

Первоначальная установка и настройка клиента Notes.....233

Установка клиентов системы Notes.....233

Процедура конфигурирования клиента Notes.....238

Другие рекомендации по проведению настройки для пользователей 239

Глава 6

Дополнительная настройка клиентов.....241

Расширенные режимы регистрации пользователей.....241

Регистрация с использованием текстового файла.....242

Регистрация пользователей Windows NT
в качестве пользователей системы Notes.....245

Обновление других почтовых программ и служб поддержки календаря	254
Автоматизация процедуры установки клиента Notes.....	257
Проведение установки пользователей со специальными требованиями ...	263
Установка мобильных пользователей.....	263
Настройка сквозного сервера.....	288
Подготовка доступа к серверам не-Domino.....	289
Настройка рабочей станции для совместного использования.....	302

ЧАСТЬ II

Обеспечение поддержки и поиск неисправностей.....305

Глава 7

Обновление сервера Domino версий 4.x и 5.x

и переход к версии 6.0.....306

Планирование и подготовка к обновлению.....	306
Проверка аппаратных средств.....	306
Проведение моделирования.....	307
Проведение обучения и организация тренингов.....	310
Процедура установки программного обеспечения R6 поверх программного обеспечения версий 4 и 5.....	311
Обновление баз данных, каталогов, функций поиска, обеспечения безопасности и контроля.....	312
Обновление баз данных.....	313
Обновление баз данных почтовой службы.....	313
Формирование обратного адреса сети Internet.....	315
Обновление поддержки каталога и каскадных книг адресов.....	316
Функции просмотра домена и перечня базы данных.....	317
Обновление системы безопасности.....	319
Программные средства мониторинга.....	320
Другие новые функции.....	322

Глава 8

Настройка и поддержка процедуры маршрутизации

почтовых сообщений.....323

Планирование процедуры маршрутизации почтовых сообщений.....	324
Домены системы Notes.....	324
Именованные сети системы Notes.....	325

Осуществление маршрутизации почтовых сообщений серверами Domino.....	326
Маршрутизация почтовых сообщений по протоколу NRPC.....	327
Маршрутизация почтовых сообщений по протоколу SMTP.....	341
Совместное использование сервером Domino маршрутизации SMTP и Notes.....	344
Настройка процедуры маршрутизации почтовых сообщений.....	346
Настройка маршрутизации почтовых сообщений по протоколу NRPC.....	346
Настройка маршрутизации почтовых сообщений SMTP.....	352
Подключение доменов системы Notes к сети Internet.....	355
Настройка календаря и расписания.....	364
Принцип работы календаря и расписания.....	364
Формирование базы данных Resource Reservations.....	365
Разрешение междоменного группового расписания в документе домена.....	368
Документы выходного дня.....	368
Проверка базы данных Free Time.....	369
Настройка и поддержка совместно используемой почтовой службы.....	369
Принципы работы совместной почтовой службы.....	370
Настройка совместной почтовой службы.....	372
Операции поддержки совместно используемой почтовой службы.....	373
Тонкая настройка маршрутизации почтовых сообщений в документах конфигурации.....	380
Настройка основных параметров.....	382
Установка ограничений.....	383
Блокирование сквозной почты через домен.....	384
Контроль соединений хостов.....	385
Блокирование входящих почтовых сообщений.....	386
Ограничение приема почтовых сообщений из сети Internet.....	386
Управление исходящими почтовыми сообщениями.....	386
Управление доставкой почтовых сообщений.....	387
Управление пересылкой почтовых сообщений.....	387
Использование входящих команд протокола SMTP.....	388
Использование исходящих команд протокола SMTP.....	389
Настройка функций вспомогательного управления.....	389

Управления передачей сообщений.....	390
Настройка режима передачи/доставки сообщений.....	390
Указание пути к файлу описания события.....	390
Использование формата MIME серверами Domino и системой Notes.....	391
Мониторинг и диагностика работы почты.....	400
Программа Domino Administrator.....	400
База данных Notes Log.....	401
База данных Outgoing Mail.....	402
Программные инструменты для сбора статистических данных, формирования отчетов и осуществления контроля.....	404
Команда консоли для вывода статистических данных.....	404
Задача статистических данных сервера.....	404
Задачи сбора данных и контроля события.....	405
Почтовые зонды.....	405
Отслеживание маршрутов почтовой службы.....	407
Отслеживание обычных/почтовых сообщений.....	408
Подготовка отчетов об использовании почтовых сообщений.....	412

Глава 9

Процедура репликации данных.....	414
Описание механизма репликации данных.....	415
Операции, выполняемые в процессе репликации данных.....	417
Расписание репликации для двух серверов.....	419
Осуществление репликации для двух серверов по требованию.....	422
Выполнение репликации для сервера и рабочей станции.....	423
Топологии репликации.....	425
Репликация и списки ACL баз данных.....	427
Формирование расписания репликации данных.....	430
Пропуск операций репликации.....	430
Избирательная репликация данных.....	432
Конфликтные ситуации, возникающие при репликации и сохранении документов.....	438
Правила разрешения конфликтных ситуаций.....	439
Разрешение конфликтных ситуаций вручную.....	440

Создание новых реплик.....	441
Создание реплик баз данных на серверах: предварительные замечания	442
Использование процесса Administration Process для создания новых реплик баз данных.....	443
Создание новых реплик баз данных вручную.....	443
Формирование новой реплики на рабочей станции системы Notes.....	446
Удаленные документы, заготовки удаления и очистка баз данных	446
Мониторинг репликации.....	449
Программные инструменты для графического мониторинга.....	455

Глава 10

Защита информации.....	456
Аутентификация.....	456
Принцип работы аутентификации по имени и паролю.....	458
Принцип работы аутентификации на основе сертификата.....	458
Ключи шифрования: шифрование, подписи и идентификация.....	459
Принцип работы системы Notes proprietary.....	463
Принцип кросс-сертификации Notes.....	464
Принцип работы аутентификации SSL.....	471
Защита сервера.....	472
Физическая защита, сетевая защита и защита операционной системы	473
Управление доступом к серверу Domino.....	475
Защита базы данных.....	480
Список управления доступом к базе данных.....	481
Просмотр списков доступа.....	491
Списки доступа формы.....	491
Поля \$Readers, Readers и Authors.....	492
Ограничение доступа к частям документа.....	492
Шифрование локальной базы данных.....	493
Защита рабочей станции.....	494
Список управления исполнением программ.....	494
Защита данных на рабочей станции.....	500
Защита SSL в Domino и Notes.....	502
Получение статуса заверителя.....	503
Настройка сервера Domino для использования протокола SSL.....	509
Применение SSL и S/MIME пользователями Notes.....	510

Глава 11

Службы каталога Domino.....	513
Каталог Domino.....	514
Настройка первичного каталога Domino.....	515
Вторичные каталоги Domino.....	518
LDAP-службы каталогов.....	519
Что такое LDAP.....	521
Настройка службы LDAP сервера Domino.....	522
Расширение и мониторинг служб LDAP.....	527
Несколько каталогов.....	528
Порядок просмотра каталогов.....	529
Перечень каталогов.....	531
Установка перечня каталогов.....	531
Поддержка каталога.....	543
Установка, репликация и идентификация базы данных	
Directory Assistance.....	543
Установка Directory Assistance для вторичных каталогов Domino.....	546
Установка Directory Assistance для LDAP-каталогов.....	548
Серверы каталогов.....	550

Глава 12

Обслуживание пользователей и устранение неполадок.....	552
Переименование пользователей.....	552
Этапы работы AdminP при переименовании пользователя.....	554
Обновление в иерархии.....	555
Изменение общего имени.....	556
Перемещение пользователей.....	559
Удаление пользователей.....	561
Инициирование запроса Delete Person.....	561
Устранение неполадок.....	564
Восстановление утерянных паролей.....	564

Глава 13

Поддержка клиентов и устранение неполадок.....	566
Клиентские средства устранения неполадок.....	566
Проверка IP-соединения.....	567

Отслеживание соединения из клиента Notes.....	568
NotesCONNECT.....	569
NotesPeek.....	571
Графический интерфейс пользователя.....	573
Начальная страница.....	573
Редактирование начальной страницы.....	573
Управление начальной страницей.....	575
Замена начальной страницы.....	577
Использование в R5/6 рабочего пространства стиля R4.....	578
Предпочтения пользователей.....	579
Динамические профили установки пользователей.....	580
Изменение почтовой службы.....	581
Почтовые правила.....	581
Автоматическая проверка орфографии.....	583
Дополнительные параметры для почты, календаря и делегирования.....	584
Дополнительные утилиты на Notes CD: Помощник Notes.....	584
Дополнительные утилиты на Notes CD: Actioneer.....	585
Подписка на документы.....	585
Управление системными файлами Notes.....	586

Глава 14

Поддержка баз данных и устранение неполадок.....	588
Развертывание приложения.....	588
Добавление новой базы данных на сервер.....	590
Начальная настройка свойств базы данных.....	591
Управление базой данных с помощью вкладки Files окна Domino Administrator.....	592
Использование инструментов базы данных.....	594
Управление списками ACL базы данных.....	595
Создание реплик нескольких баз данных.....	595
Уплотнение для освобождения пространства.....	596
Улучшение производительности базы данных.....	599
Использование квот для поддержания размера базы данных.....	602
Перенос базы данных на новый сервер.....	604
Перенос базы данных вручную.....	604

Использование инструмента Move.....	604
Перетаскивание.....	605
Защитная подпись.....	606
Временная отмена репликации.....	606
Восстановление поврежденных баз данных с помощью Fixup.....	607
Идентификация документов из журнала регистрации.....	610
Ссылки на каталоги и базы данных.....	610
Мониторинг и анализ активности базы данных.....	611
Использование Statlog для мониторинга активности.....	612
Анализ базы данных.....	613
Регистрация транзакций.....	615
Установка регистрации транзакций.....	616
Отмена регистрации транзакций для одной базы данных.....	618
Восстановление после сбоя системы или сбоя носителя.....	618
Поддержка индексов баз данных.....	619
Установка полнотекстовых индексов для поиска в базах данных.....	619
Использование задачи Update.....	621
Запуск Updall.....	621
Запуск с клавиатуры.....	623
Администрирование каталога баз данных.....	623
Создание каталога баз данных.....	623
Настройка списка ACL.....	624
Назначение категорий.....	624
Сокращение размера каталога баз данных.....	625
Удаление базы данных из каталога.....	625
Поиск в домене.....	625
Сервер каталога домена.....	625
Каталог домена.....	626
Настройка индексации файловой системы.....	626
Включение базы данных в индекс домена.....	627
Библиотеки баз данных.....	628
Создание библиотеки.....	628
Назначение библиотекарей.....	629
Публикация базы данных.....	629
Управление кэш-памятью баз данных.....	629

Глава 15

Установка Web-сервера, поддержка, настройка и устранение неполадок.....	632
Новые функции HTTP-сервера Domino R5.....	632
Новые функции HTTP-сервера Domino R6.....	633
Обзор стека HTTP сервера Domino.....	634
Почему Domino используется как HTTP-сервер.....	634
Как работает Domino.....	635
Установка HTTP.....	636
Установка HTTP на рабочем сервере Domino.....	637
Документы виртуального сервера.....	651
Использование документов защиты файлов.....	652
Использование документов отображения/переедресации.....	654
Использование Web-областей.....	656
Использование HTTP-стека Microsoft IIS.....	658
Средства, поддерживаемые Domino for IIS.....	658
Минимальные требования к Domino for IIS.....	660
Настройка IIS для поддержки Domino for IIS.....	660
Обзор защиты Domino for IIS.....	665
Настройка защиты Domino for IIS.....	668
Точная настройка.....	668
Отмена регистрации на HTTP-сервере.....	670
Оптимизация производительности HTTP-сервера на основании его активности.....	670
Создание кластера Web-сервера Domino.....	671
Настройка кэш-памяти.....	671
Настройка сетевых тайм-аутов.....	672
Настройка числа потоков сервера.....	673
Побайтная загрузка файлов.....	673
Задание метода переедресации URL.....	674
Ограничение объема данных, передаваемых серверу.....	674
Использование чересстрочной/прогрессивной развертки изображений ...	675
Ограничение числа строк, отображаемых на виде.....	675
Ограничение числа результатов поиска.....	676

Устранение неполадок.....	676
Проблемы доступа по протоколу HTTP.....	677
Пользователи не могут получить доступ к Web-серверу.....	678
Программные инструменты устранения неполадок.....	680
 Глава 16	
Почтовая служба POP3.....	686
Почта POP3 и Domino.....	686
POP3 или IMAP.....	687
Настройка протокола POP на сервере Domino.....	687
Настройка TCP/IP.....	688
Настройка POP3.....	688
Дополнительная настройка, необходимая для секционированного сервера.....	690
Запуск задачи сервера POP3.....	690
Регистрация пользователей POP3.....	691
Настройка почтового программного обеспечения пользователей.....	692
Настройка службы POP3.....	693
Контроль работы службы POP3.....	694
 Глава 17	
Почтовая служба IMAP.....	695
IMAP или POP.....	696
Почта IMAP и Domino.....	697
Установка IMAP на сервере Domino.....	697
Настройка TCP/IP.....	698
Настройка IMAP.....	698
Дополнительная настройка, необходимая для секционированного сервера.....	699
Запуск задачи сервера IMAP.....	699
Регистрация пользователей IMAP.....	700
Разрешение доступа IMAP к почтовым базам данных Notes.....	702
Настройка почтового программного обеспечения пользователей.....	702
Настройка службы IMAP.....	703
Контроль работы службы IMAP.....	704

ЧАСТЬ III

Оптимизация сервера.....	705

Глава 18

Мониторинг сервера.....	706
Почему важен мониторинг системы.....	706
Инструменты идентификации.....	707
Среда.....	709
Отслеживание использования.....	709
Определение базы.....	709
Средства мониторинга Windows NT.....	710
Диагностика Windows NT.....	710
Диспетчер задач.....	711
Системный монитор.....	712
Термины.....	713
Добавление объекта Domino и счетчиков.....	716
Запуск Системного монитора.....	716
Виды монитора производительности.....	718
Итоговые таблицы объектов и соответствующих счетчиков.....	719
Использование NT Resource Kit.....	724
Средства мониторинга Domino.....	725
Консоль сервера Domino.....	726
Включение и настройка отчетности.....	727
Серверные задачи.....	727
Мониторинг Domino из Domino Administration.....	736
Предпочтения администрирования.....	736
Свойства сервера.....	737
Информация на вкладке Status.....	738
Информация на вкладке Analysis.....	739
Информация на вкладке Monitoring.....	740
Информация на вкладке Statistics.....	742
Web Administrator.....	743
Утилита Mean Time Between Failure от Iris.....	747
Контроль соединений между сервером Domino и клиентом Notes.....	747

Глава 19

Настройка производительности	750
Компоненты	750
Аппаратное обеспечение	751
Операционные системы	753
Программное обеспечение Notes/Domino	755
Параметры notes.ini, влияющие на производительность	757
Задачи сервера	760
Задачи Multiple Replicator и Mail Router	760
Параметры, улучшающие производительность баз данных и каталогов	761
Дополнительные свойства баз данных, влияющие на производительность	762
Инструменты производительности, поставляемые с Notes R5/6	764
Тест NotesBench	766
Описание рабочих нагрузок	766
Дополнительные средства сторонних разработчиков	770
ProActive Assistant от G2 Associates	770
GroupSizr Pro, WebSizr и MailSizr от Technovations	770
IntelliWatch Pinnacle от Candle	771
Производительность сети	771
Протокол	771
Сетевая карта	771

Глава 20

Повышение доступности данных	772
Кластеры серверов Domino	773
Описание	773
Планирование, установка и настройка	782
Администрирование	785
Использование кластеров	789
Статистика	789
Использование Microsoft Cluster Server	794
Сегменты сервера Domino	797
Описание	798
Планирование, установка и настройка	798

20. DOMINO 5 & 6. АДМИНИСТРИРОВАНИЕ СЕРВЕРА

Настройка.....	800
Использование секционированных серверов в кластере Domino.....	803
Техническое обслуживание и мониторинг.....	803
Удаление.....	805
Счета и аудит.....	806
Описание.....	806
Планирование и установка.....	807
Использование счетов.....	807
Новые улучшенные службы R5/6.....	808
Менеджер кластеров Internet.....	808
Управление и мониторинг ICM.....	815
Предметный указатель.....	818

ЧАСТЬ I



ПОДГОТОВКА
К ИСПОЛЬЗОВАНИЮ
И УСТАНОВКА
ВЕРСИЙ 5 и 6

ГЛАВА

1

ХАРАКТЕРИСТИКИ СЕРВЕРА LOTUS DOMINO ВЕРСИЙ 5 и 6

Для эффективного управления системой Domino/Notes пользователь, несомненно, должен быть хорошо знаком с основными методами администрирования, описанию которых посвящено настоящее издание. Кроме того, пользователю следует ясно представлять себе характеристики и возможности соответствующих программных средств, а также лицензирование системы Notes/Domino. В данной главе приводятся важные сведения относительно сервера Domino версий R5 и R6, которые рекомендуется твердо усвоить, прежде чем переходить к решению собственно задач администрирования.

Характеристики сервера Domino и система Notes

Первые три версии Notes представляли собой практически полностью замкнутые системы. При этом пользователю требовалось применять клиент системы Notes для передачи данных на ее сервер. (Пользователи, конечно, имели возможность создавать собственные клиентские программы на основе соответствующих интерфейсных программ и с помощью языков программирования C, C++ и Visual Basic, поддерживаемых программными продуктами компании Lotus, или же специальной программы подготовки для пакета LotusScript, получившей название Lotus Notes ViP. В этом случае, однако, нельзя применять стандартные клиенты, например Web-браузеры.) Характеристики системы Notes, реализованные в упомянутых версиях, можно рассматривать как своего рода базовые функции системы Notes, а приложения, реализуемые с помощью данной системы, соответственно как базовые приложения системы Notes.

Эти базовые функции включают в себя совместное использование документно-ориентированных баз данных и формирование сообщений, обеспечение строжайшей безопасности, распределенное хранение данных в условиях их синхронной репликации, поддержку временно отключенных от проводной сети мобильных пользователей системы Notes и предоставление доступа к данным, расположенным вне системы Notes. К упомянутым приложениям относятся информационные репозитории, дискуссионные форумы, приложения для отслеживания работы над конкретными проектами и бизнес-процессами, а также приложения «рабочих потоков организаций».

Многим из тех организаций, которые работают в наши дни с сервером Domino и системой Notes, достаточно перечисленных выше базовых функций. Однако уже после создания версии 3 сотрудникам компании Lotus и другим специалистам стало очевидно, что развивающаяся сеть Internet в ближайшее время заметно изменит существующие подходы к ведению бизнеса. Специалисты уже тогда оценили огромный потенциал зарождающихся в сети Internet службы электронной почты (в ее стандартных вариантах - почтовые службы на основе протоколов SMTP/MIME), дискуссионных форумов (группы новостей Internet) и информационных репозиториях (World Wide Web), которые, по их мнению, могли послужить целям дальнейшего развития системы Notes.

Сотрудники компании Lotus видели в формирующихся тенденциях большие возможности для расширения рынка применения системы Notes и превращения ее в весьма мощную платформу для поддержки приложений сети Internet. В результате компания Lotus начала разработку версий 4.x, 5.x и 6.x системы Notes, причем эти версии все более ориентировались на использование возможностей сети Internet и позволили заметно расширить функции соответствующего сервера и клиентов (именно вследствие увеличения функциональных возможностей серверу было присвоено индивидуальное название Domino). Одновременно базовые приложения системы пополнились приложениями еще одного типа - Web-приложениями.

Ниже приводятся основные характеристики системы Notes:

- О поддержка архитектуры клиент/сервер;
- О поддержка архитектуры нереляционных, объектно-ориентированных баз данных;
- О формирование и передача сообщений;
- О поддержка распределенной архитектуры и репликация данных;
- О обеспечение безопасности;
- О поддержка мобильных пользователей;
- О поддержка различных компьютерных платформ;
- О обеспечение различных вариантов доступа к данным;
- О создание интегральной среды разработки;
- О поддержка расширений и надстроек;
- О поддержка Web-сервера;
- О поддержка Web-браузеров;
- О поддержка службы каталога;
- О обеспечение гибкого управления.

Архитектура клиент/сервер

С самого начала базы данных системы Notes основывались преимущественно на серверах Domino или Notes, а пользователи осуществляли доступ к данным с помощью клиентских программ (клиентов), запущенных на их рабочих станциях. Следует отметить, однако, что серверы Domino и Notes не являются файловыми серверами. Пользователи обращались не ко всей базе данных, а получали с серверов лишь затребованные ими наборы данных. Серверы извлекали эти наборы из баз данных и направляли их пользователям. Кроме того, пользователи сами передавали новую информацию на серверы, которые в свою очередь сохраняли ее в соответствующей базе данных. Подобный подход является классическим при создании и поддержке архитектуры клиент/сервер. Его цель - оптимизация режима, предусматривающего организацию совместного доступа к данным в условиях минимизации

сетевого трафика, путем отделения операций по запоминанию данных и управлению от операций представления данных.

Клиенты направляли запросы пользователей на сервер, в том числе и запросы на чтение и запись данных, обеспечивали форматирование принимаемых данных и их воспроизведение для пользователей.

Для версии 4.1 существовал только клиент Lotus Notes (хотя программисты имели необходимые возможности для создания собственных пользовательских программ на основе программных средств, ранее разработанных компанией Lotus и поставляемых ею на рынок). Начиная с версии 4.5 специалисты компании Lotus предложили улучшенный вариант доступа, который допускал применение типовых клиентских программ - в первое время браузеров, а позднее программ чтения почтовых сообщений сети Internet, новостей и данных в каталоге почтовой службы IMAP. В версии 5 и 6 нет никаких новых возможностей для клиентов по сравнению с версией 4.6. Однако в рамках этих новых версий предусматривается улучшение режимов взаимодействия между сервером Domino и клиентами, не относящимися к системе Notes. Так, например, начиная с версии 5 поддерживается каркас CORBA/IIOP, позволяющий программистам использовать функции системы Notes при работе с Web-браузерами. Предполагается также некоторое улучшение режима взаимодействия сервера Domino с серверами и клиентами, применяющими протокол LDAP.

Архитектура баз данных

Основой системы Notes является уникальный объект для хранения данных - файл NSF, с помощью которого реализуется функция хранения данных. Базы данных системы Notes иногда еще называют объектными хранилищами, поскольку они не хранят информацию в том виде, в котором это делают базы данных известных архитектур. Система Notes обеспечивает обработку различных типов информации, необходимой специалистам, причем эта информация на практике оказывается весьма разноплановой.

Большая часть архитектур баз данных хранит информацию в виде жестких структур, например таблиц. Любая запись в таблице должна иметь определенный набор полей, вне зависимости от присутствия в этих полях полезной информации. Каждому полю в записи выделяется определенный объем области памяти, который задается в виде описания поля еще до момента создания самих записей. Если формируемые данные требуют меньшего или большего объема памяти, ситуация заметно ухудшается, так как выделенный для поля объем памяти остается неизменным. Подобный подход весьма эффективен для больших массивов однотипных данных, поскольку он позволяет быстро выводить необходимые сведения. Однако он весьма далек от оптимального, когда требуется, например, запомнить большой объем разнородной информации.

Базы данных системы Notes являются функционально гибкими и в этом смысле лучше, чем базы данных с традиционной архитектурой. Каждая запись (называемая иногда строкой или документом) может иметь только те поля, которые реально содержат полезные сведения. В свою очередь каждое поле способно хранить столько информации, сколько пользователь намеревается ввести, для чего выделяется адекватный объем памяти. В данном случае две соседние записи базы данных совсем не обязательно должны обладать одинаковым набором полей. Пользователи могут в любое время добавлять новые поля в запись (как в момент создания записи, так и в более поздний период).

Для улучшения операции вывода подобной информации в базах данных системы Notes обеспечивается поддержка индексированных средств просмотра данных (так называемых

видов), для которых могут формироваться индексы полнотекстового поиска. Эти виды отображают табулированные матрицы данных, соответствующие каждой записи. Конкретная информация вида зависит от разработчика, который может быть как создателем самой базы данных, так и пользователем, имеющим доступ к базе на уровне не ниже **Reader** (Читатель).

Для каждой базовой версии специалисты компании Lotus создали оригинальную архитектуру баз данных, и версии 5 и 6 не составляют исключения. В версии R5 улучшена целостность базы данных, уменьшены затраты на ввод/вывод информации, полнее используются возможности центрального процессора и памяти. В результате удалось заметно усовершенствовать показатели масштабирования и управления базами данных.

В рамках версии 5 базы данных демонстрируют следующие новые возможности и характеристики:

- О максимальный размер базы данных 33 Гб;
- О выполнение регистрации транзакций, в процессе которой информация обо всех изменениях данных предварительно заносится в соответствующий журнал, а уже потом инициируется изменение самих данных; при возникновении сбоев во время записи в базу (что может повлечь разрушение данных) этот факт обнаруживается процедурой регистрации транзакций, автоматически восстанавливающей информацию в базе данных и тем самым гарантирующей целостность хранимых сведений;
- О резервирование баз данных в интерактивном режиме и применение интерфейсов прикладного программирования (API), которые разработчики приложений могут использовать в собственных программных продуктах для архивирования сведений;
- О интерактивное уплотнение базы данных на месте;
- О необязательное восстановления удаленных документов.

В версии R6 дополнительно реализованы следующие возможности баз данных:

- О оптимизация времени запуска сервера за счет улучшения использования основных видов баз данных;
- О ускорение согласования баз данных на разных серверах благодаря потоковой репликации;
- О улучшение взаимодействия клиентов и серверов вследствие более эффективного выполнения типичных команд;
- О сжатие передаваемых по сети данных, что позволяет увеличить утилизацию сети;
- О улучшенный двигатель формул, с помощью которого удастся почти в два раза ускорить обновление видов;
- О программы управления базами данных (например, compact, fixup, updall и design), которые теперь могут обеспечивать доступ на уровне не только серверов, но и каталогов.

Обмен сообщениями, поддержка календаря и планирование

Система Notes всегда предусматривала поддержку функций электронной почты, причем эти функции совершенствовались в течение целого ряда лет. Характерной особенностью данных функций является то, что все (а не только специально выделенные) базы данных системы Notes могут обмениваться документами. Поэтому почтовая служба Notes Mail выступает своего рода сопутствующим продуктом по отношению к базовым функциям обмена информацией, встроенным в сервер Domino и во все базы данных системы Notes.

Естественно, электронная почта считается весьма полезным приложением в современных сетях, поэтому компания Lotus никогда не относилась к почтовой службе системы Notes как к «побочному продукту». Они хорошо осведомлены о том, что во многих случаях сервер Domino активно используется для обмена почтовыми сообщениями, а также о том, что электронная почта каждой компании - это неотъемлемая часть ее сетевой инфраструктуры. В результате специалисты компании Lotus постоянно совершенствовали функции электронной почты и привнесли в них поддержку календаря и планирование (начиная с версии 4.5), а также обеспечили доступ к почтовой службе сети Internet (начиная с версий 4.5 и 4.6).

Одним из основных направлений маркетинговой деятельности компании Lotus для сервера Domino R5 была демонстрация его превосходства над другими программными продуктами с точки зрения инфраструктуры для передачи информационных сообщений. В рамках версии 5.0 были произведены следующие усовершенствования функций почтовой службы:

- о увеличены возможности масштабирования и производительность сервера.* Базы данных теперь содержат несколько почтовых ящиков, что приводит к улучшению масштабирования и производительности маршрутизации почтовых сообщений. Благодаря независимым серверам каталога (Directory server) удается перераспределить нагрузку при просмотре каталога так, чтобы почтовые серверы могли обслужить большее число пользователей;
- о повышена эффективность почтовой службы.* Сокращение времени на распознавание (разрешение) имен позволило ускорить процесс адресации сообщений, облегчить архивирование почты, улучшить работу интерфейсов, использовать каталог мобильных пользователей и просматривать календарь для несмежных доменов Domino;
- о улучшены показатели управляемости* за счет нового интерфейса администрирования, ориентированного на задачи, маршрутизации методом Pull (Вытягивание), отслеживания сообщений, управления маршрутизацией, а также применения средств борьбы с нежелательными сообщениями (спамом) и слишком большими по размеру сообщениями. Усовершенствованы отчеты;
- о увеличена согласованность со стандартами сети Internet*, в частности со стандартами SMTP и MIME, а также со стандартом S/MIME для передачи зашифрованных сообщений абонентам почтовой службы в сети Internet.

В версии R6 появились дополнительные улучшения службы обмена сообщениями:

- о усовершенствована маршрутизация почты.* Теперь маршрутизатор одного физического сервера Domino в состоянии поддерживать несколько организаций;
- о обеспечена установка правил для обработки сообщений.* В документе конфигурации сервера можно указать критерии и правила для обработки поступающих сообщений;
- о усовершенствовано управление почтовыми ящиками пользователей.* Введение квот на выделение дискового пространства позволяет точно управлять множеством почтовых ящиков, не задумываясь об объеме переписки каждого из абонентов;
- о улучшена функция пересылки сообщений через почтовый сервер.* Разрешено создание специальных правил, ограничивающих возможности пользователей по пересылке копий сообщений по нескольким почтовым адресам.

Службы каталога

В системе Notes во все времена обеспечивалось применение служб каталога, в которых содержались данные обо всех пользователях, серверах, группах и конфигурациях серверов системы Notes. В версии 3.x база данных каталогов получила название Public Name and Address Book (Книга общедоступных имен и адресов). В версии 4.x название было сокращено до Public Address Book (Книга общедоступных адресов). В версии 5 специалисты компании Lotus снова переименовали эту базу данных и в соответствии с существующей практикой формирования имен назвали ее Domino Directory (Каталог серверов Domino). До появления версии 5 все серверы Notes или Domino в соответствующих доменах хранили полные копии (реплики) подобной книги общедоступных адресов. Начиная с версии 5.1 сервер Domino более не нуждается в поддержке полной копии каталога Domino, а вместо этого поддерживает местный «непользовательский» каталог, который не содержит документов конкретных пользователей, баз данных входящих почтовых сообщений, ресурсов и групп.

Сервер или пользователь может получить доступ к нужной ему информации, хранящейся в указанных документах, путем просмотра данных сервера каталогов. В результате заметно уменьшается объем данных каталога сервера Domino, особенно в больших организациях с тысячами пользователей. Это также позволяет повысить эффективность, улучшить реакцию системы и масштабирование информационных потоков на почтовых серверах и серверах приложений, поскольку уже не требуется просматривать различные имена и названия. Удается даже сократить время просмотра каталогов, так как специалисты компании Lotus сделали эту процедуру намного эффективнее.

Еще в рамках версии 2 администраторы имели возможность работать с многочисленными службами каталогов, и пользователи без труда направляли почтовые сообщения пользователям системы Notes в других доменах Notes/Domino. Начиная с версии 4.6 (и уже в большей степени в версии 5) специалисты компании Lotus расширили возможности по общению с доменами не-Domino за счет применения протокола LDAP (Lightweight Directory Access Protocol - протокол упрощенного доступа к каталогу) в рамках службы каталога Domino. Это позволило серверам Domino правильно проводить аутентификацию пользователей из каталогов не-Domino. Кроме того, в клиенте Lotus Notes реализован протокол LDAP, поэтому пользователи получили возможность вести поиск имен в каталогах LDAP.

В дополнение к этому, в рамках версии 5 были усовершенствованы службы каталога:

- О увеличено максимальное число пользователей (до 1 млн) в одном домене системы (по сравнению с 150 тыс. пользователей в версии 4.x);
- О в каталоге Enterprise Directory Catalog (Каталог перечня предприятия) обеспечено (в весьма компактной форме) хранение только основной информации о пользователях, при этом на каждого пользователя выделяется примерно 100 байт, а в одном документе хранятся данные о 255 пользователях. Это позволяет администраторам поддерживать весьма объемный каталог на небольших жестких дисках и достаточно просто копировать его, в результате чего мобильные пользователи имеют в своем распоряжении локальную копию (реплику) всего каталога предприятия без увеличения требований к своему жесткому диску.

В версии R6 стали доступными следующие возможности:

- О переход от распределенной структуры каталогов к единому централизованному каталогу Domino, что особенно важно для крупных предприятий;
- О автоматическая поддержка согласованности наследования объектов в пределах всего центрального каталога Domino благодаря новой схеме Domino LDAP Schema для баз данных;
- О расширение действия каталога Domino Directory на несколько организаций за счет использования новых списков управления доступом xACL, дополняющих возможности обычных списков ACL.

Распределенная архитектура и репликация

Система Notes всегда поддерживала архитектуру с распределенным хранением данных, в которой реплики баз данных хранятся на многочисленных серверах. Пользователи получают доступ к этим серверам с помощью наиболее удобных приемов. Формируемые реплики баз данных обычно сравниваются с другими репликами в режиме по умолчанию. Затем пользователь может добавить в реплику новые данные, а сервер распространит изменения на другие реплики за счет процесса, называемого *репликацией* (тиражированием).

В течение целого ряда лет специалисты компании Lotus совершенствовали процедуру репликации. Первоначально в случае появления изменений в любом поле документа при репликации на другие серверы должен был передаваться документ целиком. Начиная с версии 4.0 на другие серверы пересылаются только данные из измененных полей.

Функция репликации разрабатывалась специально для того, чтобы обеспечить распространение приложений системы Notes по многочисленным локальным серверам. Однако такая операция оказалась весьма полезной, когда специалисты компании расширили возможности сервера Domino на сеть Internet. Это очень просто проследить на примере решения проблемы поддержки Web-сайта. Обычно пользователю требуется создать Web-сайт и загрузить его на постановочный (тестовый) сервер, затем переправить файлы на рабочий Web-сервер, непосредственно связанный с глобальной сетью. Для большей части существующих Web-серверов данная операция выполняется вручную и может оказаться весьма трудоемкой, если постановочный сервер, скажем, располагается за корпоративным брандмауэром, а рабочий находится перед ним.

Для серверов Domino передача Web-сайта с постановочного сервера на рабочий производится в автоматическом режиме и получается весьма простой. Пользователю необходимо лишь инициировать режим репликации для двух серверов, а сервер Domino позаботится об остальном. Правда, предварительно потребуется открыть соответствующий порт брандмауэра, чтобы серверы могли нормально взаимодействовать, но эту операцию придется выполнить в любом случае.

В рамках версии R5 специалисты компании Lotus не стали изменять принцип реализации функции репликации. Однако они усовершенствовали программные инструменты, предназначенные для поддержки этой функции, причем в двух основных направлениях. Во-первых, в клиентскую программу Administrator добавлена *топологическая карта репликации*, которая в графическом виде показывает взаимосвязи между серверами при выполнении операций репликации. Во-вторых, предусмотрена возможность накопления данных, указывающих на характер завершения (успешный или неуспешный) последних операций репликации, а также на планирующиеся в будущем операции репликации при общении сервера с партнерами.

В версии R6 появилась потоковая репликация (streaming replication), благодаря которой при обмене изменениями можно ограничиться запросом одного сервера, позволяющего вытащить все необходимые данные. Это значительно сокращает время на проведение репликации, а клиентам Notes уже не обязательно ожидать полного завершения процесса. Потоковая репликация основана на двух концепциях: объектный поток (открытие узла запускает объектный поток, извлекающий все необходимые сведения об объекте) и потоковый механизм (извлечение сведений об узле из базы данных предполагает создание единственной высокоуровневой транзакции, обеспечивающей получение всех необходимых данных).

Обеспечение безопасности

Разработчики системы Notes с самого начала предполагали, что пользователи захотят хранить в базах данных конфиденциальную информацию. Поэтому в системе Notes уже в первых версиях были предусмотрены необходимые средства защиты данных. В результате не составляет труда узнать, кто осуществлял доступ к серверам, базам данных, формам, окнам, документам и полям. Пользователи и серверы системы Notes автоматически аутентифицируют друг друга, проводя идентификацию на основе сертификатов компании RSA Data Security, Inc.

В рамках версии 5 специалисты компании Lotus усовершенствовали функцию обеспечения безопасности сервера Domino по целому ряду направлений:

- О *проверка качества пароля* - администраторы могут требовать от пользователей соответствия их паролей пяти уровням защиты, при этом степень надежности пароля возрастает с увеличением числа имеющихся в пароле букв, цифр и прочих символов;
- О *восстановление утерянных паролей* - администраторы и пользователи получили возможность сотрудничать между собой для снятия блокировки файла идентификационных данных и восстановления утерянного пароля;
- О *поддержка сертификатов X.509* - идентификационные данные в системе Notes могут включать в себя как сертификаты Notes, так и сертификаты X.509. Это позволяет пользователям системы Notes производить свою аутентификацию с помощью различных сертификатов и с привлечением серверов Domino и серверов сети Internet, поддерживающих протокол SSL;
- О *поддержка протоколов S/MIME* - пользователи системы Notes могут направлять и получать подписанные и шифрованные почтовые сообщения при взаимодействии с любым абонентом, программные средства которого поддерживают протокол S/MIME;
- О *управление доступом к объектам* (файлам HTML и GIF, файлам классов Java и подобным).

В версии R6 еще более усилена защита и повышена безопасность пользователей:

- О *доступ к документам в каталоге Domino Directory управляется списками ACL*, поэтому можно разрешить или запретить доступ на уровне любого документа;
- О *поддерживается стандарт PKCS#11 для смарт-карт (smartcard)*, которые обеспечивают, например, более надежную защиту при снятии блокировки с пользовательского идентификационного файла, поскольку потребует не только ввести пароль, но и предоставить записанный на смарт-карте номер персональной идентификации (PIN);
- О *реализована поддержка протокола S/MIME версии 3*, благодаря чему удастся использовать все его новые возможности.

Поддержка мобильных пользователей

Система Notes обеспечивает эффективную поддержку мобильных пользователей. Во-первых, эти пользователи имеют возможность связаться с серверами Domino по сети или по модемному подключению. С помощью модема они в состоянии соединиться непосредственно с серверами Domino, предусматривающими коммутируемый телефонный доступ, или же с удаленными сетями, после чего обратиться к серверу Domino по этой сети. Во-вторых, пользователи могут подключаться к нужному серверу Domino через промежуточные серверы. Это позволяет им набирать номер одного сервера и использовать его для связи с другими серверами Domino. И наконец, клиенты системы Notes способны поддерживать местные копии баз данных и реплицировать изменения в них на другие серверы, что обеспечивает мобильным пользователям нормальную работу даже в тех условиях, когда они непосредственно не соединены с сервером.

В версии R5 специалисты компании Lotus добавили функцию дистанционного динамического управления для пользователей настольных компьютеров. В предшествующих версиях сервер Domino также осуществлял поддержку профилей пользователей, что заметно упрощало процедуру настройки и обслуживания. Особенностью версии 5 является то, что теперь профили пользователей настраиваются еще на этапе установки клиента. Любые изменения, которые администратор производит в профиле пользователя, будут автоматически передаваться в его клиентскую программу. Подобный подход во многом облегчает задачу общения администратора с мобильными пользователями и поддержки таких пользователей.

Версия R6 обеспечивает перемещаемые профили (roaming profile), поэтому пользователь может подключаться к системе с помощью любого доступного устройства и из любого места, причем сохраняется вся его персональная информация (страница приветствия, закладки, адресная книга, журнал, идентификационный файл и т.д.).

Поддержка нескольких компьютерных платформ

Сервер Domino и клиенты системы Notes могут работать на разных аппаратных платформах и в различных операционных системах. Это позволяет пользователю общаться с системой Notes с помощью привычных вычислительных средств, не заботиться об их модернизации и переходе на новую платформу. Кроме того, при подобном подходе для серверов обеспечиваются хорошие показатели масштабирования. Небольшие фирмы, которые располагают преимущественно персональными компьютерами с операционными системами Windows и Macintosh, вполне могут применять серверы с операционной системой Windows NT, а более крупные организации - мощные серверы UNIX и даже платформы AS/400 или S/390.

Начиная с версии 5 специалисты компании Lotus более четко определили свою позицию по отношению к разным платформам. Так, они отказались от поддержки Novell NetWare в качестве платформы для сервера Domino, а также от поддержки операционных систем OS/2 и UNIX в качестве платформ для клиентов системы Notes. Пользователи этих платформ могут либо продолжать работу с клиентами Notes версии 4.x, либо взаимодействовать с серверами Domino из клиентов на языке программирования Java.

Примечательной особенностью версий R5 и R6 стала работа сервера Domino в клиентской операционной системе Windows XP Professional. В этой же среде успешно функционируют и клиентские программы Domino/Notes.

Обеспечение доступа к данным

Специалисты компании Lotus предлагают самые разнообразные программные средства для связи с источниками данных, не ориентированными на платформу Notes. Эти средства включают в себя функции @ и классы LotusScript, которые разработчики могут применять наряду с надстройками (add-in), превращающими Domino в сервер среднего уровня (middleware) между источниками данных заднего уровня (например, реляционными базами данных и системами транзакций) и средствами доступа переднего уровня, подобными клиентам Notes или Web-браузерам.

В версии 5 специалисты компании Lotus усовершенствовали доступ к данным по целому ряду направлений, таких как:

- О *предоставление доступа в реальном масштабе времени к реляционным базам данных и системам транзакций с использованием службы DECS (Domino Enterprise Connection Service - корпоративная служба подключений Domino)*. Эта служба сервера Domino является масштабированной вниз системой Lotus NotesPump (Подкачка данных);
- О *реализация доступа к службам системы Notes/Domino из браузера средствами CORBA/IIOP*, что позволяет программистам разрабатывать апплеты Java, обеспечивающие доступ к службам сервера Domino при локальном исполнении отдельных функций, которые иначе должен был бы осуществлять сам сервер Domino. Таким образом удастся снять часть нагрузки с сервера Domino, сделать браузер более мощным и уменьшить интенсивность передаваемого между данными компонентами трафика;
- О *обеспечение взаимодействия в реальном масштабе времени, включая поддержку досок объявлений и совместно используемых приложений*. Эта функция на самом деле не придана серверу Domino, а реализована в специальной клиент/серверной платформе, получившей название Lotus SameTime. Соответствующий продукт приобретается отдельно и устанавливается на независимом сервере, но тесно взаимодействует с сервером Domino и системой Notes;
- О *использование функции Domino Extended Search (Расширенный поиск)*, представляющей собой усовершенствованную процедуру поиска, применяя которую пользователи в состоянии производить одновременный поиск по нескольким индексам. Поиск осуществляется в рамках доменов Domino, файловых систем, реляционных баз данных, информационных репозиториях сети Internet и коммерческих информационных архивов. Эта функция реализуется независимой надстройкой, которая приобретается отдельно;
- О *использование каталога Expanded Database Catalog (Расширенный каталог баз данных)*, соответствующая программа хранится в файле catalog5.nsf). Эта функция дает возможность в пределах домена вести поиск в базах данных системы Notes и серверов Domino.

В версии R6 доступ к данным не претерпел существенных изменений, однако:

- О *изменена функция полнотекстового поиска Domino 6* - большая часть данных теперь обновляется на месте, без перемещения на сервер, а менеджер буферирования NSF в службах управления памятью позволяет повысить эффективность при полномасштабном поиске в домене;
- О *новая процедура кэширования при просмотре каталога* приводит к тому, что увеличивается производительность обработки запросов на просмотр, а пересылка почты или извлечение данных о маршрутизации выполняются вдвое быстрее.

Формирование интегральной среды проектирования

Специалисты компании Lotus с самого начала ожидали появления тех проблем, которые придется решать системе Notes, но даже они не могли предвидеть огромного разнообразия областей применения этой системы. Система была снабжена рядом дополнительных инструментов для разработки и проектирования, так чтобы пользователи создавали собственные приложения в соответствии с существующими требованиями.

В версиях 5 и 6 такие инструменты представлены программой Domino Designer (разработка приложений сервера Domino), служащей для формирования *интегральной среды проектирования*, специально предназначенной для построения приложений системы Notes, а также программными средствами, позволяющими разработчикам пользоваться другими подобными средами. Доступны разнообразные языки программирования - начиная с лицензированного языка формул и LotusScript и заканчивая широко применяемыми на практике C, C++, Java, Visual Basic, HTML, JavaScript и CGI.

Расширения и надстройки

Компания Lotus регулярно расширяет возможности системы Notes, чтобы полнее удовлетворять потребности пользователей и придать программным продуктам большую функциональную гибкость. Поэтому компания Lotus проводит для большого числа продуктов маркетинговые мероприятия, цель которых - эффективно дополнять уже имеющиеся функции и характеристики системы Notes. Так, в систему могут быть добавлены программные инструменты коллективной работы в режиме реального времени, инструменты для формирования беспроводных соединений с серверами Domino и специальные приложения, например приложения Extended Search (Расширенный поиск) с улучшенным двигателем поиска и Domino.Doc (Документы сервера Domino) для управления документами.

Компания Lotus также поощряет сторонних разработчиков в создании программных продуктов, способствующих расширению возможностей системы Notes. Специалисты компании предложили целый ряд интерфейсов прикладного программирования (API), обеспечивающих доступ к классам объектов системы Notes. Следует отметить, что подобный подход себя полностью оправдал, и к настоящему моменту сторонние разработчики уже сформировали много ценных дополнений для системы Notes.

Web-сервер

Web-сервер Domino на первых порах служил в качестве надстройки (начиная с версии 1.4) и стал неотъемлемой частью сервера Domino только с версии 4.5. В данном случае разработчики пошли по пути непосредственного «встраивания» Web-сервера, открыв тем самым перед серверами системы Notes целый ряд новых рынков. Именно с этого момента серверы компании Lotus стали именоваться серверами Domino.

Web-сервер Domino в данном случае представлен полномасштабным Web-сервером и, подобно любому серверу HTTP, может обслуживать файлы HTML в рамках собственной файловой системы и обеспечивать связь с программами CGI. Однако, в отличие от других серверов HTTP, этот сервер подходит также для обработки документов, поступающих из баз данных системы Notes, и передачи их на резидентный сервер.

В версии 5 предусмотрены следующие возможности по применению службы HTTP:

- О *работа с кластерами (группами серверов) HTTP*. Web-пользователи теперь могут (в случае острой необходимости или при отказе сервера) перенаправляться на наименее загруженный сервер кластера;
- О *поддержка сервера HTTP версии 1.1*;
- О *необязательная интеграция с сервером IIS (Internet Information Server) компании Microsoft*;
- О *применение системных списков ACL (Список управления доступом)*;
- О *задание диапазона в байтах*, что позволяет возобновлять загрузку, а также выполнять другие операции;
- О *перезагрузка конфигурации сервера HTTP без его перезапуска*;
- О *улучшение регистрации*.

Поскольку применение Web-сервера позволяет осуществлять доступ к данным системы Notes с помощью Web-браузера, специалисты компании Lotus также предусмотрели использование *стека Domino HTTP* в рамках программы Notes Designer (разработка приложений для системы Notes). Эта новинка появилась, начиная с версии 4.6. Благодаря ей можно тестировать доступ к приложениям из клиентов системы Notes и браузеров, не покидая окна программы Notes Designer.

В версии 6 сервера Domino Web-сервер способен:

- О *работать с документом Web Site Rule* (Правила для Web-сайта), дополняющим документ Web Site из каталога Domino Directory;
- О *обеспечить стандарт WebDAV* (Web Distributed Authoring and Version - распространение в Web авторства и версий), реализующий коллективную работу в среде проектирования. Таким образом, файлы NSF теперь могут хранить общий репозиторий элементов как для сторонних программ, так и для Designer 6.
- О *пользоваться надстройками для WebSphere*. Первоначально появились надстройки для Microsoft IIS и IBM HTTP Server, но ожидается увеличение числа поддерживаемых Web-платформ.

Web-браузер

С версии 4.0 компания Lotus начала встраивать Web-браузер в сервер системы Notes/Domino, а с версии 4.5 Web-браузер превратился в неотъемлемую часть клиента системы Notes. Браузеры поддерживали большую часть функций стандарта HTML 3.2. С версии 4.6 специалисты компании Lotus стали использовать встроенную версию браузера Internet Explorer компании Microsoft в клиентах системы Notes. Это привело к тому, что пользователи смогли беспрепятственно обращаться к Web-сайтам, поддерживавшим платформу HTML 4.9, причем не требовался отказ от сторонних браузеров. Начиная с версии 5 компания Lotus обновила внутренние браузеры системы Notes и сервера Domino с тем, чтобы обеспечить полную поддержку стандарта HTML 4.0.

Следует отметить, что применяемый сервером браузер по существу является совместно используемым и служит одновременно нескольким клиентам системы Notes, которые пересылают ему адреса URL для перенаправления на hosts сетей intranet/Internet. С встроенным браузером обычно работают те пользователи, которые не имеют возможности

непосредственно просматривать данные, поскольку их компьютеры несовместимы с протоколами TCP/IP или не располагают соответствующим программным обеспечением.

Управляющие программные инструменты

Специалисты компании Lotus уже на протяжении ряда лет разрабатывают программные инструменты для управления установкой систем Notes/Domino. Сначала эти инструменты были достаточно простыми, но уже в версии 5 компания Lotus приложила заметные усилия для создания действительно эффективных программных средств. Наиболее значимым результатом стал выпуск ориентированной на задачи программы Domino Administrator (Администрирование сервера Domino), которая является оконечным интерфейсом в операционной системе Windows и расширяет возможности клиента системы Notes. Данный графический программный инструмент обеспечивал режим перетаскивания мышью и был ориентирован на выполнение задач, а не на запуск приложений, позволяя управлять базами данных, пользователями и группами пользователей, серверами, репликацией, обменом сообщениями и т.д. Новый интерфейс администрирования зарекомендовал себя как мощное средство, поэтому его описанию в данной книге будет посвящено достаточно много места. В версии 5 был предложен также целый ряд других, не менее значимых программных инструментов, которые в данном разделе не хотелось бы подробно обсуждать. Ниже приводится перечень наиболее существенных изменений:

- О *упрощенная программа установки*, созданная в пакете InstallShield (также предусматривались некоторые усовершенствования автоматической установки);
- О *усовершенствованные программы управления на основе HTTP*, в том числе программы установки и настройки для управления сервером Domino с помощью Web-браузеров;
- О *улучшенная программа регистрации пользователей*, в том числе программные инструменты для регистрации пользователей в каталогах доменов операционной системы Windows NT и для миграции из почтовых систем cc:Mail, Microsoft Mail и Microsoft Exchange Server;
- О *централизованный контроль и управление конфигурациями рабочих станций пользователей*;
- О *многочисленные улучшения в области сбора и представления статистических данных*, включая уведомления о происходящих событиях;
- О *дополнительные программные инструменты для контроля серверов и соединений сети Internet*;
- О *средства открытия и закрытия сетевых портов*, включая порты для удаленного коммутируемого доступа, без соединения сервера (в этом случае администраторы имеют возможность реконфигурировать службу HTTP без прерывания работы сервера);
- О *усовершенствованный процесс Administration Process* (Процесс администрирования); когда процесс администрирования может распространяться на несколько доменов и проводить проверки эффективности работы серверов в организациях, планирующих консолидировать серверы системы.

В версии R6 появились следующие возможности администрирования:

- О *управлении на основе политик, заменившее управление через профили пользователей*;
- О *серверная база данных Smart Update*, позволяющая централизованно обновлять версии клиентов Notes;

О *отдельная программная консоль ServerController*, разработанная на языке Java для управления сервером Domino удаленно (с консоли Administrator) или локально (с консоли Domino Console).

Приложения системы Notes

Поскольку система Notes обладает встроенными функциями передачи сообщений, совместного использования ресурсов, работы с документно-ориентированными базами данных и применения программных средств для разработки приложений, можно считать, что она с самого начала планировалась в качестве мощной платформы для приложений. Как и сама система, эти приложения создавались в течение целого ряда лет и являются в настоящее время ее ценным дополнением. Однако система Notes может оказаться практически несовместимой с приложениями, разработанными без учета ее особенностей. Те приложения, которые имеют шансы для использования совместно с системой Notes, обычно содержат документно-ориентированные, хорошо структурированные, функционально гибкие и быстро изменяемые массивы данных различного типа. Причем приложения, непосредственно связанные с реляционными базами данных, как правило, пользуются функциями обработки данных транзакций (например, *системами бухгалтерского учета*) или предусматривают работу со структурированными *статистическими данными*, в частности с большими массивами. Система Notes отлично себя зарекомендовала в случае с реляционными базами данных и транзакционными системами, поэтому те приложения, которые обрабатывают оба указанных типа данных, должны строиться с применением обеих систем, скажем системы Notes в виде интерфейса переднего уровня и реляционным приложением для заднего уровня. Приложения системы Notes можно классифицировать в соответствии со следующими категориями:

- формирование и передача сообщений;
- управление персональными данными;
- организация и проведение дискуссий;
- формирование и поддержка информационных репозиторий;
- отслеживание проектов и рабочих потоков.

На практике сложное приложение системы Notes/Domino, связанное с решением проблем бизнеса, может относиться к различным категориям, однако для лучшего понимания функциональных возможностей системы Notes следует поговорить о каждой из этих категорий в отдельности.

Формирование и передача сообщений

Функция передачи сообщений предусматривает способность сервера Domino пересылать документы между любыми базами данных системы Notes или другими компонентами этой системы. Данная функция является базовой и обеспечивает взаимосвязь и четкое функционирование всей сложной структуры системы Notes/Domino. Однако ниже речь пойдет не о самой функции передачи сообщений, а о более простой ее разновидности - электронной почте.

Электронная почта в наши дни стала широко распространенным приложением сети Internet. Специалисты компании Lotus решили снабдить серверы Domino высокоэффективной инфраструктурой электронной почты. С этой целью компания Lotus постоянно

совершенствует и улучшает функции формирования и передачи сообщений, а также функции электронной почты в серверах Domino. Специалисты компании оптимизировали структуру серверов Domino для обеспечения взаимодействия с большим числом пользователей и эффективной маршрутизации почтовых сообщений. Они также разработали мощные программные средства, позволяющие администраторам системы легко настраивать почтовую службу и управлять ею, а также диагностировать маршрутизацию, хранение и архивирование почтовых сообщений. Кроме того, специалисты компании усовершенствовали интерфейс почтовой службы, сделав его более дружелюбным и интуитивно понятным. Компания Lotus внедрила все существующие в отрасли стандарты электронной почты, что придает процессу передачи почтовых сообщений между системой Notes и другими почтовыми системами необходимую функциональную гибкость и надежность.

Большая часть приложений системы Notes/Domino создается самими пользователями или адаптируется путем модификации типовых приложений. Дело в том, что многие проблемы бизнеса, с которыми сталкиваются пользователи, уникальны и видоизменяются во времени. В связи с этим сотрудники компании Lotus построили множество шаблонов и средств, заметно облегчающих разработку и модификацию приложений и сильно сокращающих сроки ее выполнения.

Следует отметить, однако, что почтовая служба Notes Mail (которая также может соответствующим образом адаптироваться) является одним из немногочисленных приложений, поставляемых в готовом виде и не требующих никаких модификаций. Чтобы работать с ней, нужно лишь установить сервер Domino, зарегистрировать пользователей и добавить пользовательскую программу чтения почты, позаимствовав ее из системы Lotus Notes, либо применять любой почтовый клиент SMTP или SMTP/MIME, способный обеспечить доступ к серверам POP3 или IMAPv4. Этого вполне достаточно, чтобы пользователи нормально отправляли и получали почтовые сообщения. Если в почтовом клиенте поддерживается форматирование, вложения или гипертекстовые ссылки на другие сетевые объекты, эти возможности также становятся доступными пользователям. При поддержке в программе чтения почты можно шифровать сообщения и формировать электронные или текстовые подписи, запрашивать подтверждение доставки или отказа от получения сообщений, а также отслеживать пересылку сообщений и использовать удаленные диагностические зонды.

Управление персональной информацией

Эта функция, представляющая собой неотъемлемую часть системы Notes, предусматривает формирование и обслуживание индивидуальных адресных книг, календарей, перечней работ и подобных им информационных ресурсов, не относящихся к групповой работе. В системе Notes данная функция также обеспечивает поддержку календаря и планирование для группы пользователей. Следует отметить, что поддержка календаря отсутствовала в системе Notes вплоть до версии 4.5, после чего была несколько усовершенствована в версиях 4.6 и 5. Подобно почтовой службе системы Notes, эта функция уже готова к применению и не требует доработки. Единственное, что нужно для ее нормального использования, - создание и заполнение базы данных резервирования ресурсов, чтобы планировать места проведения конференций и выделение других ресурсов на основе расписания конференций.

Дискуссионные форумы

Архитектура баз данных системы Notes всегда обеспечивала классификацию документов согласно их срочности и важности. Любая база данных системы Notes реализует эту функцию, но наиболее полезна она для базы данных дискуссий, в рамках которой группы специалистов могут проводить обсуждения различных проблем. Ход подобных дискуссий легко проследить, поскольку в соответствующем виде дискуссионный поток упорядочен так, что ответы всегда выводятся с некоторым отступом относительно обсуждаемых документов.

Базы данных дискуссий в системе Notes во многом аналогичны группам новостей сети Internet, рассылочным почтовым спискам и форумам в сети CompuServe. Именно по этой причине специалистам компании Lotus не составило труда применить на серверах Domino протокол NNTP (Network News Transfer Protocol - протокол передачи сетевых новостей), который используется серверами News Server (сервер новостей) сети Internet. При этом были сохранены практически все базовые функции протокола, а работа специалистов компании свелась к его добавлению в список протоколов, поддерживаемых серверами Domino.

Информационные репозитории

Одно из наиболее простых приложений системы Notes - база данных, хранящая объявления или справочные данные. Специалисты компании Lotus называют базу данных объявления *широковещательной*, а базу данных, содержащую справочные данные, *базой данных ссылок*. Обе базы являются, по существу, *базами знаний*, а их особенность состоит в том, что они поддерживаются небольшими группами людей, а читают информацию самые широкие слои пользователей. В этом смысле они выполняют те же функции, что и обычный Web-сайт сети Internet.

Основное различие между указанными базами данных заключается в том, что информация в базе данных ссылок изменяется редко. Информация в базе данных широкого вещания носит скорее временный характер - она может оказаться востребованной сегодня, в виде несколько устаревших новостей завтра, а затем должна претерпеть соответствующие изменения.

Любая книга ссылок способна с успехом выступать в качестве базы данных ссылок. Базой данных ссылок может быть, например, справочная база данных, поставляемая вместе с системой Notes и содержащая различные сведения о системе, или справочные системы Notes и почтовой службы cc:Mail или SmartSuite, поддерживаемые в сети Internet компанией Lotus для своих бизнес-партнеров.

Широковещательной может стать база данных объявлений о продуктах, вакансиях, меню ресторанов, пресс-релизов или любой подобной информации, публикуемой на досках объявлений.

Следует отметить, что отделы кадров были просто в восторге от баз данных обоих типов. Используемые этими отделами сложные приложения содержат долгосрочные ссылочные данные, например заявления по самым разным поводам (от проблем курения и требований к одежде сотрудников до открывающихся в будущем вакансий). В такие приложения включают и текущую информацию, скажем сообщения об открывающихся вакансиях, изменениях политики компании, назначениях, графиках отпусков сотрудников или датах и местах проведения ежегодных встреч.

Отслеживание приложений

Функция отслеживания приложений выделяет систему Notes на фоне других систем групповой работы. Для отслеживания обычно создается база данных, доступ к которой (для чтения и записи) имеет только небольшая рабочая группа или команда специалистов. Члены такого коллектива могут ознакомиться с трудами других участников проекта, поскольку в базу данных записываются документы, определяющие цели и задачи проекта, например заявление о намерениях, графики работ, основные этапы проекта и др. Члены команды вправе в любой момент обратиться к этой базе данных и выяснить текущее состояние проекта в целом. Любому из членов команды достаточно предпринять предусмотренные проектом шаги и действия, чтобы добавить или изменить документы, связанные с этими действиями, а прочие члены команды в дальнейшем сумеют ознакомиться с новым статусом и новым состоянием всего проекта.

Приложения для рабочих потоков

Подобные приложения, как правило, являются компьютеризованными версиями обычных процедур составления и ведения рабочих графиков. Эта функция может предусматривать только автоматическую рассылку форм большому числу сотрудников. Естественно, система Notes без труда справится с подобной задачей, но дополнение совместно используемой архитектурой баз данных на основе почтовой связи позволяет улучшить качество обслуживания пользователей.

Простой пример реализации данной функции связан с заказом расходных материалов. Когда требуется заказать инструмент для выполнения работ, один из членов команды должен заполнить соответствующие формы, руководитель - утвердить заказ, а уже другой член команды - направить эти формы для исполнения. В системе Notes такие операции выполняются следующим образом: сначала члену команды приходится заполнять электронную форму в собственной почтовой базе данных, а затем форма автоматически пересылается в базу данных отслеживания заказа.

При поступлении в базу нового документа активизируется программный агент на сервере, который по электронной почте направит уведомление руководителю, утверждающему формы. Руководителю достаточно щелкнуть по значку на экране, чтобы открыть форму на собственном компьютере. Утверждение форм осуществляется щелчком по соответствующему полю формы, после чего форма должна быть сохранена и закрыта. При этом активизируется другой агент, направляющий уведомление следующему члену команды, который может быть еще одним утверждающим форму руководителем или тем членом команды, который непосредственно отвечает за поставку инструмента.

Преимущества подобной системы заказа вполне очевидны. Во-первых, нет опасности потерять форму, поскольку она всегда остается в соответствующей базе данных. Во-вторых, исполнители получают уведомление об утверждении формы в виде почтового сообщения и имеют возможность сразу предпринять последующие действия. В-третьих, если формирующий заказ человек или любой другой член команды захочет просмотреть саму форму или проверить исполнение заказа, такая электронно-бумажная система предоставит полную информацию о состоянии дел.

В-четвертых, используемая в системе Notes функция обеспечения безопасности ограничивает доступ к форме только уполномоченными на это (на составление, утверждение и исполнение форм) членами команды. И наконец, применение системы Notes позволяет

реализовать различные усовершенствования базовой функции, например предусмотреть направление напоминаний исполнителям той или иной формы, если заказ остается невыполненным в течение долгого времени.

Web-приложения

Следует отметить, что Web-приложения сервера Domino являются лишь модификациями базовых приложений системы Notes. Так, Web-приложения просто расширяют область действия обычных приложений Notes и сервера Domino на сети Internet, intranet и extranet. Преимущество подобных приложений состоит в их универсальности в части расширения - например, при взаимодействии с системами поставщиков материалов, деловыми партнерами и клиентами. В прошлом для расширения приложений системы Notes (за пределы деятельности самой компании) требовалось убедить представителей других организаций внедрить у себя систему Notes. В наши дни имеется возможность использовать для этих целей уже готовые Web-браузеры. Последнее позволяет заметно увеличить область применения приложений системы Notes (специалисты компании IBM называют подобные приложения «подходящими для активного маркетинга» или «расширяющими области применения платформы») и в корне изменить методы и приемы коммерческой деятельности.

Состав версий 5 и 6

С появлением версии 5.0 компания Lotus стала активно предлагать три варианта сервера Domino, один вариант клиента системы Notes, а также две надстройки для этого клиента - Domino Designer и Domino Administrator. Три варианта сервера Domino представлены следующими версиями:

- О *сервер Domino Mail Server* (сервер почтовой службы Domino) - обеспечивает базовые функции электронной почты и служб коллективной работы;
- О *сервер Domino Application Server* (сервер приложений Domino) - соответствует стандартному варианту сервера Domino, подобному тем, которые использовались в более ранних версиях. Он выполняет функции сервера Domino Mail Server, а также реализует службы Web-приложений, поддерживает CORBA/IIOP и осуществляет связь с внешними источниками данных;
- О *сервер Domino Enterprise Server* (корпоративный сервер Domino или сервер Domino масштаба предприятия) - выполняет функции обоих предшествующих серверов и реализует кластеризацию серверов для повышения доступности данных.

Сервер Domino Mail Server разрабатывался в качестве сервера начального уровня системы Notes/Domino для тех организаций, которым требуется быстро освоить и эксплуатировать его базовые службы, например функции электронной почты, организации дискуссий, поддержки календаря и планирования, управления задачами и формирования информационных репозиториях.

Сервер Domino Application Server - стандартный сервер системы Notes/Domino с точки зрения предшествующих версий этой системы. Он предусматривает использование служб (HTTP, CORBA/IIOP), необходимых для наиболее полной реализации возможностей сервера Domino в качестве сервера Web-приложений, и предназначен для тех организаций, которые не намерены ограничиваться простейшими функциями (например, функциями почтовой связи и соответствующими службами).

Сервер Domino Go

Существует еще один вариант сервера Domino, известный под названием Domino Go. Он не является сервером Domino в том смысле, как три ранее упомянутых сервера, и представляет собой обычный сервер HTTP, не выполняющий многих функций системы Notes. Данный сервер построен на основе того же стека протокола HTTP, что и вышеперечисленные серверы Domino, и предполагает применение той же службы HTTP, однако принцип его работы оказывается совершенно иным. Здесь нет подробного описания возможностей сервера Domino Go, однако исчерпывающую информацию можно найти на сайте компании Lotus - www.lotus.com.

Сервер Domino Enterprise Server включает дополнительные службы (применение серверных кластеров, сегментирование сервера и формирование счетов), которые в рамках версий 4.x были известны под названием Domino Advanced Services (Улучшенные службы сервера Domino). Эти службы могут оказаться мощным инструментом поддержки для больших организаций и сетей Notes Public Networks (Общедоступные сети на основе системы Notes), где предлагается аренда серверов Domino для компаний организаций, не желающих заниматься созданием и поддержкой собственного сервера. Кластеризация серверов (которая в рамках версии 5 и 6 также предусматривает работу групп Web-серверов) удобна при условии, что данные с сервера Domino требуется получать круглосуточно.

Как и прежде, сервер Domino может работать на различных аппаратных платформах и в разнообразных операционных системах. Версия R5 функционирует на следующих платформах:

- О операционные системы Windows 95 и Windows NT на аппаратной платформе компании Intel;
- О операционная система Windows NT на аппаратной платформе Alpha;
- О операционная система OS/2 компании IBM;
- О операционная система AIX компании IBM;
- О операционная система HP-UX компании Hewlett Packard;
- О операционная система Solaris компании Sun на аппаратной платформе SPARC;
- О операционная система Solaris компании Sun на аппаратной платформе Intel;
- О операционная система OS/400 компании IBM;
- О операционная система OS/390 компании IBM.

Компания Lotus прекратила поддерживать операционную систему Novell NetWare (компании Novell), поскольку ее пользователей не привлекает сервер Domino.

Серверы Lotus Domino 6 работают в операционных системах Microsoft Windows NT и Windows 2000, IBM OS/400, IBM AIX, Sun Solaris/SPARC и в серверных версиях Linux (IA-32). Клиенты Lotus Notes совместимы со всеми 32-разрядными версиями Windows, а также (на компьютерах Macintosh) с операционной системой Mac OS X.

Все новые серверы Domino содержат собственно сервер Domino, клиент системы Notes и клиентскую программу Domino Administrator, которые поставляются в виде единого программного пакета. Клиенты серверов Domino для операционных систем Windows могут исполняться на сервере. Для серверов Domino других платформ предоставляются клиенты, ориентированные на операционную систему Windows.

Состав клиента Domino и его надстройки:

- О Notes Client (Клиент системы Notes) - самая совершенная клиентская программа, поддерживающая режим персонального информационного менеджера (PIM)

и универсальный входной почтовый ящик. Компания Lotus рекомендует эту программу как наилучший клиент для работы с сервером Domino;

- О Domino Designer (Дизайнер сервера Domino) - тоже клиентская программа системы Notes, но с новым интерфейсом программирования;
- О Domino Administrator (Администрирование сервера Domino) - еще одна клиентская программа системы Notes, но с интерфейсом администрирования; разработана специально для администраторов сервера Domino.

Программы Domino Designer и Domino Administrator не являются автономными клиентами. Скорее, они представляют собой надстройки для клиентской программы Notes (программа Notes Client). Так, при покупке лицензии на программу Domino Designer пользователь одновременно получает и лицензию на Notes Client, после чего может установить обе программы. Программа Domino Administrator также не лицензируется отдельно, но поставляется вместе с сервером Domino. Добавить Domino Administrator допустимо к любой ранее установленной системе Notes.

К настоящему времени уже практически не используются такие программы из версии R4, как клиент Notes Mail (Клиент почтовой службы системы Notes), клиент Notes Desktop (Клиент для настольного компьютера в системе Notes) и аналогичные клиентские программы. Начиная с версии 5 отсутствует клиент, эквивалентный программе Notes Mail, а клиент Notes заменяет программу Notes Desktop (версия 4) только в том отношении, что включает в себя все службы клиента (и соответствующие лицензии), но не содержит интерфейсных средств для разработки и администрирования. Для формирования в рамках версии 5 и 6 программы, эквивалентной полноценному клиенту Notes версии 4, в процессе установки следует выбрать все три интерфейса устанавливаемого клиента.

Клиент Notes R5 может работать в операционных системах Windows 95 и Windows NT, а также на платформе Macintosh/Apple.

Программы Domino Designer и Domino Administrator версии R5 предназначены только для операционных систем Windows 95 и Windows NT.

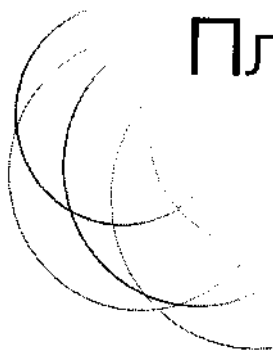
В версии R6 есть всего два типа клиентов - обычный клиент Notes или клиент Notes с надстройками Designer и Administrator. Клиенты обоих типов работают в операционных системах Windows 95/98/NT/2000/XP.

До R5 существовали клиенты системы Lotus Notes для операционной системы OS/2 и трех серверных платформ UNIX. Начиная с версии 5 компания Lotus не предлагает вариантов клиентской программы Notes для этих платформ. Вместо них включены апплеты Java, реализующие функции клиентов Notes и исполняемые в рамках программного пакета Lotus eSuite или в Web-браузере. Администраторам, желающим установить программу Domino Administrator, теперь придется переходить на компьютеры с операционной системой Windows либо работать с Web Administration (Web-администрирование). Этот программный инструмент опирается на применение базы данных сервера Domino, допускает обращение только из Web-браузера и позволяет решать различные задачи администрирования.

В настоящей главе рассмотрены возможности и характеристики системы Notes и сервера Domino, обсуждены их компоненты и перечислены пригодные для их работы платформы. В последующих четырех главах внимание будет сфокусировано в основном на планировании и выполнении процедуры развертывания домена Domino.

ГЛАВА

2



ПЛАНИРОВАНИЕ И УСТАНОВКА

Предварительное планирование - это обязательное мероприятие, способствующее успешной установке и последующей нормальной эксплуатации системы Notes/Domino. Вне зависимости от того, устанавливается новая версия сервера Domino или обновляется уже существующая, понадобится предварительно определить, что является необходимым и что следует изменить. При установке новой версии сервера Domino, когда требуется создать домен или организацию, подобное планирование оказывается особенно важным, поскольку ошибки, допущенные на первых этапах, будут постоянно сказываться в дальнейшем, а плохо спланированное и осуществленное *развертывание* со временем может привести к существенным сбоям в работе сервера. Но даже в том случае, если надо просто обновить или расширить существующую версию, отсутствие предварительного планирования может впоследствии стать причиной весьма дорогостоящих ошибок.

В данной главе кратко рассмотрены вопросы планирования и выполнения процедуры развертывания. Затем подробно описаны технические нюансы, которые требуется продумать перед установкой первого сервера Domino. Пользователь, уже принявший решение относительно целей применения этого сервера, определивший его функции и назначение и подготовившийся к процедуре установки своего первого сервера, может сразу перейти к ознакомлению с разделом «Формирование внутренней инфраструктуры сервера Domino» в конце главы. Однако, если пользователь еще не знаком с сервером Domino, рекомендуется проработать материал всей главы, поскольку этот сервер отличается большой гибкостью в функциональном отношении и призван выполнять множество различных операций. Следует отметить, что для сервера Domino уже на первых этапах его установки можно предусматривать процедуры, планируемые компанией на отдаленную перспективу. В таком случае стоит внимательно ознакомиться (если это еще не было сделано) с материалами глав 1 и 2.

Процедура развертывания сервера Domino

При планировании развертывания следует учитывать целый ряд факторов:

- О правильно сформулировать требования к системе, как в функциональном, так и в техническом плане, и проследить, каким образом сервер Domino позволит их удовлетворить (в ближайшее время и в долгосрочной перспективе);

- подобрать группу специалистов для осуществления развертывания, причем эта группа может включать в себя менеджеров, представителей пользователей, экспертов и технических специалистов;
- точно выявить имеющиеся ресурсы и определить дополнительные ресурсы, которые потребуются для выполнения упомянутой процедуры;
- составить план проекта и график его реализации. Очень важно правильно наметить объем работ для каждого члена группы, последовательно отслеживать их осуществление и использовать результаты контроля для последующего планирования;
- в процессе подготовки перед утверждением основного проекта может понадобиться разработать пилотный проект (вариант «бета-развертывания»).

Технические требования

На данном этапе следует определить, какие задачи приходится решать компании, какова природа ее деятельности и каким образом сервер Domino поможет в решении задач и проблем в ближайшее время и в долгосрочном плане, учитывая все возможные варианты применения сервера Domino, поскольку данный сервер способен:

- обеспечить формирование инфраструктуры для передачи сообщений;
- выполнять функцию связующего звена между серверами приложений и Web-серверами;
- создавать информационные репозитории;
- автоматизировать рабочие потоки внутри компании, между компанией и ее поставщиками, деловыми партнерами и клиентами.

После этого рекомендуется продумать некоторые нюансы, связанные с коммерческой и технической сторонами деятельности компании, и ответить на следующие вопросы:

- какая информация должна предоставляться конкретным пользователям, а к какой доступ должен быть ограничен;
- допускается ли компанией принцип совместного использования данных и есть ли у подразделений фирмы необходимость ограничить доступ к информации. Например, отдел продаж не всегда готов поделиться сведениями с другими отделами. Это может оказать некоторое влияние на подбор группы специалистов и на разработку приложений в будущем, а также определенным образом сказаться на выборе аппаратных средств и на процессе обучения сотрудников;
- какие корпоративные принципы требуется реализовать, есть ли у компании необходимость в сотрудничестве с другими организациями и потребует ли это изменения принципов коммерческой деятельности компании;
- кто будет контролировать ход работы над проектом, можно ли уже на этом этапе назвать исполнительных или ответственных лиц компании и сказать, каким образом их потребности/проблемы могут быть решены в рамках системы Notes;
- как компания осуществляет свою деятельность, какие информационные потоки проходят через нее и каким образом, как они связаны с различными рабочими группами, а также каков характер потоков между компанией и ее поставщиками, деловыми партнерами и клиентами;
- как и где запоминается и хранится информация и каким способом можно облегчить доступ к ней; как и кем осуществляется экспертиза информации и разрешение доступа к ней другим сотрудникам компании;

- О какие факторы влияют на деятельность компании, каковы результаты негативного воздействия и каким образом можно уменьшить отрицательный эффект от подобного воздействия;
- О какие компьютерные платформы и какое программное обеспечение применяет организация, существуют ли стандарты компании, определяющие порядок выбора компьютерных платформ.
- О какие компьютерные платформы и программное обеспечение используют поставщики, деловые партнеры и клиенты компании и какие взаимосвязи и контакты имеются между компанией и этими партнерами;
- О каким способом информация передается внутри компании, а также между компанией и сторонними организациями; на чем основывается эта передача - на телефонной связи, обмене бумажными документами или электронными данными, надежны ли принятые способы связи и как их можно усовершенствовать;
- О каково качество электронных средств связи внутри компании и для взаимодействия со сторонними организациями; каков характер компьютерной инфраструктуры, достаточно ли она проста, надежна и безопасна;
- О каким образом компания использует сеть Internet, World Wide Web и систему передачи сообщений; если у компании имеется Web-сайт, как осуществляется его поддержка;
- О насколько квалифицированы сотрудники компании, ее поставщики, деловые партнеры и клиенты в части общения с компьютерами и программным обеспечением, каков будет характер их «сопротивления» переходу к применению систем на основе серверов Domino и как его преодолеть; каковы планы относительно обучения и тренинга пользователей новой системы после их подключения к ней, как предполагается убеждать поставщиков, партнеров и клиентов перейти на новую систему.

Подбор группы

Успех процедуры развертывания сервера Domino во многом определяется квалификацией той группы сотрудников, которая будет выполнять намеченные работы. Состав этой группы зависит от размеров компании и от характера долгосрочного планирования и может изменяться по мере выполнения проекта.

Если компания небольшая или сервер Domino намечено внедрить только в одном департаменте, то достаточно немногочисленной группы (два или три сотрудника, например начальник департамента или глава компании, ведущий специалист компании по компьютерным вопросам и, возможно, внешний консультант по системе Notes/Domino). Если же компания имеет внушительные размеры, а внедрение серверов Domino планируется повсеместно, эта группа может включать в себя большое число сотрудников, причем вышеупомянутые лица должны присутствовать в ней обязательно.

В группу следует ввести менеджеров, пользователей, экспертов и технических специалистов. Менеджеры в группе нужны потому, что процедура развертывания сервера Domino требует эффективной поддержки со стороны руководства компании.

Пользователи и эксперты также должны входить в группу, поскольку сервер Domino в первую очередь призван решать их проблемы. Им необходимо участвовать в проекте, так как только они могут дать правильные советы об организации работы с сервером. Если проект предусматривает использование Web-приложений или призван решать проблемы электронной коммерции, то представители отдела продаж обязательно должны проверить

внедряемые приложения на предмет их эффективности. Менеджеры, как правило, не в состоянии осуществить подобную проверку, а пользователи могут оказаться недостаточно опытными для выполнения такой задачи. Например, внедрение Web-сайта (как средства электронной коммерческой рекламы) может потребовать привлечения экспертов по маркетингу (которые в дальнейшем не будут пользователями системы).

В группу надо непременно ввести технических специалистов по компьютерным системам, поскольку они хорошо знакомы с существующей компьютерной инфраструктурой компании и именно им предстоит производить процедуру развертывания. Желательно также, чтобы группа включала в себя экспертов по сетевым архитектурам, маршрутизации почтовых сообщений, разработке приложений, архитектуре сети Internet, обеспечению безопасности компьютерных сетей и архитектуре системы Notes. Представители разработчиков также могут дать полезные советы о необходимых ресурсах, которые понадобятся при обновлении старых или создании новых приложений системы Notes. Надо иметь в виду, что разработка приложений часто порождает потребности в новых аппаратных и программных средствах.

Оценка необходимых ресурсов

На данном этапе требуется определить, какими аппаратными, программными и сетевыми ресурсами располагает компания, а затем наметить пути модификации этих средств для поддержки развертывания сервера Domino. При этом может быть создана своего рода *карта системы*, позволяющая правильно идентифицировать аппаратные ресурсы и характер соединений между ними. Такая карта удобна для определения потребностей в серверах Domino и мест их расположения и может изменяться в ходе выполнения проекта.

Одновременно следует рассмотреть те аспекты, которые касаются текущей деятельности компании, а также ее ближайших и долгосрочных перспектив, не забывая о темпах развития и роста компании. Необходимо оценить следующие аспекты:

- *серверы*. Какие серверы применяются в текущий момент и каких затрат потребует внедрение серверов Domino? Могут ли серверы Domino быть установлены в уже имеющихся физических серверах или понадобится приобрести новые? Проанализируйте используемые операционные системы, объем дисковой памяти, объем оперативной памяти, количество и быстродействие процессоров, характеристики сетевых соединений, места расположения серверов, время доступа и характер информационной нагрузки. Также изучите новые функциональные возможности системы Notes/Domino версии 5 или 6. Так, например, если необходимо воспользоваться функцией регистрации транзакций, придется добавить или реконфигурировать дисковые накопители существующих серверов;
- *рабочие станции*. Какие рабочие станции имеются сейчас и какие станции потребуются для клиентов сервера Domino? Следует проанализировать операционные системы, объем дисковой памяти, объем оперативной памяти, количество и быстродействие процессоров, а также характеристики сетевых соединений. Надо ли устанавливать клиенты системы Notes или можно обойтись применением браузеров? Если выбор делается в пользу клиентов системы Notes, как производить их загрузку - локально или с сетевого диска? Предусматривается ли управление рабочей станцией по сети или обслуживание должен выполнять пользователь;
- *сетевые ресурсы*. Какие ресурсы имеются в наличии и какие потребуются для внедрения серверов Domino? Проанализируйте существующие аппаратные средства,

в частности кабельные соединения, сетевые адаптеры, мосты, маршрутизаторы и переключатели. Изучите используемое программное обеспечение: коммуникационные протоколы, сетевые операционные системы и программы резервного копирования. Проверьте качество сетевой защиты - брандмауэры, точки доступа и т.д. Рассмотрите методы подключения пользователей к сети, а также полосу пропускания и производительность. Проконтролируйте показатели надежности, отказоустойчивости и избыточности. Продумайте пути улучшения обслуживания пользователей и уменьшения его стоимости на основе внедрения технологических новинок, появившихся со времени создания сети. Например, если система Notes и сервер Domino работают в сети с протоколом IPX/SPX, возможно, настало время перейти к сети с протоколом TCP/IP;

- О *удаленные и мобильные пользователи*. Каким образом эти пользователи связаны с сетью? Как для них планируется доступ к серверу Domino и каким образом будет осуществляться их поддержка? Следует ли применять клиенты системы Notes? Каким способом пользователи будут обновлять коды уже установленных программ? Какие методы обеспечения безопасности/шифрования данных приемлемы для пользователей переносных компьютеров;
- О *доступ к сети Internet*. Как предоставляется в настоящее время доступ к сети Internet и должен ли он быть изменен? Какие меры безопасности при этом предпринимаются и будут ли они достаточными в будущем?

План проекта

Процедура развертывания сервера Domino - сложный проект, который требует совместных усилий многих людей. Для его успешной реализации следует составить план действий, утвердить каждый его раздел у соответствующего руководителя и в дальнейшем выполнять, не допуская заметных отклонений. Подобный подход позволит произвести все основные работы в срок и с минимальными усилиями. Он также поможет учитывать отзывы об уже выполненных этапах работы, чтобы в дальнейшем не повторять сделанных ошибок.

При подготовке плана нужно оценить необходимые ресурсы (людские, финансовые и компьютерные) и позаботиться о том, чтобы эти ресурсы были своевременно выделены.

В плане надо обязательно указывать сотрудников, несущих ответственность за осуществление определенных его разделов, причем эти сотрудники должны отчитываться о выполненных этапах (это представляется весьма важным моментом для успешной реализации всего плана). Если не назначены ответственные лица, то вполне возможно, что работа будет либо просто не сделана, либо сделана с опозданием или с низким уровнем качества. Однако у каждого сотрудника будет право указать на другого и сказать: «Я думал, что эта работа поручена ему». Если же фамилия записана в плане, человеку придется нести ответственность за ход работы (и если работа окажется незавершенной, руководитель будет знать, с кого спросить).

Необходимо также периодически отслеживать выполнение утвержденного плана. Здесь подходит типовое программное обеспечение, предназначенное для разработки и контроля проектов. Рекомендуется рассмотреть и возможность совместного применения сервера Domino и шаблона приложения TeamRoom, который присутствует в составе серверов Domino Application Server и Domino Enterprise Server версии 5. Такую деятельность лучше осуществить предварительно и придать ей статус предпилотного проекта.

Приложение TeamRoom обеспечивает совместное использование ресурсов в рамках электронного форума, где группа специалистов обсуждает различные аспекты проекта. При этом члены группы могут задавать и обсуждать различные вопросы, намечать повестку дня для следующих встреч и отслеживать результаты выполнения различных работ.

В приложении TeamRoom следует задавать название группы и определять цель ее деятельности; указывать ее руководителя, контролирующее лицо и членов группы; перечислять категории документов, которые могут формировать разные сотрудники, и типы документов, которые могут этими сотрудниками добавляться в базу данных. Имеется возможность создавать различные подгруппы, устанавливая их цели и состав, а также формулировать основные мероприятия и намечать промежуточные этапы работ.

Приложение TeamRoom применяет ряд агентов, которые автоматически удаляют старые документы из перечня используемых, уведомляют членов группы по электронной почте о появлении в базе данных документов, представляющих для них интерес, и направляют напоминания (также по электронной почте) при необходимости завершения тех или иных работ.

Приложение TeamRoom оказывается особенно полезным в тех случаях, когда группа сотрудников разнесена географически на большие расстояния и когда не все ее члены имеют в своем распоряжении компоненты системы Lotus Notes, что представляется весьма вероятным на ранних этапах выполнения проекта. Это приложение может быть установлено на сервере Domino, доступном в сети Internet или intranet. Для членов группы доступ к приложению обеспечивается с помощью клиентской программы Notes или Web-браузера.

Пилотный проект

При выполнении работ в больших компаниях их продолжительность может оказаться весьма значительной, а вероятность ошибок очень высокой. В таком случае может потребоваться реализация варианта «бета-развертывания» в виде пилотного проекта по локальному развертыванию единственного приложения. При этом следует тщательно проанализировать тип внедряемого приложения. Лучше использовать такое приложение, которое допускает достаточно простое внедрение и может быть быстро и успешно развернуто и отлажено. Тот энтузиазм, который появится при успешной реализации пилотного проекта, позволит в будущем преодолеть сопротивление некоторых пользователей.

Встраивание сервера Domino в существующую инфраструктуру

При определении методов встраивания сервера Domino в существующую инфраструктуру необходимо предварительно рассмотреть следующие аспекты:

- каким образом планируется использовать сервер Domino (как в ближайшее время, так и в долгосрочной перспективе), где будут установлены серверы Domino - во всех департаментах компании или лишь в нескольких отделах, получают ли специалисты за пределами компании (поставщики, партнеры и клиенты) доступ к этим серверам;
- как серверы Domino могут быть интегрированы в существующую сетевую инфраструктуру компании;

- О какие модификации применяемых аппаратных и программных средств потребуются для внедрения серверов Domino;
- О какова текущая корпоративная политика компании и понадобится ли в связи с внедрением концепции коллективной работы изменить подходы компании к коммерческой деятельности;
- О кто будет утверждать проект, могут ли уже сейчас быть идентифицированы исполнительные и руководящие сотрудники компании и каким образом система Notes сумеет решить их проблемы.

Оценка будущего использования системы

Количество и места расположения серверов Domino, тип применяемых клиентов и метод связи между ними определяется тем, как впоследствии планируется эксплуатировать систему Notes/Domino, а также тем, кто будет реально работать с этой системой и будут ли серверы Domino внедрены повсеместно или только в нескольких департаментах. Например, если серверы Domino намечается сделать основными компонентами системы передачи сообщений компании, необходима установка серверов Domino Mail Server. Если же внедрение серверов Domino преследует цель поддержки специальных приложений, следует установить серверы Domino Application Server. А если серверы должны обеспечить поддержку приложений, работающих в режиме 24x7 (24 часа 7 дней в неделю), то может потребоваться установка серверов Domino Enterprise Server.

Когда процедура развертывания выполняется локально (или же компания имеет только один офис), нужна установка в одном месте небольшого числа мощных серверов. Когда же развертывание намечается в масштабе всей компании, офисы которой находятся на больших расстояниях друг от друга, разумно иметь меньшее число маломощных серверов, расположенных в различных, географически удаленных местах. При подготовке проекта также следует учитывать требования к администрированию системы. Так, например, если серверы разнесены по отдаленным офисам, возникает вопрос, каким образом организовывать процесс администрирования (локально или централизованно) и в какой степени можно доверить управление системой местным администраторам.

Если пользователи системы представлены исключительно сотрудниками компании, может быть принято решение об установке клиентской программы Notes на каждом настольном компьютере. Однако в том случае, когда клиенты или деловые партнеры применяют различные приложения системы, возможно, придется установить эти приложения на Web-серверах, доступ к которым будет осуществляться с помощью Web-браузеров.

Интеграция сервера Domino в сетевую инфраструктуру

Тип применяемых серверов и места их размещения зависят от текущего и будущего состояния сети (локальная, региональная и т.д.). Задача заключается в правильном выборе типа серверов и их размещения, чтобы:

- О минимизировать сетевой трафик;
- О обеспечить удобство работы пользователей;
- О минимизировать усилия по администрированию системы;
- О снизить время отключения оборудования на техническое обслуживание.

Некоторые из этих целей иногда входят в противоречие друг с другом. Так, например, можно повысить удобство применения системы, поместив серверы Domino ближе к пользователям, чтобы не сказывалось влияние медленных соединений региональной сети (WAN). Однако для минимизации усилий по администрированию системы лучше располагать серверы в одном месте. Необходимо найти оптимальный вариант, устраивающий как пользователей, так и администраторов компании.

Минимизация сетевого трафика

Как правило, разработчики стараются минимизировать сетевой трафик для того, чтобы гарантированно избежать *информационных заторов*. Кроме того, с ростом объема трафика в сети надо увеличивать и поддерживать ее производительность (расширять *полосу пропускания*), что в свою очередь требует скоростной сетевой среды, а также увеличения числа мостов, маршрутизаторов и переключателей. А это влечет за собой необходимость привлечения к работе большого числа квалифицированных специалистов для поддержки сети в целом.

Серверы Domino генерируют высокий сетевой трафик. В то же время архитектура клиент/сервер способствует его минимизации. Приложения системы Notes уже по своей природе склонны к формированию больших объемов трафика, поскольку предполагают активный обмен сообщениями между пользователями и серверами, а также внесение изменений в базы данных, хранящиеся на различных серверах.

В общем случае минимизировать формируемый сервером Domino сетевой трафик можно за счет минимизации числа самих серверов Domino. При снижении числа серверов уменьшается репликация между базами данных, а также сетевой трафик между серверами.

Другими словами, сервер Domino должен быть установлен на большом, мощном компьютере, который в состоянии обслужить большое число пользователей. Для этих целей предусмотрено *масштабирование* сервера Domino. В последних версиях имеется возможность масштабирования отдельного сервера путем увеличения объема оперативной памяти (Random Access Memory - RAM) и числа процессоров компьютера. Чем большим будет объем оперативной памяти сервера Domino, тем больше одновременных сеансов связи он позволит обеспечить. С ростом количества процессоров сервера Domino повышаются показатели его быстродействия и снижается время реакции на запросы пользователей. Масштабирование сервера Domino может быть продолжено посредством установки в операционных системах UNIX, OS/400 или OS/390 вместо Windows или OS/2.

Обеспечение удобства работы пользователей

Если компания намеревается сделать систему Notes удобной для пользователей, она должна повысить ее производительность и эффективность. Не исключено, что пользователи, которые связываются с ближайшим сервером Domino только через медленно действующие и ненадежные линии связи региональной сети или с помощью коммутируемого телефонного соединения (а также в случае медленной реакции самого сервера), решат, что система Notes им не вполне подходит, и будут эксплуатировать систему неэффективно или совсем откажутся от ее услуг.

Чтобы этого избежать, лучше всего собрать рабочие места всех пользователей в одном и том же здании. Однако, если компания имеет многочисленные офисы, приходится вкладывать дополнительные средства для внедрения быстродействующих соединений

и формировать надежные каналы связи региональной сети, обеспечивающие нормальный режим работы для многочисленных пользователей, находящихся за десятки, сотни, а иногда и тысячи километров от сервера. Альтернативное решение состоит в увеличении числа серверов: вместо нескольких мощных серверов, расположенных в одном помещении главного офиса компании, придется установить множество маломощных серверов, разбросанных по местам работы пользователей, например непосредственно по региональным офисам компании.

Выбор стратегии на практике определяется целым рядом факторов:

- О прежде всего, типами тех приложений, с которыми планируется работать. Некоторые приложения нуждаются в постоянном и быстром доступе к серверу, а другие оказываются менее чувствительными;
- О требованиями пользователей к времени отклика сервера. Если сервер реагирует медленно и на соединение с ним уходит много времени, пользователи не станут применять систему. Если после щелчка мышью приходится ждать целую вечность, они вряд ли будут активно эксплуатировать систему. С другой стороны, если пользователи не применяют приложений, то компания зря потратит время и средства на формирование высококачественных соединений. Следует также учесть тот факт, что некоторым пользователям требуется получать доступ к серверу быстрее, чем другим;
- О текущим состоянием региональной сети и объемом денежных средств, которые могут быть потрачены на ее модернизацию. Если не удастся обеспечить надежные и быстродействующие соединения (например, согласно подсчетам специалистов компании Compaq, на каждого активного пользователя должна приходиться пропускная способность порядка 75 Кбит/с по достаточно надежной региональной сети), то единственным решением является установка локального сервера. Физический сервер вполне способен пережить медленную и ненадежную работу соединений региональной сети, чего нельзя ожидать от обычного пользователя;
- О наличием и квалификацией обслуживающего сеть персонала, например сотрудников региональных офисов компании. Если персонал в удаленном офисе не отличается высоким профессионализмом, то, возможно, руководство компании не захочет размещать в этом офисе сложное оборудование и программное обеспечение. Следует отметить, однако, что серверы Domino могут быть настроены таким образом, чтобы их обслуживание проводилось полностью дистанционно. Но для некоторых администраторов подобное положение неприемлемо, поскольку для эффективного обслуживания серверы должны находиться у них «под рукой»;
- О степенью защищенности сервера в удаленном офисе. Показатели безопасности серверов Domino во многом зависят от их физической защищенности. Если сервер не удастся должным образом защитить в том или ином офисе, руководство компании, вероятно, не захочет его там размещать.

Возможность соединения между собой удаленных офисов определяется числом этих офисов, реальным расстоянием между ними, их конкретным местоположением и бюджетом. Если офисы находятся близко друг к другу (бюджет внушительен, а уровень квалификации достаточно высок), можно попытаться проложить кабельные или организовать (в зоне прямой видимости) микроволновые линии связи между этими офисами. Для офисов, удаленных от центров цивилизации, с которыми обычная телефонная связь затруднена, весьма подходящими являются линии спутниковой телефонной связи или другие экзотические информационные технологии. Если у компании имеется доступ к кабельному

телевидению, а провайдер кабельной сети - человек прогрессивных взглядов, можно воспользоваться для решения существующих задач телевизионными кабельными линиями связи.

В большинстве случаев приходится, однако, довольствоваться общественными телефонными сетями и заключать контракт с соответствующим поставщиком услуг, в роли которого может выступать местная телефонная компания или провайдер сетевых услуг. При выборе между быстродействующими (дорогостоящими) и медленными (относительно дешевыми) соединениями обычно приходится оценивать следующие варианты:

- О формирование частной региональной сети по выделенным (арендуемым) телефонным линиям связи;
- О создание арендуемой региональной сети, например по выделенным линиям сети Frame Relay местной телефонной компании;
- О подключение к общественной региональной или глобальной сети (например, к сети Internet) по выделенным телефонным линиям, цифровым абонентским линиям DSL (Digital Subscriber Line), модемным линиям связи или коммутируемым линиям ISDN;
- О применение коммутируемых соединений по требованию между отдельными компьютерами или локальными сетями.

Среди перечисленных вариантов создание собственной региональной сети по выделенным арендуемым телефонным линиям между офисами обеспечит наилучшие показатели надежности и быстродействия, однако подобный вариант будет и самым дорогостоящим. Существенным преимуществом арендуемых телефонных линий связи является отсутствие необходимости пользоваться ими совместно с кем-то другим и можно полностью загрузить их своим трафиком.

Недостаток арендуемых линий состоит в том, что местные телефонные компании (операторы связи) сохраняют монополию на телефонные соединения с офисом, что делает такие линии достаточно дорогими. За эту монополию телефонные компании будут бороться до конца жизни, следовательно, выделенные арендуемые линии связи останутся весьма дорогостоящим решением проблемы взаимосвязи отдельных офисов компании. В отсутствие большого бюджета применение таких линий станет несбыточной мечтой, которая может быть реализована только для ограниченного числа офисов и при небольшой удаленности их друг от друга (поскольку плата взимается за каждый километр арендуемой линии).

При работе с арендуемыми телефонными линиями приходится также платить за объем трафика (то есть за полосу пропускания). Минимальная скорость передачи арендуемых линий составляет 9600 бит/с, но для наших целей больше подходят линии 56 Кбит/с. Верхняя граница скорости передачи на практике ограничивается лишь бюджетом. Для скоростей более 56 Кбит/с можно воспользоваться соединениями T-1 с пропускной способностью в 1,544 Мбит/с или соединениями T-3, пропускная способность которых достигает 45 Мбит/с. Если отсутствует необходимость в полной полосе пропускания линии T-1 или T-3, можно найти поставщиков, которые предлагают оборудование для «дробных» линий. В этом случае производится монтаж аппаратных средств, поддерживающих полную полосу пропускания линии, однако в дальнейшем используется (и оплачивается) только оговоренная часть пропускной способности. Когда требуются соединения с большей пропускной способностью, можно объединить несколько линий T-1 или T-3. Вне территории Северной Америки доступны аналогичные телефонные соединения, отличающиеся от T-1 и T-3 только названием и другими незначительными особенностями.

Частные региональные сети на основе арендуемых линий (например, сети Frame Relay) имеют следующие показатели надежности и стоимости. Скорость передачи данных в подобных сетях практически такая же, как у арендуемых линий: от 56 Кбит/с до полной линии T-1 (или выше) при дискретности увеличения 128 Кбит/с. Однако сети Frame Relay эксплуатируются совместно с другими пользователями. Телефонные компании (и подобные им провайдеры), конечно же, гарантируют быстрый доступ по крайней мере к части оплачиваемой пропускной способности, однако это совсем не означает, что доступ можно будет получить в любое удобное время. Гарантия лишь дает право не оплачивать услуги, если они предоставляются с нарушением контракта.

Компании в этом случае придется организовать для связи между офисами выделенные арендуемые телефонные линии с помощью сети Frame Relay, предоставленной провайдером. К счастью, при таких условиях плата за арендуемую линию будет небольшой, поскольку оплачивается соединение между офисом и точкой доступа (POP) провайдера, то есть фактически соединение длиной не более нескольких километров.

Следующий вариант предполагает использование в качестве региональной сети сеть Internet. Соединения с сетью Internet могут формироваться различными способами. Во-первых, имеется возможность работать с арендуемыми линиями связи между каждым офисом и ближайшей точкой доступа провайдера услуг сети Internet.

Во-вторых, в зависимости от типа услуг можно сформировать цифровые абонентские линии между каждым офисом и провайдером. Подобно арендуемым линиям связи, линии DSL обеспечат постоянную связь с сетью Internet, однако показатели быстродействия и стоимости здесь оказываются заметно меньшими, чем у арендуемых линий¹.

В-третьих, имеется возможность соединиться с провайдером с помощью коммутируемой линии связи. В общем случае для постоянной связи двух компьютеров по сети Internet необходима арендуемая линия связи или линия DSL. Те компьютеры, которые не являются постоянно доступными и сами иницируют подобный доступ к другим компьютерам в Internet, могут быть подключены по коммутируемым линиям связи.

Преимущество выбора сети Internet в качестве региональной сети состоит в низкой стоимости услуг, поскольку не приходится платить за междугородную арендуемую телефонную линию или за обслуживаемую провайдером региональную сеть. Однако следствием снижения стоимости становится заметное ухудшение показателей надежности и безопасности.

Поскольку сеть Internet не является чьей-либо собственностью, трафик в ней никем не контролируется. Поэтому никто не в состоянии гарантировать выделение необходимой полосы пропускания. В любой момент времени и без всякого уведомления скорость передачи данных между двумя компьютерами может уменьшиться в несколько раз или, что еще хуже, полностью прерваться на непредсказуемое время. Чтобы минимизировать число подобных инцидентов, следует заключить контракт с крупными национальными или международными провайдерами услуг сети Internet, поддерживающими собственные региональные сети, что позволит обеспечить устойчивую связь со всеми офисами компании. В этом случае существует определенная вероятность того, что все или по крайней мере большая часть данных между офисами будет передаваться по магистральным линиям самого провайдера, а не по магистралям сети Internet, и возникновение проблем в какой-либо

Скорее наоборот, линия DSL обладает гораздо большей пропускной способностью по сравнению с аналоговой телефонной линией, хотя в обоих случаях применяется одно и то же кабельное соединение. - *Прим. ред.*

части сети Internet не повлияет на работу компании. Естественно, что подобные провайдеры требуют более высокой оплаты своих услуг.

Другим немаловажным фактором при работе в Internet является обеспечение безопасности. Поскольку приходится пользоваться сетью Internet совместно с другими клиентами, разбросанными по всем уголкам планеты, эти клиенты способны вмешиваться в процесс передачи данных, считывать их и распоряжаться ими в преступных целях. Кроме того, посторонние лица, конкуренты и промышленные шпионы могут попытаться получить доступ (через сеть Internet) к серверам компании или просто нарушить нормальный режим работы серверов.

Следует отметить, что сервер Domino специально создан для минимизации подобных рисков. Он осуществляет аутентификацию пользователей на основе сертификатов, так что только проверенным лицам разрешается доступ к серверам, тогда как посторонние не могут установить с ним связь. Обеспечено необязательное шифрование всех данных, передаваемых через определенный порт, поэтому посторонние не в состоянии читать и использовать не по назначению передаваемые данные. Подобный метод защиты ориентирован на стандарты сети Internet и промышленные стандарты протоколов безопасности, в том числе протоколов SSL 2.0/3.0, X.509 и SMIME. Для этих целей обычно применяется встроенный прокси-сервер уровня приложений, обеспечивающий функции сквозной передачи данных вместе с поддержкой прокси-серверов HTTP или SOCKS и брандмауэров фильтрации пакетов.

Последний вариант из данного списка связан с прямым доступом по коммутируемой линии к серверу или к локальной сети (и последующим доступом через сервер к локальной или региональной сети компании). Сервер Domino поддерживает оба режима. Доступ по коммутируемым линиям самый медленный, однако он весьма дешев и достаточно безопасен. Обращение к серверу или локальной сети в этом случае может осуществляться через стандартный модем, адаптер терминала сети ISDN или маршрутизатор. Модемы обычно обеспечивают скорость передачи данных от 14,4 до 56 Кбит/с или даже до 112 Кбит/с для сдвоенных модемов, тогда как сеть ISDN позволяет передавать данные со скоростью 64 или 128 Кбит/с.

Однако только сама компания может выбрать самый подходящий вариант подключения. Пользователи (в отличие от серверов) не захотят мириться с медленными соединениями, длительным отсутствием отклика сервера и постоянно прерывающимися сеансами связи (подключениями). Поэтому на практике приходится выбирать между двумя следующими вариантами:

- О размещение серверов в центральном офисе (или нескольких центральных офисах) и предоставление соединений, способных быстро передавать большие объемы трафика пользователей. Такой подход основывается на применении региональной сети (частной региональной сети или сети с арендуемыми линиями, например сети Frame Relay или высокоскоростных соединений с сетью Internet);
- О распределение серверов по местам расположения самих пользователей, так чтобы они могли осуществлять быстрый доступ (с помощью локальной сети или быстродействующей региональной сети) к серверам, и реализация соединений, совместимых с этими серверами. Не стоит забывать, что серверы (в отличие от пользователей) допускают применение медленных и ненадежных соединений, так что можно воспользоваться низкоскоростными и относительно дешевыми региональными сетями. По той же причине удастся совсем отказаться от работы в региональных сетях, но только в том случае, если, по мнению специалистов, обеспечение коммутируемого доступа к серверам будет полностью отвечать существующим требованиям.

Минимизация усилий по администрированию системы

Минимизация усилий по администрированию совершенно необходима, поскольку не рекомендуется мириться с регулярной переработкой квалифицированных специалистов, а руководство компании вряд ли согласится нанять дополнительный персонал. Следует иметь в виду, что чем больше серверов установлено в системе, тем больший объем работы предстоит проделать. С этой точки зрения надо стремиться обойтись небольшим числом мощных серверов.

Если же в соответствии с пожеланиями самих пользователей (которые все же обладают более высоким приоритетом при выборе конфигурации) потребуется много серверов, не стоит сильно волноваться, поскольку сервер Domino воплощает в себе заветную мечту администраторов. Интерфейс администрирования в одном месте предоставляет 99% всех средств по управлению сервером, упорядоченных согласно задачам администрирования. Единственная операция администрирования, которую не удастся выполнить удаленно, - перезагрузка сервера, но и это ограничение преодолевается путем установки соответствующего программного обеспечения. Скорее всего, даже нестандартные операции с компьютером (в процессе перезапуска) легко выполнить по телефону (но это уже из области гипотез).

Снижение времени технического обслуживания

Хорошо известно, что жесткие диски выходят из строя, электронные устройства отказывают, программные средства содержат вирусы, пользователи отключают кабели, поэтому надо сразу оценить, насколько названные неполадки повредят работоспособности системы. Следует обеспечить избыточность и необходимую систему резервирования, чтобы предельные уровни риска никогда не выходили за границы, признанные допустимыми в данном проекте. Каждая компания сама устанавливает предельные уровни, а конкретные потери от простоев зависят от характера используемых приложений системы Notes. Кроме того, при попытках устранения неисправностей нельзя забывать о финансовых средствах, которые придется на это потратить.

На практике в системе могут возникать следующие типы отказов:

- О нарушения в подаче электропитания;
- О отказы дисковых накопителей;
- О отказы всего сервера;
- О отказы локальных/региональных сетей;
- О повреждения зданий.

Нарушения в подаче электропитания

Низкое качество электропитания (провалы, выбросы, помехи и шум) может вызывать различные отказы в работе оборудования. Выход из строя *устройств питания* - это лишь один пример серьезной проблемы. Требуется снабжать серверы высоконадежными *источниками бесперебойного питания* и конфигурировать программное обеспечение таким образом, чтобы оно способствовало (совместно с источниками питания) плановому отключению серверов при возникновении серьезных проблем с питанием. В зависимости от складывающейся обстановки специалисты могут предпринять и иные меры в этом направлении (например, предусмотреть аварийный генератор).

Отказы накопителей жестких дисков

Хотя дисководы представляют собой достаточно надежные устройства, все же существует риск их выхода из строя, последствия которого могут быть самыми печальными. Для защиты от отказов дисковых накопителей следует всегда предусматривать какие-либо меры резервирования, например резервные *накопители на магнитной ленте*.

Время от времени необходимо проверять работоспособность резервных устройств, чтобы убедиться в их исправности. Рекомендуются также периодически контролировать сроки хранения архивных носителей, что позволит сохранять большие объемы резервируемых данных в течение длительного времени и исключить их потерю (но сроки хранения не должны быть настолько большими, чтобы компании грозили юридические иски). И наконец, при установке сервера Domino можно попытаться модифицировать уже используемые *процедуры резервирования* с целью привнесения в них функции регистрации транзакций (новая функция, появившаяся в версии 5).

Следует также рассмотреть необходимость применения для серверов функции RAID (Redundant Array of Inexpensive/Independent Drives - избыточный массив недорогих/независимых дисков), которая обеспечивает запись данных на резервные диски, чтобы при отказе одного диска не терялась записанная на нем информация. Конечно, информация не будет потеряна и при наличии резервного накопителя на магнитной ленте. Однако в этом случае фактически утрачивается доступ к данным (вплоть до момента замены отказавшего дисковода и восстановления продублированных данных на новом диске). Такая процедура на практике может оказаться весьма трудоемкой. При использовании же функции RAID даже в условиях потери доступа к отказавшему диску доступ сохраняется к самим данным, поскольку они присутствуют на другом диске (или дисках).

Ниже рассмотрены наиболее типичные варианты функции RAID.

Функция RAID 1. Устанавливаются два идентичных диска: запись информации производится одновременно на оба диска. При отказе одного дисковода все нужные данные будут получены с другого. Преимущество такого подхода перед другими состоит в обеспечении высоких скоростей записи/чтения информации. Недостатком функции RAID 1 является высокая стоимость из-за наличия двух физических дисководов для каждого логического диска.

Функция RAID 5 (применение чередующихся наборов с контролем четности). В этом случае блоки данных чередуются и распределяются по трем или более дискам. Каждый блок дополняется служебной информацией для *контроля четности*. При отказе одного из дисководов записанные на нем данные легко восстановить по служебной информации, хранящейся на другом диске¹. Восстановление информации обеспечивается в реальном времени вплоть до момента замены отказавшего дисковода. В дальнейшем данные могут быть восстановлены и на новом диске. Функция RAID 5 оказывается более «экономной» в части расходования дисковой памяти (по сравнению с функцией RAID 1), поскольку она не предполагает записи каждого информационного разряда на два диска. С увеличением числа накопителей в массиве растут и показатели экономичности, демонстрируемые функцией RAID 5. Недостаток подхода состоит в том, что в связи с необходимостью проведения определенных преобразований замедляется процедура доступа к диску.

¹ Происходит чередование на разных накопителях основной и служебной информации. - *Прим. ред.*

Функция RAID 10 (функция RAID 0 плюс функция RAID 1 - два продублированных чередующихся блока без контроля четности). В данном случае предусматривается чередование на трех или более накопителях, что позволяет быстро считывать/записывать информацию (в условиях одновременного использования нескольких головок записи/считывания). Такой подход позволяет достичь высокой скорости при защите дублированием. В результате формируются два зеркальных чередующихся набора дисков. Преимущество этой функции перед функциями RAID 1 и RAID 5 заключается скорее в улучшении показателей быстродействия, чем в повышении целостности данных.

Отказы серверов

Отказы серверов могут происходить из-за неполадок материнской платы или источника питания, а также из-за нарушений в работе программного обеспечения. Для защиты от отказов аппаратных средств (а в некоторых случаях - и программных средств) следует формировать кластеры серверов и использовать их на уровне операционной системы или на уровне Domino (или на обоих уровнях). Серверные кластеры уровня операционной системы обычно бывают двух типов - активные и пассивные.

В *пассивном серверном кластере* два компьютера совместно работают с одним или несколькими дисковыми. Один из серверов управляет этими устройствами и выполняет соответствующие программы, тогда как другой остается в пассивном режиме и ожидает момента отказа первого сервера. После отказа первого сервера второму передается управление всеми дисковыми и он продолжает реализацию текущих программ. Недостатком описанной структуры является наличие двух компьютеров, из которых действует только один.

В *активном серверном кластере* каждый из серверов управляет одним или несколькими общими дисковыми и исполняет соответствующие программы. Если один из серверов отказывает, другой принимает на себя управление его дисковыми и продолжает выполнение текущих программ. Преимуществом этого подхода является то, что оба компьютера применяются по непосредственному назначению и не допускается длительных простоев одного из них, как в пассивной структуре.

Недостаток активной структуры состоит в том, что сервер Domino далеко не всегда может выступать в качестве сервера кластера. Например, при использовании операционной системы Windows NT, как правило, не рекомендуется исполнять какие-либо иные программы на компьютере, где установлен сервер Domino. Если один из серверов активного кластера представлен, скажем, сервером Oracle, а другой - сервером Domino, то при отказе одного из этих серверов второй будет работать за двоих, однако последствия подобной работы предсказать совершенно невозможно. В альтернативном варианте, когда каждый из серверов представлен сервером Domino, при отказе одного сервера другой попытается справиться с задачей за двоих. Однако для качественного выполнения работы следует установить на обоих компьютерах серверы Domino Enterprise Server и провести для них операцию сегментирования. При этом на одном компьютере будет установлен один *сегментированный сервер*. Тогда при его отказе второй сегментированный сервер Domino (на втором компьютере) примет на себя функции обоих серверов Domino.

При формировании кластера серверов Domino (в случае серверов Domino Enterprise Server) числом от двух до шести они могут работать совместно, поддерживая друг друга в случае отказа. Если один из серверов Domino в кластере перестанет справляться с нагрузкой или откажет, его пользователи будут автоматически переданы на другие серверы кластера (см. главу 20).

Для защиты от отказов сервера вследствие сбоев программного обеспечения можно предпринять целый ряд мер. Некоторые операционные системы (например, OS/400) обеспечивают регистрацию отказов сервера Domino и иницируют его перезапуск. Для других платформ Domino существуют программы контроля, которые выполняют перезапуск сервера Domino в случае его отказа. Примером служит программа Intellivatch компании Candle, однако на рынке присутствуют и другие программы такого типа. Нетрудно приобрести программные продукты, позволяющие перезагрузить компьютер при обнаружении сбоя в операционной системе или работающей программе. Для уменьшения рисков, которые связаны с воздействием посторонних программ, исполняемых сервером Domino, и блокированием этого сервера, необходимо следовать рекомендациям компании Lotus и никогда не пытаться установить серверы другого типа на компьютере, служащем базовым для сервера Domino (подобные проблемы не раз имели место в операционной системе Windows NT).

Компании, которым требуется быстрый доступ к серверам и приложениям, могут с помощью вышеуказанных программных инструментов улучшить методы доступа. При этом компьютеры, предназначенные для установки серверов, должны снабжаться резервными блоками, а соответствующие серверы - сегментироваться и объединяться в кластеры серверов Domino (на уровне операционной системы). Для них также надо применять программы контроля, осуществляющие слежение за функционированием серверов и принимающие необходимые меры при возникновении каких-либо проблем.

Отказы локальных/региональных сетей

Отказы локальных/региональных сетей маловероятны, но ведут к весьма серьезным последствиям. Если нужна защита от отказа локальной сети, имеет смысл установить избыточное резервное оборудование: файловые серверы с «горячей» заменой блоков (то есть без остановки серверов), дополнительные адаптеры локальной сети и резервные локальные сети. Система только выиграет от присутствия двух адаптеров, поскольку серверы смогут взаимодействовать друг с другом по одной локальной сети, тогда как пользователи будут обращаться к серверам Domino по второй локальной сети.

Если компания располагает частной региональной сетью, то появляется возможность пользоваться соединениями сети Internet как резервными. Если в качестве региональной сети планируется Frame Relay или сеть Internet, стоит предусмотреть в них ряд резервных соединений с одной или несколькими точками доступа. Допустимо также включить резервные коммутируемые соединения между серверами Domino и мобильными пользователями.

Повреждения зданий

Для защиты от таких проблем, как пожар и естественные природные катаклизмы, следует применять резервную группу серверов, расположенную в другом месте (например, в сотне километров от основной группы). В качестве менее дорогостоящей альтернативы можно рекомендовать заключение контракта на аренду сервера Domino на случай выхода из строя основного сервера.

Сетевые протоколы

Серверы Domino и клиенты системы Notes характеризуются функциональной гибкостью, особенно в части работы с сетевыми протоколами. Для связи между ними могут служить протоколы, представленные в табл. 2.1.

Таблица 2.7. Сетевые протоколы, поддерживаемые сервером Domino и системой Notes

TCP/IP	Набор (стек) протоколов позволяет взаимодействовать с сетью Internet и сетями UNIX, является наиболее удобным для работы в крупных сетях. В рамках операционной системы Microsoft Windows NT 4.0 компания Microsoft использует эти протоколы по умолчанию. В операционной системе NetWare 5.0 компании Novell данные протоколы также применяются по умолчанию
NetBIOS over IP	Сервер Domino или система Notes, использующая протокол TCP/IP, может в альтернативном варианте использовать протокол NetBIOS поверх протокола IP (вместо протокола TCP поверх протокола IP)
IPX/SPX	Протоколы, традиционно применяющиеся в сетях NetWare, которые основаны на операционной системе компании Novell. Допускается их использование в сетях на базе операционной системы Microsoft Windows NT 3.5 и выше. Протокол обеспечивает высокие показатели быстродействия в небольших сетях и может применяться в сетях с маршрутизаторами и мостами
NetBIOS over IPX	Сервер Domino или система Notes, работающая с протоколом IPX/SPX, может в альтернативном варианте использовать протокол NetBIOS поверх протокола IPX (вместо протокола SPX поверх протокола IPX)
NetBEUI/NetBIOS	Протокол, применяющийся в первых сетевых продуктах компаний Microsoft и IBM, в частности в Microsoft Network, совместно разработанным компаниями 3Com и Microsoft и поступавшим на рынок под различными торговыми марками (например, Microsoft LAN Manager, IBM LAN Server, DEC Path Works), и в операционной системе Windows NT 3.1 и выше. Это скоростной протокол для небольших сетей, в которых могут присутствовать мосты, но не маршрутизаторы
Vines	Протокол, традиционно устанавливаемый в сетях Banyan Vines, которые также обеспечивают поддержку TCP/IP
AppleTalk	Протокол, применяющийся в сетях Apple Macintosh, которые также реализуют поддержку TCP/IP

Сервер Domino и система Notes используют протокол NetBIOS в сетях NetBEUI, но могут применить его на компьютерах, работающих с протоколами TCP/IP или IPX/SPX. Преимущество, возникающее при установке на сервере Domino или в системе Notes протокола NetBIOS поверх IP или IPX, связано с тем, что два компьютера применяют разные протоколы нижнего уровня (TCP/IP, IPX/SPX или NetBEUI), но могут нормально взаимодействовать друг с другом, поскольку все три указанных протокола поддерживает протокол NetBIOS. Протокол NetBIOS обычно устанавливается в сети NetBEUI, а протоколы IP и IPX обеспечивают поддержку протокола NetBIOS вместо TCP и SPX соответственно.

За последние два года, когда сеть Internet и ее протоколы стали практически общедоступными, большое число специалистов в мире высказалось в пользу протоколов TCP/IP. Специалисты компании Lotus не являются исключением. Хотя сервер Domino и система Notes продолжают поддерживать другие сетевые протоколы, целый ряд функций сервера Domino выполняется заметно лучше для протоколов TCP/IP, а некоторые функции могут быть реализованы только совместно с этими протоколами. Например, функции автоматического восстановления после отказа и балансировка нагрузки серверов Domino в кластере

осуществляется наилучшим образом в том случае, когда клиенты выбирают для связи протоколы TCP/IP. Следует также отметить, что Web-браузеры, а также почтовые программы POP3 или ШАР, не могут взаимодействовать с сервером без протоколов TCP/IP.

Есть и другие причины (кроме интенсивного развития сети Internet), по которым протоколы TCP/IP рассматриваются в наши дни в качестве предпочтительных по сравнению с другими сетевыми протоколами. В частности, они поддерживают функции DNS, ARP, RARP и NIS и уже только благодаря этому более эффективны в крупных сетях. Поскольку все существующие сети демонстрируют тенденции к росту и появлению сложных связей, данное свойство становится весьма ценным.

Основная мысль, однако, состоит в том, что совместно с сервером Domino и системой Notes можно применять любой из поддерживаемых протоколов (см. табл. 2.1), но лучше остановиться на протоколах TCP/IP. Имеется и возможность работы с любой комбинацией из поддерживаемых протоколов. Например, сервер Domino и клиенты системы Notes могут в случае необходимости одновременно пользоваться протоколами TCP/IP и IPX/SPX.

При организации сетевой структуры необходимо помнить, что у двух взаимодействующих компьютеров должен быть один и тот же протокол связи. Так, если сервер Domino поддерживает протоколы TCP/IP, а устройство клиента системы Notes - протокол AppleTalk, они не сумеют «общаться» напрямую. То же самое относится к случаю, когда один сервер применяет протоколы TCP/IP, а второй - протоколы IPX/SPX: они, в частности, не будут в состоянии правильно выполнять операции копирования данных и маршрутизировать почтовые сообщения. (В приведенных примерах двум компьютерам удастся взаимодействовать только косвенно, например через промежуточный сервер, работающий с обоими типами протоколов, но подобная конфигурация должна быть предусмотрена в ходе первоначальной настройки.) Кроме того, если необходимо сделать выбор между обеспечением поддержки протоколов на сервере или на рабочей станции, всегда предпочтительнее остановится на варианте с сервером.

Конфигурации аппаратных средств: требуемые модификации аппаратных и программных средств

В конце главы 1 перечислены аппаратные платформы и операционные системы, подходящие для установки сервера Domino и системы Notes. Большая часть компаний выбирает платформу исходя из уже имеющихся ресурсов, с учетом приобретенного опыта администрирования. Как правило, использовалась операционная система Windows NT. Однако при большем числе пользователей на один сервер или когда необходима высокая надежность, неизбежно приходится выбирать платформы типа UNIX, AS/400 и S390: эти платформы дают заметно лучшие показатели масштабирования и надежности, чем платформа Windows NT.

Существенно более сложным при планировании развертывания сервера Domino является вопрос о мощности физического сервера, причем данный вопрос никак не связан с использованием какой-либо платформы. Одновременно приходится решать вопросы о числе серверов, числе процессоров для каждого сервера, объеме оперативной памяти, а также об объеме дисковой памяти, которые необходимы для поддержки определенного количества пользователей. Вопрос относительно числа серверов мы обсуждаем на протяжении всей главы. Ответ зависит от числа пользователей, которых может обслужить каждый сервер, что определяется числом процессоров, объемом оперативной памяти и числом жестких дисков. На вопрос об объеме жестких дисков ответить относительно просто, поэтому именно

с него и целесообразно начать обсуждение. Вопросы о числе процессоров и объеме оперативной памяти оказываются несколько более сложными и будут рассмотрены в последнюю очередь.

Требуемый объем памяти жестких дисков и их конфигурация

Если отвлечься от аксиомы, согласно которой объема дисковой памяти никогда не бывает много, то окажется, что на ранней стадии затруднительно правильно оценить этот объем. Специалисты компании Lotus утверждают, что для установки сервера Domino необходим объем дисковой памяти порядка 270 Мб, и советуют выделять порядка 1 Гб под программы и данные. Но такие рекомендации относятся к этапу установки, а в дальнейшем обязательно наступает момент, когда указанных объемов памяти перестает хватать. Кроме того, всегда желательно иметь в системе более одного дискового.

Для почтовых серверов Domino (которые нуждаются в наибольших объемах дисковой памяти) рекомендуется предусмотреть порядка 50 Мб в расчете на одного пользователя почтовой службы. Следует иметь в виду, что, как бы ни стремились администраторы системы контролировать своих пользователей (а сервер Domino предоставляет для этого мощные программные инструменты), им вряд ли удастся преодолеть тенденцию сохранять все сообщения, которые только приходят на их адрес.

Для других типов серверов Domino надо предварительно проконсультироваться с разработчиками приложений, планирующих применять эти серверы, и определить характер приложений, а также необходимые для них объемы дисковой памяти. Если связаться с разработчиками не удастся или они не оказывают должного содействия, можно организовать проверку приложений самостоятельно и найти объем дисковой памяти, требуемый для размещения различных документов (с учетом потенциально возможного их числа). Кроме того, вместо попыток заранее оценить нужный объем дисковой памяти можно просто конфигурировать сервер таким образом, чтобы в будущем не возникало проблем с добавлением новых накопителей.

Тем не менее вне зависимости от объема используемой дисковой памяти, при конфигурировании системы надо обязательно принимать во внимание изложенные ниже соображения.

Сервер должен иметь по крайней мере два независимых накопителя на жестких дисках, а еще лучше - три. При этом каталоги операционной системы и каталоги приложений сервера Domino будут храниться на одном диске, а каталоги данных сервера Domino - на другом. Журнал транзакций можно поместить на третий диск (если он присутствует) или на первый (при наличии всего двух).

Важным моментом является размещение журнала транзакций на диске, на котором не хранятся файлы данных, регистрируемые этими транзакциями. Сервер Domino обращается к базам данных системы Notes лишь эпизодически, а к журналу транзакций - регулярно. Если базы данных и транзакции будут храниться на одном физическом диске, постоянное переключение режимов доступа приведет к заметным временным задержкам при записи и быстрому истиранию рабочих головок. Первое отрицательно сказывается на данных, а второе плохо влияет на оборудование.

Рекомендуется также воспользоваться дисковым массивом RAID, а не отдельными дисковыми. При этом следует выбрать массив RAID по крайней мере для хранения журнала транзакций (в данном случае лучше работать с функциями RAID 1 или RAID 10, поскольку они получают наиболее быстрый доступ к данным). Для обеспечения надежной защиты

программы и информационные файлы также нужно хранить в массиве RAID, причем вполне допустимо применять RAID 5, поскольку в этом случае время доступа не играет большой роли. Конечно же, компании могут планировать различные конфигурации дисковых массивов RAID и устанавливать, скажем, режим RAID 7 при необходимости улучшить те показатели быстродействия или безопасности, которые реализуются в режиме RAID 1, 5 и 10.

Требуемые число процессоров и объем оперативной памяти

Минимально допустимый и рекомендуемый объемы оперативной памяти для сервера Domino составляют соответственно 44 и 96 Мб (в Windows и OS/2) или 64 и 128 Мб (в UNIX) при одном процессоре. Однако эти цифры хороши для проведения маркетинговых мероприятий, а на практике, конечно, не следует ограничиваться минимальными параметрами при условии, что сервером обслуживаются даже относительно небольшие группы пользователей (небольшой может считаться группа в 50, 100 или 200 человек).

Необходимое число процессоров и нужный объем оперативной памяти зависят от числа одновременно обслуживаемых пользователей и от того, чем эти пользователи будут заниматься: одни задачи требуют существенно больших мощностей сервера, чем другие. Например, пользователи, формирующие объемные документы, работающие с различными агентами, проводящие полнотекстовый поиск и осуществляющие репликацию данных, загружают сервер сильнее, чем те, кто ограничивается считыванием и записью почтовых сообщений.

Некоторые типы деятельности пользователей приводят к возникновению информационных заторов (узких мест). Так, при интенсивной полемике в ходе организуемых дискуссий и при продолжительном поиске в базе данных могут появиться проблемы с пропускной способностью, поскольку правом доступа в этом случае желают воспользоваться одновременно многие. В результате сервер в состоянии обеспечить существенно большее число пользователей почтовой службы, чем пользователей, участвующих в дискуссиях, проводящих поиск и применяющих другие подобные приложения.

Указанное разнообразие затрудняет оценку необходимой мощности серверов; например, заранее трудно предвидеть тот набор задач, которые придется выполнять серверу. Возможно, при этом удастся прогнозировать общее число пользователей системы, однако вряд ли получится угадать число пользователей определенного сервера Domino в определенный момент времени. И даже в том случае, когда можно достаточно точно предсказать характер планируемой деятельности, весьма непросто трансформировать эти данные в требования к конфигурации аппаратных средств. На практике такая задача является достаточно сложной, причем трудность состоит еще и в том, что специалисты компании Lotus оптимизируют сервер Domino при переходе на новые версии, и один и тот же компьютер с версией R6 оказывается в два раза эффективнее, чем с версией R5, которая обеспечивает поддержку в пять раз большего числа пользователей, чем версия R4.6. Сложно воспользоваться характеристиками производительности, которые были получены для версии R4, при попытках оптимизации конфигурации для версии R5 или R6.

Компания Lotus в настоящее время предлагает целый ряд программных инструментов для определения параметров аппаратных средств, в том числе программы Lotus Notes Bench, Domino Server.Planner и Domino Server.Load. Существуют также программные инструменты и службы других компаний, которые могут помочь в решении этой задачи:

- О *NotesBench* - программный инструмент, который может послужить изготовителям аппаратных средств для определения производительности и мощности системы Notes

на определенном компьютере. С помощью этой программы тестировщики могут запускать сценарии, моделирующие рабочую нагрузку на проверяемой платформе. Они имеют возможность последовательно увеличивать число зарегистрированных пользователей и изменять характер их деятельности в широком диапазоне. Программа NotesBench обеспечивает сбор необходимых статистических данных, например регистрирует время реакции сервера, число транзакций в единицу времени, коэффициент использования (утилизацию) центрального процессора, коэффициент использования памяти, а также коэффициент использования ввода/вывода. Сценарии и тестовые условия являются стандартными, а результаты тестирования представляются в установленной форме и проходят необходимую проверку. Это гарантирует выполнение всеми изготовителями одинаковых тестовых испытаний, а также позволяет сопоставлять и анализировать результаты, полученные разными изготовителями. Аудит результатов тестирования может осуществляться двояко: в виде результирующего отчета об испытаниях и в виде соответствующего набора данных. В отчете в краткой форме приводятся данные, необходимые для восприятия человеком, а набор данных (так называемая база данных Vendor Database) представляет собой блокированную от записи базу данных системы Notes, которую можно использовать в качестве входных данных для программы Domino Server.Planner;

- О *Domino Server.Planner* - это набор шаблонов базы данных системы Notes, которые используются с сервером Domino и позволяют провести сравнение тестовых результатов, полученных с помощью программы NotesBench, с планируемой нагрузкой сервера, что дает возможность выбрать самый приемлемый вариант конфигурации аппаратных средств. Допустимо задавать в программе дополнительные требования относительно числа пользователей с различными типами деятельности, а Server.Planner сама укажет конфигурацию, которая в наибольшей степени отвечает планируемой нагрузке;
- О *Domino Server.Load* является средой сценариев компании Lotus, в которой можно моделировать различные виды деятельности на сервере Domino, работающем на платформе Windows/Intel. С ее помощью легко разрабатывать сценарии на различных языках программирования и в реальном масштабе времени корректировать переменные в сценариях. Программа опубликована по адресу www.lotus.com/performance и будет весьма полезной для тех пользователей серверов Domino, которые хотят оценить возможности существующего оборудования (но не для того, кто впервые собирается применить сервер Domino);
- О партнеры компании Lotus поставляют следующие программные инструменты, предназначенные для планирования характеристик и параметров системы: программу ProActive Assistant компании G2 Associates (www.g2sys.com), программы GroupSizer Pro, MailSizer и WebSizer компании Technovations, Inc. (www.technovations.com), программу Intelliwatch Pinnacle компании Candle (www.candle.com) и программу interaction (www.interdotaction.com). Подобно программе Domino Server.Planner, названные программы подходят пользователям, уже применяющим сервер Domino, и оказываются менее эффективными для тех, кто только планирует установить этот сервер.

К сожалению, применение перечисленных программных инструментов для генерации данных о конфигурации сервера - дело не простое и не быстрое. Одна из возникающих при этом проблем связана с тем, что изготовители аппаратных средств не публикуют наборы данных, необходимые для программы Server.Planner (поэтому на практике следует

просто игнорировать инструкции программы Server.Planner о загрузке наборов данных с Web-сайта notesbench.org ввиду отсутствия там информации). Фактически изготовители доводят до широкой общественности только отчеты о результатах испытаний, причем таким образом, чтобы их серверы выглядели как можно привлекательнее. Для этого они, как правило, применяют тестовый сценарий, который предусматривает незначительную нагрузку на серверы, только для почтовой службы (Mail Only), что собственно и приводит к завышению числа обслуживаемых пользователей для данной аппаратной конфигурации. Однако на практике пользователи заметно интенсивнее и разнообразнее задействуют ресурсы сервера, так что он, скорее всего, не обеспечит поддержку того количества пользователей, которое указывается в итоговом отчете изготовителя.

В подобной ситуации у пользователя имеется четыре возможных варианта, которые ниже перечисляются в порядке улучшения точности и возрастания стоимости:

- О провести грубую оценку, основываясь на публикуемых данных;
- О обсудить свои проблемы с поставщиками аппаратных средств, предназначенных для создания серверов;
- О заключить контракт с какой-либо компанией для подготовки данных программы NotesBench в лабораторной среде и на основе сведений о составе задач сервера;
- О организовать проведение пилотных испытаний в собственной компании и в своей операционной среде.

Для первого варианта дальше обсуждается несколько аспектов, которые не следует упускать из виду:

- О можно найти опубликованные отчеты (по результатам работы с программой NotesBench) по адресу www.notesbench.org и на Web-сайтах компаний-изготовителей компьютерного оборудования, в том числе компаний IBM, Sun, Hewlett Packard, Compaq (www.compaq.com, www.digital.com), а также компании Dell. Как уже упоминалось, все результаты обычно приводятся для сервера Domino версии 4.x. Вероятно, к тому моменту, когда эта книга будет опубликована, появятся результаты испытаний серверов Domino R5 и R6;
- О практически все публикуемые результаты испытаний учитывают только нагрузку почтовой службы, что совершенно недостаточно для правильной оценки нагрузки сервера (изготовители справедливо полагают, что люди сначала смотрят на указанное максимальное число пользователей и лишь потом задают вопросы, если таковые возникают);
- О как правило, максимально возможное число пользователей для почтовой службы сервера Domino версии 4.6 следует разделить на три и вычесть еще по крайней мере 25% (для создания определенного запаса). Таким образом удастся реально оценить максимальное количество пользователей, обслуживаемых заданной конфигурацией. Однако в дальнейшем надо умножить результат на 1,8, чтобы учесть эффективность сервера Domino версии 5.0, или на 2,8 в случае Domino R6;
- О в действительности не существует надежных способов преобразования результатов программы NotesBench (для сервера Domino версии 5.0 или 6.0) в число реально поддерживаемых пользователей, поскольку по этим вопросам пока еще не накоплена необходимая статистика. Однако программа NotesBench позволяет грубо оценить число пользователей, поэтому в расчетах не приходится сильно занижать возможности сервера Domino версии 5.0 или 6.0, ориентируясь только на результаты, полученные для версии 4.6. Дополнительные сведения по этому вопросу имеются по адресу www.notes.org/guestdsc.nsf;

- О можно также поинтересоваться результатами практической деятельности других пользователей сервера Domino. Подобная информация имеется в двух источниках: в данных консорциума NotesBench Consortium (www.notesbench.org/guestdsc.nsf) и сведениях об успешном внедрении серверов (www.lotus.com/performance):
- О другой рекомендуемый подход связан с приблизительной оценкой минимального объема оперативной памяти сервера. Такой показатель обычно определяется путем умножения планируемого числа пользователей на 300 Кб, хотя сейчас уже никто не помнит, откуда взялась именно эта цифра;
- О число сеансов связи пользователей, которое может одновременно обеспечить сервер, ограничено доступной оперативной памятью. Время отклика сервера на запрос пользователя напрямую зависит от числа процессоров;
- О как уже упоминалось, специалисты компании Lotus не в состоянии точно указать число процессоров, которыми способен эффективно управлять сервер Domino версии 5 или 6. Они полагают, что это число составляет от 6 до 8 для процессоров RISC и от 3 до 4 для процессоров компании Intel. Дополнительные сведения представлены по адресу www.notesbench.org/guestdsc.nsf.

Что касается второго варианта определения конфигурации аппаратных средств (обсуждения с поставщиками), то заранее нельзя предсказать, насколько полезным может оказаться такое обсуждение. Тем не менее компания Lotus настойчиво рекомендует прибегнуть именно к нему. Если планируется приобретать оборудование у партнеров Lotus (речь идет о компаниях Compaq/Digital, Hewlett Packard, IBM или Sun Microsystems), их специалисты, без сомнения, окажут посильную помощь. Эти поставщики применяют программу NotesBench и имеют результаты испытаний, а значит, предоставят все необходимые наборы данных для программы Server.Planner. Можно также попросить поставщика посредством NotesBench оценить заказываемые программы и получить необходимые данные для Server.Planner.

Если поставщик не соглашается выполнить подобную работу и подготовить соответствующие наборы данных, нетрудно обратиться в стороннюю компанию. Так, компания Lotus Consulting, а также любая другая из числа партнеров Lotus, с удовольствием возьмется за эту задачу. Названия компаний, являющихся официальными партнерами Lotus (Lotus Business Partners) и обеспечивающих квалифицированное выполнение указанных работ (в частности, планирование и проведение расчетов с помощью программы NotesBench), представлены на Web-сайте компании Lotus (www.lotus.com/performance).

И наконец, как не устают повторять представители компании Lotus, наилучшим способом для определения требований к аппаратным средствам является проведение испытаний в собственной среде, то есть реализация пилотного проекта с учетом тех приложений, которые в будущем намечено установить, и последующее тщательное изучение результатов. Те же самые компании, которые посредством программы NotesBench формируют соответствующие наборы данных, помогут в организации и реализации пилотного проекта, а также квалифицированно проанализируют полученную информацию.

Формирование внутренней инфраструктуры

Во время установки первого сервера Domino обычно требуется указать имя домена, имя организации, имя сервера и имя одного пользователя, а также задать параметры защиты

для сервера Domino. Перед выполнением работ следует сформулировать политику безопасности для сервера Domino и правила присвоения имен. Для этого надо правильно представлять себе внутреннюю структуру сервера Domino и понимать, насколько она должна соответствовать внутренней структуре компании.

В следующих разделах будут рассмотрены такие понятия, как:

- *домены Domino* (сколько доменов использовать, какими могут быть их имена);
- *организация* (сколько будет организаций, сколько организационных уровней может быть сформировано, каким образом схема организации отражает внутреннюю структуру самой компании, какими могут быть имена организаций);
- *именованные сети* (со сколькими именованными сетями работать, каким образом именованные сети отражают нижележащую сетевую архитектуру, каковы допустимые имена);
- *безопасность* (какова политика в области обеспечения безопасности и какие меры предпринимать для обеспечения адекватного уровня защиты).

Пользователю также придется указать топологию, расписание и политику для репликации баз данных и маршрутизации почтовых сообщений. Следует отметить, что задание упомянутых параметров на данном этапе еще не является ответственным шагом, так что подробное обсуждение этого вопроса предстоит в последующих главах.

Структура: домены, организации, именованные

Серверы Domino могут самоорганизовываться по трем направлениям: по доменам, по организациям и по именованным сетям. Каждый сервер действует в рамках некоторого домена Domino. Имя любого из серверов зависит от организации, к которой он принадлежит. Кроме того, каждый сервер относится к одной или большему числу именованных сетей Domino и характеризуется связями с ними.

При первоначальном развертывании сервера Domino (первый сервер компании) следует задавать количество доменов, организаций и именованных сетей, а также имена и правила их присвоения. Если установка сервера Domino происходит в компании, уже применяющей подобные серверы, нужно указать место нового сервера в имеющейся инфраструктуре. В обоих случаях необходимо поместить новый сервер и его пользователей на определенный уровень существующей иерархии и присвоить им имена в соответствии с установленными правилами.

Домены

Домены Domino характеризуют те границы, которые устанавливаются для передачи почтовых сообщений и управляющих команд сервера, и соответствуют группе серверов Domino, совместно эксплуатирующих базу данных Domain Directory (Каталог домена). Эта база данных отражает структуру каждого отдельно взятого домена Domino. Данные всех серверов Domino, принадлежащих домену Domino, содержатся в упомянутой базе, копия которой хранится на сервере. (В случае присутствия на сервере нескольких баз данных Domain Directory, та из них, которая определяет домен сервера, будет храниться в файле names.nsf.) Эта ситуация проиллюстрирована на рис. 2.1.

Каждый сервер домена представлен в базе данных Domain Directory с помощью документа сервера (Server document), определяющего сам сервер и его конфигурацию. Имя сервера

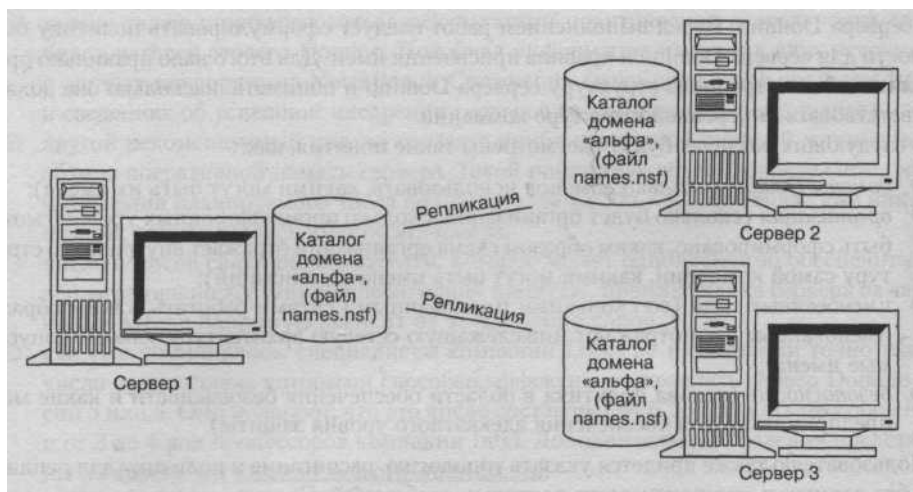


Рис. 2.1. Все серверы в домене обслуживают копии-реплики базы данных Domain Directory (файл names.nsf)

в домене (доменное имя) записано в поле **Domain** (Домен) указанного документа, а также в переменной Domain серверного файла notes.ini (текстовый файл, хранящийся в компьютере сервера и содержащий дополнительную информацию о конфигурации сервера).

Таким образом, имя домена сервера появляется в двух местах, причем оно должно быть одинаковым у всех серверов данного домена. Сервер, для которого имя домена задается некорректно хотя бы в одном месте, не будет нормально взаимодействовать с другими серверами домена.

Пользователи также принадлежат к какому-либо домену Domino. Каждый пользователь является членом того же самого домена, что и его сервер, и имеет персональный документ (Personal document) в базе данных Domain Directory, содержащий необходимое описание пользователя. Имя домена для любого пользователя указано в поле **Domain** его персонального документа, а также в поле **Domain** всех документов местоположения (Location document), присутствующих в персональной книге адресов (Personal Address Book).

Домены Domino устанавливают границы выполнения многочисленных функций, основной из которых, как правило, является передача почтовых сообщений. Почтовые сообщения, адресованные пользователям системы Notes, должны сопровождаться адресом типа username@domainname (имя пользователя@имя домена) - рис. 2.2. (Если для адресации указывается только компонент адреса username (имя пользователя), система Notes будет считать, что пользователь располагается в том же домене, что и отправитель сообщения, и направит сообщение пользователю, автоматически расширив адрес и приведя его к виду username@domainname.)

Другие функции, ограничиваемые доменом, таковы: **Database Catalog** (Каталог базы данных), **Domain Search** (Поиск в домене), **Statistics Reporting** (Формирование статистических отчетов), **Event Dispatching** (Сообщение о событиях) и **Administration Process** (Процесс администрирования), каждая из них обеспечивает построение и поддержку одной или нескольких баз данных сервера Domino. Если с этими службами работает несколько

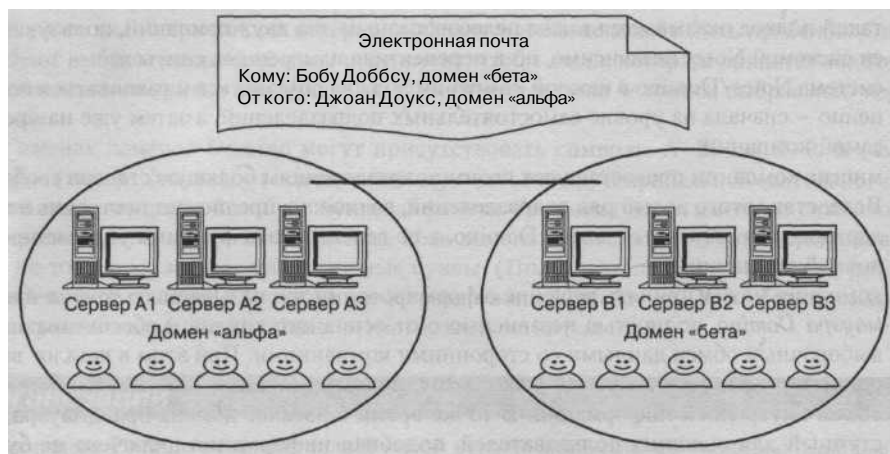


Рис. 2.2. Почтовые сообщения, адресованные пользователю в другой домен Domino, должны иметь полный адрес типа `username@domainname`

серверов домена, то в системе будут автоматически создаваться копии соответствующих баз данных, поскольку идентификационные данные реплик могут формироваться на основе соответствующих идентификационных данных, хранящихся в базе данных Domain Directory.

Домены Domino независимы по отношению к доменам сети Internet, доменам операционной системы Windows NT, доменам систем LAN Manager, LAN Server, Path Works, а также деревьям каталога операционной системы Novell NetWare. Система Notes/Domino строит собственные и независимые домены, предназначенные для облегчения управления серверами Domino.

Число создаваемых доменов Domino

На практике существует возможность иметь в рамках одной компании сколько угодно доменов Domino. Однако увеличение числа доменов обычно ведет к усложнению администрирования, поэтому надо стремиться к их минимизации. На данный момент известно несколько причин, по которым компании не следует ограничиваться лишь одним доменом Domino:

- О большим компаниям в свое время было просто необходимо создавать несколько подобных доменов (в условиях использования первых версий системы Notes/Domino), чтобы обеспечить должную поддержку книги общедоступных адресов (Public Address Book, теперь база данных Domain Directory) и сохранить небольшими ее размеры. Ранние версии системы Notes/Domino (в отличие от версий 5.0 и 6.0) не реализовали эффективную поддержку больших по размерам баз данных. Если компании планировали обслуживать в рамках системы Notes десятки или сотни тысяч пользователей, они неизбежно должны были прибегать к практике работы с многими доменами Domino. Даже в наши дни компании с самостоятельно управляемыми и практически не зависимыми в плане коммерческой деятельности подразделениями вынуждены формировать для каждого подобного подразделения собственный домен Domino;

- О такой подход оказывается также целесообразным для двух компаний, пользующихся системой Notes независимо, но в перспективе намеренных слиться;
- О система Notes/Domino в каждой компании должна создаваться и развиваться постепенно - сначала на уровне самостоятельных подразделений, а затем уже на уровне самой компании;
- О многие компании предоставляют своим подразделениям большую степень свободы. Вследствие этого целый ряд подразделений, возможно, предпочтет построить и поддерживать собственный домен Domino, а не делегировать функции управления головной компании;
- О компания может принять решение о формировании так называемого *домена-брендмауэра Domino*, полностью независимого от основного домена и обеспечивающего выборочный обмен данными со сторонними компаниями. При этом в каталог внутреннего домена, доступный только сотрудникам компании, помещается большой объем внутренней информации. В то же время в каталог домена-брендмауэра, доступный для внешних пользователей, подобная информация включена не будет. Следует отметить, что базы данных часто содержат много конфиденциальной информации, поэтому их целесообразно хранить на серверах внутреннего домена. Те базы данных, которые предоставляют общедоступную информацию, могут храниться на серверах внешнего домена (домена-брендмауэра);
- О компания также вправе создать независимый домен для общедоступных Web-серверов, чтобы имена Web-посетителей не смешивались с именами сотрудников компании, которые хранятся в каталоге внутреннего домена.

На практике известны случаи, когда компании руководствовались сразу несколькими вышеупомянутыми соображениями. Однако большая часть фирм использует тем не менее только один домен Domino или в крайнем случае внутренний домен и домен-брендмауэр (или домен Web-серверов). Поскольку увеличение числа доменов влечет за собой рост объема администрирования, рекомендуется в тех случаях, когда это возможно, ограничиваться одним внутренним доменом.

Рекомендации по выбору имен для доменов Domino

Имена доменов Domino должны в определенном смысле отражать названия тех сущностей, которые они представляют. Если уже существует зарегистрированное имя домена сети Internet, его можно употребить в качестве имени для домена Domino. Начиная с версии 5 программа настройки сервера (первого сервера в организации) использует именем домена сети Internet в режиме по умолчанию, но только в том случае, если ей удастся отыскать это имя в стеке IP сервера. Например, если зарегистрированное имя домена сети Internet представлено адресом planetnotes.com, система Notes будет применять planetnotes (в режиме по умолчанию) в качестве имени домена Domino. Некоторые специалисты считают, что в имя домена Domino должно входить название самой компании (по крайней мере, в общеизвестном виде), чтобы ее партнерам и клиентам было легче запомнить имя домена (например, оно необходимо для отправки почтового сообщения). Подсказка для поля **Domino Name** (Имя домена Domino) из базы данных Domino Setup (Установка сервера Domino) на этапе первоначального задания имени домена Domino рекомендует не вводить в него пробы, чтобы упростить администрирование. Однако многие специалисты (в том числе

и автор) не видят причин, по которым в имени домена не может быть пробелов. Они же советуют выбирать короткие и звучные имена, чтобы люди, которым придется многократно применять эти имена в будущем, не проклинали в душе человека, выбравшего неудачное имя.

В именах доменов Domino могут присутствовать символы A-Z, a-z, 0-9, & (амперсанд), - (тире), . (точка), _ (подчеркивание), ' (апостроф) и пробелы. Желательно, чтобы имя начиналось с какой-нибудь буквы алфавита. Рекомендуются имена из символов одного регистра (верхнего или нижнего). Имя домена будет проще читать, если оно включает не только заглавные или строчные буквы. (Пользователи могут, конечно, работать по своему усмотрению с верхним регистром, нижним регистром или обоими сразу, поскольку имена доменов Domino к регистру нечувствительны.)

Организации

Организация Domino не представляет собой чего-то монолитного (подобно доменам). На практике она скорее соответствует иерархической схеме присвоения имен, служащей для назначения имени каждому серверу Domino и пользователю системы Notes. Весьма важно, чтобы эта схема была хорошо продуманной, поскольку на ней базируются все методы защиты информации и обеспечения безопасности серверов Domino. (В частности, серверы Domino должны правильно распознавать обращающихся к ним пользователей и только потом предоставлять право доступа к данным.)

Схема присвоения имен первоначально была апробирована в рамках Международного стандарта каталогов X.500, он же протокол DAP (Directory Access Protocol - протокол доступа к каталогу), но сегодня дополнительно реализуется совместимость с протоколом LDAP (Lightweight Directory Access Protocol - протокол упрощенного доступа к каталогу), который является более простой версией стандарта X.500 и соответствует разрабатываемому стандарту сети Internet. Стандарт X.500 образует основу для эксплуатации службы Novell Directory Service (Служба каталогов сети Novell) и системы DNS (Internet Domain Name System - система доменных имен Internet). На протоколе LDAP базируется создание каталога Microsoft Active Directory (Активный каталог сети Microsoft) в операционной системе Windows 2000, сервера Netscape Directory Server (Сервер каталогов Netscape), а также множества общедоступных служб каталогов Internet. Если пользователи представляют себе, каким образом работает эта система присвоения имен, то они уже фактически могут считать себя ознакомленными с основными принципами организации Domino.

В соответствии со схемами присвоения имен, реализуемыми протоколами DAP и LDAP, все имена серверов и пользователей являются иерархическими. Они обычно состоят из двух или большего числа компонентов, позволяющих идентифицировать сервер или пользователя и подсказать окружающим, к какому организационному уровню иерархии относится данное имя. Имена, обладающие подобным форматом, иногда называют *хорошо различимыми*, поскольку они предназначены для четкого разделения и распознавания пользователей даже в случае совпадения их имен и фамилий. Имена серверов Domino имеют следующий вид (в приведенных ниже примерах употребляются только компоненты CN и O):

Server1/Acme или MCN=Server1/0=Acme

RobKirkland/Stillwater или CN=RobKirkland/0=Stillwater

В следующих именах присутствуют различные по виду компоненты OU:

Server2/OU=Servers/Stillwater или CN=Server2/OU=Servers/O=Stillwater
 BobDobbs/Acctg/MarshCreek/Stillwater или CN=BobDobbs/OU2=Acctg/
 OU1=MarshCreek/O=Stillwater

А здесь имеется только компонент C:

JoeDoaks/AR/Acctg/London/Acme/UK или CN=JoeDoaks/OU3=AR/OU2=Acctg/
 OU1=London/O=Acme/C=UK

Каждое имя в представленных выше примерах приводится дважды. В первом случае - в виде отдельных компонентов, разделенных косой чертой. Во втором случае оно содержит метки, идентифицирующие тип компонентов имени. Первый вариант соответствует так называемому *сокращенному формату*, а второй - полному, или *каноническому формату*.

Надо помнить, что в именах, включающих в себя компоненты OU, соответствующие номера отсчитываются слева направо.

Разделы имени сервера Domino или имени пользователя системы Notes могут иметь следующий вид:

- О **Общее имя** (CN) соответствует реально существующему имени пользователя, например Rob Kirkland (Роб Кирклэнд), или имени хоста сервера; каждое имя должно обязательно включать в себя раздел с общим именем; в неиерархических схемах формирования имен в данном разделе обычно приводят полное имя;
- О **Организационная единица** (OU или OUn, где n соответствует цифрам от 1 до 4) позволяет идентифицировать местоположение сервера или пользователя в организационной иерархии; система Notes/Domino допускает до четырех организационных уровней, однако работать на всех четырех уровнях совершенно необязательно, поэтому пользователю не следует задавать все компоненты OU, если в этом нет необходимости;
- О **Организация** (O) служит для идентификации организации, к которой принадлежит пользователь; на практике каждое имя должно содержать подобный раздел;
- О **Страна** (C) предназначен для идентификации страны принадлежности пользователя; не является обязательным; пользователь может не употреблять компонент C, если в этом нет необходимости.

Для лучшего понимания того, каким образом разделы имени отражают местоположение пользователя в иерархии организации, полезно обратиться к диаграмме на рис. 2.3.

Организация Domino описывается группой небольших двоичных файлов, называемых *файлами идентификационных данных*. Предусматривается также введение одного файла идентификационных данных *сертификатора* организации, имя которого обычно имеет вид /O=Асте (или просто /Acme)¹. По умолчанию имя этого файла cert.id. Можно поменять его на любое другое (например, на astecert.id), однако вне зависимости от выбранного имени файл должен иметь расширение .id, чтобы в дальнейшем он появился в списке файлов идентификационных данных.

Предусматривается также применение идентификационных данных сертификатора организационной единицы. Имя каждой организационной единицы состоит из собственного имени и имени родительской единицы (уровень O или более высокий уровень OU). Так, на

¹ Название Асте служит для обозначения любой компании и не должно совпадать с названием ни одной из реально существующих компаний. - Прим. ред.

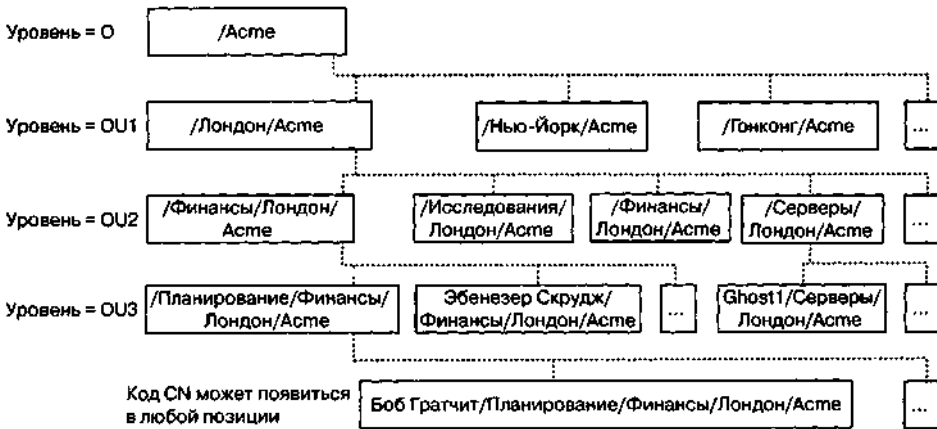


Рис. 2.3. Имена в системе Notes/Domino призваны указывать местоположение пользователя или сервера в организации

рис. 2.3 организационная единица Лондон является дочерней по отношению к /O=Асте, поэтому имеет имя /OU=Лондон/O=Асте. Именем файла по умолчанию будет london.id, хотя можно указать иное. Файлы идентификационных данных уровней O и OU должны храниться таким образом, чтобы к ним обеспечивался доступ только авторизованных (имеющих соответствующие права) пользователей.

Для каждого сервера и пользователя создается собственный файл идентификационных данных, причем эти данные обычно называют не идентификационными данными сертификата, а идентификационными данными сервера или пользователя. Имя каждого пользователя или сервера образуется из общего имени и полного имени файла с идентификационными данными для родительского сертификата. Имя файла пользователя по умолчанию задается в виде user.id, а имя файла сервера соответственно в виде server.id. В обоих случаях допустимо переименовать файлы и придать им большую смысловую нагрузку.

Как правило, не предусматривается построение специального файла идентификационных данных страны для уровня C (при условии работы с ним в данной компании). Уровень C формируется обычно в виде последнего раздела имени сертификата, сервера или пользователя. Организации редко вводят в имена компонент C.

Число используемых организаций Domino

На практике можно сделать множество организаций. Однако, как и в случае с доменами Domino, не рекомендуется создавать более одной организации. Серверы и пользователи в одной организации могут автоматически аутентифицировать друг друга, а серверы и пользователи из разных организаций в состоянии взаимно аутентифицироваться только после установки режима перекрестной сертификации между родительскими уровнями O или OU, что обычно выполняется администраторами вручную.

Иногда требуется выделить одно из подразделений компании в самостоятельную организацию, например в тех случаях, когда подобное подразделение проводит независимую коммерческую политику. Другой причиной наличия нескольких организаций в одной компании может стать слияние компаний. Так, компания Lotus в свое время была приобретена

компанией IBM, однако сотрудники компании Lotus продолжают принадлежать к организации с именем /Lotus, тогда как сотрудники компании IBM относятся к организации с именем /IBM.

Задание уровней OU

Ниже приводятся основные рекомендации для формирования организационных единиц (OU):

- организационная структура должна оставаться достаточно простой, поэтому небольшим компаниям (например, консалтинговым) необязательно прибегать к делению на OU. Более крупные компании должны применять несколько уровней OU. Однако даже весьма крупным фирмам нет смысла работать со всеми четырьмя уровнями OU, поскольку всегда полезно зарезервировать уровень OU4 для разрешения конфликтов, связанных с однотипными именами;
- следует присваивать уровни OU (если они используются) только тем подразделениям компании, которые носят устойчивый во времени характер. Таким образом удастся минимизировать усилия, затрачиваемые на переименование пользователей при расформировании соответствующего подразделения;
- серверы должны находиться в специально созданных организационных единицах, отделенных от OU пользователей. Это позволяет улучшить управление процедурами создания, администрирования и перекрестной сертификации. Даже те компании, которые не планируют вводить уровни OU для пользователей, должны рассмотреть варианты их применения для серверов;
- если политика компании создает трудности при достижении соглашения относительно необходимости уровней OU, имеет смысл отказаться от формирования организационных единиц: этим можно заняться на более поздних этапах выполнения проекта. Однако сервер после установки трудно переместить в другую организационную единицу, поэтому на ранних стадиях следует по крайней мере достичь соглашения относительно использования уровней OU для серверов;
- в компаниях с географически разнесенными офисами и представительствами уровень OU1 обычно служит для идентификации городов, в которых эти офисы и представительства расположены. Компаниям с единственным офисом (например, колледжам) OU1, как правило, нужен для идентификации отделов или департаментов. Однако подобная иерархия не является жесткой или обязательной. Так, например, компания может сначала на уровне OU1 задавать названия городов, а в дальнейшем перейти к идентификации с помощью этого компонента компаний-изготовителей.

Рекомендации по выбору имен для организационных единиц Domino

Ниже приводятся рекомендации в части выбора названий для организаций и организационных единиц (OU), а также имен серверов и пользователей:

- имена организаций, организационных единиц и серверов не должны содержать пробелов. Это позволяет облегчить процедуру администрирования серверов. Но в общие имена пользователей можно вводить столько же пробелов, сколько и в обычные имена;
- имена, присвоенные странам (посредством соответствующего компонента имени) должны состоять из двухсимвольных сокращений, установленных Международной организацией по стандартизации (International Standardization Organization - ISO);

- О в имени организации должно быть по крайней мере три символа, но не более 64, при этом следует сделать его как можно более лаконичным и легко идентифицируемым;
- О в режиме по умолчанию система Notes будет присваивать одни и те же имена домену и организации. На практике рекомендуется выбирать разные имена, чтобы упростить распознавание пользователей. Некоторые компании называют свои домены общепринятым для внешних партнеров образом (например, Winkin, Blinkin and Nod), но пользуются аббревиатурами для имен организации (например, WBN);
- О имена OU должны быть краткими (скажем, достаточно одного символа, но не более 32), что в первую очередь призвано экономить время тех, кому придется их вводить. Лучше предельно сокращать длину имен, но вместе с тем сохранять их информативность;
- О общие имена серверов должны носить индивидуальный характер (по крайней мере, в рамках организации). В общем случае рекомендуется давать уникальные имена серверам во всех организациях и доменах компании. Это уменьшит вероятность обращения пользователя к серверу ServerX/Acme в тех случаях, когда ему в действительности нужен сервер ServerX/Bard;
- О следует рассмотреть возможность употребления общих имен серверов, которые хорошо запоминаются пользователями, вместо совершенно бессмысленных кодовых комбинаций, часто присваиваемых отделом информационных технологий. В случае необходимости имя хоста или имя NetBIOS могут соответствовать требованиям отдела информационных технологий, но не стоит распространять эту практику на пользователей системы Notes;
- О общие имена пользователей обычно совпадают с их реальными именами. Необходимо сначала принять решение относительно работы с полными именами, содержащими промежуточные инициалы (например, Гай Р. Кирклэнд), или только с именами и фамилиями (например, Роб Кирклэнд), а затем неукоснительно придерживаться принятой схемы при регистрации пользователей. Если тот или иной пользователь не склонен применять свое полное имя и желает ограничиться только именем и фамилией, целесообразно это желание удовлетворить. Помните о том, что можно добавить в персональный документ (Personal document) псевдоним пользователя, так что он будет распознаваться не только по имени и фамилии;
- О если разрешены промежуточные инициалы пользователей в рамках их общих имен, следует подумать о введении в имена завершающих точек. Это позволит упорядочить записи и сделать их более привычными для восприятия;
- О если для целей идентификации планируется выбирать имена, отличные от реальных имен пользователей (например, имя входа в систему), то проблем не возникнет, ведь обязательным для заполнения является только поле **Last Name** (Фамилия);
- О максимальный размер полного имени пользователя или сервера составляет 128 символов. Однако для экономии времени тех, кто будет вводить эти имена, не рекомендуется задавать им столь длинными.

Взаимосвязь между доменами и организациями

С технической точки зрения между доменами и организациями Domino не существует никаких связей, поскольку они выполняют две различные функции и используются независимо друг от друга. Однако отношения между доменами и организациями станут более понятными, если вспомнить, что компания может иметь несколько доменов и организаций.

Наиболее простой вариант предполагает создание одного домена и одной организации с одинаковыми или разными именами. Применяемый в такой компании адрес почтового сообщения может иметь следующий вид: Joe Doaks/Acme@Acme. Эта ситуация наглядно проиллюстрирована на рис. 2.4 (Компания 1). Подобный подход рекомендуется для случаев установки первого сервера Domino в небольшой или средней фирме.

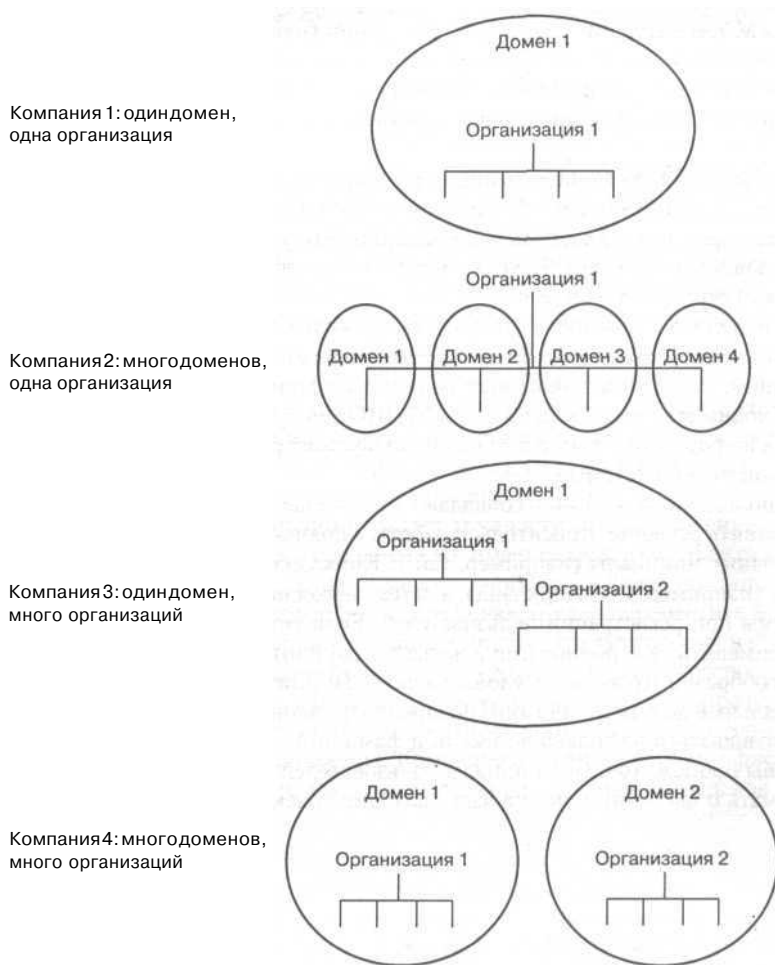


Рис. 2.4. Четыре возможных конфигурации доменов и организаций Domino

Крупные предприятия с большим числом независимых подразделений, развертывающие серверы Domino по всей компании, могут прийти к выводу о целесообразности построения одной организации, перекрывающей несколько независимых доменов. При этом все пользователи и серверы окажутся членами одной корпоративной организации, однако каждое подразделение будет формировать и поддерживать собственные каталоги доменов. Эта ситуация отражена на рис. 2.4 (Компания 2). Почтовые сообщения в данном случае могут

быть направлены двум пользователям по следующим адресам: Joe Doaks/AcmeConsulting/Acme® Acme Consulting и Bob Dobbs/AcmeWidgets/Acme® Acme Widgets.

Третий вариант, предусматривающий наличие одного домена и нескольких организаций, реализуется при условии тесного сотрудничества нескольких фирм. В этой ситуации компании, возможно, захотят оставаться в рамках одного домена для облегчения общего управления. В то же время им понадобится сохранить неизменной принадлежность пользователей к различным подразделениям, чтобы оставить существующую организационную структуру компании. Такой вариант представлен на рис. 2.4 (Компания 3). Почтовые сообщения, направляемые двум пользователям, в этом случае будут иметь следующие адреса: Joe Doaks/Acme Consulting@Acme Holdings и Bob Dobbs/AcmeWidgets@Acme Holdings.

Последний вариант (несколько доменов и несколько организаций) также может быть осуществлен на практике, например при желании нескольких подразделений независимо эксплуатировать серверы Domino или при слиянии двух или большего числа фирм. Допустима также ситуация, когда одновременно будут реализовываться второй и третий варианты (скажем, холдинговая компания планирует создание индивидуальных доменов для каждого независимого подразделения при общей схеме присвоения имен, либо подразделения компании настолько независимы, что сами принимают решения об использовании серверов Domino). Этот вариант изображен на рис. 2.4 (Компания 4). Почтовые сообщения в данном случае направляются двум пользователям по адресам: Joe Doaks/Acme©Acme и Bob Dobbs/Bard@Bard. Здесь, как нетрудно видеть, отсутствует какое-либо указание на то, что пользователи являются сотрудниками компаний, тесно связанных между собой коммерческими отношениями.

Именованные сети Domino

Третий организационный принцип серверов Domino относится к эксплуатации так называемых именованных сетей Domino, что позволяет администраторам различать серверы Domino с учетом топологий соответствующих сетей. Любой сервер Domino принадлежит к одной сети Domino согласно распознаваемым им сетевым портам. Допустимо задать сетевой порт для каждого сетевого протокола, поддерживаемого сервером. Если сервер снабжен несколькими платами (адаптерами) сетевого интерфейса, то можно произвольным образом выбирать порты для любой комбинации «плата сетевого интерфейса/протокол».

Однако подобные действия, скорее всего, не потребуются, поскольку каждый поддерживаемый протокол предполагает выделение ему определенного объема оперативной памяти и времени процессора. Рекомендуется минимизировать число протоколов для одного компьютера. Некоторые операционные системы (например, Windows) автоматически устанавливают несколько сетевых протоколов, а система Notes/Domino по умолчанию будет выделять порты для каждого протокола, указанного во время установки операционной системы. В этом случае следует отказаться от каких-либо вспомогательных протоколов в операционной системе для компьютера, используемого системой Notes/Domino, а также отменить введение в этой системе дополнительных сетевых портов.

Применение сетей Domino оказывается необходимым по двум причинам:

- О серверы Domino в рамках одной именованной сети Domino обеспечивают эффективную маршрутизацию почтовых сообщений и передают их друг другу автоматически без задержек (и без какого-либо вмешательства администраторов). Все другие серверы Domino должны маршрутизировать почтовые сообщения в соответствии с документами соединений (Connection document), присутствующих в базе данных Domain

Directory (Каталог домена). По этой причине целесообразно сосредоточить серверы в рамках небольшого числа именованных сетей;

- О в диалоговом окне **Open Database** (Открыть базу данных), а также в ряде других диалоговых окон при выборе варианта **Other** (Другие серверы) при просмотре списка серверов отобразятся только те серверы, которые относятся к порту и именованной сети Domino, соответствующей серверу самого пользователя. Из практики хорошо известно, что обычный пользователь просто теряется в тех случаях, когда сталкивается с длинными перечнями имен серверов. Для исключения подобных ситуаций список серверов формируется для каждой именованной сети и ограничивается только именами серверов, принадлежащих к этой сети.

Два сервера могут функционировать в рамках одной именованной сети Domino, если они отвечают следующим требованиям:

- О располагают для связи одним и тем же сетевым протоколом;
- О имеют постоянную связь друг с другом по локальной сети либо по региональной сети с мостами или маршрутизаторами.

Возможность эксплуатировать два сервера в рамках одной сети еще не означает, что делать это надо обязательно. С другой стороны, серверы способны при необходимости работать в рамках именованной сети даже в том случае, когда вышеупомянутые требования не выполняются.

Сети Domino должны корректным образом создаваться в рамках домена, так как:

- О правильное задание принадлежности серверов к именованным сетям позволит избежать возникновения проблем у пользователей и исключить необходимость разбираться в длинном перечне незнакомых имен серверов, что может испортить пользователям настроение и заставить их отказаться от обращения к базам данных серверов, с которыми они соединены, особенно в условиях медленных и перегруженных линий связи;
- О при включении двух серверов в одну именованную сеть Domino (даже при нарушении вышеупомянутых требований) удастся организовать обмен почтовыми сообщениями между ними и (иногда) между другими серверами.

Последняя причина представляется весьма важной, поскольку два сервера в одной сети Domino изначально предполагают соединение по локальной или региональной сети. Если в действительности серверы соединены лишь телефонной линией, то сначала они попытаются связаться по сети и только после многих безуспешных попыток постараются установить сеанс с помощью телефонного подключения. В этих условиях передача сообщений между серверами существенно замедляется, но сообщения все же передаются.

Если серверы «полагают», что наиболее быстрая связь между ними обеспечивается по локальной сети, процедура передачи почтовых сообщений между ними становится неэффективной. Но все же некоторые сообщения будут приходить по телефонной линии, поэтому проблемы со связью обнаружатся лишь после того, как от пользователей поступит множество жалоб на медленную пересылку писем.

Такие ошибки весьма вероятны, поскольку в рамках версии 4.6 и более поздних процедура установки сервера Domino по умолчанию предполагает введение имени сети для каждого порта. Если настройка серверов выполняется для локальных сетей, связанных друг с другом только с помощью телефонной линии, а задание имен производится в режиме по умолчанию, избежать проблем будет весьма непросто.

Имена для сетей Domino могут выбираться произвольным образом, однако специалисты компании Lotus рекомендуют задавать их так, чтобы они удовлетворяли двум условиям. В частности, если группа серверов взаимодействует через порт TCP/IP и эти серверы относятся к одной и той же локальной сети (например, используемой в главном офисе компании), лучше поместить их в одну сеть Domino с именем TCP/IP_HQ.

В режиме по умолчанию процедура установки сервера будет сама обеспечивать соответствие между сетями и портами и присваивать сетям имена типа Portname Network (компонент имени portname отвечает имени сетевого порта, с которым соединена соответствующая сеть). Лучше изменять эти имена сетей, например согласно описанной выше схеме выбора имен, что позволит избежать проблем с нахождением двух удаленных серверов в одной именованной сети Domino.

Далее приводится ряд советов по установке именованных сетей Domino:

- необходимо сосредоточить серверы в пределах как можно меньшего числа сетей Domino с учетом указанных ниже ограничений;
- следует ограничивать число серверов в каждой сети Domino, скажем на уровне семи или даже менее;
- не стоит работать с серверами, связанными с помощью медленных соединений региональной сети, в рамках одной и той же именованной сети Domino;
- не рекомендуется устанавливать два сервера, соединенных между собой только посредством телефонной линии или линии связи удаленной локальной сети, в рамках одной и той же сети Domino;
- не следует сохранять имена сетей Domino, присвоенные им по умолчанию. Лучше изменить эти имена так, чтобы они позволяли идентифицировать сетевой порт и местоположение каждой сети.

Проблемы обеспечения безопасности

Система Notes/Domino достаточно хорошо защищена (даже при выборе параметров защиты в режиме по умолчанию), а сама защита носит многоуровневый характер. Поэтому, когда нужна надежная система для хранения данных, система Notes/Domino вполне подходит. Если же проблем с обеспечением безопасности не возникает, соответствующие функции серверов Domino могут оказаться невостребованными.

Первым вопросом, который требует решения при планировании процедуры установки сервера Domino, является вопрос о мерах обеспечения безопасности. Если не предполагается с помощью серверов Domino хранить конфиденциальную информацию, то, скорее всего, проблем с обеспечением безопасности в дальнейшем не появится. Однако в том случае, когда присутствующая на серверах информация носит сугубо конфиденциальный или даже секретный характер (речь может идти, кстати, и о долгосрочной перспективе), следует уделить должное внимание характеристикам и функциям сервера Domino, связанным с гарантией безопасности, еще на этапе установки первого подобного сервера в организации. Если в этот момент (или на последующих этапах выполнения проекта) не позаботиться о должном уровне защиты, то в дальнейшем, когда обеспечение безопасности станет насущной проблемой, будет сложно вернуться к этому вопросу и реализовать эффективную защиту больших массивов данных.

Серверы Domino реализуют принцип проверки (аутентификации) пользователей на основе специальных сертификатов и предоставляют доступ к данным только аутентифицированным пользователям. Необходимо помнить о том, что сервер позволяет лишь

идентифицировать пользователя и проверить факт наличия у него разрешения на доступ к данным.

Сервер Domino распознает три типа пользователей: пользователей, аутентифицируемых по сертификатам; пользователей, аутентифицируемых в процессе запросов и ответов; и анонимных пользователей. Самой надежной является идентификация пользователей, распознаваемых с помощью сертификатов, поскольку они имеют в своем распоряжении и представляют серверу сертификат, подписанный доверенной третьей стороной, причем такой сертификат обычно содержит открытый ключ, связанный с именем пользователя. В отсутствие подобного подписанного сертификата пользователю будет трудно «убедить» сервер в своей принадлежности к системе, так что сервер, скорее всего, не вступит в контакт с ним.

Доверенную третью сторону, которая подписывает сертификат, в системе Notes иногда называют *сертификатором*, а в системе SSL соответственно *авторизатором сертификации* (Certificate Authority - CA). Сертификатор, или CA, может подписывать сертификат¹ посредством пары ключей (открытого и закрытого, которые иногда называются общим и личным). Как того требуют методы обеспечения безопасности системы Domino, эти ключи (коды) хранятся в зашифрованных с помощью пароля файлах, называемых *файлами идентификационных данных сертификатора*. Этот файл является ключевым для всей системы обеспечения безопасности серверов Domino. Владелец такого файла (и соответствующего пароля для дешифрации) имеет возможность использовать любые функции, связанные с обеспечением безопасности, за исключением одной, относящейся к шифрованию полей. Вот почему так важно, чтобы данный файл не попал в чужие руки.

Идентификационные данные сертификатора организации (наивысший уровень сертификации в системе Notes) создаются автоматически в процессе установки первого сервера. (Пользователь также вправе заблаговременно и самостоятельно вводить такие данные вручную.) Этот двоичный файл cert.id обычно имеет размер порядка 2200 байт. На первый взгляд данный файл, хранящийся в каталоге данных сервера, ничем не примечателен и не привлекает внимания. Можно легко скопировать его на дискету (при наличии надлежащего права доступа) или в домашний каталог, а затем переименовать. (На практике не так просто подобрать пароль, если человек никогда не знал пароля для дешифрации этого файла.)

Если проблемы обеспечения безопасности данных на сервере Domino представляют интерес (или могут оказаться интересными в будущем), весьма важно предпринять необходимые шаги уже при создании файла cert.id, в частности исключить возможность его несанкционированного использования. Работая с этим файлом, при создании идентификационных данных сертификаторов более низких организационных единиц следует принимать аналогичные меры для его надежной защиты.

¹ Речь идет о цифровой подписи, поскольку все сертификаты существуют только в электронном виде. - *Прим. ред.*

ГЛАВА

3



ПРОЦЕДУРА УСТАНОВКИ И НАСТРОЙКА ПЕРВОГО СЕРВЕРА

Установка первого сервера Domino в компании может сопровождаться различными проблемами. К счастью, большинство администраторов не сталкиваются с ними, поскольку получают в свое распоряжение практически полностью сконфигурированный сервер. Как правило, специалистам доводится устанавливать сервер один раз в жизни, и лишь малому числу профессионалов (обычно инструкторам и консультантам) приходится повторять эту процедуру снова и снова. Конечно, квалифицированные специалисты хорошо знакомы с существующими проблемами и стараются избежать их появления. Однако те из них, кто выполняет установку достаточно редко, иногда попадают в ловушку. Именно в помощь таким специалистам и была написана данная глава.

Установка первого сервера в организации - это процедура, состоящая из трех этапов. На первом этапе следует принять ряд организационных решений, на втором - установить программное обеспечение сервера на соответствующем компьютере и, наконец, на третьем - задать конфигурацию самого сервера.

Принимаемые на первом этапе решения в основном связаны с формированием схемы присвоения имен, а также установкой политики безопасности. В процессе конфигурирования сервера вводятся различные имена, а также принимаются первые решения относительно мер защиты (в том числе и в долгосрочном плане) информации в базах данных системы Notes. Если схема присвоения имен уже разработана, а решения относительно мер безопасности приняты, можно пропустить первый этап и сразу переходить ко второму. Разрешается также временно отложить эти вопросы и вернуться к ним уже на этапе задания конфигурации сервера. Однако подобный подход представляется крайне нежелательным, поскольку часть имен задается системой в режиме по умолчанию, а пользователям потом еще долго придется жить и работать с неудобными именами. Поэтому лучше не спеша решить все вопросы на первом этапе с учетом тех рекомендаций, которые обсуждались в главе 2. Если читатели с ней своевременно не ознакомились, то сейчас самое время восполнить пробел.

Установка программного обеспечения сервера Domino

Второй этап, связанный с установкой программного обеспечения сервера Domino, оказывается наиболее простым. Для его выполнения требуется предварительно закрыть все

программы, в том числе экранные заставки и антивирусные программы, и только после этого начинать поэтапную процедуру установки.

Установка сервера Domino в операционной системе Windows производится с помощью стандартного Мастера установки InstallShield Wizard. Мастер InstallShield Wizard может быть запущен непосредственно с установочного компакт-диска системы Domino или с сетевого файлового сервера, куда предварительно скопировано содержимое компакт-диска. Установка начинается вручную двойным щелчком по файлу setup.exe в Проводнике Windows или в режиме автозапуска (AutoPlay) компакт-диска либо файлового сервера. Рассмотрим имеющиеся варианты:

- О *запуск в режиме **AutoPlay** непосредственно с компакт-диска CD-ROM*. Если устройство чтения компакт-дисков не обеспечивает автоматического запуска программ, установите этот режим вручную. Щелкните правой кнопкой мыши по значку компакт-диска в Проводнике Windows и укажите режим автозапуска в контекстном меню. Если для монитора задан режим воспроизведения 16 цветов, появится сообщение об ошибке. Не обращайте на него внимания и выполните автозапуск обычным образом;
- О *запуск в режиме **AutoPlay** с файлового сервера*. Если вся информация диска CD-ROM системы Domino переписана на сетевой файловый сервер, причем в точности сохранена структура каталогов, автозапуск установки сервера можно инициировать непосредственно с файлового сервера, запустив файл setup.bat. Этот файл должен присутствовать в самом верхнем каталоге, в который скопировано содержимое компакт-диска;
- О *запуск Мастера InstallShield Wizard в режиме **AutoPlay***. Последовательно укажите **Install** (Установка), **Servers** (Серверы), а также вариант устанавливаемого сервера. Выберите **Custom Install** (Пользовательская установка) или **Standard Install** (Стандартная установка). В первом случае после запуска Мастера появится экран, где можно задавать для установки определенные наборы файлов. В режиме стандартной установки **Standard Install** Мастер не выводит этот экран;
- О *запуск Мастера InstallShield Wizard вручную*. Именем файла Мастера будет setup.exe. На диске CD-ROM системы Domino данный файл находится в папке \Servers\W32Intel или \Servers\W32Alpha. На файловом сервере папки имеют аналогичные имена.

Мастер InstallShield Wizard последовательно предлагает задать всю необходимую информацию для установки сервера Domino. Вводимая информация зависит от режима установки (вручную или в режиме автозапуска с компакт-диска). Если используется режим **AutoPlay**, имеется возможность определенного выбора, причем Мастер не будет запрашивать в будущем сведения, которые были введены во время автозапуска.

Ниже приводится перечень тех решений, которые требуется принять в процессе установки независимо от того, что применяется - режим автозапуска, Мастер InstallShield Wizard или программа установки для других платформ Notes/Domino (эти решения ориентированы на ОС Windows, однако основные положения остаются такими же и для других операционных систем):

- О *устанавливаемый сервер*. Надо выбрать один из следующих серверов - Domino Mail Server, Domino Application Server и Domino Enterprise Server;
- О *стандартная или пользовательская установка*. При задании **Custom Installation** (Пользовательская установка) появится дополнительный экран для указания необходимых классов и файлов. В операционной системе Windows NT режим **Custom**

Installation позволяет установить сервер Domino в виде службы NT. В режиме **Standard Installation** (Стандартная установка) этого сделать нельзя, а в дальнейшем потребуется повторный запуск Мастера InstallShield Wizard (установка сервера Domino в качестве службы NT позволяет автоматически запускать сервер Domino во время загрузки компьютера, а также обеспечивает независимое отслеживание всех сеансов связи пользователей; на других платформах для достижения аналогичных целей придется подготавливать пакетные файлы или специальные сценарии - более подробно об этом говорится в конце данной главы);

- О *установка сегментированного сервера*. Если имеется намерение установить на компьютере несколько сегментированных серверов, надо указать вариант **Partitioned Server Installation** (Установка сегментированного сервера). Если же пользователь не уверен в необходимости подобного подхода, этот вариант выбирать не следует;
- О *местоположение файлов (несегментированные серверы)*. Пользователю надо задать местоположение файлов программ и файлов данных сервера Domino. Если на соответствующем компьютере ранее не устанавливался сервер Domino и этот компьютер имеет операционную систему Windows или OS/2, то файлы программ по умолчанию размещаются в каталоге c:\lotus\domino, а файлы данных - в каталоге c:\lotus\domino\data. (Если же на компьютере сервер Domino уже устанавливался, программа инсталляции может предложить для режима по умолчанию ранее созданные файлы.) Когда сервер имеет несколько жестких дисков, файлы программ следует заносить на один накопитель, а файлы данных - на другой. Например, в системе с двумя дисковыми файлами программ лучше поместить в c:\lotus\domino, а файлы данных в d:\data (см. главу 2);
- О *местоположение файлов (сегментированные серверы)*. При выборе варианта **Partitioned Server Installation** приходится задавать местоположение для файлов программ на первом шаге, а для файлов данных каждого сегментированного сервера - на последующих шагах. В остальном процедура подобна применяемой для несегментированных серверов. Как и в случае несегментированных серверов, при наличии нескольких накопителей жестких дисков рекомендуется записывать файлы программ на один жесткий диск, а файлы данных - на другие. И наконец, следует задавать имя для каждой папки данных сервера таким образом, чтобы в дальнейшем не возникало проблем с выяснением принадлежности папки конкретному серверу. Так, имена папок данных могут выбираться согласно общим именам серверов (скажем, в виде d:\osprey);
- О *местоположение ярлыков и значков*. В операционной системе Windows Мастер InstallShield Wizard создает ярлык для запуска каждого сервера. В операционной системе OS/2 программа установки формирует значок (или значки) в группе программ. В режиме по умолчанию ярлыки Windows появляются в меню в разделе **Programs/Lotus Applications** (Программы/приложения системы Lotus Notes). Значки операционной системы OS/2 размещаются в группе программ Lotus Applications (Приложения системы Lotus Notes), при этом имеется возможность использовать для них другую группу программ.

Мастер InstallShield Wizard обеспечивает установку большей части файлов программ в предварительно указанную папку вместе с исполняемыми модулями некоторых Web-серверов в подпапке configuration и файлов данных в подпапке data, а также нескольких специальных файлов в подпапках нижнего уровня. Среди этих подпапок имеются: help для справки по базам данных, sample для базы данных примера Web-сайта, modems для файлов с командами модемов и W32 для файлов, связанных с Lotus SmartIcons (Интеллектуальные

значки системы Lotus). В папку domino попадут файлы данных службы HTTP сервера Domino. И наконец, для сегментированных серверов каждый раздел будет содержать полный набор папок и файлов.

Другие платформы обладают похожей иерархической структурой папок, однако в ряде случаев имена папок будут другими. Так, в операционной системе OS/2 файлы SmartIcons хранятся в папке OS2 (вместо папки W32 ОС Windows).

Когда устанавливаются несегментированные серверы, в папке программ program находится текстовый файл notes.ini. При установке одного или нескольких сегментированных серверов экземпляры этого файла (с нужными параметрами каждого сервера) будут присутствовать в папке данных каждого сегментированного сервера. Файл notes.ini отвечает файлу конфигурации и включает в себя список переменных и их значений. Во время запуска сервера Domino (или системы Notes) производится поиск указанного файла, после чего конфигурация сервера в памяти устанавливается согласно значениям соответствующих переменных. Если не удастся найти файл notes.ini, сервер Domino (или систему Notes) запустить нельзя.

Master InstallShield Wizard также создает ярлык для запуска сервера Domino. Этот ярлык появляется в меню операционной системы Windows под именем, которое оговаривается в процессе установки (в режиме по умолчанию определяется разделом Lotus Applications). Для несегментированных серверов на платформе Windows/Intel командная строка для ярлыка будет иметь следующий вид:

```
[путь]\nserver.exe
```

Для любого сегментированного сервера на платформе Windows/Intel командная строка для ярлыка выглядит так:

```
[путь]\nserver.exe = [путь]\notes.ini
```

В каждом из приведенных выше примеров параметр [путь] указывает местоположение соответствующего файла на диске. Если в данных примерах задать местоположение для файлов программ как c:\lotus\domino, а для файлов данных как c:\osprey, то вид командных строк получится иным: для несегментированного сервера c:\lotus\domino\nserver.exe, для сегментированного сервера c:\lotus\domino\nserver.exe =d:\osprey\noted.ini.

Второй параметр в командной строке для сегментированного сервера начинается со знака равенства. Между знаком равенства и следующим за ним именем пути не предусматривается пробела. Второй параметр помогает легко отыскать файл notes.ini и быстро начать его исполнение. Если попытаться запустить сервер Domino каким-либо иным способом (например, щелкнув по файлу notes.ini или nserver.exe в Проводнике Windows), сервер может не обнаружить этого файла, что будет препятствовать запуску.

Следует отметить также, что в приведенных выше командных строках указано имя исполняемого файла nserver.exe, который также служит для запуска сервера Domino. Данный файл на платформе Windows/Alpha имеет имя aserver.exe, на платформе OS/2 - iserver.exe, а в UNIX - server.

Для всех платформ сервер Domino может быть представлен в виде набора одновременно исполняемых файлов программ. Запуск базы данных сервера (файл nserver.exe) обеспечивается из командной строки. Затем база данных сервера считывает значение переменной servertasks в файле notes.ini и запускает указанные в этой переменной программы. Каждая из них связана с определенной службой сервера Domino.

На платформе Windows/Intel каждому исполняемому файлу программы присвоено имя в виде n*.exe, где * отвечает имени службы в списке серверных задач servertasks. Например, если переменная servertasks содержит значения router, replica, update, amgr, adminp и stats, файл nserver.exe будет производить загрузку программ (файлов) с именами nrouter.exe, nreplica.exe, nupdate.exe, namgr.exe, nadminp.exe, nstats.exe. На платформе Windows/Alpha соответствующие имена файлов начинаются с буквы «a», на платформе OS/2 – с буквы «i», а в UNIX не имеют префикса имени.

Конфигурирование первого сервера Domino

Третий этап настройки первого сервера связан с его конфигурированием. Эта процедура сама состоит из двух этапов. На первом этапе запускается сервер Domino (но не система Notes) на серверном компьютере, заполняется соответствующая форма, затем нужно немного подождать, чтобы система Notes в операционной системе Windows (или сервер Domino в других операционных системах) создала новый каталог Domino Directory, сформировала некоторые идентификационные данные и выполнила несколько вспомогательных операций. На втором этапе предстоит проанализировать все произведенные операции и исправить те недочеты, которые система Notes не заметила в автоматическом режиме.

Но не стоит слишком торопиться, поскольку в ряде случаев приходится вводить еще один подготовительный этап и только потом переходить к конфигурированию сервера. Готовность к выполнению процедуры конфигурирования зависит от того, была ли в процессе планирования создана схема присвоения имен (этому вопросу посвящена глава 2). Если организационные единицы (Organizational Unit) в схеме присвоения имен не нужны, можно смело продолжать процедуру конфигурирования. Если же такие единицы будут применяться в рамках схемы, необходимо внимательно ознакомиться со следующим разделом, содержащим рекомендации по заданию единиц OU для первого сервера.

Задание организационных единиц для первого сервера

При заполнении формы на первом этапе процедуры конфигурирования сервера приходится вводить (наряду с другими сведениями) имена нового домена и организации, имя конфигурируемого сервера и имя одного пользователя. Затем система Notes создает эти объекты и присваивает им соответствующие имена. В режиме по умолчанию имена сервера и пользователя будут задаваться в виде servername/orgname и username/orgname, где servername, username и orgname соответствуют именам сервера, пользователя и организации.

Формирование организации Domino без организационных единиц OU (см. главу 2) можно признать хорошим решением, поскольку с этими задачами нецелесообразно связываться при настройке самого первого сервера. Однако, если планируется сделать серверы и пользователей членами определенной организационной единицы, понадобится принимать достаточно сложные решения. Напомним, что сервер и пользователь еще не принадлежат ни к какой организационной единице, поэтому необходимо для начала определить такую принадлежность.

Пусть, например, имя организации – Stillwater, а серверы относятся к организационной единице Servers. Пользователи также войдут в эту организационную единицу, а их имена

должны указывать на местоположение офиса, в котором они работают. В данном случае вид имен серверов будет следующим: имя_сервера/Servers/Stillwater, причем Osprey/Servers/Stillwater – имя первого сервера (Osprey). Имена пользователей выглядят так: имя_пользователя/имя_OU/Stillwater. Если первым пользователем является Роб Кирклэнд, работающий в офисе города Марш Крик, то его полное имя имеет вид Rob Kirkland/MarshCreek/Stillwater. (Здесь надо снова напомнить, что решение о создании организационных единиц должно быть хорошо взвешенным, а в случае принятия такого решения рекомендуется тщательно формировать имена, поскольку на более поздних этапах достаточно сложно вносить какие-то изменения – см. главу 2.)

Процедура настройки первого сервера не обеспечивает автоматического включения сервера и пользователя в организационную единицу. Так, в режиме по умолчанию проводится только включение в организацию (O). В рассмотренном выше примере это определяется именами Osprey/Stillwater и Rob Kirkland/Stillwater.

Таким образом, необходимо выполнить присваивание вручную. Существуют три способа выполнения указанной операции:

- О перед запуском установки первого сервера можно создать файлы идентификационных данных для организации, одной или нескольких организационных единиц, для первого сервера и (необязательно) для первого пользователя. Затем, уже во время установки, можно работать с этими файлами при заполнении формы и задании конфигурации первого сервера. В результате для первого сервера и (необязательно) для первого пользователя будут правильно указаны имена;
- О после завершения установки первого сервера допустимо сформировать идентификационные данные для OU, а в дальнейшем с их помощью переименовать первый сервер и пользователя;
- О существует также возможность создания так называемых промежуточных первого сервера и первого пользователя с последующей регистрацией и установкой организационной единицы. Далее формируются реальный сервер и пользователь в уже готовой организационной единице, а промежуточные сервер и пользователь с некорректными именами удаляются.

К сожалению, ни один из способов не является идеальным. Все они требуют выполнения большого числа промежуточных операций. Однако, если необходимо ввести в схему присвоения имен организационные единицы (Organizational Unit), придется прибегнуть к одному из этих способов для решения поставленной задачи. В версиях 5 и 6 рекомендуется третий способ, однако ниже подробно рассмотрены все три способа, так чтобы при желании можно было воспользоваться тем из них, который представляется менее трудоемким.

Первый способ: предварительное создание идентификационных данных

Таким способом можно заблаговременно зарегистрировать организацию, организационную единицу и первый сервер (еще до его установки). Это потребует создания ряда файлов идентификационных данных. В дальнейшем во время установки первого сервера необходимо проинформировать систему Notes о том, что планируется использовать файлы идентификационных данных организации и первого сервера. Когда система Notes предложит ввести указанные файлы, надо это сделать. После завершения установки первого сервера

придется также выполнить две вспомогательные операции. Во-первых, вручную воссоздать документы сертификата (Certificate document) для идентификационных данных сертификатора организационной единицы. Во-вторых, вручную повторно ввести открытый ключ сервера в документ сервера (Server document).

Необходимо также предварительно зарегистрировать первого пользователя, хотя заниматься этим в данный момент нет никакого желания. Цель состоит в том, чтобы устранить переименование сервера, тогда как операция по переименованию пользователя не представляет никакой проблемы, поэтому о ней нет смысла заботиться при регистрации первого пользователя. Учтите: чем большее количество OU задается предварительно, тем многочисленнее будут исправления после установки первого сервера. Другими словами, целесообразно минимизировать работу за счет заблаговременной регистрации первого сервера и его организационной единицы OU, но не первого пользователя.

Для практического осуществления этого способа еще до начала установки первого сервера необходимо иметь доступ к рабочей станции системы Notes и к серверу Domino. (В рамках более ранних версий допускалось реализовывать данный способ без доступа к серверу, однако начиная с версии 5 так делать нельзя.) Если работы выполняет консультант, которого клиент нанял для установки первого сервера, все подготовительные операции можно произвести в офисе, а новые идентификационные данные просто «прихватить» с собой в офис клиента в тот день, когда планируется установка. Предпочтительнее, однако, провести предварительные работы с помощью переносного компьютера в офисе клиента в день установки (это возможно только в том случае, если переносной компьютер имеет сервер Domino или к подобному серверу есть непосредственный доступ по локальной сети или через модем). Создавать идентификационные данные лучше на дискете, что позволит гарантировать клиенту отсутствие несанкционированного копирования и использования идентификационных данных.

Если пользователь не очень хорошо знаком с системой Notes и не в состоянии нанять консультанта для установки первого сервера, но все-таки вынужден решать эту задачу, первый способ представляется не самым подходящим. Он требует предварительной настройки сервера Domino, клиента системы Notes и работы с программой Domino Administrator задолго до выполнения основных операций по установке и с единственной целью формирования идентификационных данных. Если пользователь желает проделать все это для тренировки, для приобретения опыта или из простого любопытства, можно смело рекомендовать ему данный способ. Но прибегать к нему просто для того, чтобы подготовить идентификационные данные, значит не жалеть своего времени и усилий.

К тому же пользователь вряд ли захочет создавать идентификационные данные сразу для всех OU, которые могут понадобиться в дальнейшем в рамках схемы присвоения имен. Скорее всего, нужно создать только те данные, которые позволят без проблем сформировать идентификационные данные первого сервера. В рассмотренном примере, когда именем сервера было Osprey/Servers/Stillwater, пришлось вводить только три элемента идентификационных данных: идентификационные данные сертификатора организации /Stillwater, идентификационные данные сертификатора организационной единицы первого уровня OU1 с именем /Servers/Stillwater и идентификационные данные сервера Osprey/Servers/Stillwater. Если для первого сервера решено применить организационные единицы OU2 и OU3, необходимо иметь дополнительные идентификационные данные сертификатора для этих компонентов.

Сформируйте идентификационные данные с помощью такой процедуры:

1. Определите качество пароля для своих идентификационных данных. Программа Domino Administrator в режиме по умолчанию будет задавать следующие коды качества пароля (по шкале от 0 до 16): не ниже 10 для идентификационных данных сертификатора, не ниже 8 для идентификационных данных пользователя и 0 для идентификационных данных сервера (в ряде публикаций специалисты компании Lotus рекомендуют пользоваться кодами качества пароля не ниже 14). Для примера: выбор кода равным 10 означает, что пароль для идентификационных данных должен быть длиной не менее 10 букв одного регистра, 9 букв разных регистров или 9 символов. Если работы проводятся консультантом, необходимо убедиться в том, что клиент правильно понимает значение качества (стойкости) пароля и согласен с теми паролями, с которыми придется работать. Получить более подробную информацию о паролях для идентификационных данных можно, ознакомившись с материалами главы 20.
2. Зарегистрируйте идентификационные данные сертификатора для организации (О).
3. С помощью идентификационных данных сертификатора уровня О зарегистрируйте идентификационные данные сертификатора организационной единицы первого уровня (OU1) для первого сервера.
4. Примените идентификационные данные сертификатора OU1 для регистрации идентификационных данных сертификаторов следующих уровней (например, для второго уровня организационной структуры - OU2, если такие данные есть) или (в отсутствие этих данных) для регистрации первого сервера.
5. Если проведена регистрация на уровне OU2, воспользуйтесь полученными данными и зарегистрируйте последующие идентификационные данные (OU3, при наличии этих данных) или первый сервер.
6. Продолжайте выполнять аналогичные действия.

Процедура регистрации сертификатора организации в системе Notes осуществляется следующим образом:

1. Запустите программу Domino Administrator.
2. Перейдите на вкладку **Configuration** (Конфигурация) - рис. 3.1.
3. Раскройте поле **Registration** (Регистрация), после чего щелкните по пункту **Organization** (Организация), чтобы открыть диалоговое окно **Register Organization Certifier** (Регистрация сертификатора организации) - рис. 3.2.
4. Введите в поле **Registration Server** (Регистрирующий сервер) имя сервера, к которому имеется доступ.
5. Нажмите кнопку **Set ID File** (Формирование файла идентификационных данных) и укажите путь к файлу идентификационных данных, который должен быть создан. Затем сохраните этот файл на дискете, так чтобы его путь имел вид а: \имя_файла.id, где компонент имя_файла соответствует имени организации или имени типа «о-хуз» (символ «о» указывает на сертификатора организации XYZ, а «хуз» определяет имя организации).
6. Задайте имя организации в поле **Organization** (Организация). В нашем примере именем будет Stillwater. Если решено использовать код страны, следует вводить двухсимвольный код ISO (Международная организация по стандартизации) в поле **Country code** (Код страны).

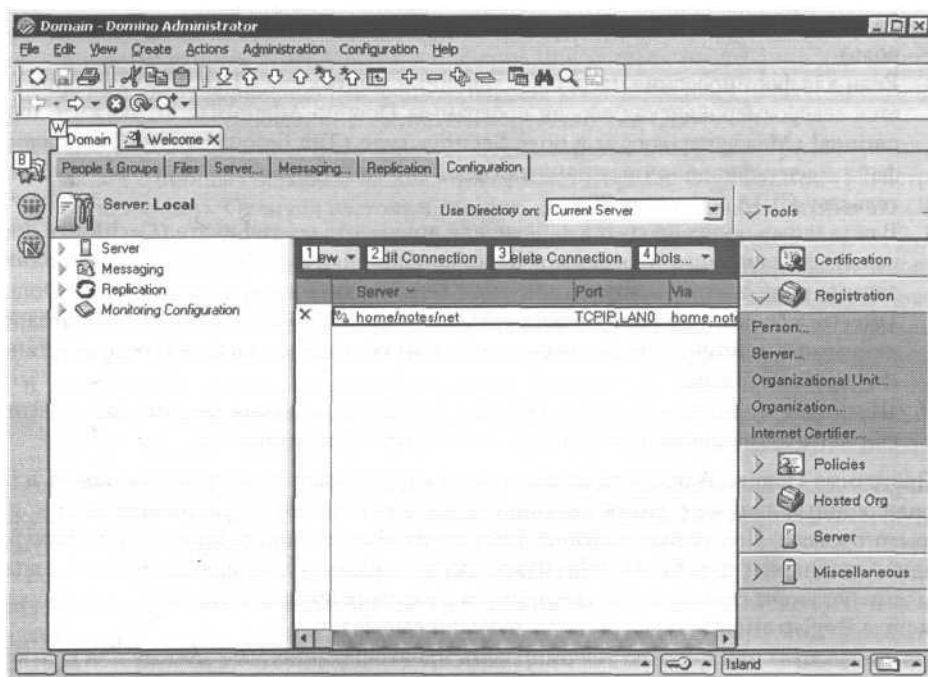


Рис. 3.7. Программные инструменты для регистрации находятся на панели **Tools** страницы **Configuration** программы **Domino Administrator**

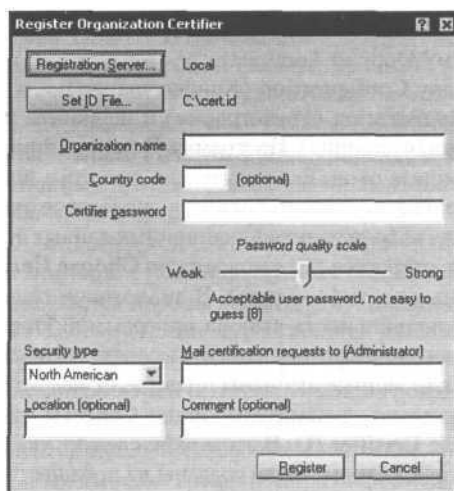


Рис. 3.2. Введите имя сертификатора и его пароль. Заполнять другие поля необязательно

7. Задайте стойкость пароля по шкале качества и введите пароль в поле **Password** (Пароль).
8. Если для формирования идентификационных данных вне США и Канады применяется североамериканская версия программы Domino Administrator, укажите **International** (Международный) в поле **Security type** (Тип безопасности). Полученный файл идентификационных данных будет соответствовать экспортному законодательству США (см. главу 20).
9. В остальных полях вводятся данные для документа сертификата (Certificate document), создаваемого программой Domino Administrator. Можете либо заполнить данные поля, а затем вставить документ сертификата в новую базу данных Domain Directory (когда уже установлен первый сервер), либо оставить эти поля незаполненными и повторно сформировать документ сертификата вручную после установки первого сервера.
10. Щелкните по кнопке **Register** (Регистрация) - программа Domino Administrator создаст новые идентификационные данные сертификатора.

Программа Domino Administrator формирует пару открытого/закрытого ключей, идентификационные данные с этими ключами и документ сертификата, содержащий копию открытого ключа. Программа сохранит файл идентификационных данных сертификатора в папке, указанной в поле **Set ID File** (Формирование файла идентификационных данных). При этом документ сертификата генерируется в каталоге компьютера, имя которого указано в поле **Registration Server** (Регистрирующий сервер).

На следующем этапе нужно сформировать идентификационные данные для сертификатора одной или нескольких организационных единиц. Лучше создавать их не все сразу, а только те, которые необходимы для построения идентификационных данных первого сервера. Так, в примере с первым сервером Osprey/Servers/Stillwater требуются лишь идентификационные данные сертификатора организационной единицы /Servers/Stillwater. Чтобы создать идентификационные данные сертификатора организационной единицы уровня OUI, выполните следующие действия:

1. Запустите программу Domino Administrator.
2. Перейдите на вкладку **Configuration** (Конфигурация).
3. Раскройте пункт **Registration** (Регистрация) и щелкните по кнопке **Organizational Unit** (Организационная единица). Программа Domino Administrator выведет на экран одно из двух диалоговых окон. Если вставлена дискета с идентификационными данными последнего сертификатора, то появится диалоговое окно **Enter Password** (Ввод пароля) для указания пароля идентификационных данных этого сертификатора. Если дискета отсутствует, откроется диалоговое окно **Choose Certifier ID** (Выбор идентификационных данных сертификатора). В диалоговом окне **Enter Password** (Ввод пароля) проверьте правильность выбора программой Domino Administrator идентификационных данных (которые должны соответствовать недавно созданному сертификатору). Если данные выбраны правильно, введите пароль и нажмите кнопку **OK**, а если неправильно - нажмите на кнопку **Cancel** (Отмена), чтобы открыть диалоговое окно **Choose Certifier ID**. В этом окне следует указать идентификационные данные сертификатора, которые были созданы на предшествующем шаге, и щелкнуть по кнопке **Open** (Открыть). Появится диалоговое окно **Enter Password**, где надо задать пароль и щелкнуть по **OK**.

4. Появится предупреждающее сообщение, указывающее на отсутствие в идентификационных данных сертификатора информации, которая необходима для восстановления идентификационных данных/пароля. На данном шаге можете проигнорировать подобное сообщение и щелкнуть по кнопке **Yes** (Да).
5. Откроется диалоговое окно **Register Organizational Unit** (Регистрация организационной единицы), похожее на диалоговое окно **Register Organization** (Регистрация организации). Отличия состоят в том, что присутствует кнопка **Certifier ID** (Идентификационные данные сертификатора) и нет поля для ввода кода страны. Если на предшествующем шаге идентификационные данные сертификатора были некорректными, можете нажать указанную кнопку и повторить ввод. В таком случае необходимость в поле кода страны отсутствует, поскольку формируемые идентификационные данные уже содержат необходимый код страны для сертификатора организации.
6. Заполняйте поля точно таким же образом, как для идентификационных данных сертификатора организации. В рассматриваемом примере именем OU является Servers. Завершив ввод данных, щелкните по кнопке **Register** (Регистрация).

После этого программа Domino Administrator повторно сформирует пару открытого/закрытого ключей, создаст файл идентификационных данных, а также соответствующий документ сертификата.

Если требуется указать сертификатор для очередного уровня (OU2 или OU3), стоит еще раз выполнить описанную выше процедуру, но с одним небольшим изменением: не следует задавать идентификационные данные сертификатора на шаге 3. Напротив, рекомендуется указывать сертификатор OU1 для построения сертификатора уровня OU2, а сертификатор OU2 - для уровня OU3. То же самое производится во время создания идентификационных данных первого сервера: выбирается сертификатор уровня OU1, OU2 или OU3, который соответствует родительской организационной единице сервера. Формирование файла идентификационных данных сервера предполагает выполнение следующей процедуры:

1. Запустите программу Domino Administrator.
2. Перейдите на вкладку **Configuration** (Конфигурация).
3. Раскройте пункт **Registration** (Регистрация) и щелкните по кнопке **Server** (Сервер). Как и в предыдущем случае, программа Domino Administrator выведет на экран одно из диалоговых окон - **Enter Password** (Ввод пароля) или **Choose Certifier ID** (Выбор идентификационных данных сертификатора). В окне **Enter Password** проконтролируйте правильность выбора программой Domino Administrator идентификационных данных для родительской единицы OU сервера. В нашем примере имя такой организационной единицы - \Servers\Stillwater. Если именно для этого имени сертификатора запрашивается пароль, введите его и щелкните по ОК. Иначе щелкните по кнопке **Cancel** (Отмена), после чего откроется диалоговое окно **Choose Certifier ID**. В нем надо правильно определить идентификационные данные сертификатора OU и щелкнуть по кнопке **Open** (Открыть). Снова появится диалоговое окно **Enter Password**, в котором требуется задать пароль и щелкнуть по кнопке ОК.
4. На экране отобразится предупреждающее сообщение, указывающее на отсутствие в идентификационных данных сертификатора информации, которая необходима для восстановления идентификационных данных/пароля. Можете проигнорировать это сообщение и щелкнуть по **Yes** (Да).

5. Появится диалоговое окно **Register Servers** (Регистрация серверов), в котором присутствует четыре поля. Следует сосредоточить внимание только на трех полях:
 - **Registration Server** (Регистрирующий сервер) позволяет заменить **Local** (Локальный) на имя сервера Domino, к которому имеется доступ;
 - **Certifier ID** (Идентификационные данные сертификатора) дает возможность исправить ошибочно указанные на шаге 3 идентификационные данные сертификатора;
 - **Security type** (Тип безопасности). В случае использования североамериканской версии программы Domino Administrator для регистрации сервера вне США или Канады задайте здесь **International** (Международный).
6. Щелкните по кнопке **Continue** (Продолжение), чтобы вывести второе диалоговое окно - **Register Server** (Регистрация сервера). В этом случае следует снова сфокусировать свое внимание лишь на нескольких полях:
 - в поле **Server Name** (Имя сервера) введите имя первого сервера, которое в рассматриваемом примере соответствует Osprey;
 - для большей части серверов поле **Password** (Пароль), вероятно, останется незаполненным, поскольку после установки пароля для сервера перестает действовать автоматический перезапуск после краха. Пароль серверу надо присвоить только в том случае, когда нет уверенности в обеспечении надежной физической защиты для соответствующего компьютера;
 - если поле **Password** остается незаполненным, то на шкале **Password quality scale** (Шкала качества пароля) установите значение 0, что указывает на необязательность пароля;
 - в поле **Domain** (Домен) на этом шаге может вводиться произвольная информация, но требуется задать какое-нибудь имя домена;
 - поле **Administrator** (Администратор) заполняется подобно полю **Domain**.
7. Щелкните по кнопке **Other** (Другие) для вывода других полей. В поле **Store Server ID** (Хранение идентификационных данных сервера) укажите **In file** (В файле) вместо варианта **In Domain Directory** (В каталоге Domain Directory). Учитывая особые условия, связанные с созданием идентификационных данных сервера для несуществующего домена, на этом шаге желательно не заносить новые идентификационные данные сервера в каталог домена. Щелкните по кнопке **Set ID File** (Формирование файла идентификационных данных) и определите путь к файлу. Если файл идентификационных данных записан на диске (как в данном примере), то надо ввести a:\osprey.id (в качестве имени файла идентификационных данных выбрано общее имя сервера).
8. Щелкните на кнопке **Registrar** (Регистрация). Программа Domino Administrator создаст файл идентификационных данных, затем документ сервера для нового сервера в каталоге Domain Directory сервера, указанного в поле **Registration Server** (Регистрирующий сервер). В нашем случае следует удалить документ сервера.

Завершено формирование набора идентификационных данных, необходимых для установки первого сервера. По окончании этой процедуры у первого сервера появится корректное имя и в дальнейшем не понадобится его переименовывать (или исключать из каталога). После установки первого сервера придется выполнить несколько дополнительных операций, в частности переименовать первого пользователя, идентификационные данные которого задавались произвольным образом (процедура переименования пользователей

достаточно проста). Рассматриваться эти действия будут, однако, несколько позже (после полного описания процедуры установки сервера).

Второй способ: последующее переименование первого сервера и пользователя

Вместо заблаговременного формирования корректного файла идентификационных данных сервера (см. описанный выше способ) здесь предусматривается проведение установки с введением некорректных имен первых сервера и пользователя (например, задаваемых в режиме по умолчанию) и последующее их переименование. Подобный подход оказывается весьма просто реализовать для имени пользователя, поскольку основная работа выполняется автоматически процессом Domino Administration Process. С другой стороны, эта задача не очень сложна и для первого сервера. Просто в данном случае приходится проделывать достаточно большой объем работы самостоятельно и учитывать множество нюансов. Если пропустить какой-нибудь шаг или допустить ошибку, поиск и устранение погрешности могут перерасти в серьезную проблему. Именно поэтому другие два способа предпочтительнее. Поскольку здесь весь объем работ нужно выполнять самостоятельно (по завершении установки первого сервера), нет смысла описывать его подробно: к нему все равно придется вернуться после обсуждения процедуры установки первого сервера (которое представлено в следующих разделах данной главы).

Третий способ: создание промежуточного первого сервера и его последующее удаление

Третий способ предусматривает создание первого сервера и пользователя с некорректно заданными именами (как и второй способ). Однако вместо реальных имен сервера и пользователя в этом случае вводятся промежуточные имена типа Temp1 для сервера и какие-нибудь короткие имена для пользователя. В дальнейшем данный способ предполагает не переименование первых сервера и пользователя, а регистрацию сертификатора организационной единицы OU и применение его для регистрации реальных серверов и пользователей, имеющих вполне корректные имена. После создания второго сервера можно отменить действия первого сервера. К этому моменту рабочая станция пользователя еще не нужна, следовательно, можно не заботиться относительно «потери» первого сервера и просто удалить его. Одновременно может быть выполнена операция по удалению первого пользователя, существенно более простая, чем переименование пользователя, поскольку непосредственно переименовать первого из пользователей нового сервера нельзя. Допустимо перенести этого пользователя на другой почтовый сервер.

Как и во втором способе, указанные действия выполняются уже по окончании процедуры установки первого сервера, поэтому более подробно они будут описаны ниже.

Конфигурирование первого сервера R5

Подготовившись к завершению установки первого сервера в организации, запустите на нем сервер Domino. На платформе Windows 9x/NT/Intel достаточно указать Domino в меню операционной системы. На других платформах загрузка Domino производится специальной

командной строкой, которая запускает приложения с помощью браузера. Так, для платформы Windows NT/Alpha эта команда имеет вид

[путь]\ahttphtpsetup

для платформы OS/2

[путь]\ihhtphtpsetup

I

а для UNIX соответственно

/opt/lotus/bin/htphtpsetup

На платформе Windows NT/Intel сервер Domino попытается загрузиться, но неудачно, поскольку еще не проведена настройка (конфигурирование). На экране дисплея появится сообщение об ошибке. Однако волшебным образом система Notes все же запустится. Присутствующая в файле notes.ini переменная (SetupDB=Setup.nsf) предписывает системе Notes открыть базу данных Domino Configuration (конфигурация сервера Domino, файл setup.nsf), которая формируется в процессе установки в каталоге данных. За счет этой базы данных автоматически откроется многоэкранная форма **Configuration** (Конфигурация). Следует аккуратно заполнить поля всех четырех экранов формы, указать параметры настройки сервера и щелкнуть по кнопке **Finish** (Готово) на последнем экране.

На платформах OS/2, UNIX и Windows NT/Alpha будет запущена сокращенная версия Domino, что позволит обеспечить доступ к базе данных Domino Web Setup (Установка Web-сервера Domino) из браузера. В этом случае приходится заполнять аналогичную форму установки и использовать ее в дальнейшем для отправки на сервер. Для доступа к серверу из браузера следует применять IP-адрес сервера в виде адреса URL (например, адрес http://192.168.0.9).

Затем системой Notes (на платформе Windows/Intel) или сервером Domino (на других платформах) выполняется основная часть процедуры установки первого сервера, при этом предусматриваются следующие действия:

1. Занесение в файл notes.ini необходимых переменных для корректного исполнения сервера Domino, в том числе и тех переменных, которые предназначены для сетевых портов и портов последовательного обмена данными, а также переменной, служащей для идентификации домена сервера.
2. Формирование каталога Domain Directory (файл names.nsf) с помощью шаблона проектирования (файл pubnames.ntf)- В этом случае первый сервер и первый пользователь добавляются в список ACL каталога Domain Directory в виде «руководителей», а первому серверу придается статус **Administrator Server** (Сервер администратора) в Domain Directory.
3. Формирование идентификационных данных сертификатора организации (или ввод этих данных), а также создание соответствующего документа сертификата в каталоге Domain Directory.
4. Формирование идентификационных данных пользователя (или ввод этих данных), а также создание соответствующего личного документа (Personal document) в каталоге Domain Directory. Идентификационные данные пользователя сохраняются в личном документе. В папке данных создается подпапка mail (Почтовая служба) и одновременно - база данных почтовой службы для первого пользователя.
5. Формирование идентификационных данных сервера (или ввод этих данных) для первого сервера, а также создание соответствующего документа сервера в каталоге

Domain Directory и добавление сервера в уже существующую в каталоге Domain Directory группу **LocalDomainServers** (Локальные серверы домена Domino).

По завершении выполнения сервером Domino описанных операций появляется последний экран формы с информацией о результатах действий по конфигурированию сервера. Здесь можно сформировать некоторые группы.

Для заполнения формы **Domino Configuration** (Конфигурация Domino) на платформе Windows NT/Intel необходимо проделать следующее (для других платформ процедура носит аналогичный характер):

1. На первом экране формы выберите **First Domino Server** (Первый сервер Domino), после чего щелкните по кнопке - • (стрелка вправо) для перехода на второй экран. Следует отметить, что данный и последующий экраны используются для вывода большого объема информации. Поэтому стоит внимательно знакомиться с информацией на каждом экране, а также перемещаться по экранам вперед и назад, чтобы сравнить доступные альтернативные варианты. При тщательном планировании конфигурации системы (как это рекомендовалось в главе 2) большая часть выведенных сведений окажется знакомой. Тем не менее лучше еще раз прочесть всю представленную информацию.
2. Выберите один из вариантов: **Quick and Easy Configuration** (Быстрое и простое конфигурирование) или **Advanced Configuration** (Дополнительное конфигурирование), после чего щелкните по кнопке -> для перехода на третий экран. Если известно, что не потребуются никаких необязательных служб, рекомендуется установить режим **Advanced Configuration**. В режиме **Quick and Easy Configuration** придется задать всего лишь несколько значений на третьем и четвертом экранах. Однако может оказаться, что имеется слишком много ненужных дополнительных служб. Например, в ряде случаев достаточно установить почтовые службы POP3 и SMTP без почтовой службы ШАР. В режиме **Quick and Easy Configuration** разрешается применять только все три службы одновременно или ни одну из них. Тщательно изучите экраны обоих режимов, чтобы в дальнейшем принять оптимальное решение. До щелчка по кнопке **Finish** (Готово) на четвертом экране допустимы любые изменения.
3. Если на втором экране выбран режим **Quick and Easy Configuration**, то на третьем экране установите режим доступа к серверу Domino: из Web-браузеров, из программ почтовой службы сети Internet и из программ чтения новостей Internet, а также возможность доступа из сервера к внутренним оконечным источникам данных с помощью службы DECS (Domino Enterprise Connection Services - корпоративная служба подключения к Domino). В режиме **Advanced Configuration** потребуется более детальный анализ вариантов по каждому из указанных направлений и параметров, напрямую не связанных с установкой определенных служб сервера Domino. Подробное описание этих возможностей будет приведено ниже, а пока взгляните на четвертый экран.
4. В обоих режимах (**Quick and Easy Configuration** и **Advanced Configuration**) четвертый экран служит для ввода имен домена, организации, первого сервера, первого пользователя, а также параметров сетевых и последовательных портов. В режиме **Advanced Configuration** процедура выбора носит более детальный характер (подробнее она обсуждается ниже), но в любом случае в конце щелкните по кнопке **Finish**, расположенной в правой верхней части формы. Форма закроется и запустится процесс автоматической установки, рассмотренный выше.

После завершения этого процесса появится последний экран формы. На нем находится несколько информационных сообщений и элементов управления:

- имена первого сервера и пользователя, а также пароли сертификатора и пользователя. До закрытия формы позаботьтесь о запоминании пароля, поскольку система Notes выводит его на экран дисплея в последний раз. Если впоследствии пароль будет утерян, идентификационные данные окажутся недоступными;
 - информация о возникших ошибках и рекомендации по их устранению;
 - предложение указать значение последнего параметра (см. ниже^), который позволяет добавить запись **Manager** (Менеджер) в список ACL всех существующих баз данных, причем пользователям настоятельно рекомендуется не пренебрегать этой возможностью;
 - информационное сообщение о необходимости установить копию программы Domino Administrator перед продолжением процедуры конфигурирования (подробное описание этой процедуры приведено в конце главы).
6. После дополнения списка ACL (Список управления доступом) закройте форму, щелкнув по кнопке **Exit Configuration** (Завершение процедуры конфигурирования), что позволит полностью остановить систему Notes.

Параметры конфигурирования сервера Domino, третий экран

После щелчка по кнопке **Finish** на шаге 4 описанной выше последовательности операций система Notes установит стандартный набор базовых служб Domino вместе со службами, которые пользователь указал на третьем экране формы (рис. 3.3).

Набор обязательных стандартных служб сервера Domino представлен ниже (в скобках приводятся названия соответствующих файлов для платформы Windows NT/Intel):

- Administration Process (Процесс администрирования, файл nadminp.exe) - программа автоматизации разнообразных административных задач;
- Agent Manager (Менеджер агентов, файл namgr.exe) - программа для управления на сервере агентами системы Notes;
- Indexer (Индексация, файл nupdate.exe) - поддержка видов и полнотекстовых индексов в базах данных системы Notes;
- Mail Router (Маршрутизация почтовых сообщений, файл nrouter.exe) - пересылка почтовых сообщений на другие серверы и их доставка получателям данного сервера;
- Replicator (Репликатор, файл nreplica.exe) - управление репликацией баз данных между серверами.

В режиме **Quick and Easy Configuration** устанавливается ряд базовых служб сервера Domino, которые в режиме **Advanced Configuration** являются необязательными:

- Schedule Manager (Менеджер планирования, файл nsched.exe) - поддержка базы данных Free Time (Свободное время, файл busytime.nsf), содержащей информацию обо всех календарных записях пользователей локальной почты, так чтобы пользователи имели возможность проследить, когда их партнеры заняты, и правильно планировали время встречи;
- Calender Connector (Коннектор календаря, файл ncalconn.exe) - извлечение из других серверов Domino данных о нераспределенном (свободном) времени пользователей;

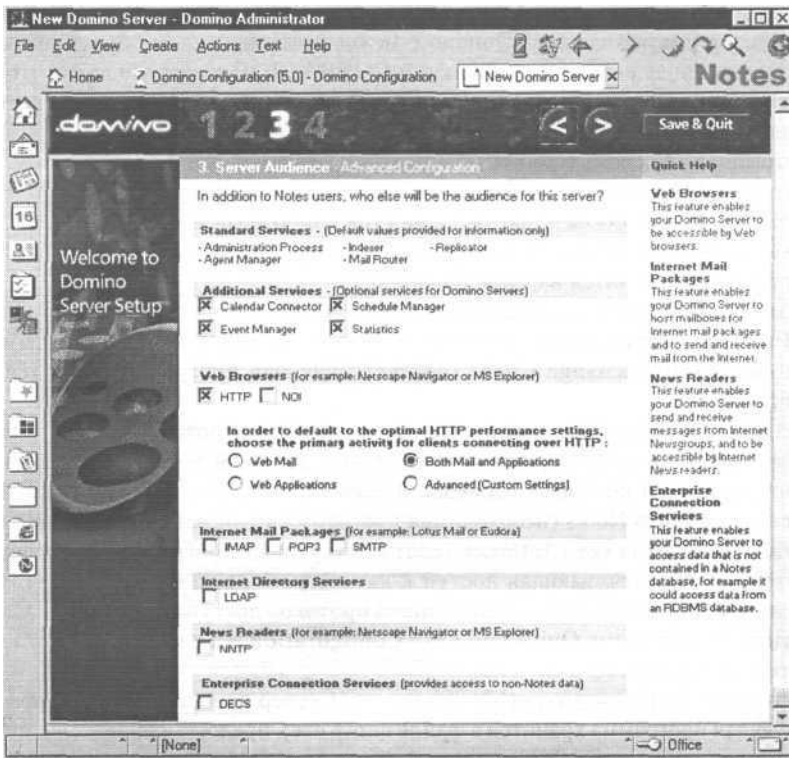


Рис. 3.3. Система Notes автоматически устанавливает службы сервера Domino, выбранные на третьем экране формы конфигурирования сервера

- Event Manager (Менеджер событий, файл nevent.exe) - отслеживание заранее заданного набора событий и уведомление администраторов об их возникновении;
- Statistics (Статистика, файл nstats.exe) - сбор статистических данных о работе сервера по электронной почте или после ввода команды.

В обоих режимах (**Quick and Easy Configuration** и **Advanced Configuration**) можно задать установку нескольких необязательных служб: службы Web-сервера Domino, службы почты Internet, службы каталога, службы сервера Network News (Сетевые новости) и службы Enterprise Connection Services (Корпоративная служба соединений). В режиме **Advanced Configuration** эти службы разделяются на группы:

- Web-службы сервера Domino:
 - служба HTTP (nhhttp.exe), которая соответствует стеку HTTP сервера Domino. После выбора этой службы на экране появляется дополнительное поле, в котором следует определить основную операцию Web-посетителей - просмотр данных, работу с базами данных почты, совместное проведение вышеупомянутых действий или какую-либо иную форму деятельности;

- служба ДИОР (Domino Internet Inter-ORB Protocol - протокол взаимодействия службы Internet сервера Domino с межсетевым брокером объектных запросов), разрешающая выполнение функций CORBA/ИОР сервера Domino, что позволяет клиентам не-Notes воспользоваться функциями этой системы (соответствующая программа хранится в файле ndiior.exe);
- О почтовая служба сети Internet:
 - сервер ШАР, предоставляющий почтовую службу по протоколу IMAP4 (Internet Mail Access Protocol - протокол доступа к почтовым сообщениям сети Internet), например для почтовой программы Netscape Communicator (соответствующая программа хранится в файле nimap.exe);
 - сервер POP3, предлагающий почтовую службу по протоколу POP3 (Post Office Protocol - протокол почтового офиса), например для почтовых программ Eudora и Microsoft Exchange Client (соответствующая программа хранится в файле pop3.exe);
 - сервер SMTP, допускающий к почтовой службе по протоколу SMTP (Simple Mail Transfer Protocol - упрощенный протокол передачи почтовых сообщений) всех отправителей почтовых сообщений сети Internet, в том числе и пользователей системы Lotus Notes (необходимая программа хранится в файле nsmtip.exe);
- О служба каталогов сети Internet (соответствующая программа хранится в файле nldap.exe), обеспечивающая доступ к каталогу по протоколу LDAP (Lightweight Directory Access Protocol - облегченный протокол доступа к каталогу). Следует отметить, что в режиме **Quick and Easy Configuration** эта служба отображается ниже почтовой службы сети Internet;
- О служба Internet Newsgroup (NNTP) Server (Сервер новостей сети Internet, соответствующая программа хранится в файле nnntp.exe), предоставляющая дискуссионные формы по протоколу NNTP (Network News Transfer Protocol - протокол передачи сетевых новостей);
- О служба Domino Enterprise Connection Service (Корпоративная служба соединений сервера Domino, соответствующая программа хранится в файле ndecs.exe), обеспечивающая в реальном масштабе времени и на основе форм связи между базами данных системы Notes и другими источниками данных, например системами управления реляционными базами данных SQL, системами транзакций или источниками данных ODBC.

Не всегда очевидно, какие службы следует установить. Поэтому на практике рекомендуется выбирать только те из них, назначение которых понятно. При возникновении каких-либо сомнений вводить службу не стоит, поскольку не составляет труда добавить любую из них на более позднем этапе.

Параметры конфигурирования сервера Domino, четвертый экран

В режиме **Advanced Configuration** четвертый экран выводится в режиме **Edit Mode** (Режим редактирования) - рис. 3.4. В режиме **Quick and Easy Configuration** этот экран открывается в режиме **Read Mode** (Режим чтения), но достаточно щелкнуть по кнопке **Edit** (Редактирование), чтобы перейти в режим редактирования. Состав четвертого экрана может несколько изменяться в зависимости от ранее выбранного режима. Ниже представлен

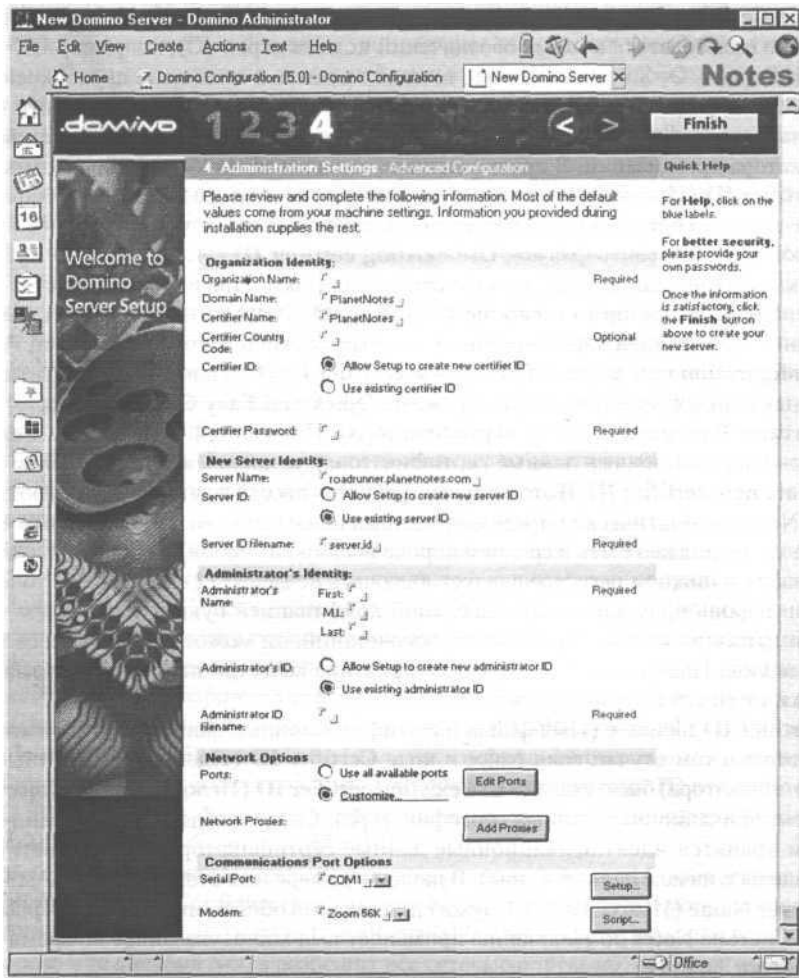


Рис. 3.4. В режиме *Advanced Configuration* выводится подробный список устанавливаемых служб для нового сервера

перечень всех полей четвертого экрана, в котором отмечены различия этого экрана в режимах **Advanced Configuration** и **Quick and Easy Configuration**.

- О **Domain Name** (Имя домена). Предназначено для ввода выбранного ранее имени домена в соответствии с принятой схемой присвоения имен. Система Notes в режиме по умолчанию указывает имя домена в сети Internet (заданное при установке протоколов TCP/IP, за исключением части имени, определяющей супердомены, например org, net и т.д.);
- О **Certifier Name** (Имя сертификатора). В этом поле следует указывать имя организации, которое было ранее выбрано для уровня O имен пользователя и сервера. Система Notes по умолчанию обычно предлагает имя хоста компьютера;

- **Code Certifier Country** (Код страны сертификатора). Если ранее было принято решение пользоваться в схеме обозначений кодами стран (C), например CN=Osprey/OU=Servers/O=Stillwater/C=US, то надо задавать в этом поле двухбуквенный код страны, определенный Международной организацией по стандартизации (International Standardization Organization - ISO), для идентификационных данных сертификатора организации. В других случаях это поле остается незаполненным;
- **Certifier ID** (Идентификационные данные сертификатора). Если идентификационные данные сертификатора вводятся заблаговременно, как упоминалось выше, необходимо установить флажок **Use existing certifier ID** (Использование существующих идентификационных данных сертификатора). Иначе рекомендуется выбрать вариант **Allow Setup to create new certifier ID** (Разрешить во время установки создание новых идентификационных данных сертификатора) в режиме **Advanced Configuration** или вариант **Create new certifier ID** (Создание новых идентификационных данных сертификатора) в режиме **Quick and Easy Configuration**;
- **Certifier Password** (Пароль сертификатора). Появляется, если в поле **Certifier ID** (Идентификационные данные сертификатора) установлен вариант **Allow Setup to create new certifier ID**. В этом случае требуется ввести в данном поле пароль. Система Notes автоматически определяет минимальное качество пароля равным 8 (то есть пароль не должен быть в среднем короче восьми символов). В буквенные пароли из словаря в нижнем регистре следует включать не менее 12 символов. В то же время, если пароль представлен произвольной комбинацией букв, цифр, знаков пунктуации и/или ничего не значащих словосочетаний, он может состоять всего из шести символов. Надо иметь в виду, что на практике качество пароля всецело зависит от сложности его дешифрования;
- **Certifier ID filename** (Имя файла идентификационных данных сертификатора). Вводится в том случае, если ранее в поле **Certifier ID** (Идентификационные данные сертификатора) было указано **Use existing certifier ID** (Использование существующих идентификационных данных сертификатора). Следует задать путь к файлу, в котором хранятся идентификационные данные сертификатора (см. соответствующие разделы в начале данной главы). В нашем примере имя этого файла - a:\stillwater.id;
- **Server Name** (Имя сервера). Служит для задания общего имени (CN) первого сервера. Система Notes по умолчанию применяет имя хоста, указанное во время установки стека TCP/IP;
- **Server's Hostname** (Имя хоста сервера). Система Notes заполняет его самостоятельно, используя значение из стека IP;
- **Server ID** (Идентификационные данные сервера). Если идентификационные данные сервера созданы заблаговременно (см. соответствующие разделы в начале данной главы), следует выбирать вариант **Use existing server ID** (Использование существующих идентификационных данных сервера), иначе - вариант **Allow Setup to create new server ID** (Разрешить во время установки создание новых идентификационных данных сервера) или в режиме **Quick and Easy Configuration** вариант **Create new server ID** (Создание новых идентификационных данных сервера);
- **Server ID filename** (Имя файла идентификационных данных сервера). Открывается при условии, что в поле **Server ID** задан вариант **Use existing server ID**. Введите имя файла идентификационных данных сервера, который было ранее создан (см. разделы в начале данной главы). В рассматриваемом примере именем файла будет a:\osprey.id;

- О **Administrator Name** (Имя администратора). В нем указывается имя первого пользователя. Когда отсутствует другое подходящее имя, можно воспользоваться собственным. Если планируется в дальнейшем отказаться от работы с первым сервером и первым пользователем, разрешается выбрать любое имя (см. соответствующие разделы в начале данной главы). Фамилия и отчество необязательны, но имя пользователя требуется непременно;
- О **Password** (Пароль). Это поле появляется после выбора варианта **Allow Setup to create new administrator ID** (Разрешить во время установки создание новых идентификационных данных администратора) в поле **Administrator ID** либо варианта **Create new administrator ID** (Создание новых идентификационных данных администратора) в режиме **Quick and Easy Configuration**. Здесь вводится пароль, а система Notes автоматически задает качество равное 8. Это означает, что длина пароля в среднем будет не меньше восьми символов. Буквенные пароли из словаря в нижнем регистре должны содержать не менее 12 символов. Если же пароль представлен произвольной комбинацией букв, цифр, знаков пунктуации и/или ничего не значащих словосочетаний, он может состоять всего из шести символов. Следует помнить, что на практике качество пароля целиком определяется сложностью его дешифрования;
- О **Administrator ID** (Идентификационные данные администратора). Если идентификационные данные сервера были созданы заблаговременно, укажите **Use existing administrator ID** (Использование существующих идентификационных данных администратора), в других случаях - вариант **Allow Setup to create new administrator ID** (Разрешить во время установки создание новых идентификационных данных администратора) или вариант **Create new administrator ID** (Создание новых идентификационных данных администратора) в режиме **Quick and Easy Configuration**;
- О **Administrator ID filename** (Имя файла идентификационных данных администратора). Появляется после выбора варианта **Use existing administrator ID** в поле **Administrator ID**. Введите путь к файлу идентификационных данных пользователя. В рассматриваемом примере это будет a:\kirkland.id;
- О **Ports** (Порты). Видно на экране только в режиме **Advanced Configuration**. В режиме **Quick and Easy Configuration** система Notes автоматически устанавливает все доступные порты. Если указать **Use all available ports** (Использование всех имеющихся портов), то система Notes разрешит все сетевые порты, которые допускаются операционной системой. После выбора **Customize** (Настройка) на экране появится кнопка **Edit Ports** (Редактирование портов). Она открывает диалоговое окно **Port Setup** (Установка портов), где показана таблица, строки которой соответствуют доступным сетевым портам. Нужно отключить порты, не используемые сервером Domino;
- О **Network Proxies** (Сетевые прокси). Это поле появляется только в режиме **Advanced Configuration**. Если серверу необходим доступ к другим серверам, расположенным за брандмауэром, требуется указать имена хостов или IP-адреса прокси-серверов. Для этого щелчком по кнопке **Add Proxies** (Добавить прокси) откройте диалоговое окно **Proxy Server Configuration** (Конфигурация прокси-серверов). Поскольку сервер Domino поддерживает прокси-серверы HTTP, Socks и Notes RPC, в диалоговом окне предусмотрено поле для каждого типа прокси-сервера. Для любого типа сервера, с которым в будущем предстоит взаимодействовать новому серверу Domino, вводится имя хоста или IP-адрес. В том случае, когда доступ через прокси к другим серверам, находящимся до брандмауэра, не нужен, указывается имя домена, имя хоста

или IP-адрес таких серверов в поле **No proxy for these hosts or domains** (Без использования прокси для этих хостов или доменов). Если информация отсутствует, ее можно добавить на более поздних этапах, например после запуска сервера;

- О **Serial Port** (Порт последовательного обмена данными). Если предполагается, что с сервером будут работать один или большее число модемов, можно в этом поле поставить в соответствие одному из модемов порт COM (настройка других модемов выполняется уже после запуска сервера);
- О **Modem** (Модем). Если планируется применять модем, здесь можно указать его драйвер. Драйверы модемов в списке являются файлами *.mdm из подпапки modems данного сервера;
- О **Setup** (Установка). После выбора порта COM и модема (с помощью двух вышеупомянутых полей) достаточно щелкнуть по этой кнопке, чтобы вывести диалоговое окно **Additional Setup** (Дополнительная установка), в котором можно определять различные параметры модема (подробное описание приведено в главе 4);
- О **Script** (Сценарий). Если имеющийся модем подключен к сети Frame Relay или X.25, в этом поле разрешается указать сценарий, позволяющий корректно формировать необходимые соединения. Щелчком по кнопке **Script** откройте диалоговое окно **Connect Script** (Сценарий подключения), в котором предлагается выбрать из списка подходящий сценарий и задать его аргументы. Появляющиеся в этом списке сценарии являются файлами *.scg из подпапки modems папки data данного сервера.

Параметры конфигурирования сервера Domino, последний экран

Последний экран, предназначенный для выбора конфигурации сервера и имеющий название **Congratulations!** (Поздравления), предлагает воспользоваться кнопкой **Set Access Control List Entry** (Установка записи в списке управления доступом), причем рекомендуется обязательно сделать такую запись в списке ACL. Щелкните по кнопке для открытия диалогового окна **Set Default Database Access** (Установка параметров по умолчанию для доступа к базе данных), где можно выполнить две операции:

- О ввести в списки ACL всех существующих баз данных группу или пользователя с уровнем доступа **Manager** (Менеджер). Лучше всего произвести эту операцию в режиме по умолчанию, что предполагает добавление группы **Administrators** (Администраторы). В таком случае сервер Domino создаст документ группы (Group document), после чего добавит имя группы **Manager** в списки ACL всех существующих баз данных;
- О внести в списки ACL всех существующих баз данных пользователя **Anonymous** (Анонимный) и присвоить ему статус **No Access** (Без права доступа). Рекомендуется внимательно изучить возможности, предлагаемые в рамках этого варианта.

После выбора одного из двух вариантов щелкните по кнопке OK - система Domino быстро модифицирует все базы данных и вернется на экран **Congratulations!**. Здесь элемент управления для модификации списков ACL будет заменен сообщением о том, что в х баз данных были успешно добавлены элементы ACL либо что такая операция не удалась (в этом случае сообщается о причинах неудачного добавления). Запишите данные о возникших ошибках, запомните пароль и щелкните по кнопке **Exit Configuration** (Завершение конфигурирования). Сервер Domino будет остановлен, но при следующем запуске начнет работать в нормальном режиме.

Конфигурирование первого сервера R6

Установка сервера Domino R6 стала гораздо проще, поскольку многие параметры настройки сервера задаются по умолчанию. В системе Windows после завершения работы Мастера установки выберите в меню **Lotus Application** (Приложения системы Lotus) пункт **Lotus Domino Server** (Сервер Lotus Domino). Для других платформ выполните те же команды, что и для сервера R5. Запустится программа установки сервера R6 (в нашем случае это будет первый сервер). На экране **Welcome to Domino Server Setup** (Добро пожаловать в программу установки сервера Domino) можно щелкнуть по кнопке **Help** (Справка), чтобы ознакомиться с рекомендациями компании Lotus по установке сервера. А для перехода на следующий экран Мастера установки нужно щелкнуть по кнопке **Next** (Далее).

На втором экране доступны два варианта: **Set up the first server or a stand-alone server** (Установка первого или автономного сервера) и **Set up an additional server** (Установка дополнительного сервера). В данном случае, несомненно, надо выбрать первый вариант и щелкнуть по кнопке **Next**.

На третьем экране следует ввести имя сервера (**Server name**) и его описание (**Server title**), а также установить флажок **I want to use an existing server ID file** (Использовать существующий файл идентификационных данных сервера), если выполнены предложенные выше рекомендации и уже подготовлены идентификационные данные для сервера. Для этого требуется щелкнуть по кнопке **Browse** (Просмотр) и выбрать нужный файл идентификационных данных сервера (server.id), который обычно находится в каталоге lotus\domino\data.

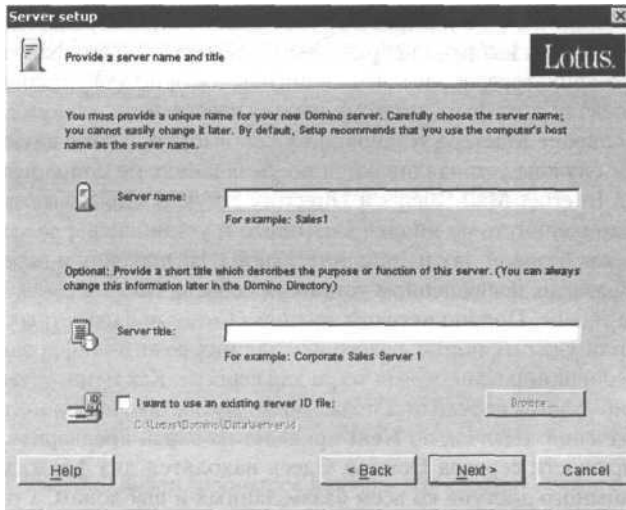


Рис. 3.5. Ввод имени и описания сервера

На четвертом экране Мастера установки необходимо ввести имя организации (это некое логическое понятие, которое не обязательно совпадает с реальной организацией или компанией), а также пароль сертификата организации (O), который придется подтвердить в соседнем поле. Флажок **I want to use an existing certifier ID file** (Использовать

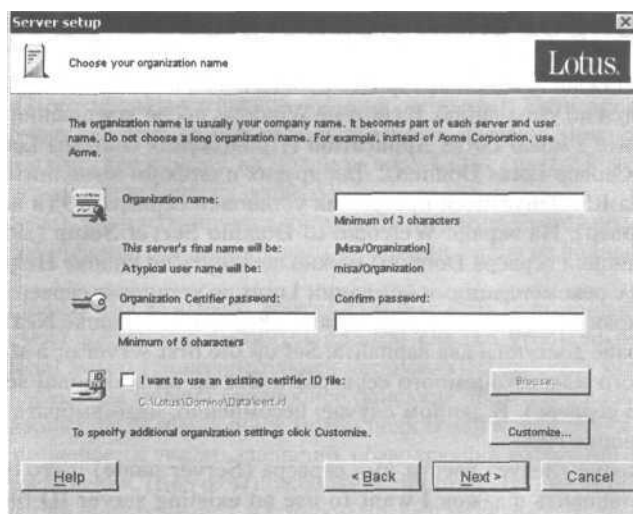


Рис. 3.6. Ввод имени и пароля организации

существующий файл идентификационных данных сертификатора) позволит воспользоваться уже подготовленным идентификационным файлом сертификатора организации. Кнопкой **Customize** (Настройка) открывается еще один экран, где вводятся имя и пароль организационной единицы (OU), а также двухбуквенный код страны (для США это US, а для России - RU). Если выбрано использование существующего файла идентификационных данных сертификатора, появится дополнительное окно для указания пароля на этот файл. Мы сами создали этот файл, поэтому пароль известен.

На следующем экране Мастера установки нужно выбрать состав служб сервера. Заметим, что основные службы устанавливаются по умолчанию, но дополнительно можно задать Web Browser, Internet Mail Clients и Directory Services. Для более точной настройки состава служб надо щелкнуть по кнопке **Customize** и установить флажки для любой доступной службы (как базовой, так и дополнительной). Назначения и перечень служб подробно описаны в разделе, посвященном установке сервера R5.

На следующем экране, **Domino network settings** (Сетевые параметры сервера Domino), можно добавить или удалить порты, разрешить для них режим шифрования, а также ввести полностью квалифицированное имя хоста для сервера. Как и при установке версии R5, эти параметры допускается определить позже, поэтому достаточно принять предложенные по умолчанию значения. Щелчок по **Next** приведет на экран предварительной установки параметров безопасности сервера Domino. Здесь находятся два флажка, определяющие запрещение анонимного доступа ко всем базам данных и шаблонам, а также добавление группы Local Domain Admins (Администраторы локального домена) во все базы данных и шаблоны. Как резонно замечено в нижней части экрана, если назначение флажков непонятно, следует оставить их без изменения.

На последнем экране перечислены итоговые параметры настройки сервера. Внимательно проверьте их и при необходимости вернитесь назад, чтобы внести необходимые изменения. Если все параметры указаны правильно, щелкните по кнопке **Setup** (Установка), чтобы

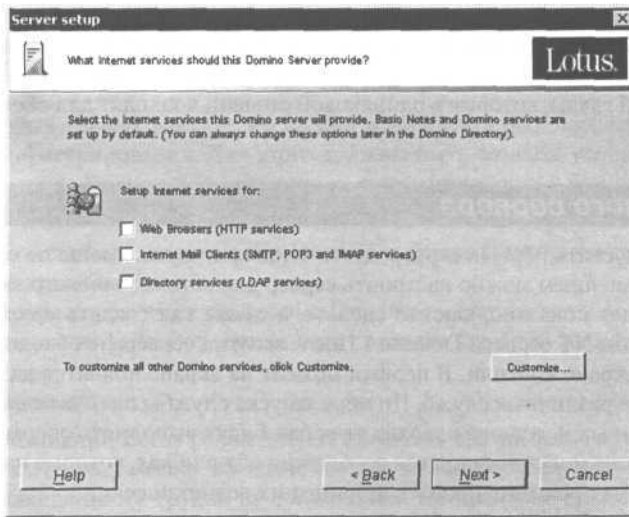


Рис. 3.7. Выбор состава устанавливаемых служб сервера Domino 6

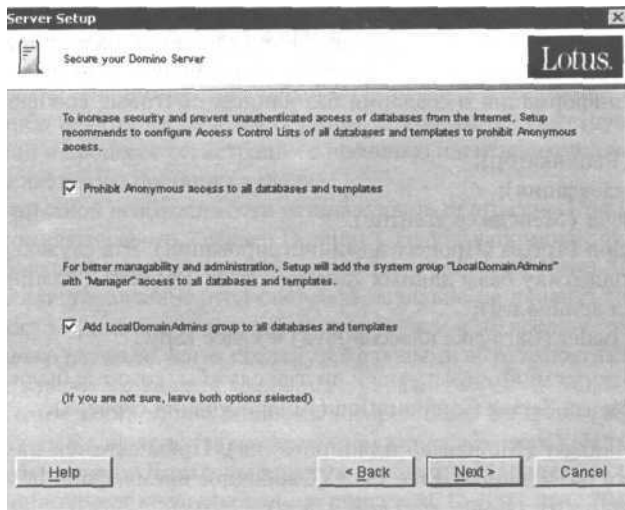


Рис. 3.8. Выбор параметров безопасности сервера Domino 6

начать установку сервера (до этого устанавливалось программное обеспечение данного сервера). После инсталляции всех выбранных компонентов сервера появится заключительный экран Setup summary (Итоги установки), где будут отмечены все обнаруженные ошибки (надеемся, их не будет, если следовать всем нашим рекомендациям). Если все прошло успешно, щелкните по кнопке Finish (Завершение), чтобы закрыть экран и перейти

к запуску сервера Domino. Как нетрудно заметить, процедуры установки версий R5 и R6 отличаются друг от друга не параметрами настройки, а выводимыми интерфейсными экранами. В обоих случаях задаются одни и те же параметры, что подтверждается следующими разделами этой главы, которые в одинаковой степени подходят для обеих версий сервера Domino.

Запуск первого сервера

Теперь, чтобы запустить первый сервер, достаточно щелкнуть в меню по соответствующему ярлыку. В дальнейшем можно настроить сервер для автоматического запуска. (В конце данной главы будет показано, как это сделать, а также как создать ярлыки для запуска и остановки службы NT сервера Domino.) После запуска сервера необходимо отслеживать информацию на экране консоли. В первый момент на экране появятся данные о последовательном запуске различных служб. По мере запуска службы начинают обращаться к различным базам данных и, если не находят этих баз, будут выполнять операции по их созданию. На экран также могут выводиться сообщения об ошибках, которые надо внимательно отслеживать, чтобы проанализировать причины их возникновения.

Перечислим службы, которые обычно иницируются при запуске нового сервера (в порядке их запуска):

- Mail Router (Маршрутизация почтовых сообщений). Обеспечивает формирование и поддержку одной или многих баз данных Incoming Mail (Входящие почтовые сообщения), соответствующих файлу mail.box (для одной базы данных) или файлам mailn.box (для n баз данных, где n равно целому числу в диапазоне от 1 до 9). Более подробная информация о создании баз данных почтовых сообщений приводится в главе 8;
- Replicator (Репликатор);
- Indexer (Индексация);
- Agent Manager (Менеджер агентов);
- Administration Process (Процесс администрирования). Эта служба обеспечивает создание и поддержку базы данных Administration Requests (Административные запросы, файл admin4.nsf);
- Java Class Loader (Загрузка классов Java) и класс ISpy.

В этот момент могут иницироваться и другие службы, которые были выбраны на третьем экране документа Server Configuration (Конфигурация сервера):

- Schedule Manager (Менеджер планирования). Предназначен для формирования и поддержки базы данных Free Time (Свободное время, файл busytime.nsf);
- Calendar Connector (Коннектор календаря);
- Stats (Сбор статистических данных). Создает базы данных [имя_сервера] Stats/[InMfl_организации] (файл statmail.nsf) и соответствующие документы Mail-In Database (База данных входящих почтовых сообщений). В дальнейшем эта служба контролирует сформированную базу данных и отслеживает направленные по почте запросы о статистических данных;
- Events (События). Создает и отслеживает базу данных Statistics & Events (Статистические данные и события, файл events4.nsf) и базу данных Statistics Reports (Отчеты по статистическим данным, файл statrep.nsf).

Установка учетной записи первого пользователя

Теперь, когда первый сервер фактически введен в эксплуатацию, необходимо завершить процедуру его конфигурирования. Для этого должны быть созданы условия нормального исполнения программы Domino Administrator, инсталляция которой до сих пор еще не проводилась. На практике имеется три варианта ее установки:

- О на том же компьютере, что и сервер Domino, и с использованием тех же папок программ и папок данных;
- О на том же компьютере, что и программа Domino, но с применением иной папки данных (исполняемые файлы программ могут находиться в той же или в другой папке программ);
- О на другом компьютере.

Специалисты компании Lotus рекомендуют выбирать третий или (в том случае, когда требуется установить программное обеспечение клиента на сервере) второй вариант, причем с этими рекомендациями трудно не согласиться. На практике существует несколько причин, по которым не следует устанавливать клиентские программы на компьютере, используемом для установки сервера.

Во-первых, исполнение каких-либо посторонних фоновых программ приводит к заметному возрастанию нагрузки на процессор, а это в свою очередь плохо влияет на возможности сервера по обслуживанию удаленных клиентов.

Во-вторых, разрешение локального доступа к серверу иногда отрицательно сказывается на системе его защиты. Например, локальный пользователь в состоянии манипулировать данными каким-либо неавторизованным образом. Кроме того, существует опасность, что внесение изменений в процессе регистрации с помощью идентификационных данных сервера приведет к ослаблению функции аудита.

И наконец, нет никакой необходимости устанавливать программу Domino Administrator на том же самом компьютере, что и сервер Domino. Следует напомнить, что администраторы, накопившие большой практический опыт работы с системой Notes/Domino версии 4, обычно осуществляли управление этой системой локально из клиента Notes. Многие администраторы просто привыкли к подобным процедурам и не исключено, что они почувствуют себя несколько неуютно, когда столкнутся с новыми возможностями версии 5 или 6. Однако начиная с версии 5 функция удаленного управления стала весьма простой.

На самом деле единственной причиной, по которой было бы целесообразно управлять сервером версии 5 или 6 локально (за исключением запуска сервера), является блокирование списка ACL базы данных. Локальный доступ дает право **Manager** на списки ACL (если система Notes/Domino имеет несогласованные списки ACL - см. главу 20). Однако для обращения к списку ACL достаточно работать с клиентом Notes, а не с программой Domino Administrator. При этом клиент Notes устанавливается (на платформе Windows/Intel) совместно с сервером Domino (файл nlnotes.exe).

Для запуска клиента Notes на сервере Domino следует воспользоваться файлом nlnotes.exe. Когда файл notes.ini находится в папке программ сервера Domino или в любой другой папке из списка путей поиска операционной системы Windows, клиент Notes запускается командой

[путь]\nlnotes.exe

Если файл `notes.ini` расположен в папке данных сервера Domino (куда он и должен быть помещен для сегментированного сервера) или вне путей поиска операционной системы Windows, для запуска Notes потребуется команда

`[путь]\nlnotes.exe = [путь]\notes.exe`

В обоих примерах параметр `[путь]` указывает на реальное местоположение соответствующего файла.

Из сказанного следует, что практически в любой ситуации можно установить программу Domino Administrator на любом компьютере, кроме компьютера сервера. Единственным исключением является ситуация с использованием только одного компьютера. Например, может потребоваться иметь сервер Domino у провайдера Internet или установить тестовый или демонстрационный сервер Domino на переносном компьютере.

В подобной ситуации рекомендуют установку программы Domino Administrator в отдельном от сервера Domino наборе папок. Если объем свободной памяти на диске ограничен, можно поместить программу в папки сервера Domino, но при этом файлы данных должны храниться в других папках.

Если ранее было принято решение о том, что Notes и Domino должны находиться в одной папке программ, необходимо перенести папку данных в файл `notes.ini`, созданный в процессе первой установки. В противном случае при второй установке файл `notes.ini` будет перезаписан. Кроме того, требуется соответствующим образом отредактировать ярлыки, сформированные при первой установке - так, чтобы их структура указывала на факт переноса файла `notes.ini` из папки программ.

Программа Domino Administrator, как правило, устанавливается одновременно с клиентом Notes. Поскольку программы Domino Administrator и Domino Designer являются своего рода альтернативными оболочками для клиента Notes, программа InstallShield всегда дополнительно устанавливает стандартный клиент системы Notes. Следует отметить, что программа InstallShield обеспечивает, наряду с выполнением множества других функций, добавление ярлыков в меню для каждой клиентской программы.

Для первого запуска клиента можно задействовать любой ярлык, но лучше воспользоваться ярлыком программы Domino Administrator, поскольку только она позволит завершить процедуру выбора конфигурации сервера. При первом запуске клиента Notes появится диалоговое окно **Lotus Notes Client Configuration Wizard** (Мастер конфигурирования клиента системы Lotus Notes). Как указано на первом экране этого Мастера, можно выбрать различные режимы настройки, включая соединение с сервером Domino, а также с одним или несколькими серверами сети Internet. Цель в данном случае состоит в настройке клиента для завершения конфигурирования первого сервера, поэтому ниже внимание в основном будет сконцентрировано на соответствующих возможностях. В главе 5 более подробно рассмотрен ряд других параметров настройки клиента.

Ниже представлены рекомендации по выбору ответов на запросы Мастера:

1. Ознакомьтесь с информацией на первом экране и щелкните по кнопке **Next** (Далее).
2. Оставьте предложенный по умолчанию режим **I want to connect to a Domino server** (Подключение к серверу Domino) и щелкните по кнопке **Next**.
3. Воспользуйтесь методом соединения по умолчанию: **Set up a connection to a local area network** (Установка подключения по локальной сети), после чего щелкните по кнопке **Next**.
4. Введите имя первого сервера. В нашем примере это **Osprey/Stillwater**, **Osprey/Servers/Stillwater** или **Templ/Stillwater** (в зависимости от того способа, который был выбран

для установки первого сервера и пользователя в организационной единице OU - см. начало данной главы), затем щелкните по кнопке Next.

5. Сообщите серверу Domino идентификационные данные первого пользователя. При этом возможны два варианта:
 - если регистрация пользователя уже проводилась раньше (этот вопрос не рассматривался в данной главе), рекомендуется первый вариант - **My Notes User ID has been supplied to me in a file** (Идентификационные данные пользователя системы Notes предоставлены в файле). Затем нужно заполнить поле **First Name** (Имя пользователя) и щелкнуть по кнопке **Next**. Если указываемый файл еще не занесен в папку данных системы Notes, последует запрос на его копирование. Ответьте **Yes** (Да), введите пароль, а затем щелкните по кнопке OK;
 - если регистрация первого пользователя не была проведена, файл идентификационных данных первого пользователя находится в его персональном документе (Personal document). В этом случае следует выбрать второй вариант - **Use my name as identification** (Использовать имя пользователя для идентификации) и ввести общее имя **Common Name** полного имени пользователя (в рассматриваемом примере - Rob Kirkland), а затем щелкнуть по кнопке Next.
6. Клиент Notes постарается подключиться к серверу по локальной сети. Если подключение пройдет успешно, появится экран с соответствующим сообщением, затем надо щелкнуть по кнопке Next. Если попытка окажется неудачной, будет выведен экран, где можно скорректировать имя сервера, задать его сетевой адрес и указать сетевой протокол, которым должен пользоваться клиент Notes. После ввода этой информации следует снова щелкнуть по кнопке **Next**, а клиент Notes сделает еще одну попытку подключения к серверу. В случае ее успешного завершения отобразится соответствующий экран с сообщением, после чего необходимо щелкнуть по кнопке Next. В случае неудачного завершения и этой попытки появится одно из перечисленных ниже сообщений об ошибке:
 - сообщение **Server not responding** (Сервер не отвечает). Одной из причин подобной ошибки может послужить:
 - задание неверного сетевого адреса или протокола (произведите необходимую коррекцию и повторите попытку);
 - не работает сервер Domino (запустите сервер и повторите попытку);
 - программное обеспечение сетевого протокола неправильно настроено на компьютере или сервере (закройте клиент Notes, устраните имеющиеся проблемы и повторите попытку);
 - сама сеть блокирует формирование соединения между рабочей станцией и сервером, например из-за отказа сетевых аппаратных или программных средств (закройте клиент Notes, устраните имеющиеся проблемы и повторите попытку);
 - сообщение **Connection denied. The server you connected to has a different name from the one requested** (Подключение запрещено. Сервер, к которому осуществляется подключение, имеет иное имя, чем указано в запросе). Возможно, имя сервера было задано неверно, поэтому проверьте полное имя сервера и при необходимости введите его повторно. Либо в сети может оказаться несколько серверов с одинаковыми именами. В этом случае придется остановить один из серверов и удалить его или отключить от сети.
7. Мастер спросит об установке почтовой учетной записи в сети Internet. Если в этом есть необходимость, Мастер выведет ряд экранов для ввода требуемых данных.

8. На последнем экране сообщается о завершении установки клиента Notes. Щелкните по кнопке **Finish** (Готово).
9. После этого система Notes сформирует необходимое соединение с сервером Domino, который в свою очередь проверит идентификационные данные пользователя в каталоге Domain Directory и обеспечит завершение настройки клиента Notes. Если на шаге 5 было введено новое имя, клиент Notes запросит пароль для файла идентификационных данных, скопирует его в локальный каталог данных и присвоит ему имя user.id. Затем клиент Notes перейдет к настройке рабочей станции, а по завершении этой процедуры сообщит о ее результатах. Щелкните по кнопке ОК. После выполнения ряда дополнительных операций по конфигурированию на экране появится интерфейс программы Domino Administrator (или клиента Notes).

Интерфейс программы Domino Administrator

Если пользователю раньше не приходилось сталкиваться с интерфейсом программы Domino Administrator (рис. 3.9), следует внимательно его изучить. Программа Domino Administrator в операционной системе Windows запускается либо щелчком по соответствующему ярлыку в меню, либо из клиента Notes (щелчком по вкладке в левой части экрана). Кроме того, можно использовать команду **Tools** (Программные инструменты) Domino Administrator из меню **File** (Файл) клиента Notes.

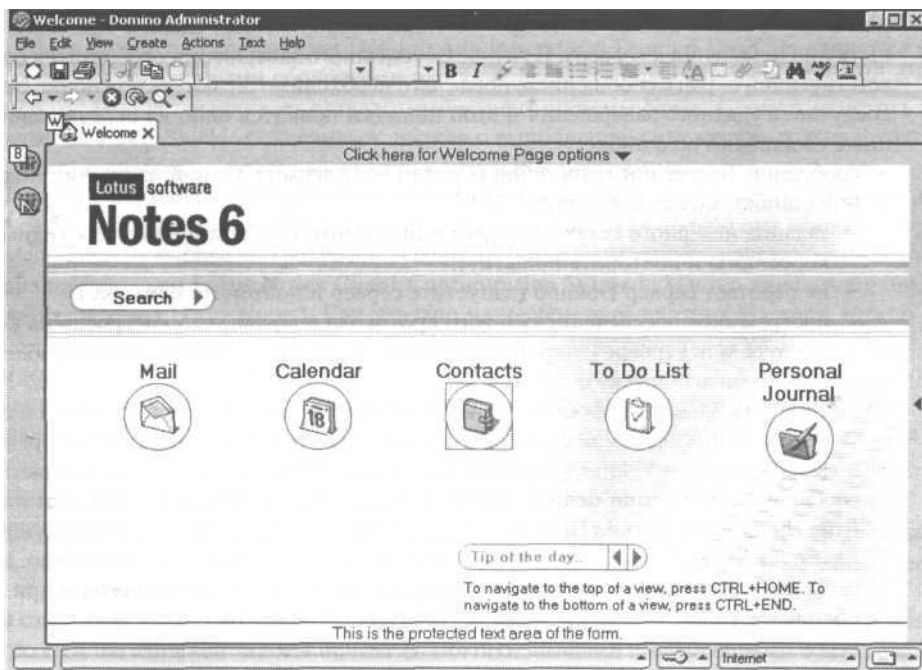


Рис. 3.9. Программа Domino Administrator версии R6

Мы не приводим сведения относительно интерфейса и соответствующих функций программы Domino Administrator, поскольку пользователи в состоянии ознакомиться с ними самостоятельно. Начать подобное знакомство рекомендуется со страницы **Welcome** (Приветствие), которая появляется при первом запуске программы Domino Administrator.

Для лучшего понимания можно воспользоваться меню **Help** (Справка) и запустить **Guided Tour** (Ознакомительный тур), представляющий собой анимационное интерактивное слайд-шоу об основных возможностях подпрограммы. Назовем элементы интерфейса, на которые следует обратить особое внимание при ознакомлении с программой:

- *контекстно-зависимая (контекстная) справка.* Если при работе с программой Domino Administrator возникнет потребность в дополнительных сведениях, нажмите функциональную клавишу F1, чтобы вывести нужные страницы из базы данных Domino Administration Help (Справка по администрированию сервера Domino R6);
- меню, программные инструменты и раскрывающиеся меню. Большую часть задач обычно можно решать тремя способами - обратиться к меню **Actions** (Операции) в верхней части экрана, воспользоваться панелью **Tools** в правой части экрана или щелкнуть правой кнопкой мыши по соответствующему объекту для вывода раскрывающегося (контекстного) меню, содержащего доступные для этого объекта операции;
- масштабируемые, закрываемые и закрепляемые панели. Пользователи могут перетаскивать мышью границы между панелями для изменения размеров панелей. Решается также закрыть панели **Tools** (Программные инструменты) и **Servers** (Серверы) или закрепить (pin) их на экране, чтобы они были постоянно открытыми;
- интерфейс с перетаскиванием мышью. Можно перетащить (drag-and-drop) имя пользователя на сервер, чтобы изменить почтовый сервер этого пользователя. Перетаскивание имени базы данных на сервер приведет к ее копированию на данный сервер;
- административные предпочтения - см. пункт **Preferences** (Предпочтения) в меню **File**. Можно указать администрируемые домены Domino, состав столбцов в списке файлов на вкладке **Files** (Файлы), а также параметры по умолчанию для экранов регистрации. Допустимо также точно настроить параметры мониторинга сервера;
- обновление списка серверов в меню **Administration** (Администрирование). Предназначено для обновления списка серверов после их добавления или удаления из администрируемого домена.

Завершение процедуры конфигурирования первого сервера

Теперь, после успешного завершения конфигурирования и запуска первого сервера и клиентской программы Domino Administration, можно закончить процедуру конфигурирования первого сервера. Для этого следует выполнить указанные ниже операции:

- добавление или удаление портов (при необходимости);
- настройка именованных сетей Domino;
- создание групп администрирования;
- установка Administration Process (Процесс администрирования);
- редактирование списков доступа в документе сервера (Server document);
- редактирование (при необходимости) некоторых полей в документе сервера;

- О создание (при необходимости) документов сертификата (Certificate document) и повторное копирование открытого ключа сервера из файла идентификационных данных сервера в документ сервера (при этом можно ограничиться указанными выше действиями, если при задании конфигурации первого сервера применялись заблаговременно подготовленные идентификационные данные сервера и сертификатора);
- О переименование (при необходимости) пользователя и сервера либо создание нового сервера или отмена использования прежнего. Эти действия необходимы, когда требуется включить пользователя и сервер в организационную единицу OU, а программе Server Configuration (Конфигурация сервера) разрешено формировать идентификационные данные сервера и сертификатора; однако в таком случае настоятельно рекомендуется выполнить эти действия еще до создания каких-либо иных серверов или пользователей).

Настройка портов

Если к этому моменту на форме Server Configuration (Конфигурация сервера) еще не определен сетевой порт для взаимодействия с сервером, что происходит только в режиме Advanced Configuration (Дополнительное конфигурирование), система Notes будет конфигурировать все доступные сетевые порты. Рекомендуется проконтролировать параметры портов и отменить использование тех портов, которые не требуются для последующей работы сервера. Это сэкономит память и уменьшит нагрузку на процессоры.

Более того, если на сервере предполагается установить несколько сетевых адаптеров (например, один адаптер для подключения пользователей к серверу, а второй для соединения между серверами), возможно, понадобится дополнительно создать новые порты, например организовать второй порт для протоколов TCP/IP.

Аналогично, если планируется применить на сервере порт COM (например, для доступа к модему) и данный порт еще не был разрешен на форме Server Configuration, это может быть сделано теперь. Надо помнить, что форма Server Configuration допускает описание только одного модема, поэтому при установке сервера с несколькими модемами необходимо разрешить несколько дополнительных портов.

И наконец, когда намечается эксплуатировать порты сети Internet или прокси-серверы для обращения к сети Internet, возможно, понадобится провести конфигурирование этих портов.

Существует три способа запрещать, разрешать, создавать, переименовывать и удалять порты: в клиенте Notes, в программе Domino Administrator или в консоли управления сервера Domino. Клиент Notes позволяет выполнять эти операции только локально, причем серверы нельзя использовать в моменты проведения подобных операций, поэтому на практике клиент Notes целесообразно применять только для разрешения/запрета портов рабочих станций. Управлять серверами следует с помощью программы Domino Administrator или консоли сервера Domino, поскольку оба средства в состоянии разрешать/запрещать применение портов без прерывания работы сервера. В этом смысле программа Domino Administrator имеет дополнительные преимущества, поскольку обеспечивает удаленное управление.

Для разрешения или запрета порта в программе Domino Administrator выполните следующие действия:

1. Убедитесь в том, что правильно выбран сервер, порты которого будут разрешены или запрещены. При первом запуске программы Domino Administrator обычно указан

- вариант **Local** (Локальный). Для выбора другого сервера щелкните в левой части экрана по закладке с именем домена (**[имя_домена]**), затем укажите нужный сервер.
2. Перейдите на страницу **Servers** (Серверы) и выберите **Server => Port Information** (Сервер => Информация порта) на панели **Tools** (Программные инструменты) или в меню **Server** (Сервер). В версии R6 команда называется **Setup Ports** (Установка портов). Если в этот момент наблюдать за консолью управления, то можно проследить, как программа Domino Administrator направляет группы команд **Show Configuration** (Показать конфигурацию) на сервер для сбора информации о текущем состоянии его портов, а затем воспроизводит полученную информацию в диалоговом окне **Port Setup for [имя_сервера]** (Установка портов соответствующего сервера).
 3. В списке **Communication Ports** (Порты связи) выберите тот порт, который планируется разрешить или запретить, для чего установите или сбросьте флажок **Port Enable** (Разрешение порта).
 4. Щелкните по кнопке ОК. На консоли управления будет видно, как программа Domino Administrator направляет на сервер группу консольных команд **Set Configuration** (Установка конфигурации), которые изменяют конфигурацию выбранного сервера.

Чтобы разрешить или запретить порт с помощью консоли управления сервера Domino, требуется ввести команду `start port [имя_порта]` или `stop port [имя_порта]`, где параметр `[имя_порта]` определяет имя соответствующего порта.

Состояние портов на сервере определяется командой `show allports`. Команда покажет как сетевые, так и последовательные порты.

Разрешение или запрещение сетевого порта на практике является двухшаговой процедурой, причем все вышеописанные действия относятся к ее первому шагу. Для завершения процедуры необходимо изменить значение в поле **Enabled** (Разрешено) для портов в документе сервера (Server document). Для этого следует открыть документ сервера в режиме **Edit Mode** (Режим редактирования), перейти на страницу **Ports/Notes Network Ports** (Порты/сетевые порты Notes) и указать в соответствующем поле значение **Enabled** (Разрешено) или **Disabled** (Запрещено).

Чтобы выполнить полное конфигурирование порта последовательного обмена данными, потребуется выбрать программу-драйвер для модема и соответствующим образом ее настроить (см. главу 4).

Для создания, удаления или переименования портов в программе Domino Administrator служит аналогичная процедура/Единственным отличием станет использование диалогового окна **Port Setup** (Установка порта), где следует указать **New** (Новый), **Rename** (Переименование) или **Delete** (Удаление).

При создании второго порта для определенного протокола (например, второго порта TCP/IP) следует выбирать понятное имя. С другой стороны, допустимо одновременно переименовать первый порт, так чтобы его имя заметно отличалось от имени второго порта. Например, при наличии двух портов для протоколов TCP/IP (один для связи с пользователями, а другой для связи с другими серверами кластера) можно присвоить им имена TCP/IP-Users и TCP/IP-Cluster.

Настройка именованных сетей

Система Notes обеспечивает автоматическое присвоение имен сетям Domino в соответствии с именами разрешенных портов, указанных во время конфигурирования первого сервера. При этом настоятельно рекомендуется впоследствии переименовывать эти сети.

Как уже отмечалось в главе 2, при сохранении для сетей имен по умолчанию пользователи рискуют столкнуться с целым рядом проблем, особенно в ситуации, когда потребуется добавить дополнительные серверы в домен Domino.

Так, когда два сервера применяют порты протоколов TCP/IP, но связаны друг с другом лишь через модемы, сохранение имен по умолчанию способно замедлить процесс передачи почтовых сообщений, причем не только между этими двумя серверами, но и между другими серверами домена. Если сервер *A* и сервер *B* имеют одинаковые сетевые имена, они могут предположить, что между ними в сети сформировано постоянное соединение (с помощью соответствующих одноименных портов). В результате они будут пытаться передать почтовые сообщения по несуществующему соединению и только после многих неудавшихся попыток перейдут к работе с модемом.

Другие серверы также будут полагать, что между серверами *A* и *B* присутствует постоянное сетевое соединение. Кроме того, они могут считать, что маршрут через серверы *A* и *B* имеет наименьшую функциональную «стоимость» и станут направлять почтовые сообщения именно по этому маршруту, что приведет к весьма печальным последствиям.

Если в домене нет серверов, подключаемых к другим серверам по модемному соединению, такая проблема не обязательно возникнет. Однако в том случае, если существует хотя бы небольшая вероятность установления модемной связи в будущем, необходимо предвидеть результаты подобного подхода и своевременно переименовывать все сети Domino. На практике эта процедура достаточно проста и предусматривает выполнение следующих действий:

1. Откройте документ сервера для используемого сервера в режиме **Edit Mode**. Настройка других серверов также осуществляется с помощью документов сервера.
2. Перейдите на вкладку **Ports** (Порты).
3. Перейдите на вкладку **Notes Network Ports** (Сетевые порты системы Notes).
4. Для каждого порта измените имя сети Domino в столбце Notes **Network** (Сеть системы Notes). Если пользователь последовал рекомендациям, приведенным в главе 2, и заблаговременно разработал схему присвоения имен (еще на этапе установки первого сервера), то уже известны имена, которые надо назначить именованным сетям. Если же упомянутые рекомендации выполнены не были, дайте сетям имена location protocol, где location соответствует названию города/офиса/локальной сети, где будет размещен сервер, а protocol отвечает имени установленного протокола. Например, сервер Osprey в городе Марш Крик (Marsh Creek), работающий с протоколами TCP/IP, получит имя Marsh Creek TCP. Имейте в виду, что в имени сети Domino вполне допускается вводить пробелы.

Создание административных групп

На более поздних этапах пользователю придется отредактировать для вновь создаваемого сервера несколько *списков доступа* в документе сервера. Эти списки доступа (списки управления доступом, ACL) будут включать в себя в основном имена различных групп. Задача по редактированию подобных списков заметно облегчится (и риск появления ошибок уменьшится), если пользователь заранее создаст группы, которые в дальнейшем будут добавляться к уже существующим.

Как и для других именованных объектов системы Notes, в данном случае требуется заблаговременно разработать схему присвоения имен (еще на этапе установки первого сервера) и тем самым упростить назначение имен группам. Однако среди тех групп, которые понадобятся в дальнейшем, по крайней мере две следует создать уже на данном этапе.

Во-первых, речь идет о группе, содержащей имена всех администраторов сервера Domino, - ее можно назвать **Administrator**, **Admins**, **DominoAdmins** или **GlobalAdmins**. Если был выбран вариант **Set Access Control List Entry** (Установка элемента в списке управления доступом) на одном из последних этапов процедуры конфигурирования первого сервера (эта процедура подробно описана в начале данной главы), то сервер Domino уже создаст подобную группу. В ней будет присутствовать имя первого пользователя, а сама группа окажется добавленной с правом **Manager** в списке ACL всех существующих баз данных.

Во-вторых, речь идет о группе «запрещенного доступа», которая включает в себя имена (сотрудников, групп и серверов), принадлежащие нежелательным посетителям соответствующего домена Domino. На данном этапе имена в группе отсутствуют, однако со временем она будет заполняться (например, по мере ухода сотрудников из компании). Для этой группы может быть выбрано имя **Terminated** (Прекратившие деятельность пользователи), **Inactive Users** (Неактивные пользователи), **Outlaws** (Несанкционированные пользователи) или любое другое.

Необходимо заблаговременного сформировать по крайней мере эти две (а иногда и другие) группы. Группа создается при выполнении следующих операций:

1. Откройте вид **Groups** (Группы) в каталоге Domain Directory. В программе Domino Administrator этот вид доступен на странице **People and Groups** (Сотрудники и группы). При этом пользователь обнаружит две уже созданные группы - **LocalDomainServers** (Локальные серверы домена Domino) и **OtherDomainServer** (Серверы других доменов Domino).
2. Сформируйте новый документ группы (Group document). В программе Domino Administrator для этого достаточно щелкнуть по кнопке **New Group** (Добавление группы), расположенной на панели над видом **Groups**.
3. Заполните следующие поля:
 - **Group name** (Имя группы). В этом поле вводится имя, с помощью которого в дальнейшем группа будет идентифицироваться во всех списках. В имени группы допускаются пробелы, а для лучшего восприятия следует задавать его в определенном регистре. Имя должно быть коротким, но хорошо описывающим группу;
 - **Group type** (Тип группы). Для групп администраторов подходящим является один из двух вариантов - **Multipurpose** (Многоцелевой) или **Access Control List only** (Только для списков управления доступом). Для группы неактивных пользователей (Inactive Users) может быть выбран вариант **Deny List only** (Только список запрещения доступа). Обычно не стоит делать группу многоцелевой, если только заранее не известно, что имя группы будет присутствовать одновременно в списках доступа и в списках почтовой службы. Надо помнить о том, что программа Domino формирует индекс для каждой возможной функции группы. Поэтому ей придется сильно «постараться» для поддержки многоцелевой группы, затратив гораздо больше времени, чем в случае обычной целевой группы. Таким образом, одним из путей повышения эффективности системы является формирование для всех серверов только целевых групп;
 - **Category** (Категория). Раскрывающийся список в этом поле позволяет указать, добавить или изменить ключевое слово для поиска данной группы в каталоге;
 - **Descriptions** (Описания). Рекомендуются всегда вводить для группы соответствующее описание - это окажет неоценимую помощь по прошествии нескольких лет с момента создания группы (как самому пользователю, так и его преемнику).

В будущем, несомненно, появится множество различных групп, о назначении которых вы забудете. Наличие описаний поможет быстро решить проблему;

- **Members** (Члены группы). Для добавления новых членов группы укажите их имена (остерегайтесь опечаток) или, что лучше, щелкните по вспомогательной кнопке рядом с этим полем и введите имя в диалоговом окне **Names** (Имена). Членами группы могут быть сотрудники, пользователи, серверы и другие группы, причем разрешается пять уровней вложения групп друг в друга для маршрутизации почтовых сообщений и шесть уровней для выполнения других функций. Однако это теоретические ограничения; рекомендуется вообще не прибегать к вложенным группам;
- **Owners** (Владельцы). Клиент Notes по умолчанию указывает в этом поле имя пользователя, выполняющего установку сервера. В будущем можно отредактировать данный документ, дополнить или изменить имя группы;
- **Administrators** (Администраторы). Клиент Notes по умолчанию задает здесь имя пользователя, выполняющего установку сервера. В будущем можно отредактировать данный документ, дополнить или изменить имя группы;
- **Foreign directory sync allowed** (Разрешение на синхронизацию с внешним каталогом) по умолчанию имеет значение **Yes** (Да), что позволяет серверу Domino направлять данные о группы во внешние каталоги.

4. После заполнения полей следует сохранить и закрыть созданный документ.

Теперь группа **Administrators** (Администраторы) появится на виде **Groups** (Группы), где не будет группы **Inactive Users** (Неактивные пользователи), поскольку она относится к категории **Deny Access** (Запрет доступа). Подобные группы отображаются только на виде **Deny Access** (Запрет доступа), который открывается через вид **Deny Access Groups** (Группы запрещенного доступа) каталога Domain Directory, так что увидеть его смогут лишь администраторы. Для открытия этого вида в программе Domino Administrator перейдите на вкладку **People and Groups** (Сотрудники и группы) или **Configuration** (Конфигурация) и выберите **Server => Deny Access Groups** (Сервер => Группы запрещенного доступа) в меню **View** (Вид).

Настройка службы Administration Process

Administration Process (Процесс администрирования) - это серверная служба, автоматизирующая задачи, которые сложно или долго выполнять вручную. Использование данной службы в общем случае необязательно, однако преимущества от ее применения настолько очевидны, что нет никаких причин от нее отказываться. Установка службы для сервера Domino R5 и R6 производится автоматически, за исключением нескольких действий, которые придется выполнить самостоятельно.

Для эффективной работы службы Administration Process нужно соблюдать следующие условия:

- О задача администрирования сервера adminp должна выполняться на всех серверах домена Domino;
- О на всех серверах домена Domino требуется присутствие правильной реплики базы данных Administration Requests (Административные запросы, файл admin4.nsf);

- О для каталога Domain Directory надо назначить сервер администрирования Administration Server;
- О сервер Administration Server нужен и для других баз данных;
- О наличие базы данных Certification Log (Регистрация параметров сертификации, файл certlog.nsf) необходимо на каждом сервере, который планируется в качестве регистрирующего для сертификатов, пользователей и серверов.

Выполнение первых трех требований в приведенном выше списке обеспечивает нормальное функционирование службы Administration Process, причем программа Domino осуществляет это автоматически. Последние два требования необязательны, поэтому пользователь сам принимает решение и производит соответствующие действия вручную.

Назначение административных серверов

В число различных функций службы Administration Process (Процесс администрирования) входит обновление баз данных. При переименовании сотрудника или исключении его из системы служба Administration Process может модифицировать списки ACL баз данных, а также информацию в полях **Readers** (Читатели) и **Authors** (Авторы). Однако такие действия будут выполнены только в том случае, если сервер Administration Server назначен для обновления каждой базы данных. Поэтому в интересах пользователя своевременно гарантировать назначение службы для нормальной эксплуатации сервера.

Служба Administration Process реализуется следующим образом:

1. Пользователь или процесс формирует запрос в базу данных Administration Requests (Административные запросы) определенного сервера. Следует отметить, что на практике пользователи никогда не создают документы в этой базе. Напротив, они выбирают пункт меню **Actions** (Операции), обычно в каталоге Domain Directory, а в результате система генерирует нужный запрос.
2. За счет репликации запрос появляется в репликах базы данных Administration Requests, хранящихся на всех серверах домена Domino. В зависимости от содержимого документа конфигурации этот запрос может также передаваться в другие домены.
3. Серверы постоянно отслеживают изменение информации в базе данных Administration Requests. При появлении запроса определенный сервер, который отвечает за этот запрос (поскольку выполняет функцию административного для заданной базы данных или группы баз данных), приступает к его обработке (например, переименовывает пользователя в списке ACL базы данных).
4. В процессе обработки запроса (успешной или неуспешной) сервер модифицирует информацию в базе данных Administration Requests. В ответ на исходный документ запроса создается документ, в котором сообщается об успешности обновления или дается описание проблем, приведших к неудовлетворительному результату. В случае успешного формирования документа сервер может обработать и другие запросы (в контексте всей процедуры), например запросы на переименование пользователей.
5. Процесс репликации баз данных предусматривает индивидуальный вклад всех серверов в общую процедуру и передачу на каждый сервер обновленной копии базы данных Administration Requests. Со временем в рамках домена выполняются все необходимые действия для передачи запроса. После успешного завершения последнего шага система удалит из базы данных все промежуточные документы.

Назначить сервер Administration Server (Административный сервер) для базы данных можно в списке ACL соответствующей базы данных или на странице **Files** (Файлы) программы Domino Administrator. Если нужно назначить сервер администрирования только одной базе данных (например, нового сервера, добавляемого в систему), рекомендуется воспользоваться списком ACL. Когда сервер требуется нескольким базам данных (скажем, при создании нового домена), целесообразнее применить программу Domino Administrator (как в нашем случае).

Для назначения сервера Administration Server одной базе данных (с помощью списка ACL) выполните следующие действия:

1. Обратитесь к списку ACL требуемой базы данных.
2. Выберите **Advanced** (Дополнительно).
3. Ниже пункта **Administration Server** укажите **Server** (Сервер), после чего введите полное имя сервера (скажем, Osprey/Servers/Stillwater, а не просто Osprey) или выберите его в списке серверов. Щелкните по кнопке OK.

Чтобы назначить административный сервер нескольким базам данных (в программе Domino Administrator):

1. Выберите сервер, на котором хранится требуемая база (или базы) данных.
2. Перейдите на страницу **Files** (Файлы) и в списке баз данных укажите одну или несколько баз (для выделения нескольких баз в списке держите нажатой клавишу **Ctrl**), для которых нужно выполнить данные операции. Следует выделять только те базы, в которые планируется занести одинаковые данные.
3. Выберите команду **Database => Manage ACL** (База данных => Управление списком ACL) на панели **Tools** (Программные инструменты) или в меню **Files** (Файлы).
4. В диалоговом окне **ACL Management** (Управление ACL) укажите **Advanced**.
5. На панели **Advanced** (Дополнительно) выберите вариант **Modify Administration Server** (Модификация параметров административного сервера), после чего выделите пункт **Server** (Сервер) и введите полное имя сервера или укажите это имя в соответствующем списке.
6. Задайте в поле **Modify** (Модификация) значение **Reader** (Читатель) или **Author** (Автор) в том случае, если требуется модифицировать эти поля с помощью службы Administration Process. Обычно ставится именно такая задача, хотя в некоторых случаях приходится решать и более сложные. Установка такого варианта предусматривает проверку службой Administration Process всех документов в базе данных. Для больших баз данных подобный процесс может занять весьма продолжительное время. Поэтому пользователь далеко не всегда захочет задать описанный вариант, особенно если заранее известно, что в базе данных не применяются поля **Reader** и **Author** или когда содержимое этих полей остается практически неизменным.
7. Щелкните по кнопке OK.

На практике возникает законный вопрос о назначении наиболее удобного для взаимодействия с базой данных административного сервера. В общем случае выбор сервера не является делом принципиальным, поскольку все серверы R4, R5 и R6 способны выполнять такую функцию. Однако некоторые администраторы стараются разместить службу Administration Process на одном сервере, в частности на сервере концентратора,

и назначают только один административный сервер для очень большого числа баз данных (пока это еще возможно). Конечно, некоторые базы данных могут находиться на других серверах. Например, базы данных почтовой службы пользователей обычно хранятся только на серверах почтовой службы. Для них лучше определить в качестве административного тот сервер, на котором размещается база данных.

Остается, правда, еще вопрос о базах данных, хранящихся на рабочих станциях пользователей. Примером таких баз данных являются Personal Address Book (Персональная адресная книга) и Headlines (Заголовки). В этом случае пользователи могут вводить свои имена в поле **Server** (Сервер) панели Advanced (Дополнительно) соответствующего списка ACL таких баз данных. (Например, в этом случае можно было бы ввести имя Rob Kirkland/MarshCreek/Stillwater.) При изменении имени пользователя система Notes будет модифицировать информацию в подобных базах.

Создание базы данных Certification Log

Certification Log (Журнал сертификации) представляет собой базу данных, в которой серверы Domino размещают информацию о сертификации. Каждый раз при регистрации идентификационных данных сертификатора, сервера или пользователя соответствующие записи заносятся в эту базу. В ней также хранятся записи обо всех изменениях сертификатов и переименованиях.

Такая база данных может находиться на любом регистрирующем сервере или сервере, предназначенном для запроса новых имен. Можно поддерживать нереплицируемые копии базы данных на всех серверах, если независимо создавать такие копии на каждом из них. Однако лучше поддерживать на любом сервере реплицируемую копию (реплику) базы данных, которая будет содержать записи обо всех сертификациях домена. При поиске данных о сертификации уже не придется просматривать несколько нереплицируемых копий базы данных Certification Log. Для репликации одной базы Certification Log на группу серверов достаточно сформировать базу данных на одном сервере, а затем реплицировать ее на другие.

Для создания базы данных Certification Log необходимо выполнить три операции:

1. В меню **Files** (Файлы) выберите **Database => New** (База данных => Новая).
- 2г-В диалоговом окне **New Database** (Новая база данных) измените значения в полях:
 - **Server** (Сервер) - укажите (или выберите в списке) полное имя сервера, в котором планируется создать базу данных. В рассматриваемом примере введите имя Osprey/Stillwater или Osprey/Servers/Stillwater;
 - **Title** (Заглавие) - задайте Certification Log (Журнал сертификации-).
 - **File Name** (Имя файла) - имя файла certlog.nsf, которое и будет употребляться в дальнейшем;
 - **Template Server** (Шаблон сервера). Шаблон Certification Log (файл certlog.ntf) обычно хранится на серверах, поэтому, если не предусматривается применение программы Domino Administrator или клиента Notes для совместной работы с каталогом данных сервера, замените в данном поле значение **Local** (Локальный) на имя сервера. Для этого щелкните по кнопке **Template Server** (Шаблон сервера), введите или выберите имя сервера и щелкните по кнопке ОК. Изменится список шаблонов баз данных, и в нем отобразятся шаблоны данного сервера. Прокрутите новый список вниз и выделите в нем пункт **Certification Log** (Журнал сертификации).

3. Содержимое остальных полей может оставаться неизменным. По окончании работы щелкните по кнопке ОК. Если пользователь обладает правом создавать новые базы данных на соответствующем сервере (это следует разрешить на ранних стадиях процедуры конфигурирования), сервер Domino построит новую базу данных Certification Log. В противном случае на экране появится сообщение об ошибке.

Поскольку к этому моменту другие серверы еще не сформированы, вопрос репликации базы данных будет подробно рассмотрен позже, в главе 5.

Заполнение полей с параметрами доступа к серверу

Ряд полей в документе сервера (Server document) служит для задания списков доступа. В этих полях определяется, кто может осуществлять доступ к серверу и с какими целями, причем конфигурация сервера считается сформированной не полностью до тех пор, пока эти поля остаются незаполненными. Как правило, в них заносятся имена групп и подстановочные символы. Следует иметь в виду, что сервер не обеспечивает автоматического распознавания изменений содержимого для целого ряда полей. Поэтому после модификации значений в полях необходимо остановить сервер, а затем перезапустить его - оба действия выполняются консольной командой **Restart Server** (Перезапуск сервера) - чтобы он правильно распознал произошедшие изменения. Однако если в этих полях указаны только имена групп, можно свободно добавить или удалить членов групп, а сервер распознает изменения без остановки и повторного запуска.

Допустимо также задать в полях подстановочные символы. Например, можно добавить запись вида */MarshCreek/Stillwater, что позволит любому пользователю организационной единицы MarshCreek осуществлять деятельность, разрешенную для членов группы, содержащейся в данном поле. Наличие звездочки означает всех пользователей, включенных в каталог Domain Directory.

В этих полях также могут присутствовать имена видов каталога Domain Directory. Сначала вводится звездочка, затем имя вида. На все объекты данного вида будут действовать ограничения, определенные в таком поле.

Ниже представлен перечень необходимых для заполнения полей (состав полей в документе сервера зависит от параметров настройки и может различаться на разных серверах).

Страница **Security** (Безопасность), заголовок **Administrators** (Администраторы):

- О поле **Administrators** (Администраторы). Пользователи, указываемые в этом поле, могут направлять команды на сервер из программ Domino Administrator и Remote Console (Удаленная консоль), назначать административные серверы для баз данных, уплотнять хранящиеся на сервере базы данных, создавать, модифицировать и удалять полнотекстовые индексы для сервера, а также создавать, модифицировать и удалять папки, каталоги и связи баз данных для сервера.

Страница **Security**, заголовок **Access server** (Доступ к серверу):

- О поле **Allow server access only to users listed in this Directory** (Разрешение доступа к серверу пользователям, перечисленным в данном каталоге). В этом поле по умолчанию выбран вариант No (Нет), причем в большей части случаев этот вариант оказывается вполне приемлемым. При задании значения **Yes** (Да) доступ к серверу разрешается только тем пользователям, чей персональный документ (Personal document) хранится в каталоге сервера. Одновременно запрещается доступ к этому серверу для всех других серверов. Если в поле установлено значение No, следует

добавить в поле **Access server** (Доступ к серверу) имена тех серверов, групп серверов или серверов организационной единицы (например, */Servers/Stillwater), которые в состоянии нормально взаимодействовать с данным сервером.

- О поле **Access server** (Доступ к серверу). В режиме по умолчанию это поле не заполняется, поэтому все объекты имеют возможность обращаться к данному серверу. Добавление сюда записей указывает на ограничение доступа к серверу только теми объектами, которые перечислены в поле. Чтобы не увеличивать продолжительность входа на сервер, лучше поле не заполнять, пока не возникнет потребность в поименном ограничении доступа. Вместе с какими-либо записями следует ввести в это поле также соответствующие имена групп (например, **LocalDomainServers**) и тем самым разрешить другим серверам доступ к данному серверу для репликации и маршрутизации почты;
- О поле **Not access server** (Запрет доступа к серверу). Имена, представленные в этом поле, указывают на объекты, которым не разрешается доступ к серверу, причем даже в том случае, когда они одновременно присутствуют в поле **Access server** (Доступ к серверу). Названное поле имеет более высокий приоритет, и если оно остается незаполненным, фактически все объекты вправе обращаться к серверу. На данном этапе требуется ввести в поле имя группы **Inactive Users** (Неактивные пользователи);
- О поле **Create databases and templates** (Создание базы данных и шаблона). Если в этом поле присутствуют какие-либо данные, например имена, то только объекты с названными именами будут иметь право создавать новые базы данных командой **File => Database => New** (Файл => База данных => Новая). Когда поле не заполнено, подобным правом может воспользоваться любой объект. Обычно такое право предоставляется только администраторам и разработчикам приложений, которых можно объединить в группе **Designers** (Разработчики);
- О поле **Create new replica** (Создание новой реплики). Только те объекты, имена которых перечислены в этом поле, в состоянии формировать реплики баз данных командой **File => Replication => New Replica** (Файл => Репликация => Новая реплика). Если поле остается незаполненным, право формировать реплики баз данных не предоставляется никому. На данном этапе следует добавить сюда группы **LocalDomainServers** (Серверы локального домена) и **Administrators** (Администраторы);
- О поле **Allowed to use monitors** (Разрешить использование мониторов). Только те объекты, которые указаны здесь, могут организовывать процедуры мониторинга. Пользователи выполняют мониторинг путем формирования системы индексации для баз данных, причем выделенные для этих целей базы осуществляют поиск индексированных баз данных и инициируют проведение для них соответствующих изменений. Чем больше объем подобного контроля, тем сильнее это влияет на характеристики системы в целом. В поле можно определить, кому разрешено организовывать мониторинг для данного сервера. Незаполненное поле означает, что практически все объекты (за исключением указанных в следующем поле) будут иметь право организовывать мониторинг с помощью специально выделенных баз данных;
- О поле **Not allowed to use monitors** (Запрет на использование мониторов). Объекты, имена которых содержатся здесь, не имеют возможности проводить индексацию баз данных для указанного сервера;
- О поле **Administer the server from a browser** (Администрирование сервера с помощью браузера). Только те объекты, чьи имена занесены в это поле, могут применять

приложение Domino Web Administrator (Web-администрирование сервера Domino) для администрирования сервера из Web-браузера. Когда данное поле не заполнено, ни один объект такого права не получает и администрирование сервера с помощью Web-браузера запрещается. Следует отметить, что поле остается неиспользованным в том случае, если не предусматривается обращение к серверу посредством протокола HTTP.

Страница **Security**, заголовок **Passthru Use** (Использование сквозного сервера):

- О поле **Access this server** (Доступ к данному серверу). Только объектам, имена которых указаны в этом поле, можно обращаться к данному серверу с помощью сквозного сервера, а если поле остается незаполненным, такой способ доступа к серверу запрещен;
- О поле **Route through** (Сквозной маршрут). Только объекты, чьи имена присутствуют здесь, могут использовать данный сервер в качестве сквозного при обращении к другому серверу Domino. Если поле не заполнено, делать это нельзя;
- О поле **Cause calling** (Осуществление вызова). Только объекты, чьи имена приводятся в указанном поле, могут вызывать со сквозного сервера другие серверы через модем или удаленную локальную сеть. Незаполненное поле обозначает, что такого права не предоставляется ни одному объекту;
- О поле **Destinations allowed** (Разрешение доступа к адресатам). В этом поле предлагается перечень имен серверов, доступ к которым может реализовать сервер, выполняющий функции сквозного. Когда данное поле не заполнено, доступ разрешен ко всем серверам.

Страница **Security**, заголовок **Agent Restrictions** (Ограничения на использование агентов):

- О поле **Run Personal Agents** (Запуск персональных агентов). Объекты, чьи имена указаны здесь, имеют возможность пользоваться персональными агентами на данном сервере. Если поле остается незаполненным, такие агенты могут работать со всеми объектами. При вводе любых имен соответствующие объекты (а также объекты, перечисленные в двух следующих полях) могут применять персональных агентов;
- О поле **Run restricted LotusScript/Java agents** (Запуск ограниченных агентов LotusScript/Java). Объекты, чьи имена включены в это поле, в состоянии запускать персональных агентов LotusScript и Java (последнее зависит от возможностей самих агентов). При незаполненном поле право применения подобных агентов не предоставляется никому, за исключением тех объектов, которые заданы в следующем поле. На данном этапе сюда должны быть добавлены группы **LocalDomainServers** (Серверы локального домена) и **Administrators** (Администраторы). Может также потребоваться внести в него другие группы (например, группу **OtherDomainServers** - серверы другого домена), которые перенаправляют пользователей на серверы в других доменах Domino;
- О поле **Run unrestricted LotusScript/Java agents** (Запуск неограниченных агентов LotusScript/Java). Объекты, чьи имена указаны в этом поле, получают доступ к любым агентам LotusScript и Java, в том числе и к тем, которые позволяют управлять системными часами, вводом/выводом файлов и операционной системой. Если данное поле останется незаполненным, такого права не будет ни у одного объекта. Нельзя забывать, что с помощью указанных агентов могут совершаться кражи или разрушение данных либо выполняться иные операции, нарушающие защиту системы, поэтому к работе с ними следует допускать только доверенных пользователей.

Страница **Security**, заголовок **HOP Restrictions** (Ограничения ПОР) содержит два поля. Указанные в этих полях объекты могут (через ПОР из браузера) разрешить серверу исполнение агентов LotusScript и Java, поддерживающих каркас CORBA:

- поле **Run restricted Java/JavaScript** (Запуск ограниченных агентов Java/JavaScript). Для этого поля реализуются те же правила, что и для поля ограниченных агентов LotusScript/Java (см. предыдущий раздел). Поле может быть оставлено незаполненным, тогда ни один объект не будет использовать подобные агенты;
- поле **Run unrestricted Java/JavaScript** (Запуск неограниченных агентов Java/JavaScript). Для этого поля установлены те же правила, что и для неограниченных агентов LotusScript/Java (см. предыдущий раздел). При незаполненном поле права запускать агенты не получает ни один объект. Следует помнить, что существует риск использования указанных агентов в целях кражи или разрушения данных либо выполнения иных операций, нарушающих защиту системы, поэтому допускать к работе с ними можно только доверенных пользователей.

Большая часть остальных полей в документе сервера (Server document) правильно заполняется на этапе его создания системой Notes. Тем не менее существует несколько полей, которые нужно изменить уже сейчас.

Заполнение других серверных полей

Ниже перечислены поля в документе сервера, которые не связаны с предоставлением доступа, но должны быть отредактированы в данный момент.

Страница **Basics** (Основные параметры), заголовок **Basics** содержит следующее поле:

- **Server's phone number(s)** (Телефонные номера сервера). Если сервер будет принимать входящие телефонные вызовы с помощью модема и телефонные номера известны, введите их в этом поле.

Страница **Basics**, заголовок **Server Location Information** (Данные о местоположении сервера) содержит поля, определяющие набор номера для исходящих телефонных звонков и прием входящих телефонных вызовов:

- **Prefix for outside line** (Префикс внешней линии). Если сервер будет с помощью модема набирать дополнительный префикс для выхода на внешнюю линию¹, его надо указать в данном поле;
- **International prefix** (Международный префикс, код). Здесь следует вводить префикс телефонного номера для международных вызовов. По умолчанию выбран префикс 011, который принят в США;
- **Country code at this location** (Код страны для данного места). Поле служит для ввода кода страны, на территории которой располагается сервер. Для Соединенных Штатов этот код равен 1;
- **Long distance prefix** (Междугородный префикс, код). Здесь требуется указать префикс для междугородных звонков. По умолчанию выбран код 1, применяемый на территории США;
- **Area code at this location** (Код области для данного места). Поле предназначено для ввода кода области, соответствующего местоположению сервера. Например,

Например, 9 в офисных АТС. - *Прим. ред.*

для города Марш Крик код 610. В других странах он может совпадать с кодом города, скажем для Мельбурна (Австралия) это 3;

- **Calling card access number** (Номер доступа по телефонной карточке). Если сервер будет оплачивать счета за исходящие вызовы по кредитной карточке, необходимо указать в данном поле номер телефона, который должен набрать сервер (например, для компании AT&T в США телефонный номер оплаты по кредитной карточке - 800-225-5288);
- **Calling card number** (Номер телефонной карточки). Если сервер будет оплачивать счета за исходящие вызовы по кредитной карточке, то здесь указывается номер кредитной карточки;
- **Network Dialup idle timeout** (Тайм-аут коммутируемого доступа к сети). В данном поле устанавливается количество минут, по истечении которых сервер разорвет (в отсутствие какой-либо активности в телефонной линии связи) соединение Microsoft RAS. Если поле не заполнено, сервер сделает это сразу после завершения всех запланированных действий (обычно пользователи предпочитают не заполнять его).

Страница **Basics**, заголовок **Servers** (Серверы) содержит поля, определяющие совместное использование клиентом системы Notes папки данных сервера:

- **Mail Server** (Сервер почтовой службы). Определяет почтовый сервер (если таковой существует), совместно с которым клиент системы Notes работает с папками данных;
- **Passthru server** (Сквозной сервер). Задаёт сквозной сервер по умолчанию (если он существует), с которым клиент системы Notes совместно пользуется папками данных. Если клиенту Notes требуется обратиться к другому серверу, не имеющему сформированного соединения, сервер с помощью сквозного сервера обеспечит такое подключение;
- **InterNotes server** (Сервер InterNotes). Указывает прокси-сервер для Web-просмотра, с которым клиент системы Notes совместно использует папки данных. Клиенту Notes необходим сервер InterNotes только в том случае, если для этого сервера не задан порт протоколов TCP/IP.

Страница **Security** (Безопасность), заголовок **Security Settings** (Параметры защиты) содержит следующие поля:

- **Compare Notes public keys against those stored in Directory** (Сравнение открытых ключей Notes с ключами в каталоге). По умолчанию для этого поля задается вариант **No** (Нет). Выбор варианта **Yes** (Да) приводит к тому, что сервер начинает сравнивать открытые ключи, введенные пользователем, с аналогичными ключами из персонального документа (Personal document) пользователя в каталоге Domain Directory. Если ключи не совпадают, пользователь не пройдет аутентификацию на сервере и будет блокирован. С помощью данной функции может быть блокирован доступ к серверу неавторизованных владельцев файлов идентификационных данных или пользователей, не имеющих персональных документов. Не следует также забывать о том, что при выборе варианта **Yes** заметно замедляется процедура аутентификации пользователей;
- **Allow anonymous Notes connections** (Разрешение доступа для анонимных пользователей системы Notes). Эта функция дает возможность пользователям системы Notes осуществлять доступ к серверу без аутентификации. В таком случае серверу не нужно идентифицировать пользователя по имени, так что он фактически остается

анонимным. Для разрешения анонимного доступа требуется изменить списки доступа сервера и базы данных, включив в них запись **Anonymous**. Обычно такая учетная запись присутствует только на серверах, предназначенных для общественного применения. На странице **Internet Ports** (Порты сети Internet) также имеются соответствующие поля, которые служат для разрешения или запрещения анонимного доступа для пользователей Web-приложений, каталога LDAP, новостей, ПОР и обмена входящей почтой;

- О **Check passwords on Notes IDs** (Проверка паролей по идентификационным данным системы Notes). По умолчанию проверка не производится. Разрешение проверки приводит к тому, что сервер во время аутентификации начинает сравнивать пароль, защищающий файл идентификационных данных пользователя, с паролем для файла персонального документа. Если пароли не совпадают, пользователя просят изменить пароль для обеспечения его соответствия ранее заданному. Подобный подход позволяет запретить доступ неавторизованных владельцев файлов идентификационных данных, а также заставить пользователей периодически менять свои пароли. Если необходимо воспользоваться этой функцией, надо активизировать ее в персональном документе. Не следует забывать, что функция запрещает доступ к данному серверу клиентов системы Notes версии до 4.5. Также изменяются идентификационные данные пользователей и серверов, которые имеют доступ к данному серверу, что не позволяет обратиться к серверам версий до 4.5. Для организации доступа к серверам в обоих упомянутых случаях рекомендуется поддерживать несколько независимых копий файла идентификационных данных.

Страницы **Ports** (Порты) и **Proxy** (Прокси), заголовок **Proxy Configuration** (Конфигурация прокси). Если сервер обращается к другим серверам через брандмауэр и первым из установленных серверов не является прокси-сервер, следует указать его на данных страницах документа сервера (Server document). Для этого необходимо ввести в соответствующих полях имя прокси-сервера в виде `hostname:portnumber`, где `hostname` - полностью квалифицированное доменное имя (Fully Qualified Domain Name - FQJDN), а `portnumber` - номер IP-порта, который будет отслеживаться прокси-сервером. Если активизированы один или несколько прокси-серверов, но исходному серверу нужно обходить прокси при обращении к другим локальным серверам, укажите в поле **No proxy for these hosts and domains** (Без прокси для данных хостов и доменов) имена доменов, имена хостов или IP-адреса нужных локальных серверов.

Страница **Miscellaneous** (Вспомогательные параметры), заголовок **Contact Information** (Контактная информация). Поля, находящиеся ниже этого заголовка, служат для более точной идентификации каждого сервера. Как правило, на первых стадиях идентифицирующие данные малочисленны, однако и они могут применяться эффективно. Указанные поля бывают особенно полезными в тех случаях, когда появляются новые сотрудники или когда надо спланировать настройку многочисленных серверов, разбросанных по различным местам.

Страница **Miscellaneous**, заголовок **Administration** (Администрирование) содержит следующие поля:

- О **Owner** (Владелец). В этом поле следует вводить имена пользователей или групп, которым планируется разрешить редактирование документа сервера;
- О **Administrators** (Администраторы). В данном поле необходимо указать имена пользователей или групп, которым будет предоставлено право редактирования документа сервера.

На странице **Transactional Logging** (Регистрация транзакций) также может потребоваться скорректировать данные в некоторых полях. Функция **Transactional Logging** (Регистрация транзакций) применяется в серверах Domino начиная с версии 5. Наличие этой функции позволяет заметно улучшить целостность, безопасность и управляемость данных, находящихся на сервере. Функция обеспечивает быстрый перезапуск после отказов сервера. Она также способствует сокращению времени ожидания ответов на запросы пользователей, поскольку сервер может проводить модификацию баз данных в периоды его небольшой загрузки. Упрощается процедура резервного копирования (архивирования), поскольку появляется возможность выполнять дополняющее ежедневное архивирование вместо резервного копирования всей базы данных целиком.

С другой стороны, применение функции регистрации транзакций приводит к увеличению объема работ по администрированию, и этот факт должны хорошо осознавать администраторы, которым надо быть готовыми к возрастанию нагрузки. Например, некоторые операции, проводимые без воздействия на незарегистрированную базу данных, могут потребовать незапланированного и полномасштабного резервного копирования зарегистрированной базы данных. Кроме того, не рекомендуется использовать функцию регистрации транзакций на компьютере, имеющем всего один накопитель жестких дисков или всего один контроллер жестких дисков. На практике, естественно, могут возникать и другие ситуации, когда применение этой функции оказывается нецелесообразным.

Итак, на данном этапе не рекомендуется активизировать описанную функцию, за исключением случаев, когда пользователь уже основательно ознакомился с ее особенностями и с самого начала процедуры настройки планировал ее применение (см. главы 14 и 19).

Перечень полей этой страницы:

- **Transactional logging** (Регистрация транзакций). Функция регистрации транзакций по умолчанию отключена для нового сервера. Чтобы разрешить функцию, укажите в данном поле значение **Enabled** (Разрешено);
- **Log path** (Путь к журналу). Это поле предназначено для ввода пути к папке, в которой будут храниться файлы (журнал) регистрации транзакций. Если имя папки уже задано (например, logdir), папка будет создана в папке данных data сервера Domino. Однако для повышения эффективности лучше хранить журнал регистрации транзакций на независимом специально выделенном диске. Так, если диск G: специально зарезервировать для хранения журнала транзакций, то в поле надо указать g:\logdir. Следующий неплохой вариант связан с созданием журнала транзакций на любом диске, кроме предназначенного для хранения базы данных. Скажем, операционная система, файлы программ сервера Domino и журнал транзакций могут находиться на диске C:, а базы данных соответственно на диске D;
- **Use all available space on log device** (Использование всего доступного объема памяти на устройстве регистрации транзакций). При выделении для журнала транзакций специального диска необходимо выбрать в поле значение **Yes** (Да). В других случаях следует задавать вариант **No** (Нет);
- **Maximum log space** (Максимальный размер журнала). Это поле появляется только при условии, что в предшествующем поле установлен вариант No (Нет). Здесь следует задавать максимальный объем дисковой памяти (в мегабайтах), выделяемый для регистрации транзакций на совместно используемом диске. По умолчанию предоставляется 192 Мб (минимальный объем), однако рекомендуемый минимальный

объем составляет 1 Гб. Максимально допустимый объем памяти для циклической регистрации равен 4 Гб, но не ограничен для архивной регистрации транзакций (см. ниже);

- О **Automatic fixup of corrupt database** (Автоматическая фиксация поврежденных баз данных). Эта функция активизируется по умолчанию. Если она действует, но сервер Domino не может восстановить базу данных из журнала транзакций, он автоматически запускает процедуру восстановления базы данных Fixup (Фиксация). Если функция отменена, сервер Domino уведомит администратора о необходимости запуска процедуры Fixup;
- О **Runtime/Restart performance** (Производительность исполнения/перезапуска). По умолчанию выбран вариант **Standard** (Стандартный), который является промежуточным между двумя другими вариантами (быстрое исполнение программ или быстрый повторный запуск). Когда задан режим быстрого исполнения программ, сервер Domino достаточно редко инициирует обновление баз данных. При этом в журнале транзакций накапливается много записей до обновления информации в базе данных, что приводит к увеличению времени восстановления в случае отказа сервера. Если выбирается вариант с быстрым перезапуском сервера, сервер Domino будет чаще обновлять базы, что уменьшит время восстановления при отказах сервера, но одновременно снизит производительность других его служб;
- О **Logging style** (Стиль регистрации). Допустимы значения **circular** (циклическая) и **archive** (архивная). По умолчанию задается циклическая регистрация транзакций, хотя на практике рекомендуется архивная. В циклическом режиме журнал транзакций постоянно перезаписывается, новые данные заносятся в файлы вместо старых, поэтому старые данные могут быть утеряны при отказах оборудования. При архивной регистрации запускается специальная утилита архивирования (начиная с версии R5), которая не позволяет перезаписывать транзакционные записи до их архивирования. Поскольку журнал имеет резервную копию, восстановление базы данных можно проводить даже при ошибках на носителе. На практике рекомендуется именно вариант с архивированием, когда доступна программа резервного копирования, совместимая с версиями R5 или R6. В противном случае, естественно, приходится выполнять циклическую регистрацию;
- О **Quotas** (Квоты). В версии R6 появился новый механизм выделения дополнительного дискового пространства для журналов. Он основан на квотах, заранее предусмотренных для журнала. Превысить выделенную квоту можно только при участии администратора соответствующей базы данных.

Рекомендации по выполнению дополнительных операций

В начале главы отмечалось, что если сервер принадлежит организационной единице, можно пропустить некоторые операции по конфигурированию первого сервера. Это связано с тем, что по умолчанию первый сервер и первый пользователь создаются на уровне организации (О). Были предложены три способа решения возникающих проблем:

- О заблаговременное создание идентификационных данных для первого сервера, а также организации и организационной единицы с последующим их использованием для заполнения формы **Server Configuration** (Конфигурация сервера) уже на этапе конфигурирования первого сервера;

- О переименование первого сервера и пользователя;
- О формирование временного первого сервера, а затем его удаление после создания и конфигурирования одного или большего числа последующих серверов.

Вне зависимости от того, какой способ будет применен, необходимо предусмотреть целый ряд дополнительных операций. Их описанию посвящен следующий раздел книги.

Предварительная подготовка идентификационных данных

Если уровни О и ОУ, а также идентификационные данные сервера созданы еще до начала процедуры установки первого сервера, потребуется выполнить по крайней мере две дополнительные операции. При этом следует сформировать один или несколько документов сертификата (Certificate document), а также скопировать открытый ключ сервера из его файла идентификационных данных в документ сервера (Server document). Как правило, при построении идентификационных данных сертификатора организационной единицы система Notes сама создает (наряду с идентификационными данными) документ сертификата в каталоге Domain Directory (или в Personal Address Book). Поскольку идентификационные данные подготавливаются для организации, организационной единицы сервера и самого сервера (а иногда и для других объектов), то прежде, чем начинается процедура конфигурирования первого сервера, необходимые документы сертификата создаются в другом каталоге (а не в новом каталоге, формируемом в процессе конфигурирования первого сервера).

При конфигурировании первого сервера новый документ сертификата появляется уже в новом каталоге Domain Directory для идентификационных данных сертификатора организации, если именно этот сертификатор указывался в соответствующей форме **Server Configuration**. Однако документа сертификата для организационной единицы сервера или любой другой предварительно созданной организационной единицы пока не существует. Необходимо сделать такой документ вручную, либо, если доступен каталог с уже имеющимся документом сертификата, скопировать его в новый каталог.

Операция создания документа сертификата (Certificate document) достаточно проста и требует заполнения лишь трех полей. Однако она должна выполняться опосредованно. Кроме того, предполагается копирование открытого ключа из соответствующего файла идентификационных данных. В программе Domino Administrator эта операция выполняется следующим образом:

1. Переключитесь на сервер.
2. Перейдите на вкладку **Configuration** (Конфигурация).
3. На панели **Tools** (Программные инструменты) выберите **Certification => ID Properties** (Сертификация => Свойства идентификационных данных).
4. В диалоговом окне **Choose ID File to Examine** (Выбор файла идентификационных данных для проверки) найдите файл идентификационных данных пользователя, для которого формируется документ сертификата. Выберите этот файл, а затем щелкните по кнопке **Open** (Открыть).
5. Введите пароль для файла идентификационных данных сертификатора - откроется диалоговое окно **User ID** (Идентификационные данные пользователя).
6. Задайте **More Options => Copy Public Key** (Другие операций => Копирование открытого ключа), затем щелкните по кнопке **ОК**. Копия открытого ключа пользователя (из его идентификационных данных) будет скопирована в буфер обмена.

7. На панели **Tasks** (Задачи) в левой части экрана укажите **Miscellaneous => Certificates** (Вспомогательный => Сертификаты). Появится вид **Certificates** (Сертификаты) со всеми существующими сертификатами, в перечень которых пока должен входить только сертификат организации (или организационной единицы).
8. Щелкните по кнопке **Add Certifier** (Добавление сертификатора) и заполните следующие поля:

- **Certifier name** (Имя сертификатора). Введите имя организационной единицы, для которой создается документ. В нашем примере организационная единица сервера имеет имя /Servers/Stillwater. Записывайте имя в указанном формате, то есть со слэшем (символ «косая черта») в первой позиции.
- **Issued by** (Выдан). Укажите имя создателя организационной единицы. Для /Servers/Stillwater таким именем будет /Stillwater, а для /Servers/MarshCreek/Stillwater - /MarshCreek/Stillwater. При вводе соблюдайте указанный формат, когда в первой позиции присутствует слэш;
- **Certified public key** (Утвержденный открытый ключ). Вставьте в это поле открытый ключ, который был скопирован на шаге 6.

При необходимости заполните поля на других вкладках, в частности поле, служащее для указания контактов на вкладке **Contact Information** (Контактная информация).

9. Сохраните и закройте созданный документ. Повторите эту последовательность операций для всех ранее созданных организационных единиц.

Следует отметить, что по непонятным причинам открытый ключ в документе сервера при одновременном формировании идентификационных данных сервера никогда не совпадает с ключом в этих идентификационных данных. В результате при запуске сервера появляется следующее сообщение об ошибке: **Error updating local ID file: The information in the supplied certificates from the Address Book entry is out of date** (Ошибка обновления локального файла идентификационных данных: информация в предоставленном сертификате из элемента адресной книги не соответствует текущему моменту). Для устранения возникшей проблемы следует вставить новую копию открытого ключа сервера из идентификационных данных сервера в документ сервера. При этом можно воспользоваться такой последовательностью действий:

1. В программе Domino Administrator выберите вкладку **Configuration** (Конфигурация).
2. На панели **Tools** (Программные инструменты) выберите **Certification => ID Properties** (Сертификация => Свойства идентификационных данных).
3. В диалоговом окне **ID File to Examine** (Файл идентификационных данных для проверки) найдите файл идентификационных данных сервера, выделите его и щелкните по кнопке **Open** (Открыть).
4. Если последует запрос на ввод пароля (этого может и не произойти), введите пароль сервера.
5. В диалоговом окне **User ID** (Идентификационные данные пользователя) выберите **More options => Copy public key** (Другие варианты => Копирование открытого ключа), после чего щелкните по кнопке ОК. Копия открытого ключа будет помещена в буфер обмена.
6. Вернитесь на страницу **Configuration**, укажите сервер (при необходимости), после чего выполните **Server => Current Server Document** (Сервер => Текущий документ сервера) на панели **Tasks** (Задачи). Откроется документ сервера.
7. В документе сервера выберите **Edit Server** (Редактирование сервера).

8. Откройте страницу **Administration** (Администрирование).
9. Выделите содержимое поля **Certified public key** (Утвержденный открытый ключ) и выполните **Edit => Paste** (Редактирование => Вставить). Копия открытого ключа из буфера обмена заменит копию, которая ранее присутствовала в этом поле.
10. Сохраните и закройте документ сервера.
11. Если сервер продолжает работать, перезагрузите его консольной командой **Restart server** (Перезапуск сервера), чтобы он обнаружил новую копию открытого ключа в документе сервера.

Переименование сервера и пользователя

Если в процессе установки первого сервера были автоматически сгенерированы идентификационные данные организации, сервера и пользователя, то на данном этапе следует переименовать пользователя и либо переименовать сервер, либо создать другой сервер с корректным именем, после чего удалить первый сервер. Переименование пользователя и сервера предусматривает перенос соответствующих объектов в еще не существующую организационную единицу, поэтому сначала надо сформировать организационную единицу, куда предполагается перенести объекты. С помощью программы Domino можно переименовать пользователя, причем программа сама позаботится обо всех сопутствующих нюансах. Однако в случае с сервером все тонкости придется учитывать самому.

В начале данной главы уже рассматривался процесс регистрации идентификационных данных сертификатора определенной организационной единицы. Повторим пройденное и попробуем зарегистрировать организационную единицу с помощью вкладки **Configuration** программы Domino Administrator. Выберите **Registration => Organizational Unit** (Регистрация => Организационная единица) на панели **Tools** для задания идентификационных данных сертификатора организационной единицы на родительскую организацию или организационную единицу формируемой OU. Наличие пароля является обязательным, поскольку программа Domino Administrator посредством закрытого ключа родительских идентификационных данных проверяет открытый ключ создаваемой организационной единицы.

После завершения генерирования идентификационных данных сертификатора нужной организационной единицы (в которую попадут первый сервер и пользователь) можно приступить к переименованию сервера и пользователя.

Переименование пользователя

Если не учитывать многочисленные подготовительные операции, то задача по переименованию пользователя является достаточно простой:

1. В программе Domino Administrator перейдите на страницу **People & Groups** (Сотрудники и группы).
2. Выберите вид **People** (Сотрудники) на панели **Navigator** (Навигатор), расположенной в левой части экрана.
3. Укажите конкретного сотрудника (пользователя) на виде **People** панели **View** (Вид).
4. Выполните **People => Rename** (Сотрудники => Переименование) на панели **Tools** (Программные инструменты).
5. В диалоговом окне **Certify Selected Entries** (Сертификация выбранных элементов), которое позволяет одновременно переименовывать несколько объектов, выберите **Request Move to New Certifier** (Запрос на переход к новому сертификатору).

6. В диалоговом окне **Choose Original Certifier ID** (Выбор исходных идентификационных данных сертификатора) найдите сертификатора для организации (О). В нашем примере следует указать файл stillwater.id. Выберите этот файл и щелкните по кнопке **Open**, после чего в ответ на запрос введите пароль.
7. В диалоговом окне **Request Move For Selected Entries** (Запрос на переход для заданных элементов) задайте имя организационной единицы, которая планируется для пользователя. В данном примере - /MarshCreek/Stillwater. Затем щелкните по кнопке **Submit Request** (Исполнение запроса). Программа Domino Administrator начнет обработку запроса, после чего выведет на экран дисплея полученные результаты (успешное завершение или отказ). При получении запроса от системы щелкните по кнопке ОК.
8. Перейдите на страницу **Files** (Файлы) программы Domino Administrator. Найдите базу данных Administration Requests R6.0 (Административные запросы R6.0, файл admin4.nsf) и двойным щелчком откройте ее.
9. Если появится экран **About Administration Requests** (Сведения относительно административных запросов), ознакомьтесь с представленной в нем информацией, закройте его и выведите вид **All Requests by Server** (Все запросы сервера). Далее перейдите на вид **Name Move Requests** (Запросы на перенос имен).
10. Выберите имя пользователя, а затем выполните команду **Complete Move** (Завершение переноса) из меню **Actions** (Операции).
11. Найдите новые идентификационные данные сертификатора организационной единицы в диалоговом окне **Choose Certifier ID** (Выбор идентификационных данных сертификатора). Это идентификационные данные для организационной единицы, в которую переносится пользователь. Выберите их и щелкните по кнопке **Open** (Открыть), после чего введите пароль.
12. В диалоговом окне **Complete Move For Selected Entries** (Завершение переноса для выбранных элементов) отредактируйте данные соответствующего поля (при необходимости) и щелкните по кнопке **Certify** (Сертификация). Программа Domino Administrator обработает запрос и проинформирует о результате (успешное завершение или отказ). При появлении системного запроса щелкните по кнопке ОК.

Теперь остается только немного подождать. По прошествии необходимого времени (возможно, от 24 до 48 часов) программа Domino Administrator произведет все необходимые операции по переименованию пользователя. В дальнейшем при попытке зарегистрироваться под уже существующим именем пользователя на экран будет выведено диалоговое окно с предложением о замене имени. Вам придется подтвердить факт переименования, поскольку без этой выполненной вручную процедуры продолжение процесса становится невозможным.

Процесс переименования можно несколько ускорить, проделав следующее:

1. В программе Domino Administrator перейдите на вкладку **Server** (Сервер) и выберите требуемый сервер (при необходимости), после чего отметьте **Admin Process** (Процесс администрирования) в списке задач сервера.
2. Выберите **Tasks => Tell** (Операции => Сообщение) и укажите **All requests** (Все запросы). В альтернативном случае можно выполнить команду **Console** (Консоль) и ввести необходимую команду `tell adminp process all` в командной строке в нижней части экрана.

3. Зарегистрируйтесь в качестве переименованного пользователя (если такая регистрация была осуществлена раньше, нажмите клавишу F5 для выхода из системы, а затем откройте любую базу данных сервера для повторной регистрации). Появится диалоговое окно **Name update request** (Запрос на изменение имени), в котором будет предложено подтвердить новое имя пользователя, что и следует сделать с помощью кнопки **Yes** (Да).
4. Заключительная часть процесса переименования проходит без участия пользователя. Однако в случае надобности можно повторно воспользоваться командой `tell adminp process all`, чтобы ускорить выполнение различных шагов этого процесса.

Для получения более подробной информации о переименовании пользователей обратитесь к главе 5.

Переименование сервера

Операция по переименованию сервера представляет собой существенно более сложную задачу по сравнению с переименованием пользователя. В данном случае надо выполнить следующие действия:

1. Переименовать сервер в его файле идентификационных данных посредством повторной сертификации через соответствующего сертификатора организационной единицы.
2. Изменить (вручную или с помощью соответствующего агента) имя сервера во всех полях и позициях.
3. Перезапустить сервер.

Позиции и поля, в которых требуется изменить имя сервера:

- О документы в каталоге Domain Directory и адресных книгах Personal Address Book (Книга персональных адресов) всех пользователей (см. в конце раздела перечень документов, в которых может встретиться имя сервера);
- О списки ACL баз данных (следует проверить списки ACL всех баз данных и все шаблоны проектирования данного сервера);
- О файл `notes.ini` сервера (нужно открыть этот файл в текстовом редакторе и провести поиск по общему имени сервера);
- О файл `notes.ini` каждого пользователя, для которого данный сервер применяется в качестве сервера почтовой службы (к счастью, весь перечень пользователей пока представлен одним первым пользователем, поэтому достаточно открыть один файл в текстовом редакторе и снова провести поиск по общему имени сервера);
- О документы в других базах данных. Пока существует только одна база данных, в которой может присутствовать старое имя сервера, - Statistics & Events (Статистические данные и события). В ней следует просмотреть раздел **Server Statistic Collection Profile** (Профиль сбора сервером статистических данных) на виде **Server Statistic Collection** (Сбор сервером статистических данных);
- О заголовки баз данных. По меньшей мере две базы данных содержат в заголовках полное различающееся имя сервера - Notes log (Журнал системы Notes) и Stats (Статистические данные), причем рекомендуется изменить эти заголовки с помощью соответствующих полей **Database Properties** (Свойства баз данных), выполнив команду **File => Database** (Файл => База данных), а затем команду **Properties** (Свойства).

Документы в каталоге Domain Directory и базе данных Personal Address Book пользователя, которые могут содержать ссылку на сервер:

- О документы сервера (Server document) в каталоге Domain Directory. Поля **Server name** (Имя сервера), **Mail server** (Сервер почтовой службы), **Passthru server** (Сквозной сервер) и **InterNotes server** (Сервер InterNotes), а также поля для разрешения доступа к серверу;
- О документы групп (Group document) в каталоге Domain Directory и существующей базе данных Personal Address Book. Поля **Members** (Члены группы), особенно для группы **LocalDomainServers** (Серверы локального домена Domino) для данного домена и группы **OtherDomainServers** (Серверы других доменов Domino);
- О персональные документы (Personal document) в каталоге Domain Directory, поле **Mail server**;
- О документы каталога Domain Directory, поле **Mail Server**;
- О документы базы данных входящей почты (Mail-in Database) в каталоге Domain Directory, поле **Server** (Сервер);
- О документы ресурсов (Resource document) в каталоге Domain Directory, поле **Server**;
- О документы соединений (Connection document) в каталоге Domain Directory и в существующей базе данных Personal Address Book, поля **Source server** (Исходный сервер) и **Destination server** (Сервер адресата). Эти поля могут быть созданы для других доменов;
- О документы местоположения (Location document) в каталоге Domain Directory и существующей базе данных Personal Address Book, поле **Notes mail server** (Сервер почтовой службы системы Notes);
- О документы сертификатов (Certificate document) в каталоге Domain Directory и существующей базе данных Personal Address Book, поле **Notes mail server**;
- О документы конфигурации (Configuration document) в каталоге Domain Directory. Поля **Group or Server name** (Имя группы или сервера), **Allow to track messages** (Разрешение на отслеживание сообщений) и **Allow to track subjects** (Разрешение на отслеживание объектов);
- О документы домена (Domain document) в каталоге Domain Directory других доменов (для серверов Domino и иных типов), поле **Calendar server** (Сервер поддержки календаря);
- О документы информации о сетях внешних доменов (External Domain Network Information document) в каталоге Domain Directory. Поля **Requesting server** (Запрашивающий сервер) и **Information server** (Информационный сервер). Эти поля могут быть созданы для других доменов;
- О документы программ (Program document) в каталоге Domain Directory, поле **Server to run on** (Используемый сервер);
- О документы профиля установки пользователя (User Setup Profile document) в каталоге Domain Directory (имя сервера может присутствовать во многих полях);
- О документы Web-конфигурации (Web Configuration document) в каталоге Domain Directory, поле **Applies to** (Относится к) для документов Web Realm (Web-сфера).

Именно из-за присутствия имени сервера во многих местах и документах требуется изменить его как можно быстрее. Число полей, которые придется просмотреть и изменить, неуклонно возрастает с увеличением числа применяемых организационных единиц, серверов, пользователей, баз данных и документов. Конечно, на практике допустимо воспользоваться

известными приемами для автоматизации этого процесса. Например, если временно ввести полнотекстовые индексы для каталога Domain Directory, поиск имени сервера позволит выявить перечень тех документов, которые его содержат. В других случаях результаты анализа для **Decommission Server** (Отменяемый сервер) также помогут обнаружить все документы, в которые включено имя сервера. Тем не менее процесс переименования сервера не относится к числу автоматически выполняемых, поэтому целесообразно привести соответствующие рекомендации.

Для повторной сертификации сервера (чтобы в имени сервера было указано имя нужной организационной единицы) проделайте следующее:

1. Убедитесь в наличии файла идентификационных данных сервера и файла идентификационных данных сертификатора организационной единицы, в которой планируется разместить сервер.
2. Подготовьте копию файла идентификационных данных сервера.
3. В программе Domino Administrator выберите **Certification => Certify** (Сертификация => Подтверждение) на панели **Tools** (Программные инструменты) страницы **Configuration** (Конфигурация).
4. В диалоговом окне **Choose certifier ID** (Выбор идентификационных данных сертификатора) найдите файл идентификационных данных сертификатора нужной организационной единицы (в нашем примере - файл для Servers/Stillwater). Выберите его, затем щелкните по кнопке **Open** (Открыть). Далее введите пароль сертификатора организационной единицы и после получения запроса нажмите клавишу **Enter** или щелкните по кнопке **OK**.
5. В диалоговом окне **Choose ID to Certify** (Выбор идентификационных данных для сертификации) найдите файл идентификационных данных сервера. В нашем примере это файл для Osprey/Stillwater, а его имя, скорее всего, будет иметь вид server.id. Отметьте файл и щелкните по кнопке **Open** (Открыть).
6. В диалоговом окне **Certify** (Подтверждение) выберите **Re-certify** (Повторное подтверждение).
7. В диалоговом окне **Certify ID** (Подтверждение идентификационных данных) отредактируйте несколько полей:
 - **Server** (Сервер). Если справа от кнопки **Server** присутствует запись **Local** (Локальный), щелкните по этой кнопке и введите или выберите в списке исходное имя сервера, в нашем примере - /Osprey/Stillwater. Сервер будет выполнять функции регистрирующего сервера (Registration Server), то есть на нем в процессе сертификации произойдет поиск журнала Certification Log (Журнал сертификации) и каталога Domain Directory для внесения необходимых изменений;
 - **Expiration date** (Срок завершения действия сертификата). По умолчанию срок сертификации сервера истекает через 100 лет, а действие сертификата пользователя заканчивается через два года. Процедура повторной сертификации сервера достаточно нетипична, так что система Notes может по ошибке предположить, что для сервера истек упомянутый двухгодичный срок. Поэтому следует изменить указанную дату и задать ее со сдвигом в 100 лет.
8. Все прочие поля должны оставаться без изменений. Щелкните по кнопке **Certify** (Подтверждение).

Система Notes повторно сертифицирует идентификационные данные сервера, обновит журнал Certification Log, изменит имя сервера в документе сервера и добавит новое имя

сервера в группу **LocalDomainServers** (Серверы локального домена Domino). При этом система не будет удалять старое имя сервера из указанной группы или изменять его в полях прочих документов, даже в поле **Mail server** (Сервер почтовой службы) документа сервера.

Одноразовый сервер

При использовании так называемого одноразового сервера удастся избежать поиска и редактирования вручную имени переименованного сервера. Однако вместо этого приходится искать и удалять имя первого сервера. Кроме того, надо вводить данные для нового административного сервера (для каталога Domain Directory), поэтому объем работы в целом оказывается не намного меньшим, чем в предыдущем случае.

Один из приемов, который может оказаться весьма полезным при применении такого способа, связан с использованием результатов анализа Decommission Server Analysis (Анализ для отменяемого сервера), позволяющих подготовить перечень операций, которые необходимо выполнить для успешного удаления первого сервера. Чтобы эффективно реализовать эту возможность, выполните следующие действия:

1. Убедитесь в том, что отменяемый сервер и тот сервер, которым его планируется заменить, готовы к действию и доступны с рабочей станции.
2. На странице **Server/Analysis** (Сервер/анализ) программы Domino Administrator выберите **Analyse => Decommission Server** (Анализ => Отменяемый сервер) на панели **Tools** (Программные инструменты) или пункт **Decommission Server Analysis** (Анализ для отменяемого сервера) в меню **Actions** (Операции). Появится диалоговое окно **Decommission Server Analysis** (Анализ для отменяемого сервера).
3. В поле **Source server** (Исходный сервер) следует ввести полное отличительное имя (можно выбирать его из соответствующего списка) отменяемого сервера. В поле **Target server** (Целевой сервер) укажите (или отметьте в списке) имя того сервера, который будет выполнять в дальнейшем функции первого сервера.
4. Щелкните по кнопке ОК, после чего программа Domino Administrator сравнит параметры двух серверов и передаст результаты в базу данных Decommission Server Analysis (Анализ для отменяемого сервера), хранящуюся на используемой рабочей станции.

После завершения анализа информация из этой базы данных начнет выводиться на экран дисплея. Она будет состоять из набора документов, касающихся тех функций, которые новый сервер должен выполнять вместо отменяемого. Функции, при выполнении которых новый сервер не в состоянии на текущий момент заменить отменяемый сервер, будут помечаться красным символом «X», а причина возникновения каждой такой проблемы будет поясняться в сопутствующем *маркируемом документе* (рис. 3.10). Конечная цель в данном случае заключается в устранении всех указанных проблем (и соответственно красных символов «X»). Только после этого можно спокойно выключить первый сервер.

Прочие рекомендации

Существует много других рекомендаций, как завершить процедуру конфигурирования первого сервера. Большая часть из них зависит от того набора служб, который планируется установить на сервере, и более подробно будет обсуждаться в последующих главах. Тем не менее несколько советов остаются справедливыми при любой конфигурации сервера.

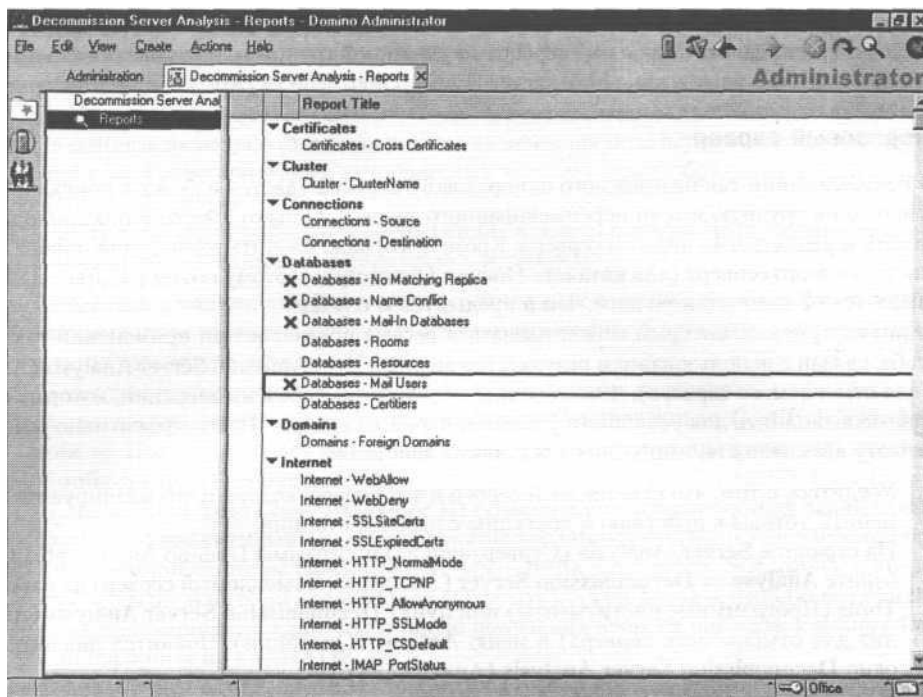


Рис. 3.10. Данные о несоответствии между двумя серверами маркируются с помощью красного символа «X»

Это необходимо обеспечить:

- О автоматический запуск сервера;
- О установку дополнительных ярлыков;
- О защиту папки данных на уровне операционной системы.

Автоматический запуск сервера

Обычно запускать сервер Domino желательно автоматически, то есть во время загрузки компьютера. Однако вплоть до данного момента такая возможность отсутствовала. Для большей части поддерживаемых платформ следует добавить специальную командную строку в пакетный файл запуска или сценарий. В операционной системе Windows NT необходимо установить сервер Domino в качестве службы NT, после чего настроить эту службу таким образом, чтобы ее запуск выполнялся автоматически. Подобный подход имеет два преимущества. Во-первых, сервер Domino будет запущен одновременно с компьютером. Во-вторых, он окажется полностью независимым от сеансов связи пользователей.

Например, в Windows NT можно войти в систему по учетной записи пользователя NT, а затем выйти из системы без остановки сервера Domino. В этом случае удастся «увидеть» сервер Domino и начать взаимодействовать с ним после входа в операционную систему,

а также остановить его и (при необходимости) перезапустить. Пользователь не обязан оставаться в системе для продолжения работы самого сервера, как это пришлось бы делать, если бы сервер не запускался в виде службы NT.

Во время установки сервера в операционной системе Windows NT Мастер InstallShield Wizard будет устанавливать сервер Domino как службу NT только при условии, что это указано в предварительно выбранном режиме **Custom Install** (Пользовательская установка). Если задается только тип сервера, Мастер не установит его в качестве службы NT. В такой ситуации придется снова обращаться к Мастеру InstallShield Wizard и на соответствующем шаге процедуры установки выбирать **Customize** (Настройка) или **Custom Install** (Пользовательская установка). После этого можно сбросить все параметры установки за исключением задания сервера Domino в виде службы NT Service. Следует отметить, что Мастеру требуется всего несколько секунд для выполнения подобных преобразований.

Несложно проверить, был ли сервер Domino установлен в виде службы NT. Откройте панель управления операционной системы Windows NT и выберите **Services** (Службы). В диалоговом окне **Services** (Службы) найдите запись **Lotus Domino Server** (Сервер Lotus Domino) в упорядоченном по алфавиту списке служб. Если эта запись отсутствует, обратитесь к Мастеру InstallShield повторно (как описано выше).

Если подобная запись имеется, можно выяснить, был ли инициализирован запуск сервера и в каком режиме это выполняется: **Automatic** (Автоматический), **Manual** (Ручной) или **Disabled** (Отмена). В данном случае должен быть указан режим **Automatic**, что позволяет запускать сервер Domino одновременно с компьютером. Если применялся другой тип запуска, следует изменить его. Для этого щелкните по кнопке **Startup** (Запуск) - появится диалоговое окно **Service** (Служба), в котором нужно указать режим **Automatic**, после чего щелкнуть по кнопке OK (рис. 3.11).

Допустимо также вручную запускать и останавливать сервер Domino в диалоговом окне **Services** (Службы). Для этого выберите **Start** (Запуск), чтобы запустить сервер, или **Stop** (Останов), чтобы его остановить. Остановка возможна только для сервера Domino, работающего как служба NT. Сервер Domino разрешается останавливать и другим, традиционным, способом (вводом команды quit, q, exit или-е с серверной консоли) вне зависимости от того, установлен ли сервер Domino в качестве службы NT.

Добавление ярлыков операционной системы Windows NT

Вне зависимости от запуска сервера Domino - в виде службы NT или из меню, рано или поздно может потребоваться создать удобный способ для его запуска и остановки вручную. Например, весьма привлекательно сформировать на Рабочем столе операционной системы Windows NT ярлыки, которые позволят обойтись без обращения к меню при запуске сервера. Такой ярлык сделать несложно - достаточно скопировать его из меню. Кроме того, полезно иметь в меню или на Рабочем столе ярлыки для запуска и остановки службы Domino NT, чтобы каждый раз не открывать диалоговое окно **Services** на панели управления.

Копирование ярлыка на Рабочий стол операционной системы Windows NT

Для копирования ярлыка, служащего для запуска сервера Domino, из меню на Рабочий стол операционной системы Windows NT необходимо найти ярлык, созданный Мастером InstallShield во время установки сервера Domino, после чего скопировать его в буфер обмена, а затем вставить на Рабочий стол операционной системы.

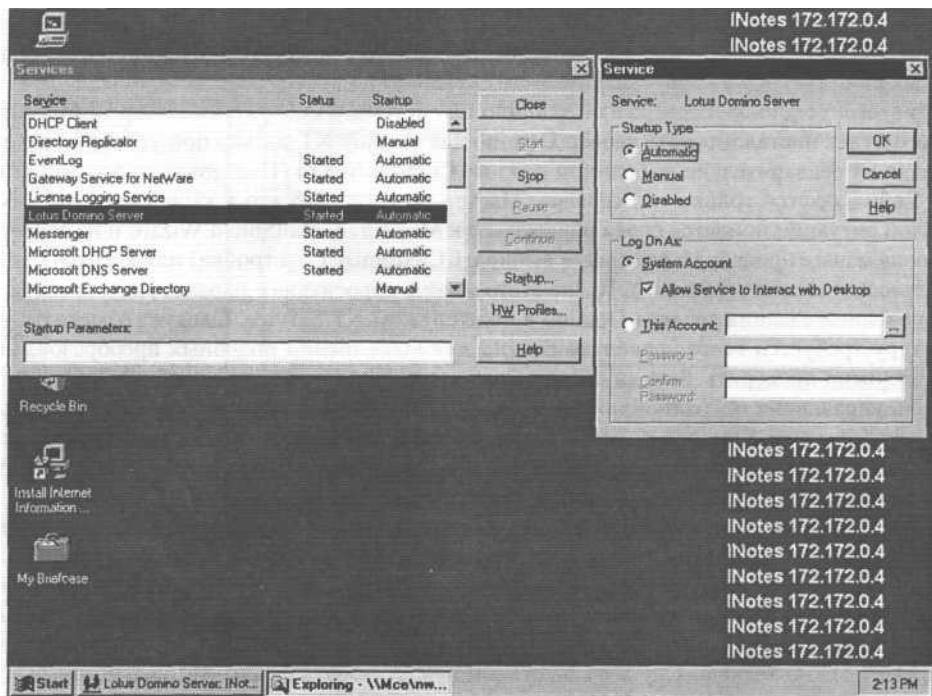


Рис. 3.11. Для выбора режима запуска сервера следует щелкнуть по кнопке *Startup* в диалоговом окне *Services* (слева), чтобы открыть диалоговое окно *Service* (справа)

Наиболее сложная часть операции состоит в поиске нужного ярлыка. Этот ярлык находится в папке, которая ранее была указана Мастеру InstallShield для его размещения. Папка в свою очередь расположена в папке Programs (Программы), которая сама обычно присутствует в папке Start Menu (Меню запуска), вложенной (в операционной системе Windows NT) в папку с именем той учетной записи, которая использовалась во время работы с Мастером InstallShield. Например, если пользователь вошел в систему по учетной записи **Administrator** (Администратор), папка Start Menu будет находиться в папке Administrator (Администратор). А уже эта папка - в папке Profiles (Профили), вложенной в папку Windows NT.

Попробуем пройти через все названные папки. В Проводнике Windows перейдите в папку Windows NT и найдите папку Profiles. В ней вы обнаружите папки для всех локальных учетных записей пользователей. Каждая из них содержит папку Start Menu и подпапку Programs. Папка сервера Domino и ярлыка, который мы ищем, помещается в одной из папок Programs. Найдите нужный ярлык, скопируйте его, а затем вставьте на Рабочий стол операционной системы Windows NT.

Перенос ярлыка в профили всех пользователей

Проблема для сервера Domino состоит в том, что Мастер InstallShield создает ярлык таким образом, что он появляется в меню только того пользователя, учетная запись которого изменялась во время установки сервера Domino на данном компьютере. Это означает, что все

администраторы, желающие локально работать с сервером Domino, должны входить в операционную систему по данной учетной записи. Однако лучше позволить администраторам входить в операционную систему по собственным учетным записям: в такой ситуации можно точнее провести аудит, поскольку в случае ошибки будет известен виновник проблемы, который работал в системе в данный момент.

Если скопировать папку сервера Domino и ярлык из папки Programs той учетной записи, которая применялась во время установки сервера Мастером InstallShield, в папку Programs профиля All Users (Все пользователи), это позволит выводить папку Domino и соответствующий ярлык в нижней части меню любого пользователя, вошедшего в операционную систему (рис. 3.12).

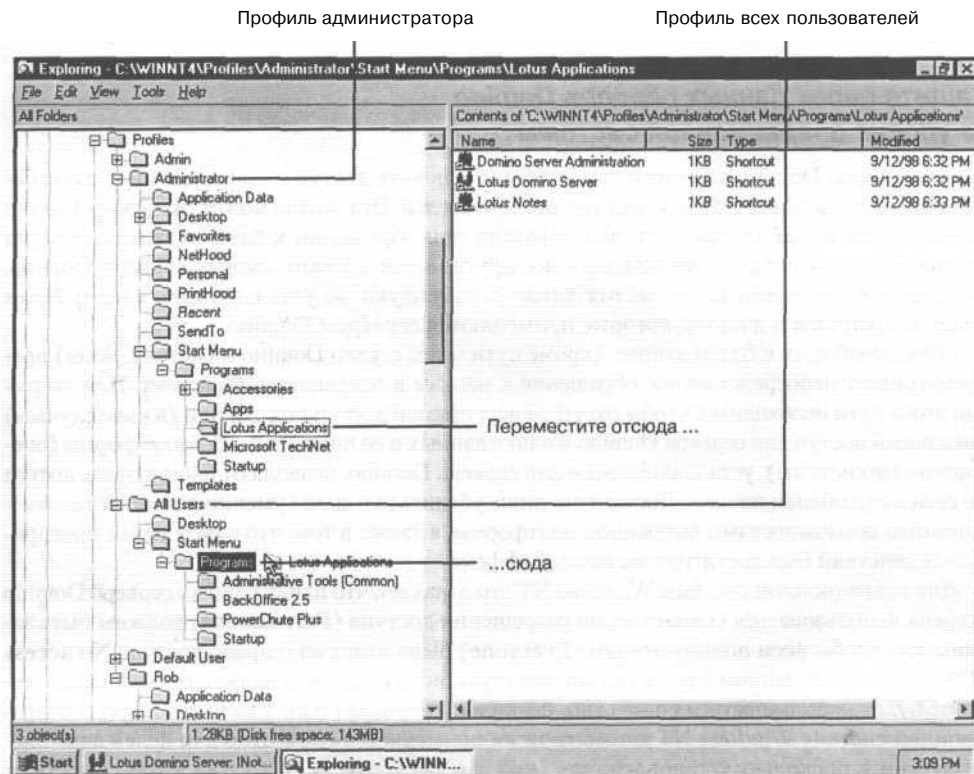


Рис. 3.12. Перенесите папку в указанное место, чтобы ярлык сервера Domino появился в меню любого пользователя

Создание ярлыков для запуска/остановки службы NT

После создания ярлыков для запуска и остановки (вручную) сервера Domino, установленного в виде службы NT, можно обойтись без обращения к диалоговому окну Services (Службы). Сделать ярлыки допустимо на Рабочем столе или в меню операционной системы Windows NT (либо в обоих местах). Для создания ярлыков на Рабочем столе щелкните по нему правой кнопкой мыши и выполните **New => Shortcut** (Создать => Ярлык). Если

требуется создать ярлык в папке (пункте) меню, выделите эту папку, затем выполните команду **New => Shortcut** в меню **File** (Файл). В обоих случаях запустится Мастер Create Shortcut (Создание ярлыка), в котором нужно указать командную строку и название для ярлыка.

Командная строка для запуска сервера Domino, являющегося службой NT, имеет следующий вид:

```
%windir%\system32\net.exe start "Lotus Domino Server"
```

а командная строка для его останова выглядит так:

```
%windir%\system32\net.exe stop "Lotus Domino Server"
```

где %windir% - стандартная переменная среды Windows NT, хранящая имя пути к папке WindowsNT.

Защита папок данных сервера Domino на уровне операционной системы

Задача сервера Domino состоит в том, чтобы обеспечить доступ к информации в своих базах данных только для авторизованных пользователей. Эта задача может быть эффективно решена лишь в том случае, если пользователи при обращении к данным проходят через сервер. Поэтому следует перекрывать все другие пути к базам данных сервера Domino. Сотрудники компании Lotus настоятельно рекомендуют не устанавливать клиент Notes в папки программ и данных, которые применяются сервером Domino.

Очевидный путь к базам данных (кроме пути через сервер Domino и систему Notes) предусматривает непосредственное обращение к папкам в операционной системе. Для закрытия этого пути необходимо, чтобы отсутствовал прямой доступ по сети или (в ряде случаев) локальный доступ для сервера Domino к папке данных и ее подпапкам. Все платформы (операционные системы), устанавливаемые для сервера Domino, позволяют блокировать доступ по сети к отдельным папкам. Достаточно лишь убедиться в своем умении пользоваться имеющимися возможностями выбранной платформы, а также в том, что в результате предпринятых действий был достигнут желаемый эффект.

Для операционной системы Windows NT это означает, что папка данных сервера Domino должна использоваться совместно, но разрешения доступа (**Permissions**) должны быть заданы так, чтобы всем пользователям (**Everyone**) было назначено право доступа **No access** (Нет доступа). В данном случае нет ничего страшного в том, что папка данных практически не будет использоваться совместно, поскольку корневая папка каждого диска в операционной системе Windows NT автоматически применяется совместно для целей администрирования, поскольку установлена как [имя_диска] \$, то есть C\$, D\$ и E\$ в зависимости от буквы диска. При этом только администраторы будут использовать корневую папку совместно, хотя можно блокировать и доступ администраторов. Такой общий ресурс нужно запретить для всех пользователей за исключением владельца ресурса, то есть в нашем случае пользователя с учетной записью **Administrator** (Администратор).

Кроме того, не следует запускать службы NSF и FTP (лучше их вообще не устанавливать) на компьютере с сервером Domino. Если такие службы должны работать, им нельзя разрешать доступ к папкам сервера Domino.

Можно (и рекомендуется) блокировать локальный доступ к папкам данных сервера Domino на уровне операционной системы, когда это позволяет файловая система установленной ОС. Так, в Windows NT разрешается блокировать локальный доступ к папкам

в разделах NTFS/H0 не к папкам дисковых разделов FAT. В OS/2 можно блокировать локальный доступ к папкам в разделах HPFS, а в UNIX подобная возможность обеспечивается для любых дисковых разделов. Поэтому в Windows NT рекомендуется размещать данные в разделах NTFS, а в OS/2 - в разделах HPFS. При работе с дисковым разделом FAT следует предусмотреть другие методы защиты данных, например за счет отключения или блокирования клавиатуры.

Необходимо также постоянно помнить о команде **Set Secure** (Установка безопасности) консоли сервера Domino, которая хотя бы частично закрывает локальный доступ к данным. Защищенный таким образом сервер отказывается воспринимать некоторые команды, например команды `tell` и `load`, и требует ввода пароля при задании других команд, в частности предлагает ввести команду в виде `quit [пароль]`.

В предыдущей главе описана процедура установки первого сервера в домене Domino. Ниже рассматриваются процедура установки других серверов и способы ее автоматизации.

Установка других серверов

Процедура инсталляции дополнительных серверов для домена Domino во многом аналогична процедуре установки первого сервера. Основным отличием в данном случае является то, что для других серверов должны формироваться лишь копии каталога Domain Directory, тогда как для первого сервера домена подобную базу данных приходится создавать с нуля. Кроме того, поскольку в домене используется несколько серверов, необходимо организовать эффективное взаимодействие между ними.

Процедура установки нового сервера для уже существующего домена состоит в следующем:

1. Зарегистрируйте новый сервер, создав в процессе регистрации документ сервера (Server document) и файл идентификационных данных сервера, содержащий открытый и закрытый ключи, а также сертификат, подписанный с помощью файла идентификационных данных сертификатора. При регистрации обеспечивается, кроме того, добавление нового сервера в группу **LocalDomainServers** (Серверы локального домена Domino).
2. Установите программное обеспечение сервера на соответствующем компьютере и выполните его конфигурирование. Наряду с решением других вопросов, создайте средства для взаимодействия этого сервера с уже существующим сервером домена и организуйте передачу с существующего сервера реплики каталога Domain Directory.
3. Проведите настройку портов и маршрутизации почтовых сообщений, чтобы обеспечить нормальное взаимодействие данного сервера с существующим.
4. Проведите установку и конфигурирование (при необходимости) других служб сервера с учетом особенностей его эксплуатации в будущем.

Регистрация идентификационных данных сервера

Перед установкой нового сервера домена следует его правильно зарегистрировать. Процедура регистрации идентификационных данных нового сервера во многом аналогична

процедуре, описанной в предыдущей главе, но имеет ряд небольших отличий, которые ниже специально отмечены:

1. На первом этапе надо получить идентификационные данные сертификатора (а также соответствующий пароль) для организации или организационной единицы, где планируется поместить новый сервер. Если следовать ранее приведенными рекомендациями, нужно использовать организационную единицу, уже созданную для сервера. Кроме того, требуется обеспечить доступ с правом **Editor** (Редактор) к журналу Certification Log (Журнал сертификации) регистрирующего сервера (который будет назначен на шаге 5).
2. В программе Domino Administrator регистрацию сервера можно осуществлять на экране **People & Groups** (Сотрудники и группы) или **Configuration** (Конфигурация) путем выбора пункта **Registration Server** (Регистрация сервера), выполнив на панели **Tools** (Программные инструменты) команду **Registration => Server** (Регистрация => Сервер), либо на экране **People & Groups**, выполнив эту команду в меню **People** (Сотрудники).
3. Если программа Domino Administrator находит последние идентификационные данные сертификатора (Certifier ID), она выводит диалоговое окно **Enter Password** (Ввод пароля) или **Enter Passwords** (Ввод паролей) для этих данных. Если программа выберет нужные идентификационные данные, можно продолжить процедуру и задать соответствующий пароль (или пароли), иначе следует щелкнуть по кнопке **Cancel** (Отмена).
4. Если же программа Domino Administrator не сможет обнаружить последние идентификационные данные сертификатора, а после щелчка по кнопке **Cancel** (Отмена) на шаге 3 появится диалоговое окно **Choose Certifier ID** (Выбор идентификационных данных сертификатора), найдите и укажите здесь те идентификационные данные, которые планируется использовать в дальнейшем. Для этого необходимо щелкнуть по кнопке **Open** (Открыть) и ввести пароль (или пароли) для идентификационных данных.
5. Откроется диалоговое окно **Register Servers** (Регистрация серверов) с четырьмя требующими заполнения полями:
 - **Registration Server** (Регистрирующий сервер). Этот сервер содержит копию каталога Domain Directory, на основе которой создается документ сервера (Server document) для вновь регистрируемого сервера. Если только не предусматривается применения программы Domino Administrator, пользующейся каталогом данных совместно с сервером, запись **Local** (Локальный) надо заменить именем самого сервера. Кроме того, сервер, имя которого задается здесь, должен быть в данный момент доступен из программы Domino Administrator. Если не удастся обеспечить выполнение двух названных условий, программа не сможет создать новый документ сервера;
 - **Certifier ID** (Идентификационные данные сертификатора). Если на предшествующем этапе были введены некорректные идентификационные данные сертификатора, теперь их можно изменить щелчком по кнопке **Certifier ID**;
 - **Security type** (Тип безопасности). Если выбранные идентификационные данные сертификатора (Certifier ID) указывают на североамериканский (North American) вариант обеспечения безопасности, в то время как для сервера необходимо предусмотреть международный вариант, рекомендуется в данном поле указать **International** (Международный). Этот вариант нужно назначить и в том случае, когда

сервер находится вне территории США и Канады. Выбор варианта **International** позволяет серверу применять более простые ключи шифрования данных. Для упрощения работы администраторы международных организаций иногда предпочитают такой вариант для всех своих серверов (находящихся как в пределах, так и вне североамериканской территории). Однако подобный подход, строго говоря, необязателен, поскольку серверы, для которых задается североамериканский вариант обеспечения безопасности, обычно имеют открытые ключи обоих типов и автоматически связываются с международными серверами и пользователями с помощью нужного ключа;

- **Certificate expiration date** (Дата завершения срока действия сертификата). По умолчанию для серверов срок действия сертификата истекает через 100 лет, что в большей части случаев вполне приемлемо.
6. Правильно заполнив указанные выше поля, откройте щелчком по кнопке **Continue** (Продолжение) диалоговое окно **Register Server** (Регистрация сервера). Оно имеет два экрана: **Basics** (Основные параметры) и **Other** (Другие параметры); на первом из них необходимо заполнить следующие поля:
- **Server Name** (Имя сервера). Здесь вводится общее имя сервера, а остальная часть полного имени наследуется из идентификационных данных соответствующего сертификатора;
 - **Password** (Пароль). Для большей части серверов данное поле может оставаться незаполненным. Пароль серверу придается только в тех случаях, когда используемый для его установки компьютер не может быть защищен должным образом на физическом уровне. Причина подобного подхода состоит в том, что сервер с защищенным паролем файлом идентификационных данных нельзя запустить вручную вплоть до ввода соответствующего пароля. Это может создавать определенные проблемы, например в случае отказа сервера ночью или в выходные дни;
 - **Password quality scale** (Шкала качества пароля). Если не планируется заполнять поле пароля, надо в данном поле задавать значение 0 (пароль необязателен);
 - **Domain** (Домен). Это поле предназначено для ввода имени домена. Когда нет полной уверенности относительно имени, его можно поискать в нескольких местах, например в заголовке каталога **Domain Directory** (в поле **Domainname** каталога), в поле **Domain** (Домен) различных документов, в том числе документов сервера (Server document) и персональных документов (Personal document), а также в переменной **Domain**, присутствующей в каждом файле **notes.ini** сервера;
 - **Administrator** (Администратор). Содержимое указанного поля обычно переносится в два поля **Administrator** документа сервера, одно из которых находится в начале, а другое - в конце документа сервера. Значение из этих полей обычно присваивается переменной **Admin** в файле **notes.ini** сервера. В данном случае нужно вводить в поле имя группы (например, имя группы администраторов сервера, что предпочтительнее) или полное различающееся имя пользователя.
7. Затем требуется щелкнуть по кнопке **Other** (Другие поля) и заполнить следующие поля:
- **Server Title** (Название сервера). В этом необязательном поле можно вводить описание сервера;
 - **Network** (Сеть). В данном поле задается имя сети **Domino**, которая устанавливается одновременно с сервером. По умолчанию здесь указано имя **Network 1**, однако на практике рекомендуется заменить это значение реальным именем сети **Domino**,

к которой данный сервер подключается через порт, использованный на начальной стадии установки для связи с существующим сервером. При сохранении в поле значения по умолчанию возможно повреждение функций маршрутизации почтовых сообщений данного сервера и других серверов домена;

- **Local Administrator** (Локальный администратор). Содержимое этого поля обычно переносится в поле **Owner** (Владелец) документа сервера для данного сервера. Поле служит для ввода имени группы или полного различающегося имени пользователя (рекомендуется указать имя группы администраторов сервера). В тех случаях, когда за администрирование сервера отвечает один администратор, можно задать его имя;
- **Store Server ID** (Хранение идентификационных данных сервера). Файл идентификационных данных, создаваемый командой **Register** (Регистрация), может сохраняться в виде вложения (In Address Book) в документ сервера, в виде файла (In File) или в обоих этих местах. При выборе варианта **In Address Book** (В книге адресов) надо ввести пароль в поле **Password** экрана **Basics**, причем даже в том случае, если в поле **Password Quality Scale** (Шкала качества пароля) указано значение 0. В дальнейшем, уже после завершения установки сервера, придется вручную удалять этот пароль. Сервер Domino требует пароля, чтобы защитить базы данных сервера от несанкционированного доступа, например от доступа к базе данных Domain Directory с правом **Reader** (Читатель), то есть доступа практически любого пользователя домена. Злоумышленник может извлечь файл идентификационных данных и позже с их помощью добраться до конфиденциальной информации. По указанной причине многие администраторы предпочитают сначала выбирать вариант **In File** (В файле), отказавшись от варианта **In Address Book**. Это позволяет избежать многих неприятностей, связанных с удалением пароля по завершении установки сервера и теми рисками, которые возникают из-за доступности защищенного паролем сервера любому пользователю в домене;
- **Set ID file** (Установка файла идентификационных данных). Если для предыдущего поля выбирается вариант **In File**, сервер Domino по умолчанию создает новый файл идентификационных данных на гибком диске, установленном в дисковом A:. Имя файла в таком случае будет servername.id (здесь servername соответствует первым восьми символам в общем имени сервера). Для изменения местоположения или имени нового файла идентификационных данных достаточно щелкнуть по кнопке его установки, а затем задать новые местоположение и имя.

После заполнения всех указанных полей можно щелкнуть по одной из следующих кнопок:

- О **Next** (Далее) - предназначена для добавления еще одного сервера или просмотра перечня других серверов (после щелчка по кнопке **Previous**);
- О **Previous** (Предшествующий) - позволяет проконтролировать и отредактировать данные для ранее зарегистрированных серверов;
- О **Delete** (Удалить) - дает возможность очистить все поля для данного сервера;
- О **Register** (Регистрация) - служит для регистрации данного и всех прочих серверов, которые настраивались в рамках текущего сеанса связи.

После щелчка по кнопке **Register** программа Domino Administrator завершит процедуру регистрации сервера, выполнив следующие действия (информируя пользователя по мере получения промежуточных результатов):

1. Подключение к регистрирующему серверу (Registration Server).
2. Создание файла идентификационных данных в памяти с генерацией пары открытого/закрытого ключей, которые заносятся в файл идентификационных данных.
3. Создание сертификата для нового сервера и запоминание его (наряду с копиями сертифицирующих файлов сертификатора и всех его преемников) в файле идентификационных данных.
4. Обновление базы данных журнала Certification Log (Журнал сертификации) для регистрирующего сервера.
5. Формирование документа сервера для вновь зарегистрированного сервера в копии каталога Domain Directory, хранящейся на регистрирующем сервере.
6. Добавление нового зарегистрированного сервера в список членов группы **LocalDomainServers** (Серверы локального домена Domain), определенной в копии каталога Domain Directory, которая находится на регистрирующем сервере.
7. В зависимости от сделанного ранее выбора в диалоговом окне **Register Servers** (Регистрация серверов) сохранение файла идентификационных данных происходит в виде вложения в документ сервера или в виде файла либо одновременно.

Процедуры установки

После регистрации нового сервера необходимо установить его на соответствующем компьютере, а затем настроить. Для первого сервера домена требовалось сначала произвести установку, а потом настройку, но для следующих серверов разрешается (при необходимости) изменить порядок операций, однако предпочтительнее начать с процедуры настройки (конфигурирования), а затем уже устанавливать серверы на компьютерах. Допустимо сперва установить серверы, а после этого их конфигурировать. Обычно рекомендуется провести на первых этапах как можно больше операций по конфигурированию, поэтому ниже процесс настройки описан с учетом подобного подхода (предварительное конфигурирование, далее установка, а на завершающем этапе окончательное конфигурирование).

Предварительное конфигурирование

Перед установкой новых серверов могут быть выполнены следующие операции конфигурирования:

- О добавление серверов в документы группы (Group document);
- О редактирование списков управления доступом в документе сервера. <

Редактируемые документы групп - это документы, созданные изначально. Программа Domino Administrator в процессе регистрации серверов автоматически добавляет новые серверы в список группы **LocalDomainServers** (Серверы локального домена Domino). При этом настоятельно рекомендуется проверять и модифицировать другие списки групп серверов, намеченных к применению в будущем.

Перечень полей, которые следует отредактировать в каждом документе сервера, приведен в главе 3 и здесь не повторяется. Если требуется осуществить конфигурирование только одного из двух новых серверов, каждый документ сервера можно редактировать в индивидуальном порядке. Однако в том случае, когда необходимо настраивать сразу несколько серверов, рекомендуется создать агент для автоматизации этого процесса.

Принцип создания агента достаточно прост, но сложность процедуры его реализации зависит от конкретной ситуации. Наиболее трудная часть работы связана с выяснением характера записей в тех полях, которые агент призван модифицировать. Например, при желании добавить в поле **Not access server** (Сервер без доступа) каждого документа сервера группу **Inactive Users** (Неактивные пользователи) следует помнить о том, что это не реальное имя поля, а только маркер, служащий для описания его назначения. Поэтому при модификации записей данного поля с помощью агента потребуются отыскать его реальное имя.

Самым простым решением такой задачи является открытие формы **Server** (Сервер) в режиме **Design** (Режим проектирования), что легко осуществить в случае права доступа к базе данных Domain Directory на уровне **Manager** (Менеджер) или **Designer** (Разработчик) и, конечно же, при наличии ранее установленной программы Domino Designer. Однако, если уровень доступа оказывается более низким, задача заметно усложняется, поскольку сервер не позволит открыть форму **Server** в режиме проектирования.

В отсутствие права доступа на уровне **Designer** к базе данных Domain Directory можно попробовать убедить администратора базы присвоить нужное вам право доступа, а если это не удастся - создать локальную копию каталога Domain Directory и затем открыть ее в режиме проектирования (в программе Domino Designer).

Локальная копия каталога Domain Directory формируется таким образом:

1. В клиенте Notes щелкните правой кнопкой по каталогу Domain Directory на вкладке **Bookmarks** (Закладки). Затем в контекстном меню выберите **Database => New Copy** (База данных => Новая копия).
2. В диалоговом окне **Copy Database** (Копирование базы данных) измените имя файла в поле **File Name** (Имя файла). Этот шаг представляется весьма важным, поскольку в данном случае нет намерения изменять записи в базе данных Personal Address Book, которая, как и база данных Domain Directory, соответствует файлу names.nsf.
3. При необходимости сбросьте флажок **Access Control List** (Список управления доступом) и щелкните по кнопке ОК.

Чтобы создать локальную реплику каталога Domain Directory, проделайте следующее:

1. В клиенте Notes щелкните правой кнопкой по каталогу Domain Directory на вкладке **Bookmarks**. Затем в контекстном меню выберите **Replication => New Replica** (Репликация => Новая реплика).
2. В диалоговом окне **New Replica** (Новая реплика) измените имя файла в поле **File Name** (Имя файла). Этот шаг также очень существенен, так как в данном случае не планируется менять записи базы данных Personal Address Book, которая, как и база данных Domain Directory, соответствует файлу names.nsf.
3. При необходимости сбросьте флажок **Access Control List** (Список управления доступом) и щелкните по кнопке ОК.

После получения права доступа к базе данных, присутствующей в шаблоне файла pubnames.ntf, на уровне **Designer** (или более высоком) появляется возможность открыть форму **Server** (Сервер) в режиме **Design** (Режим проектирования) в программе Domino Designer и ознакомиться с реальными именами тех полей, которые упоминаются в этой форме. В данном примере поле с описанием **Not access server** (Сервер без доступа) имело имя **DenyAccess** (Запрет доступа) - рис. 4.1. Рекомендуется выписывать реальные имена всех полей, для которых намечается проведение каких-либо модификаций.

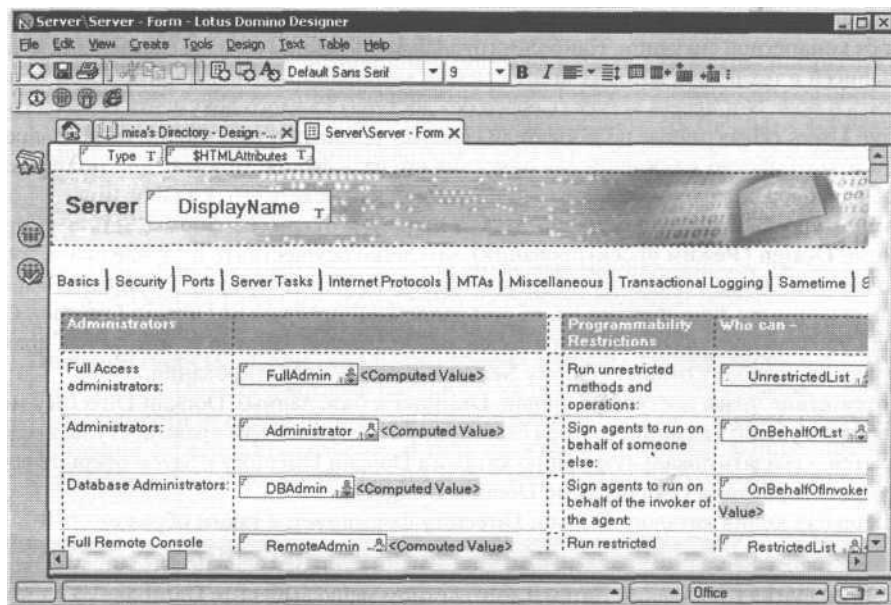


Рис. 4.1. Наиболее простой путь определения реальных имен полей на большой форме, например форме Server, предусматривает ее открытие в режиме Design

При создании агента, предназначенного для вставки записей в соответствующие поля, необходимо выполнить следующие действия:

1. Откройте базу данных, в которой планируется изменить записи. В рассматриваемом случае это каталог Domain Directory.
2. В меню **Create** (Создание) выберите **Design => Agent** (Дизайн => Агент), появится окно **Untitled Agent** (Безымянный агент) - рис. 4.2.
3. В поле **Name** (Имя) введите имя, например **Edit fields** (Редактирование полей). В дальнейшем при необходимости работать с данным агентом придется открыть меню **Actions** (Операции) и выбрать именно это имя.
4. Если доступно поле **Shared Agent** (Совместно используемый агент), что возможно только в том случае, если доступ к базе данных осуществляется на уровне **Manager** или **Designer**, его следует оставить без изменений. После установки флажка **Shared Agent** любому пользователю разрешается применять созданный агент, хотя реально никто не сможет эффективно его эксплуатировать, кроме пользователей, имеющих право записи уровня **Author** (Автор) на данный документ. В рассматриваемом случае с агентом будет работать исключительно его создатель, который не имеет намерения пользоваться им совместно с кем-либо другим.
5. В поле **When should this agent run?** (Когда запускается агент?) задайте **Manually from the Actions Menu** (Вручную из меню Операции), что соответствует варианту, выбранному по умолчанию.
6. В поле **Which document(s) should it act on?** (Документы, обрабатываемые агентом) отметьте пункт **Selected documents** (Выделенные документы), который также соответствует варианту, установленному по умолчанию.

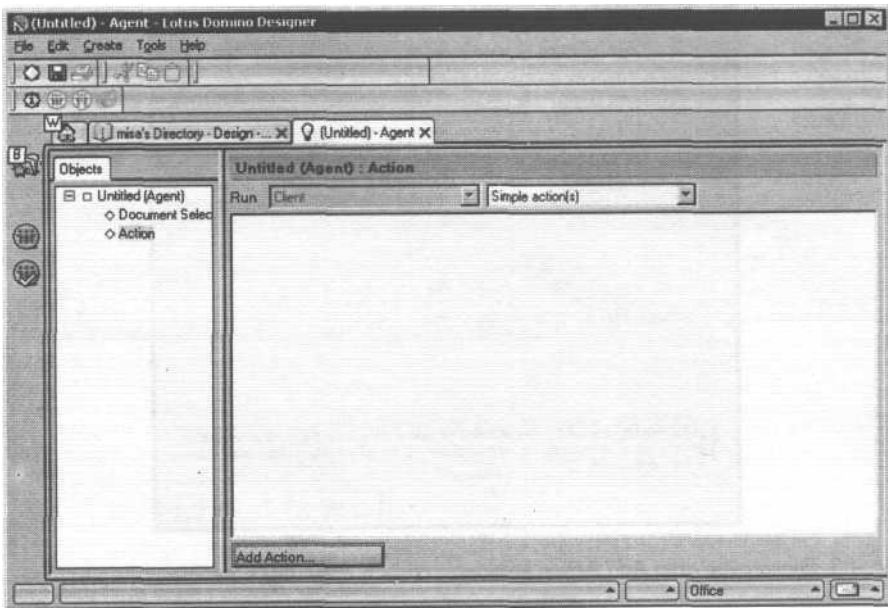


Рис. 4.2. Для создания агента можно воспользоваться значениями по умолчанию для многих полей в окне Agent

7. В поле Run (Исполнение) укажите Simple actions (Простые операции), то есть значение по умолчанию, или Formula (Формула). В рассматриваемом случае вполне достаточно остановиться на первом варианте.
8. Щелкните по кнопке Add Action (Добавление операции) - появится диалоговое окно Add Action.
9. В поле Action (Операция) выберите Modify Field (Модификация поля), что соответствует варианту, задаваемому по умолчанию.
10. В поле Field (Поле) установите имя поля, которое планируется модифицировать. В данном случае это Deny Access (Запрет доступа). Если прокрутить форму вниз, то нетрудно убедиться, что документ сервера имеет много полей. Для ускорения процесса можно нажать клавишу D и сразу перейти к первому полю, имя которого начинается с буквы «D», а затем продолжить прокрутку формы.
- И. В поле Value (Значение) введите величину параметра, которую требуется вставить в поле Deny Access (Запрет доступа). В нашем примере этим значением будет Inactive Users (Неактивные пользователи) - рис. 4.3.
12. Далее укажите Replace value (Замена значения) или Append value (Добавление значения). В рассматриваемом примере это не принципиально, поскольку пока в поле Deny Access информация отсутствует.
13. Щелчком по кнопке ОК выведите указанный для агента маркер в окне Action (Операция). Если ранее была допущена какая-либо неточность, можно дважды щелкнуть по кнопке маркера и повторно открыть диалоговое окно Add Action для исправления ошибок.

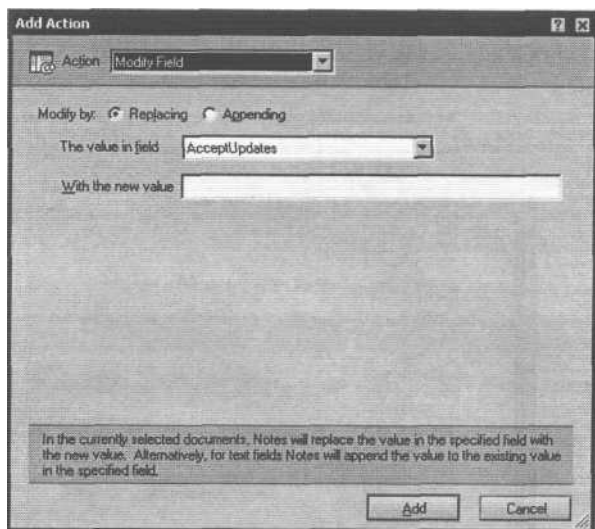


Рис. 4.3. Диалоговое окно AddAction позволяет создать агент без программирования его кода

14. Если необходимо добавить другие операции, следует вернуться к шагам 9-13. Например, нужно ввести имена **Administrators** (Администраторы), **Designers** (Разработчики) и группу **LocalDomainServers** (Серверы локального домена Domino) в поле с маркером **Create new databases** (Создание новых баз данных), причем реальным именем поля является **CreateAccess** (Задание прав доступа). Для этого в поле **Value** (Значение) на шаге 11 введите все три значения (разделить несколько значений можно с помощью запятой или точки с запятой). После закрытия диалогового окна **Add Action** в окне **Action** появится вторая (третья или четвертая) этикетка (маркер) - рис. 4.4.
15. Выполнив все упомянутые действия, закройте окно **Agent Window** (Окно агента) и щелкните по кнопке **Yes** (Да) для сохранения агента.

После этого созданный агент появится в меню **Actions** и соответствующем списке **Agents** (Агенты), что позволит работать с ним:

- О чтобы просмотреть список **Agents** надо выбрать пункт **Agents** в меню. **View** (Вид) или в программе Domino Designer отметить этот список на вкладке **Bookmarks**, которая показывает список баз данных, если щелкнуть по закладке в левой части экрана;
- О для редактирования агента достаточно дважды щелкнуть по его кнопке в списке **Agents**;
- О запустить агент можно, открыв вид **Servers** (Серверы), выбрав документ сервера или документы, которые планируется отредактировать, а затем указав агент в меню **Actions**.

Следует весьма осторожно выбирать редактируемые документы перед обращением к агенту. Если агент применяется для неправильно заданного документа, он может (в зависимости от типа параметров, указанных на шаге 12) изменить те записи документа, которые

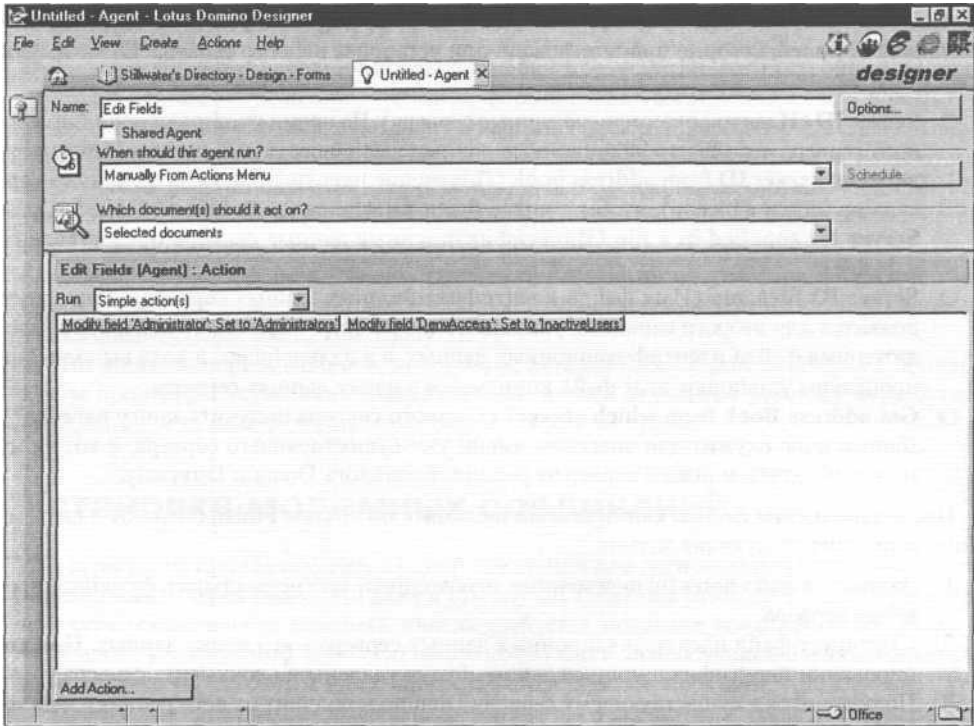


Рис. 4.4. В окне Action указаны две операции, которые будет выполнять данный агент

должны сохраняться постоянными. В этом случае придется вручную восстанавливать параметры, поскольку не существует способа отменить действия, выполненные агентом.

Установка

Процедура установки и предварительной настройки дополнительных серверов домена во многом аналогична процедуре установки и настройки первого сервера. Небольшие отличия связаны с тем, что при настройке первого сервера одновременно создавались домен и организация, а при установке дополнительных серверов формируется новый предварительно зарегистрированный сервер в уже существующих домене и организации.

В обоих случаях необходимо установить серверное программное обеспечение на компьютере, а затем уже выполнять начальное конфигурирование в программе Domino, заполнив форму **Configuration** (Конфигурация) в базе данных Domino Configuration. Этот процесс описан в главе 3, поэтому здесь он не рассматривается, за исключением тех моментов, которые касаются различий между процедурами настройки первого и последующих серверов.

Первое отличие состоит в том, что вместо выбора **First Domino Server** (Первый сервер Domino) на первом экране формы **Configuration** следует указать **Additional Domino Server** (Дополнительный сервер Domino). В результате четвертый экран будет содержать набор

полей, предназначенных для установки нового сервера уже существующего домена и отличающихся от полей, которые присутствовали при установке первого сервера. Отметим эти поля отдельно:

- О **Server ID** (Идентификационные данные сервера). Во время установки дополнительного сервера его идентификационные данные уже существуют, поэтому можно задать **Get server ID from address book** (Получение идентификационных данных сервера из книги адресов), чтобы данные были выведены из документа сервера, или **Server ID supplied in a file** (Идентификационные данные сервера предоставлены в файле);
- О **Server ID filename** (Имя файла идентификационных данных сервера). Такое поле появится для второго варианта, указанного в рассмотренном выше поле. Здесь вводится имя файла идентификационных данных, а в дальнейшем, в ходе выполнения процедуры установки, этот файл копируется в папку данных сервера;
- О **Get address Book from which server?** (С какого сервера получить книгу адресов?). Данное поле служит для внесения имени уже существующего сервера, к которому может обратиться новый сервер за репликой каталога Domain Directory.

После заполнения формы **Configuration** щелкните по кнопке **Finish** (Готово) - система Notes выполнит следующие задачи:

1. Запишет в файл notes.ini переменные, необходимые для нормального функционирования сервера.
2. Скопирует файл идентификационных данных сервера в его папку данных. При копировании идентификационные данные будут удалены из документа сервера.
3. Подключится к существующему серверу Domino и получит от него реплику каталога Domain Directory.
4. Возможно, при выборе каких-либо специальных операций на третьем экране формы **Configuration** изменит сам документ сервера, создаст другие документы в каталоге Domain Directory или сформирует иные базы данных. Разобраться в нюансах каждой конкретной операции процедуры установки сервера поможет знакомство с материалами соответствующих глав данной книги.

Другое отличие от процедуры установки первого сервера заключается в том, что иногда нужно иметь много дополнительных серверов, поэтому требуется автоматизировать процедуру их установки. Для этого необходимо заблаговременно создать *документы конфигурирования серверов*, а в дальнейшем, когда придет время их установки, лишь щелкнуть по кнопке **Finish**. Указанную операцию понадобится выполнять в обязательном порядке, поскольку форма **Configuration** находится в базе данных Domain Configuration (Конфигурация домена, файл setup.nsf), которая копируется на все серверы во время установки. Если сервер Domino создается в операционной системе Windows, форма **Configuration** будет в первый раз открываться именно в этой базе данных, поскольку в файле notes.ini присутствует переменная SetupDB= setup.nsf.

Однако для заполнения формы конфигурирования сервера вовсе не требуется ждать первого запуска сервера. Документ конфигурирования сервера допускается создавать заблаговременно в любой копии базы данных Domain Configuration. Можно скопировать базу данных на сервер (для замены копии, помещенной во время установки) еще до первого запуска сервера Domino. После запуска сервера форма **Configuration** откроется как обычно, но вместо ее заполнения будет достаточно закрыть форму, открыть созданный ранее документ конфигурирования сервера и щелкнуть по кнопке **Finish**.

Заключительное конфигурирование

Процедура конфигурирования после установки предусматривает настройку или отмену работы с портами сети и/или модемами, формирование соединений между новым и уже существующими серверами и детальную настройку различных серверных задач. Вопросы подготовки и отмены применения сетевых портов обсуждаются в главе 3, поэтому здесь в деталях не рассматриваются - просто помните о необходимости отключения всех портов, которые не предполагается использовать на сервере, а также о присвоении сетевых имен всем сетевым портам сервера. Другая рекомендация повторяется в каждой главе, однако дело того стоит: не следует оставлять присвоенные по умолчанию сетевые имена, сформированные во время автоматической установки сервера. Нужно вручную присвоить уникальные сетевые имена (см. главу 3).

Что касается портов модемов, этот вопрос детально обсуждается ниже. Все прочие аспекты процедуры установки сервера описаны либо в отдельных разделах данной главы, либо, когда речь идет о специальных задачах, в других главах.

Установка модемных соединений

Два сервера, не принадлежащие к одной локальной или региональной сети, должны взаимодействовать через модем. Но даже в том случае, когда они относятся к одной региональной сети (скажем, сети Internet), иногда требуется модемное соединение, например для резервного копирования. Это соединение может быть подключением с непосредственным набором номера, сквозным или с набором телефонного номера сети.

Прямое коммутируемое соединение формируется в тех случаях, когда два сервера располагают модемами, соединенными по телефонным линиям связи. (Вызывающий сервер может иметь непосредственный доступ к пулу модемов, а не пользоваться собственным модемом.) Каждый сервер способен просто набрать номер другого модема и установить с ним прямой контакт. На рис. 4.5 проиллюстрировано соединение с непосредственным набором номера.

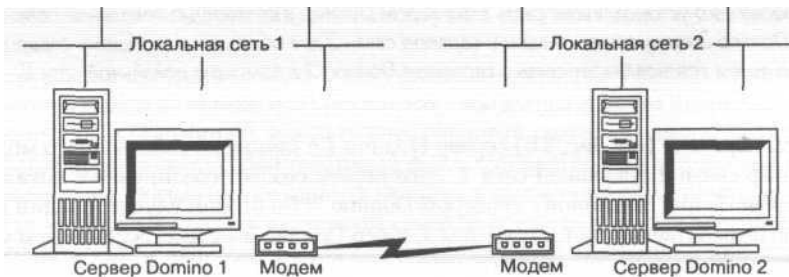


РИС. 4.5. Средство Notes Direct Dial-up позволяет двум серверам Domino взаимодействовать с помощью собственных модемов

Сквозные соединения не всегда являются модемными, но могут применяться при самых различных обстоятельствах. С помощью такого соединения один сервер Domino в состоянии воспользоваться ресурсами другого сервера Domino для получения доступа к третьему

серверу Domino. Первый сервер фактически проходит «сквозь» второй сервер для достижения третьего и ему совсем не обязательно иметь модем.

Соединения с набором телефонного номера сети формируются при условии, что один или оба сервера относятся к сети, которая содержит специальный *сервер связи*. В этом случае модемное соединение фактически устанавливается между сервером и удаленной сетью, причем сервер подключается к удаленной локальной сети. На рис. 4.6 показаны два варианта применения подобного соединения.

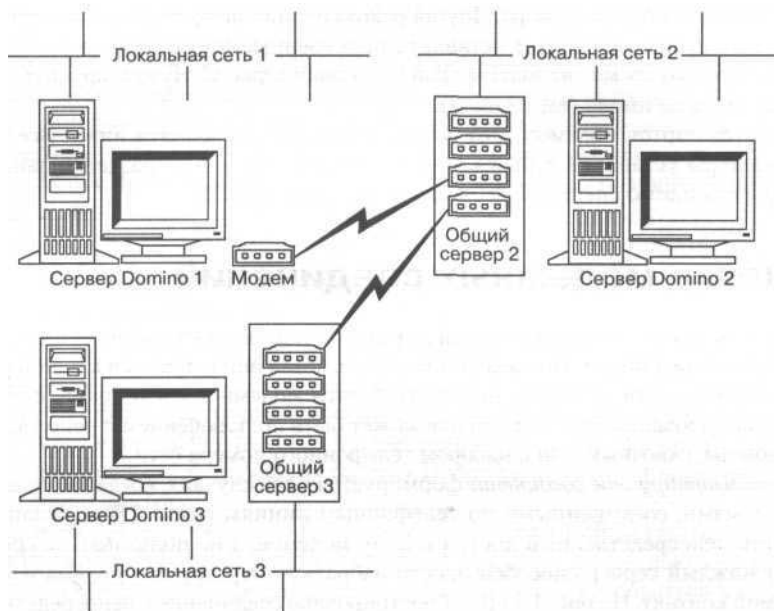


РИС. 4.6. (1) Сервер Domino 1 через свой модем обращается к общему серверу связи 2, после чего устанавливает связь с сервером Domino 2 с помощью локальной сети.

(2) Сервер Domino 3 «заимствует» модем у сервера связи 3 для обращения к общему серверу связи 2, а затем устанавливает связь с сервером Domino 2 с помощью локальной сети 2

В первом варианте (см. рис. 4.6) сервер Domino 1 с помощью собственного модема вызывает сервер связи 2 локальной сети 2. Этот сервер создает соединение с локальной сетью, непосредственно связанной с сервером Domino 2. Во втором случае ни один из серверов Domino не работает со своим модемом. Сервер Domino 3 «заимствует» модем у сервера связи 3, чтобы установить контакт с сервером связи 2. При формировании *соединений модема* с непосредственным набором номера для серверов Domino необходимо выполнить такие действия:

1. Установить модемы на формирующем и вызываемом серверах. В альтернативном варианте на вызываемом сервере должно быть программное обеспечение для разрешения доступа к пулу модемов, поддерживаемому сервером связи локальной сети.
2. Настроить порты серверов Domino для работы с модемами, что предполагает выполнение процедуры конфигурирования драйверов модемов.

3. Создать документ соединения (с непосредственным набором номера) для вызывающего сервера.

Чтобы сформировать соединения модема с набором номера сети для серверов Domino, требуется проделать следующее:

1. Установить модем на формирующем вызов сервере. В альтернативном варианте на вызывающем сервере нужно иметь программное обеспечение для разрешения доступа к пулу модемов, поддерживаемому сервером связи локальной сети.
2. Настроить порты серверов Domino для каждого применяемого модема, что предполагает выполнение процедуры конфигурирования драйверов модемов.
3. Сконфигурировать программное обеспечение Microsoft Dial-up Networking (компании Microsoft), также известное под названием службы Microsoft RAS (Remote Access Service - служба удаленного доступа), на вызывающем сервере и на компьютере вызываемого сервера локальной сети, работающего с операционной системой Windows NT. На вызывающем сервере программное обеспечение RAS должно настраиваться для коммутируемых исходящих вызовов (а не для ответа на телефонные соединения), а на отвечающем на вызов компьютере - для ответа на вызовы, а также, при необходимости, для набора номеров при исходящих телефонных вызовах.
4. Сформировать документ соединения (с набором сетевого номера) для вызывающего сервера.

Способ установки модема на компьютере зависит, в частности, от типа используемой операционной системы. Процедура установки модема в данном разделе, естественно, не описывается в деталях, поскольку это выходит за рамки настоящего изложения. Здесь стоит только порекомендовать еще в момент приобретения модема проконсультироваться по поводу его полной совместимости с сервером Domino и посмотреть сопроводительную документацию, поставляемую совместно с компьютером и операционной системой.

Для обеспечения доступа компьютера к пулу модемов требуется установить специальное программное обеспечение на вызывающем сервере. Например, такой физический сервер должен иметь программный коммуникационный сервер связи, который управляет пулом модемов, поэтому следует внимательно изучить документацию на соответствующий сервер связи.

Для реализации автоматического «заимствования» сервером Domino нужного модема (из соответствующего пула модемов) без какого-либо вмешательства оператора необходимо предварительно разработать и задать определенный *сценарий заимствования*. Подобный сценарий представляет собой текстовый файл, который содержит команды, ключевые слова и параметры, указывающие серверу Domino, в какой момент и с помощью какой команды надо установить контакт с сервером связи. В идеальном случае программное обеспечение сервера связи включает в себя сценарий, который уже готов к применению или может быть загружен с Web-сайта разработчика сервера связи. Если готовых сценариев не существует, всегда есть возможность подготовить собственный или модифицировать один из существующих образцовых, поставляемых совместно с сервером Domino. Подобные сценарии Domino обычно находятся в файле имя_файла.8sc, расположенном в подпапке модемов, который в свою очередь вложен в папку данных сервера Domino. В сценарии заимствования модемов входят, как правило, файлы comserv.scr и sprntpad.scr.

Программное обеспечение Microsoft Dial-Up Networking обычно входит в состав операционной системы Windows NT. Установка этих программных средств производится в виде

настройки сетевой службы. Для этого на панели управления выберите **Сеть** (Networking), затем **Службы** (Services). Более подробная информация имеется в документации на операционную систему Windows NT или в интерактивной справке.

Настройка порта

Настройка порта модема (или порта локальной сети) осуществляется посредством задания набора переменных в файле notes.ini сервера Domino. Этот набор в данном случае содержит переменные <portname>, Ports и DisabledPorts. Если заглянуть в файл notes.ini, вы увидите:

TCP/IP=TCP, 0, 15, 0

LAN0=NETBIOS, 0, 15, 0

LAN1ipx=NETBIOS, 1, 15, 0

LAN2ip=NETBIOS, 2, 15, 0

SPX=NWSPX, 0, 15, 0

VINES=VINES, 0, 15, 0

AppleTalk=ATALK, 0, 15, 0

LAN3=NETBIOS, 3, 15, 0

LAN4=NETBIOS, 4, 15, 0

LAN5=NETBIOS, 5, 15, 0

LAN6=NETBIOS, 6, 15, 0

LAN7=NETBIOS, 7, 15, 0

LAN8=NETBIOS, 8, 15, 0

COM1=XPC, 1, 15, 0

COM2=XPC, 2, 15, 0, , 12292, , usrspx2.mdm, 60, 15

COM3=XPC, 3, 15, 0

COM4=XPC, 4, 15, 0

COM5=XPC, 5, 15, 0

Ports=TCP/IP,SPX,LAN0,LAN1ip,LAN2 ipx

DisabledPorts=VINES,AppleTalk,LAN3,LAN4,LAN5,LAN6,LAN7,LAN8,COM1,COM3,COM4,COM5

В приведенном листинге переменная Ports описывает те порты, которые задействованы в текущий момент. Система Notes или сервер Domino используют эти порты в той последовательности, в которой они приводятся в перечне переменной. Переменная DisabledPorts определяет остальные порты, а обе переменные вместе содержат список всех потенциально разрешенных к применению портов (в целом описываются с помощью переменной <portname>). Переменная <portname> служит для реального именования портов, а в ее перечень входят следующие порты: TCP/IP, SPX, Vines, AppleTalk, причем названия портов определяют протокол локальной сети. Этот перечень также включает в себя порты LAN0, LAN1ipx, LAN2ip и LAN3 - LAN8, обеспечивающие поддержку протокола NetBIOS. Так, порт LAN1ipx поддерживает протокол NetBIOS поверх IPX, порт LAN2ipx - протокол NetBIOS поверх IP, а остальные порты - протокол NetBIOS поверх NetBEUI. И наконец, порты COM1 - COM5 являются портами последовательного обмена данными и осуществляют поддержку протокола X.PC (коммуникационный протокол модема).

Все порты в показанном листинге настраиваются автоматически системой Notes в процессе установки сервера. Автоматически разрешается применение портов TCP/IP, SPX, LAN0, LAN1ipx и LAN2ip, поскольку сами протоколы TCP/IP и SPX разрешаются к применению соответствующей операционной системой.

Переменные LAN <portname> и неконфигурируемые переменные COM <portname> предусматривают использование следующих параметров:

- О driver - имя файла библиотеки динамической компоновки DLL, служащей для управления портом;
- О unit_ID - логический номер, присвоенный порту (соответствует п в обозначениях типа LANn и COMn);
- О max_sessions - максимальное число одновременно поддерживаемых сеансов связи для порта;
- О buffer_size - размер (в килобайтах) буферной памяти порта.

Конфигурируемые переменные COM <portname> обычно применяют вышеупомянутые параметры, а также перечисленные ниже:

- О null - не содержит значения (значение не определено, «пусто»);
- О flags - включает в себя сумму чисел, указывающих на группу выставленных флагов, которые определяют большую часть значений в диалоговом окне Additional Setup (Дополнительная установка);
- О modem_speed - скорость передачи данных (Кбит/с) модемом;
- О modem_volume - уровень громкости для модема и режим набора номера;
- О modem_filename - имя файла для файла команд модема (файлы команд модема находятся в подпапке модемов, которая сама относится к папке данных);
- О dial_timer - тайм-аут (поддержание соединения без передачи информации) соединения (в секундах);
- О hangup_timeout - продолжительность паузы (в минутах), по завершении которой сервер Domino отменяет соединение модема.

Конечно же, параметры файла notes.ini сложно задавать вручную, и никто не делает этого без особой необходимости. Гораздо проще предоставить системе Notes или программе Domino Administrator устанавливать такие параметры автоматически после выбора вариантов в соответствующих диалоговых окнах. После щелчка по кнопке ОК в диалоговом окне заданные параметры будут автоматически преобразованы в значения переменных файла notes.ini.

Ниже описываются два различных диалоговых окна, которые служат для определения параметров модема. Так, в системе Notes можно воспользоваться диалоговым окном **User Preferences** (Предпочтения пользователя) - рис. 4.7. Окно открывается командой **Preferences** (Предпочтения) в меню **File** (Файл), после чего выбирается **User Preferences** (Предпочтения пользователя), а затем **Ports** (Порты).

В программе Domino Administrator это делается в аналогичном диалоговом окне **User Preferences** (Предпочтения пользователя) или диалоговом окне **Port Setup for <имя_сервера>** (Установка порта определенного сервера) - рис. 4.8. Окно **Port Setup** (Установка порта) может быть открыто на экране **Server** (Сервер) программы Domino Administrator. При этом следует сначала выбрать нужный сервер на панели **Bookmarks** (Закладки), расположенной в левой части экрана. Потом можно открыть диалоговое окно с помощью меню **Server** или панели **Tools** (Программные инструменты), причем в обоих случаях надо воспользоваться командой **Server**, а затем указать **Setup Ports** (Установка портов).

Оба диалоговых окна предусматривают выполнение одних и тех же операций, поэтому выбор остается за самим пользователем. Окно **Port Setup for <имя_сервера>** удобнее, поскольку предоставляет возможность производить настройку портов удаленно на любом доступном сервере. Кроме того, оно позволяет разрешать и отменять применение портов

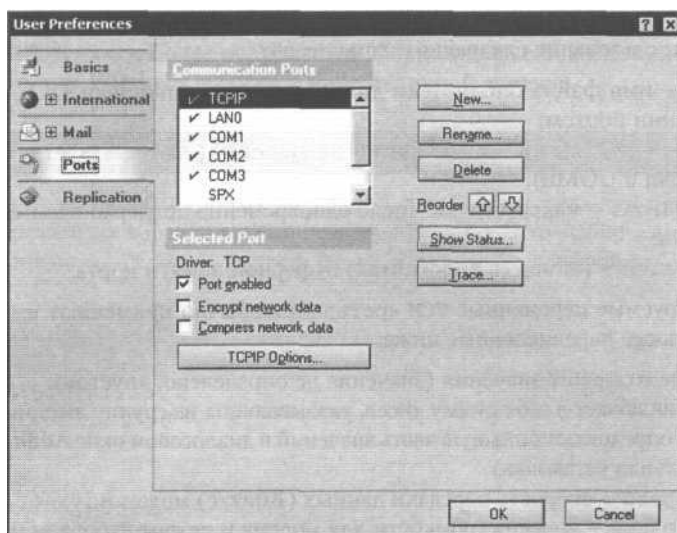


Рис. 4.7. Установка портов в системе Notes/Domino осуществляется в диалоговом окне **User Preferences**

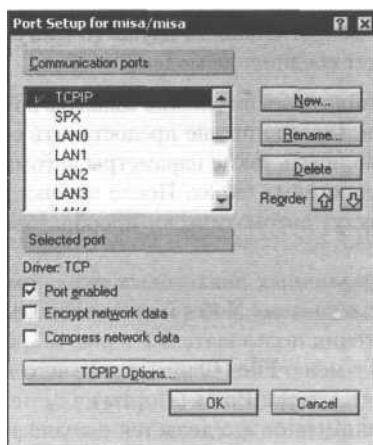


Рис. 4.8. Настройка портов для любого доступного сервера Domino проводится с помощью команды **Setup Ports**

без предварительного закрытия удаленного сервера. Диалоговое окно портов в клиенте Notes служит для настройки только портов в системе Notes, с которой осуществляется взаимодействие. Если система Notes использует файл notes.ini совместно с сервером Domino, то приходится инициировать остановку сервера перед тем, как разрешать или запрещать порты в диалоговом окне **User Preferences**.

Для настройки порта модема с помощью одного из диалоговых окон необходимо проделать указанные ниже операции:

1. Сначала выбирается порт, который будет указан в поле **Communication Ports** (Порты связи). В качестве подобных можно задавать порты локальной сети и порты последовательного обмена данными. Обычно модемы подключаются к последовательным портам, поэтому следует выбирать именно такой порт¹. На компьютерах с операционной системой Windows NT или OS/2 именами портов последовательного обмена данными являются COM1, COM2 и т.д. Для компьютеров с операционной системой UNIX эти порты имеют названия /dev/cuaO/, /dev/cuaL и т.д., а внутренние порты соответственно /dev/ttyO/, /dev/ttyL и т.д.
2. Затем порядок следования портов при необходимости изменяется кнопками **Reorder** (Переупорядочивание). Когда в документе соединения (Connection document) не содержится указаний на используемый порт, система Notes/Domino начинает обращаться к портам согласно упорядоченному списку.
3. После этого устанавливается флажок в поле **Port Enabled** (Разрешенный порт). Надо отметить, что в диалоговом окне **User Preferences** клиента Notes для работающего сервера активизация такого флажка запрещена.
4. Затем можно отметить (при необходимости) флажок **Encrypt network data** (Шифрование сетевых данных). Установка флажка приводит к увеличению сетевой нагрузки и уменьшению скорости передачи данных, поэтому обращаться к данному полю следует только в том случае, если существует вероятность перехвата конфиденциальной информации в сети.
5. Далее нужно щелкнуть по кнопке **<имя_порта> Options** (Параметры порта определенного типа), чтобы открыть диалоговое окно **Additional Setup** (Дополнительная установка).
6. В данном окне при установке модема заполняются следующие поля:
 - **Modem type** (Тип модема). Приводится перечень командных файлов модема, который фактически соответствует списку файлов в каталоге данных/модемов с расширением .mdm. Надо выбирать файл, в наибольшей степени пригодный для применяемого модема. Если повезет, удастся отыскать в списке файл, который непосредственно предназначен для работы с данным модемом. В противном случае стоит определить наиболее подходящий, выбирая различные файлы. Может возникнуть и такая ситуация, при которой ни один из имеющихся файлов не обеспечит нормальной работы модема;
 - **Maximum port speed** (Максимальная скорость передачи данных для порта). В этом поле приводится перечень типовых скоростей передачи данных, реализуемых для порта модема. Следует выбирать максимальную скорость, которую в состоянии обеспечить модем и порт последовательного обмена данными;
 - **Speaker volume** (Уровень громкости). Предназначено для регулирования уровней громкости в динамике модема (например, при наборе номера). Этот уровень надо обеспечить достаточно высоким, чтобы пользователь контролировал все выполняемые действия в процессе проверки уровня громкости, однако для других режимов работы он должен быть минимальным;

Для внешнего модема. - Прим, ред.

- **Dial mode** (Режим набора номера). В данном случае могут задаваться варианты **Tone** (Тональный сигнал) и **Pulse** (Импульсный сигнал). Первый вариант выбирается только при условии, что телефонная система поддерживает режим формирования тональных сигналов при наборе номера;
- **Log modem I/O** (Регистрация вводимых/выводимых данных модема). Функция включается лишь на время тестирования связи с другими модемами. После установки флажка каждая команда, пересылаемая системой Notes/Domino на модем, и каждый ответ модема будут регистрироваться и заноситься в базу данных Notes Log (Журнал системы Notes). Функция весьма полезна при отладке, однако приводит к большому числу записей в журнале регистрации; по этой причине она применяется только в режиме проверки модема;
- **Log script I/O** (Регистрация вводимых/выводимых данных сценариев). Указанную функцию следует активизировать лишь при проверке сценариев, то есть в ситуациях, когда требуется заимствовать модем в пуле модемов, получать через сеть X.25 доступ к серверу или обращаться к защищенному устройству. Как и в случае предшествующей функции, ее активизация обеспечивает регистрацию каждой команды сценария и каждого ответа в базе данных Notes Log, что позволяет достаточно легко выявлять возникающие ошибки. Однако эту функцию надо отменять при переходе к какому-либо иному режиму работы;
- **Hardware flow control** (Аппаратное управление информационным потоком). Функция задается в режиме по умолчанию. Отменять ее действие требуется исключительно тогда, когда известно, что данный модем поддерживает только режим программного управления информационным потоком (такая ситуация возникает достаточно редко);
- **Wait for dialtone before dialing** (Ожидание гудка перед набором номера). Эта функция устанавливается в режиме по умолчанию. Она отключается, только если другим способом не удастся «заставить» модем работать правильно;
- **Dial timeout** (Временной интервал при наборе номера). В данном поле по умолчанию назначается величина 60 с. Эта величина характеризует временной интервал, в течение которого используемый модем должен сформировать соединение с другим модемом. Если модем за такой временной интервал не установил необходимого соединения, система Notes прервет подключение и попытается установить соединение позже. Данный вариант рекомендуется оставлять без изменений, если только на этот счет нет специальных указаний;
- **Hang up if idle for** (Временной интервал до отключения после завершения активности). Здесь по умолчанию задается величина 15 минут, соответствующая тому временному интервалу, по истечении которого в отсутствие активности со стороны модема система Notes/Domino автоматически отменит соединение. На практике не рекомендуется менять этот вариант, кроме случаев, когда изменения особо оговариваются;
- **Port number** (Номер порта). В поле определяется номер порта для установленной операционной системы. В операционных системах Windows NT и OS/2 этот номер совпадает с номером п в обозначении СОМп и не требует каких-либо изменений. При создании нового порта последовательного обмена данными или переименовании порта, отличного от СОМп, можно воспользоваться данным полем для идентификации того порта (операционной системы), с которым планируется работать;

- кнопка **Modem File** (Файл модема). Щелкните по этой кнопке, чтобы отредактировать файл команд модема, указанный в поле **Modem type** (Тип модема). Данный файл представляет собой текст, содержащий переменные и их значения. Переменные являются ключевыми словами, описывающими выполняемые модемом операции, а значения - кодовыми последовательностями, иницирующими выполнение этих операций модемом. Кнопкой можно открыть файл для просмотра, однако реальное изменение файла следует производить только в том случае, если не удастся добиться нормальной работы модема и не представляется возможным воспользоваться каким-либо иным файлом;
 - кнопка **Acquire Script** (Сценарий заимствования). Если модем, с которым организует взаимодействие данный порт, является компонентом пула модемов определенного сервера связи, надо щелкнуть по этой кнопке, чтобы указать режим заимствования. Откроется одноименное диалоговое окно с перечнем возможных сценариев, который на практике соответствует списку файлов каталога данных/модемов, имеющих расширение .sen Следует выбрать из перечня требуемый сценарий, с помощью команды **Edit** (Редактирование) отредактировать его, а затем щелкнуть по кнопке ОК и вернуться в окно **Additional Setup**.
7. По окончании настройки в диалоговом окне **Additional Setup** надо щелчком по кнопке ОК закрыть данное окно и вернуться в диалоговое окно **Port Setup** или **User Preferences**. Затем можно кнопкой ОК закрыть и это окно.

Создание документа соединения

Для завершения процесса формирования соединения модема (между двумя серверами) следует создать один или несколько документов соединения (Connection document) в каталоге Domain Directory. В подобном документе даются инструкции для системы Notes/Domino, указывающие на порядок действий при формировании соединения с другим компьютером и последующем применении этого соединения. В данном случае речь идет о разрешении на установку модемного соединения между двумя серверами Domino, поэтому внимание далее будет сконцентрировано на трех типах такого соединения: с непосредственным набором номера, с набором номера сети и сквозном.

Создание документа соединения требует выполнения следующих действий:

1. Запустите программу Domino Administrator и перейдите на экран **Configuration** (Конфигурация). Если для данного сервера задан вариант **Local** (Локальный), укажите имя доступного сервера. В противном случае выберите сервер в поле **Use Directory on...** (Использование каталога на...). Если описанных действий не предпринять, то в каталоге Domain Directory местной рабочей станции сформируется новый документ соединения, но для подключения пользователя к серверу, а не для соединения двух серверов. Рекомендуется установить сервер, для которого создается новый документ соединения; однако, если этот сервер на текущий момент не используется или просто недоступен, можно обратиться к любому другому серверу в том же домене.
2. Воспользуйтесь командами **Server** (Сервер), потом **Connections** (Соединения) на панели **Navigator** (Навигатор) в левой части экрана. Вид **Server => connections** (Сервер => Соединения) базы данных Domino Directory появится на панели **View** (Вид) в правой части экрана. В этом окне будет присутствовать перечень существующих документов соединения.

3. Затем щелкните по кнопке **Add Connection** (Добавление соединения), расположенной в верхней части вида, после чего на экран дисплея будет выведен пустой документ соединения сервера.
4. На заключительной стадии заполните поля документа в соответствии с приведенными ниже рекомендациями, далее сохраните и закройте его. В результате в окне вида **Connections** (Соединения) будет показан вновь созданный документ соединения.

Форма **Connection**, открывающаяся на шаге 3, содержит пять вкладок (рис. 4.9). В данном разделе речь пойдет только о вкладке **Basics** (Основные параметры). Сначала задается тип соединения в поле **Connection type** (Тип соединения). В зависимости от характера заполнения этого поля в дальнейшем потребуются заполнить различные группы полей.

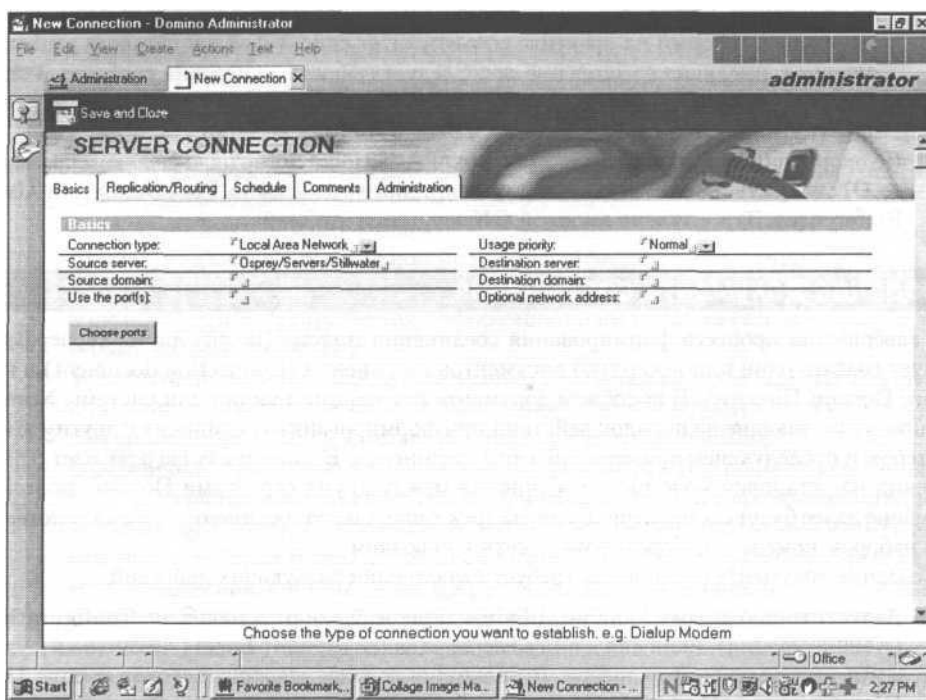


Рис. 4.9. Перечень полей, образующих данный раздел документа соединения, меняется в зависимости от варианта, указанного в поле *Connection type*

Однако существуют поля, которые необходимо заполнять для всех типов соединения без исключения:

- О **Connection type** (Тип соединения). По умолчанию для этого поля устанавливается вариант **Local Area Network** (Локальная сеть). Если данный сервер будет использовать собственный модем (или обращаться к пулу модемов) для связи с другим модемом сервера Domino, рекомендуется выбрать вариант **Notes Direct Dialup** (Непосредственное коммутируемое подключение в системе Notes) - см. рис. 4.5.

Если же данный сервер с помощью своего модема (или через пул модемов) сформирует соединение с сервером, применяющим программные средства Microsoft Dial-Up Networking (первый сценарий на рис. 4.6), известные также под названием Microsoft Remote Access Server (RAS), или с сервером дистанционного доступа AppleTalk Remote Access, следует задавать вариант **Network Dialup** (Коммутируемый сетевой доступ);

- О **Usage priority** (Приоритет использования). Установленный здесь вариант определяет, будет ли сервер Domino сначала проводить поиск данного документа соединения или выждет и попробует все возможные способы создания соединения, а уже затем, при необходимости, обратится к данному документу. В этом поле надо отмечать пункт **Normal** (Нормальный) при модемном соединении. Другой вариант, **Low** (Низкий), допускается задавать только в тех случаях, когда два сервера взаимодействуют с помощью нескольких протоколов локальной сети. Если сервер Domino может выбирать между несколькими документами соединения, он будет обращаться к ним в следующем порядке: локальная сеть, коммутируемый сетевой доступ, непосредственное коммутируемое соединение, сквозной сервер, целевая группа сквозных серверов;
- О **Source server** (Исходный сервер). В данном поле следует определить полное имя сервера, который будет инициировать формирование соединения между серверами. По умолчанию здесь вводится имя того сервера, копия каталога Domain Directory которого служит в текущий момент для создания документа соединения;
- О **Destination server** (Сервер адресата). В это поле необходимо внести полное имя сервера, с которым будет устанавливаться связь исходный сервер;
- О **Source domain** (Исходный домен) и **Destination Domain** (Домен адресата). Поля предназначены для назначения имен доменов исходного сервера и сервера адресата (сервера назначения). Если эти серверы располагаются в одном домене, поля можно не заполнять;
- О **Use the ports** (Использование портов). Здесь требуется указать название одного или нескольких портов. Если задано несколько портов, сервер Domino обращается к ним в том порядке, в котором они перечислены. При выборе варианта **Local Area Network** (Локальная сеть) в поле **Connection type** после щелчка по кнопке **Choose Ports** (Выбор портов) можно отметить один или большее число портов из предлагаемого перечня. Кроме того, вариант **Local Area Network** позволяет оставлять данное поле незаполненным. В этом случае сервер Domino последовательно обратится ко всем разрешенным портам локальной сети, начиная с того из них, который успешно использовался последним.

Для локальной сети и непосредственного коммутируемого соединения требуется заполнить дополнительное поле:

- О **Optional network address** (Необязательный сетевой адрес). Если ранее был выбран вариант **TCP/IP** для поля **Use the ports** (Использование портов), то здесь можно указать полное различающееся имя сервера адресата или его IP-адрес. Задание IP-адреса избавляет сервер Domino от необходимости запроса к стеку протокола IP для получения IP-адреса сервера адресата. При изменении IP-адреса сервера адресата придется, конечно, поменять его и в данном поле. В случае назначения имени хоста для сервера адресата сервер Domino будет с помощью этого имени обращаться к стеку протокола IP за IP-адресом сервера адресата. Если оставить поле незаполненным, сервер Domino воспользуется при запросе к стеку IP общим именем сервера адресата в системе Notes.

Дополнительная вкладка **Network Dialup** (Сетевой коммутируемый доступ) появляется только для документа соединений, созданного с целью одноименного подключения. Эта вкладка содержит поле **Choose a service type** (Выбор типа службы), для которого имеются следующие варианты: **AppleTalk Remote Access**, **Macintosh PPP** и **Microsoft Dial-Up Networking**. Перечень других полей зависит от того, какой вариант будет задан в первом поле. Поскольку на практике весьма маловероятно, чтобы один сервер обращался по коммутируемому сетевому доступу к другому посредством **AppleTalk Remote Access** или **Macintosh PPP**, далее будут рассмотрены только те поля, которые выводятся для варианта **Microsoft Dial-Up Networking**. После щелчка по кнопке **Edit Configuration** (Редактирование конфигурации) предоставляется возможность указать параметры в соответствующем диалоговом окне. Два из раскрывающихся при этом полей имеют в окне одни названия, а в форме – несколько иные. В представленном ниже списке полей названия, присутствующие в форме, указываются в круглых скобках сразу после названий из диалогового окна:

- **Dial-Up Networking name (Remote connection name)** (Имя подключения сетевого коммутируемого доступа, Имя удаленного соединения). Поле предназначено для ввода названия (имени) соединения, задаваемого в программе Microsoft Dial-Up Networking;
- **Login name (Remote network login name)** (Имя входа, Имя входа в удаленную сеть). В данном поле указывается то имя, под которым сервер будет регистрироваться в удаленной сети;
- **Password** (Пароль). Здесь можно задать пароль, который серверу нужен для регистрации в удаленной сети (для входа в удаленную сеть);
- **Country code, Area code и Phone number** (Код страны, Код области и Номер телефона). В этих полях устанавливается код страны, код области и номер телефона, с помощью которых сервер будет подключаться к удаленной сети;
- **Dial-back phone number** (Телефонный номер обратного вызова). В данном поле вводится телефонный номер исходного сервера (а также код области или города и код страны).

Все перечисленные поля заполняются только в случае необходимости – например, когда требуется дополнить параметры соединения недостающим компонентом или когда остается незаполненным соответствующее поле в документе для соединения типа Microsoft Dial-up Networking. Код страны нужен, когда исходный сервер и сервер адресата находятся в разных странах и этот код не был указан для соединения типа Microsoft Dial-Up Networking. Если ввести код в дополнительное поле, при том что в соответствующем поле для документа соединения типа Microsoft Dial-Up Networking также присутствует определенный код, система Notes будет пользоваться именно кодом из поля. И наконец, при сохранении документа соединения сервер будет автоматически шифровать данные в поле пароля по закрытому ключу исходного сервера, а также по именам, указанным в полях **Owners** (Владельцы) и **Administrators** (Администраторы) страницы **Administration** (Администрирование).

Перечень дополнительных полей для прямого коммутируемого соединения Notes:

- **Destination country code, Destination area code и Destination phone number** (Код страны адресата, Код области адресата и Номер телефона адресата). В данном случае коды страны и местности задаются, только если это требуется, однако номер телефона должен быть внесен обязательно;

- **Always use area code** (Обязательное указание кода области). По умолчанию здесь установлен вариант **No** (Нет), менять который на **Yes** (Да) следует в том случае, когда код области нужен для местных телефонных звонков;
- **Login script file name** (Имя файла для сценария входа). В поле вводится имя файла для соответствующего сценария, по которому устанавливается контакт с сервером адресата. Например, при обращении к общедоступному серверу в сети компании CompuServe после набора номера (перед непосредственным обращением к серверу) надо указать идентификационные данные и пароль пользователя этой сети;
- **Login script arguments** (Аргументы для сценария входа). Сюда допускается вносить до четырех параметров, которые передаются в сценарий входа в систему адресата в виде аргументов. Так, в рассмотренном выше примере с сетью CompuServe можно ограничиться вводом двух параметров: идентификационных данных и пароля пользователя.

К сожалению, система Notes не обеспечивает шифрование пароля в документе соединения для непосредственного коммутируемого подключения, как это делается в документе коммутируемого сетевого подключения. При необходимости защиты данных, например пароля пользователя, приходится прибегать к какому-либо иному способу. Возможно, проще всего ограничить доступ к самому документу, выполнив следующие действия:

1. Сохраните и закройте документ соединения (Connection document).
2. Щелкните правой кнопкой по этому документу на виде **Connections** (Соединения). Появится контекстное меню. Выберите **Document Properties** (Свойства документа) - откроется одноименное окно.
3. Выберите вкладку **Security** (Безопасность) в окне **Document Properties** (Свойства документа) - на языке этой вкладки изображен ключ от двери.
4. В разделе **Who can read this document** (Допущенные к чтению данного документа) сбросьте флажок **All readers and above** (Все читатели и лица с большими правами) и укажите в находящемся ниже списке всех авторизованных пользователей своего документа. Если нужного пользователя, сервера или группы в списке нет, щелкните по кнопке справа. Развернется диалоговое окно **Select Names** (Выбор имен), в котором можно указать имена пользователей, серверов и групп по своему усмотрению. Эти имена допускается заимствовать из любой книги адресов или каталога, которые перечислены в поле, расположенном в левом верхнем углу диалогового окна. Следует помнить, что в список имен авторизованных пользователей должен обязательно попасть исходный сервер данного документа соединения. Кроме включенных в упомянутый список право чтения документа (а также его редактирования) будут иметь пользователи, присутствующие в поле **Owners** (Владельцы) или **Administrators** (Администраторы), равно как и имеющие статус **[NetModifier]** (Изменение сетевых параметров).

Существует другой способ активизации функции шифрования данных для тех полей, которые содержат конфиденциальную информацию: внесение необходимых изменений в соответствующем разделе шаблона проектирования каталога Domain Directory. Подобный подход предполагает хорошее знание всего процесса проектирования приложений системы Notes, что характерно для весьма ограниченного числа пользователей, поэтому в настоящем разделе детально не рассматривается. Кроме того, делать это просто не рекомендуется, поскольку индивидуальная настройка баз данных Domain Directory может усложнить в дальнейшем процедуры их модификации.

Установка сквозных серверов

Сквозное соединение через один или большее число серверов Domino позволяет компьютеру установить связь с сервером адресата, что полезно при подключении пользователей по модемным соединениям к сетям и сетевым серверам, не имеющим модемов (эти возможности подробно обсуждаются в следующей главе). Непосредственная выгода от наличия подобного соединения может быть получена в следующих случаях:

- О у сервера 1 отсутствует модем, однако он способен через один или большее число сквозных серверов, у которых есть собственные модемы, организовать доступ к серверу 4 удаленной локальной сети (рис. 4.10);
- О для сервера 1 (конфигурация с поддержкой протокола TCP/IP) сервер 2 (конфигурация с поддержкой протоколов TCP/IP и IPX/SPX) служит в качестве сквозного для связи с сервером 3 (конфигурация с поддержкой протокола IPX/SPX) в одной локальной сети, при этом сервер 2 обеспечивает преобразование данных для серверов 1 и 3, которые иначе не могли бы нормально взаимодействовать.

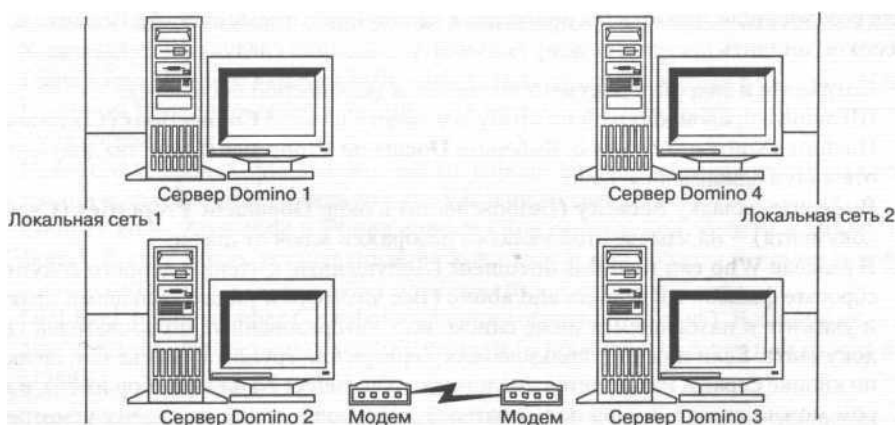


Рис. 4.10. Сервер 1 может пользоваться серверами 2 и 3 как сквозными для взаимодействия с сервером 4 (на практике сервер способен применять до девяти сквозных серверов для достижения десятого)

Чтобы реализовать взаимодействие серверов с помощью сквозного соединения, приходится создавать один или несколько документов соединения для сквозных серверов. Этот документ практически ничем не отличается от других документов соединения - за тем исключением, что в данном случае необходимо указывать имя сквозного сервера, а не оговаривать порт, служащий для связи с сервером адресата. Достаточно задать вариант Passthru Server (Сквозной сервер) в поле Connection type (Тип соединения) и ввести имя сквозного сервера в поле **Use passthru server or hunt group** (Использование сквозного сервера или группы поиска).

У сквозного сервера должен быть способ достижения сервера адресата. Он может иметь собственные документы соединения, содержащие сведения о том, каким образом установить контакт или какими службами для этого воспользоваться. Например, для представленного на рис. 4.10 случая должны выполняться следующие условия:

- О сервер 1 знает из имеющегося документа сквозного соединения, что взаимодействие с сервером 4 может быть обеспечено только через сервер 2. Серверу 1 известно, как обратиться к серверу 2, поскольку они относятся к одной локальной сети и работают с одним и тем же протоколом связи. Так, если оба сервера поддерживают протокол TCP/IP, сервер 1 в состоянии запрашивать адрес сервера 2 из локального файла хостов или из сервера имен DNS;
- О серверу 2 из имеющегося документа сквозного соединения должно быть понятно, что взаимодействие с сервером 4 реализуется только через сервер 3, а из документа прямого коммутируемого соединения (Notes Direct Dialup) - как добраться до этого сервера;
- О сервер 3 должен найти маршрут к серверу 4 в службе имен (так же, как сервер 1 находит маршрут к серверу 2 на шаге 1).

Установка процедуры репликации

Для обеспечения нормального взаимодействия нового сервера с уже существующими серверами домена Domain, серверы обязаны совместно использовать одинаковую информацию. Каждому серверу следует знать имена других серверов, иметь возможность связаться с ними и быть хорошо осведомленными о составе служб, предоставляемых ими.

Серверы отслеживают данные друг друга за счет совместного обеспечения нескольких баз, в которых хранится нужная информация, причем все серверы в домене поддерживают местные копии этих баз данных, в том числе каталога Domain Directory (Каталог доменов), базы данных Administration Requests (Административные запросы) и некоторых других.

Таким образом, дополнительной причиной для установки нового сервера может стать необходимость поддержки резервных копий пользовательских баз данных (в частности, для удобства доступа пользователей или реализации высокой доступности данных).

Итак, вне зависимости от первоначальных соображений серверы Domino поддерживают резервные копии нескольких баз данных. Изменение, сделанное в одной из таких копий, должно передаваться в копии баз данных других серверов, чтобы серверы могли по-прежнему нормально взаимодействовать друг с другом. Процедура распространения изменений по всем базам данных, называемая *репликацией*, более подробно описана в главе 9. Пока необходимо лишь ясно осознать, что процедура репликации для серверов Domino не запускается автоматически, за исключением специального случая - кластера серверов Domino, который в деталях обсуждается в главе 20. Хотя указанная процедура может быть эпизодически инициирована соответствующей командой, на практике целесообразно выполнять ее в соответствии с определенным расписанием и без вмешательства оператора. Для этого необходимо создать один или большее число документов соединения, разрешить в них проведение репликации (запустить соответствующую задачу) и составить расписание подключений.

Если перед установкой серверов был выработан необходимый план, то к данному моменту уже хорошо известно, какие потребуются документы соединений, чтобы гарантировать правильное выполнение репликации между новым и существующими серверами домена. Однако эти вопросы в книге не рассматривались, поскольку обсуждение репликации отложено до главы 9.

Предположим (при описании процесса настройки репликации дополнительного сервера с существующим), что первый сервер домена уже инициировал процедуру репликации.

Теперь репликацию нужно запустить на дополнительном сервере Osprey/Servers/Stillwater для обмена данными с сервером Kestrel/Servers/Stillwater. Реализация этой процедуры требует подготовки документа соединения и заполнения по крайней мере следующих полей на вкладке **Basics** (Основные параметры):

- О **Source server** (Исходный сервер). В него заносится имя Osprey/Servers/Stillwater;
- О **Destination server** (Сервер адресата). В данное поле вводится имя Kestrel/Servers/Stillwater.

Кроме того, надо заполнить несколько полей на вкладке **Replication/Routing** (Репликация/маршрутизация):

- О **Replication task** (Задача репликации), в котором следует задать вариант **Enabled** (Разрешено);
- О **Routing task** (Задача маршрутизации), где нужно выбрать пункт **None** (Отмена), если серверы принадлежат к одной именованной сети Domino. Когда серверы находятся в различных сетях Domino, документ соединения может применяться (при необходимости) для выполнения операций репликации баз данных и маршрутизации почтовых сообщений, передаваемых между двумя серверами (см. главу 7),

а также одно поле на вкладке **Schedule** (Расписание):

- О **Schedule** (Расписание), где надо указать вариант **Enabled**.

Во всех прочих полях рекомендуется воспользоваться теми вариантами и значениями, которые назначены по умолчанию.

В ряде случаев может потребоваться изменить (в зависимости от типа соединения между двумя серверами) установки, заданные по умолчанию, например для полей вкладки **Basics** документа соединения.

Следует отметить, что создаваемый документ соединения обеспечивает дублирование данных и их передачу в обоих направлениях между двумя указываемыми серверами. Это связано с тем, что в поле **Replication type** (Тип репликации) на вкладке **Replication/Routing** по умолчанию определен вариант **Pull Push** (Вытягивание/выталкивание). В этом режиме репликации исходный сервер сначала затребует (вытянет) изменения копии базы данных сервера адресата, а затем направит (вытолкнет) серверу адресата сообщение относительно изменений собственной копии базы данных. Таким образом, в некоторых ситуациях достаточно сформировать всего один документ соединения, чтобы гарантировать репликацию между двумя серверами.

В случае, когда (как в рассмотренном выше примере) требуется производить репликацию между первым сервером (с именем Osprey) и каждым новым вводимым в эксплуатацию, нет необходимости задавать процедуру репликации между очередным сервером и каждым существующим. Поскольку сервер Osprey инициирует репликацию с каждым сервером домена, те изменения, которые вносятся в копии баз данных новых серверов, будут автоматически передаваться на сервер Osprey.

Этот пример - типичный случай использования *топологии репликации* с радиальным концентратором, которая является наиболее эффективной. В рассмотренном примере сервер Osprey представляет собой *концентратор*, а сервер Kestrel и другие серверы образуют радиальные вторичные компоненты (см. главу 8).

Установка процедуры маршрутизации почтовых сообщений

Возможно, пользователям и не придется заниматься вопросами настройки процедуры маршрутизации почтовых сообщений между новым и существующими серверами. Если два сервера относятся к одной именованной сети Domino, они будут автоматически пересылать друг другу почтовые сообщения, так что пользователю нет нужды вмешиваться в процесс. Однако когда два сервера находятся в разных именованных сетях Domino, может потребоваться создать один или большее число документов соединения для обеспечения почтовой маршрутизации между двумя серверами. Возможен также вариант взаимодействия этих серверов через вспомогательные серверы, для которых уже сформированы соответствующие документы соединения.

Если требуется организовать маршрутизацию почтовых сообщений между новым сервером и серверами другого домена Domino (или между новым сервером и почтовыми системами не-Notes, например cc:Mail, SMTP или X.400), также не понадобится выполнять какие-либо сложные или специальные операции. В таком случае, естественно, придется предварительно конфигурировать соединения для передачи почтовых сообщений между по меньшей мере одним шлюзовым сервером домена Domain и одним или несколькими серверами почтовой связи, располагающимися за границами домена. При этом можно посредством типовых операций обеспечить для других серверов домена эффективное применение формируемого соединения через шлюз. Поскольку остальные серверы домена в состоянии свободно направлять почтовые сообщения шлюзовому серверу (непосредственно или косвенным образом), они автоматически получают возможность маршрутизации почтовых сообщений за пределы домена.

Другими словами, конфигурирование процедуры маршрутизации для нового сервера зависит от его взаимосвязи с другими серверами домена и от тех соединений (для передачи почтовых сообщений), которые уже созданы на данный момент. Более подробно этот вопрос рассматривается в главе 8, а пока нужно хорошо усвоить следующее.

Во-первых, все серверы Domino должны иметь возможность обмениваться почтовыми сообщениями с другими серверами домена - даже в том случае, если они изначально не конфигурировались в виде серверов почтовой службы. Следует отметить, что все базы данных системы Notes поддерживают функции почтовой службы. Они осуществляют пересылку документов между серверами (базами данных) с использованием процедуры маршрутизации почтовых сообщений. В связи с этим каждый сервер Domino должен передавать почтовые сообщения на другой сервер.

Во-вторых, если требуется создать документ соединения для маршрутизации почтовых сообщений между новым сервером и другими серверами домена, необходимо предусмотреть возможность пересылки сообщений в обоих направлениях. В более ранних версиях системы Notes/Domino (до 5.0) в таких случаях приходилось создавать два документа соединения, поскольку процедура маршрутизации почтовых сообщений обеспечивалась только в одном направлении (выгалкивание). Каждый сервер должен был инициировать работу собственного соединения, а затем выгалкивать исходящие сообщения на сервер адресата. Начиная с версии 5 серверы могут функционировать по принципу Pull Push и обходиться при передаче

почтовых сообщений всего одним документом соединения. В результате изначально требуется создать только один документ соединения и модифицировать в нем содержимое двух полей на вкладке **Replication/Routing**:

- **Routing task** (Задача маршрутизации) - здесь надо задать вариант **Enabled** (Разрешено);
- **Router type** (Тип маршрутизации) - в этом поле по умолчанию установлен вариант **Pull Push**. При выборе какого-либо иного варианта маршрутизации необходимо создать второй документ соединения для обеспечения передачи почтовых сообщений в направлении, противоположном выбранному,

а также содержимое одного поля на вкладке **Schedule** (Расписание):

- **Schedule** - в нем нужно указать вариант **Enabled** (Разрешено).

Все остальные поля могут быть заполнены в режиме по умолчанию.

В-третьих, временной интервал для маршрутизации почтовых сообщений определяется в документе соединения соответствующим «с 8 часов утра до 10 часов вечера». Однако временной интервал для передачи почтовых сообщений с низким уровнем приоритета может быть установлен по умолчанию «с 12 часов ночи до 6 часов утра». Если не изменить границы указанных временных диапазонов (задаваемых по умолчанию) так, чтобы они хотя бы частично перекрывались, могут возникнуть трудности с передачей и приемом почтовых сообщений, имеющих низкий приоритет. Поэтому при создании любого документа соединения, разрешающего маршрутизацию почты, приходится менять по меньшей мере одну из границ этих временных интервалов. Для изменения временного интервала, выделяемого для передачи почтовых сообщений с низким приоритетом, необходимо модифицировать следующую переменную в серверном файле `notes.file`:

`MailLowPriorityTime=time-range`

Параметр `time-range` представлен в 24-часовом формате. Например, эта переменная может задаваться в виде

`MailLowPriorityTime=21:00-23:00`

При этом можно указать временной интервал для передачи почтовых сообщений с низким приоритетом «с 9 часов утра до 11 часов вечера».

Установка процесса администрирования

Процесс администрирования представляет собой функцию сервера, позволяющую выполнять самые разнообразные (в том числе сложные) операции, которые обычно приходится делать администратору вручную. Ниже приводится перечень задач, обеспечиваемых этой процедурой:

- поддержка схемы присвоения имен (в частности, переименование пользователей и групп, удаление пользователей и групп, а также серверов, повторная сертификация пользователей и хранение сертификатов сети Internet);
- поддержка файлов почтовых сообщений (в частности, их перемещение и удаление);
- поддержка документов сервера (в частности, автоматическая модификация различных полей).

Процесс администрирования для каждого сервера запускается автоматически, поскольку параметр `adminp` присутствует в переменной `Servertasks` файла `notes.ini` каждого сервера. Завершить процесс можно с помощью команды `tell adminp quit` серверной консоли. Для перезапуска процесса служит команда `load adminp`. Процесс администрирования использует базу данных `Administration Requests` (файл `admin4.nsf`), записи которой позволяют проследить последовательность выполняемых серверами операций. Разрешается редактировать и читать документы базы данных, однако возможности создавать документы вручную в этом случае не предусматривается. Процесс администрирования берет на себя задачу создания всех документов в базе данных и делает это по запросу, сформированному администраторами, или с учетом тех событий, которые происходят на сервере.

Многие задачи, обеспечиваемые процессом администрирования, требуют участия нескольких серверов и могут протекать как последовательно, так и одновременно. Для этого база данных `Administration Requests` (Административные запросы) реплицируется на все серверы (для версии 4.0 и последующих) домена. В ходе обработки каждым сервером своей части задачи сервер модифицирует записи собственной копии базы данных, изменяя запрос или добавляя документ отклика. Во время репликации изменения передаются на другие серверы. В результате все серверы способны нормально отслеживать процесс выполнения различных частей задачи и своевременно к нему подключаться.

Серверы, которые реально отслеживают запросы, поступающие в базу данных `Administration Requests`, иногда называют *административными*. Рекомендуется предусматривать такие серверы для определенных баз данных. Каждой базе данных ставится в соответствие только один административный сервер (правда, он не всегда выделяется специально). В тех случаях, когда базы данных хранятся лишь на одной рабочей станции пользователей, в качестве административного сервера может выступать один из пользователей. Каждый раз при регистрации подобного пользователя на его «собственном» сервере система `Notes` будет опрашивать базу данных `Administration Requests`, чтобы найти запросы к базе данных, для которой пользователь играет роль административного сервера, и, обнаружив такие запросы, передаст их данному пользователю.

Административный сервер каталога `Domain Directory` обычно берет на себя большой объем работы. В частности, ему приходится изменять записи документов, хранящихся в этой базе данных, и содержимое ее списка `ACL`. У административных серверов других баз данных объем работы обычно меньше. Они отвечают за изменение содержимого баз данных для списков `ACL` и в ряде случаев за изменения в полях **Reader** и **Author**.

Reader (Читатель) и **Author** (Автор) – два типа данных для полей, определяющих имена пользователей, причем далеко не все базы предусматривают присутствие данных такого типа. При выделении административного сервера для конкретной базы данных необходимо принять решение о том, будет ли этот сервер что-либо менять в указанных полях или ограничится модификациями в списке `ACL`. Конечно, в том случае, если база данных не планирует применять поля **Reader** или **Author**, бессмысленно заставлять административный сервер контролировать изменения в них.

Если нет полной уверенности в том, что база данных содержит указанные поля, следует обратиться к ее разработчику либо воспользоваться программой `Domino Designer` и определить структуру базы. По выявленной структуре можно проследить все формы, разделы и совместно используемые поля, после чего с помощью команды **Find/Replace** (Поиск/замена) найти слова «`reader`» и «`author`». В данном случае ведется поиск полей с названиями **reader** и **author**, причем нас интересуют только те места, где эти слова находятся справа от слова «`database`».

ОДНИМ ИЗ организационных вопросов, который придется решить во время установки домена Domino, является вопрос о том, какой из серверов будет управлять (администрировать) конкретной базой данных. Задачи администрирования могут распределяться по разным серверам или, наоборот, консолидироваться на одном или нескольких серверах. Не исключено, что решающим фактором окажется удобство работы пользователей. На практике следует создавать серверы максимально доступными для пользователей, поэтому нежелательно нагружать активно эксплуатируемый сервер дополнительными задачами по администрированию баз данных. Для этих целей надо выделять серверы, которые непосредственно не работают с пользователями, например концентраторы репликации.

Однако на практике, как правило, не удастся полностью высвободить сервер только для решения задач администрирования баз данных или только для обслуживания пользователей, поскольку каждый сервер имеет базы данных, которые хранятся лишь на нем. Так, базы данных почтовой службы пользователя обычно имеются исключительно на серверах почтовой службы. Поэтому даже в том случае, когда серверы почтовой службы оказываются перегруженными, им все-таки приходится выполнять функции по администрированию собственных баз данных почтовой службы. Тем не менее не рекомендуется загружать сервер, активно пересылающий почтовые сообщения или исполняющий приложения, задачами по администрированию тех баз данных, которые находятся на других серверах.

Для нормальной организации процедуры администрирования на практике должно соблюдаться несколько условий. Они уже упоминались в главе 3, однако представляется целесообразным повторить их еще раз в данном разделе. Итак, требуется обеспечить:

- О непрерывную работу процесса Adminp на любом сервере, участвующем в процессе администрирования (этот режим обычно задается по умолчанию);
- О присутствие реплики базы данных Administration Requests (Административные запросы) на каждом сервере, исполняющем административные функции (процесс Adminp создает такую базу автоматически при первом запуске);
- О выделение одного из серверов в качестве административного сервера каталога Domain Directory. Он будет проводить все изменения, инициируемые в ходе процесса администрирования для каталога Domain Directory. По умолчанию такую функцию принимает на себя первый сервер домена, однако в дальнейшем она может быть передана другому серверу;
- О присутствие на любом сервере, способном выполнять функции регистрирующего в процессе повторной сертификации или переименования пользователей, базы данных Certification Log (Журнал сертификации, файл certlog.nsf). Эта база может быть репликой одноименной базы данных, хранящейся на другом сервере домена. Создавать такую базу обязательно, а способы ее создания подробно описаны в главе 3;
- О выделение административного сервера для каждой требующей этого базы данных домена. Базу данных, для которой не предусмотрено административного сервера, нельзя в дальнейшем модифицировать в рамках общего процесса администрирования.

Чтобы создать новую реплику существующей базы данных Certification Log, выполните следующие действия:

1. Запустите программу Domino Administrator на любой рабочей станции и войдите в систему по учетной записи пользователя, имеющего право создавать новые реплики базы данных на соответствующем сервере.
2. Щелчком по вкладке **Files** (Файлы) выведите экран, аналогичный показанному на рис. 4.11.

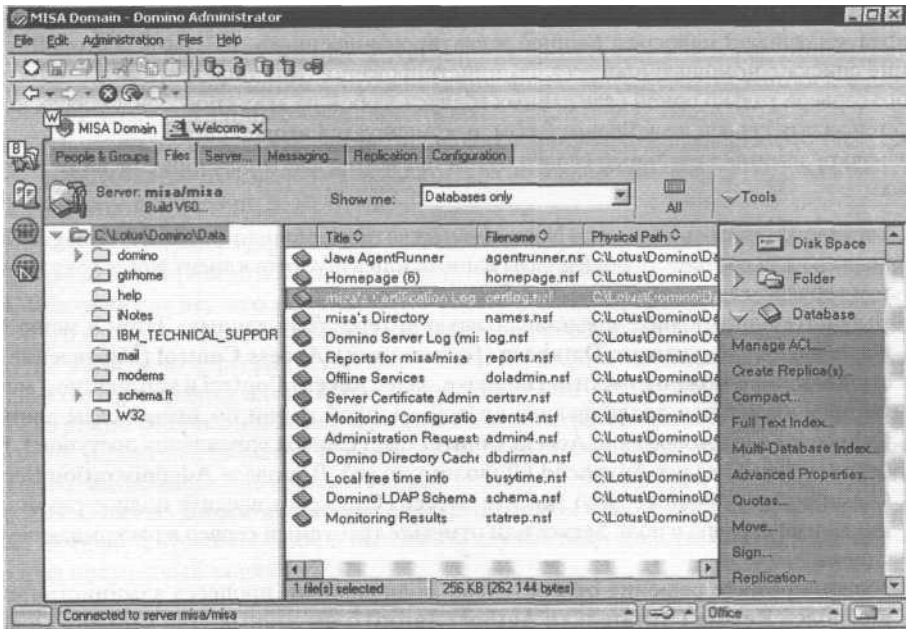


Рис. 4.11. Экран **Files** показывает папки и файлы, находящиеся в папке данных выбранного сервера, а также предоставляет средства для работы с ними

3. На панели **Bookmarks** (Закладки), расположенной в левой части экрана, выберите любой работающий в данный момент (и доступный) сервер, на котором существует копия базы данных **Certification Log**. Можно щелкнуть по значку домена, затем по значку требуемого сервера - имя выбранного сервера будет отображено ниже язычков вкладок в верхней части экрана. На экране появятся имена файлов, присутствующих в соответствующем каталоге данных.
4. Укажите базу данных **Certification Log** в списке файлов, после чего откройте диалоговое окно **Create Replica(s)** (Создание реплики). Существует три различных способа выполнения этой операции: можно либо воспользоваться пунктом **Create Replica(s)** на панели **Tools** (Программные инструменты), либо последовательно выбрать **New** (Новый) и **Replica(s)** (Реплика) в меню **File** (Файл) или в контекстном меню, появляющемся при щелчке правой кнопкой мыши на строке в списке для базы данных **Certification Log**.
5. В диалоговом окне **Create Replica** отметьте имена серверов, для которых планируется создание реплики. Если имя сервера в списке отсутствует, щелкните по пункту **Other** (Другие серверы) и либо введите имя сервера, либо выберите его из предложенного списка, после чего щелкните по кнопке **ОК**. При этом не рекомендуется изменять путь или имя файла для новой реплики базы данных. На каждом сервере реплика должна находиться в главном каталоге данных и соответствовать файлу с именем **certlog.nsf**. Выбрав все необходимые серверы, щелкните по кнопке **ОК**. Во время последующих циклов репликации процесс администрирования создаст новую реплику на всех указанных серверах, а процесс репликации наполнит эти реплики данными из уже существующих документов.

Существует два способа назначения административного сервера для базы данных. Первый предусматривает непосредственное редактирование списка ACL базы, а второй - изменение списка с помощью процесса администрирования. Для определения административного сервера только одной базе данных годится любой из этих способов. Однако, когда требуется задать сервер нескольким базам, рекомендуется второй способ.

Назначьте административный сервер путем прямого редактирования списка ACL базы данных:

1. Зарегистрируйтесь в клиенте Notes в качестве пользователя с правом **Manager** (Менеджер) для соответствующей базы данных или запустите клиент Notes локально на том сервере, где хранится нужная база данных.
2. Выберите или откройте представляющую интерес базу данных. Затем в меню **File** последовательно укажите **Database** (База данных), **Access Control** (Управление доступом). Либо можно отметить **Database**, далее **Access Control** в контекстном меню, которое выводится после щелчка правой кнопкой мыши по значку базы данных.
3. Откроется диалоговое окно **Access Control List** (Список управления доступом). Выберите в нем вкладку **Advanced** (Дополнительно). В разделе **Administration Server** (Административный сервер) задайте **Server** (Сервер) и введите полное различающееся имя сервера в поле **Server** или отметьте требуемый сервер в раскрывающемся списке.
4. Теперь примите решение относительно модификации процесса администрирования полей **Reader** (Читатель) и **Author** (Автор) базы данных. Для каталога Domain Directory и других баз данных, которые не предусматривают использования этих полей, определите **Do not modify Names fields** (Не изменять поля имен), а для всех прочих баз данных - **Modify all Reader and Author fields** (Изменять все поля Reader и Author). После выполнения указанных операций щелкните по кнопке OK.

Чтобы посредством процесса администрирования назначить административный сервер для модификации списков ACL одной или нескольких баз данных, выполните следующие действия:

1. Зарегистрируйтесь в программе Domino Administrator с помощью идентификационных данных пользователя с уровнем доступа **Manager** к соответствующей базе данных. На панели **Bookmarks** выберите сервер, где хранится интересующая вас база данных.
2. На экране **Files** (Файлы) укажите одну или большее число баз данных. На последующих этапах будет определен административный сервер и принято решение относительно модификации записей полей **Reader** и **Author** для выбранных баз. Таким образом, на настоящем этапе задаются только те базы данных, которые должны характеризоваться одинаковыми параметрами в обоих полях.
3. На панели **Tools** раскройте пункт **Database** и выберите **ACL Management** (Управление списком ACL) либо перейдите в меню **Files** и выберите **Access Control**, затем **Management** (Управление).
4. Появится диалоговое окно **Multi ACL Management** (Управление несколькими списками ACL), где нужно выбрать вкладку **Advanced**, а затем воспользоваться пунктом **Modify Administration Server settings** (Модификация параметров административного сервера). Укажите **Server** и введите полное различающееся имя того сервера, который планируется применять в качестве административного, или выберите его в раскрывающемся списке.

5. Для каталога Domain Directory и любых других баз данных, не предусматривающих наличия полей **Reader** и **Author**, следует сбросить флажок **Modify fields of type Reader and Author** (Модификация полей типа Reader и Author), а для всех остальных баз данных - установить его.
6. Щелчком по кнопке ОК закройте диалоговое окно **ACL Management**. Если для каких-то баз данных намечается задать другие параметры, выберите такие базы и повторите шаги с 3 по 5.

На основе контроля записей базы данных Administration Requests (Административные запросы) можно проверить правильность функционирования процесса администрирования. Вскоре после первого запуска новый сервер должен сформировать запросы для занесения его номера сборки, числа центральных процессоров и информации об операционной системе в документ сервера (Server document). Появление такого запроса означает, что на данном сервере процесс администрирования протекает нормально.

Если режим репликации между сервером и административным сервером каталога Domain Directory установлен должным образом, последний обязан обработать запрос в течение нескольких часов после занесения его в собственную реплику базы данных Administration Requests. Ответ на запрос в этой базе данных продемонстрирует правильность работы процесса администрирования (или, в противном случае, безуспешную попытку сформировать ответ на полученный запрос).

Установка менеджера агентов

Управление агентами - это серверная задача, заключающаяся в регулировании функционирования агентов на сервере. Агенты могут значительно загрузить сервер, поэтому следует заранее планировать выделение им ресурсов. Кроме того, агенты способны выйти из-под контроля сервера - нужно предусмотреть возможность при необходимости завершить работу агента принудительно. Менеджер агентов не позволяет им завладеть всеми ресурсами компьютера.

Менеджер агентов автоматически запускается на любом сервере, поскольку параметр **Amgr** присутствует в переменной **Servertasks** во всех файлах **notes.ini** серверов. Остановить менеджера агентов можно командой **tell amgr quit** консоли сервера, а перезапустить - командой **load amgr**.

Конфигурирование менеджера агентов производится в двух местах документа сервера. Во-первых, в разделе **Agent Restrictions** (Ограничения для агентов) вкладки **Security** (Безопасность). Так, в этом разделе указываются пользователи, имеющие возможность запускать различные агенты на данном сервере (назначение соответствующих полей обсуждалось в главе 3).

Во-вторых, на вкладке **Agent Manager** (Менеджер агентов), которая находится на вкладке **Server Tasks** (Задачи сервера). Поля вкладки позволяют конфигурировать параметры менеджера агентов. Следует отметить, что агенты по-разному функционируют в дневное и ночное время (рис. 4.12), причем днем, когда сервер активно обслуживает различных пользователей, деятельность агентов заметно ограничена. Пользователю разрешено изменять число работающих на сервере агентов, а также максимальный объем памяти, выделяемый каждому из них. Тем не менее на практике не рекомендуется менять уже введенные в поля значения, если только не предусматривается установка специального агента, предъявляющего особые требования к серверу, или подобные условия не выдвигаются самими пользователями.

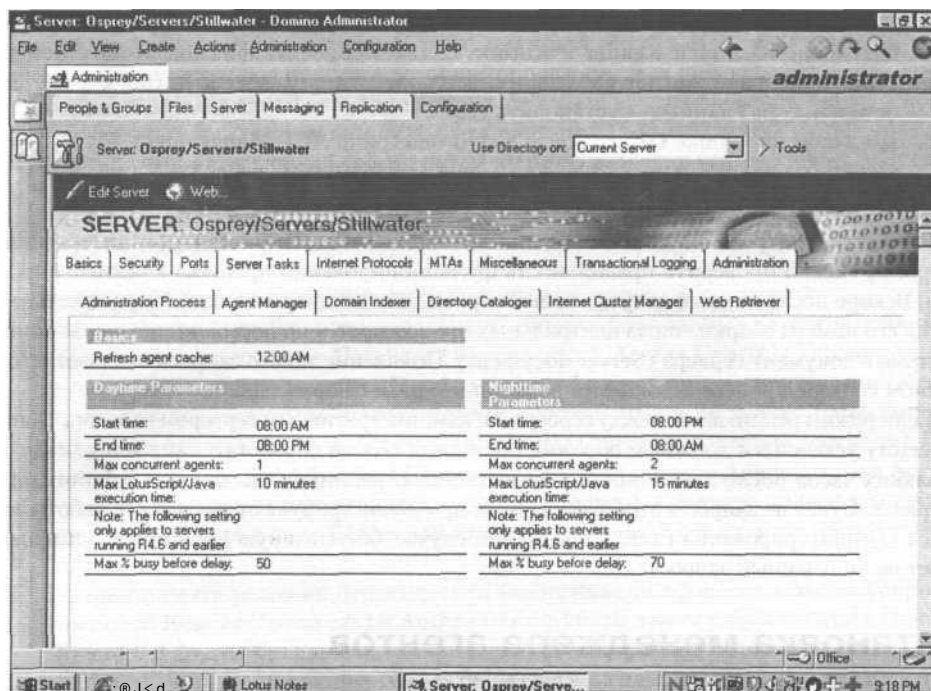


Рис. 4.12. Менеджер агентов обеспечивает разные режимы управления агентами в дневное и ночное время. Разрешается определить дневные и ночные часы для работы агентов, а также характер их деятельности в каждый период

Настройка процедуры регистрации транзакций

Как и для первого сервера, в этом случае требуется предварительно принять решение относительно необходимости выполнения дополнительным сервером *функции регистрации транзакций*, что зависит от конфигурации аппаратных средств каждого сервера. Специалисты компании Lotus настоятельно рекомендуют вводить названную функцию на всех серверах, поскольку она позволяет получить целый ряд преимуществ, в том числе улучшить показатели целостности баз данных, сократить время ответа пользователям и повысить показатели быстродействия, а также обеспечить более надежное функционирование системы в целом и снизить вероятность возникновения отказов. Тем не менее выполнение процедуры регистрации транзакций оказывает определенное влияние на резервное копирование, например на использование утилит *fixup* и *compact*. Поэтому, прежде чем разрешить процедуру регистрации транзакций, важно правильно оценить все последствия ее применения. Подробное описание процесса настройки данной процедуры, а также возможных последствий ее запуска приводится в главе 14.

Специальные серверы

Если сервер предназначен для определенных целей, может потребоваться провести его конфигурирование индивидуально. Специальные функции, которые должен выполнять сервер, и рекомендации по его настройке в деталях обсуждаются в последующих разделах.

Серверы почтовой службы

Серверы почтовой службы являются частыми «гостями» в базах данных почтовой службы пользователей. Базы данных почтовой службы системы Notes выполняют типовые почтовые функции, а также функции управления расписанием и управления задачами. Многие пользователи с помощью этих функций постоянно создают почтовые сообщения, задачи и записи в календарном расписании. Одновременно осуществляется прием поступающих в их адрес почтовых сообщений и сохранение копий пересылаемых сообщений, что приводит к быстрому росту соответствующих баз данных.

Многие организации в наши дни выделяют для почтовой связи отдельный сервер (или даже несколько серверов). Эта практика стала настолько привычной, что один из вариантов сервера Domino, сервер Domino Mail Server, специально предназначен для решения подобных задач, а наиболее типичные тесты NotesBench неизменно показывают широкое распространение Mail.

Специальная настройка сервера почтовой службы предполагает решение нескольких вопросов, каждый из которых подробно освещается в различных главах настоящей книги:

- О создание нескольких баз данных Outgoing Mail (Исходящие почтовые сообщения) - см. главу 8;
- О настройка совместно используемого почтового сервера - см. главу 8;
- О настройка функций почтовой связи в сети Internet, в том числе протоколов SMTP, POP3, ШАР и LDAP - см. главы 8, 11, 16 и 17;
- О запуск службы HTTP, чтобы пользователи почтовой службы имели доступ к своим базам данным (почтовой службы) с помощью браузера - см. главу 5;
- О настройка процедуры Message Tracking (Отслеживание сообщений) - см. главу 8;
- О настройка базы данных Resources (Ресурсы), позволяющая планировать выделение корпоративных ресурсов, скажем помещения для конференций, - см. главу 8;
- О передача некоторых функций, например функции просмотра каталогов, другим серверам - см. главу 11.

Серверы приложений

Серверы приложений широко применяются в системах Notes/Domino (за исключением задач, связанных с работой почтовой службы, поддержкой календаря и управления задачами). Приложения могут иметь самые различные назначения: от поддержки дискуссий и репозиториях с документами до поддержки сложных приложений обслуживания корпоративных рабочих потоков. Серверы приложений, как правило, исполняют задачи NNTP, HTTP и DIIOP, поскольку приложения системы Notes в наши дни иницируются браузерами и новыми клиентскими программами так же часто, как клиентами самой системы Notes. Более подробно описание задач HTTP и DIIOP будет представлено в главе 15.

Если ни одно из приложений сервера не предусматривает выполнения задач sched и calconn, их легко отменить. Эти задачи обычно поддерживают функции группового календаря, которые часто берут на себя серверы почтовой службы. Для завершения таких задач служат команды `tell sched quit` и `tell calconn quit` консоли сервера. Чтобы исключить использование данных функций в будущем, достаточно удалить соответствующие параметры из переменной `Servertasks` в файле `notes.ini` сервера.

Серверы коммутируемого доступа и сквозные серверы

Организациям, имеющим большое число мобильных пользователей, которые связываются с серверами через брандмауэры, имеет смысл предусмотреть один или несколько серверов специально для управления подобным трафиком. Намотившиеся тенденции к активному использованию сети Internet и унификации связей привели к заметному росту потребности в серверах подобного типа. Идея в данном случае заключается в том, чтобы выделить один или несколько серверов для приема всего входного модемного трафика. Пользователи, традиционно обращающиеся к серверу коммутируемого доступа, смогут по-прежнему направлять вызовы на сервер и применять его в качестве сквозного для связи с собственным сервером почтовой службы и приложений, доступ к которому осуществляется только из локальной сети. При этом не требуется предоставлять прямой модемный доступ к серверу почтовой службы или серверу приложений - достаточно обратиться по телефону к одному из серверов, чтобы получить доступ ко всем остальным.

Серверы коммутируемого доступа и сквозные серверы обычно устанавливаются сегментированными, а их сегменты — непосредственно связанными с соответствующими модемами. На этих серверах можно отменить все задачи, за исключением `router`, `update`, `adminp` и `amgr`.

Если мобильные пользователи поддерживают местные реплики некоторых баз данных, следует внимательно рассмотреть вопрос о поддержке копий этих баз данных непосредственно на сервере коммутируемого доступа, что позволит выполнять репликацию только с таким сервером. Подобный подход приводит к заметному уменьшению трафика в локальной сети. Весьма вероятным кандидатом на подобное обслуживание может стать база данных `Directory Catalog` (Каталог перечня), которая предназначена для хранения разнообразных записей мобильных пользователей.

Концентраторы почтовой службы и репликации

При увеличении числа эксплуатируемых серверов свыше трех или четырех приходится позаботиться об организации эффективной топологии репликации и маршрутизации почтовых сообщений. Здесь существует опасность быстро достигнуть того состояния, при котором окажется весьма неразумным разрешать всем серверам проводить репликацию (а возможно, и маршрутизацию почтовых сообщений) и потребуются переход на топологию с радиальным концентратором (см. главы 7 и 8). По этой причине один (или большее число) из применяемых серверов может быть выделен в качестве *сервера концентратора*, который примет на себя функцию репликации (а может быть, и маршрутизации почтовых сообщений).

Сервер концентратора обычно строится на основе весьма мощного сервера, непосредственно не участвующего в процессе обслуживания пользователей (как правило, доступ к нему разрешен только администраторам) и обеспечивающего прямой доступ к себе для

всех прочих серверов. В такой ситуации пользователи с низкими уровнями приоритета доступа будут взаимодействовать только со своими серверами почтовой службы и приложений.

При большой нагрузке сервер концентратора обеспечивает протекание нескольких процессов репликации. В общем случае его можно настраивать на работу с несколькими (n) потоками репликации путем задания переменной `replicators=n` в файле `notes.ini` сервера. При появлении вопроса относительно числа подобных потоков на сервере концентратора обычно рекомендуется задавать не более двух на одном процессоре. В этих условиях однопроцессорный сервер способен обслуживать лишь два потока репликации, а сервер, имеющий два процессора, - четыре таких потока. Однако на практике редко возникает необходимость в таком количестве потоков репликации. Репликация серверов Domino реализована весьма эффективно, что позволяет перемещать огромные массивы данных между концентратором репликации и радиальными серверами репликации (см. главу 8).

При необходимости создания концентратора для почтовой связи ему, без сомнения, будут придаваться несколько баз данных Outgoing Mail (Исходящие почтовые сообщения, файл `mail.box`).

Если сервер концентратора становится своего рода перекрестком сетевых трафиков, возможно, понадобится организовать для него независимую высокоскоростную локальную сеть, связанную с остальными сетевыми компонентами посредством переключателя. И наконец, поскольку сервер концентратора становится единой точкой для возникновения общей неисправности, нужно строить его на основе сегментируемых (с помощью операционной системы) компьютеров. При этом сервер будет работать на одном из компьютеров, но в случае его отказа право управления дисковым массивом будет передано другому компьютеру (фактически передаются право управления данными системы Notes/Domino, IP-адрес отказавшего компьютера и имя соответствующего хоста). В такой ситуации временной интервал, необходимый для повторного запуска сервера Domino, не должен превышать нескольких минут.

Серверы с коллективным использованием браузера

В 1996 году, когда сеть World Wide Web только появилась, для большинства специалистов слово «браузер» было еще внове, не говоря уже о службе, предусматривающей совместное использование браузера. Именно этот подход был предложен специалистами компании Lotus в версии 4.0 системы Notes. Он позволял пользователям системы Notes общаться с сетью World Wide Web через специальные серверы, которые в то время еще не носили название Domino. Пользователи системы Notes не работали с протоколом IP локально и не нуждались в услугах дополнительного браузера. Сервер, предусматривавший применение службы с коллективно используемым браузером (получившим имя Web Retriever), в дальнейшем был назван сервером InterNotes.

Тогда пользователи системы Notes имели возможность просто щелкнуть по адресу URL или обратиться к соответствующему диалоговому окну, а система Notes обеспечивала автоматическую пересылку адреса URL на сервер InterNotes, который в свою очередь переправлял его на Web-сервер. При необходимости Web-сервер возвращал документ HTML обратно на сервер InterNotes, который преобразовывал его в документ системы Notes и запоминал в базе данных Web Navigator сервера InterNotes. В дальнейшем этот сервер отсылал сохраненные документы запрашивающим пользователям.

Служба Web Retriever позволяла эксплуатировать браузеры с относительно небольшими скоростями передачи данных, при этом те пользователи, которые взаимодействовали

с сетью с помощью стандартного браузера, обычно на нем и останавливали свой выбор. Тем не менее браузер обладал целым рядом преимуществ, не последним из которых было запоминание полученных Web-страниц в совместно используемой базе данных системы Notes. Это означало, что все группы пользователей системы Notes могли обращаться к накопленным общими усилиями данным из сети Internet, причем база данных Web Navigator содержала несколько агентов, что усиливало положительный эффект при работе с ней.

В наши дни пользователи системы Notes в большинстве своем являются одновременно пользователями локальных сетей с протоколом IP, непосредственно связанных с сетью Internet, и располагают собственными браузерами. Так, уже начиная с версии 4.1 клиенты системы Notes получили функции браузера. Однако и сейчас еще можно встретить сервер со службой Web Retriever, хотя подавляющая часть пользователей о нем практически забыла.

И все же, эта служба существует и применяется серверами Domino, поскольку демонстрирует целый ряд полезных функций, привлекательных для некоторых организаций. Например, с ее помощью администратор может не разрешить пользователям выводить страницы с запрещенных для просмотра Web-сайтов. Кроме того, базе данных Web Navigator весьма просто придать требуемую структуру, а сервер Domino, поддерживающий службу Web Retriever, представляет собой совсем недорогое средство для организации эффективного брандмауэра, не требующего больших усилий при настройке. Поэтому компаниям, вводящим жесткие ограничения на просмотр Web-сайтов для своих пользователей и сильно обеспокоенным возможностью несанкционированного проникновения из сети Internet в их внутреннюю корпоративную сеть, служба Web Retriever вполне подойдет.

При желании ознакомиться с вопросами настройки и конфигурирования службы Web Retriever на сервере Domino (а также со способами его использования клиентами системы Notes) рекомендуется обратиться к материалам главы 25 «желтой книги» компании Lotus, поставляемой совместно с пакетом программного обеспечения.

Серверы сети Internet

Службы HTTP и NNTP могут быть приданы практически любому серверу приложений Domino, однако в большей части случаев подобная настройка имеет своей целью обеспечить доступ к определенным приложениям для внутренних пользователей, которые не располагают клиентами системы Notes. При необходимости сделать эти приложения доступными для внешних пользователей не следует просто открывать брандмауэр и подвергать атакам сервер Domino. Более удачным в данном случае оказывается выделение одного или двух серверов с внешней стороны брандмауэра и соединение их непосредственно с сетью Internet. Такие серверы обычно относятся к числу корпоративных Web-серверов и серверов новостей (News server). На них следует размещать не все базы данных, а только те, к которым можно предоставить широкий доступ.

При настройке подобных серверов надо их тщательно защищать, чтобы не допустить посторонних лиц к конфиденциальной информации. Эти серверы должны поддерживать репликацию с внутренними серверами, причем необходима избирательная репликация, предполагающая обмен документами, в которые включена только общедоступная информация.

Если все-таки придется открыть брандмауэр и предоставить внешним пользователям доступ к внутренним серверам (непосредственно или через прокси), встанет проблема их всесторонней защиты. На практике подобная ситуация обычно возникает для серверов почтовой службы компании.

Серверы-брандмауэры

Большая часть компаний весьма озабочена тем, что между сетью Internet и их частными сетями (или сетями intranet) возможен неконтролируемый обмен информацией, причем их опасения в большей части случаев вполне оправданы. Для решения возникшей проблемы компании создают брандмауэры, содержащие маршрутизаторы с фильтрацией пакетов и хосты, а также различные прокси-серверы, которые позволяют блокировать неавторизованный внешний трафик в частную локальную сеть.

К прокси-серверам, используемым в режиме брандмауэров, относятся прокси-серверы уровня приложений, предназначенные для обработки сетевых пакетов, которые формируются определенными приложениями. Следует особо отметить, что все серверы Domino в состоянии функционировать в качестве таких серверов приложений. При настройке сквозной сервер Domino всегда конфигурируется как прокси-сервер уровня приложений.

Если брандмауэр разделяет сеть Internet и частную сеть компании, доступ к сквозному серверу Domino обеспечивается из сети Internet, причем такой сервер обладает правом отправлять (и получать) информацию через любые фильтрующие маршрутизаторы на серверы Domino, расположенные по другую сторону от этих маршрутизаторов. Сервер-брандмауэр может применяться для предоставления пользователям системы Notes доступа к внутренним серверам Domino непосредственно из сети Internet. Для этого необходимо выполнить следующие операции:

1. Назначить сервер-брандмауэр сквозным в документе местоположения (Location document) для сети Internet.
2. Предоставить пользователям сети Internet право посредством этого сервера взаимодействовать с другими серверами Domino в документе сервера (Server document), созданном для брандмауэра.
3. Разрешить пользователям сети Internet доступ к внутренним серверам через сквозной сервер в документах сервера, сформированных для внутренних серверов.
4. Открыть порты с номером 1352 (общезвестный порт для трафика Notes и Domino) на всех маршрутизаторах фильтрации пакетов, находящихся между брандмауэром и внутренними серверами.

Слабо загруженный общедоступный Web-сервер Domino или NNTP вполне способны справиться с функциями брандмауэра. Эти функции может на практике выполнять и сервер почтовой службы Domino, оказывающий почтовые услуги внешним пользователям в сети Internet.

Серверы каталога

Процедура установки сервера Domino обеспечивает и автоматическую настройку основных служб каталога Domino. Так, во время установки первого сервера (см. главу 3) создается база данных каталога домена (файл names.nsf). При установке дополнительных серверов предусматривается репликация каталога домена на все вновь создаваемые серверы. Фоновая репликация между серверами позволяет синхронизировать все копии каталога домена.

Каталог Domino предоставляет ряд высокоэффективных служб, весьма полезных для пользователей и серверов. Он также дает пользователям возможность достаточно просто обмениваться почтовыми сообщениями и производить поиск информации о почтовых

адресах. Кроме того, каталог помогает серверам быстро находить друг друга, определять службы, поддерживаемые каждым сервером, а также получать маршруты для передачи почтовых сообщений пользователям и базам данных.

Замкнутая однодоменная система, не имеющая мобильных пользователей, может ограничиться одной службой каталога. Однако, когда речь идет о системе более сложной, часто возникает необходимость в *дополнительных службах каталога*:

- **Server directory catalogs** и **Mobile directory catalogs** (Каталоги перечня серверов и мобильных пользователей). Соответствует специальной базе данных системы Notes (на основе файла dircat6.ntf), которая накапливает наиболее часто используемые данные одного или большего числа каталогов Domino в едином облегченном каталоге, оптимизированном для быстрого просмотра. Каталог перечня сервера обычно хранится на сервере Domino, а каталог перечня мобильных пользователей - на рабочей станции пользователя системы Notes;
- **Directory assistance** (Поддержка каталога). Каталог дает возможность пользователям системы Notes просматривать несколько каталогов Domino и LDAP. Он также помогает серверам аутентифицировать с помощью идентификационных данных, находящихся в каталогах LDAP, Web-пользователей. Кроме того, позволяет серверу Domino LDAP предоставлять сведения относительно клиентов LDAP другим каталогам LDAP;
- **Dedicated directory servers** (Выделенные серверы каталогов). По умолчанию серверы почтовой службы Domino предоставляют службы просмотра каталогов пользователям почтовой службы системы Notes. Имеется также возможность перемещать эти службы на другие серверы, чтобы высвободить сервер почтовой службы и увеличить его скорость его работы (для обслуживания большего числа клиентов), тогда как специально выделенный сервер каталогов будет обеспечивать быстрый просмотр каталогов;
- **LDAP directory services** (Службы каталогов LDAP). LDAP - это стандартный протокол для предоставления доступа к службам каталога, широко распространенный в сети Internet. Сервер Domino, применяющий службу каталогов LDAP, становится по существу сервером каталогов LDAP и может разрешить клиентам LDAP читать и записывать информацию в каталоге Domino. Он также в состоянии производить поиск в других каталогах LDAP и снабжать данными относительно клиентов LDAP другие каталоги LDAP.

Ниже перечислено несколько ситуаций, в которых может потребоваться воспользоваться дополнительными службами каталогов:

- предоставление пользователям системы Notes наиболее быстрой службы поиска имен (предполагается установка сервера перечня каталога);
- наличие мобильных пользователей системы Notes, которые не имеют постоянной связи с сервером Domino (имеется в виду хранение каталога перечня мобильных пользователей у самих пользователей);
- присутствие множества пользователей почтовой службы, создающих большую нагрузку на сервер почтовой службы (речь идет о добавлении одного или нескольких дополнительных серверов каталога);
- наличие нескольких доменов Domino (при таких условиях необходим вспомогательный каталог Domino, открывающий домены для пользователей из других доменов);

- О потребность в аутентификации различных клиентов сети Internet (Web/IIOP, POP3, IMAP, NNTP и LDAP), а также клиентов системы Notes. В этом случае легко отследить клиентов разного типа путем размещения их в различных базах данных каталога - например, пользователей системы Notes заносить в базу данных Domino Directory (файл names.nsf), а пользователей не-Notes - в один или несколько других каталогов (например, в файл inetnames.nsf). При организации доступа к этим каталогам всем пользователям системы Notes для проведения поиска по имени нужны вспомогательный каталог и каталог перечня;
- О необходимость обслуживания клиентов почтовых служб POP3 или ШАР (для организации доступа этих клиентов к базе данных Domino Directory приходится организовывать службу каталога LDAP).

На практике рекомендуется устанавливать:

- О каталог перечня даже в том случае, когда планируется организовать администрирование только одного небольшого домена Domino;
- О каталог перечня и вспомогательный каталог, если необходимо организовать администрирование нескольких взаимосвязанных доменов Domino или предоставить службу LDAP;
- О один или несколько выделенных серверов каталогов при условии, что придется обслуживать многих пользователей почтовой службы;
- О службу LDAP, если намечается обслуживать клиентов не-Notes или с помощью каталога LDAP аутентифицировать Web-пользователей.

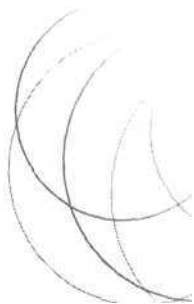
Более подробно процедуры установки каждой службы каталога описаны в главе 11.

Каталог домена и служба поиска

Начиная с версии 5 сервер Domino обладает возможностями поиска на основе функции Domain Search (Просмотр домена), которые позволяют пользователям просматривать весь домен Domino и получать сведения из баз данных системы Notes и файловых систем. Для установки службы Domain Search необходимо выделить один или несколько серверов, которые будут в дальнейшем применяться в качестве серверов Domain Catalog (Каталог домена). Такие серверы обеспечивают поддержку каталога баз данных в домене, а также полнотекстовой индексации (названной Domain Index). Служба Domain Index предусматривает работу баз данных и файловых систем, выбранных для индексации. Пользователи могут производить поиск во вложенных файлах документов, а также в файлах индексированных файловых систем, пользуясь текстовыми фрагментами и индексированными базами данных, присутствующими в этих документах. Заложенный механизм поиска позволяет выявлять только те документы, вложения и файлы, на которые пользователь имеет право доступа **Reader** (Читатель) и выше.

Серверы Domain Catalog/Search Server (Сервер каталога домена/поиска в домене) должны располагать большой вычислительной мощностью, большой оперативной памятью и значительным дисковым пространством. Задачи каталогизации (которая запускается в 1 час ночи) и индексации (которая по умолчанию инициируется с интервалом в один час) предполагают отвлечение существенного объема ресурсов процессора и оперативного запоминающего устройства. Полнотекстовые индексы обычно занимают внушительные пространства на диске, поэтому специалисты компании Lotus настоятельно

советует устанавливать для сервера каталога домена операционную систему Windows NT, работающую на компьютере с процессором Pentium 266 МГц и выше, оперативной памятью не менее 256 Мб и свободным пространством на диске (для полнотекстовой индексации), составляющим не менее 75% от суммарного размера индексируемых баз данных и файлов. Однако это лишь минимальные требования. Так, в других публикациях для сервера Domain Catalog рекомендуются только многопроцессорные компьютеры, а если в домене не менее восьми серверов, предлагается освободить сервер Domain Catalog от выполнения всех прочих задач. Кроме того, целесообразно формировать кластер для сервера Domain Catalog, чтобы повысить надежность и отказоустойчивость, а также обеспечить балансировку нагрузки. Подробно процедура настройки сервера Domain Catalog/Search Server рассмотрена в главе 7.



ПРОЦЕДУРА РЕГИСТРАЦИИ ПОЛЬЗОВАТЕЛЕЙ И НАСТРОЙКИ КЛИЕНТОВ

В данной главе рассмотрены вопросы, связанные с проведением установки учетной записи типичного пользователя системы Notes, то есть обычного сотрудника компании, который ежедневно приходит в офис и обращается к почтовой службе системы Notes и ее базам данных, но далеко не всегда работает со средствами этой системы, предназначенными для взаимодействия с сетью Internet. Более подробно речь о мобильных пользователях системы Notes и тех пользователях, которые применяют клиент системы Notes для обращения к серверам почтовой службы, каталогам и новостям сети Internet, пойдет в главе 6.

Ниже описаны операции, которые придется последовательно выполнить при определении учетных записей для новых пользователей (то есть при их установке):

1. Создание сертификатора для организационной единицы пользователей (если планируется введение сертификатора, но он пока не задан).
2. Добавление альтернативных языков для сертификаторов организации (О) и организационной единицы (OU), если планируется работа с альтернативными именами.
3. Выбор профилей установки для пользователей (User Setup Profiles) в R5 или соответствующей политики в R6.
4. Задание определяемого по умолчанию списка управления исполнением (Execution Control List) и подписывание ранее не подписанных баз данных.
5. Установка процедуры восстановления идентификационных данных и паролей.
6. Регистрация пользователей.
7. Установка и конфигурирование клиента Notes на компьютерах пользователей.

Большая часть из указанных операций необязательна для исполнения. Однако многие из них позволяют заметно уменьшить объем работ и затраты времени, поэтому настоятельно рекомендуется не пренебрегать ими. Ниже представлены примеры, из которых понятно, какую пользу может принести своевременное проведение этих операций:

- О задание профилей установки или политик пользователей позволит сформировать единое место, в котором определены различные параметры (в противном случае такие параметры потребуются указывать индивидуально в процессе конфигурирования для каждого пользователя системы Notes);
- О операции по восстановлению идентификационных данных/пароля облегчают жизнь в ситуациях, когда пользователи забывают свои пароли или теряют файлы с идентификационными данными;

- О благодаря применению списка управления исполнением удастся ограничить число операций, которые осуществляются программами на рабочей станции пользователя (и тем самым защитить систему от почтовых вирусов и подобных сюрпризов).

Однако возникает одна небольшая проблема, поскольку установку функций восстановления идентификационных данных/пароля нужно провести еще до регистрации пользователей - при такой последовательности действий восстановленная информация в момент регистрации автоматически попадет в файл идентификационных данных пользователя. В противном случае придется пересылать информацию о восстановленных идентификационных данных пользователям, которым в свою очередь надо будет принимать эту информацию, а затем по электронной почте отправлять копию своего файла идентификационных данных в специальную базу.

Очевидно, что подобный процесс может быть автоматическим только наполовину, причем пользователи, как правило, слишком заняты собственными проблемами, чтобы активно участвовать в нем и помогать администраторам. В ряде случаев пользователи просто боятся щелкнуть не по той кнопке и постоянно обращаются за консультациями. Именно по этим причинам рекомендуется сначала провести установку функции восстановления идентификационных данных/пароля.

Тем не менее лучше все-таки предварительно провести установку по крайней мере административных пользователей и только потом переходить к активизации указанной функции. Дело в том, что открытые ключи администраторов, служащие для восстановления идентификационных данных и паролей, должны быть доступны на момент разрешения функции восстановления идентификационных данных/пароля. Поэтому в данной главе операции установки пользователей рассматриваются в следующем порядке:

- О создание профилей установки пользователей или политик (сначала формируются профили или политики для администраторов);
- О определение списка управления исполнением в режиме по умолчанию;
- О задание сертификатора для организационной единицы;
- О выбор альтернативных языков;
- О регистрация основных параметров пользователей (с целью помочь в регистрации административных пользователей);
- О настройка функции восстановления идентификационных данных/пароля (после разрешения этой функции и назначения профилей для пользователей, не являющихся администраторами, можно начать регистрацию остальных пользователей);
- О установка и конфигурирование основных параметров для клиента системы Notes.

Создание профиля установки пользователей

Несмотря на то что профили пользователей версии R5 заменены политиками версии R6, мы все же рассмотрим создание профиля установки для пользователей, который продолжает действовать в версии R6 (хотя и не имеет всех возможностей соответствующих политик) и является весьма полезным средством, позволяющим заметно экономить усилия и время при регистрации каждого нового пользователя. Профиль унифицирует процесс установки учетных записей и дает возможность обновлять параметры рабочих станций существующих пользователей. Для установки профиля выполните следующие действия:

1. Запустите программу Domino Administrator и перейдите на вкладку **People & Groups** (Сотрудники и группы).
2. На панели **Servers** (Серверы) выберите тот сервер, на котором находится копия каталога Domain Directory, где предполагается задать требуемый профиль.
3. На панели **Tasks** (Задачи) укажите вид **Setup Profiles** (Профили установки) для соответствующего каталога домена. При этом на панель **Results** (Результаты) будут выведены уже существующие профили установки.
4. Щелкните по кнопке **Add Setup Profile** (Добавление профиля установки), расположенной на панели операций, находящейся выше панели **Results**, - на экране появится форма **User Setup Profiles** (Профили установки пользователей).
5. Заполните поля этой формы, после чего сохраните ее и закройте.

Ниже приводится перечень полей формы **User Setup Profiles**, находящихся на вкладке **Basics** (Основные параметры):

- **Profile name** (Имя профиля). В этом поле можно вводить любое информативное название. При регистрации новых пользователей определенное на данном этапе название будет присутствовать в списке доступных профилей;
- **Internet browser** (Браузер сети Internet). Здесь следует задавать браузер системы Notes, который активизируется при щелчке или вводе пользователем адреса URL. Одновременно будет заполняться одноименное поле в документах местоположения (Location document) пользователя. Имеются следующие варианты:
 - **Notes**. Клиент Notes обеспечивает возможности браузера, соответствующего стандарту HTML 4.0;
 - **Notes with Internet Explorer**. Браузер (обозреватель) Internet Explorer запускается в окне клиента Notes;
 - **Netscape Navigator**. Браузер Netscape Navigator запускается вне окна клиента Notes;
 - **Microsoft Internet Explorer**. Браузер Microsoft Internet Explorer запускается вне окна клиента Notes;
 - **Other**. При выборе данного варианта разрешается применить любой сторонний браузер, однако задать его в параметрах профиля нельзя;
- **Directory server** (Сервер каталога). В это поле надо внести полное различающееся имя сервера, с помощью которого будет производиться поиск имен;
- **Catalog/Domain Search server** (Сервер поиска каталогов/домена). Поле предназначено для ввода полного различающегося имени сервера, посредством которого пользователь намерен осуществлять поиск в домене;
- **Retrieve/open pages** (Извлечение/открытие страниц). В данном поле должен быть оговорен способ вывода Web-страниц. Такая необходимость возникает только в случае, если в поле **Internet browser** ранее был задан вариант **Notes**;
- Э **from InterNotes server** (С сервера InterNotes). Поле требуется заполнять для пользователей, которые собираются обращаться не к собственным браузерам, а к серверу InterNotes в сети Domino;
- **from Notes Workstation** (С рабочей станции системы Notes). Поле заполняется для пользователей, которые уже имеют собственные браузеры и будут их применять;
- **no retrievals** (Без извлечения). Это поле должно быть заполнено для тех пользователей, которые не планируют взаимодействовать со службой World Wide Web.

Одновременно следует производить заполнение полей вкладки **Databases** (Базы данных). В перечисленных ниже полях можно вставить ссылки на базы данных - откройте базу данных, выполните **Edit=*Copy as Link=>Database Link** (Редактирование=>Копирование ссылки=>Ссылка базы данных), затем поместите курсор в нужное поле и отметьте **Edit=>Paste** (Редактирование=>Вставка):

- **Default databases added to bookmarks** (Базы данных, добавленные по умолчанию в закладки). В этом поле требуется указать ссылки на все базы данных, которые намечено добавить в рабочую область пользователей;
- **Create As new replicas on user's machine** (Создание новой реплики на компьютере пользователя). Здесь надо определить ссылки на все базы данных, которые будут реплицированы на рабочих станциях пользователей;
- **Mobile directory catalogs** (Перечень мобильных каталогов). В данном поле задаются линии связи базы данных для ссылки на перечни мобильных каталогов, реплицируемых на рабочих станциях пользователей.

Затем необходимо заполнить раздел **Default Passthru Server** (Сквозной сервер по умолчанию) вкладки **Dial-up Connections** (Коммутируемые соединения). Поля этого раздела определяют используемый по умолчанию сквозной сервер. Задаваемое имя сервера появится в поле **Passthru Server** (Сквозной сервер) в документах местоположения (Location document) пользователей. Также будет сформирован и записан в персональные адресные книги пользователей документ прямого коммутируемого соединения для сквозного сервера. Речь идет о следующих полях для сквозного сервера, активизируемого по умолчанию:

- **Server name** (Имя сервера) - сюда вводится полное различающееся имя;
- **Country code** (Код страны) - в это поле вносится код страны (при его наличии);
- **Area code** (Код области) - здесь указывается код области (при его наличии);
- **Phone number** (Номер телефона) - в данное поле вводится местный телефонный номер (при его наличии).

Теперь можно переходить к заполнению раздела **Default Connections to Other Remote Servers** (Соединения по умолчанию для других удаленных серверов) той же вкладки. Поля раздела позволяют задать параметры соединения с удаленными серверами. При установке пользователя на основе профиля система Notes создаст документ прямого коммутируемого соединения для каждого из перечисленных серверов.

Во всех полях можно делать несколько записей, разделяя их запятыми, точками с запятой или (для перехода на следующую строку) символом абзаца («возврат каретки»).

Записи следует вносить во все поля для каждого сервера, причем в одинаковых полях записи должны быть однотипными (например, записи для первого сервера надо помещать на первой позиции в поле, записи для второго сервера - на второй и т.д.). Итак, поля для удаленных серверов:

- **Server names** (Имена серверов) - в этом поле назначаются полные различающиеся имена;
- **Country codes** (Коды страны) - поле предназначено для ввода кодов стран;
- **Area codes** (Коды области) - здесь указываются коды областей;
- **Phone number** (Номер телефона) - в данное поле вносятся местные телефонные номера.

Теперь наступает очередь заполнения вкладки **Accounts** (Учетные записи). В полях этой вкладки можно задать ту информацию, которая потребуется системе Notes для связи

с серверами сети Internet. Для любой содержащейся на вкладке учетной записи программа установки рабочей станции создаст документ учета (Account document) в персональных адресных книгах пользователей.

В каждом поле допускается помещать несколько записей, разделенных запятыми, точками с запятой или символами «возврат каретки».

Записи надо вносить во все поля для каждого сервера, делая их однотипными для одинаковых полей (например, записи для первого сервера должны находиться на первой позиции в каждом поле, записи для второго сервера - на второй и т.д.):

- **Account Names** (Имена учетных записей) - в этом поле можно задавать информативные названия, которые планируется придать документам учета, создаваемым в персональных адресных книгах пользователей;
- **Server Addresses** (Адреса серверов) - в данное поле следует ввести полные различающиеся имена хостов или IP-адреса для каждого учетного сервера;
- **Protocols** (Протоколы) - здесь надо указывать протокол сети Internet для каждого учетного сервера (например, LDAP, POP, IMAP или SMTP);
- **Use SSL connection** (Использование соединения SSL) - в этом поле требуется задать для каждой перечисленной учетной записи значение 0 (без использования протокола SSL для формирования соединения) или 1 (для соединения с сервером по протоколу SSL).

Далее заполняются поля вкладки **Name Server** (Сервер имен) и определяется резервный сервер Domino, поиск которого предпримет система Notes в том случае, если не сможет обнаружить выделенный домашний сервер. Представленные ниже поля требуют заполнения только в случае необходимости:

- **Secondary TCP/IP Notes name server** (Вторичный сервер Notes для протоколов TCP/IP) - сюда вводится полное различающееся имя резервного (вторичного) сервера, доступного по протоколам TCP/IP;
- **Secondary TCP/IP host name or address** (Имя хоста или IP-адрес вторичного сервера TCP/IP) - в данном поле указывается полное различающееся имя или IP-адрес вторичного сервера;
- **Secondary NDS Notes name server** (Вторичный сервер Notes для службы NDS) - поле служит для задания полного различающегося имени резервного сервера, который является зарегистрированным объектом в каталоге имен сервера Novell Name Server;
- **Secondary NDS name server address** (Имя хоста или IP-адрес вторичного сервера NDS) - здесь вносится полное различающееся имя вторичного сервера в сети Novell.

Следующей заполняется вкладка **Applet Security** (Безопасность апплета). Надо иметь в виду, что апплеты Java могут инициировать сетевые соединения с другими компьютерами и организовывать с ними сеансы связи. В ряде случаев это создает потенциальную проблему в плане обеспечения безопасности, так что в нижеперечисленных полях стоит ограничить сетевой доступ к системе Notes из апплетов Java:

- **Trusted hosts** (Доверенные хосты) - хосты или домены, из которых допускается загрузка апплетов. Введите имена хостов, имена доменов и частичные или полные IP-адреса (например, 205.159.212*). Если оставить поле незаполненным, доверенными станут все хосты;

- **Network access for trusted hosts** (Сетевой доступ для доверенных хостов) - в этом поле следует задать уровень сетевого доступа из возможных вариантов:
 - **Disable Java** (Запретить апплеты Java) - блокируется исполнение апплетов на языке Java;
 - **No access allowed** (Запрещение доступа) - запрещается взаимодействие апплетов Java с другими компьютерами;
 - **Allow access only to originating hosts** (Доступ разрешен только к хостам-источникам) - апплетам Java разрешается взаимодействовать лишь с компьютерами, из которых эти апплеты получены;
 - **Allow access to any trusted hosts** (Разрешение доступа всем доверенным хостам) - апплеты Java могут взаимодействовать с хостами, перечисленными в поле **Trusted hosts** (Доверенные хосты);
 - **Allow access to any host** (Разрешение доступа всем хостам) - апплетам Java позволено взаимодействовать с любым достижимым хостом;
- **Network access for untrusted hosts** (Сетевой доступ для недоверенных хостов) - поле определяет уровень сетевого доступа для недоверенных хостов. Можно выбрать следующие уровни: **Disable Java**, **No access allowed** и **Allow access only to originating host** (три ограничивающих варианта, предлагаемые для доверенных хостов).

После этого можно заняться вкладкой **Proxies** (Прокси). Если пользователям придется проходить через прокси-сервер, чтобы достичь нужного сервера, необходимо указать IP-адреса и порты для сервера или серверов прокси:

- **HTTP proxy** (Прокси HTTP). В этом поле вводится имя или IP-адрес хоста, а также номер порта (например, 192.168.0.12:8080);
- **Use HTTP proxy for all Internet protocols** (Использование прокси HTTP для всех протоколов сети Internet). Здесь следует задавать вариант **Yes** (Да), если прокси-сервер, указанный в поле **HTTP proxy**, способен служить в качестве прокси для протоколов FTP, Gopher и SSL Security. В этом случае следующие три поля можно не заполнять;
- **FTP proxy** (Прокси FTP). Если в предшествующем поле установлен вариант **No** (Нет), то в данном поле надо указать имя или IP-адрес прокси и номер порта;
- **Gopher proxy** (Прокси Gopher). Если во втором поле выбран вариант **No**, то здесь вносится имя или IP-адрес прокси и номер порта;
- **Security proxy** (Прокси безопасности). Если во втором поле задан вариант **No**, в этом поле следует определить имя или IP-адрес прокси и номер порта;
- **HTTP Tunnel proxy** (Прокси для туннеля HTTP). Поле предназначено для введения имени или IP-адреса прокси и номера порта;
- **SOCKS proxy** (Прокси SOCKS). Здесь указывается имя или IP-адрес прокси и номер порта;
- **No proxy for these hosts and domains** (Отсутствуют прокси для данных хостов и доменов). В этом поле назначаются серверы или хосты, к которым пользователи могут обращаться напрямую, то есть без применения прокси. Обычно они представлены серверами или хостами в собственной локальной сети пользователя. В поле следует ввести имена доменов, имена хостов и IP-адреса. Символ «звездочка» (*) является подстановочным, то есть заменяет собой любую часть имени или адреса (например, 192.168.0.*).

Дальнейшие операции связаны с заполнением вкладки **MIME**. На ней всего одно поле - **Format for messages addressed to internet addresses which cannot be found when sending** (Формат сообщений, направляемых по адресам сети Internet, которые не могут быть обнаружены при отправке). Здесь могут быть заданы следующие варианты: **Notes Rich Text format** (Расширенный текстовый формат системы Notes), который установлен по умолчанию, и **MIME format** (Формат MIME). Указываемый в этом поле вариант фактически определяет значение в поле **Format for messages addressed to internet addresses** (Формат сообщений, направляемых по адресам сети Internet) в документах местоположения пользователей. Когда пользователь системы Notes отправляет сообщение, система производит поиск персонального документа (Personal document) адресата в различных каталогах и при его обнаружении проверяет поле **Format preference for incoming mail** (Предпочитаемый формат для входящих почтовых сообщений), чтобы выбрать способ форматирования сообщения, направляемого этому адресату (в соответствии с одним из двух заданных вариантов). Если система Notes не находит персонального документа адресата или обнаруживает, что в упомянутом поле указан вариант **No Preference** (Без предпочтений), она будет использовать тот параметр, который установлен в обсуждаемом нами поле.

На заключительном этапе заполняется вкладка **Administration** (Администрирование), содержащая два поля: **Owners** (Владельцы) и **Administrators** (Администраторы), которые здесь выполняют те же самые функции, что и во всех остальных документах каталога Domain Directory, - назначение сотрудников, имеющих право редактировать данный документ. По умолчанию в обоих полях указывается имя автора документа, однако можно добавлять имена других пользователей, а также имена серверов или групп.

Создание профиля установки в версии R6

В сервере Domino R6 профили заменены политиками с целью обеспечения более точного администрирования в крупных корпоративных системах Notes/Domino. Однако политики действуют только на клиентские системы версии выше 4.6a, поэтому некоторое время будут одновременно присутствовать и профили, и политики. К сожалению, в программе Domino Administrator 6 уже нельзя создавать новые профили для устаревших систем, хотя допустимо изменять существующие профили. В отличие от профилей, политики устанавливаются на определенном организационном уровне и действуют на всех пользователей, находящихся в иерархии каталога Domino Directory ниже этого уровня. Основным отличием политики от профиля является наследование значений параметров из родительских политик (политик, установленных на верхних уровнях иерархии каталога) в дочерние. Однако на любом уровне можно блокировать наследование за счет введения явной политики или отмены действия наследования. Таким образом, все политики подразделяются на две категории:

- О **Explicit policy** (Явная политика) действует на отдельных пользователей и группы;
- О **Organization policy** (Организационная политика) действует на всех пользователей той организационной единицы, где она установлена.

Другая отличительная особенность политики состоит в ее динамическом характере. К пользователю (точнее, к его учетной записи) применяется действующая политика, которая определяет параметры по умолчанию на момент использования политики, причем

значения извлекаются из всех вышестоящих политик, подходящих для данного пользователя. Другими словами, администратор может изменить значение в одной из политик высокого уровня и не заботиться о распространении этих изменений по всем дочерним политикам. Как только возникает потребность в использовании измененной политики, нужные значения будут учтены в действующей политике нижнего уровня.

Все установленные политики связаны отношением «родитель-потомок» и отношением наследования параметров. Параметры политик определяются в соответствующих документах политик, которые по своему составу практически полностью соответствуют использовавшимся в версии R5 профилям.

Политики действуют по пяти направлениям, для каждого из которых формируются отдельные и независимые документы политик, определяющие значения по умолчанию:

- О **Registration** (Регистрация) - для процесса регистрации пользователей Notes (включая пароль пользователя, формат адресов Internet, назначение пользователя перемещаемым и характеристики его почты);
- О **Setup** (Установка) - для устанавливаемого нового клиента Notes. Эти значения служат для заполнения документа местоположения того пользователя, для которого устанавливается клиентская программа Notes. Они задают браузер сети Internet, параметры прокси-сервера, параметры безопасности апплетов, а также предпочтения для Рабочего стола системы и самого пользователя;
- О **Desktop** (Рабочий стол) - для управления и изменения операционной среды пользователя;
- О **Mail archiving** (Архивирование почты) - для архивирования полученных и исходящих почтовых сообщений пользователя (например, время проведения архивирования и критерии отбора сообщений);
- О **Security** (Безопасность) - для устанавливаемых списков ECL (см. ниже). Кроме того, определяются методы управления паролями, включая синхронизацию паролей Internet и Notes.

Пока нас интересует только политика установки. Чтобы ее создать, необходимо иметь право (уровень доступа) **Editor** (Редактор) для каталога Domino Directory и одну из следующих ролей: **PolicyCreator** (Создатель политики) для создания документа политики или **PolicyModifier** (Модификатор политики) для его редактирования. Чтобы создать документ политики установки, выполните следующие операции:

1. В программе Domino Administrator перейдите на вкладку **People & Groups** (Сотрудники и группы) и откройте вид **Settings** (Параметры).
2. Щелкните по кнопке **Add Settings** (Добавить параметры) и выберите политику **Setup** (установка).
3. Заполните поля в документе политики.
4. Сохраните и закройте документ политики установки.

Как и документ профиля установки, документ политики установки содержит вкладки **Basics** (Основные параметры), **Databases** (Базы данных), **Dial-up Connections** (Коммутируемые соединения), **Accounts** (Учетные записи), **Name Servers** (Серверы имен), **Applet Security** (Безопасность апплетов) и **Proxies** (Прокси). Вкладка **MIME** заменена вкладкой **Mail** (Почта), появились вкладки **Preferences** (Предпочтения) и **Comments** (Комментарии). Состав заполняемых полей в документе политики тот же самый, что и в документе профиля (см. предыдущий раздел), поэтому не будем повторяться, но обсудим несколько новых команд, свойственных только политике.

Для большей части параметров, знакомых по профилю установки, в политике установки появились флажки:

- **Inherit from parent policy** (Наследовать из родительской политики);
- **Enforce in child policies** (Применить в дочерних политиках).

Эти флажки позволяют управлять наследованием определенных параметров из родительских политик в дочерние. Если требуется одинаковым образом установить флажки для всех параметров, щелкните по кнопке **Inheritance** (Наследование) в верхней части формы и выберите **Enable for all fields** (Разрешить для всех полей) или **Disable for all fields** (Запретить для всех полей). Соседняя кнопка **Enforcement** (Применение) позволяет разрешить или запретить наследование значений из всех полей в дочерних политиках.

По умолчанию на форме политики установки сброшены все флажки наследования из родительской политики и применения в дочерних политиках, поэтому политика R6 будет действовать точно так же, как и профиль версии 5.

Подготовка списка управления исполнением для режима по умолчанию

Список управления исполнением (Execution Control List - ECL) позволяет клиентам системы Notes защитить пользователя от попадающих в систему некорректных программ, например почтовых вирусов. В клиенте системы Notes версии 5 можно активизировать эту функцию на экране **Basics** диалогового окна **User Preferences**, щелкнув по кнопке **Security Options** (Параметры защиты). В результате откроется диалоговое окно **Workstation Security: Execution Control List** (Защита рабочей станции: список управления исполнением). В клиенте Notes R6 следует выполнить команду **File => Security => User Security** (Файл => Безопасность => Безопасность пользователя) и перейти на вкладку **What Others Do => Using Workstation** (Действия других => Использование рабочей станции) - рис. 5.1.

Список ECL во многом напоминает списки управления доступом баз данных. Можно добавлять имена пользователей, групп, серверов (с использованием подстановочных символов), указывающих на конкретные организации или подразделения организаций, в список **When code signed by** (Когда код подписан), расположенный в левой части экрана. После этого допустимо выбрать одну из записей в списке и установить (в правой части экрана) необходимое число флажков **Allow** (Разрешение). В данном случае требуется весьма внимательно устанавливать флажки, поскольку все они относятся к потенциально опасным операциям, которые могут выполняться программами в системе Notes. Система Notes реализует поддержку трех независимых списков разрешенных операций, соответствующих трем расположенным в верхнем правом углу диалогового окна ссылкам, которые обеспечивают защиту от потенциально опасных:

- сценариев и формул LotusScript - **Using Workstation** (Использование рабочей станции);
- апплетов Java - **Using Applets** (Использование апплетов);
- приложений JavaScript - **Using JavaScript** (Использование сценариев JavaScript).

Когда программа пытается выполнить ту или иную операцию, присутствующую в списке, система Notes проверяет наличие цифровой подписи того человека, который авторизован разрешить запуск программы. Если человек не указан в списке или не подписана

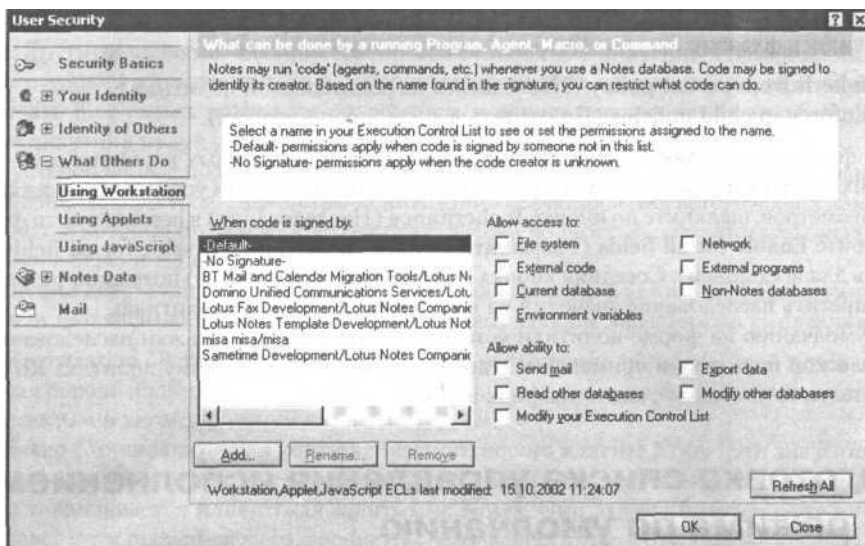


Рис. 5.1. По умолчанию программам на языке LotusScript разрешено выполнение любых операций

сама программа, система Notes разрешает программе произвести те из операций, которые перечислены в списках **Default** (По умолчанию) или **No Signature** (Без подписи).

Если программа пытается проделать операцию, не разрешенную в списке ECL, система Notes выводит для пользователя диалоговое окно **Execution Security Alert** (Нарушение режима безопасности), аналогичное показанному на рис. 5.2.

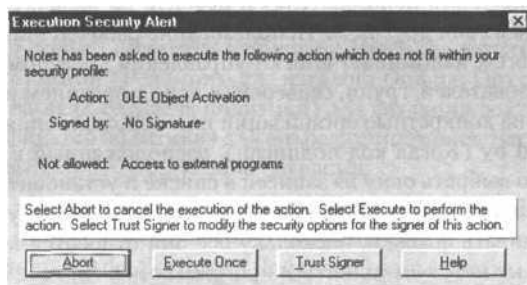


Рис. 5.2. При попытках программы выполнить операцию, не разрешенную в списке ECL рабочей станции, на экран дисплея будет выведено подобное диалоговое окно

Пользователю в этом случае придется решать вопрос о том, разрешать дальнейшее исполнение программы или нет, путем щелчка по соответствующей кнопке в диалоговом окне:

- О **Abort** (Аварийное завершение) - выполнение программы системой Notes прерывается;
- О **Execute Once** (Однократное исполнение) - системе Notes можно осуществить запрошенную операцию. Если в дальнейшем эту операцию потребуется выполнить еще раз, снова будет выведено диалоговое окно с предупреждением;

- О **Trust Signer** (Подпись доверенного лица) - системе Notes позволено выполнить запрошенную операцию и одновременно модифицировать список ECL так, чтобы в дальнейшем выполнение аналогичной операции не требовало получения специального разрешения;
- О **Help** (Подсказка) - открытие базы данных Administrative Help (Административная справка) для этого диалогового окна.

По умолчанию действие списка ECL обычно отменяется, но для всех оговоренных выше вариантов, в том числе **Default** и **No Signature**, обеспечивается возможность выполнения любых операций. На практике администраторы вправе изменять параметры по умолчанию так, чтобы при проведении установки нового пользователя его списки ECL реально применялись для ограничения выполнения тех или иных операций. Чтобы изменить параметры режима по умолчанию, необходимо:

1. В программе Domino Administrator перейти на вкладку **Files** (Файлы).
2. На панели **Servers** (Серверы) выбрать любой доступный сервер домена.
3. Открыть базу данных Domain Directory.
4. В меню **Actions** (Операции) выбрать пункт **Edit Administration ECL** (Редактирование административного списка ECL). На экране появится диалоговое окно **Administration ECL** (Администрирование ECL), которое полностью соответствует аналогичному диалоговому окну, воспроизводимому для рабочей станции версии R5. В этом окне следует внести требуемые изменения, а затем закрыть его.

При установке нового пользователя домена система Notes задействует те параметры режима по умолчанию, которые были определены для данного окна. Имеется также возможность передать измененные параметры режима на соответствующую рабочую станцию (см. главу 10).

На этом этапе представляется также целесообразным назначить уполномоченного компании для цифровой подписи программ, ввести его имя в окне **Administration ECL** (Администрирование ECL) и придать необходимые полномочия. Не следует забывать о том, что по мере развития компании будут появляться новые типы приложений, поэтому желательно иметь уполномоченного, который мог бы разрешать всем пользователям работать с такими приложениями без обращения к диалоговому окну **Execution Security Alerts** (Нарушение режима безопасности), показанному на рис. 5.2.

В качестве уполномоченного допускается назначить любого зарегистрированного сотрудника компании, в том числе и того, который специально выделен для подписи шаблонов проектирования. Случай применения подобного уполномоченного проиллюстрирован на рис. 5.1 - см. в списке строку **Lotus Notes Template Development/Lotus Notes** (Разработка шаблонов системы Lotus Notes/система Lotus Notes). Этот файл соответствует файлу идентификационных данных системы Notes (по крайней мере изначально имел такое назначение) и служит для подписания шаблонов баз данных системы Notes, входящих в состав дистрибутива Notes/Domino.

В нашем примере компания Stillwater Enterprises может, например, зарегистрировать пользователя под именем Stillwater Template Development/Stillwater, а затем с помощью упомянутого файла снабдить цифровой подписью те базы данных, которые будут создаваться и распространяться этим пользователем. Тот же пользователь вправе подписывать шаблоны и базы данных, распределяемые в системе Notes/Domino и не подтвержденные в свое время компаний Lotus. Следует отметить, однако, что в версии 5.0 подобных неподписанных компонентов осталось весьма немного, а в версии R6 цифровую подпись имеют все компоненты.

Если заблаговременно не предусмотреть такого подтверждения, пользователям придется часто иметь дело с диалоговым окном **Execution Security Alerts**. В какой-то момент они найдут средство избавиться от этого окна навсегда и воспользоваться вариантом **Trust Signer** (Подпись доверенного лица). После этого система Notes начнет считать доверенными неподписанные программы, которым будет разрешено выполнение операций, запрещенных списком ECL. В результате при появлении некорректной программы (например, в сообщении электронной почты) окажется, что список ECL просто не в силах обеспечить необходимую защиту.

Степень риска в данном случае определяется политикой по обеспечению безопасности, которую проводит организация. Компания Lotus обычно распространяет систему Notes с отключенными списками ECL (в режиме по умолчанию), поскольку ее специалисты хорошо представляют себе сложившуюся на текущий момент ситуацию и знают, что клиенты чаще всего не заботятся о мерах безопасности и не обращают внимания на функцию ECL. Однако, если организация серьезно заботится о режиме безопасности, следует активизировать списки ECL еще до того, как будет установлено большое число рабочих станций: настройку этой функции проще производить для новых пользователей, чем для уже существующих.

Сертификаторы для организационной единицы

Если к данному моменту еще не сформированы организационные единицы (но в дальнейшем планируется поместить в них пользователей), то теперь самое подходящее время заняться их созданием. Введение OU всецело определяется ранее разработанной политикой. Если подобные решения еще не приняты, рекомендуется обратиться к материалам главы 2 и восполнить пробелы.

Рекомендации о регистрации организационных единиц приводились в главе 3. В данном разделе эта операция обсуждается лишь в общих чертах. Так, при регистрации сертификатора OU1 приходится привлекать данные сертификатора O, а при регистрации сертификатора OU2 - данные сертификатора OU1 и т.д. Для регистрации сертификатора в общем случае необходимо выполнить следующие операции:

1. В программе Domino Administrator перейдите на вкладку **Configuration** (Конфигурация).
2. На панели **Tools** выберите **Registration => Organizational Unit** (Регистрация => Организационная единица).
3. Выберите родительского сертификатора для новой организационной единицы (OU) и введите пароль.
4. Заполните поля диалогового окна **Register Organizational Unit Certifier** (Сертификатор регистрации организационной единицы), а затем выполните команду **Register** (Регистрация).

Альтернативные имена и языки

Если компания является международной, приходится активизировать функцию, связанную с применением альтернативных языков и имен (названий). Это позволяет задавать два

имени для каждого пользователя: основное (распознаваемое на международном уровне) и вспомогательное (на родном языке пользователя с введением соответствующих символов). После этого система Notes сможет воспроизводить документы и списки имен на родном языке пользователя.

Подобный подход позволяет решить целый ряд проблем. Например, в Китае фамилии пользователей указываются первыми, а имена последними, что прямо противоположно способу, принятому в Европе. Наличие рассматриваемой функции позволит китайским пользователям правильно ориентироваться в именах, которые будут отображаться с помощью иероглифов. В то же время европейцы смогут воспринимать китайские имена в привычном для них виде (поскольку эти имена будут воспроизводиться и буквами латинского алфавита).

В качестве другого примера можно упомянуть южноамериканские имена, в которых фамилии пользователей содержат имена отца и матери, разделенные дефисом. В разговорной речи в родительских именах произносится только та часть, которая предшествует дефису (то есть лишь имя отца). А вот англоязычные пользователи обычно отбрасывают этот элемент имени, зато употребляют элемент, следующий за дефисом, считая его собственно именем пользователя. Функция применения альтернативных имен позволяет испаноговорящим пользователям регистрироваться с помощью имени отца на международном уровне и одновременно вводить более привычное имя в качестве альтернативного.

Для реализации этой функции требуется добавить альтернативные языки в идентификационные данные сертификатора, причем рекомендуется начать процедуру с компонента О. На практике можно добавлять несколько языков (по числу языков общения пользователей), распознаваемых системой Notes (38 языков в версии 5.0). Следует отметить, что в версии R6 реализована поддержка Unicod, что позволяет вносить в имена символы любых языков¹. Идентификационные данные сертификатора организации должны содержать сведения относительно всех альтернативных языков, с которыми планируется работать. Данные сертификатора организационной единицы могут включать в себя только подгруппы языков общения (по отношению к группе языков, применяемых для организации). Идентификационные данные пользователя содержат сведения относительно только двух языков, принадлежащих к той группе, которая ранее была задана для соответствующего родительского сертификатора.

Например, на уровне /Stillwater разрешается употреблять четыре языка. Для уровня /MarshCreek/Stillwater допустимы все четыре языка или любые их комбинации. В то же время на этом иерархическом уровне нельзя прибегать к другим языкам, поскольку они сначала должны быть добавлены для старшего компонента иерархии. Идентификационные данные пользователя (Rob Kirkland/MarshCreek/Stillwater) могут содержать сведения относительно двух языков, позволенных на уровне MarshCreek/Stillwater/ (только из числа разрешенных языков).

Для добавления альтернативных языков и имен в данные сертификатора приходится проводить процедуру сертификации еще раз. Альтернативные языки добавляются в идентификационные данные пользователя во время регистрации или в процессе повторной сертификации.

¹ Вместе с тем сохранена поддержка отдельных кодировок, включая кириллицу Cyrillic с кодировками KOI8-R, ISO-8859-5 и Windows-1251. - *Прим. ред.*

Добавление альтернативного языка в идентификационные данные сертификатора

Процедура добавления альтернативного языка в идентификационные данные сертификатора предусматривает выполнение ряда перечисленных ниже операций:

1. Сначала в программе Domino Administrator перейдите на вкладку **Configuration**.
2. Затем на панели **Tools** последовательно выберите пункты **Certification** (Сертификация) и **Certify** (Утверждение).
3. В диалоговом окне **Choose a Certifier** (Выбор сертификатора) найдите и отметьте требуемого сертификатора. При определении данных для сертификатора организации укажите идентификационный файл уровня O. Для сертификации сертификатора организационной единицы выберите дочернего сертификатора, после чего введите его пароль.
4. В результате на экране появится диалоговое окно **Choose ID to Certify** (Выбор идентификационных данных для сертификации), где следует указать повторно сертифицируемого сертификатора (для сертификатора организации следует выбирать его самого). Еще раз введите пароль сертификатора.
5. Откроется окно **Certify ID** (Сертификация идентификационных данных) с полем **Subject name** (Имя объекта). В нем задайте **Add** (Добавление).
6. Будет выведено диалоговое окно **Specify Alternate Organization Name** (Задание альтернативного названия организации) или **Specify Alternate Organizational Unit Name** (Задание альтернативного имени организационной единицы), в котором необходимо заполнить поля:
 - **Language** (Язык). Предназначено для введения альтернативного языка. Если подтверждается сертификатор организации (O), можно внести все языки, распознаваемые системой Notes. В случае подтверждения данных сертификатора организационной единицы допустимы только языки общения, ранее установленные на уровне O;
 - **Country code**. Это поле заполнять необязательно, причем оно появляется только в том случае, когда в список сертификатора организации добавляются имена. Для сертификаторов OU автоматически сохраняется тот код страны, который ранее был установлен на уровне организации. В качестве кода страны требуется ввести двухсимвольный код, утвержденный Международной организацией по стандартизации, однако делать это следует только в том случае, если ранее компания уже приняла решение относительно употребления кода страны в качестве части имени организации;
 - **Organization** (Организация). Такое поле появляется при подтверждении данных для сертификатора организации (O). Здесь надо выбрать новое, уникальное имя, которое не присутствует в характеристиках других языков. Например, если компания приняла испанский язык как альтернативный, английское название может сохраняться в виде /Stillwater, но система Notes не позволит оставить это имя и в испанском варианте. Придется придумать другое имя на испанский манер, скажем /AguaSerena, или сохранить название в английском варианте в виде /Stillwater.sp;

- **Org Unit** (Организационная единица). Это поле выводится при повторном утверждении данных сертификатора организационной единицы (OU). В нем (в отличие от поля с альтернативным именем организации) не требуется задавать уникальное имя. Так, если имя сертификатора в английском варианте /MarshCreek/Stillwater, в испанском варианте оно может иметь вид /MarshCreek/AguaSerena. Поскольку имена на уровне организации являются уникальными, на уровне организационных единиц можно обойтись одинаковыми именами.

7. Щелкните по кнопке ОК, после чего альтернативные имя и язык появятся в списке **Subject name** (Имя объекта).
8. Затем повторите шаги с 5 по 9 для других альтернативных языков. Имеется также возможность применить команды **Rename** (Переименование) и **Remove** (Удаление), чтобы изменить альтернативное имя или исключить альтернативный язык.
9. Если данные указываются для сертификатора организационной единицы, следует обратиться к полю **Expiration date** (Дата завершения действия). Не надо забывать, что срок завершения действия сертификата для файла идентификационных данных первоначально устанавливается равным 100 годам (считая с момента создания сертификатора для организации). Однако при повторном утверждении программа Domino Administrator предлагает еще раз указать дату завершения действия так, чтобы она отстояла всего на два года от текущей. В этом случае можно отказаться от значения по умолчанию и снова назначить дату завершения действия сертификата со сдвигом в 100 лет.
10. После выполнения всех перечисленных операций щелкните по кнопке **Certify** (Утверждение).

События, связанные с добавлением нового языка в идентификационные данные сертификатора

В процессе повторной сертификации происходит выдача родительским сертификатором новых сертификатов для дочерних сертификаторов. Исключение в данном случае представляет сертификат организации, которая сертифицирует себя сама. Родительский сертификат выдает сертификаты всем дочерним объектам с новыми альтернативными именами, но старыми открытыми ключами. Сказанное несложно проверить, ознакомившись с содержимым файла идентификационных данных для альтернативного имени. Для этого выполните следующие действия:

г,

1. В программе Domino Administrator перейдите на вкладку **Configuration**.
2. На панели **Tools** выберите **Certification => ID Properties** (Сертификация => Свойства идентификационных данных).
3. Найдите требуемые идентификационные данные, выделите соответствующий файл в списке и введите пароль.
4. В версии R5 появится диалоговое окно **User ID - IDname** (Идентификационные данные пользователя - название идентификационных данных), где нужно отметить **Choose Certificate** (Выбор сертификатов). В результате будет выведен перечень всех сертификатов, присутствующих в идентификационных данных (с указанием всех

предшествующих сертификатов и их идентификаторов) - рис. 5.3. В версии R6 окно имеет немного другой вид, причем нужные данные находятся на вкладках **Your Identity => Your Names** (Ваша идентификация => Ваши имена) и **Your Identity => Your Certificates** (Ваша идентификация => Ваши сертификаты).

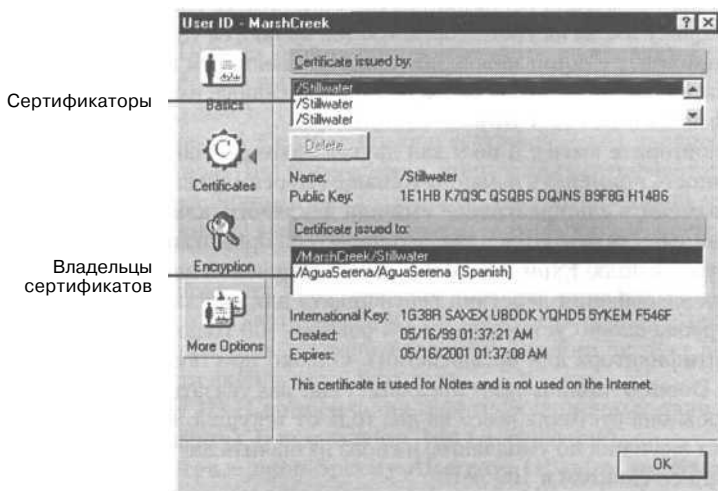


РИС. 5.3. В диалоговом окне указаны сертификаты (вверху) и владельцы выданных им сертификатов (внизу)

В списке **Certificate issued by** (Сертификат выдан) для идентификационных данных (см. рис. 5.3) имя /Stillwater появляется три раза, что указывает на факт присутствия в идентификационных данных по меньшей мере трех сертификатов, выданных сертификатом с именем /Stillwater. Если выбрать первый сертификат, то в списке **Certificate issued to** (Сертификат выдан для) будут показаны имена объектов, которым выдан данный сертификат. В рассматриваемом случае сертификат был создан для объектов /MarshCreek/Stillwater и /MarshCreek/AguaSerena. Сертификат идентифицируется открытым ключом сертификатора MarshCreek (в данном случае используется международный вариант открытого ключа), имеющего два альтернативных имени.

Второй сертификат также был сформирован для объектов /MarshCreek/Stillwater и /MarshCreek/AguaSerena, однако он предназначен для идентификации североамериканской версии открытого ключа для двух имен. Третий сертификат является копией того, который создавался сертификатом /Stillwater для себя, и служит для связи открытого ключа сертификатора (/Stillwater) со всеми его альтернативными именами. Если приведенное выше описание окажется слишком сложным, обратитесь к главе 10.

Регистрация основных параметров пользователя

Обычно пользователь системы Notes имеет собственный персональный документ (Personal document) в каталоге Domain Directory. Такой пользователь может быть членом нескольких

групп, иметь свою базу данных почтовой службы, хранящуюся на сервере почтовой службы, и владеть собственным файлом идентификационных данных. Названный файл содержит по меньшей мере один сертификат, утвержденный вышестоящим сертифицированным (то есть лицом, его выдавшим) и позволяет идентифицировать пользователя с помощью индивидуального открытого ключа. Этот открытый ключ и соответствующий ему закрытый ключ также хранятся в файле идентификационных данных.

К счастью, пользователю не требуется постоянно держать всю информацию под рукой, поскольку программа Domino Administrator дает возможность автоматически формировать ключи, сертификаты, файл идентификационных данных, персональный документ (Personal document) и базу данных почтовой службы, а также добавлять пользователя в заданные группы. Эти действия выполняются указанной программой в процессе регистрации пользователя, причем все, что требуется сделать самому пользователю, – заполнить регистрационную форму и предоставить программе Domino Administrator необходимую информацию для проведения настройки.

Предварительные условия для регистрации

Перед заполнением упомянутой формы необходимо обеспечить выполнение некоторых требований:

- иметь доступ или владеть идентификационными данными сертифицированного пользователя, осуществляющего сертификацию для тех пользователей, которых планируется зарегистрировать, а также знать соответствующий пароль;
- организовать доступ рабочей станции к серверу Domino, который будет служить в качестве регистрирующего сервера;
- получить статус (роль) **UserCreator** (Создатель пользователя) и право доступа, по крайней мере на уровне **Author** (Автор), к базе данных Domain Directory регистрирующего сервера;
- обладать правом доступа, по крайней мере на уровне **Editor** (Редактор), к журналу Certification Log (Журнал сертификации, файл certlog.nsf) регистрирующего сервера;
- иметь право доступа на уровне **Create new databases** (Создание новых баз данных) к каждому серверу почтовой службы пользователей, если намечается в процессе регистрации сформировать для них соответствующие файлы почтовых сообщений. Либо можно создать почтовые базы данных новых пользователей во время установки рабочих станций. В этом случае, однако, каждому новому пользователю должно быть предоставлено право доступа на уровне **Create new databases** к его собственному серверу почтовой службы, что реализуется по умолчанию.

Необходимо отметить, что в случае создания нового домена и следования рекомендациям, приведенным в главах 3 и 4, все указанные требования выполняются автоматически.

Задание параметров по умолчанию для осуществления регистрации

В дополнение к вышесказанному еще до начала регистрации можно задать несколько значений по умолчанию. Для этого надо в диалоговом окне **Administration Preferences** (Предпочтения администрирования) выбрать в меню **File** (Файл) пункты **Preferences => Administration Preferences** (Предпочтения => Административные предпочтения). В открывшемся

диалоговом окне **Administration Preferences** следует щелкнуть по ссылке **Registration** (Регистрация) и затем заполнить следующие поля:

- поле **Registration domain** (Домен регистрации). В этом поле следует ввести имя домена, где, вероятнее всего, будет проведена процедура регистрации;
- кнопка **Registration server** (Регистрирующий сервер) открывает окно для ввода полного различающегося имени сервера, копия каталога Domain Directory которого будет использована для хранения нового персонального документа (Personal document) и изменения в документах группы (Group document);
- кнопка **Certifier ID** (Идентификационные данные сертификатора) позволит найти и указать идентификационные данные того сертификатора, который, скорее всего, будет задействован при регистрации новых пользователей. При этом система может запросить пароль для выбранных идентификационных данных;
- кнопка **Mail Options** (Параметры почтовой службы) откроет диалоговое окно для указания почтовой службы, с которой будут работать новые пользователи. В версии R5 выводятся следующие варианты: **Lotus Notes**, **Other Internet**, **POP**, **IMAP**, **Other** и **None**, но в версии R6 существенно расширен список почтовых служб, хотя по умолчанию предлагается применять вариант **Mail (R6)**, то есть почтовую службу сервера Domino 6. В зависимости от выбранной службы в списке **Mail system** (Почтовая система) появляются следующие два поля (если выбрана служба **Lotus Notes**, **POP** или **IMAP**);
- кнопка **Mail server** (Сервер почтовой службы) позволит указать полное различающееся имя того сервера, через который новые пользователи будут получать доступ к своим базам данных почтовых сообщений;
- **Mail template** (Шаблон почтовой службы). Поле доступно в версии R5. В нем задается шаблон почтовой службы, предназначенный для создания баз данных почтовой службы новым пользователям;
- поле **ID file folders** (Папки файлов идентификационных данных в R5) или кнопка **User ID/Password Options** (Параметры пользовательского идентификатора/пароля) служат для ввода имен папок, в которых планируется разместить новые файлы идентификационных данных (сотрудники, серверы и сертификаторы);
- поле **Password quality settings** (Параметры качества пароля) или кнопка **User ID/Password Options** позволяют устанавливать ползунком качество пароля (минимальный размер по умолчанию) для каждого файла идентификационных данных (сотрудники, серверы и сертификаторы). Компания Lotus определяет это минимальное значение (в режиме по умолчанию) равным 8 для пользователей, 0 для серверов и 10 для сертификаторов. Шкала качества допускает задание значений в интервале от 0 (пароль необязателен) до 16 (трудно дешифрируемый пароль). Специалисты компании Lotus советуют назначать для серверов значение 0 (по умолчанию), поскольку серверы обычно размещаются в защищенных местах, причем без установки пароля серверы могут запускаться автоматически сразу после возникновения отказа. Для сотрудников и сертификаторов компания Lotus рекомендует значения (в режиме по умолчанию), трудно поддающиеся дешифрованию. Порядок ввода паролей и периодичность их замены зависят от политики обеспечения безопасности в домене, разработанной и проводимой компанией;
- **Internet domain** (Домен Internet, только в R5). Здесь вносится имя домена сети Internet, с которым будут взаимодействовать вновь регистрируемые пользователи;

- О **User setup profile** (Профиль установки пользователя). В этом поле указывается профиль, соответствующий вновь регистрируемым пользователям;
- О **Explicit policy** (Явная политика, только в R6). Данное поле позволяет выбрать для регистрации пользователей определенную явную политику.

На практике можно каждый раз, когда требуется зарегистрировать новую группу пользователей, просматривать режимы по умолчанию, предназначенные для целей регистрации и установленные в диалоговом окне **Administration Preferences** (Предпочтения администрирования). Если необходимо зарегистрировать много новых пользователей, то задание параметров по умолчанию на данном этапе позволит сэкономить время. Рекомендуется также тщательно проверить введенные в поля значения, поскольку возникающие сейчас ошибки будет достаточно трудно исправить впоследствии.

Заполнение регистрационной формы

После выполнения предварительных условий и установки параметров по умолчанию можно переходить к регистрации новых пользователей. Для этого проделайте такие операции:

1. Сначала убедитесь в том, что соблюдены все указанные выше условия.
2. В программе Domino Administrator перейдите на вкладку **People & Groups** или на вкладку **Configuration** - они обе позволяют провести регистрацию пользователей.
3. Отметьте на вкладке **People & Groups** пункт **Tools => People => Register** (Программные инструменты => Сотрудники => Регистрация) или на вкладке **Configuration - Tools => Registration => Person** (Программные инструменты => Регистрация => Сотрудник).
4. Программа Domino Administrator будет пытаться найти файл идентификационных данных сертификатора, имя которого задается в параметрах по умолчанию. Если имя сертификатора не указано, программа Domino Administrator постарается найти сертификат, который использовался последним. В ходе этого процесса на экран могут быть выведены одно или несколько следующих диалоговых окон:
 - **Enter Password** (Ввод пароля). Здесь вносится правильный пароль для получения доступа к содержимому файла идентификационных данных сертификатора. При появлении такого окна убедитесь, что в нем запрашивается пароль именно того файла идентификационных данных, с которым планируется работать в дальнейшем. Если запрос сформулирован правильно, введите требуемый пароль и щелкните на кнопке ОК, а затем приступайте к выполнению шага 5. Если же запрос сформулирован некорректно, то, воспользовавшись кнопкой **Cancel** (Отмена), выберите другой файл идентификационных данных сертификатора. Если в очереди на регистрацию остались пользователи (еще с предыдущей процедуры регистрации), которые должны регистрироваться с привлечением иных сертификатов, чем текущий сертификат по умолчанию, система сформирует запрос на ввод паролей для всех участвующих сертификаторов;
 - **Choose Certifier ID** (Выбор идентификационных данных сертификатора) Если программа Domino Administrator не находит файла идентификационных данных или обнаруживает другой файл, отличный от намеченного к применению, либо был сделан щелчок по кнопке **Cancel** (Отмена) в этом диалоговом окне, то откроется

- окно **Choose Certifier ID** для явного указания файла идентификационных данных сертификатора;
- **Domino Administrator** (Администрирование сервера Domino). Если еще не была разрешена функция восстановления идентификационных данных сертификатора, может появиться диалоговое окно, призванное предупредить пользователя об отсутствии информации для этой функции. Пользователь, четко следуя всем приводившимся выше рекомендациям, настройкой рассматриваемой функции пока не занимался (как это делается, описано ниже в настоящей главе), так что данное диалоговое окно обязательно развернется и рекомендуется выбрать **Yes (Да)** или **No (Нет)** для его закрытия.
5. В дальнейшем откроется диалоговое окно **Register Person - New Entry** (Регистрация сотрудника - новая запись). Работа с этим окном требует особой аккуратности (см. рис. 5.4 и список полей, которые следует заполнить).

Рис. 5.4. Экран регистрации пользователя для режима Advanced. /

В обычном окне регистрации отсутствуют кнопки Mail, ID Info и Other.

Готовые к регистрации пользователи перечислены в списке Registration Queue

Регистрационная форма (Registration form) содержит в верхней части окна от двух до пяти значков, что зависит от флажка **Advanced** (Дополнительно), находящегося в левой нижней части диалогового окна, а также следующих полей:

- О **Registration queue** (Очередь регистрации). Очередь регистрации обычно занимает нижнюю часть диалогового окна и представляет собой перечень подготовленных к регистрации пользователей;

- кнопка **Add Person** (Добавление сотрудника). Сначала следует задать данные двух-пяти экранов для каждого пользователя и только потом щелкнуть по кнопке **Add Person**. При этом соответствующий пользователь отобразится в очереди регистрации. Кнопка не имеет названия и помечена зеленым значком «галочка». Она становится видимой после заполнения полей формы;
- кнопка **Import Text file** (Импорт текстового файла). Вместо того чтобы вручную вводить данные сотрудников в диалоговом окне **Register Person** (Регистрация сотрудника), можно импортировать нужные значения из текстового файла со специальным разделителем полей (см. главу 6);
- кнопка **Migrate people** (Миграция сотрудника). Программа Domino Administrator позволяет переносить пользователей из других систем, в том числе из систем Lotus cc:Mail, Windows NT, Microsoft Exchange, Microsoft Mail, каталогов LDAP (в файле LDIF), Novell GroupWise 4.1 и 5.0 и Netscape Messaging Server (см. главу 6);
- кнопка **Register** (Регистрация) и кнопка **Register All** (Регистрация всех). После завершения операции добавления пользователей (или еще до ее завершения) можно с помощью кнопок **Register** или **Register All** указать программе Domino Administrator на необходимость проведения регистрации выделенных в очереди регистрации пользователей или всех пользователей, присутствующих в этой очереди. Если процесс регистрации не настраивался дополнительно (кнопкой **Options**), успешно зарегистрированные пользователи будут исчезать из очереди регистрации, а те, кому отказано в регистрации, изменят свой статус;
- кнопка **Apply** (Применить). Можно выбрать одного или нескольких пользователей в очереди регистрации, а затем отредактировать ранее заданные для них значения (в верхней части экрана). Кнопка **Add User** (Добавление пользователя) превратится в кнопку **Apply** в тех случаях, когда изменение данных пользователей инициируется для уже присутствующих в очереди регистрации. Щелкните по кнопке **Apply** для подтверждения изменений и замены названия кнопки на **Add User**;
- кнопка **Delete** (Удаление). Позволяет удалять заданных пользователей из очереди регистрации;
- кнопка **Options** (Параметры). Служит для изменения способа действия диалогового окна **Register Person** (Регистрация сотрудника):
 - **Do not continue on registration errors** (Не продолжать после ошибок регистрации). Если в ходе регистрации возникает ошибка, обычно прерывается регистрация того сотрудника, для которого эта ошибка была обнаружена, но регистрируются другие пользователи из списка. При выборе данной строки процесс регистрации будет полностью прекращаться после обнаружения любой ошибки;
 - **Keep successfully registered people in the queue** (Сохранение успешно зарегистрированных пользователей в очереди). Пользователи, как правило, удаляются из очереди в случае их успешной регистрации. Если отметить эту строку, они будут сохраняться в очереди, но их статус изменится на **Registered** (Зарегистрированный);
 - **Try to register queued people with error status** (Попытка регистрации в очереди пользователей со статусом ошибки). При задании подобной строки будут продолжаться попытки зарегистрировать и того пользователя, для которого ранее имела место ошибка и в конечном итоге вероятен отказ в регистрации;

- **Allow registration of previously registered people** (Разрешение регистрации для ранее зарегистрированных сотрудников). На практике нет никакой необходимости в этом режиме, но он все же существует;
 - **Search all directories for duplicate names** (Поиск совпадающих имен во всех каталогах, только R6). Предоставляется возможность выявить дублирующиеся имена, даже если они присвоены в разных каталогах;
 - **Enforce short name uniqueness** (Предписать уникальность кратких имен, только R6). Название этого режима регистрации полностью определяет его назначение;
 - **Don't prompt for a duplicate person** (Не реагировать на совпадающих пользователей). Если полное и сокращенное имена регистрируемого пользователя повторяют имена уже существующего пользователя, программа Domino Administrator выведет запрос для изменения данных уже существующего пользователя. При установке этого флажка и выборе варианта **Skip the person registration** (Пропуск сотрудника при регистрации) попытка регистрации пользователя с уже существующим именем будет автоматически инициировать отказ в регистрации. Если же указать **Update the existing address book entry** (Изменение существующих записей адресной книги), то программа Domino Administrator будет инициировать изменение данных для уже существующего пользователя без формирования запроса;
 - **Don't prompt for a duplicate mail file** (Не реагировать на совпадающие почтовые файлы). Если существует еще один файл почтовых сообщений с тем же именем, программа Domino Administrator направит запрос, чтобы изменить имя этого файла. При установке данного флажка допустимо отметить один из трех вариантов (режимов). Рекомендуется вариант **Skip the person registration** (Пропуск сотрудника при регистрации), что приводит к отказу в регистрации при возникновении описанной ситуации. Можно также выбрать **Generate a unique mail file name** (Формирование уникального имени почтового файла), чтобы программа Domino Administrator внесла соответствующие изменения имени существующего файла, или вариант **Replace the existing mail file** (Замена существующего почтового файла), чтобы программа заменила существующий файл почтовых сообщений, не формируя запрос. Последний вариант возможен только для пользователя, располагающего правом доступа на уровне **Manager** (Менеджер) к существующему файлу почтовых сообщений. Такой выбор оказывается неприемлемым, если для создания файла почтовых сообщений требуется воспользоваться процессом администрирования (Administration Process). Подобная ситуация может возникнуть в режиме **Create file in background** (Создание файла в фоновом режиме), установленном на экране **Mail** (Почта) регистрационной формы;
 - **Don't prompt for a duplicate roaming directory** (Не реагировать на совпадающие перемещаемые каталоги, только в R6). После установки этого флажка можно выбрать режим **Skip the person registration** (Пропуск сотрудника при регистрации) или **Generate unique roaming directory name** (Генерировать уникальное имя перемещаемого каталога);
- О **Done** (Выполнить). После окончания регистрации пользователей (или при прерывании еще до завершения процесса) отметьте **Done** и закройте диалоговое окно

регистрации. Если в очереди останутся незарегистрированные пользователи (или не добавленные в список пользователей в верхней части экрана), система выведет запрос о сохранении сведений. При подтверждении сохранения информация о таких пользователях запоминается в местной базе данных User Registration Queue (Очередь регистрации пользователей, файл userreg.nsf) и снова появляется в очереди регистрации, когда начинается следующий процесс добавления пользователей на той же рабочей станции.

Поля диалогового окна регистрации сотрудника

Перечень полей, которые необходимо заполнить для регистрации сотрудника, зависит от того, был ли выбран режим **Advanced** (Дополнительно) в диалоговом окне **Register Person** (Регистрация сотрудника). Если соответствующий флажок сброшен, достаточно ввести только имя сотрудника и его пароль, а также указать, в какие группы следует добавить его имя. В остальных полях разрешается оставить значения по умолчанию. Когда требуется зарегистрировать множество пользователей, лучше позволить системе самой заполнить как можно больше полей формы. Существует несколько стратегий автоматизации процесса ввода данных в тех случаях, когда параметры режимов по умолчанию не подходят для всех регистрируемых пользователей.

Первая стратегия. Задайте параметры по умолчанию в диалоговом окне **Administration Preferences** (Предпочтения администрирования) в полном соответствии с приведенными выше рекомендациями. После этого сбросьте флажок **Advanced** и внесите данные обо всех пользователях, задав их имена и пароли. Затем просмотрите очередь регистрации и выберите тех пользователей, для которых параметры совпадают. (Чтобы указать нескольких пользователей, достаточно добавить метки каждому из них щелчком по крайнему левому столбцу.) Далее перейдите в режим **Advanced** и введите данные, являющиеся нетипичными и в то же время индивидуальными для данной группы. При этом не будут занесены те поля, которые должны быть уникальными для каждого пользователя. Щелкните по кнопке **Apply** (Применить) для присвоения измененных параметров всем выбранным пользователям. В дальнейшем следует повторять описанную процедуру вплоть до присвоения корректных значений всем пользователям в очереди регистрации.

Вторая стратегия. Сначала назначьте режим **Advanced**, затем укажите данные для одного пользователя и внесите его в очередь регистрации. После этого отмените режим **Advanced** и добавьте другого пользователя, задав для него только имя и пароль (и при необходимости - группы). Совпадающие параметры будут устанавливаться согласно параметрам первого пользователя. Придется повторить указанную процедуру для всех групп пользователей, имеющих разные параметры регистрации.

Основная идея здесь заключается в том, чтобы минимизировать объем работ и время на ввод данных. Одновременно удастся также снизить вероятность возникновения ошибки. Можно дать еще одну полезную рекомендацию: внимательно вносите данные и проверяйте их несколько раз. Наличие ошибок способно привести в будущем к возникновению серьезных проблем.

Перечень полей, заполняемых в диалоговом окне **Register Person**, приведен в табл. 5.1.

Таблица 5.1. Перечень полей, заполняемых на форме **Register Person Form**

Название поля	Назначение
	Вкладка Basics (Основные параметры)
First name (Имя)	Здесь следует вводить имя пользователя
MI (Инициалы)	В этом поле нужно задавать инициалы. Позволяется вводить до двух символов, что считается достаточным для указания буквы и точки. Необходимо принять решение (в соответствии с проводимой компанией политикой) о применении точки совместно с инициалами. Точку надо ставить всегда или никогда
Last name (Фамилия)	Поле является обязательным для заполнения и в нем должна задаваться фамилия пользователя
Short name (Краткое имя)	Программа Domino Administrator автоматически заполняет поле, используя имя пользователя и первые инициалы. Имя должно быть уникальным в домене. Если известно, что данное требование не соблюдается, следует изменить имя. Когда у пользователя имеются какие-либо сомнения на этот счет, рекомендуется оставить все без изменения. На момент регистрации программа Domino Administrator в режиме по умолчанию уведомит пользователя и предоставит ему возможность изменить имя
Password (Пароль)	Это поле необходимо заполнять всегда, кроме случая, когда в поле Password Quality Scale (Шкала качества пароля) указано значение 0. Здесь приводится тот самый пароль, посредством которого снимается блокировка с файла идентификационных данных пользователя. Пользователи должны немедленно изменить пароль после завершения установки рабочей станции. Увеличить качество пароля можно путем задания в качестве пароля трудного для запоминания сочетания символов (например, набора бессмысленных произвольных символов) или слишком длинной фразы. Если не планируется применять стандартный пароль для всех пользователей, следует записывать индивидуальные пароли в каком-нибудь журнале. После удаления имени пользователя из очереди регистрации система Notes больше нигде не покажет установленный для пользователя пароль
Password Quality Scale (Шкала качества пароля)	Здесь требуется задавать качество пароля: от 0 (необязательный пароль) до 16 (трудно дешифрируемый пароль). Значение выбирается с помощью бегунка. Система Notes анализирует качество пароля в соответствии с алгоритмом, учитывающим факт наличие в пароле слов из словаря системы Notes, символов разных регистров, цифр, пробелов и прочих символов. В зависимости от вида и сочетания символов длина пароля может быть установлена в диапазоне от 6 до 12 символов, чтобы достичь качества, равного 8
Set internet password (Пароль для Internet)	Задаваемый в этом поле пароль отличается от рассмотренного выше. Он соответствует полю в персональном документе (Person document) и является тем самым паролем, который Web-пользователь должен ввести для аутентификации его Web-сервером Domino. Если пароль отсутствует, пользователя не удастся правильно аутентифицировать при обращении из Web-браузера. Тем не менее поле может оставаться пустым, чтобы пользователь лично вводил пароль сети Internet в персональный документ в том случае и в тот момент, когда он готов обратиться к Web-браузеру для доступа к Web-серверу Domino

Таблица 5.1. Перечень полей, заполняемых на форме **Register Person Form** (продолжение)

Название поля	Назначение
Internet address (Адрес сети Internet) В версии R6 находится на вкладке Address	Программа Domino Administrator самостоятельно заполняет это поле и задает для пользователя адрес почтовой службы сети Internet с помощью имени пользователя и данных из поля Internet Domain , причем форматирование адреса выполняется согласно значению, выбранному кнопкой Format (Формат) в R5 или указанному в поле Address name format (Формат имени для адреса) в R6. Можно также непосредственно внести значение в поле, чтобы задать любое законное почтовое имя в сети Internet. Пользователь, не планирующий взаимодействовать с почтовой службой сети Internet или не имеющий зарегистрированного имени домена сети Internet, может оставить поле незаполненным
Internet domain (Домен сети Internet)	Пользователю следует указать здесь домен сети Internet (при ее наличии), к которой он относится
Format (Формат) Только для R5	Эта кнопка открывает диалоговое окно Set Internet Address Format (Установка формата для адреса сети Internet). Пользователь может задавать формат адреса сети Internet и разделительный знак для почтового имени в той же сети. По умолчанию устанавливаются имя и фамилия пользователя (из полей First name , Last name), а разделительный знак не предусматривается. В таком случае почтовый адрес автора принимает следующий вид: RobKirkland@NHM_fiOMeHa. Допустимо изменить порядок следования имени пользователя, его фамилии и инициалов. В качестве разделительного знака могут применяться подчеркивание, точка или знак равенства. В версии R6 все эти параметры вводятся на вкладке Address (Адреса), доступной в режиме Advanced (Дополнительно)
Вкладка Mail (Почтовая служба)	
Mail Server (Сервер почтовой службы)	В этом поле указывается имя сервера, на котором будет храниться выделяемая пользователю база данных почтовой службы
Mail file template (Шаблон файла почтовой службы)	Здесь следует указывать шаблон проектирования, который станет основой выделяемой пользователю базы данных почтовой службы. Для пользователей R6 рекомендуется шаблон Mail (R6.0), пользователям системы Notes версии 5, а также пользователям почтовой службы POP или IMAP следует выбрать в этом поле Mail (R5.0) , а пользователям системы Notes версии 4.x надлежит ввести имя одного из более ранних шаблонов проектирования
About (Сведения о шаблоне)	Кнопка открывает окно документа About This Database (Сведения относительно базы данных) для выбранного шаблона проектирования
Set database quota (Задание квоты базы данных)	В этом окне следует вводить значение в мегабайтах для задания максимального размера выделяемой пользователю базы данных почтовой службы. После достижения базой указанного размера пользователь уже не сможет сохранять свои почтовые сообщения
Set warning threshold (Задание порога предупреждения)	Здесь следует вводить значение в мегабайтах для порога предупреждения о превышении выделяемой пользователю базы данных почтовой службы. При достижении базой этого порога будет выведено предупреждающее сообщение в журнале Notes Log (Журнал

Таблица 5.1. Перечень полей, заполняемых на форме **Register Person Form** (продолжение)

Название поля	Назначение
Set warning threshold	системы Notes) почтового сервера пользователя. Можно настраивать сервер так, чтобы он уведомлял пользователя о появлении подобного сообщения (см. главу 18)
Mail system (Система почтовой службы)	Возможные варианты для данного поля включают в себя: Lotus Notes (Система Lotus Notes), Other Internet (Другие службы Internet), POP , IMAP , Other (Другие службы) и None (Не задается). В версии R6 введен дополнительный вариант iNotes . Серверы Domino поддерживают Lotus Notes, POP, IMAP и iNotes (в R6). При выборе варианта, отличного от названных, последующие два поля становятся недоступными
Mail file name (Имя файла почтовой службы)	Программа Domino Administrator использует краткое имя пользователя для формирования имени файла базы данных почтовой службы. Если пользователь знает о существовании файла почтовой службы с идентичным именем, он может отредактировать повторяющееся имя и заменить его другим либо оставить без изменений. При его регистрации и возникновении конфликтной ситуации программа Domino Administrator по умолчанию уведомит о конфликте и предоставит возможность изменить имя файла
Mail file owner access (Доступ владельца файла почтовой службы)	По умолчанию пользователям обеспечивается наивысший уровень доступа — Manager — к файлам почтовой службы. Некоторые администраторы предпочитают предоставлять более низкий уровень доступа, что позволяет избавить любопытных пользователей от серьезных проблем
Create file now (Создание файла сразу)	Следует установить один из двух флажков. Вариант Create file now предложен по умолчанию. При выборе другого варианта процесс Administration Process сервера почтовой службы сформирует этот файл позже, что позволит заметно ускорить операцию регистрации (поскольку отпадет необходимость ожидать создания файла почтовой службы). Но в таком случае могут возникнуть сбои при регистрации, если ранее уже был создан файл почтовой службы с идентичным именем
Create file in background (Создание файла в фоновом режиме)	
Create full text index (Создание полнотекстового индекса)	Установка этого флажка предписывает программе Domino Administrator создание полнотекстового индекса для базы данных почтовой службы. Подобные индексы существенно ускоряют процесс поиска в базе данных, но занимают много места на жестком диске
Вкладка ID Info (Информация об идентификационных данных)	
Certifier ID (Идентификационные данные сертификата)	Щелкните по этой кнопке, чтобы изменить идентификационные данные сертификатора для определенного пользователя
Security type (Тип обеспечения безопасности)	Здесь следует задать вариант International (Международный) при работе с пользователем, который находится за пределами территорий США и Канады
Certificate expiration date (Дата завершения действия сертификата)	По умолчанию временной интервал продолжительностью в два года отсчитывается от текущей даты (после чего необходима повторная сертификация пользователя). Этот срок можно изменить

Таблица 5.1. Перечень полей, заполняемых на форме **Register Person Form** (продолжение)

Название поля	Назначение
Certificate expiration date	желаемым образом, но надо помнить, что идентификационные данные необходимо периодически менять. Иначе со временем накапливается большое число неиспользуемых идентификационных данных и возрастает вероятность несанкционированного доступа к серверу, поскольку одни сотрудники увольняются, а другие приходят
Location for storing user ID (Место хранения идентификационных данных пользователя): In Domino directory (В каталоге сервера Domino) In file (В файле) In mail file (В почтовом файле, R6)	В этом поле следует указать место хранения вновь созданных идентификационных данных: в персональном документе нового пользователя, в файле идентификационных данных на диске или в почтовом файле (R6). Если выбирается вариант In file или In mail file , можно щелкнуть по кнопке Set ID File (Установка файла идентификационных данных) для изменения местоположения на диске и имени файла. Файлы с новыми идентификационными данными следует запоминать в персональном документе в том случае, если предусматривается использование трудно дешифрируемого пароля. Файлы с новыми идентификационными данными надо сохранять на диске, если пароль считается легко дешифрируемым. Сбросьте все флажки при создании пользователей не-Notes (например, пользователей почтовых служб POP или IMAP)
Вкладка Groups (Группы)	
Assign person to group(s) (Занесение пользователя в группу или группы)	В этом поле будет присутствовать перечень групп базы данных Domain Directory (Каталог домена). Щелкните по группе для ее выделения в списке или выберите несколько групп, щелкнув по левому столбцу для добавления маркеров к выбираемым группам
Selected groups (Выбранные группы)	Группы, появляющиеся в данном списке, соответствуют группам, в которые планируется добавить пользователя
Add (Добавить), Remove (Удалить), Remove All (Удалить всех)	Щелкните по кнопке Add для добавления в правый список групп, выбранных в левом списке Щелкните по кнопке Remove , если надо удалить выбранные группы из правого списка Щелкните по кнопке Remove All , чтобы убрать все группы из правого списка
Вкладка Other (Прочие)	
Setup profile (Задание профиля)	С помощью этого поля следует указать профиль для данного пользователя
Unique org unit (Уникальная организационная единица)	Здесь нужно задавать полное различающееся имя так, чтобы ни у кого из пользователей не было совпадающих имен. Однако всегда остается небольшая вероятность того, что два пользователя имеют одинаковые имена, инициалы и фамилии, а также принадлежат к одной организационной единице (OU). Если на практике возникает подобная ситуация, необходимо указывать в этом поле уникальное имя OU, чтобы правильно различить таких сотрудников. Для данной OU в таком случае не существует сертификатора. Подобный подход является типовым для различения сотрудников, имеющих совпадающие имена, фамилии и инициалы

Таблица 5.1. Перечень полей, заполняемых на форме **Register Person Form** (окончание)

Название поля	Назначение
Location (Местоположение)	Поле предназначено исключительно для информационных целей. Присутствующие в нем сведения передаются в поле Location (Местоположение) персонального документа пользователя
Local administrator (Локальный администратор)	В поле можно вводить имена пользователей или групп. Пользователи, чьи имена появляются (если они имеют уровень доступа Author к базе данных Domain Directory), будут передаваться в поле Administrators (Администраторы) их персонального документа и получают право на редактирование данного документа. Воспользуйтесь этим полем для придания административных полномочий узкому кругу руководителей
Comment (Комментарии)	Указанное поле используется исключительно для информационных целей. Данные из него будут переноситься в поле Comment (Комментарии) персонального документа пользователя
Alternate name language (Альтернативный язык для имен)	Если планируется применение альтернативного языка для ввода имен, следует выбрать этот язык в списке (см. раздел об альтернативных языках)
Alternate name (Альтернативное имя)	Здесь рекомендуется вводить имя пользователя в том виде, в котором оно приводится на альтернативном языке
Alternate org unit (Альтернативное имя организационной единицы)	Если пользователь включен в уникальную организационную единицу (OU), имя этой OU указывается так, как оно выглядит на альтернативном языке
Add this person to Windows NT (Добавление данного пользователя в операционную систему Windows NT) в R5 или кнопка Windows User Options (Параметры пользователя в системе Windows) в R6	Рекомендуется установить флажок (R5) или щелкнуть по кнопке (R6) в случае необходимости сформировать учетную запись пользователя в операционной системе с помощью программы Domino Administrator. Такую возможность надо предварительно обсудить с администратором, ответственным за поддержку операционной системы. В версии R6 пользователь добавляется в операционные системы Windows NT и Windows 2000
Windows NT user name (Имя пользователя в операционной системе Windows NT)	Если решено добавить пользователя в Windows, следует ввести в этом поле учетное имя пользователя в операционной системе
Add person to Windows NT group (Добавить пользователя в группу операционной системы Windows NT)	Если решено добавить пользователя в Windows, следует выбирать группу операционной системы Windows NT для добавления в нее пользователя, например группу Domain Users (Пользователи домена)

Добавление информации для восстановления в идентификационные данные сертификатора

После регистрации хотя бы административных пользователей можно заняться установкой восстановления идентификационных данных и пароля. Эта функция, появившаяся в версии 5, позволяет автоматизировать процесс восстановления утерянных идентификационных данных, в частности тех, пользователи которых забыли свой пароль. В более ранних версиях системы Notes/Domino идентификационные данные могли быть заменены архивными копиями. Однако такое решение проблемы трудно признать идеальным, поскольку подобные копии зачастую не учитывают ряда изменений, скажем тех, которые имели место с момента повторной сертификации (за это время могли добавиться ключи шифрования, поменяться имена, а также появиться другая информация). Кроме того, при проведении архивирования в большей части организаций администраторы системы Notes обычно оставляют под рукой нешифрованные резервные копии всех идентификационных данных и паролей, что увеличивает шансы их несанкционированного использования.

В версии 5.0 предложен новый способ восстановления идентификационных данных и паролей, когда информация, служащая для открытия файла идентификационных данных (в случае утери пароля), записывается непосредственно в сам файл. Ранее архивированная копия идентификационных данных (используемая для замены утерянных данных) хранится в базе данных системы Notes в зашифрованном виде, а новая резервная копия автоматически передается в базу данных архивирования при каждом изменении в рабочей копии пользователя.

Для использования преимуществ, которые предоставляет восстановление идентификационных данных, следует добавлять в эти данные соответствующую информацию о восстановлении, что лучше всего делать на этапе создания самих идентификационных данных, поскольку в этот момент добавление может быть организовано автоматически. Если формированием системы восстановления данных не удастся заняться до создания большого числа серверов и пользователей, в дальнейшем будет труднее вносить указанную информацию, поскольку в процесс приходится вовлекать самих владельцев идентификационных данных. Владельцы и пользователи - люди, конечно, весьма занятые, сосредоточенные на решении собственных проблем, - весьма неохотно откликаются на просьбы администраторов. Особенно сложно оказывается добавлять подобную информацию для пользователей, располагающих несколькими копиями идентификационных данных. В этом случае приходится работать с каждой копией индивидуально и учитывать ту информацию, которая ранее заносилась в другие копии.

Иначе говоря, имеется настоятельная необходимость активизировать функцию восстановления идентификационных данных/паролей и дополнить эти данные соответствующей информацией уже на настоящем этапе, то есть еще до проведения регистрации большого числа серверов и пользователей. Возникает, однако, одна проблема, поскольку необходимо сначала зарегистрировать администраторов, которые будут участвовать в процессе восстановления идентификационных данных до привнесения дополнительной информации. Дело в том, что открытые ключи администраторов потребуются во время установки и запуска процесса восстановления.

В соответствии со способом восстановления идентификационных данных и паролей, реализуемым начиная с версии R5, зашифрованная копия каждого файла идентификационных данных пользователя хранится в специально созданной базе данных. Шифрование файла идентификационных данных производится с помощью одного или нескольких случайным образом формируемых паролей, каждый из которых также зашифрован посредством открытого ключа администратора. Таким образом, для дешифрования архивного файла идентификационных данных администратор должен инициировать операцию дешифрования, воспользовавшись зашифрованными паролями.

При установке восстановления идентификационных данных/паролей надо принять решение относительно числа администраторов, которые будут привлекаться к операции дешифрования файла. Следует, конечно, стремиться к уменьшению этого числа, однако специалисты компании Lotus рекомендуют, чтобы их было не менее трех человек, поскольку тем самым будут созданы определенные трудности для администраторов, желающих дешифровать идентификационные данные пользователей в собственных целях. Настройку описанной функции можно, скажем, производить таким образом, чтобы шифрование идентификационных данных производилось пятью открытыми ключами различных администраторов, а для дешифрования данных было достаточно любых трех из них. И если администраторы *A* и *B* будут не в состоянии осуществить дешифрование, другие администраторы, *C*, *D* и *E*, все-таки сумеют выполнить эту операцию.

Тем не менее число дешифрирующих лиц в значительной степени зависит от политики обеспечения безопасности, которую проводит компания. Обычно достаточно троих-пяти администраторов, а в ряде случаев и двоих. Если же проблема безопасности не стоит очень остро, можно вообще обойтись только одним администратором.

Если общее число администраторов в организации невелико и они не справляются с многочисленными функциями, требующимися для цифровой подписи различных данных и документов, можно привлекать сотрудников, не имеющих статуса администраторов. Необходимо лишь убедиться, что эти сотрудники являются постоянными работниками компании и останутся таковыми еще в течение продолжительного времени. Если в дальнейшем они покинут организацию, придется внести изменения в информацию, предназначенную для восстановления идентификационных данных и паролей. При инициировании такой операции система Notes будет автоматически обновлять информацию для соответствующих пользователей.

В некоторых организациях может быть принято решение о создании так называемых *функциональных идентификационных данных*, которые служат исключительно при дешифровании. Подобная практика типична для систем Notes и предусматривает формирование специальных идентификационных данных для разрешения различных проблем администрирования. Так, один консультант всегда пользовался именем Primary Administrator (Первый администратор) при установке первого сервера, а затем передавал это имя собственно администраторам системы Notes (совместно с соответствующими идентификационными данными). Описанная практика в целом аналогична той, при которой сетевые администраторы регистрируются под именами Admin, Administrator, Supervisor, SuperUser или root при решении различных административных задач.

Однако в большинстве случаев не рекомендуется пользоваться специальными именами администраторов и формировать специальные идентификационные данные, поскольку это заметно усложняет идентификацию пользователей системы Notes. Кроме того, при привлечении сразу нескольких администраторов они обязательно выберут имя типа Primary

Administrator/Stillwater, что не позволит провести аудит и выяснить конкретные результаты работы каждого администратора в отдельности.

Для настройки функции восстановления идентификационных данных/пароля необходимо выполнить следующие операции:

1. Создайте базу данных для входящих почтовых сообщений, которая намечена для хранения резервных копий файлов идентификационных данных пользователей.
2. Добавьте в файлы идентификационных данных сертификатов информацию для восстановления - имена администраторов, которых планируется привлечь к процессу восстановления; название базы данных Mail-In (Входящие почтовые сообщения), в которой будут храниться идентификационные данные; число администраторов, необходимых для восстановления файла идентификационных данных.
3. Модифицируйте уже существующие идентификационные данные пользователей с помощью заданной информации о восстановлении (идентификационные данные, которые ранее регистрировались по идентификационным данным сертификатора с уже добавленной информацией для восстановления, автоматически получают сведения для собственного восстановления).

Создание базы данных входящих почтовых сообщений

Формировать базу данных входящих почтовых сообщений (на шаге 1) можно с помощью шаблона базы данных. Компания Lotus предлагает специальные шаблоны баз данных почтовой службы. Если на жестком диске имеется свободное пространство, то проблем практически не возникает, но лучше все же создавать собственную базу данных. Возможно, это всего лишь перестраховка, однако применение шаблона базы данных размером в 5,3 Мб для хранения файлов идентификационных данных пользователей представляется недостаточно обоснованным. Предпочтительнее воспользоваться обычной базой данных (размером 400 Кб), имеющей один вид и одну форму. Таким образом, пользователям лучше самостоятельно построить базу данных (без обращения к шаблонам) с одним видом и одной формой (о которых мы расскажем ниже).

Теперь следует непосредственно заняться созданием базы данных для входящих почтовых сообщений:

1. В программе Domino Administrator выполните **File => Database => New** (Файл => База данных => Новый), в результате чего появится диалоговое окно **New Database** (Новая база данных). Заполните следующие поля:
 - **Server** (Сервер). Укажите тот сервер, на котором будет храниться создаваемая база данных. Здесь не следует задавать вариант **Local** (Локальный), если только не предусматривается применение копии программы Domino Administrator, использующей папки данных совместно с сервером;
 - **Title** (Заголовок). Введите заголовок произвольного вида (размером до 32 символов), например ID Recovery Database (База данных для восстановления идентификационных данных);
 - **File name** (Имя файла). Внесите в поле имя файла, например idrecovery.nsf;
 - **Encryption** (Шифрование). Щелкните по этой кнопке и в открывшемся диалоговом окне запретите локальное шифрование базы данных. Каждая запись нашей базы данных будет автоматически шифроваться процессом администрирования;

- **Template** (Шаблон) и **Server** (Сервер). Допускается оставить эти поля без изменения с установленным вариантом **Blank** (Не заполнено) или указать имя сервера, на котором будет храниться база данных, а затем назначить шаблон почтовой службы **Mail (R5.0)** или **Mail (R6.0)**, причем шаблон версии 4 также оказывается вполне приемлемым.
2. Затем необходимо щелкнуть по кнопке **Advanced** (Дополнительно), а в открывшемся диалоговом окне **Advanced Database Options** (Дополнительные параметры базы данных) установить следующие флажки:
 - **Don't maintain unread marks** (Не поддерживать нечитаемые метки);
 - **Don't support specialized response hierarchy** (Не поддерживать иерархии специализированных ответов);
 - **Don't allow headline monitoring** (Запретить мониторинг заголовков).
 3. Далее, воспользовавшись кнопкой **OK**, вернитесь в диалоговое окно **New Database**. Снова щелкните по кнопке **OK**, чтобы начать формирование базы данных на сервере, причем пользователь и сервер получают уровень доступа **Manager** в соответствующем списке **ACL**. Затем база данных будет открыта.
 4. В открытой новой базе данных выполните **File => Database => Access Control** (Файл => База данных => Управление доступом), чтобы вызвать диалоговое окно **Access Control List** (Список управления доступом). Для параметра **-Default-** (По умолчанию) укажите значение **No access** (Без доступа). После этого добавьте группу **Administrators** (Администраторы) и определите для нее тип пользователя **Person Group** (Группа сотрудников), а уровень доступа - **Reader** (Читатель). Вновь щелкните по кнопке **OK** и закройте диалоговое окно. Одновременно можно закрыть и саму базу данных.

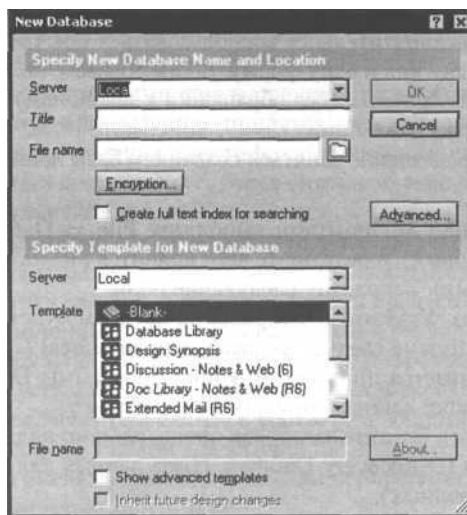


Рис. 5.5. При создании базы для восстановления идентификационных данных требуется выбрать только сервер, заголовок и имя файла

Создание документа базы данных входящих почтовых сообщений

Созданная база данных пока еще не может считаться базой данных почтовой службы, поэтому для завершения процесса необходимо выполнить следующие действия:

1. В программе Domino Administrator убедитесь в том, что правильно выбран сервер домена, а затем перейдите на вкладку **People & Groups** (Сотрудники и группы).
2. В левой части экрана на панели **Tasks** (Задачи) выберите **Mail-In Databases & Resources** (Базы данных и ресурсы входящих почтовых сообщений). В центре экрана появится соответствующий вид.
3. Щелкните по кнопке **Add Mail-In Database** (Добавление базы данных входящих почтовых сообщений), расположенной в центре экрана над видом базы данных. Откроется форма **Mail-In Database** (База данных входящих почтовых сообщений), в которой необходимо заполнить ряд полей:
 - на вкладке **Basics** (Основные параметры):
 - **Mail-In Name** (Имя базы данных входящих почтовых сообщений). Здесь можно вводить любое информативное имя, например ID Recovery Archive (Архив для восстановления идентификационных данных), которое не обязано совпадать с именем файла или заголовком созданной ранее базы данных, хотя на практике это допускается. Указанное имя будет служить в качестве адреса базы данных входящих почтовых сообщений, причем в дальнейшем его разрешается изменить (при добавлении информации для восстановления в идентификационные данные сертификатора);
 - **Description** (Описание). Поле предназначено для внесения описания, призванного напомнить о назначении данного документа, например **The ID and Password Recovery database** (База данных для восстановления идентификационных данных и пароля);
 - на вкладке **Database Information** (Информация о базе данных) требуется заполнить три поля. В R6 эти поля находятся в разделе **Location** (Местоположение) вкладки **Basics**:
 - **Domain** (Домен). В это поле вводится имя домена, например Stillwater;
 - **Server** (Сервер). Следует указать полное различающееся имя сервера, на котором планируется хранить базу данных (если ее предполагается поместить на нескольких серверах, достаточно указать имя только одного из них). В нашем примере таким именем может стать Osprey/Servers/Stillwater;
 - **Filename** (Имя файла). Поле предназначено для внесения имени файла базы данных, хранящейся на сервере, имя которого определено в предшествующем поле (например, idercovary.nsf).
4. Сохраните и закройте новый документ базы данных входящих почтовых сообщений.

Создание формы и вида

Если отказаться от применения шаблона проектирования в процессе формирования базы для восстановления идентификационных данных, потребуется создавать соответствующие

форму и вид, чтобы помочь администратору в поиске резервных файлов идентификационных данных пользователей. Для этих целей понадобится программа Domino Designer.

Создание формы

Создаваемая форма имеет три поля: текстовое поле **From** (От), поле данных/времени **ComposedDate** и поле расширенного текста **Body** (рис. 5.6).

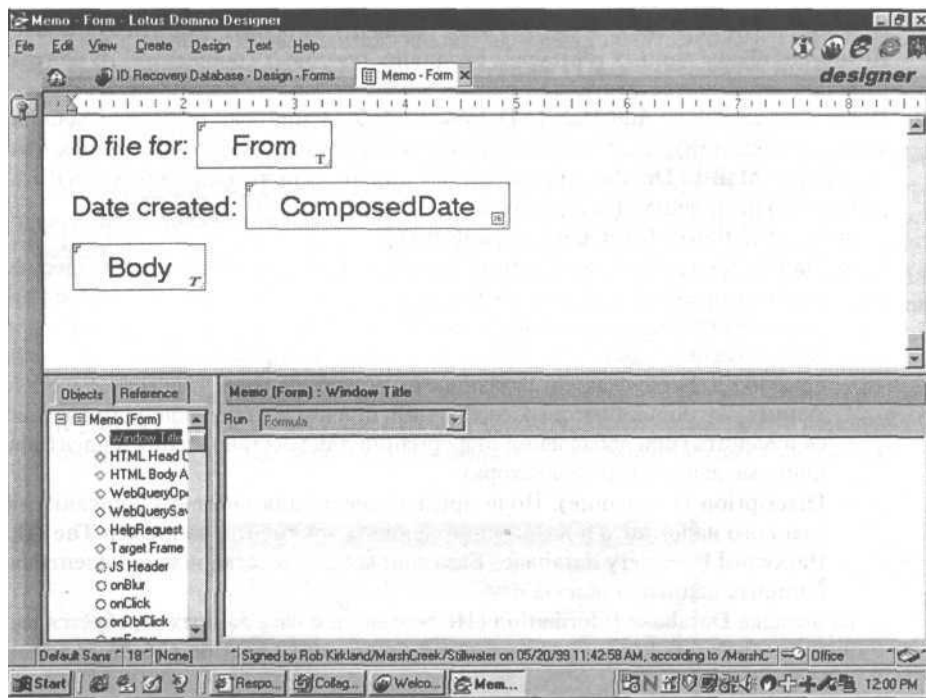


Рис. 5.6. б небольшой форме можно помещать текст, набранный крупным шрифтом
(в данном случае величиной 18 пунктов)

Чтобы добавить такую форму в базу данных, выполните следующие действия:

1. Откройте базу данных в программе Domino Designer. Это можно сделать несколькими способами. Наиболее простой из них предполагает выбор команды **Design** (Проектирование) в меню **View** (Вид), что не всегда возможно.
2. База данных будет выведена на виде **Forms** (Формы). Если такого не произойдет, щелкните по закладке **Recent Databases** (Последние использовавшиеся базы данных), расположенной в правой части экрана, и обратитесь к панели **Design** (Проектирование). На панели появится значок нужной базы данных; раскройте его, чтобы показать виды, затем выберите **Forms** (Формы). В результате на панели **Work** (Рабочая) отобразится незаполненный список форм.
3. Щелкните по кнопке **New Form** (Новая форма), находящейся в верхней части панели **Work**, после чего на экране будет видна новая форма.

4. В меню выберите **Design => Form Properties** (Проектирование => Свойства формы).
5. На вкладке **Form Properties => Form Info** (Свойства формы => Данные формы) заполните три поля, потом закройте окно свойств формы:
 - **Name** (Имя) - укажите имя формы, например Мемо;
 - **Display** (Показ) - задайте вариант **Include in menu** (Включить в меню);
 - **Options** (Параметры) - выберите **Default database form** (Форма базы данных по умолчанию).
6. Теперь установите две метки в отдельных строках формы: «**ID file for:**» (Файл идентификационных данных для) и «**Creation Date:**» (Дата создания), причем после каждого двоеточия вставьте пробел (см. рис. 5.6).
7. Добавьте два поля справа от меток полей и третье поле в строке, расположенной под первыми двумя строками. Для этого поместите курсор в том месте, где планируется вставить поле, и укажите в меню **Create** (Создание) пункт **Field** (Поле). Любое вновь созданное поле появится в форме и одновременно откроется диалоговое окно **Field Properties** (Свойства поля), в котором следует поместить информацию для каждого поля, причем имена полей необходимо указывать в полном соответствии с теми именами, которые приводятся в табл. 5.2 (с учетом регистра и пробелов).
8. После завершения операций сохраните и закройте форму.

Таблица 5.2. Имена полей и типы данных для формы Мемо

Поле	Вводимые данные
Первое поле, рядом с меткой ID FILE FOR: (Файл идентификационных данных для):	
Имя	From
Тип	Text, Editable (Текст, редактируемый)
Второе поле, рядом с меткой DATE CREATED: (Дата создания)	
Имя	ComposedDate
Тип	Data/Time, Editable (Дата/время, редактируемые)
Третье поле	
Имя	Body
Тип	Rich Text, Editable (Расширенный текст, редактируемый)

Создание вида

#

На следующем этапе необходимо преобразовать созданный и неозаглавленный вид в полезный программный инструмент. Для этого вида рекомендуется задать имя **By Name** (По имени) и организовать два столбца для занесения имени автора (**Author**) и даты создания (**Creation Date**) соответственно. В обоих столбцах будет выполняться операция сортировки (по возрастающей) - рис. 5.7.

Чтобы создать требуемый вид:

1. В программе Domino Designer щелчком по значку **Recent Databases** (Последние использованные базы данных), расположенному на правой границе экрана, вызовите панель **Design** (Проектирование). Под значком базы данных выберите **Views** (Виды), и на панель **Work** (Рабочая) будет выведен перечень форм.
2. Разверните вид **Untitled** (Без заголовка), дважды щелкнув по нему мышью.

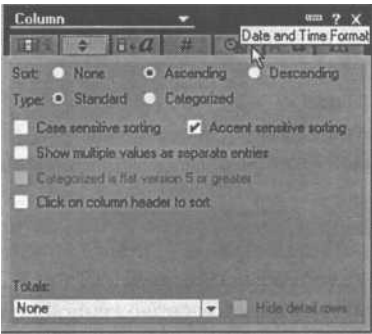


Рис. 5.7. Задержав указатель мыши на вкладке в окне **Properties**, можно получить справку с названием этой вкладки

- 3. В меню выполните Design => View Properties (Проектирование => Свойства вида) для открытия окна View Properties (Свойства вида).
- 4. На вкладке View Properties => View Info (Свойства вида => Данные вида) задайте в поле Name (Имя) вариант By Name (По имени).
- 5. На данном шаге вид имеет только один столбец, в заголовке которого находится символ #. После двойного щелчка по кнопке заголовка столбца окно View Properties преобразуется в окно Colomn Properties (Свойства столбца). Теперь необходимо произвести соответствующие изменения с учетом данных из табл. 5.3.

Таблица 5.3. Свойства первого столбца

Метка	Операции
Title (Заглавие)	Вкладка COLUMN INFO (Данные столбца). Удаление знака #
Sort (Сортировка)	Вкладка SORTING (Сортировка) Ascending (Сортировка по возрастающей)

- 6. Проверьте, что остался выделенным заголовок первого столбца, а затем выполните Simple Function (Простая функция) и Author(s) => Simple Name (Авторы => Простое имя) на панели Programmer's Pane (Панель программиста), расположенной в правой нижней части экрана.
- 7. В меню выберите Create => Append New Column (Создание => Добавление нового столбца).
- 8. В окне Colomn Properties (Свойства столбца) для нового столбца следует ввести данные согласно табл. 5.4.
- 9. Закройте окно Colomn Properties.
- 10. Убедитесь в том, что выделен заголовок второго столбца, затем выполните Simple Function и Create Date (Дата создания) на панели Programmer's Pane.
- 11. Сохраните и закройте созданный вид.

Таблица 5.4. Свойств второго столбца

Метка	Операция
Sort (Сортировка)	Вкладка SORTING (Сортировка) Ascending (Сортировка по возрастающей)
Show (Вывод)	Вкладка DATE AND TIME FORMAT (Формат для даты и времени) Data only (Только дата)

Добавление информации о восстановлении в идентификационные данные сертификатора

Чтобы добавить информацию, предназначенную для восстановления идентификационных данных, в идентификационные данные сертификатора, необходимо выполнить следующие операции:

1. В программе Domino Administrator убедитесь в том, что сервер выбран правильно и перейдите на вкладку **Configuration** (Конфигурация).
2. На панели **Tools** (Программные инструменты) выберите **Certification => Edit Recovery Information** (Сертификация => Редактирование информации для восстановления).
3. В диалоговом окне **Choose a Certifier** (Выбор сертификатора) укажите те идентификационные данные сертификатора, которые планируется использовать для регистрации сотрудников. После этого щелкните по кнопке **Open** (Открыть) и введите пароль для идентификационных данных. В результате появится диалоговое окно **Edit Master Recovery Authority List** (Редактирование главного списка авторизаторов восстановления) - рис. 5.8.

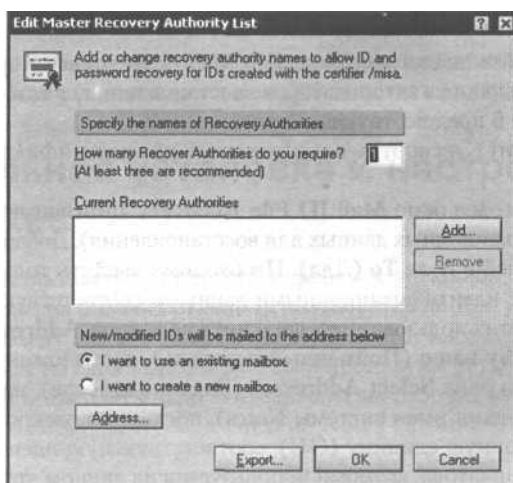


Рис. 5.8. Добавьте имена администраторов в список *Current Recovery Authorities*. Одновременно следует ввести имя базы данных входящих почтовых сообщений, щелкнув по кнопке *Address*, и принять решение о числе администраторов, участвующих в процедуре восстановления идентификационных данных

Задайте число в поле **How many Recovery Authorities do you require?** (Число требуемых для восстановления авторизаторов). Следует отметить, что чем более жесткие требования предъявляются в компании к мерам обеспечения безопасности (в частности, к защите идентификационных данных), тем большее число ответственных лиц надо привлекать к такому процессу. Естественно, это число не должно быть больше числа имен, установленного в поле **Current Recovery Authorities**

(Текущие авторизаторы восстановления), а на практике не должно превышать трех человек.

5. Щелкните по кнопке **Add** (Добавление), чтобы добавить имена администраторов в поле **Current Recovery Authorities** (Текущие авторизаторы восстановления). Для добавления сотрудник должен располагать собственным персональным документом в доступном каталоге, а также корректным открытым ключом, который также указывается в персональном документе – см. поле **Notes certified public key** (Открытый ключ сертификации системы Notes) в персональном документе пользователя.
6. Щелчком по кнопке **OK** закройте диалоговое окно или выполните **Export** (Экспорт) для передачи новой информации о восстановлении существующим пользователям, сертифицированным выбранным ранее сертифициатором. Более подробно операция экспорта описана в следующем разделе главы.

Экспорт информации о восстановлении существующим пользователям

Теперь следует передать новую информацию, предназначенную для целей восстановления, уже существующим пользователям, чтобы обновить идентификационные данные сертификации:

1. Повторно откройте диалоговое окно **Edit Master Recovery Authority List** (Редактирование главного списка авторизаторов восстановления) в том случае, если оно было закрыто на шаге 6 предшествующего упражнения.
2. Выполните **Export** (Экспорт) и введите пароль для идентификационных данных сертифициатора.
3. Появится диалоговое окно **Mail ID File Recovery Information** (Отправка по почте файла идентификационных данных для восстановления). Добавьте имена существующих пользователей в поле **To** (Для). Необходимо вводить только имена пользователей, связанных с идентификационными данными соответствующего сертифициатора. Для выделения этих пользователей щелкните по кнопке **Address** (Адрес) и поменяйте вариант **List by name** (Поименный перечень), расположенный в нижнем левом углу диалогового окна **Select Addresses** (Задание адресов), на вариант **Notes name Hierarchy** (Иерархия имен системы Notes), после чего раскройте организацию (О) или организационную единицу (OU), соответствующую идентификационным данным того сертифициатора, который используется на данном этапе. В результате нужные имена появятся ниже значка организации или организационной единицы.
4. При необходимости информацию можно заносить и в другие поля. Например, пояснения допускается добавлять в поле **Body**, скажем в виде *This will allow us to recover your password should you forget it or to recover your ID file should it become lost or corrupted in the future* (это позволяет восстанавливать пароль в случае его утери и файл идентификационных данных, если он утерян или поврежден).
5. Щелкните по кнопке **Send** (Пересылка) для передачи этого сообщения адресатам и закройте диалоговое окно. Затем щелчком по кнопке **OK** закройте диалоговое окно **Edit Master Recovery Authority List**.

При получении данного почтового сообщения адресаты должны выполнить команду **Accept Recovery Information** (Принять информацию для восстановления) в меню **Action**

(Операции). Появится запрос на ввод пароля, после задания которого откроется диалоговое окно **Backup ID file** (Файл резервных идентификационных данных), где адресат должен щелкнуть по кнопке **Send** (Пересылка).

Это позволит загрузить информацию, связанную с процессом восстановления, в файл идентификационных данных, а также в ту его копию, которая будет передана в базу, предназначенную для восстановления идентификационных данных. Направленная по почте копия файла шифруется с помощью случайно выбранного ключа, который в свою очередь будет зашифрован открытыми ключами лиц, привлекаемых к процедуре восстановления, и может быть дешифрован только с их участием.

По поводу последних этапов можно дать несколько общих рекомендаций.

Все пользователи, зарегистрированные с использованием идентификационных данных сертификатора, в дальнейшем будут автоматически снабжаться копиями своих идентификационных данных, направляемых в базу данных восстановления идентификационных данных во время регистрации.

Если в будущем информация о восстановлении в некотором файле сертификатора изменится, например в результате добавления или исключения из соответствующего перечня администраторов, придется экспортировать обновленную информацию всем существующим пользователям, а они должны будут ее принимать и выполнять необходимые действия для обновления (см. выше).

В нежелательной ситуации, когда пользователь теряет файл идентификационных данных или забывает пароль, придется воспользоваться рекомендациями главы 12 для проведения процедуры восстановления пароля или файла идентификационных данных.

Первоначальная установка и настройка клиента Notes

После регистрации пользователей следует перейти к установке и конфигурированию клиентов системы Notes на рабочих станциях пользователей. Для установки клиента следует запустить программу InstallShield (файл setup.exe) и выбрать параметры. Программа InstallShield возьмет на себя выполнение всей процедуры установки. Для конфигурирования клиентов системы Notes надо запустить их на рабочих станциях пользователей и указать еще несколько параметров, а система Notes автоматически настроит клиентские программы.

Установка клиентов системы Notes

Существует несколько способов установки клиентов системы Notes на рабочих станциях пользователей. Так, можно сделать это с помощью режима **AutoRun** (Автозапуск) или программы InstallShield. Установку проводят непосредственно с дистрибутивного диска CD-ROM или предварительно скопировав содержимое этого диска на файловый сервер и затем обратившись при инсталлировании к данному серверу. Возможна также стандартная установка или установка с совместным использованием (когда несколько пользователей совместно применяют одну папку программы, но имеют собственные папки данных). И наконец, допустимо автоматизировать процедуру с помощью *файла ответных сообщений* (см. главу 6).

Устанавливаемые программы

При установке клиента Notes надо одновременно устанавливать целый ряд программ, присутствующих на диске CD-ROM:

- О Adobe Acrobat Reader. Программа позволяет читать файлы Adobe PDF (Формат перемещаемых документов). Основной смысл ее присутствия на диске CD-ROM состоит в том, что можно будет читать и выводить на печать форматированные копии справочных данных (файл readme.pdf) еще до установки самой клиентской программы;
- О Domino Global WorkBench. Предназначена исключительно для разработчиков приложений и дает им возможность заметно уменьшить объем усилий при создании многоязычных приложений;
- О Actioneer for Lotus Notes. Эта относительно небольшая по размерам программа, которую пользователь системы Notes может загрузить в память во время запуска компьютера, служит для добавления записи в календарь, списка работ и персонального журнала без обращения к клиенту системы Notes. Следует лишь открыть окно **Actioneer** (Инициатор действий), дважды щелкнув по значку программы на панели задач операционной системы Windows или воспользовавшись специальной клавиатурной комбинацией, после чего можно приступать к формированию и внесению записей. Программа Actioneer при вводе различает записи по типам и автоматически направляет информацию в календарь, список работ или журнал, что весьма удобно;
- О IBM ViaVoice Runtime. Спустя некоторое время после выхода версии R5 программа Actioneer for Lotus Notes «научилась» реагировать на речевые команды. Для этого необходима библиотека реального времени IBM ViaVoice Runtime, которую допустимо устанавливать уже на данном этапе, чтобы сразу расширить возможности программы Actioneer.

Комбинация программ, планируемая к установке на рабочей станции, полностью зависит от действий и операций, которые намерены выполнять разные группы пользователей:

- О для большей части пользователей системы Notes на рабочих станциях можно ограничиться при установке клиента Notes программами **IBM ViaVoice Runtime** и **Actioneer**;
- О для разработчиков приложений требуется программа **Domino Designer** вместо клиента Notes (на практике устанавливаются обе программы) и, возможно, программы **Domino Global WorkBench**, **IBM ViaVoice Runtime** и **Actioneer**;
- О для администраторов серверов Domino следует установить программу **Domino Administrator**, а не клиент Notes (на практике устанавливаются обе программы), а также программы **IBM ViaVoice Runtime** и **Actioneer**.

Для некоторых пользователей (возможно, для читателей нашей книги) нужны все три оконечных компонента клиента системы Notes (**Lotus Notes**, **Domino Administrator** и **Domino Designer**). Однако учтите, что их установка допускается только при наличии лицензии.

Если кто-либо из сотрудников в организации вместе с системой Notes R5 использует пакет **SmartSuite**, придется установить **SSN5 Update for Notes 5** и **SmartSuite**. В этом случае удастся, в частности, устранить ошибку, связанную с очень медленной работой приложений **SmartSuite** совместно с Notes 5 (см. папку \Apps\SmartSuite на диске CD-ROM). Версия R6 поддерживает пакет **SmartSuite 2.0**, причем пока не замечено каких-либо противопоказаний для совместной работы сервера Domino 6 или клиента Notes R6 и **SmartSuite 2.0**.

Для работы с кодировками, отличными от латинского алфавита, на диске CD-ROM имеется набор шрифтов TrueType, обеспечивающий поддержку греческого алфавита, кириллицы, славянских символов, букв турецкого и арабского алфавитов, символов иврита, японских иероглифов, а также упрощенных и традиционных китайских иероглифов.

Сравнение возможностей AutoRun и InstallShield

Основным преимуществом режима AutoRun (Автозапуск) является то, что необходим только дистрибутивный диск CD-ROM. Пользователь может посмотреть короткий вступительный анимационный комментарий (продолжительностью 15 с), сопровождающийся легкой музыкой. Анимационная программа имеет хороший интерфейс управления, а главное - внимание в этом комментарии фокусируется на проблемах, которые, по мнению специалистов компании Lotus, должны быть пользователям хорошо известны (например, необходимость познакомиться с Guided Tours), но при просмотре внушительного перечня папок их легко упустить из виду.

После щелчка по кнопке **Install** (Установка) одна из оконечных программ системы Notes запустит Мастера InstallShield, который позволит указать параметры установки клиентской программы Notes. Здесь приходится иметь дело с меньшим числом экранов (чем в режиме AutoRun), поэтому процедура установки идет быстрее.

Тем не менее пользователям рекомендуется хотя бы один раз воспользоваться функцией AutoRun. Если после этого им не захочется прослушивать пространственные комментарии, а появится желание сразу начать работать с InstallShield, нужно в Проводнике Windows (Windows Explorer) перейти в определенную папку и запустить файл setup.exe (для клиента системы Notes обычно обращаются к файлу install.exe, а для некоторых приложений - к файлу имяпрограммы.exe). Затем Мастер InstallShield запросит те же данные, что и AutoRun, и результат установки будет тем же самым независимо от способа применения программы InstallShield (прямого или опосредованного).

Сравнение сетевой установки и установки с компакт-диска CD-ROM

Безразлично, где находятся дистрибутивные файлы на момент установки. При установке клиента Notes на сетевых рабочих станциях может оказаться более удобным обращаться к файлам, размещенным на файловом сервере, чем к диску CD-ROM. В случае установки Notes на рабочих станциях, не имеющих доступа к файловому серверу (или подключенных по медленным соединениям региональной сети), проще воспользоваться непосредственно диском CD-ROM.

При копировании содержимого диска CD-ROM на файловый сервер допустимо переписать все содержащиеся на нем программы, в том числе программу автозапуска AutoRun, или только отдельные папки, в которых находятся необходимые файлы. Программа AutoRun обычно хранится в одноименной папке, поэтому отменить ее копирование легко.

На дистрибутивном компакт-диске Notes 5.0 и Notes 6.0 есть программы для установки клиентов на платформе Intel/Windows (Windows 95/98/NT, а также Windows 2000/XP для версии R6) и на платформе Alpha/Windows NT. Кроме того, клиент Notes 6.0 может работать на платформе Apple Macintosh, включая операционные системы Macintosh OS 9 и Macintosh OS X (только версия 10.1). Программные средства для каждой версии клиента хранятся в отдельных папках, а все прочие приложения находятся в подпапках большой папки Apps (Приложения).

Стандартная и совместно используемая установка

Стандартная установка системы Notes предусматривает размещение программ и папок в указанном месте и занесение файла notes.ini (текстовый файл инициализации в формате ASCII) в папку программ системы Notes. Либо можно инициировать режим *совместно используемой установки* (задается в Мастере InstallShield), в котором одна папка программ системы Notes обычно хранится на файловом сервере (но не на сервере Domino) и доступна для нескольких пользователей.

Подход, предусматривающий формирование совместно используемого каталога программ, обладает некоторыми преимуществами. Во-первых, в этом случае экономится память на жестких дисках рабочих станций пользователей. Во-вторых, что более важно, при обновлении системы Notes для большого числа пользователей можно ограничиться изменением только одной папки программ. В то же время данный подход имеет и два серьезных недостатка. Пользователям приходится запрашивать файлы программ клиента Notes каждый раз, когда возникает в них потребность, что приводит к заметному возрастанию сетевого трафика и способно отрицательно сказаться на характеристиках самой системы Notes и многих сопутствующих приложений. Появляется опасность эпизодического выхода из строя сервера, на котором хранится папка программ. Кроме того, обновления системы Notes зачастую касаются не только файлов программ, но и шаблонов баз данных. Поэтому при проведении подобной модификации требуется устанавливать файлы данных для каждой рабочей станции пользователей. В результате преимущество, связанное с возможностью одновременной модификации файлов программ, представляется весьма условным.

Когда решено использовать совместную установку клиента Notes, процедура практически остается той же. Пользователь должен указать папку программ и папку данных, а Мастер InstallShield автоматически создаст эти папки, заменяя установленные прежде. Небольшое отличие состоит лишь в том, что программа устанавливает файл notes.ini в папку операционной системы Windows, а не в папку программ системы Notes. Нельзя заносить файл notes.ini в папку программ, так как каждый пользователь должен располагать его индивидуальной копией.

Существует также два способа осуществления совместной установки. Во-первых, некоторые администраторы предпочитают установить папки данных пользователей на файловом сервере (обычно в домашней папке каждого пользователя). Такой подход имеет два несомненных преимущества. При совмещении с перемещаемыми профилями операционной системы Windows NT он позволяет пользователям регистрироваться в домене Windows NT с любого компьютера и применять собственные файлы программ и данных системы Notes. Кроме того, в данном случае проще формировать резервные файлы данных пользователей, поскольку они располагаются на файловом сервере, а не на индивидуальных рабочих станциях пользователей.

Во-вторых, разрешается установить файлы программ на рабочей станции пользователя, а локальные файлы данных - в его домашней папке. При этом пользователи могут локально запускать клиент Notes, но сохранять централизованное архивирование (резервное копирование) данных. К тому же они вправе запускать клиент Notes с любой рабочей станции, на которой установлен такой клиент, причем им достаточно лишь зарегистрироваться в сети, чтобы получить доступ к собственной домашней папке.

В этой ситуации может возникнуть желание отредактировать файл notes.ini для организации локального кэширования (файл cache.dsk). Система Notes сформирует подобный файл при повторном запуске, что позволит улучшить показатели быстродействия, так как

кешированные компоненты проектирования будут доступны локально и отпадет необходимость пересылать их по сети, благодаря чему заметно уменьшится сетевой трафик.

В данном случае возможны определенные варианты, связанные с размещением файлов desktop.dsk, notes.ini и user.id (на сервере файлов или локально), причем попытки синхронного использования файлов могут создавать некоторые проблемы. На практике с этими проблемами помогает справиться процедура репликации NT, а также применение пакетных командных файлов. Однако обсуждение нюансов функционирования указанных процедур выходит за рамки нашего изложения и пользователям придется прорабатывать их самостоятельно.

Для установки пользователя с размещением его папки данных на файловом сервере придется вручную копировать каждый файл notes.ini пользователя из операционной системы Windows или локальной папки системы Notes в домашнюю папку пользователя, расположенную на файловом сервере. Затем надо отредактировать командную строку для ярлыка каждого пользователя, так чтобы система Notes искала нужный файл notes.ini в папке данных пользователя. Это можно сделать двумя способами: путем редактирования поля **Target** (Целевой) либо **Start in** (Запуск в) в диалоговом окне ярлыка.

Редактирование записи в поле **Target** производится следующим образом. Управляющая команда для стандартного ярлыка клиента Notes (когда файлы программ Notes хранятся в папке p:\notes) обычно имеет вид

```
p:\notes\notes.exe
```

Эту команду следует отредактировать (если папка данных пользователя - h:\notes) таким образом:

```
p:\notes\notes.exe=h:\notes\notes.ini
```

Следует особо отметить, что в управляющей команде перед знаком равенства стоит пробел, тогда как после знака равенства подобного пробела не предусмотрено.

Либо рекомендуется редактировать поле **Start in** (если папка данных пользователя - h:\notes):

```
h:\notes
```

При изменении управляющей команды обязательно убедитесь в том, что для папки данных правильно указана буква диска. Ярлыки операционной системы Windows поддерживают стандартную схему именования этой операционной системы - например, имена типа (\\имя_компьютера\ресурс), а не отображаемые буквы дисков. Однако в файле notes.ini должны быть указаны именно буквы дисков, в частности переменная Directory этого файла указывает место файлов данных Notes с помощью букв дисков, поэтому отображенная буква диска (в рассмотренном примере - h:) должна сохраниться для всех перемещаемых профилей пользователей.

Процедура установки

Поскольку последовательность действий во время установки может быть различной и зависит от способа ее проведения (AutoRun или InstallShield), ниже эта процедура описана не пошагово, а только в общих чертах. При выполнении установки следует принять ряд решений, в частности по таким вопросам, как:

- О согласие с требованиями лицензионного соглашения;
- О совместно используемая установка (см. выше);

- О местоположение папок данных и программ:
 - если клиент Notes прежде не устанавливался на данном компьютере, местоположения папок в режиме по умолчанию соответствуют c:\lotus\notes для программ и c:\lotus\notes\data для данных;
 - если клиент Notes уже устанавливался прежде, Master InstallShield, скорее всего, предложит воспользоваться теми же папками, что и раньше (в зависимости от того, была ли инициирована отмена установки и удалены ли вручную оставшиеся папки). Кроме того, еще до начала самой процедуры установки может потребоваться сформировать резервные копии файлов names.nsf, desktop.dsk, notes.ini, а также других файлов, оставшихся от процедуры предыдущей установки (поскольку эти файлы могут быть перезаписаны);
 - следует внимательно проверять предложенные имена папок. При необходимости внесения изменений удостоверьтесь, не осталось ли копий старых данных. Не исключено, что, если система Notes в дальнейшем обнаружит данные предыдущей установки, она будет некорректно задавать местоположения для папок и файлов;
- О состав устанавливаемого клиента, определяющий, какую программу устанавливать:
 - для обычных пользователей - Notes Clients (клиент системы Notes);
 - для разработчиков приложений системы Notes целесообразно установить программу Domino Designer (обычно одновременно устанавливаются Notes Designer и Domino Designer);
 - для администраторов серверов Domino - Domino Administrator (обычно одновременно устанавливаются Notes Administrator и Domino Administrator);
 - для тех пользователей, которые планируют заниматься как разработкой, так и администрированием, можно, рекомендовать вариант **All Clients** (Все клиентские программы);
- О пользовательская настройка процедуры установки. Такой подход позволяет выбирать только те файлы, которые требуется установить. Это целесообразно, если установка производится на компьютере с ограниченной свободной дисковой памятью или при необходимости добавления какого-либо файла, например дополнительного файла справки;
- О место в меню операционной системы Windows, куда следует заносить ярлыки системы Notes. По умолчанию эти ярлыки будут размещаться в пункте меню **Lotus Applications** (Приложения системы Lotus Notes), а ярлык для Notes Minder (Напоминание пользователям системы Notes) попадает в папку меню **Startup** (Пуск). Программа Notes Minder является резидентной в памяти и служит для уведомления пользователей о поступающих в их адрес почтовых сообщениях.

Процедура конфигурирования клиента Notes

Для конфигурирования клиента Notes достаточно просто запустить в первый раз эту клиентскую программу. Если в файле notes.ini отсутствуют какие-либо необходимые параметры, система Notes активизирует Мастер Notes Client Configuration Wizard (Мастер конфигурирования клиента Notes). В процессе выполнения Мастера придется ввести ряд данных, а система Notes использует новые данные для конфигурирования клиента.

При конфигурировании клиента Notes выполняются следующие операции:

- О задание в файле notes.ini соответствующих значений переменных;
- О формирование соединения с домашним сервером пользователя и получение необходимых данных;
- О копирование файла идентификационных данных пользователя в папку данных (если это еще не было сделано);
- О создание базы данных Personal Address Book (Персональная адресная книга, файл names.nsf), журнала Notes Log (Журнал системы Notes, файл log.nsf), базы данных Headlines (Заголовки, файл headline.nsf) > базы данных абонентов (файл subscription.nsf) и баз данных настольного компьютера и кэш-памяти (файлы desktop5.dsk или desktop6.dsk и cache.dsk);
- О настройка документов местоположения (Location document) в базе Personal Address Book с помощью данных зарегистрированного пользователя;
- О добавление документов соединения (Connection document) в базу Personal Address Book (при необходимости);
- О добавление документов учетных записей (Account document) в базу Personal Address Book (при выборе этой операции во время установки);
- О конфигурирование списка Execution Control List (Список управления исполнением) пользователя.

Здесь не обсуждаются нюансы исполнения Мастера Lotus Notes Client Configuration Wizard, поскольку это уже было сделано в главе 3. Следует лишь отметить, что в данной главе под целевым пользователем понимался пользователь, работающий в офисе, связанный с локальной сетью и не испытывающий необходимости в модемном доступе к серверу или получении учетной записи для сети Internet. Поэтому процедура настройки для него практически полностью совпадает с процедурой, описанной в главе 3.

В главе 3 также проанализированы проблемы, которые могут возникать при настройке учетной записи пользователя; в случае появления сообщений об ошибках рекомендуется обратиться к материалам этой главы и выяснить причины ошибок и сбоев.

Процедура установки пользователей, которым требуется модемное соединение с сервером, подробно рассматривается в главе 6. Там же в деталях обсуждается процедура установки учетной записи для пользователя, которому требуется доступ к сети Internet (почтовая служба, каталоги, новости).

Другие рекомендации по проведению настройки для пользователей

В соответствии с рекомендациями, приведенным в начале данной главы, целый ряд важных решений должен быть принят, в частности на этапе предварительной установки. Уже проведена регистрация администраторов, которые в дальнейшем стали авторизаторами восстановления, и установка клиентских программ Notes на рабочих станциях пользователей. После этого были настроены функции восстановления идентификационных данных и пароля (см. предыдущий раздел).

Теперь система подготовлена для регистрации оставшихся пользователей, а также для установки и конфигурирования для них копий клиентов Notes. Если число пользователей, которые требуют регистрации и настройки, относительно невелико, можно прибегнуть к вышеописанной процедуре. Если же надо зарегистрировать большое число пользователей, следует автоматизировать процесс установки.

В главе 6 подробно обсуждаются следующие способы, позволяющие автоматизировать процедуры регистрации и настройки пользователей и представляющие несомненный интерес для администраторов системы:

- О регистрация пользователей с помощью текстового файла;
- О одновременная регистрация пользователей в системе Notes и операционной системе Windows NT как из клиента системы Notes, так и из средства User Manager for Domains (Диспетчер пользователей домена) операционной системы Windows NT;
- О обновление почтового программного обеспечения пользователей, применявших сторонние почтовые клиенты;
- О автоматизация процедуры установки Notes;
- О автоматизация процедуры конфигурирования Notes.

И наконец, может потребоваться провести процедуру настройки для пользователей специальных служб и программ. Так, на практике часто случается иметь дело с мобильными пользователями, которым приходится связываться с локальной сетью или сквозным сервером Domino по коммутируемым телефонным линиям, чтобы получить доступ к своим домашним серверам. Вероятно, понадобится также подключить пользователей к серверам почтовой службы сети Internet, серверам каталогов или серверам новостей. Кроме того, иногда нужно установить несколько учетных записей пользователей на одной рабочей станции (см. главу 6).



В настоящей главе продолжается обсуждение процедуры установки и настройки пользователей. В главе 5 описаны предварительные операции, которые следует производить перед внесением учетной записи, а также основные операции самого процесса установки. Здесь рассматриваются способы, позволяющие выполнять регистрацию и настройку большого числа пользователей, а также вопросы, связанные с установкой и настройкой пользователей, решающих специфические задачи, например мобильных пользователей, пользователей серверов и сети Internet и пользователей, совместно применяющих одну рабочую станцию.

В данной главе внимание сосредоточено на следующих проблемах:

- О регистрация объектов с помощью текстового файла;
- О одновременная регистрация пользователей системы Notes и операционной системы Windows NT;
- О обновления сторонних почтовых программ и импорт учетных записей пользователей из Security Accounts Manager (Диспетчер учетных записей безопасности) операционной системы Windows NT;
- О установка с помощью файла ответных сообщений для рабочих станций;
- О настройка мобильных пользователей;
- О обеспечение доступа к серверам сети Internet;
- О настройка совместно используемых рабочих станций.

Расширенные режимы регистрации пользователей

Для регистрации большого числа пользователей подходит любой программный инструмент, помогающий экономить время и усилия. Сервер Domino предоставляет несколько таких инструментов. Во-первых, можно вводить данные только один раз на экране регистрации пользователей сервера Domino или в средстве User Manager for Domino операционной системы Windows NT и одновременно создавать обе учетные записи. Во-вторых, данные пользователей могут быть получены не только обычным вводом их с клавиатуры. Допускается импортировать их из любой программы, которая позволяет сформировать

текстовый файл (в формате ASCII), из множества программ службы электронной почты, а также из менеджера Security Accounts Manager операционной системы Windows NT.

Регистрация с использованием текстового файла

Если пользователи, которых требуется зарегистрировать, уже сведены в список той или иной базы данных и этот список представлен в виде текстового файла с разделителями, лучше обойтись без повторного ввода данных и импортировать содержимое такого файла. Составляющие подобный файл данные не обязательно должны включать в себя всю необходимую информацию для регистрации. На практике небольших объемов информации, например сведений об именах пользователей, вполне хватает.

Сформировать текстовый файл можно одним из следующих способов:

- О в диалоговом окне **Register Person** (Регистрация сотрудника) импортировать данные о новых пользователях в очередь регистрации, а затем добавить к ним недостающие сведения;
- О регистрировать пользователей непосредственно с помощью текстового файла и в обход диалогового окна **Register Person**. Для этого следует выбирать **People from File** (Сотрудники из файла) в меню **Configuration => Registration** (Конфигурирование => Регистрация) на вкладке **Configuration** (Конфигурация) или **Registration from File** (Регистрация с помощью файла) в меню **People => People** (Сотрудники => Сотрудники) на вкладке **People & Groups** (Сотрудники и группы). В версии R6 следует щелкнуть по кнопке **Import Text File** (Импорт текстового файла) в окне **Register Person**. При таком подходе текстовый файл должен включать в себя пароли пользователей (и, как минимум, их имена).

В том случае, когда общие сведения для регистрируемых пользователей в текстовом файле оказываются различными (например, разные идентификационные данные сертификатора, регистрирующие серверы, серверы почтовой службы, имена существующих групп), необходимо провести импорт пользователей в очередь регистрации. В дальнейшем не составит труда ввести недостающую информацию, выбирая группы пользователей и указывая данные для конкретной группы в относительно небольшом числе полей. Если общие сведения для пользователей одинаковы, то можно смело действовать вторым способом.

Текстовый файл способен содержать до двадцати полей, расположенных в следующем порядке:

- О **Last name** (Имя). Заполняется обязательно;
- О **First name** (Фамилия);
- О **Middle initial** (Промежуточные инициалы). В данном случае можно ввести точку, если принятая в организации схема присвоения имен это допускает;
- О **User-unique organizational unit** (Индивидуальная организационная единица пользователя) в R5 или **Organizational unit** (Организационная единица) в R6. Поле следует заполнять только в том случае, когда требуется различить пользователей, имеющих одинаковые имена и использующих одни и те же идентификационные данные сертификатора (например, если в организации /Acctg/Stillwater работают две Мэри Джейн Смит, но одна из них относится к подразделению Accounts Receivable, а другая - к подразделению Accounts Payable, они могут быть обозначены соответственно как Mary Jane Smith/AR/Acctg/Stillwater и Mary Jane Smith/AP/Acctg/Stillwater, а в данном поле надо ввести символы AR для первой из них и AP для второй);

- **Password** (Пароль). Данное поле обязательно при импорте текстового файла с помощью соответствующего меню;
- **ID file folder** (Папка файла идентификационных данных) в R5 или **ID file directory** (Каталог файла идентификационных данных) в R6. Здесь указывается место хранения файла идентификационных данных пользователя (такая папка должна быть уже создана);
- **ID file name** (Имя файла идентификационных данных). Если это поле остается незаполненным, система Notes сформирует имя файла на основе имени самого пользователя;
- **Mail server name** (Имя сервера почтовой службы). Предназначено для задания имени в сокращенном виде (например, Osprey/Servers/Stillwater);
- **Mail file folder** (Папка файла почтовых сообщений) в R5 или **Mail file directory** (Каталог файла почтовых сообщений) в R6. В данном поле в папке данных сервера определяется место расположения базы данных почтовой службы пользователя;
- **Mail file name** (Имя файла почтовых сообщений). Если пользователь не укажет это имя, оно будет сформировано из первого символа его фамилии и первых семи символов имени. Специально задавать файл почтовых сообщений надо лишь в том случае, когда для двух пользователей, файлы которых находятся в одной папке, совпадают инициалы и фамилии;
- **Location** (Местоположение). Запись из поля будет передаваться в одноименное поле персонального документа;
- **Comments** (Комментарии). Отсюда запись передается в одноименное поле персонального документа;
- **Forwarding address** (Адреса передачи). Запись из данного поля будет передана в одноименное поле персонального документа;
- **Profile name** (Имя режима). Эта запись передается в одноименное поле персонального документа;
- **Local administrator** (Локальный администратор). Запись передается в одноименное поле персонального документа;
- **Internet address** (Адрес сети Internet). Запись будет передана в одноименное поле персонального документа;
- **Short name** (Сокращенное имя). Если это поле останется незаполненным, сокращенное имя пользователя будет сформировано с помощью первого символа имени пользователя и его фамилии. Следует помнить, что сокращенные имена в домене Domain должны быть сугубо индивидуальными, поэтому их требуется специально задавать в том случае, если совпадают имена, созданные по умолчанию;
- **Alternate name** (Альтернативное имя). Идентификационные данные сертификатора должны содержать информацию относительно альтернативного языка;
- **Alternate organization unit** (Альтернативное имя организационной единицы). В идентификационные данные сертификатора нужно включать информацию об альтернативном языке;
- **Mail template file name** (Имя файла шаблона почтовой службы). Если это поле не заполняется, система Notes формирует имя файла с применением имени самого пользователя.

Программа Domino Administrator предполагает, что отдельные поля импортируемого текстового файла будут разделяться с помощью точки с запятой (;). Однако для этих целей годятся и другие символы, надо только добавить переменную BatchRegSeparator=cMMBon (где

значение символ соответствует используемому разделительному символу) в файл notes.ini той рабочей станции, на которую будет передаваться текстовый файл. Текстовый файл может иметь произвольное имя, но при регулярном применении подобного подхода удобно задать имя по умолчанию, например путем введения переменной BatchRegFile=m<w_<Lai«a в файл notes.ini.

Импорт файла с помощью меню

При вызове текстового файла с помощью меню система запрашивает местоположение, имя текстового файла и пароля (для идентификационных данных сертификатора); можно щелкнуть по кнопке **Cancel** (Отмена) и выбрать другие идентифицирующие данные сертификатора, после чего появится диалоговое окно **Register People from Text File** (Регистрация сотрудников с помощью текстового файла) - рис. 6.1.

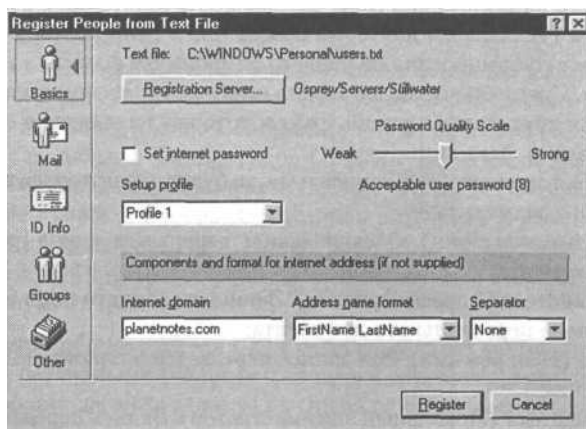


Рис. 6.1. В данном диалоговом окне определяются общие данные для всех импортируемых пользователей и шаблонов, к которым система Notes может прибегнуть при формировании данных для различных пользователей

Это диалоговое окно во многом напоминает диалоговое окно **Register Person** (Регистрация сотрудника). В него вносятся параметры, которые нельзя задать иным путем. Если введенный параметр заменяет значение, полученное из текстового файла импорта, в поле записывается введенное значение, а не импортированное. После заполнения всех полей рекомендуется воспользоваться кнопкой **Register** (Регистрация).

Импорт пользователей в очередь регистрации

Для передачи пользователей в очередь регистрации следует открыть диалоговое окно **Register Person**. Значения по умолчанию можно заносить в любые поля (за исключением тех, которые становятся недоступными; в версии R6 поля аналогичные, но окно имеет немного другой внешний вид - рис. 6.2), если в очереди регистрации выделено более одного пользователя. Выполните **Import Text file** (Импорт текстового файла), после чего найдите и укажите необходимый файл, затем щелкните по кнопке **Open** (Открыть).



Рис. 6.2. При выборе нескольких пользователей в очереди регистрации некоторые поля могут стать недоступными, например поле Mail file name (Имя файла почтовых сообщений). Состав полей, допускающих редактирование, меняется для каждого выделенного пользователя

Программа Domino Administrator будет импортировать пользователей из текстового файла в очередь регистрации. В дальнейшем можно выбирать отдельных пользователей (или группы пользователей) в очереди регистрации, редактировать значения в полях и регистрировать пользователей.

Регистрация пользователей Windows NT в качестве пользователей системы Notes

Если регистрируемые пользователи системы Notes уже имеют учетные записи в домене Windows NT, появляется возможность импортировать их в очередь регистрации либо зарегистрировать в диспетчере User Manager (Диспетчер пользователей) или User Manager for Domains (Диспетчер пользователей домена) Windows NT. Если же пользователь не имеет учетной записи в Windows NT, но требуется придать ему этот статус (для доменов Domino и Windows NT), достаточно выполнить операцию один раз в любой из систем. Программа Domino Administrator обеспечит одновременную регистрацию в Notes и Windows NT.

Первый способ, связанный с импортом пользователей Windows NT в очередь регистрации, предусматривает применение программного инструмента миграции из Microsoft Windows NT в систему Notes. Этот инструмент может быть (но не обязательно) установлен на компьютере с Windows NT во время установки программы Domino Administrator.

Миграция пользователей из операционной системы Windows NT в систему Notes

Упомянутый выше программный инструмент миграции - лишь один из подобных необязательных средств, которые можно установить в процессе инсталляции программы Domino Administrator или на более позднем этапе. Следует отметить, что его допустимо установить только на компьютере, использующем Windows NT, но не операционные системы типа Windows 9x.

Для установки инструмента миграции необходимо выбрать пользовательский вариант установки Domino Administrator. Если Мастер InstallShield запускается косвенно из оконечной надстройки AutoRun и с дистрибутивного диска CD-ROM, следует задать вариант **Custom Install** (Пользовательская установка). Если Мастер InstallShield запущен непосредственно (например, из файла setup.exe в подпапке клиентов), то надо на пятом экране задать вариант **Customize** (Пользовательский). В обоих случаях откроется экран Мастера InstallShield, где можно индивидуально выбрать устанавливаемые компоненты. В нашем случае следует указать **Migration Tools** (Программные инструменты миграции) и (необязательно) щелкнуть по кнопке **Change** (Изменение), чтобы отменить установку других программных инструментов миграции, если известно, что они в дальнейшем не потребуются.

Таблица 6.1. Параметры миграции «имени группы» для существующей группы

Параметр	Назначение
Use the existing Notes group (Использование существующей группы системы Notes)	Позволяет добавлять членов выбранной группы операционной системы Windows NT в существующую группу системы Notes
Create a new group - don't use the Notes group (Создание новой группы без использования группы системы Notes)	Позволяет добавлять членов выбранной группы операционной системы Windows NT в новую группу системы Notes
Skip this group - don't migrate it for now (Пропуск группы без незамедлительного переноса группы)	Позволяет отменить миграцию группы и ее членов

Для использования программного инструмента Microsoft Windows NT to Notes migration (Миграция пользователей операционной системы Windows NT в систему Notes) зарегистрируйтесь в качестве администратора (Administrator) или оператора учета (Account Operator) в домене NT, с которым предстоит взаимодействовать, и выполните следующие операции:

1. В программе Domino Administrator перейдите на вкладку **People & Groups**, затем откройте **Tools => People** (Программные инструменты => Сотрудники) и выполните **Register**, чтобы открыть диалоговое окно **Register Users** (Регистрация пользователей).
2. Задав параметры для режимов по умолчанию (например, качество пароля), укажите **Migrate People** (Миграция сотрудников).
3. Появится диалоговое окно **People and Groups Migration** (Миграция сотрудников и групп). В поле **Foreign directory source** (Внешний исходный каталог) задайте вариант **Windows NT Users/Groups** (Пользователи/группы операционной системы Windows NT). Если в поле присутствует только значение **None** (Нет), значит, программный инструмент миграции не установлен. В таком случае закройте программу Domino Administrator и проведите процедуру пользовательской установки этой программы или добавьте все клиентские программы сразу (**All clients**). В процессе

пользовательской установки появится возможность выбрать необходимые программные инструменты миграции и правильно их настроить.

4. Откроется диалоговое окно **Choose Windows NT Domain** (Выбор домена операционной системы Windows NT). В нем указаны доступные домены операционной системы Windows NT (а также имя используемого компьютера, если он не является контроллером домена). Назначьте домен, из которого планируется импортировать пользователей, и щелкните по кнопке ОК.
5. Пользователи и группы выбранного домена появятся в списке **Available People/Groups** (Доступные сотрудники/группы). Выберите необходимых пользователей с помощью клавиш **Ctrl**, **Shift** и **Ctrl+Shift** (выбор записей), после чего щелкните по кнопке **Add** (Добавление) либо нажмите на кнопку **Add All** (Добавление всех), а затем исключите нежелательные записи из списка миграции. При задании группы в списке **Available People/Groups** на экран будет выведено одно или несколько диалоговых окон. Так, поле **Existing Group имя_группы Migration Options** (Параметры миграции группы) появится, если будет добавлена группа операционной системы Windows NT с таким же именем, как у существующей группы системы Notes. Возможные в этом случае варианты представлены в табл. 6.1. Поле **Group Migration Options** отображается в тех случаях, когда выбранная группа Windows NT имеет имя, отличное от имени существующей группы системы Notes, или при совпадении этих имен, но после щелчка по ОК в диалоговом окне **Existing Group имя_группы Migration Options** (Параметры миграции группы). Те варианты, которые допустимы в этом случае, перечислены в табл. 6.2.
6. Можете также воспользоваться *параметрами миграции* (табл. 6.3).
7. В общем случае рекомендуется в режиме **Advanced** (Дополнительно) выбрать способ, который будет применен программным инструментом миграции при преобразовании полного имени пользователя Windows NT в фамилию, промежуточные инициалы и имя пользователя системы Notes, а также указать вариант, в соответствии с которым имя пользователя Windows NT автоматически становится сокращенным именем пользователя системы Notes.
8. Выполните **Migrate** (Миграция), при этом пользователи попадут в очередь регистрации. Затем, после завершения миграции в систему Notes, нажмите **Done** (Выполнено).

Таблица 6.2. Параметры миграции групп

Параметр	Назначение
Create a new Notes group with the following settings (Создание новой группы системы Notes со следующими параметрами)	Когда установлен данный флажок, можно ввести имя, тип и описание для новой группы системы Notes. Члены выбранной группы операционной системы Windows NT при этом станут членами новой группы системы Notes
Add members of this group to the existing Notes group (Добавление членов этой группы в существующую группу системы Notes)	Такой флажок появляется, если пользователь выбирает Use the existing Notes group (Использование существующей группы системы Notes) в диалоговом окне Existing Group имя_группы Migration Options (Параметры миграции существующей группы). Члены выбранной группы Windows NT в этом случае добавляются в существующую группу системы Notes

Таблица 6.2. Параметры миграции групп (окончание)

Параметр	Назначение
Add nested groups contained in this group and their members (Добавление вложенных групп, входящих в эту группу, и их членов) или Add people contained in nested groups as Notes users (Добавление членов вложенных групп в виде пользователей системы Notes)	Появляется одно из полей в зависимости от того, установлены ли вышеупомянутые флажки При установке данного флажка члены и группы операционной системы Windows NT, вложенные в выделенные группы, будут добавлены в группы системы Notes
Use above setting for all currently selected or nested groups, don't prompt again (Использование указанных параметров для всех текущих выбранных или вложенных групп без дополнительного запроса)	При установке этого флажка все остальные выделенные или вложенные группы получают те же самые параметры миграции, что и у выделенной группы

Таблица 6.3. Другие параметры миграции

Параметр	Назначение
Generate random passwords (Формирование случайных паролей)	Новым пользователям системы Notes, присутствующим в очереди регистрации, будут присвоены пароли, отвечающие заданному стандарту качества. Пароли запоминаются в базе данных (файл NTSynch45.nsf)
Add full name provided to the Notes person document (Добавление полного имени в персональный документ системы Notes)	Полное имя пользователя NT будет преобразовано в одно из вторичных имен в поле Full name (Полное имя) персонального документа пользователя
Allow addition of empty groups to Notes (Разрешение добавления пустых групп в систему Notes)	По умолчанию программный инструмент миграции не инициирует импорт группы, если в системе Notes эта группа окажется пустой (вследствие изначального отсутствия в ней членов еще в Windows NT или из-за того, что она содержит имена членов, не зарегистрированных в качестве пользователей Windows NT)

Переносимых пользователей, введенных в очередь регистрации, можно выделить в списке, чтобы изменить их параметры. Закончив подготовительные операции, воспользуйтесь кнопкой **Register** (Регистрация).

Синхронизация пользователей в системах Windows NT и Notes

Для пользователей системы Notes, которые имеют учетные записи в домене операционной системы Windows NT или являются опытными администраторами Windows NT, свободно владеющими ее программными средствами, инструмент Domino Directory NT Sync Services (Служба синхронизации системы Windows NT и каталога Domino Directory) может оказаться весьма полезным подспорьем. Эта служба помогает экономить время и сокращать

объем работы при установке новых пользователей или изменении параметров уже существующих. На практике данная служба позволяет выполнять следующие операции:

- О в диспетчере User Manager выбирать существующих пользователей и группы Windows NT и задавать их в качестве пользователей и групп системы Notes;
- О в диспетчере User Manager при добавлении новых пользователей или групп Windows NT одновременно указывать их в качестве пользователей или групп системы Notes;
- О в программе Domino Administrator при регистрации новых пользователей системы Notes добавлять их в качестве пользователей Windows NT;
- О в диспетчере User Manager при переименовании пользователя Windows NT вносить новое имя в персональный документ пользователя базы данных Domino Directory;
- О в диспетчере User Manager при удалении пользователя Windows NT исключать соответствующего пользователя системы Notes;
- О в диспетчере User Manager синхронизировать задание параметров конкретного пользователя операционной системы Windows NT с параметрами для соответствующего пользователя системы Notes.

Служба Domino Directory NT Sync Services устанавливается автоматически вместе с программой Domino Administrator на компьютере, использующем операционную систему Windows NT или 2000 (но не Windows 9x, с которыми эти службы работать не могут). Во время установки служба образует независимое меню (**Notes**) в диспетчере Windows NT User Manager (операционная система Windows NT Workstation) или в диспетчере Windows NT User Manager for Domains (операционная система Windows NT Server в домене Windows NT). Можно установить службу синхронизации на компьютере без инсталляции программы Domino Administrator, например в режиме пользовательской установки; при этом те службы, которые применять не планируется, следует сразу же отменить (то есть в рассматриваемой ситуации выбрать только службу Domino Directory NT Sync Services). Это позволит сформировать меню **Notes** в диспетчере User Manager данного компьютера.

При установке служб синхронизации может возникнуть несколько проблем. Во-первых, обеспечение доступа к учетным записям пользователей домена операционной системы Windows NT, а не локальным учетным записям системы Windows NT Workstation. Однако при установке программы Domino Administrator или службы Domino Directory NT Sync Services на компьютере с системой Windows NT Workstation меню **Notes** добавляется в диспетчер User Manager, а не в User Manager for Domains. Проблема решается путем проведения нескольких административных операций на компьютере с Windows NT Server. Однако, если данный компьютер действительно выполняет функции сетевого сервера, нецелесообразно применять его для синхронизации. В таком случае потребуется проделать следующее:

1. Установить службу Domino Directory NT Sync Services одновременно на основном контроллере домена Domino (Primary Domain Controller) и рабочей станции с Windows NT Workstation.
2. Установить клиентские средства сетевого администрирования Windows NT на этой рабочей станции.
3. Запустить клиентскую версию диспетчера User Manager for Domains на той же самой рабочей станции. Появится меню **Notes** и станут доступными соответствующие функции.

Чтобы установить на рабочей станции клиентские средства сетевого администрирования Windows NT, найдите дистрибутивные файлы программного сервера Windows NT Server, которые могут храниться на сетевом файловом сервере или на дистрибутивном компакт-диске Windows NT Server. Затем на рабочей станции запустите пакетный файл (файл setup.bat) из папки \client\srvttools\winnt компакт-диска. Начнется копирование нескольких файлов в системную папку Windows NT на рабочей станции, затем появится приглашение создать ярлыки для следующих программ: dhcpcadm.exe, poledit.exe, rasadmin.exe, plpmgr.exe, srvmgr.exe, usrmgr.exe и winsadm.exe. В данном случае нужен файл usrmgr.exe, что, однако, не уменьшает значимости и полезности других программ.

Вторая проблема со службой Domino Directory NT Sync Services возникает после установки операционной системы Windows NT: в сети создается главный домен и домен ресурсов (при стандартной установке одного домена - главного домена и домена ресурсов одновременно - учетные записи пользователей обычно располагаются в главном домене, а службы, например сервер Domino, попадают в домен ресурсов, причем ресурсные домены по умолчанию доверяют главному).

Таким образом, в ряде ситуаций не представляется возможным обеспечить доступ к учетным записям пользователей в главном домене, например при запуске диспетчера User Manager for Domains на компьютере из ресурсного домена, поскольку главный домен не доверяет домену ресурсов (не формирует с ним доверительных отношений). Для преодоления проблемы требуется организация двустороннего отношения доверия между главным и ресурсным доменами. Эту задачу можно считать частично решенной, поскольку ресурсный домен уже имеет доверительное отношение к главному. Остается провести настройку главного домена таким образом, чтобы появилось отношение доверия к ресурсному домену. Для получения более подробной информации следует обратиться к пособию компании Lotus «Регистрация пользователей системы Notes в сети Windows NT с главным доменом или несколькими главными доменами», документ #150871 в библиотеке Базы знаний компании Lotus (Lotus Notes Knowledgebase, www.lotus.com/support).

И наконец, для применения службы Domino Directory NT Sync Services необходимо располагать правами доступа на уровне администратора или оператора учета в тех доменах Windows NT, где находятся соответствующие учетные записи пользователей. Нужно также обладать правами доступа к базам данных Domain Directory (Каталог домена), Administration Requests (Административные запросы) и Certification Log (Журнал сертификации) сервера Domino, где проводится изменение статуса пользователей, а также правами доступа к идентификационным данным сертификатора в системе Notes на случай создания новых пользователей.

После правильной установки службы Domino Directory NT Sync Services в диспетчере User Manager появится меню **Notes**. Следующая задача связана с конфигурированием службы, причем при первом обращении в меню **Notes** будет присутствовать только один пункт - **Notes Synchronization Options** (Параметры синхронизации системы Notes). Выбор этого пункта приведет к выводу на экран диалогового окна **Enable Notes Synchronization Options** (Параметры разрешения синхронизации системы Notes). Задаваемые здесь значения позволяют активизировать другие пункты меню. В табл. 6.4 приведены варианты, которые могут быть указаны в данном диалоговом окне.

Пользователь, который не хочет возвращаться к этому окну при каждом запуске диспетчера User Manager, должен убедиться, что установлен флажок **Save Settings on Exit** (Сохранение параметров при выходе) в меню **Options** (Параметры) диспетчера User Manager.

Таблица 6.4. Параметры синхронизации систем Lotus Notes и Windows NT

Параметр	Назначение
Enable all synchronization operations (Разрешение всех операций синхронизации) или Select synchronization operations to enable (Выбор разрешенных операций синхронизации)	Используйте первый вариант для разрешения применения всех операций синхронизации Применяйте второй вариант для индивидуального разрешения трех операций синхронизации (станут доступными три флажка, назначение которых описано ниже)
User/Group registration (Регистрация пользователя/группы)	Разрешает работу диспетчера User Manager для регистрации существующих пользователей или групп NT в качестве пользователей или групп системы Notes, причем новые пользователи Notes и Windows NT могут создаваться как в User Manager, так и в системе Notes
User/Group deletion (Удаление пользователя/группы)	Разрешает удаление пользователей в диспетчере User Manager при одновременном удалении из системы Notes
User synching (Синхронное задание данных для пользователя)	Разрешает выполнение следующих действий: 1) при переименовании пользователя Windows NT в диспетчере User Manager автоматически изменяется содержимое поля Network account name (Имя сетевой учетной записи) персонального документа пользователя в системе Notes 2) при изменении полного имени пользователя Windows NT в диспетчере User Manager автоматически добавляется новое полное имя в поле User name (Имя пользователя) персонального документа пользователя в системе Notes
Set common password on user synching (Синхронное задание одинаковых паролей для пользователя)	Если выбран режим User synching (Синхронное изменение данных пользователя), можно синхронизировать пароль сети Internet пользователя системы Notes и его пароль в операционной системе Windows NT
Prompt to confirm/cancel synchronization operations (Запрос на подтверждение/отмену операций синхронизации)	Можно выбрать режим с постоянным выводом запросов, отменить такие запросы или выводить их только при удалении пользователя/группы
Name format for full name parsing (Выбор формата имени для полного синтаксического анализа)	Можно выбрать наиболее подходящий формат для представления имени на основе стандартного метода форматирования полных имен пользователей Windows NT в диспетчере User Manager

После разрешения синхронной регистрации пользователей/групп служба синхронизации обеспечит выполнение следующих операций:

- О создание учетной записи пользователя Windows NT (и добавление этой учетной записи в одну из групп) для каждого нового пользователя системы Notes, регистрируемого в программе Domino Administrator;
- О формирование учетной записи пользователя или группы системы Notes для каждого нового пользователя или группы Windows NT, регистрируемых в диспетчере User Manager;

- О выбор существующих учетных записей пользователей или групп Windows NT и создание соответствующих пользователей и групп системы Notes.

Если установлен режим синхронного удаления пользователей и групп, служба синхронизации исключит сопоставленных пользователя или группу системы Notes одновременно с удалением пользователя или группы операционной системы Windows NT в диспетчере User Manager.

При активизации функции синхронизации для пользователя служба синхронизации модифицирует заданные поля персонального документа пользователя (системы Notes) после изменения имени или полного имени пользователя Windows NT.

Создание нового пользователя NT в программе Domino Administrator

Для формирования новой учетной записи пользователя операционной системы Windows NT в программе Domino Administrator достаточно установить флажок **Add this person to Windows NT** (Добавление данного сотрудника в Windows NT) перед добавлением новых пользователей в очередь регистрации программы Domino Administrator. В результате в поле имени пользователя Windows NT по умолчанию будет занесено сокращенное имя пользователя системы Notes, которое может быть изменено в дальнейшем. Разрешается указать одну из групп Windows NT в поле **Add person to Windows NT group** (Добавление сотрудника в группу Windows NT); при этом новый пользователь будет добавлен к указанной группе.

Создание нового пользователя системы Notes в диспетчере Windows NT User Manager

Чтобы создать нового пользователя системы Notes в диспетчере User Manager операционной системы Windows NT, надо предварительно задать параметры по умолчанию в двух диалоговых окнах, которые вызываются из меню **Notes**. Команда **Registration Setup** (Установка регистрации) выводит на экран диалоговое окно **Notes Registration Setup** (Установка регистрации системы Notes). Диалоговое окно **Notes Mail/ID Registration Options** (Параметры регистрации почтовых сообщений/идентификационных данных системы Notes) открывается при указании в меню пункта **Mail/ID Registration Options** (Параметры регистрации почтовых сообщений/идентификационных данных).

Эти окна предназначены для задания различных параметров, которые во многом напоминают записи в полях диалогового окна **Register User** (Регистрация пользователя) программы Domino Administrator. Именно по причине большого сходства здесь фни подробно не описываются, за исключением нескольких полей диалогового окна **Notes Registration Setup** (Установка регистрации системы Notes):

- О **Internet registration only (no Notes ID or mail created)** (Регистрация только для сети Internet, без создания файла почтовых сообщений или идентификационных данных системы Notes). Если требуется сформировать персональные документы для новых пользователей, рекомендуется выбрать именно это поле. В таком случае новый пользователь сможет в режиме аутентификации по имени и паролю получить доступ к серверам Domino непосредственно из Web-браузеров, клиентов LDAP или новых клиентских программ, но в то же время не будет иметь доступа к базе данных почтовой службы системы Notes, а также возможности пользоваться клиентами системы Notes для доступа к большей части серверов Domino;

- О **Use common password** (Использование общего пароля). Установите этот флажок при задании общего пароля в операционной системе Windows NT и для идентификационных данных системы Notes, а возможно - и для доступа из системы Notes в сеть Internet. Если пользователь Windows NT уже существует, его пароль заменится общим паролем. Этот случай представляет особый интерес при установке функций однократного входа в систему Notes на компьютерах с Windows NT Workstation (но не ОС Windows 9x). При таких условиях вход в систему Windows NT фактически предполагает вход в систему Notes, а пользователю не приходится повторно вводить пароль при запуске клиента Notes на компьютере (см. главу 10).

После определения параметров для режимов по умолчанию появляется возможность создания в одном процессе новых пользователей или групп системы Notes и операционной системы Windows NT с привлечением уже существующих пользователей или групп. При создании нового пользователя или группы Windows NT и выборе команды **Add** (Добавление) автоматически откроется диалоговое окно, предлагающее ознакомиться с информацией системы Notes относительно нового пользователя или группы. Если новый пользователь или группа системы Notes формируются по уже существующим пользователям или группам Windows NT, следует сначала выбрать их в диспетчере User Manager, а затем выполнить команду **Add Selected NT Users/Groups to Notes** (Добавление выбранных пользователей/групп NT в систему Notes) в меню **Notes**.

При добавлении новых пользователей системы Notes (любым способом) появится диалоговое окно **Enter Notes User Information** (Ввод данных для пользователей системы Notes). В нем можно уточнить, изменить или ввести имя и пароль пользователя для системы Notes. При щелчке по кнопке ОК диспетчер User Manager подтвердит возможность обращения к серверам Domino, перечисленным в диалоговых окнах **Registration Setup** (Установка регистрации) и **Mail/ID Registration Options** (Параметры регистрации почтовых сообщений/идентификационных данных). Если подобный доступ обеспечить не удается, будет выведено сообщение об ошибке, а сам процесс прервется. При успешном подключении к нужному серверу Domino диспетчер User Manager развернет диалоговое окно с подтверждением. В этом окне для завершения процесса создания пользователя системы Notes выбирается пункт **Begin Registration** (Начать регистрацию).

Когда добавляется новая группа системы Notes (любым способом), открывается диалоговое окно **Group Registration Options** (Параметры регистрации групп системы Notes), в котором можно подтвердить или изменить имя и тип группы (многоцелевая, только для почтовых целей и т.д.), а также ввести описание, поменять состав группы и принять решение относительно регистрации ее членов в качестве пользователей системы Notes. Затем следует щелкнуть по кнопке ОК, после чего диспетчер User Manager немедленно создаст в системе Notes группу с указанными параметрами.

При регистрации членов группы в качестве пользователей системы Notes на экран вызывается ряд дополнительных диалоговых окон. Сначала система спросит, необходима ли подобная регистрация, на что надо ответить положительно. Затем последует вопрос об имени и пароле для каждого пользователя, и на экран будет выведено несколько диалоговых окон **Enter Notes User Information** (Ввод информации пользователя системы Notes). Если же ранее будет выбран вариант **Register users at once without additional prompts** (Регистрация пользователей без дополнительных запросов), то диспетчер User Manager проведет анализ соответствующего полного имени, чтобы сформировать имя пользователя системы Notes, а затем сгенерирует случайный пароль для идентификационных данных

пользователя в системе Notes. При этом диспетчер User Manager подтвердит право доступа к тем серверам Domino, которые указаны в диалоговых окнах **Registration Setup** и **Mail/ID Registration Options**, либо выведет на экран сообщение об ошибке и прервет процесс регистрации. Если же для программы обеспечивается доступ к требуемым серверам Domino, она отобразит на экране диалоговое окно с подтверждением числа регистрируемых пользователей системы Notes. Щелкните по **Begin Registration** для завершения процедуры.

Иногда при выполнении процедуры регистрации пользователей появляются диалоговые окна с сообщениями о возникновении тех или иных проблем (например, о наличии других пользователей или почтовых файлов с идентичными именами). В этом случае необходимо сразу принять решение о порядке устранения подобных сложностей. По завершении регистрации раскроется диалоговое окно, которое проинформирует о количестве успешных регистраций и сообщит число имевших место ошибок.

Другими словами, процесс создания новых пользователей и групп в диспетчере User Manager оказывается практически аналогичным процессу, реализованному в самой системе Notes: требуется указывать те же самые данные, отвечать на те же самые вопросы и анализировать те же самые сообщения об ошибках. Основным отличием от регистрации в программе Domino Administrator является применение диспетчера User Manager. В остальном разница весьма незначительна и связана с наличием нескольких специальных диалоговых окон. Еще одно отличие состоит в том, что в диспетчере User Manager можно вводить новых пользователей в несколько групп NT, но только в одну группу системы Notes, в то время как в программе Domino Administrator новых пользователей допускается вносить в несколько групп системы Notes, но только в одну группу NT.

Рассмотренная функция администрирования системы Notes была заложена уже в версиях 4.x. Появление версии R6 с поддержкой операционной системы Windows 2000 позволяет достичь большего уровня интеграции между системами Notes и Windows, поскольку рассмотренные нами средства одновременной регистрации пользователей и групп теперь добавляются в диспетчер Active Directory Manager (Диспетчер каталога Active Directory) Windows 2000, что обеспечивает регистрацию в пределах всего каталога Active Directory.

Обновление других почтовых программ и служб поддержки календаря

При модификации пользователей в процессе их переноса в систему Notes из других систем почтовой службы иногда удается отыскать на дистрибутивном диске CD-ROM программный инструмент, позволяющий осуществлять миграцию пользователей из старых программ почтовой службы в очередь регистрации системы Notes. Наряду с программным инструментом Windows NT to Notes migration, описанным выше, на компакт-диске системы Lotus Notes R5 могут присутствовать и другие инструменты, осуществляющие миграцию данных из следующих почтовых программ и служб каталога:

- О почтовая служба Lotus cc:Mail;
- О почтовая служба Microsoft Mail;
- О программный сервер Microsoft Exchange;
- О программа Novell Groupwise версии 4.x;
- О программа Novell Groupwise версии 5.x;
- О сервер Netscape Microsoft Server;
- О каталоги LDAP (с помощью файла LDIF).

В системе Domino/Notes R6 служба Domino Upgrade Services (Службы обновления Domino) поддерживает несколько иной состав инструментов миграции почтовых служб и служб каталогов:

- О файлы LDIF (формат обмена данными Data Interchange Format для каталогов LDAP);
- О совместимые с LDAP внешние каталоги;
- О Lotus cc:Mail и Organizer 2.x for cc:Mail;
- О Microsoft Exchange;
- О Microsoft Mail;
- О Microsoft Windows NT Server;
- О Microsoft Active Directory.

Все названные программные инструменты могут использоваться точно так же, как и инструмент миграции для Windows NT, описанный в предшествующих разделах. Доступ к этим программам обеспечивается командой **Migrate people** (Миграция сотрудников) в диалоговом окне **Register Person** (Регистрация сотрудника). Следует указать вариант, связанный с выбором определенного внешнего каталога, затем задать имена пользователей и групп во внешнем каталоге, установить доступные параметры миграции, например выбрать **Generate random passwords** (Генерация случайных паролей), и щелкнуть по кнопке **Migrate** (Миграция). Программный инструмент миграции создаст эквивалентных пользователей в очереди регистрации системы Notes. При регистрации новых пользователей в режиме **Convert mail** (Преобразование почтовых сообщений) содержимое соответствующих почтовых ящиков (исходных почтовых систем) также будет передано в новые базы данных почтовой службы системы Notes. Следует отметить, однако, что подобные данные не всегда передаются в требуемой форме. Так, при переносе пользователей почтовой службы cc:Mail содержимое ее баз данных Organizer (Организатор) может быть перенесено практически целиком. Но когда переносятся данные пользователей из каталогов LDAP (с помощью файла LDIF), бывает трудно преобразовать файлы почтовых сообщений, поскольку протокол LDAP не относится к числу стандартных протоколов почтовой службы.

Описанные выше программные инструменты миграции обеспечивают перенос общедоступных, хранящихся централизованным образом данных из унаследованных систем в систему Notes. Но старые системы, как правило, предполагают локальное хранение части информации пользователей. Сами программные инструменты миграции не имеют доступа к этим данным, а переносимые пользователи таким правом обладают. Поэтому система Notes предусматривает применение второго набора программных инструментов миграции, предназначенных собственно для переносимых пользователей и позволяющих им передавать свои данные из более старых систем в новые базы данных системы Notes.

Компания Lotus предлагает Мастеров обновления для следующих трех систем почтовой связи: cc:Mail, Microsoft Mail и Microsoft Exchange/Outlook. После переноса и регистрации новых пользователей имеется возможность направить каждому из них сообщение электронной почты со специальной ссылкой. Если пользователь щелкнет по этой ссылке, будет запущен Мастер обновления. Пользователю останется только ответить на вопросы Мастера, чтобы выполнить миграцию в систему Notes своих данных, в том числе частных адресов, списков почтовой службы и почтовых архивов.

Для отправки сообщения электронной почты с вложенным Мастером обновления выберите **Send Upgrade Notifications** (Отправка уведомлений об обновлении) на виде **Server/Mail Users** (Пользователи сервера/почтовой службы) базы данных Domino Directory. В программе Domino Administrator укажите сервер и перейдите на вкладку **People & Groups**. На панели **Tasks** (Задачи) раскройте значок каталога Domino Directory (при необходимости),

щелкните правой кнопкой по имени каталога, а затем выполните **Open Directory** (Открытие каталога). Дальнейшие операции для версий R5 и R6 различаются. В версии R5 в открытом каталоге следует щелкнуть по значку **Server** (Сервер) на панели **Navigator** (Навигатор) и выбрать вариант **Mail Users** (Пользователи почтовой службы), после чего выполнить команду **Send Upgrade Notifications** (Отправка уведомлений об изменении) в меню **Actions** (Операции) или на панели **Action** (Операция). Для версии R6 в меню **Lotus Notes** нужно выполнить команду **File => Database => Access Control** (Файл => База данных => Управление доступом), затем на панели **Basics** (Основные параметры) диалогового окна **Access Control List** (Список управления доступом) указать необходимый файл идентификационных данных администратора (Administrator ID) и выбрать в поле **Roles** (Роли) значение **UserModifier** (Модификатор пользователей) или **NetModifier** (Модификатор сети). Щелкните по ОК, перейдите на вкладку **Messaging** (Сообщения), затем на вкладку **Mail** (Почта) и щелкните по **Mail Users** (Пользователи почтовой службы). В меню **Action** (Операция) выберите команду **Send Upgrade Notifications** (Отправка уведомлений об изменении).

В окне **Upgrade Message** (Обновление сообщения) версии R5 или окне **Mail Conversion Options** (Параметры преобразования почты) введите имена пользователей, которым предназначено сообщение, а затем воспользуйтесь вариантом **Send out cc:Mail/MS Mail/MS Exchange convert local information notices** (Пересылка в системы почтовых служб cc:Mail/MS Mail/MS Exchange уведомления о преобразовании локальных данных), назначьте системе почтовой службы для каждого пользователя и внесите другие необходимые данные. После щелчка по кнопке **Send** (Пересылка) пользователи получают сообщение, состоящее из содержимого поля **Additional Information** (Дополнительная информация) и кнопки **Convert Local Data to Notes** (Преобразование локальных данных в данные системы Notes). При нажатии этой кнопки будет запущен Мастер Lotus Notes Upgrade Services Wizard. В процессе его работы пользователь должен принять несколько простых решений, а затем щелкнуть по кнопке **Finish** (Готово) и тем самым передать свои локальные данные из прежней программы в систему Notes.

Для пользователей других почтовых систем и программ поддержки календаря, перечисленных в табл. 6.5, система Notes R5 предлагает ряд баз данных, создаваемых на виде **Binary Tree** (Двоичное дерево) и позволяющих переносить частные почтовые сообщения и данные календаря в систему Notes. Базы данных и программы почтовой службы/поддержки календаря, допускающие миграцию данных, представлены в табл. 6.5.

Таблица 6.5. Базы данных и миграция данных

Имя базы данных	Миграция данных из
C&S 1.0 for Notes 5.0	Lotus Organizer 1.1 Lotus Organizer 97 Microsoft Schedule+ 1.0 Microsoft Schedule+ 7.0
Groupwise 5 > Notes 1.3	OpenText On Time
MoiPortforGW4v1.06	Groupwise 5.x
Netscape > Notes 1.12 (окончательный вариант)	Groupwise 4.1
Eudora > Notes v1.52	Netscape Messenger из состава Netscape Navigator 3.x и 4.x или Netscape Communicator 4.x Qualcomm Eudora

Каждая из этих баз данных содержит полный набор инструкций по ее применению. В основном они сводятся к тому, что допускается два способа передачи данных. Первый предусматривает задание администратором параметров на форме **Settings** (Параметры) и отправку сообщений электронной почты переносимым пользователям. В сообщении пользователю рекомендуется щелкнуть по одной или нескольким кнопкам, находящимся в информационной части (теле) сообщения. Кнопки служат для активизации агентов, которые выполняют основную работу по миграции данных пользователя из прежней системы в систему Notes. Во втором случае пользователь открывает саму базу данных, вводит соответствующие параметры и запускает упомянутых агентов. Таким способом устраняются ненужные промежуточные операции и отпадает надобность в направлении сообщений электронной почты.

В версии R6 допускается селективная миграция отдельных архивов из унаследованных систем в архивные базы данных Notes. По умолчанию Мастер обновления переносит все архивы в один файл почтовой базы данных Notes даже при миграции из нескольких унаследованных систем. Такая база данных создается в подпапке mail папки данных системы Notes (если иное не указано в файле notes.ini). Во время создания архивной базы данных пользователю придется ввести свой пароль в системе Notes. Имена файлов архивных баз данных формируются автоматически: к первым шести символам имени мигрируемого пользователя добавляется префикс A_. Например, для пользователя Rob Kirkland будет сформирована архивная база данных с именем A_KIRKLA.NSF.

Автоматизация процедуры установки клиента Notes

Следующим вопросом, связанным с проведением установки пользователей, является вопрос автоматизации процедуры установки клиентов Notes на рабочих станциях пользователей. Существует два способа автоматизировать эту процедуру. Во-первых, можно проводить так называемую установку по умолчанию, в которой предусматривается создание файла ответных сообщений, содержащего ответы на некоторые или все вопросы, задаваемые Мастером InstallShield. Подобным образом удастся управлять процессом установки, что во многом облегчает задачу как для пользователей, так и для самого администратора.

Во-вторых, можно подготовить процесс установки для копирования дополнительных или заменяемых файлов: например, добавить собственные приложения в список устанавливаемых файлов или заменить стандартные шаблоны на индивидуально сформированные, учитывающие ряд специальных требований.

Однако прежде чем начать действовать одним из этих способов, следует твердо усвоить, что начиная с версии 5.0.1 ни один из них не рекомендуется для применения. Так, способ установки по умолчанию не является функционально гибким, а его применение сопряжено с появлением целого ряда проблем. Копирование дополнительных файлов, как отмечено в документации Lotus, может вообще не сработать. Поэтому нельзя исключать самого худшего поворота событий.

Автоматизация процедуры установки клиентов

На практике не существует простого способа автоматизации процедуры установки клиентов системы Notes, особенно в тех случаях, когда требуется установка большого числа приложений. В этой связи можно упомянуть хотя бы программу Actioneer for Lotus Notes, которая оказывается весьма эффективной надстройкой для системы Notes. Некоторые специалисты

считают, что привнесение этой функции стало чуть ли не единственным поводом для замены версий 4.x на версию 5.0. К счастью, в версии R6 устранены все недочеты, связанные с установкой по умолчанию, а также введены файлы трансформации, позволяющие настроить установку клиентов на рабочих станциях. Кроме того, появились средства Upgrade-by-mail (Обновление по почте) и Lotus Notes Smart Upgrade (Интеллектуальное обновление Lotus Notes), позволяющие подготовить на файловом сервере все необходимые для установки файлы (включая дополнительные приложения), а затем уведомить пользователя об их существовании. Пользователям остается щелкнуть пару раз мышью, чтобы обновить свои клиентские системы до версии R6. Заметим, что средство Lotus Notes Smart Upgrade дает возможность указать временной период, в течение которого пользователь обязан обновить свое клиентское программное обеспечение - если он этого не сделает, доступ к системе Notes/Domino будет заблокирован.

Для полной автоматизации процедуры установки системы Notes или Actioneer нет необходимости выполнять какие-либо сложные операции. Достаточно сформировать файл ответных сообщений, который будет направлять ответы на запросы программы InstallShield в те моменты, когда потребуются принимать ответственные решения. После этого файл ответных сообщений может быть перенесен в то место, где планируется провести автоматическую установку.

Однако для одновременной установки системы Notes и программы Actioneer одной управляющей командой, создания пакетного файла явно недостаточно. В таком случае приходится формировать собственный сценарий установки, который, будучи относительно несложным, требует заметного отвлечения времени и средств. Во-первых, нужно запастись дорогостоящей программой InstallShield Pro (или более дешевой InstallShield Express, хотя она вряд ли позволит в полном объеме подготовить режим установки с файлом ответов в условиях, когда необходимо установить несколько различных приложений). Во-вторых, понадобится еще некоторое время для изучения нюансов этой программы и тренировки, чтобы подготовить сценарий на используемом языке программирования.

Создание файла ответных сообщений

Вопросы, связанные с подготовкой сценария InstallShield, выходят далеко за рамки настоящего обсуждения. Поэтому в данном случае вполне можно ограничиться описанием создания и применения файла ответных сообщений. Наиболее простой путь формирования такого файла предусматривает его непосредственную запись:

1. Запустите программу установки setup (допускается употреблять иное имя, если это отмечено в Мастере InstallShield) в режиме записи. Управляющая команда должна иметь вид Setup -г.
2. Проведите полную установку представляющей интерес программы. Ответные сообщения для всех возможных параметров будут сохранены в файле setup.iss, который располагается в системном каталоге. Расширение .iss в данном случае означает InstallShield Silent (режим по умолчанию Мастера InstallShield).

Затем скопируйте файл ответных сообщений (setup.iss) в тот каталог, где хранятся файлы установки (он, как правило, располагается на файловом сервере), переименовав, если требуется, файл ответных сообщений.

Использование файла ответных сообщений во время установки

Для выполнения процедуры установки с помощью файла ответных сообщений (в режиме по умолчанию) рекомендуется воспользоваться одной из следующих управляющих команд:

```
setup-s
```

или

```
setupup -s -flsetup.iss
```

или

```
setup -s -flsetup/iss
```

В первом примере файл setup.exe будет искать сценарий setup.iss в собственной папке. Во втором и третьем случаях указывается имя файла iss. Если этого файла нет в папке программы setup.exe, необходимо указать полный путь к файлу ответов.

Обратите внимание, что во втором и третьем случаях соответственно предусмотрено и не предусмотрено применение пробела между аргументами -fl и setup.iss. Введение пробела в данном случае необязательно. Об этом следует помнить, поскольку в представленных ниже примерах пробел между -f2 и setup.log запрещен. В тех случаях, когда требования относительно пробела отсутствуют, предпочтительнее его вносить: читать командную строку проще, когда она соответствует привычным синтаксическим правилам.

Если планируется запустить программу установки не из папки файлов setup.exe и setup.iss, а из иной, потребуется ввести управляющую команду с указанием полного пути к файлу setup.exe (и, возможно, к файлу setup.iss). В противном случае команда не сможет обнаружить эти файлы. Так, например, если файлы установки расположены по адресу

```
p:\clients\w32intel\
```

где p: соответствует отображенному сетевому диску, управляющая команда (вводится в командной строке или в пакетном файле) должна выглядеть так:

```
p:\clients\w32intel\setup.exe -s -fIn:\clients\w32intel\setup.iss
```

В то же время надо, чтобы управляющая команда для ярлыка имела следующий вид:

```
n:\clients\w32intel\setup.exe - -flsetup.iss
```

если только файл setup.iss не расположен в той же папке, что и файл setup.exe (в этом случае придется указывать полный путь к файлу setup.iss).

Использование Setup.log

При исполнении Мастера InstallShield с файлом ответов формируется файл журнала (регистрации) с именем setup.log. Если в процессе установки возникает ошибка, этот процесс может быть остановлен до его полного завершения. Причины появления ошибки могут быть проанализированы по журналу установки. На практике допускается задавать местоположение и имя файла setup.log путем добавления аргументов в управляющую команду:

```
-f2<имя_файла_журнала>
```

Так, например, Masterpy InstallShield можно предписать занесение регистрационных записей журнала установки в папку пользователя системы Notes:

```
p:\clients\w32intel\setup.exe -s -fIn:\clients\w32intel\setup.iss -
f2c:\lotus\notes\setup.log
```

Журнал регистрации, сформированный Мастером InstallShield, будет включать в себя переменную ResultCode, которая обычно равна некоторому числу. Числа, генерируемые для режима по умолчанию, приведены в табл. 6.6, причем это далеко не все возможные числа, а только те, которые соответствуют данному режиму.

Таблица 6.6. Коды результатов работы Мастера InstallShield

Код	Комментарии
0	Успешное завершение
	Имеет место ошибка общего типа
	Требуемые данные не найдены в файле setup.iss
-4	Недостаточный объем памяти
-5	Файл не существует
-8	Некорректно задан путь к файлу setup.iss
-11	Ошибка неизвестного типа
-51	Невозможно создать заданную папку
-52	Невозможен доступ к заданному файлу или заданной папке

Создание ярлыков для запуска установки в режиме по умолчанию

Для запуска установки с файлом ответов, но без употребления длинных управляющих команд (подобных приведенным выше) можно создать ярлык (с управляющей командой), а затем обращаться в файл setup.exe с его помощью. Для этого необходимо выполнить следующие действия:

1. В Проводнике Windows щелкните правой кнопкой по файлу setup.exe и выберите **Create Shortcut** (Создать ярлык) - в соответствующей папке появится ярлык **Shortcut to Setup.exe** (Ярлык для setup.exe).
2. Щелкните правой кнопкой по ярлыку **Shortcut to Setup.exe** и выполните **Properties** (Свойства). На экране откроется диалоговое окно **Shortcut to Setup.exe Properties** (Свойства ярлыка setup.exe), в поле **Target** (Объект) которого будет отображена определенная запись (обычно здесь указывается управляющая команда, предназначенная для запуска файла setup.exe).
3. Переместите текстовый курсор вправо от управляющей команды в поле **Target** и внесите дополнение к управляющей команде

```
-s -f l<имя_файла> -E2<путь>
```

где <имя_файла> определяет файл с расширением .iss, а <путь> задает имя и местоположение файла регистрации. На практике, естественно, нет необходимости в угловых скобках, но все пробелы, в том числе и перед аргументом -s, обязательны. Вводить команду следует весьма аккуратно, поскольку любая ошибка может повлечь за

собой серьезные проблемы. С учетом вышесказанного результирующая управляющая команда должна выглядеть так:

```
h:\clients\w32intel\setup.ex -s -f1setup.iss-f2c:\lotus\notes\setup.log
```

4. Щелкните по кнопке ОК.
5. Рассмотрите возможность переименования файла ярлыков, чтобы в дальнейшем его назначение было совершенно очевидным. Например, можно выбрать название типа «Дважды щелкните по этому ярлыку для установки стандартного клиента системы Lotus Notes» (Double-click here to install Lotus Notes for standard users).

Заключительные замечания

Для автоматизации установки, скажем, Notes и Actioneer, можно подготовить файлы ответных сообщений для обеих программ, после чего создать для каждой из них файл ярлыков и занести его в соответствующую папку, доступную для потенциальных пользователей. Затем следует направить сообщение электронной почты пользователям с просьбой открыть папку ярлыков и задействовать сначала ярлык для системы Notes, а затем ярлык для Actioneer. Если у пользователя возникнут проблемы и он обратится за помощью, то, скорее всего, его проблемы удастся решить с помощью файла регистрации (журнала установки).

В данном случае одна из проблем при установке клиента Notes может быть связана с самим характером установки по умолчанию, поскольку Мастер InstallShield не выводит никакой информации ни о ее выполнении, ни о завершении. Единственным индикатором является постоянное мерцание светодиодов дискового накопителя, а свидетельством окончания процедуры установки становится факт завершения исполнения определенного сценария Мастером InstallShield и переход в программу регистрации продукта компании Lotus. В данном случае на успешное завершение установки клиента Notes указывает только появляющийся в конце процедуры экран, предлагающий перейти к регистрации установленной клиентской программы.

В дальнейшем возможна еще одна проблема. Так, если нет необходимости регистрировать для всех пользователей копии клиентов Notes в системе Lotus и разрешать им заносить в базы данных большой объем почтовых сообщений либо возникают трудности в процессе регистрации, можно переименовать подпрограмму регистрации, что не позволит программе InstallShield напрямую ею воспользоваться. Эта подпрограмма обычно хранится в файле LotusProductRegistration.exe. Конечно, в случае ее переименования пользователи так никогда и не узнают о факте завершения исполнения Мастера InstallShield и о результатах установки клиента Notes. Поэтому им не будет точно известно, когда начинать установку программы Actioneer. Для преодоления указанного неудобства рекомендуется создать программу, информирующую о завершении процедуры установки клиента системы Notes, назвать ее файл LotusProductRegistration.exe и заменить старый файл новым. Эту процедуру пользователям придется опробовать самостоятельно, поскольку никаких конкретных советов по ней дать невозможно.

В заключение отметим, что на практике отсутствует простой и четкий способ полностью автоматизировать установку клиентов системы Notes, по крайней мере без создания собственного сценария InstallShield. По этому вопросу написано множество книг и пособий, дополнительную информацию можно получить по адресу www.installshield.com, а при необходимости более подробно ознакомиться с порядком подготовки файла ответных сообщений или режимом по умолчанию для Мастера InstallShield - обратиться по адресу

www.installshield.com, где следует отыскать документ ID Q101901 «Подготовка к установке с файлом ответов» (How to: Creating a Silent Installation). По адресу www.notes.net представлены рекомендации для версий 5 и 6 (следует провести поиск по ключевому слову «InstallShield»). Большая часть новых средств версии R6, связанных с процессом установки, относится к процедурам обновления старых версий клиентов Notes или сторонних программ до версии Notes 6. Для развертывания в сети вновь устанавливаемых клиентских программ Notes 6 вполне подходят стандартные средства операционной системы Windows 2000, позволяющие «вытолкнуть» на рабочие станции любые программные продукты. Разумеется, без участия владельца рабочей станции (по крайней мере, без его подтверждения) эта процедура невозможна.

Добавление баз данных в файлы установки

При установке клиентов Notes допустимо настроить то, что будет копироваться на компьютеры пользователей. Например, в ряде случаев требуется установить локальные файлы сторонних приложений, которые развертываются в сети вместе с программным обеспечением системы Notes.

В этом случае, естественно, разрешается с помощью профиля или политики установки скопировать специфические базы данных в папку данных пользователей во время задания конфигурации для конкретных рабочих станций. Однако на практике нужно копировать и другие файлы (отличные от баз данных). Кроме того, при определенных обстоятельствах удобнее копировать файлы в процессе установки программного обеспечения, а не реплицировать их с сервера при проведении установки пользователей. Например, подобная ситуация может возникнуть для пользователя, связанного с сервером Domino только с помощью модема. В этом случае удастся скопировать файлы (достаточно быстро) с дистрибутивного диска CD-ROM в процессе установки клиента либо, затратив больше времени, – при репликации во время ввода учетной записи пользователя (выбор лучше сделать в пользу первого варианта).

К сожалению, описанный в документации компании Lotus способ пользовательской установки не срабатывает, поскольку он связан с созданием перечня дополнительных файлов, сохранением этого перечня в файле `copyfile.txt` в папке, содержащей файлы установки, и переносом указанных в перечне файлов в ту же самую папку.

Проблема в данном случае состоит в том, что в документации компании Lotus не полностью описан синтаксис перечня, заносимого в файл `copyfile.txt`, причем никому из участников форума [notes.net](http://www.notes.net) так и не удалось выявить этот таинственный синтаксис. Специалисты компании Lotus и разработчики программы InstallShield также ничего не могут пояснить. Возможно, что данное средство просто удалено в версиях 5.0 и выше, хотя его Описание сохранилось в справке Administration Help (Административная справка).

Тем не менее это совсем не означает, что нельзя настроить Master InstallShield. Так, версия InstallShield Professional 5.0 содержит утилиту `iscab.exe`, которая позволяет модифицировать содержимое файлов InstallShield Cabinet (сжатые файлы, хранящие файлы установки). Не исключено, что с помощью данной утилиты могут быть добавлены дополнительные файлы в файлы CAB, предоставляемые компанией Lotus на дистрибутивном компакт-диске системы Notes. Для получения более подробной информации обратитесь к пособию «Q103003 HOWTO; Создание индивидуального набора файлов с уплотненными данными» (Q103003 HOWTO; Creating a Custom Set of Compressed Files), опубликованному по адресу suDDort.installshield.com.

По слухам, можно также загрузить файл `iscab.exe` с сайта support.installshield.com, однако никому этот файл по данному адресу отыскать не удалось. Вероятно, следует загрузить ознакомительную версию программы InstallShield Professional 5.0, чтобы добраться до указанного файла. Если сделать это не удастся, придется купить лицензионный пакет InstallShield Professional 5.0. Конечно, при насущной потребности в подобной программе для более полной реализации всех возможностей программы установки компании Lotus имеет смысл создать собственный вариант программы установки системы Notes на основе InstallShield.

Не исключено, что к тому моменту, когда настоящая книга увидит свет, рассматриваемая проблема уже будет решена компанией Lotus. Чтобы ознакомиться с состоянием дел, стоит провести поиск по ключевому слову «InstallShield» на сайте notes.net, а также в Базе знаний системы Notes (Notes Knowledgebase) по адресу www.lotus.com/support.

Проведение установки пользователей со специальными требованиями

Далеко не все пользователи системы Notes применяют ее одинаково. Так, некоторые из них используют ее только в течение рабочего дня (в офисе) для доступа к локальной сети. Другие работают с системой в отеле, дома и в других местах. Кто-то обращается только к серверам Domino, а кто-то взаимодействует и с серверами сети Internet. И наконец, не все пользователи имеют личный компьютер и иногда вынуждены делить его с другими сотрудниками. Рассмотрим установку системы именно для таких пользователей, выдвигающих специальные требования к системе.

Установка мобильных пользователей

Мобильные пользователи системы Notes не всегда подключены к локальной сети компании. В ряде случаев им приходится соединяться со своими серверами Domino с помощью модема или локальной сети другой компании. В некоторые моменты времени они вообще не могут связаться со своими серверами. Поэтому для подобных пользователей следует задавать при установке несколько местоположений и создавать несколько документов местоположения (Location document), сформировав локальные реплики баз данных, которые могут потребоваться пользователям для доступа в тех случаях, когда отсутствует возможность связаться с серверами Domino обычным способом. Если на момент установки клиента системы Notes планируется обслуживание подобных пользователей, можно прибегнуть к услугам Мастера Lotus Notes Client Configuration Wizard, который сам выполнит необходимые действия, либо проделать эту работу самостоятельно на более позднем этапе. В справке версии R6 мобильные (mobile) пользователи названы перемещаемыми (roaming), что отражает современные тенденции, но не меняет сути дела. В последнее время мобильными считают пользователей беспроводных систем сотовой связи, но в версии R5 этот термин применялся с другими целями, поэтому в справке версии R6 такие пользователи названы «перемещаемыми». Ниже мы будем употреблять старый термин, не забывая о том, что речь идет о перемещаемых пользователях (точнее, о перемещаемых учетных записях этих пользователей).

Проведение настройки для мобильных пользователей требует решения двух основных вопросов, которые не возникают в случае работы в офисе:

- О мобильные пользователи должны принять решение относительно формирования соединения с серверами Domino. Способ выполнения соединений определяется техническими возможностями в местах подключения и типами тех соединений, которые разрешается использовать серверам и компьютерам. Например, если требуется применение модема, то набираемый телефонный номер может различаться в зависимости от мест подключения мобильного пользователя;
- О мобильным пользователям часто приходится иметь дело с медленными модемными соединениями для связи со своими серверами Domino. Передача документа с сервера со скоростью работы модема может потребовать достаточно много времени, а сам документ появится на экране компьютера пользователя с большой задержкой. Не исключено, что после нескольких продолжительных ожиданий мобильный пользователь вообще откажется от услуг системы Notes. Кроме того, в целом ряде случаев мобильные пользователи просто не в состоянии связаться со своим сервером, хотя очень нуждаются в получении информации.

Следует отметить, однако, что система Notes позволяет провести необходимую адаптацию с тем, чтобы удовлетворить потребности мобильных пользователей. Система Notes располагает следующими возможностями:

- О документы местоположения и соединения. Система Notes обеспечивает соединение с сервером из любого места, поскольку хранит данные обо всех местоположениях в рамках единого документа местоположения (Location document), а данные относительно различных вариантов соединения - в соответствующих документах соединения (Connection document). Если документы местоположения и соединения пользователя были подготовлены правильно, все, что надлежит сделать пользователю для связи с сервером, - это просто выбрать соответствующий документ местоположения и начать формирование соединения;
- О репликация данных с сервера на рабочую станцию. Система Notes хранит локальные копии баз данных и реплицирует изменения в процессе выполнения фоновой серверной задачи. При этом мобильным пользователям не приходится долго ожидать появления документа на экране дисплея, поскольку они имеют возможность обратиться к *локальным копиям баз данных*. Пользователи не замечают длительных процедур загрузки/выгрузки данных (являющихся следствием медленных соединений), поскольку они выполняются в те моменты времени, когда пользователи заняты другими делами;
- О временное локальное хранение отправленных почтовых сообщений. Когда пользователь, удаленный на значительное расстояние от своего сервера, щелкает по кнопке **Send** (Пересылка), отправленное сообщение временно запоминается в базе данных Outgoing Mail (Исходящие почтовые сообщения) и хранится там, пока пользователь не сможет переслать его на сервер (эта пересылка выполняется в фоновом режиме).

Администратор системы должен четко представлять себе характер взаимодействия документов местоположения и документов соединения для успешного формирования соединений между мобильным пользователем и сервером. При ясном понимании ситуации необходимое соединение удастся установить достаточно быстро. Следует особо отметить, что за эти вопросы администратор системы несет прямую ответственность.

Рассмотрим пример с Джо Доаксом. Когда Джо работает в своем офисе и пользуется переносным компьютером, соединенным с локальной сетью офиса, соответствующий документ местоположения офиса (Office location document) информирует систему Notes о том, что порт локальной сети (TCP/IP) доступен и что почтовые сообщения Джо хранятся на домашнем сервере (сервер 1). Поэтому, когда Джо открывает свою базу данных почтовой службы, система Notes соединяет его с сервером 1 с помощью порта локальной сети и обеспечивает на сервере открытие соответствующей базы данных. Когда Джо открывает базу данных поддержки продаж, система Notes обеспечивает связь с сервером 2 с помощью локальной сети и загрузку нужной копии базы данных.

На следующий день Джо отправляется с визитом к клиенту в другой город. Перед отъездом он заносит реплику базы данных поддержки продаж на свой переносной компьютер и обновляет копию базы данных почтовой службы, уже реплицированную во время взаимодействия с серверами 1 и 2. Для этого ему следует перейти на страницу **Replication** (Репликация), щелкнув по ее вкладке на панели **Bookmarks** (Закладки) и выполнив команду **Start** (Запуск). Значки для его баз данных почтовой службы и поддержки продаж появятся на странице, причем будут отмечены символом «галочка» (поэтому система Notes подключится по сети к каждому серверу, чтобы провести репликацию необходимой информации).

Вечером, после возвращения домой из офиса, Джо включает портативный компьютер, подключает его к телефонной линии через модем, после чего запускает клиент Notes и переключается на один из своих домашних документов местоположения (Home location document). Выбирается документ щелчком по соответствующему значку в левом нижнем углу экрана или с помощью меню **File => Mobile** (Файл => Мобильный). Указанный таким образом документ местоположения сообщает системе о том, что: единственным доступным портом является порт COM1; используемая Джо почтовая служба заменена на локальную (Local) переносного компьютера; репликацию следует проводить каждый час, а сервер 3 является сквозным (по умолчанию). При этом система Notes сначала пытается выполнить репликацию с помощью серверов 1 и 2. В рассматриваемом случае отсутствуют документы соединения, информирующие систему Notes о вариантах связи с серверами для данного местоположения, однако существует документ, указывающий на возможность формирования соединения с сервером 3 путем набора телефонного номера 5556666 для модема, подключенного к порту COM1. Поэтому система Notes наберет указанный номер, свяжется с сервером 3 и запросит соединение с сервером 1. Если сервер 3 разрешит такое сквозное соединение, система Notes организует связь с сервером 1 и реплицирует необходимые Джо почтовые сообщения. Затем она запросит сервер 3 о связи с сервером 2, на котором планирует произвести репликацию базы данных поддержки продаж. По завершении этих операций система Notes прервет связь с сервером 3.

Когда Джо открывает свой почтовый ящик, система Notes вызывает локальную копию соответствующей базы данных. Джо читает новое почтовое сообщение и отвечает на него. Поскольку для почтовой службы Джо задан режим **Local** (Локальный), система Notes помещает ответное сообщение в базу данных Outgoing Mail (Исходящие почтовые сообщения). При этом система Notes набирает номер сервера 3 и с его помощью обеспечивает доступ к серверу 1 и передачу ответного сообщения серверу 1, после чего завершает телефонное соединение (а Джо отключает питание компьютера).

На следующее утро на борту самолета Джо вновь включает компьютер, запускает систему Notes, а затем переключается на документ местоположения Island (Остров). Этот

документ информирует систему Notes о том, что ни один из портов не доступен, и даже в том случае, если Джо попытается связаться с сервером, он не сможет этого сделать.

Вечером в отеле Джо обращается к документу местоположения Travel (В дороге). При этом открывается диалоговое окно, запрашивающее у Джо телефонный номер, предоставляющий доступ к внешней линии связи (Джо задает 8), а также код страны и код области для его текущего места. Документ местоположения Travel сообщает системе Notes, что порт протокола TCP/IP и порты COM1 позволяют формировать соединение.

Джо щелкает по кнопке **Start** (Запуск) на экране **Replicator** (Дублирование) для дублирования баз данных почтовой службы и поддержки продаж с соответствующих серверов. На этот момент задействованы два документа соединения. Из одного документа (того же, который применялся предыдущим вечером в домашних условиях) система Notes узнает о возможности взаимодействия с сервером 3 через порт COM1 и номер 44455556666. (Поскольку текущее место требует другого кода области, системе Notes известно о необходимости междугородного звонка.) Другой документ информирует систему Notes о возможности связи с сервером 3 по протоколу TCP/IP с помощью службы Windows Dial-Up Networking для обращения к местному узлу сети CompuServe и к серверу 3 по сети Internet посредством сетевого соединения. Данный документ прошлым вечером в домашних условиях был бесполезен, поскольку для него специально оговаривалось применение только в режиме **Travel** (В дороге). Система Notes выбирает именно этот документ, так как у него приоритет использования **Normal** (Нормальный), а у другого документа - **Low** (Низкий).

Система Notes автоматически набирает 8 плюс местный телефонный номер узла сети CompuServe. Допустим, номер оказывается занятым, тогда система Notes делает еще несколько попыток и, если результат остается тем же, обращается к другому документу соединения. Поскольку документ указывает на выполнение междугородного звонка и содержит последовательность номеров для оплаты вызова с помощью кредитной карты Джо (Компания AT & T), Джо набирает номер 8, затем 1-800-CALL-ATT, затем 1, а в конце код области сервера 3, местный телефонный номер и номер PIN компании AT&T. При этом обеспечивается формирование необходимого телефонного соединения.

Джо не приходится прилагать никаких усилий - вся информация о соединении содержится в соответствующих документах соединения и местоположения. А вот администратору Джо следует предварительно продумать все детали-, поскольку Джо Доакс не захочет забивать себе голову и будет ожидать формирования быстрого и надежного соединения для продолжения работы в любом месте.

Настройка мобильных пользователей при установке новой рабочей станции

Если уже на этапе установки новой рабочей станции системы Notes известно, что предполагается работа мобильного пользователя, можно задействовать Мастер Lotus Notes Client Configuration Wizard (Мастер конфигурирования клиента Lotus Notes). Этот Мастер обеспечивает создание документов местоположения и соединения для одного удаленного местоположения, а также формирование локальной реплики базы данных почтовой службы (для соответствующего пользователя), что позволит сэкономить усилия и время.

Так, на третьем экране Мастер спросит: **How Do You Want to Connect to a Domino Server?** (Каким образом следует подключаться к серверу Domino?). Возможные варианты ответа:

- **Set up a connection to a local area network (LAN)** (Установка соединения с локальной сетью) - предназначен для пользователя, который применяет систему Notes только в офисе (этот случай подробно рассмотрен в главе 5);
- **Set up a phone connection to a Domino or remote network** (Установка телефонного соединения с сервером Domino или удаленной сетью) - удобен в домашних условиях или в удаленном офисе, когда пользователь взаимодействует с сервером Domino с помощью модема;
- **Set up both a LAN and phone line connection** (Установка телефонного соединения и соединения по локальной сети) - для пользователей переносных компьютеров, которые иногда работают на компьютере в офисе, иногда в домашних условиях, а иногда в дороге. Относится как раз к обслуживанию мобильных пользователей.

Если выбирается второй или третий вариант, Мастер на более поздних этапах (на следующих экранах) предложит заполнить поле **Type of Phone Connection** (Тип телефонного соединения). В этом случае существуют такие возможности:

- **Dial directly into a Domino server** (Непосредственное телефонное подключение к серверу Domino) - выбирается, если пользователь намерен обращаться на сервер Domino, располагающий одним или несколькими собственными модемами. Это может быть сервер адресата, например домашний сервер самого пользователя, или сквозной сервер (более подробно использование сквозных серверов рассмотрено в следующем разделе). Для этого варианта соединения система Notes самостоятельно прорабатывает все характеристики соединения, а пользователю остается лишь правильно указать набираемые телефонные номера;
- **Dial a remote network server** (Коммутируемый доступ к серверу удаленной сети). Вариант задается, когда пользователю требуется связаться (путем непосредственного телефонного соединения) с сервером удаленной сети (возможно, с компьютером без сервера Domino), чтобы соединиться с нужной локальной сетью и далее с одним или несколькими серверами Domino. С точки зрения самой системы Notes (а также тех серверов, с которыми планируется установить контакт) этот пользователь будет инициировать соединение по локальной сети. Однако такое соединение является весьма медленным и предполагает наличие модема. При формировании соединения система Notes применяет службу удаленного доступа соответствующей операционной системы (Dial-Up Networking в Windows, AppleTalk Remote Dial-Up или Macintosh PPP в Macintosh) для управления модемом, набора телефонного номера и организации связи с сервером адресата, а также для последующего отключения. В этом случае система Notes направляет операционной системе запрос на формирование соединения, а затем работает с этим соединением точно так же, как с соединением локальной сети. Затем система Notes обращается к соответствующей службе операционной системы для прерывания сеанса связи и отмены соединения. Конечно, чтобы подобное соединение было сформировано корректно, служба операционной системы должна быть правильно настроена и сконфигурирована;
- **Set up both types of phone connections** (Установка обоих типов телефонного соединения). Если пользователь предполагает, что ему понадобятся оба типа соединения, следует указывать именно этот вариант.

В зависимости от сделанного выбора Мастер в дальнейшем предложит различную последовательность экранов, на которых надо будет вводить информацию, необходимую для

формирования соединений. Если задан первый вариант, появится экран **Dialing a Domino Server Directly** (Непосредственный коммутируемый доступ к серверу Domino). При назначении второго варианта откроется экран **Dialing a Remote Network Server** (Непосредственный коммутируемый доступ к серверу удаленной сети), а в третьем варианте придется иметь дело с шестью различными экранами.

На экране **Dialing a Domino Server Directly** необходимо задать следующие параметры:

- **Domino server phone number** (Номер телефона сервера Domino). Вводится полный телефонный номер, код области или города, в том числе и в случаях, когда пользователь планирует только местные звонки. Так, например, номер записывается в виде 161055666, даже если для вызова достаточно набрать 5556666;
- **Dialing prefix, if any** (Дополнительный префикс, при необходимости). Скажем, если пользователю для выхода во внешнюю линию связи надо набирать 9, это должно быть отражено в данном поле;
- **Modem type** (Тип модема). Здесь достаточно указать тип модема в предлагаемом списке. Когда модем в списке отсутствует, выбирается наиболее близкий к нему тип. Если ни для одного модема из списка не реализуется нормальный режим связи, можно выбрать **Auto Configure** (Автоматическое конфигурирование; только для отсутствующих в списке модемов) или **Generic All-Speed Modem File** (Общий файл модема для любой скорости обмена данными). Если один из этих вариантов дает положительный результат, на более позднем этапе потребуются уточнить тип модема, поскольку оба описанных варианта позволяют формировать соединения с относительно низкими скоростями передачи данных (заметно меньшими тех, которые может обеспечить соответствующий модем). В случае возникновения каких-либо трудностей воспользуйтесь рекомендациями главы 3;
- **Modem port** (Порт модема). Укажите порт COM, с которым соединен модем пользователя;
- **Modem setup** (Установка модема). Открывается диалоговое окно **Addinional Setup** (Дополнительная настройка), в котором определяются параметры модема и назначается сценарий (при необходимости). На данном шаге вполне допустимо оставить параметры модема без изменений. (Имейте в виду, что в будущем появится возможность модифицировать исходные настройки.) Однако для нескольких полей настройку можно произвести уже сейчас. Речь идет о следующих полях:
 - **Maximum port speed** (Максимальная скорость передачи данных для порта). По умолчанию скорость меньше максимальной величины, допустимой для модема, поэтому при желании измените параметры настройки и предусмотрите возможность передачи данных на максимальной скорости. В дальнейшем вы сможете вновь уменьшить этот показатель, например если окажется, что модем не обеспечивает устойчивую связь с сервером на максимальной скорости передачи данных;
 - **Log modem I/O** (Регистрация данных ввода/вывода для модема). Эту функцию лучше отменить, активизировав только в том случае, если появятся проблемы с формированием соединения. После решения проблем функцию рекомендуется вновь отменить: в противном случае каждая команда, направляемая компьютером на модем, будет регистрироваться в базе данных Notes Log (Журнал системы Notes) вместе со всеми ответными сообщениями модема. Если оставить этот режим, жесткий диск пользователя быстро переполнится регистрируемой информацией;

- **Log script I/O** (Регистрация сценариев при вводе/выводе). Для данного поля остается справедливым все сказанное выше. Функцию рекомендуется отменять во всех случаях, за исключением отладки соответствующего сценария;
- **Wait for dialtone before dialing** (Ожидание гудка перед набором номера). Данную функцию, скорее всего, придется отменить для пользователей, набирающих номер в домашних условиях. Некоторые модемы распознают не все сигналы, которые формируют современные телефонные службы. Например, если телефонная компания пользователя обеспечивает службу автоответчика, то посредством специального тонального сигнала можно информировать абонента о пропущенных им вызовах. Для отключения тонального сигнала (гудка) пользователь должен набрать соответствующий номер и прослушать пропущенные сообщения. Отмена этой функции позволяет модемам набирать номер даже в тех случаях, когда тональный сигнал формируется автоответчиком, но в то же время не дает возможности модему считать линию занятой;
- **Acquire Script** (Заимствование сценария). В ряде случаев приходится искать подходящий сценарий, например когда пользователь не располагает собственным модемом, а вынужден заимствовать его в пуле модемов. Об этом, естественно, желательно узнать заблаговременно и скопировать требуемый файл со сценарием в папку модемов пользователя до выполнения данной операции.

На экране **Dialing a Remote Network Server** (Коммутируемый доступ к серверу удаленной сети) приходится задавать следующие данные:

- О **Phonebook entry to us** (Запись телефонной книги для использования). Для клиентов Notes в операционной системе Windows подобная запись относится к службе Dial-Up Networking. Все существующие записи в службе Dial-Up Networking станут доступными пользователю;
- О **Create New Entry** (Создание новой записи). Если ни одна из существующих записей службы Dial-Up Networking не подходит для пользователя (или эти записи отсутствуют), можно этой кнопкой запустить Мастер Make New Connection Wizard (Мастер формирования нового соединения) службы Dial-Up Networking. Мастер предложит ввести имя нового соединения, выбрать ранее установленный модем и указать номер телефона компьютера адресата. При этом также появится возможность конфигурирования модема заданным образом (см. главу 3).

Заполнение перечисленных ниже полей необязательно. Если оставить их пустыми, система Notes поместит туда данные из полей коммутируемого соединения, указанного в поле **Phonebook entry to use** службы Dial-Up Networking (если и эти поля окажутся незаполненными, система Notes будет направлять пользователю запрос относительно необходимых данных каждый раз, когда он начнет формировать соединение). Имеются в виду следующие поля:

- О **User name** (Имя пользователя). В поле вносится имя пользователя, для которого компьютер адресата обеспечит правильное распознавание;
- О **Password** (Пароль). Здесь указывается пароль, позволяющий связаться с системой адресата;
- О **Phone number** (Номер телефона). В этом поле вводится номер телефона для компьютера адресата;

- **Dialing prefix, if any** (Телефонный префикс, при необходимости). Поле предназначено для номеров, которые приходится набирать перед телефонным номером компьютера адресата. Например, для выхода на внешнюю линию часто служит цифра 9. Если поле остается незаполненным, система Notes воспользуется префиксом из поля **Dialing from** (Вызов из) службы Dial-Up Networking. Чтобы узнать этот префикс, отметьте пункт **Dial Properties** (Свойства набираемого номера) в диалоговом окне **Connect To** (Соединение с) соответствующего соединения службы Dial-Up Networking.

Заполнив все названные поля, щелкните по кнопке **Finish** (Готово) – Мастер создаст на рабочей станции пользователя перечисленные ниже объекты. Они будут сформированы в полном соответствии с параметрами, определенными в диалоговых окнах Мастера. Следует отметить, что Мастер создаст эти объекты в дополнение к другим объектам, которые уже были сделаны ранее с помощью других диалоговых окон. Вновь созданные объекты:

- **A Notes Direct Dialup connection document to the user's home server** (Документ прямого коммутируемого соединения Notes с домашним сервером пользователя). Подобный документ формируется в том случае, если на экране **Type of Phone Connection** (Тип телефонного соединения) был выбран вариант **Dial directly into a Domino server** (Непосредственный набор номера сервера Domino). Подобное соединение позволит системе Notes производить набор телефонного номера самого домашнего сервера пользователя;
- **A Network Dialup connection document to the user's home server** (Документ сетевого коммутируемого соединения с домашним сервером пользователя). Создается, если на экране **Type of Phone Connection** был задан вариант **Dial a Remote network server** (Коммутируемый доступ к серверу удаленной сети). Назначение документа – предоставить системе Notes возможность с помощью службы Windows Dial-Up Networking формировать коммутируемое соединение с удаленной локальной сетью и применять его для связи с домашним сервером пользователя;
- **A local replica of the user's mail database** (Местная реплика базы данных почтовой службы пользователя). Эта копия располагается в подпапке почтовой службы пользователя;
- **An entry for the user's mail database on the Replicator page of the Notes client** (Запись для базы данных почтовой службы пользователя на странице репликации клиента Notes). Позволяет организовать репликацию указанной базы данных в фоновом режиме;
- **An entry called Send outgoing mail on the Replicator page of the Notes client** (Запись для отправленной исходящей почты на странице репликации клиента Notes). Служит для пересылки (в фоновом режиме) исходящего почтового сообщения на сервер почтовой связи пользователя. Появляется на экране **Replicator** (Репликатор) пользователя только при условии, что для текущего местоположения ранее был задан вариант **Local** (Локальный) в поле **Mail file location** (Местоположение файла почтовых сообщений) вкладки почтовой службы (Mail) соответствующего документа местоположения;
- **An Outgoing Mail database** (Запись для базы данных исходящей почты, файл mail.box). Когда рабочая станция пользователя является удаленной по отношению к серверу Domino, исходящие почтовые сообщения запоминаются в этой базе данных после щелчка пользователя по кнопке **Send** (Пересылка). Сообщения передаются на сервер

почтовой службы пользователя командами **Start => Send & Receive Mail** (Запуск => Пересылка и прием почтовых сообщений) или **Other Actions => Send Outgoing Mail** (Другие операции => Пересылка исходящих почтовых сообщений) на экране **Replicator**. Местоположение считается удаленным от сервера Domino в том случае, если документ местоположения имеет значение **Local** в поле **Mail file location** (Местоположение файла почтовых сообщений) вкладки почтовой службы.

Установка существующих пользователей в качестве мобильных

Если на более ранних стадиях настройки при исполнении Мастера Lotus Notes Client Configuration Wizard не были сделаны соответствующие уточнения, придется теперь создавать все упомянутые выше объекты самостоятельно. На практике далеко не всегда заранее известно, что мобильность потребуется уже существующему пользователю. Поэтому необходимо свести все рассуждения в единый перечень для правильного уяснения тех действий, которые следует выполнить в случае обращения пользователя с просьбой обеспечить доступ к удаленному серверу. Задача, по сути, сведется к перенастройке уже имеющейся рабочей станции системы Notes для мобильных пользователей, для чего потребуются создать:

- О документ местоположения (Location document) - при необходимости. Если пользователь планирует работать в нескольких местах, например переезжая из одного места в другое, понадобится соответствующее число документов местоположения (Office, Home, Internet, Island, Travel), причем не исключено, что даже этих документов будет недостаточно, чтобы удовлетворить все потребности. В ряде специфических случаев придется создавать дополнительные документы местоположения. Например, в некоторых отелях пользователь, возможно, захочет сам оплачивать телефонные счета, а в других отелях оплата счетов будет производиться по кредитной карте. Следовательно, нужны два документа местоположения Travel - один, предусматривающий введение номера кредитной карты при формировании вызова, а другой, напротив, предполагающий наличный расчет. Пользователь, разумеется, будет иметь возможность обратиться к любому документу местоположения Travel в зависимости от конкретной обстановки;
- О по меньшей мере один документ соединения (Connection document). Его тип зависит от характера соединения, посредством которого пользователь собирается связываться с домашним (или с другим) сервером;
- О локальную реплику базы данных почтовой службы пользователя. Эта копия базы данных должна размещаться в подпапке почтовой службы на рабочей станции пользователя, поскольку именно там документы местоположения (Home, Internet, Island, Travel) будут пытаться ее обнаружить. Наличие локальной реплики приведет также к тому, что на странице **Replicator** появится новая запись для базы данных почтовой службы пользователя;
- О локальную базу данных Outgoing Mail (Исходящие почтовые сообщения). Система Notes обычно формирует эту базу данных автоматически еще при первом обращении к документу местоположения, у которого в поле **Mail file location** (Местоположение файла почтовых сообщений) задан вариант **Local** (Локальный). Кроме того, система Notes добавит вариант **Send Outgoing Mail** (Пересылка исходящих почтовых сообщений) на страницу **Replicator**, когда документ местоположения станет текущим.

Документы местоположения

Документ местоположения (Location document) содержит все переменные, определяющие конкретное местоположение пользователя, например информирует систему Notes о необходимости соединения с сервером по локальной сети или с помощью модема, для которого дополнительно указывается местное телефонное соединение или междугородний телефонный вызов.

Вновь настроенная рабочая станция системы Notes содержит шесть типовых документов местоположения:

- **Office (Network)** - документ местоположения офиса. Предназначен для работы в офисе, когда пользователь через локальную сеть легко связывается со своим домашним сервером;
- **Home (Network Dialup)** - домашний документ местоположения с коммутируемым доступом к сети. Предполагает работу дома, а также применение соединения с удаленной локальной сетью для связи с сервером Domino. Эта связь осуществляется через порт локальной сети, а подключение к сети - посредством коммутируемого доступа к серверу удаленного доступа этой сети или сети, имеющей связь с нужной сетью;
- **Home (Notes Direct Dialup)** - домашний документ местоположения с прямым коммутируемым доступом к системе Notes. Рассчитан на работу в домашних условиях при наличии непосредственного коммутируемого доступа к серверу Domino с помощью модема, подключенного к порту COM;
- **Travel (Notes Direct Dialup)** - документ местоположения путешествия с прямым коммутируемым доступом к системе Notes. Позволяет работать в любом месте, кроме дома и офиса; требуется непосредственный коммутируемый доступ к серверу Domino через модем, подключенный к порту COM;
- **Internet** - документ местоположения сети Internet. Необходима постоянная связь по локальной сети с Internet (но необязательно с домашним сервером пользователя);
- **Island (Disconnected)** - документ изолированного (отключенного) местоположения — «островок». Отсутствует возможность связи с любой локальной сетью или подключения к телефонной линии связи, а также к любому серверу Domino.

Если в процессе настройки клиента Notes планируется создание учетных записей почтовой службы сети Internet, могут потребоваться другие документы местоположения, специально предназначенные для работы с учетными записями. Тем не менее перечисленных выше документов обычно вполне достаточно для пользователей системы Notes, в том числе и мобильных. Следовательно, для большей части пользователей системы Notes нужно лишь отредактировать тот или иной документ. Возможно, конечно, что кому-то из пользователей потребуются и другие документы местоположения, поэтому в ряде случаев придется формировать новые документы. И хотя некоторые пользователи в состоянии создавать подобные документы самостоятельно, подавляющее большинство все-таки полагается на своих администраторов. Можно (при необходимости) создать новый документ местоположения для пользователя непосредственно на рабочей станции пользователя либо сделать его на собственной рабочей станции, а затем скопировать в вид **Locations** (Местоположения) базы данных Domino Directory и предложить пользователям в дальнейшем копировать документ в их персональные базы данных Personal Address Book.

Для создания нового документа местоположения необходимо сделать следующее:

1. Перейдите на вид **Advanced => Locations** (Дополнительно => Местоположение) базы данных Personal Address Book.

2. Выберите Add Location (Добавление местоположения) на панели Toolbar (Панель программных инструментов) или команду Location (Местоположение) в меню Create (Создание).
3. Заполните поля формы, после чего сохраните ее и закройте.

Документ местоположения представляет собой достаточно объемную и сложную форму, содержащую множество полей. В табл. 6.7 представлено описание всех этих полей с комментариями. Тем не менее назначение некоторых полей будет обсуждаться в последующих разделах (в табл. 6.7 даны соответствующие ссылки).

Таблица 6.7. Некоторые важные поля документа местоположения

Имя поля*	Назначение
	Вкладка Basics (Основные параметры)
Location type (Тип местоположения)	В зависимости от сделанного в этом поле выбора разрешается использование тех или иных полей и вкладок. Если выбран вариант Local Area Network (Локальная сеть), исчезает вкладка Phone Settings (Параметры телефонной линии связи). Если используется вариант No Connection (Без формирования соединения), пропадают вкладки Servers (Серверы), Ports (Порты) и Phone Settings (Параметры телефонной линии связи). Выбор варианта Local Area Network , Network Dialup or Custom (Локальная сеть, коммутируемый сетевой доступ или особый доступ) позволяет задать местоположение в локальной сети. Вариант Notes Direct Dialup (Прямой коммутируемый доступ к системе Notes) даст возможность указать параметры модемного подключения, а No Connection определяет отключенное местоположение
Location name (Имя местоположения)	В это поле следует вводить описательное название. В дальнейшем при просмотре вида Locations (Местоположения) документы местоположения будут приводиться в последовательности, определяемой их названиями
Internet mail address (Адрес почтовой службы сети Internet)	В это поле следует заносить обратный адрес сети Internet. Любые сообщения, направляемые абонентам сети Internet из данного местоположения, будут снабжены обратным адресом, указанным здесь. Адрес может быть введен в виде имя@домен или показанное_имя<имя@домен>
Prompt for time/date/phone (Запрос на ввод времени/даты/номера телефона)	Значение Yes (Да) приведет к выводу диалогового окна с предложением указать время, дату и телефонный номер каждый раз, когда будет происходить обращение к документу местоположения. Рекомендуется задавать в этом поле вариант Yes для любого документа местоположения, который планируется применять в дороге, например для пересылки сообщений из различных уголков планеты
Proxy (Прокси)	Это поле появляется только в том случае, если в поле Local type (Тип местоположения) указано Local Area Network , Network Dialup или Custom . В поле следует вводить имя хоста или IP-адрес любого прокси-сервера, который будет использоваться для связи с данным местоположением. Можно также щелкнуть по соответствующей кнопке и задать несколько прокси, хостов или доменов для подключения в обход прокси-сервера

Все значения являются необязательными, кроме специально отмеченных.

Таблица 6.7. Некоторые важные поля документа местоположения (продолжение)

Имя поля*	Назначение
Default display name (Выводимое по умолчанию имя)	Здесь указывают Display primary names (Показ основных имен) или Display alternate names (Показ альтернативных имен). В соответствии со сделанным выбором система Notes выводит список имен пользователей на основном или альтернативном языках
Вкладка Servers (Серверы) для всех типов местоположений, за исключением No connection	
Home/Mail Server (Домашний/ почтовый сервер)	В зависимости от сделанного в этом поле выбора сервер системы Notes будет по-разному извлекать и доставлять почтовые сообщения. В режиме по умолчанию предусматривается использование сервера Home/Mail (Домашний/почтовый), указанного в персональном документе (Personal document) пользователя в базе данных Domino Directory. Обычно этот режим оказывается вполне подходящим, однако при определенных нетипичных условиях следует задавать другой домашний/почтовый сервер. Так, например, если пользователь проводит много времени в лос-анджелесском и токийском офисах компании, он может создать домашний/почтовый серверы для применения в обоих офисах посредством размещения реплики базы данных почтовой службы в каждом офисе. Все серверы будут направлять почтовые сообщения этому пользователю на тот почтовый сервер, который указан в его персональном документе, хранящемся в каталоге Domino Directory. Но когда пользователь начнет выбирать и читать свои почтовые сообщения или отправлять новые, система Notes станет обращаться к серверу, определенному в данном поле
Pass-thru server (Сквозной сервер)	Если система не может найти путь к требуемому серверу Domino, она будет искать сервер Domino с именем, приведенным в этом поле, и просить разрешения пользоваться им для сквозного доступа к нужному серверу. В режиме по умолчанию домашний/почтовый сервер зарегистрированного пользователя задается в качестве такого сквозного сервера
Catalog/domain search server (Сервер для поиска в каталоге/домене)	Сервер служит для поиска баз данных во всем домене
Domino Directory server (Сервер каталога Domino Directory)	Сервер предназначен для просмотра имен в базе данных Domino Directory или Directory Catalog при адресации почтовых сообщений
Вкладка Ports (Порты) для всех местоположений за исключением No Connect	
Ports to use (Используемые порты)	В этом поле приводится список всех разрешенных портов в данной копии клиента системы Notes. Выбирать следует те порты, которые планируется сделать доступными в данном месте
Вкладка Mail (Почта)	
Mail file location (Местоположение файла почтовых сообщений)	Здесь может быть задан вариант Local (Локально) или On server (На сервере). Если выбирается вариант Local , система Notes будет полагать, что почтовый сервер недоступен. По щелчку почтовой закладки система откроет локальную базу данных почтовых сообщений и сохранит все отправляемые почтовые сообщения

Таблица 6.7. Некоторые важные поля документа местоположения (продолжение)

Имя поля*	Назначение
Mail file location	в локальной базе данных Outgoing Mail (Исходящие почтовые сообщения). При выборе варианта On server система Notes будет считать, что почтовый сервер находится поблизости и откроет серверную копию базы данных почтовых сообщений. Все отправляемые почтовые сообщения будут переправляться в базу данных Outgoing Mail сервера
Mail file (Файл почтовых сообщений)	В этом поле следует вводить часть пути к файлу базы данных почтовой службы. Если местоположением файла Mail (Почтовая служба) является Local , то указывается путь к локальной копии базы данных почтовой службы. В противном случае задается путь к серверной копии базы данных почтовой службы. При неправильном заполнении поля невозможно создать новое почтовое сообщение командой Mail в меню Create (Создание), а ярлык для работы с почтой работает некорректно
Notes mail domain (Домен почтовой службы системы Notes)	Запишите в этом поле имя домена для почтового сервера Domino
Internet domain for Notes addresses when connecting directly to the Internet (Домен Internet для адресов системы Notes при соединении с Internet)	Здесь следует вводить имя домена сети Internet для используемого почтового сервера
Recipient name type-ahead (Предварительный ввод имен адресатов)	В этом поле нужно указать, будет ли система Notes просматривать имена пользователей во время ввода, чтобы автоматически закончить не полностью введенное имя. Когда почтовый сервер или сервер каталога расположены поблизости, обычно используется значение Local than Server (Локальный, а затем сервер), а для удаленных серверов - значение Only Local (Только локально)
Recipient name lookup (Просмотр имен адресатов)	В этом поле следует указывать, каким образом система Notes будет просматривать имена адресатов. Система может останавливаться (Stop) после обнаружения первого соответствия или продолжать (Exhaustive) проверку всех адресных книг. Первый метод является более быстрым, а второй гарантирует отсутствие случайных совпадений имен
Mail addressing (Адресация почтовых сообщений)	Данное поле появляется только в том случае, если в поле Mail file location задается значение Local . Если в этом поле указан вариант Only Local (Только локально), что происходит в режиме по умолчанию, то для просмотра и анализа имен применяются только локальные адресные книги. При пересылке нового сообщения в локальную базу данных Outgoing Mail система Notes не будет проверять имена на предмет их корректности. Если в поле задается вариант Local and Server (Локально и сервер), система Notes станет проверять все имена адресатов в локальных книгах адресов и адресных книгах сервера (каталогах), а также проводить синтаксический анализ всех этих имен

Таблица 6.7. Некоторые важные поля документа местоположения (продолжение)

Имя поля*	Назначение
Mail addressing	перед отправкой сообщения. Конечно, если отсутствует быстрый и простой доступ к серверу (например, по локальной сети), пользователь вряд ли захочет выбирать вариант Local and Server , поскольку подобный просмотр может затянуться на целую вечность
Send outgoing mail (Пересылка исходящих почтовых сообщений)	В данном случае допустимо пересылать все исходящие почтовые сообщения с помощью сервера Domino или непосредственно в сеть Internet, когда исходящие почтовые сообщения сразу адресуются абонентам сети Internet. Система Notes может передавать подобные сообщения на почтовые хосты SMTP или на сервер Domino (который в свою очередь будет переправлять их на хост SMTP). Подобный подход оказывается удобным для пользователей системы Notes, применяющих эту систему для чтения почтовых сообщений по учетным записям службы POP и/или IMAP, не принадлежащим к системе Domino
Format for messages addressed to Internet addresses (Форматирование почтовых сообщений согласно адресам сети Internet)	Этот формат сообщения задается по умолчанию. Чтобы использовать другие форматы для пересылки конкретных почтовых сообщений, следует выбрать Notes Rich Text Format (Формат расширенного текста системы Notes) или MIME Format (Формат MIME). В первом случае сообщения, направляемые абонентам сети Internet, будут преобразованы в текстовый формат, во втором случае сохраняется формат MIME. Для подписывания или шифрования сообщений, представленных в формате MIME, нужны сертификат X.509 и пара ключей, хранящихся в файле идентификационных данных пользователя. Более подробная информация о формате MIME и сертификатах X.509 содержится в главах 8 и 10
Send outgoing mail if _____ messages pending (Пересылка исходящих почтовых сообщений при накоплении _____ сообщений)	Данное поле появляется только в том случае, если для поля Mail file location выбирается вариант Local . При этом система Notes будет автоматически инициировать передачу почтовых сообщений базы данных Outgoing Mail на сервер, когда их число достигнет указанного значения. По умолчанию данное поле не заполняется, то есть система Notes никогда не инициирует отправку почтовых сообщений, за исключением пересылки по запросу или в ходе запланированной репликации
Вкладка Internet Browser (Браузер сети Internet)	
Internet browser (Браузер сети Internet)	В этом поле можно выбрать браузер, который будет запускаться системой Notes при обращении к Web-серверу из клиента Notes. Следует указать Notes to user Notes's or Domino's own, internal browser (Связь с системой Notes и сервером Domino браузером Notes, внутренний браузер). Внутренним браузером системы Notes является Personal Web Navigator (Персональный Web-навигатор) для клиента Notes или Server Web Navigator (Серверный Web-навигатор) для Domino. Допустимо также задать вариант Notes with Internet Explorer (Клиент Notes с обозревателем Internet Explorer), установленный по умолчанию, и воспользоваться одной из версий браузера Internet Explorer, которая открывается в окне любой из двух упомянутых выше программ или в собственном окне. Кроме того, можно указать Netscape Navigator или Microsoft Internet Explorer, чтобы работать

Таблица 6.7. Некоторые важные поля документа местоположения (продолжение)

Имя поля*	Назначение
Internet browser	с одноименными браузерами в их диалоговых окнах. Пункт Other (Другие варианты) позволит определить любой другой браузер, запускаемый в собственном диалоговом окне ¹
Retrieve/open pages (Извлечение/открытие страниц)	Это поле будет появляться в том случае, если ранее выбран режим Notes (Система Notes) или Notes with Internet Explorer (Система Notes с браузером Internet Explorer). В режиме Notes доступен вариант From InterNotes server (С сервера InterNotes), то есть с сервера Domino, использующего программу Server Web Navigator и действующего в режиме прокси-браузера, что полезно для рабочих станций без поддержки стека TCP/IP, либо вариант для рабочих станций системы Notes с одноименным браузером и запрещением извлечения страниц при отключении Web-просмотра. Если же выбран вариант Notes with Internet Explorer , в данном поле можно указать From Notes (Извлечение страниц из системы Notes) либо No retrieve (Без извлечения)
Internet browser path (Путь к браузеру сети Internet)	Если для браузера выбирается вариант Other (Другие), появится эта кнопка, которая позволяет определять исполняемый файл браузера в файловой системе Вкладка Replication (Репликация)
Schedule (Планирование)	В режиме по умолчанию для этого поля задается вариант Disabled (Отмена). Если разрешить планирование репликации, появятся другие поля (см. ниже)
Replicate daily between (Ежедневная репликация в интервале между)	Здесь следует задавать временной интервал, в течение которого репликация данных будет выполняться автоматически. Допускается также указать точное время ее проведения
Repeat every (Повторение каждые)	Если в предыдущем поле был задан временной интервал, в данном поле также будет указан временной интервал, определяющий периодичность выполнения репликации системой Notes
Days of week (Дни недели)	Здесь могут указываться дни недели, когда система Notes будет осуществлять репликацию в соответствии с расписанием, заданным в предшествующих полях
High priority replication (Репликация с высоким уровнем приоритета)	Это поле используется для задания индивидуального плана репликации баз данных, имеющих высокий уровень приоритета. По умолчанию всем базам данных присваивается приоритет среднего уровня. Однако пользователь имеет возможность задать для базы данных собственный приоритет репликации в диалоговом окне Replication Settings (Параметры репликации). В этом случае следует выполнить в меню команду File => Replication => Settings (Файл => Репликация => Параметры), затем выбрать Other (Другие варианты) - станет доступен дополнительный набор параметров репликации

Браузер Web Navigator в системе Notes R5/6 заметно усовершенствован по сравнению с версией 4. Среди прочего обеспечена поддержка стандарта HTML 4.0, например кадров.

Таблица 6.7. Некоторые важные поля документа местоположения (продолжение)

Имя поля*	Назначение
Вкладка Phone Settings (Параметры телефонной связи) для всех типов местоположения, за исключением Local Area Network и No Connection	
Prefix for outside line (Префикс для выхода на внешнюю линию связи)	B это поле следует вводить число (например, 8 или 9), необходимое для получения доступа к внешней линии связи
International prefix (Префикс международных вызовов)	Здесь нужно указать префикс, который требуется при международном телефонном вызове
Country code at this location (Код страны для данного местоположения)	В данном поле необходимо задать телефонный код страны даже в том случае, если международные вызовы не планируются
Long distance prefix (Префикс междугородной связи)	По умолчанию значение равно 1. При необходимости код может быть изменен
Area code at this location (Код области для данного местоположения)	Здесь следует ввести код области независимо от того, намечаются ли междугородные вызовы
Calling card access number (Номер доступа телефонной карты при вызове)	В этом поле нужно задать номер доступа телефонной карты, если планируется оплачивать телефонные вызовы с ее помощью
Calling card number or extension (Номер или расширение для телефонной карты)	В данном поле указывают номер телефонной карты для оплаты телефонных вызовов, или дополнительный номер в том случае, когда местоположение вызывающей стороны предусматривает его набор после набора номера вызываемого абонента (или если требуется вводить этот номер уже после того, как вызываемый абонент поднял трубку)
Dialing Rules (Правила набора номера)	Нажмите данную кнопку после заполнения других полей раздела. Появится диалоговое окно, указывающее на последовательность цифр, которые система Notes будет направлять в модем. Проверьте правильность ранее введенных данных
Вкладка Advanced (Дополнительно), подкладка Basics (Основные параметры)	
Use operating system's timezone settings (Использование параметров временных зон операционной системы)	По умолчанию выбирается вариант Yes (Да). При изменении записи параметры временных зон в систему Notes станут независимыми от операционной системы
Only for user (Только для пользователя)	По умолчанию здесь вводится звездочка, которая разрешает доступ для любого пользователя. Если задать имя конкретного пользователя, то только он в дальнейшем будет иметь право использовать данный документ местоположения
UserID to switch to (Идентификационные данные пользователя для переключения на)	В этом поле можно указать путь или выбрать файл идентификационных данных. При переключении на данный документ местоположения, система Notes одновременно переключится на указанный файл идентификационных данных и откроет диалоговое окно для ввода пароля

Таблица 6.7. Некоторые важные поля документа местоположения (продолжение)

Имя поля*	Назначение
Load images (Загрузка изображений)	В этом поле по умолчанию задается вариант Always (Всегда), который указывает на загрузку изображений, являющихся частью документов. Значение On request (По запросу) приведет к запрету автоматической загрузки изображений, хотя их можно получить по запросу
Bookmarks filename (Имя файла для закладок)	Здесь следует вводить имя файла для базы данных Bookmarks (Закладки), которая хранит параметры закладок для заданной копии клиента системы Notes. По умолчанию в это поле записывается имя файла bookmark.nsf
Subscriptions filename (Имя файла для подписей)	В поле нужно указать имя файла для базы данных, которая хранит подписи и связанные с ними записи. По умолчанию вводится имя файла headline.nsf
Network dialup idle timeout (Тайм-аут для сетевого коммутируемого доступа)	В этом поле необходимо задать число минут бездействия (интервал ожидания), которые должны истечь перед тем, как система Notes прервет соединение. В режиме по умолчанию обычно ничего не указано (значение «пусто»), поэтому система Notes никогда не прерывает соединения

Вкладка **Advanced**, подкладка **SSL** (Защищенный уровень сокета)

Accept SSL site certificates (Прием сертификатов от сайтов SSL)	По умолчанию в данном поле задается вариант No (Нет), то есть система Notes не примет сертификаты сайтов от неизвестных ей авторизаторов сертификации
Accept expired SSL certificates (Прием сертификатов SSL с истекшим сроком действия)	По умолчанию здесь указан вариант Yes (Да), то есть система Notes не учитывает срок действия сертификатов
SSL protocol version (Версия протокола SSL)	По умолчанию в этом поле задается вариант Negotiated (Согласование) - система Notes использует любую версию, приемлемую для сервера SSL, или конкретную версию протокола SSL

Вкладка **Advanced**, подкладка **Web Retriever** (Web-извлечение)

Web Navigator database (База данных программы Web Navigator)	По умолчанию в этом поле задано имя файла perweb.nsf. Оно соответствует базе данных, которую система Notes использует для хранения извлеченных документов HTML в том случае, если применяется браузер Notes
Concurrent retrievers (Число одновременных операций извлечения)	Здесь следует указывать максимальное число операций извлечения документов HTML, которые система Notes в состоянии провести одновременно. По умолчанию обычно задается число 15
Retrieve log level (Уровень регистрации процедуры извлечения)	В этом поле нужно задавать показатели сообщений программы Web Retriever, заносимых в журнал рабочей станции (файл log.nsf). По умолчанию обычно выбран вариант No logging (Без регистрации), но можно указать Terse (Кратко) и Verbose (Подробно)
Update cache (Обновление кэш-памяти)	Поле определяет, как часто система Notes будет обновлять в своем кэше извлеченные Web-страницы. По умолчанию задается вариант Once per session (Один раз за сеанс связи). Это означает, что после перезапуска клиента Notes и обращения к уже кэшированной Web-странице система Notes проверит на Web-сайте содержимое

Таблица 6.7. Некоторые важные поля документа местоположения (продолжение)

Имя поля*	Назначение
Update cache	собственной копии Web-страницы. Если страница не изменилась, будет предоставлена копия из кэш-памяти, а страница, подвергшаяся изменению, загрузится с Web-сайта. Другие возможные варианты: Never (Никогда) и Every time (Каждый раз)
Вкладка Advanced , подкладка Java Applets Security (Безопасность апплетов Java), см. также главу 5	
Trusted hosts (Доверенные хосты)	В этом поле следует указывать хосты и домены TCP/IP, апплеты из которых считаются корректными
Network access for trusted hosts (Сетевой доступ для доверенных хостов)	Здесь задается уровень сетевого доступа, разрешенный системой Notes для апплетов Java из доверенных хостов
Network access for untrusted hosts (Сетевой доступ для недоверенных хостов)	В поле нужно описать уровень сетевого доступа, разрешенный системой Notes для апплетов Java из недоверенных хостов
Trust HTTP proxy (Доверенный прокси HTTP)	По умолчанию здесь задается вариант No (Нет). Это означает, что система Notes не будет полагаться на прокси-сервер HTTP при разрешении имени хостов, из которых получены апплеты Java с использованием IP-адреса хоста. Другими словами, система Notes будет сама проводить операцию разрешения (определения) имен хостов даже в том случае, если прокси-сервер позволяет решать аналогичную задачу
Вкладка Advanced , подкладка Secondary Servers (Вторичные серверы)	
Secondary TCP/IP Notes name server (Вторичный сервер имен Notes для протокола TCP/IP)	Данные этого поля имеют смысл только в сетях TCP/IP, Если домашний/почтовый сервер пользователей (применяющий протокол TCP/IP) оказывается недоступен, система Notes попытается связаться с вторичным сервером имен Notes для проведения поиска по имени. Если этот сервер также оказывается недоступен (или вообще не установлен), система Notes выведет в сеть широковещательную рассылку и будет пользоваться услугами первого из откликнувшихся серверов имен. Поскольку широковещательная рассылка осуществляется с помощью стека TCP/IP, откликнуться смогут только серверы, которые поддерживают названные протоколы
Secondary TCP/IP host name or address (Имя или адрес вторичного хоста TCP/IP)	В этом поле вводится имя или IP-адрес вторичного хоста (сффера) имен
Secondary NDS Notes name server (Вторичный сервер имен Notes для NDS)	Данные указанного поля имеют смысл только в сетях SPX, то есть для файловых серверов NetWare 4 или выше (в NetWare 3 и более ранних версиях служба каталога NDS не поддерживается). Если домашний/почтовый сервер пользователей (применяющий протокол NDS/SPX) оказывается недоступен, система Notes попытается связаться с вторичным сервером имен Notes для проведения поиска по имени. Если этот сервер также оказывается недоступен (или вообще не установлен), система Notes выведет в сеть широковещательную рассылку и будет пользоваться услугами первого из откликнувшихся

Таблица 6.7. Некоторые важные поля документа местоположения (окончание)

Имя поля*	Назначение
Secondary NDS Notes name server	серверов имен. Поскольку для широковещательной рассылки используется протокол SPX, откликнуться смогут только серверы, которые поддерживают названный протокол
Secondary NDS name server address (Адрес вторичного сервера имен NDS)	Здесь следует вводить имя NDS вторичного сервера. В данном случае имена NDS совпадают с именами Notes, поскольку основаны на схеме именования из стандарта X.500. Различия между именами только в том, что в именах NDS отдельные компоненты (C, O, OU и CN) будут разделяться с помощью точек, а не слэша
Secondary NetBIOS Notes name server (Вторичный сервер имен Notes для протокола NetBIOS)	Данные этого поля имеют смысл только в сетях NetBIOS, NetBIOS over IP или NetBIOS over SPX. Если домашний/почтовый сервер пользователей (применяющий протокол NetBIOS) оказывается недоступен, система Notes попытается связаться с вторичным сервером имен Notes для проведения поиска по имени. Если этот сервер также оказывается недоступен (или вообще не установлен), система Notes выведет в сеть широковещательную рассылку и будет пользоваться услугами первого из откликнувшихся серверов имен. Поскольку для широковещательной рассылки используется протокол NetBIOS, откликнуться смогут только серверы, которые поддерживают этот протокол

Вкладка **Advanced**, подвкладка **MIME Settings** (Параметры MIME)

Outbound attachment encoding method (Метод кодирования исходящих вложений)	По умолчанию здесь задается вариант Base64, но можно указать кодировку Quoted-Printable . Рекомендуется использовать вариант по умолчанию, если только нет необходимости применять другую кодировку
Outbound Macintosh attachment conversion (Метод кодирования исходящих вложений Macintosh)	По умолчанию в этом поле задается вариант BinHex 4.0 , но можно указать кодировку AppleDouble (только при Base64). Рекомендуется использовать вариант по умолчанию во всех случаях когда не требуется другая кодировка

Вкладка **Administration** (Администрирование)

Owner (Владелец)	По умолчанию здесь указано имя создателя данного документа. Владелец имеет возможность редактировать документ, если обладает правом доступа к соответствующей базе данных не ниже Author (Автор)
Administrators (Администраторы)	В это поле следует вводить имена тех администраторов, которые будут обладать правом редактирования данного документа, но только в том случае, если они обладают правом доступа к соответствующей базе данных на уровне не ниже Author

Документы соединения

Документ соединения (Connection document) информирует систему Notes о способе подключения к одному или нескольким серверам Domino (обычно к одному). Этот документ можно создать двумя способами.

Во-первых, с помощью Мастера Connection Configuration Wizard (Мастер конфигурации соединения). Часто одновременно с документом местоположения требуется создавать

дополнительный документ соединения, поэтому система предлагает прибегнуть к услугам Мастера Connection Configuration Wizard, кнопка которого выводится на панели **Action** (Операции) любого документа местоположения. Мастер позволит выполнить все необходимые действия. Результирующий документ соединения в этом случае будет иметь тот же тип (Local Area Network, Network Dialup или Notes Direct Dialup), что и связанный с ним документ местоположения, что полезно при работе с текущим документом местоположения.

Во-вторых, можно сформировать документ соединения вручную:

1. Откройте адресную книгу (Address Book) пользователя.
2. Перейдите на вид **Advanced** => **Connections** (Дополнительно => Соединения). Найдите документ соединения в меню **View** (Вид) или с помощью значка программного инструмента, находящегося в правой нижней части панели **Navigator** (Навигатор) адресной книги.
3. Выберите **Add Connection** (Добавление соединения) на панели **Actions** или **Server Connection** (Серверное соединение) в меню **Create**.
4. Заполните поля открывшейся формы, затем сохраните и закройте новый документ соединения.

На практике допускается создание пяти различных документов соединения. Для этого служит поле **Connection type** (Тип соединения), которое является первым полем документа соединения. В данном поле возможны следующие варианты:

- **Local Area Network** (Локальная сеть) - для соединения с сервером по локальной или региональной сети с помощью сетевых протоколов. На практике нет необходимости формировать именно этот документ соединения, поскольку система Notes обычно обнаруживает серверы локальной сети автоматически (путем опроса сначала домашнего сервера, затем локальных серверов имени и, наконец, посредством широковещательной рассылки в локальной сети). Если системе Notes не удастся найти сетевой сервер, она делает вывод о том, что сервер просто не был соответствующим образом настроен. Например, в локальной базе данных DNS или в локальных файлах хостов может отсутствовать правильная запись о сервере. Обычно пользователи создают подобные документы соединения, чтобы заставить систему Notes работать с определенным сетевым протоколом в тех случаях, когда доступны несколько из них;
- **Network Dialup** (Сетевой коммутируемый доступ) - для соединения с сервером по удаленному сетевому подключению. Если не считать прямого коммутируемого соединения Notes, можно рассматривать данное соединение в качестве наиболее распространенного. В случае соединения такого типа система Notes дает указание службе удаленной локальной сети определенной операционной системы (например, Windows или Macintosh) сформировать коммутируемое подключение к нужной удаленной сети, а затем с помощью протокола сети связаться с сервером Domino той же сети; подключение прервется по завершении сеанса связи. Такой тип соединения рекомендуется тем пользователям, которые подключаются к сети Internet через модем и уже в Internet организуют доступ к локальной сети компании, а следовательно - к ее серверам Domino. Следует отметить, что по мере увеличения числа пользователей сети Internet с доступом с домашних или портативных компьютеров этот тип соединения становится все более популярным и востребованным;
- **Notes Direct Dialup** (Прямой коммутируемый доступ Notes) - для формирования соединения с сервером по прямому модемному подключению. Данный выбор

реализуется по умолчанию при создании нового документа соединения (Connection document) и чаще других встречается на практике. Наиболее ценной информацией, содержащейся в этом документе, является номер телефона сервера адресата и порт модема;

- О **Passthru Server** (Сквозной сервер) - для соединения с сервером при помощи другого сервера Domino. Этот тип соединения применяется достаточно редко, как правило в специфических условиях, поскольку задаваемый по умолчанию сквозной сервер (оговаривается в документе местоположения) чаще всего сам принимает решения о способе сквозного подключения. Более подробная информация по вопросу настройки сквозного сервера содержится в следующем разделе настоящей главы;
- О **Hunt Group** (Группа поиска). В больших организациях, применяющих систему Notes, для удовлетворения потребностей многочисленных мобильных пользователей предусматривается сразу несколько сквозных серверов, которые объединяются в так называемые *группы поиска*, что позволяет более равномерно распределять информационную нагрузку. В такой ситуации пользователи могут набирать один и тот же телефонный номер, а любой из серверов группы ответит на направленный вызов и обеспечит соединение с сервером адресата. С началом широкого внедрения Internet как единой широкомасштабной сети организация подобных групп поиска стала неэффективной. Более подробная информация о настройке и подготовке групп поиска приводится в следующих разделах данной главы.

Состав полей в документе соединения зависит от того, какой из вышеуказанных вариантов был выбран для первого поля. Следовательно, в дальнейшем перечень полей придется рассматривать для каждого вида документа соединения. У документов соединения типа Local Area Network и Network Dialup поля практически одни и те же, но в документе Network Dialup присутствует дополнительная вкладка с необходимыми для набора телефонного номера данными. Подробный перечень полей для этих документов представлен в табл. 6.8, однако раздел Network Dialup относится только к документу соединения Network Dialup. Список полей документа соединения типа Notes Direct Dialup включен в табл. 6.9. Поля для сквозного сервера и групп поиска более детально обсуждаются в следующих разделах данной главы.

Таблица 6.8. Перечень полей для документов соединения Local Area Network и Network Dialup, присутствующих в базе данных Personal Address Book

Название поля	Назначение
Вкладка Basics (Основные параметры), раздел Basics	
Connection type (Тип соединения)	В этом поле следует выбирать вариант Local Area Network (Локальная сеть) или Network Dialup (Прямой коммутируемый доступ)
Use LAN port (Использование порта локальной сети)	В поле приводится список всех портов локальной сети, используемых клиентом Notes. Следует указать один или несколько портов локальной сети
Вкладка Basics , раздел Destination (Адресат)	
Server name (Имя сервера)	В этом поле вводится имя сервера Domino, для которого данный документ является документом соединения. Можно задавать имена нескольких серверов (в виде списка)

ДОПОЛНИТЕЛЬНАЯ НАСТРОЙКА КЛИЕНТОВ

Таблица 6.8. Перечень полей для документов соединения *Local Area Network* и *Network Dialup*, присутствующих в базе данных *Personal Address Book* (продолжение)

Название поля	Назначение
Вкладка Network Dialup (Прямой коммутируемый доступ), только для одноименного документа соединения	
Choose a server type (Выбор типа службы)	Здесь возможны следующие варианты: AppleTalk Remote Access , Microsoft Dial-Up Networking и Macintosh PPP
Edit Configuration (Редактирование конфигурации)	Щелчком по этой кнопке открывается диалоговое окно с параметрами службы, установленной в поле Choose service type (Выбор типа службы). Данные необходимы службе удаленного доступа для создания соединения с сервером удаленного доступа. Любая служба предполагает указание имени удаленного соединения, имени входа и пароля, кода страны, кода области и номера телефона. Для службы Microsoft Dial-Up Networking также отображается поле для ввода обратного телефонного номера. В любом случае обязательным является только поле с именем удаленного соединения, поскольку данные в остальных полях дублируют (хотя и могут быть изменены) данные соответствующих полей документа удаленного соединения
Другие поля этой вкладки	Перечень прочих полей, которые могут появляться на этой вкладке, зависит от службы, указанной в поле Choose service type , причем все данные предназначены только для чтения. Для редактирования записей следует щелкнуть по кнопке Edit Configuration (Редактирование конфигурации)
Вкладка Comments (Комментарии)	
Comments (Комментарии)	В этом поле может вводиться любая информация, которая в дальнейшем поможет лучше понять назначение и содержание данного документа. Здесь помещаются специальные сведения, например контактная информация администраторов сервера адресата, которая оказывается весьма полезной в том случае, когда сервер адресата расположен в другом домене компании
Вкладка Advanced (Дополнительно)	
Only from locations (Только для местоположений)	Поле следует использовать при задании местоположений, допустимых для данного документа соединения. По умолчанию в поле вводится звездочка, которая указывает, что данное соединение может применяться для всех местоположений. Чтобы ограничить число местоположений, достаточно указать определенные документы соединения
Only for user (Только для пользователя)	В поле следует перечислить тех пользователей, которые могут применять данное соединение. По умолчанию здесь вводится имя пользователя, который вошел в систему на момент создания документа (в R6 по умолчанию выводится звездочка, что означает «все пользователи»). Когда сразу несколько пользователей вправе пользоваться этой копией клиента <i>Notes</i> , в поле ставится звездочка, указывающая на то, что с соединением может работать любой пользователь
Usage priority (Приоритет использования)	Для данного поля возможны следующие варианты: Normal (Нормальный), который задается по умолчанию, и Low (Низкий). При попытках отыскать наилучший вариант подключения к данному

Таблица 6.8. Перечень полей для документов соединения *Local Area Network* и *Network Dialup*, присутствующих в базе данных *Personal Address Book* (окончание)

Название поля	Назначение
Usage priority	серверу система Notes сначала воспользуется документами соединения с нормальным уровнем приоритета, после чего будет опрашивать домашний сервер и серверы имен локальной сети, затем выполнит широковещательную рассылку в сети для поиска сервера адресата и только потом воспользуется документом соединения с низким уровнем приоритета. Поэтому имеется возможность применения документа соединения с низким приоритетом для создания резервного канала связи с сервером
Destination server address (Адрес сервера адресата)	Заполнение этого поля не является обязательным. Обычно его оставляют пустым, однако оно может быть использовано для задания сетевого адреса сервера адресата. В сетях TCP/IP можно вводить имя хоста или IP-адрес сервера. Если указан IP-адрес, рабочая станция не будет обращаться к серверу имен для определения IP-адреса сервера адресата

Таблица 6.9. Перечень полей для документа соединения *Notes Direct Dialup*, присутствующего в базе данных *Personal Address Book*

Название поля	Назначение
Вкладка Basics (Основные параметры), раздел Basics	
Connection Type (Тип соединения)	В поле укажите вариант Notes Direct Dialup (Прямой коммутируемый доступ Notes)
Always use area code (Всегда использовать код области)	По умолчанию здесь задается вариант No (Нет). Рекомендуется задавать значение Yes (Да), если местная телефонная компания в области размещения сервера адресата требует в обязательном порядке использовать код для местных вызовов
Вкладка Basics , раздел Destination (Адресат)	
Server name (Имя сервера)	В этом поле следует вводить имя сервера Domino, для которого данный документ позволяет сформировать соединение. В нем может указываться несколько серверов (в виде списка или с использованием подстановочных символов)
Country code (Код страны)	Здесь указывают код страны для сервера адресата. Этот код рекомендуется вводить во всех случаях (даже в случае необязательного заполнения поля). При заполнении полей, связанных с кодами страны и области, для документов соединения и местоположения система Notes в дальнейшем сама сможет принять решение о необходимости набора кода страны, кода области и телефонного номера. Если в документе местоположения или документе соединения отсутствует код страны или код области, система Notes будет полагать, что необходимо набирать номер полностью
Area code (Код области)	В этом поле нужно задать код области для сервера адресата (или код города). Рекомендуется вносить код области, причем даже в тех случаях, когда поле заполнять не требуется

Таблица 6.9. Перечень полей для документа соединения *Notes Direct Dialup*, присутствующего в базе данных *Personal Address Book* (продолжение)

Название поля	Назначение
Phone number (Номер телефона)	В поле следует вводить местный телефонный номер для сервера адресата
Comments (Комментарии)	Вкладка Comments (Комментарии) Это поле содержит информацию, которая призвана помочь пользователю или его преемнику при определении назначения данного документа в будущем. Сюда можно также заносить специальные данные, например контактную информацию администраторов серверов адресата. Последнее оказывается весьма полезным, если сервер адресата располагается в другом домене компании Вкладка Advanced (Дополнительно)
Only from Location(s) (Только для местоположений)	Поле рекомендуется использовать при задании местоположений, для которых можно будет применять данное соединение. По умолчанию здесь ставится звездочка, показывающая, что с данным соединением разрешается работать в любом местоположении. Чтобы ограничить (при необходимости) использование данного соединения, достаточно задать конкретные документы местоположения
Only for user (Только для пользователя)	Поле служит для указания тех пользователей, которым предназначено данное соединение. По умолчанию сюда помещается имя пользователя (в R6 — символ «звездочка», обозначающая всех пользователей), вошедшего в систему на момент создания документа. Если с клиентом системы <i>Notes</i> работают несколько пользователей, лучше поставить звездочку, разрешающую применять данное соединение любому пользователю
Usage priority (Приоритет использования)	Для этого поля возможны следующие варианты: Normal (Нормальный), реализующийся в режиме по умолчанию, и Low (Низкий). При попытке формирования соединения для заданного сервера система <i>Notes</i> сначала будет искать документы соединения с уровнем приоритета Normal , затем обращаться к домашнему серверу и серверам имен локальной сети, а далее проводить широковещательную рассылку в локальной сети и только затем искать документы соединения с уровнем приоритета Low . Таким образом, документ соединения с низким уровнем приоритета может использоваться при формировании резервных связей с сервером
Modem port(s) (Порты модемов)	Допускается задавать в этом поле один или больше портов (если они доступны). Если не указан ни один из портов, система <i>Notes</i> будет поочередно обращаться ко всем разрешенным к применению портам COM
Login script filename (Имя файла сценария входа в систему)	Если требуется воспользоваться сценарием соединения при формировании подключения к удаленному серверу, следует ввести в это поле имя файла соответствующего сценария. Обычно сценарий соединения необходим для взаимодействия с сервером службы удаленного доступа (например, CompuServe), когда нужно набирать телефонный номер локального узла сети X.25 такой службы.

Таблица 6.9. Перечень полей для документа соединения *Notes Direct Dialup*, присутствующего в базе данных *Personal Address Book* (окончание)

Название поля	Назначение
Login script filename	По указанной причине требуется имя пользователя и пароль для получения разрешения на доступ к службе. Сценарий соединения позволяет переслать эту и иную информацию на хост-сервер локального узла доступа
Login script arguments (Аргументы сценария входа в систему)	Здесь задаются параметры, которые сценарий может передавать в службу подключения. Обычно требуется указать всего два аргумента: имя пользователя и пароль
Only to servers in domain (Только для серверов домена)	В это поле следует вводить имя домена для сервера адресата. Поле можно не заполнять, а по умолчанию в нем будет задаваться звездочка, что указывает на факт приемлемости имени любого домена. Допустимо ограничить применение данного соединения, чтобы им могли воспользоваться серверы только того домена, имя которого здесь указано

Создание локальной реплики базы данных почтовой службы пользователя

Мобильным пользователям часто требуется для работы локальная копия базы данных почтовой службы. Администратор или пользователь могут быстро сделать такую реплику командой **New Replica** (Новая реплика) в меню **File => Replication** (Файл => Репликация). В этом случае следует помнить, что новой копии надо присвоить имя файла серверной копии и поместить реплику в подпапку почтовой службы. При создании новой реплики имя файла в режиме по умолчанию в диалоговом окне будет тем же самым, что и имя файла копии на сервере, однако она будет расположена в папке данных. Для изменения местоположения рекомендуется добавить к имени файла префикс **mail**.

Например, база данных почтовой службы Джо Доакса, хранящаяся на сервере почтовой службы, может находиться в файле с именем **mail\jdoaks.nsf**. При создании новой локальной реплики система **Notes** решит присвоить этому файлу имя **jdoaks.nsf**, однако необходимо вмешаться и изменить имя на **mail\jdoaks.nsf**, чтобы соответствующая копия базы данных относилась к подпапке почтовой службы (как и для сервера).

Если своевременно не переименовать создаваемую реплику, закладки **Mail**, **Calendar** и **To Do** будут неправильно функционировать при активизации документа местоположения. Кроме того, исчезнут необходимые пункты в меню **Create => Mail** (Создание => Почтовая служба). Для исправления ситуации нужно либо перенести локальную базу данных почтовой службы в подпапку **mail** (внутри папки данных), либо задать в поле **Mail file location** (Местоположение файла почтовых сообщений) каждого документа местоположения вариант **Local** (Локальный) и отредактировать соответствующим образом поле **Mail file** (Файл почтовых сообщений), так чтобы имя файла для копии было имя_файла.пзф, а не таИ\имя_файла.пзф.

Следует отметить, что несоответствие между местоположением локальной базы данных почтовой службы и ее именем в документе местоположения является наиболее типичной ошибкой пользователей при настройке, поэтому очень важно своевременно проверять задаваемые данные.

База данных исходящих почтовых сообщений

Система Notes автоматически создает локальную базу данных исходящих почтовых сообщений, когда пользователь делает текущим документ местоположения; при этом в поле **Mail file location** устанавливается вариант **Local**. Таким образом, базу данных не требуется формировать вручную, достаточно переключиться в режим **Note** (Домашний) или **Travel** (В дороге). В качестве имени файла для базы данных задается имя mailbox, причем оно не появится в списке баз данных, выводимом командой **File => Database => Open** (Файл => База данных => Открытие). Тем не менее всегда можно открыть эту базу путем ввода имени файла в поле **File name** (Имя файла) диалогового окна **Database Open** (Открытие базы данных).

Один из неприятных сюрпризов, который ожидает пользователей, применяющих локальную почтовую службу вместо почтовой службы сервера, состоит в том, что случайное нажатие кнопки **Send** (Пересылка) удаляет сообщение из локальной базы данных исходящих почтовых сообщений. Если эта кнопка нажимается в условиях соединения с сервером, сообщение сразу же отсылается, а не стирается. Даже в том случае, когда пользователю удается открыть базу данных **Outgoing mail** (Исходящие почтовые сообщения) сервера перед тем, как сервер направит сообщение адресату, пользователь просто не имеет права удалять сообщение из базы данных. Некоторые пользователи задают для поля **Mail file location** в документе местоположения офиса вариант **Local** исключительно для того, чтобы воспользоваться указанным преимуществом.

Недостаток этого подхода связан с тем, что приходится периодически щелкать по кнопке **Send** для отправки исходящих почтовых сообщений, в противном случае ни одно из сообщений не покинет компьютер вплоть до момента выхода из клиента системы Notes (когда система Notes напомнит о том, что имеются неотправленные почтовые сообщения). На практике можно, конечно, решить проблему путем периодического (по расписанию) выполнения репликации для документа местоположения.

Настройка сквозного сервера

Вопросы, связанные со сквозными серверами, уже обсуждались в главе 4. Здесь эта проблема рассматривается еще раз, но уже с точки зрения пользователей. С помощью функции **Server Passthru** (Сквозной сервер) системы Notes/Domino система Notes и серверы Domino могут через одни серверы получать доступ к другим. Функция предоставляет, например, целый ряд преимуществ мобильным пользователям системы, поскольку им достаточно набирать телефонный номер только одного сервера и с его помощью взаимодействовать с другими серверами системы (напомним, что раньше мобильному пользователю требовались телефонные номера каждого задействованного сервера). Кроме того, администраторам серверов Domino в этом случае приходится настраивать модемы не всех серверов, а лишь специально выделенных сквозных.

Другое преимущество сквозных серверов связано с тем, они становятся прокси-серверами на уровне приложения. Такой сервер может настраиваться как брандмауэр между локальной сетью (или сетью intranet) и сетью Internet. Любой пользователь сети Internet имеет возможность обратиться к сквозному серверу, однако доступ за брандмауэр открывается только аутентифицированным пользователям системы Notes и серверам Domino.

Учитывая описанные преимущества, многие компании настраивают сквозные серверы, чтобы обеспечить поддержку своим пользователям сети Internet и мобильным пользователям. Сквозные серверы с коммутируемым доступом обычно используют *многопортовые*

интерфейсы последовательного типа, что позволяет одновременно применять несколько (4, 8, 16 или больше) модемов и обслуживать несколько линий телефонной связи.

Компании, обслуживающие многочисленных мобильных пользователей, иногда объединяют сквозные серверы в упоминавшиеся выше группы поиска. В такую группу собирают серверы Domino, совместно эксплуатирующие несколько телефонных линий связи, при этом все пользователи имеют возможность набирать одни и те же телефонные номера, а их обслуживание осуществляется одним из серверов в группе поиска. Пользователь получает доступ к требуемым серверам адресата через сервер группы поиска.

Для настройки функции сквозного сервера необходимо разрешить ее применение пользователям, подготовить соответствующие сквозные серверы и предусмотреть их взаимодействие с серверами адресата. Если одно из звеньев цепи не налажено, сквозной доступ реализовать не удастся. При подготовке необходимо выполнить следующее:

- О пользователям нужно назначить сквозные серверы по умолчанию в своих документах местоположения, в частности в поле **Passthru server** (Сквозной сервер) вкладки **Servers** (Серверы) либо создать специальный документ соединения для сквозного сервера и указать в нем, что для доступа к серверу 1 служит сервер 2. Однако удобнее непосредственно назначить сквозной сервер в документе местоположения;
- О пользователям надо сформировать соединение с назначенным сквозным сервером. Для мобильных пользователей потребуются документ соединения (с прямым коммутируемым доступом Notes или сетевым коммутируемым доступом), в котором задан путь к сквозному серверу;
- О сквозной сервер должен разрешить пользователям взаимодействие с сервером адресата. Документ сервера содержит три поля, записи которых позволяют выполнить данное требование. В разделе **Security => Passthru Use** (Обеспечение безопасности => Использование сквозного сервера) это поля **Route through** (Маршрут через), **Cause calling** (Условия для вызова) и **Destination allowed** (Разрешение на взаимодействие с адресатом);
- О нужный пользователям сервер адресата должен разрешить взаимодействие со сквозным сервером. Поле **Access this server** (Доступ к данному серверу) в документе сервера (Server document) предназначено для внесения необходимой записи. Это поле находится в разделе **Security => Passthru Use** (Обеспечение безопасности => Использование сквозного сервера).

Более подробная информация относительно сквозных серверов приведена в главе 4.

Подготовка доступа к серверам не-Domino

Пользователи системы Notes могут взаимодействовать не только с серверами Domino. В данном случае имеются в виду серверы Web, FTP, Gopher, почтовые серверы и серверы новостей сети Internet, а также серверы каталогов LDAP. После установки в режиме по умолчанию клиент Notes готов для доступа к серверам Web, FTP, Gopher и некоторым серверам LDAP. Для обеспечения доступа к серверам других типов необходимо предусмотреть определенные операции при настройке.

Подготовка доступа к серверам Web, FTP и Gopher

Система Notes предоставляет возможность доступа к серверам Web (HTTP), FTP и Gopher в режиме по умолчанию путем выбора типа браузера, хотя система Notes должна иметь доступ

к порту протоколов TCP/IP (надо, чтобы в сети также были серверы Web, FTP или Gopher, доступные через выбранный порт). Через этот порт можно подключаться к сети с прокси-сервером или, что менее вероятно, получать непосредственный доступ к сети Internet, если применяется порт для коммутируемого доступа к провайдеру услуг сети Internet. По умолчанию система Notes работает с ОЕ-версией обозревателя Internet Explorer, запущенной в окне браузера системы Notes. Можно изменить тип браузера в поле **Internet Browser** (Браузер сети Internet) документа местоположения и выбрать любой другой браузер, в том числе браузер системы Notes, совместимый со стандартами HTML 4.0 и HTTP 1.1.

Для пользователей системы Notes, не имеющих доступа к порту протоколов TCP/IP, подготовка доступа к серверам Web, FTP и Gopher предусматривает выполнение дополнительных операций. Эти пользователи должны располагаться в локальной сети с протоколом SPX или NetBIOS. Для них следует настраивать сервер Domino в качестве сервера InterNotes, выполняющего функции прокси-браузера. В этом случае надо направить адрес URL на сервер InterNotes, который перешлет запрос от своего имени на сервер сети Web и получит запрошенную Web-страницу. Затем сервер запомнит страницу в совместно используемой базе данных Server Web Navigator (файл web.nsf) и перешлет результирующий документ базы данных системы Notes пользователю системы Notes. Из-за достаточно большого числа операций этот вариант оказывается более медленным, чем непосредственное общение, однако позволяет предоставить пользователю всю необходимую информацию.

Чтобы установить сервер InterNotes:

1. Убедитесь в том, что назначенный сервер InterNotes доступен из порта протоколов TCP/IP. Этот порт должен быть портом локальной сети и обеспечивать соединение с сетью Internet или по крайней мере с сетью intranet компании.
2. В выбранном сервере InterNotes запустите задачу InterNotes Web Retriever. Для запуска вручную введите **Load Web** (Загрузка Web) на консоли сервера или укажите **Web Retriever** (Извлечение Web-страниц) в диалоговом окне **Start New Task** (Запуск новой задачи) программы Domino Administrator. Для этого на экране **Server => Status** (Сервер => Статус) следует выполнить **Tools => Start** (Программные инструменты => Запуск). Эта программа будет инициироваться автоматически (каждый раз при запуске сервера), если добавить параметр web в переменную ServerTasks файла notes.ini сервера:

```
servertask=..., web.
```

При первом запуске задачи InterNotes Web Retriever на сервере создается база данных Server Web Navigator (файл web.nsf). Задача InterNotes Web Retriever сохраняет все извлеченные документы HTML в этой базе данных, причем любому пользователю предоставляется возможность обращения к ней.

3. В соответствующих профилях пользователя введите имя сервера InterNotes в поле **InterNotes server** (Сервер InterNotes) и задайте вариант **From InterNotes server** (С сервера InterNotes) для поля **Retrieve/open pages** (Извлечение/открытие страниц) вкладки **Basics** (Основные параметры).
4. В документах местоположения пользователей укажите имя сервера InterNotes в поле **InterNotes server** вкладки **Servers** (Серверы) и **Notes** (Система Notes) в поле **Internet Browser** (Браузер сети Internet) и **From InterNotes server** в поле **Retrieve/open pages** (Извлечение/открытие страниц) вкладки **Internet Browser** (Браузер сети Internet).

5. Проинформируйте заинтересованных пользователей о возможности доступа к сети Web (или по крайней мере к Web-серверам компании) с помощью системы Notes и укажите им на целесообразность обращения к базе данных Server Web Navigator, хранящейся на сервере InterNotes.

Конечно, задача InterNotes Web Retriever на сервере Domino не является для пользователей столь же заманчивой, как собственный браузер. Однако для тех, у кого нет другого доступа к сети World Wide Web, это решение представляется вполне удовлетворительным. На практике даже при наличии своего браузера серверный Web-браузер может оказаться достаточно привлекательным, поскольку применяется совместно. В результате он обеспечивает хранение запрошенных страниц в совместно используемой базе данных системы Notes, обладающей целым рядом ценных свойств, в частности функцией **Web Tour** (Просмотр сети Web) и **Web page rating** (Рейтинг Web-страниц). Кроме того, пользователи могут делиться опытом работы с серверным браузером. Для получения более подробных сведений о задаче InterNotes Web Retriever и усовершенствованных функциях базы данных Server Web Navigator обратитесь к главе 13.

Другие серверы сети Internet

Клиент Notes может выступать в качестве клиента по отношению к другим серверам сети Internet, в том числе к серверам почтовых служб POP и IMAP, хостам SMTP, серверам новостей NNTP и серверам каталогов LDAP. За исключением нескольких учетных записей LDAP, которые система Notes формирует автоматически, все учетные документы в соответствующей базе данных Personal Address Book приходится создавать вручную еще до того, как система Notes сможет нормально взаимодействовать с серверами POP, IMAP, SMTP, NNTP или LDAP.

Кроме того, для обеспечения нормального взаимодействия с серверами почтовой службы POP приходится создавать специальный документ местоположения, а возможно - и специальный документ соединения. Нужно выделять для этих целей специальную локальную базу данных почтовой службы (допустим, базу данных почтовой службы системы Notes или иную почтовую базу), в которой следует запоминать почтовые сообщения службы POP.

Чтобы правильно взаимодействовать с серверами почтовой службы IMAP, необходимо также иметь специальный документ местоположения и, может быть, специальный документ соединения. Система Notes создаст прокси-базу данных, которую затем можно будет преобразовать в базу данных для репликации учетных записей IMAP, хранящихся на сервере ШАР.

Создание учетных документов

Учетные документы создаются или в Мастере Lotus Notes Client Configuration Wizard при настройке рабочей станции системы Notes, или вручную для уже существующей рабочей станции. В любом случае требуется вводить информацию, нужную системе Notes для взаимодействия с внешним сервером. В начале процедуры создания учетной записи необходимы следующие данные:

- О номер телефона для связи с провайдером услуг сети Internet;
- О имя домена сети Internet для провайдера услуг сети Internet (например, isp.com);

- О полное различающееся имя домена для того сервера сети Internet, на котором предполагается создать учетную запись (например, mail.isp.com);
- О имя пользователя, присвоенное провайдером услуг сети Internet;
- О пароль, выданный провайдером услуг сети Internet.

Для создания учетных документов в процессе настройки рабочей станции системы Notes достаточно дать ответ **Yes** (Да) на вопросы, которые выводятся в соответствующем диалоговом окне. Можно формировать любые типы учетных записей сети Internet. В процессе создания (при необходимости) учетных документов для почтовых служб POP и ШАР система Notes будет одновременно формировать и другие объекты, нужные при использовании этих учетных записей, в том числе документы местоположения и базы данных.

Чтобы создать документ учетной записи (Account document) для уже существующей рабочей станции системы Notes, откройте вид **Advanced => Accounts** (Дополнительно => Учетные записи) базы данных Personal Address Book пользователя и выберите команду **Account** (Учетная запись) в меню **Create** (Создание) или кнопку **Add Account** (Добавление учетной записи) на панели инструментов. Появится форма **Account** (Учетная запись), которая в зависимости от типа создаваемой учетной записи будет содержать две или три вкладки. Однако для учетной записи любого типа в этой форме придется заполнять поля, включенные в табл. 6.10.

Таблица 6.10. Поля документа учетной записи

Название поля	Назначение
Вкладка Basics (Основные параметры)	
Account name (Имя учетной записи)	В поле можно вводить любое информативное имя. Учетная запись на виде Accounts (Учетные записи) будет выведена с выбранным именем
Account server name (Имя сервера учетных записей)	Здесь следует указать полное различающееся имя домена (например, mail.isp.com) или IP-адрес сервера учетных записей
Login name (Имя входа)	В данном поле нужно вводить имя входа для каждой учетной записи, требующей использования подобного имени
Password (Пароль)	В поле задают пароль для учетных записей, которые требуют использования пароля
Protocol (Протокол)	В этом поле определяется протокол, для которого создается учетная запись. Доступны IMAP Offline, IMAP Online, LDAP, NNTP^OP и SMTP
SSL (Уровень SSL)	В данном поле следует задавать вариант Enabled (Разрешено), если того требует сервер. Если сервер не считает использование SSL обязательным, этот вариант выбирают только в том случае, если необходимо обеспечить безопасное соединение сервера. Если сервер не поддерживает протокол SSL, такой вариант использовать не рекомендуется (см. описание уровня защищенного сокетa SSL в главе 20)
Only from locations (Только для местоположений)	По умолчанию здесь вводится звездочка, которая указывает, что учетной записью можно воспользоваться из любого места. Если необходимо ограничить доступ к учетной записи лишь несколькими местоположениями, достаточно вместо звездочки ввести документы

Таблица 6.10. Поля документа учетной записи (окончание)

Название поля	Назначение
Only from locations	местоположения. При создании учетной записи почтовой службы, когда документ местоположения еще не сформирован и необходимо поставить ему в соответствие документ местоположения, следует сделать паузу, сформировать и сохранить учетную запись местоположения, а затем, когда все данные будут готовы, вернуться к этому документу и завершить его создание Вкладка Advanced (Дополнительно)
Port number: (Номер порта)	В поле по умолчанию вводится номер общеизвестного порта (для каждого протокола), причем данный номер не рекомендуется изменять, если только в этом нет насущной необходимости (например, при наличии указания от администратора сервера учетных записей) Вкладка Advanced, когда на вкладке Basics (Основные параметры) разрешено использование уровня SSL
Accept SSL site certificates (Прием сертификатов от сайтов SSL)	В этом поле следует выбирать вариант Yes (Да) для приема сертификатов от неизвестных авторизаторов. При выборе варианта No (Нет) подобные сертификаты приниматься не будут, и появляется возможность принять или отклонить подобный сертификат при его поступлении
Accept expired SSL certificate (Прием просроченных сертификатов SSL)	Здесь указывают вариант Yes для приема просроченных сертификатов от сайтов. При выборе варианта No подобные сертификаты приниматься не будут, потому появляется возможность принимать или отклонять сертификаты при их поступлении
Send SSL certificates when asked (outbound connection only) (Отправка сертификатов SSL по запросу, только для случая исходящих соединений)	В поле нужно задать вариант Yes, что позволяет автоматически пересылать сертификаты на сервер, затребовавший их. При выборе варианта No в подобном запросе серверу будет отказано
Verify account server name with remote server's certificate (Проверка имени сервера учетных записей по сертификату удаленного сервера)	При задании для этого поля варианта Enabled (Разрешено) система Notes будет сравнивать имя сертификата сервера с именем в поле Account server name (Имя сервера учетных записей) вкладки Basics
SSL protocol version (Версия протокола SSL)	По умолчанию здесь задается вариант Negotiated (Согласование), что предусматривает использование системой Notes любой версии (с 2.0 по 3.0) протокола SSL после согласования с сервером. Можно также указать конкретную версию протокола. На практике рекомендуется пользоваться вариантом по умолчанию, если только не требуется (например, во время диагностики) явно назвать 'Определенную версию протокола SSL

Другие поля, которые заполняются для конкретных типов учетных документов, рассмотрены ниже.

Создание учетных записей почтовой службы POP

На ранних этапах развития почтовой службы сети Internet (электронная почта) хосты были постоянно подключены к сети и почтовые сообщения мгновенно доставлялись всем пользователям, имеющим соответствующие учетные записи. При появлении небольших компьютеров, которые нельзя оставлять включенными 24 часа 7 дней в неделю, возникла необходимость иметь сервер, предназначенный для приема почтовых сообщений и их хранения до момента, пока пользователь не включит собственный компьютер и не извлечет свои сообщения. Протокол почтового офиса (Post Office Protocol - POP) специально создавался для этих целей. В настоящее время версия 3 данного протокола (POP3) предусматривает наличие сервера почтовой службы, обеспечивающего хранение почтовых сообщений пользователей до тех пор, пока они не будут востребованы. После того как клиент почтовой службы POP выберет свое почтовое сообщение, оно будет загружено в файлы этого клиента. В режиме по умолчанию почтовый клиент стирает копии сообщений на сервере сразу после их загрузки, однако данный режим можно отменить. После загрузки клиент почтовой службы POP обрабатывает сообщения самостоятельно.

Система Notes, выполняющая функции клиента почтовой службы POP, загружает сообщения в стандартную базу данных системы Notes, подготовленную с помощью шаблона почтовой службы системы Notes. Пользователь вправе применять собственную базу данных почтовой службы системы Notes (база данных, в которой запоминаются почтовые сообщения, принимаемые от пользователей системы Notes) или сформировать специальную базу данных почтовой службы для почтовых сообщений на одну или несколько учетных записей POP.

При создании учетной записи почтовой службы POP следует сформировать документ учетной записи (Account document) и документ местоположения (Location document) в базе данных Personal Address Book. Если не предполагается пользоваться документом местоположения сети Internet в других целях, можно именно с его помощью сформировать учетную запись и не делать нового документа. Для загружаемых сообщений также необходимо выделить базу данных системы. Чтобы связываться с сетью Internet через модем, требуется документ соединения с прямым коммутируемым доступом (Network Dialup), соответствующий уже существующему документу местоположения. Если подобного документа еще нет, следует обратиться к Мастеру Connection Configuration Wizard. Пользователь может запустить Мастер из панели **Action Bar** (Панель операций) открытого документа местоположения.

Процесс создания документов местоположения и учетных записей подробно описан в начале данной главы. Ниже рассмотрены лишь некоторые нюансы, специфичные для почтовой службы POP.

Документ учетной записи почтовой службы POP имеет только одно специальное поле - табл. 6.11.

Таблица 6.11. Поле документа почтовой службы POP

Поле	Назначение

Вкладка **Protocol Configuration** (Конфигурация протокола)

Leave mail on server
(Сохранение почтовых сообщений на сервере)

, Положительный ответ означает, что при загрузке почтовых сообщений с сервера почтовой службы POP эти сообщения стираться не будут, а отрицательный ответ — что они будут удалены. Обычно по умолчанию задается вариант **Yes**, но для многих серверов почтовой службы POP, отличных от сервера Domino, выбирается вариант No

Специальные поля документа местоположения, предназначенного для создания учетной записи почтовой службы POP, приведены в табл. 6.12.

Таблица 6.12. Поля документа местоположения для учетной записи в почтовой службе POP

Название поля	Назначение
Вкладка Basics (Основные параметры)	
Location Type (тип местоположения)	В этом поле следует задавать вариант Local Area Network (Локальная сеть), если предусматривается постоянное соединение для связи с провайдером услуг Internet. Если связь с провайдером обеспечивается с помощью модема, укажите вариант Network Dialup (Сетевой коммутируемый доступ). Если предусматривается использование соединений различного типа, удобен вариант Custom (Пользовательский)
Location name (Название местоположения)	В поле нужно вводить имя, указывающее на конкретного провайдера услуг Internet и используемый протокол (например, Eagle POP Mail)
Internet mail address (Адрес почтовой службы сети Internet)	В данном поле указывают обратный адрес сети Internet для конкретного провайдера (например, RobK@isp.com). Этот адрес может использоваться для получения корреспонденции
На вкладке Servers (Серверы)	Не следует вводить имя сервера почтовой службы провайдера, но можно задать имена собственных серверов Domino
Вкладка Mail (Почтовая служба)	
Mail file location (Местоположение файла почтовых сообщений)	Здесь выбирают вариант On Server (На сервере), если файл почтовых сообщений, использующийся для приема почтовых сообщений сети Internet, установлен на сервере Domino (например, применяется база данных почтовой службы системы Notes). Этот вариант следует задавать только в том случае, если сервер почтовой службы доступен по локальной сети. Выбирайте вариант Local (Локально), когда файл почтовых сообщений, необходимый для приема почтовых сообщений сети Internet, находится на рабочей станции
Mail file (Файл почтовых сообщений)	Здесь указывается частичный путь из имени базы данных, которая будет получать почтовые сообщения от сервера POP (например, mail\EagleMail.nsf)
Internet domain for Notes addresses when connecting directly to the Internet (Домен сети Internet в системе Notes для адресации при прямом подключении к Internet)	В это поле следует вводить имя домена провайдера услуг сети Internet (например, isp.com)
Send outgoing mail (Отправка исходящих почтовых сообщений)	Если планируется использовать учетную запись SMTP на сервере SMTP провайдера, в данном поле задают вариант Directly to Internet (Непосредственно в сеть Internet). Для передачи исходящих сообщений на сервер почтовой службы Domino следует выбирать вариант Through Domino Server (Через сервер Domino)
На вкладке Replication (Репликация)	Можно указать расписание репликации, согласно которому система Notes будет принимать и доставлять почту сети Internet

После назначения существующей базы данных (например, базы данных почтовой службы, хранящейся на сервере почтовой службы, или уже имеющейся локальной реплики этой базы данных) и указания ее имени в поле **Mail file** (Файл почтовых сообщений) в документе местоположения процесс создания учетной записи почтовой службы можно считать завершенным.

Если выбрана, но еще не создана локальная реплика базы данных почтовой службы, придется сформировать ее теперь (см. выше в данной главе).

Если назначается база данных, которая вообще не формировалась (например, база данных, отличная от базы почтовой службы), следует создать ее, выполнив в меню **File** (Файл) команду **Database => New** (База данных =Ф Новая), при этом появится диалоговое окно **New Database** (Новая база данных), поля которого надо заполнить с учетом рекомендаций, представленных в табл. 6.13.

Таблица 6.13. Поля диалогового окна **New Database**

Поле	Назначение
Server (Сервер)	В поле следует выбрать вариант Local (Локально), если в поле Mail file location (Местоположение файла почтовых сообщений) документа местоположения выбран тот же вариант. Укажите сервер почтовой службы, сервер, назначенный в поле Home/Mail server (Домашний/почтовый сервер) документа местоположения, если в поле Mail file location документа местоположения ранее был задан вариант On server (На сервере). Для выбора сервера необходимо право создания новых баз данных на этом сервере, иначе процедура завершится отказом
Title (Заголовок)	Здесь вводится описательный заголовок базы данных (длиной не более 32 символов)
File Name (Имя файла)	В данном поле указывается путь к новой базе данных (например, mail\EagleMail.nsf)
Template Server (Сервер шаблона)	Для этого поля следует выбрать вариант Local , если подобный вариант был ранее задан в поле Mail file location документа местоположения. В противном случае укажите имя того сервера, который ранее был в поле Server (Сервер). Для любого из названных вариантов в списке под кнопкой Template Server (Сервер шаблона) следует выбрать Mail (R5.0) или Mail (R6.0) в зависимости от версии клиента Notes
Advanced (Дополнительно)	Поле может не заполняться, а при его заполнении рекомендуется вариант Allow soft deletions (Разрешение мягкого удаления)

Щелкните по кнопке **OK**, и система Notes сформирует требуемую базу данных. После этого можно считать, что учетная запись почтовой службы POP успешно создана. Далее рекомендуется переключиться на документ местоположения почтовой службы POP и работать с ним. Однако прежде может потребоваться сформировать учетную запись SMTP (см. следующий раздел).

Создание учетных записей почтовой службы SMTP

Если при создании документа местоположения почтовой службы POP в поле **Send outgoing mail** (Отправка исходящих почтовых сообщений) указан вариант **Domino Server** (Сервер

Domino), учетную запись почтовой службы SMTP формировать не требуется. Но если в этом поле задано прямое подключение к сети Internet, придется делать учетную запись почтовой службы SMTP, которая используется совместно с учетной записью почтовой службы POP.

При этом будет обеспечиваться прием почтовых сообщений с помощью сервера почтовой службы POP, а также передача исходящих почтовых сообщений с помощью сервера почтовой службы SMTP. Как правило, каждый провайдер сети Internet, предлагающий услуги почтовой службы POP, предоставляет и сервер SMTP. Имя сервера может быть smtp.isp.com или mail.isp.com, однако всегда следует уточнить (вместе с провайдером услуг сети Internet) имя сервера SMTP (или проверить по ping имена хостов, чтобы найти нужный).

Для создания учетной записи почтовой службы SMTP нужно создать документ учетной записи SMTP (SMTP account document) в базе данных Personal Address Book. К этому документу не предъявляются специальных требований, следует лишь указать значение SMTP в поле **Protocol** (Протокол) и выбрать вариант **POP mail location** (Местоположение почтовой службы POP) в поле **Only from location(s)** (Только для местоположений). Нет необходимости создавать специальный документ местоположения, поскольку учетная запись может пользоваться тем документом местоположения, который был составлен ранее для учетной записи POP.

При первой пересылке почтового сообщения с помощью документа местоположения почтовой службы POP система Notes создаст базу данных для хранения исходящих почтовых сообщений SMTP (если это не было сделано ранее) и запишет в нее исходящее сообщение. База данных получила название Outgoing Mail (Исходящие почтовые сообщения), а файл - smtp.box. Такое имя представляется несколько странным, поскольку база данных для исходящих почтовых сообщений системы Notes также называется Outgoing Mail (однако соответствует файлу mail.box). Правда, большей части пользователей весьма редко случается обращаться к этим базам. Если все же такая необходимость появляется, но не вполне понятно, с которой из баз данных приходится иметь дело, выполните **File => Database => Properties** (Файл => База данных => Свойства) - на вкладке **Database Basics** (Основные параметры базы данных) будет выведено имя соответствующего файла. В окне **Database Basics** можно изменить имя базы данных. Для этого следует назвать файл smtp.box именем Outgoing SMTP Mail (Исходящие почтовые сообщения SMTP), а файлу mail.box присвоить имя Outgoing Notes Mail (Исходящие почтовые сообщения системы Notes). Если ранее подобные базы данных уже добавлялись в папку закладок, может также потребоваться переименовать соответствующие закладки. В таком случае достаточно щелкнуть по кнопке соответствующей закладки и задать **Rename** (Переименование).

Создание учетных записей почтовой службы IMAP

Существенный недостаток почтовой службы POP состоит в необходимости загружать почтовые сообщения, чтобы их прочесть и сформировать ответ. У пользователей системы Notes, предусматривающих хранение почтовых сообщений на серверах почтовой службы, такой проблемы нет. Однако большинство пользователей сети Internet могут получить доступ к своим почтовым сообщениям только с помощью одного компьютера. Почтовая служба IMAP была специально создана с целью устранения этого недостатка.

Почтовая служба IMAP организуется на базе сервера IMAP подобно тому, как система Notes строится на базе сервера Domino. Клиент Notes является также клиентом почтовой службы IMAP, причем располагает средствами чтения, способными работать с почтовыми

сообщениями в интерактивном режиме (on-line), пребывать в отключенном состоянии или действовать в автономном режиме (off-line). В системе Notes два последних состояния принято называть *автономным режимом off-line* (см. подробное описание почтовой службы IMAP в главе 17).

В интерактивном режиме пользователи загружают *заголовки почтовых сообщений* в свои клиентские почтовые программы. После анализа заголовков можно загружать отдельные сообщения по специальному запросу. Ответ пользователя на почтовое сообщение передается на сервер IMAP, который в дальнейшем пересылает его адресату. По завершении процедуры считывания и формирования ответных сообщений все сообщения остаются на сервере ШАР. Если пользователь желает организовать папку почтовых сообщений, сервер ШАР обеспечит ее поддержку. При переходе в режим отключения пользователи почтовой службы ШАР могут загружать группы сообщений в свои клиентские программы, отключиться от сервера и продолжать обрабатывать сообщения в автономном режиме, а затем восстановить соединение и перезагрузить на сервер внесенные изменения. На заключительном этапе (в автономном режиме) пользователи имеют возможность (при необходимости) передать сообщения на сервер, после чего удалить исходные сообщения на сервере, сохранив только локальные копии (именно так действуют клиенты почтовой службы POP).

Во время установки пользователю системы Notes учетной записи службы ШАР для интерактивного режима система создает прокси-базу данных, предназначенную для хранения заголовков и загрузки тела сообщений. Тем не менее эта база данных будет служить только для временного хранения информации, поскольку система Notes удаляет сообщения по завершении сеанса связи с сервером ШАР.

В интерактивном режиме связи с сервером IMAP система Notes разрешает загружать сообщения одним из следующих двух способов. Во-первых, допускается загружать сообщения в базу данных почтовой службы системы Notes. Все сообщения, полученные подобным образом, попадают в почтовый ящик Inbox (Входящие). Если сообщения находились в папках сервера ШАР, будут потеряны взаимосвязи с копиями в базе данных почтовой службы системы Notes. В этом случае реализуется типичный интерактивный режим сервера IMAP. Преимуществом подобного подхода является то, что все поступающие почтовые сообщения оказываются в одном почтовом ящике (специалисты компании Lotus называют такой почтовый ящик универсальным).

Во-вторых, допустимо реплицировать учетную запись ШАР в базу данных системы Notes. Все загружаемые сообщения останутся в той же самой папке, в которой они хранились на сервере ШАР. Взаимосвязь между папками сервера может быть изменена в любом месте, но система Notes все равно согласует данные во время репликации. Это типичный режим отключения от сервера ШАР. Здесь недостаток заключается в том, что требуется поддерживать сразу несколько почтовых ящиков: один для почтовых сообщений системы Notes, а другие - для почтовых сообщений службы ШАР.

Чтобы сделать учетную запись ШАР, приходится создавать документ местоположения (Location document) и документ учетной записи (Account document). При этом система Notes сформирует прокси-базу данных сразу после сохранения документа учетной записи. Если документ местоположения сети Internet не предназначен для каких-либо иных целей, можно с его помощью создавать новый документ.

В процессе формирования документа учетной записи следует придерживаться рекомендаций, представленных выше. В поле **Protocol** (Протокол) документа учетной записи лучше задавать вариант **IMAP Offline** (Автономный режим ШАР) или **IMAP Online**

(Интерактивный режим IMAP). При выборе варианта **IMAP Offline** не появится никаких дополнительных полей, а если задать вариант **IMAP Online**, то откроется вкладка **Protocol Configuration** (Конфигурирование протокола), где надо указать значения в полях **Sent folder name** (Имя папки отправленных сообщений) и **Drafts folder name** (Имя папки черновиков). По умолчанию здесь устанавливаются варианты **Sent** и **Drafts** соответственно.

Если папки отправленных сообщений и черновиков уже созданы на сервере ШАР, убедитесь в том, что варианты в рассматриваемых полях документа учетной записи определены в соответствии с названиями этих папок на сервере ШАР. Если же папок на сервере ШАР еще нет, заполнять поля не рекомендуется, поскольку система Notes сама создаст папки для сервера ШАР (с именами **Sent** и **Drafts** или другими, указанными ранее).

При создании документа местоположения воспользуйтесь рекомендациями для почтовой службы POP (см. выше). При модемном подключении к сети Internet потребуется документ соединения с прямым коммутируемым доступом (Network Dialup), который будет применяться только совместно с создаваемым документом местоположения. Если такого документа не существует, сформируйте его с помощью Мастера Connection Configuration Wizard. Запустить Мастер можно с панели **Action** (Операция) открытого документа местоположения.

Когда будет готова учетная запись ШАР (для интерактивного или автономного режимов), можно начать ее обработку. Для этого перейдите в соответствующий документ местоположения и выполните одну из трех операций:

- О щелкните по значку **Mail** (Почтовая служба) на панели **Bookmark** (Закладка);
- О выберите **Open Proxy** (Открытие прокси) в меню **Actions** (Операции) или в окне **Action** (Операция), когда документ учетной записи почтовой службы ШАР открыт в режиме чтения;
- О вызовите прокси-базу данных. Ее имя - accountname (IMAP), где accountname соответствует названию, заданному в поле **Account name** (Имя учетной записи) документа учетной записи почтовой службы ШАР.

Для автономной учетной записи IMAP в выбранном местоположении, где эта запись доступна, на странице **Replicator** (Репликатор) надо заполнить два новых поля: **Receive Internet mail** (Прием почтовых сообщений сети Internet) и **Send outgoing Internet mail** (Отправка исходящих почтовых сообщений сети Internet). Щелчок по кнопке **Start** (Запуск) или **Send & Receive Mail** (Пересылка и прием почтовых сообщений) на странице **Replicator** предписывает системе Notes извлечь новые сообщения для учетной записи ШАР и занести их копии в ящик почтовой службы системы Notes. Одновременно система будет направлять все отложенные сообщения на сервер ШАР.

Если вместо занесения почтовых сообщений ШАР в почтовый ящик системы Notes надо создать локальную реплику учетной записи ШАР, это можно организовать с помощью следующих операций:

1. Откройте прокси-базу данных ШАР.
2. Выберите **File => Replication => New Replica** (Файл => Репликация => Новая реплика), при этом прокси-база данных ШАР станет репликой базы данных ШАР.
3. На странице **Replicator** укажите **Start** для извлечения в реплику базы данных информации из учетной записи IMAP. На более позднем этапе, после изменений в реплике, модифицированные данные будут «вытолкнуты» на сервер ШАР (в дополнение к «вытягиванию» в реплику изменений с сервера ШАР).

Создание учетных записей новостей сети Internet

Группы новостей Usenet представляют собой дискуссионные форумы сети Internet. Серверы новостей Internet обслуживают группы новостей, причем в Internet установлено большое число таких серверов. Обычно пользователь в состоянии отслеживать новости и приносить в них свои записи без регистрации, однако все зависит от конкретного сервера новостей. Большая часть этих серверов поддерживается провайдерами для собственных пользователей, поэтому доступ к ним ограничен. Кроме того, серверы новостей могут хранить реплицируемые копии других групп новостей, так что далеко не каждый пользователь может обратиться к серверу новостей и принять участие в обсуждении.

Обсуждения новостей (по группам) обычно ограничиваются теми вопросами, для которых была создана та или иная группа. Имена групп задаются в соответствии с принятой иерархической схемой присвоения имен, что позволяет легко классифицировать и идентифицировать рассматриваемые темы. Так, например, группу новостей, которая планирует заниматься проблемами, связанными с администрированием системы Lotus Notes, логично назвать comp.groupware.lotus-notes.admin.

Пользователи применяют программы чтения новостей для связи с сервером новостей. Обычно пользователь сначала знакомится со всеми темами, предлагаемыми на сервере. Если в соответствии с именем группа новостей представляет потенциальный интерес или может быть полезной, пользователь становится ее абонентом. После этого он получает возможность читать материалы и публиковать статьи (дискуссионные документы) в выбранных группах. Серверы новостей и программы чтения новостей взаимодействуют по протоколу NNTP (Network News Transport Protocol - сетевой протокол передачи новостей).

Естественно, клиент Notes сам может обеспечивать чтение новостей. Для этого достаточно подготовить документ учетной записи NNTP (NNTP account document), что не требует создания дополнительного документа местоположения. Тем не менее при формировании документа учетной записи NNTP может понадобиться ограничить его распространение объектами, имеющими доступ к сети Internet.

В процессе создания документа учетной записи NNTP поля **Login name** (Имя входа) и **Password** (Пароль) заполнять не следует, за исключением тех случаев, когда приходится регистрироваться на сервере новостей. В качестве протокола назначается протокол NNTP, при этом появляется поле **Use Replication history when replication will appear** (Использование журнала репликации при повторении операции), в котором надо сохранить вариант **Yes** (Да), тем самым предписав системе Notes не загружать заголовки сообщений, которые уже загружались ранее. Последнее позволяет заметно ускорить обращение к серверу новостей.

При сохранении документа учетной записи NNTP система Notes создаст учетную запись прокси с именем accountname (NNTP), где компонент accountname отвечает имени, введенному в поле **Account name** (Имя учетной записи) документа учетной записи. Эта запись обеспечивает временное запоминание загруженных аннотаций статей и самих статей, однако стирает их сразу после закрытия базы данных.

Для доступа к серверу новостей откройте прокси-базу данных, чтобы система Notes сформировала соединение с сервером новостей. Щелкните по кнопке **Newsgroups** (Группы новостей) для загрузки перечня групп новостей с сервера. Затем подпишитесь на загружаемые группы новостей, чтобы получать из них аннотации публикуемых статей. Просмотрев этот список, загрузите, если хотите, текст статьи или ответьте на нее собственной публикацией.

Вместо запоминания аннотаций и статей только на время интерактивного режима можно сформировать локальную базу данных, которая обеспечит хранение копий, загруженных из соответствующих групп новостей. При этом появится возможность читать и отвечать на статьи в автономном режиме. На более позднем этапе, в процессе выполнения процедуры репликации, сформированные ответы будут переданы на сервер новостей, а новые записи, сделанные другими пользователями, поступят в локальную базу данных.

Для создания реплики учетной записи новостей:

1. Откройте прокси-базу данных NNTP.
2. Подпишитесь на группы новостей, которые планируется реплицировать.
3. Выполните **File => Replication => News Replica** (Файл => Репликация => Новая реплика) - прокси-база данных станет репликой исходной базы данных.
4. Щелкните по кнопке **Start** на странице **Replicator**, чтобы занести в новую базу данных статьи из группы новостей.

Создание учетных записей каталогов LDAP

Каталог LDAP представляет собой каталог протокола LDAP (Lightweight Directory Access Protocol - облегченный протокол доступа к каталогу) и состоит из списка объектов. Хотя в общем случае объекты могут быть совершенно произвольными, на практике в каталоги LDAP включены объекты, соответствующие каталогам сотрудников, поэтому они помогают при поиске данных сотрудников, например адресов электронной почты. Следует отметить, что каталоги LDAP во многом напоминают базу данных Domino Directory (которая совместима с каталогами LDAP) и базу данных Personal Address Book, содержащую информацию о пользователях системы Notes.

В предшествующих разделах уже приводилась достаточно подробная информация относительно протокола LDAP. Он является подмножеством протокола DAP (Directory Access Protocol - протокол доступа к каталогу), который известен также под названием протокола каталога X.500. Причина, по которой уже пришлось обсуждать этот протокол, состоит в том, что база данных Domino Directory и схема присвоения имен создавались на основе стандарта X.500 и потому совместимы с протоколом LDAP. Следует отметить, что иерархическая схема присвоения имен системы Notes, в рамках которой пользователям даются имена типа CN=Osprey/OUI=Servers/O=Stillwater/C=US, возникла в результате совместного применения стандарта X.500 и каталога LDAP. Сотрудники в других каталогах LDAP получают точно такие же имена.

Совместимость с протоколом LDAP дает возможность любому клиенту, использующему протокол LDAP (например, клиенту системы Lotus Notes), производить поиск данных в любом совместимом с протоколом LDAP каталоге. Таким образом, любой пользователь, применяющий клиент LDAP, теоретически может искать имена в базе данных Domino Directory (если подобные операции ему изначально разрешены), а посредством клиентов системы Notes - информацию о сотрудниках в каталогах LDAP.

В наши дни в сети Internet существует множество общедоступных каталогов LDAP, причем любому пользователю разрешается вводить свои данные в их списки. Учетные документы для большей части этих хорошо известных и общедоступных каталогов заносятся в базу данных Personal Address Book пользователя системы Notes еще в момент ее создания, поэтому все, что остается пользователям, - это эффективно обрабатывать такую информацию.

В дополнение можно создать учетные документы для любого другого каталога LDAP, выбрав в качестве сетевого протокол LDAP. В таком случае нет необходимости вводить имя входа (регистрации) или пароль, если только не требуется зарегистрироваться в системе. Учетные документы LDAP имеют целый ряд дополнительных полей на вкладке **Protocol Configuration** (Конфигурирование протокола) - табл. 6.14.

Таблица 6.14. Дополнительные поля на вкладке **Protocol Configuration** для документа учетной записи ШАР

Поле	Назначение
Searchtimeout (Тайм-аут поиска)	В этом поле следует задавать величину временного интервала (в секундах), в течение которого система Notes будет ожидать возвращения сервером LDAP тех результатов поиска, которые были затребованы. По умолчанию указано число 60
Maximum entries to return (Максимальное число возвращаемых записей)	В данном поле должно определяться максимальное число записей каталога, которое должно возвращаться по результатам поиска. В режиме по умолчанию вводится число 100
Search base (База поиска)	Если оставить это поле незаполненным, поиск будет проводиться в рамках всего каталога. Имеется также возможность ограничить круг поиска отдельными разделами каталога, которые следует указать здесь. Например, при вводе символов c=us удастся ограничить поиск записями, которые относятся к США
Check names when sending mail (Проверка имен при пересылке почтовых сообщений)	По умолчанию в этом поле задается вариант No (Нет). При изменении на Yes (Да) система Notes будет просматривать имена адресатов в каталоге (в дополнение к базе данных Personal Address Book, базе данных Domain Directory и другим каталогам, которые обычно участвуют в процедуре поиска имен)

Чтобы на основе созданного документа учетной записи LDAP провести поиск в каталоге:

1. Щелкните по кнопке со стрелкой и изображением увеличительной линзы справа от значка **Search** (Поиск) или нажмите комбинацию клавиш **Alt+Shift+S**. В результате появится меню с параметрами поиска.
2. Выполните **Find People** (Поиск сотрудников), при этом откроется диалоговое окно **Directories** (Каталоги).
3. Выберите требуемый каталог. Следует помнить о том, что среди доступных каталогов находится база данных Personal Address Book и другие местные книги адресов, а также все каталоги LDAP, для которых ранее были созданы учетные документы и которые достижимы из данного местоположения.
4. Введите параметры поиска, например имена или адреса. Можно также выполнить команду **Detailed Search** (Подробный поиск) для поиска по заданным условиям (путем ввода параметров поиска в соответствующих полях).

Настройка рабочей станции для совместного использования

Некоторые пользователи системы Notes не сидят перед компьютером в течение всего рабочего дня, а иногда вообще не имеют собственного компьютера. Как правило, они делят

компьютер с одним или несколькими другими пользователями и садятся за клавиатуру только для выполнения определенных действий, например для приема сообщения электронной почты или обновления используемых баз данных. На практике существует несколько способов настройки рабочей станции системы Notes для ее совместного применения несколькими пользователями:

- О установка на компьютере нескольких копий клиентов Notes (по одной для каждого пользователя). К достоинствам такого подхода относится простота настройки, когда каждому пользователю присваиваются индивидуальные идентификационные данные, а его недостатки связаны с тем, что требуется большой объем памяти на жестком диске;
- О установка одной копии клиента Notes и организация нескольких наборов папок данных (по одному набору в расчете на одного пользователя). Положительной стороной этого способа (по сравнению с предыдущим) является некоторое уменьшение занятого объема памяти жесткого диска при сохранении идентификационных данных для каждого пользователя (хотя необходимый объем памяти остается все же весьма значительным). Кроме того - и это относится к недостаткам данного способа - приходится выполнять весьма сложную настройку. Записи в реестре операционной системы предписывают запуск последней установленной копии клиента Notes (следовательно, другие пользователи не смогут щелкнуть по кнопке базы данных системы Notes в Проводнике Windows, чтобы запустить свою копию клиента системы Notes);
- О настройка одной копии клиента Notes с одним набором папок данных, совместно применяемых всеми пользователями. В данном случае приходится создавать отдельные документы местоположения и файлы идентификационных данных для каждого пользователя, чтобы пользователь располагал собственной базой данных почтовой службы. Преимущества подхода связаны с четкой идентификацией пользователей и наличием отдельных файлов почтовых сообщений. Кроме того, не требуется большого объема дисковой памяти. К недостаткам способа следует отнести необходимость совместного применения локальных баз данных. При этом пользователи должны помнить о необходимости очистки своих паролей после завершения работы в клиенте Notes;
- О настройка одной копии клиента Notes с единым файлом идентификационных данных (например, с именем Shipping Department - отдел доставки). Преимуществом этого способа является отсутствие специальных требований к установке: не нужно много дисковой памяти и достаточно одной пользовательской лицензии Notes. Недостаток же состоит в том, что пользователи не идентифицируются (не различаются) системой Notes и не имеют личных файлов почтовых сообщений, поэтому нельзя отследить выполняемые ими действия.

Для использования первого способа следует установить каждую копию клиента Notes в отдельную папку программ и папку данных, назначив им отдельные ярлыки. Если на компьютере указаны разные профили пользователей, можно не задавать индивидуальные ярлыки для папок, однако надо убедиться в том, что во время инсталлирования клиента системы Notes вход в операционную систему сделан по учетной записи нужного пользователя.

При определении путей к ярлыкам в Мастере InstallShield (при установке клиента Notes) допускается вводить название папки в виде Lotus Notes\Rob Kirkland. При этом Мастер InstallShield поместит ярлыки данной копии клиента в подпапку Rob Kirkland, которая сама расположена в папке Lotus Notes, находящейся в папке Programs.

Второй способ требует многократной установки клиента системы Notes (по одной копии на каждого пользователя). Каждый раз следует указывать одну и ту же папку программ, но индивидуальные папки данных. Имена для папок данных можно задавать по именам пользователей, чтобы впоследствии было ясно, какая из папок кому принадлежит. После завершения каждой очередной процедуры установки приходится переносить вновь созданный файл `notes.ini` из папки программ в новую папку данных. Кроме того, при любой процедуре установки надо либо назначать новую папку данных (именованную вышеупомянутым образом) для размещения в ней ярлыков, либо (если есть несколько профилей пользователя) входить в операционную систему по учетной записи определенного пользователя. Затем редактируется набор ярлыков, чтобы они указывали на нужное место файла `notes.ini` в папке данных, иначе система Notes не сможет отыскать файл `notes.ini` и провести запуск. Например, если имя папки программ `c:\lotus\notes`, а папки данных — `c:\lotus\joedoaks`, в поле **Target** (Целевой) каждого ярлыка должна присутствовать запись:

`c : \lotus\notes\notes.exe =c: \lotus\joedoaks\notes. ini`

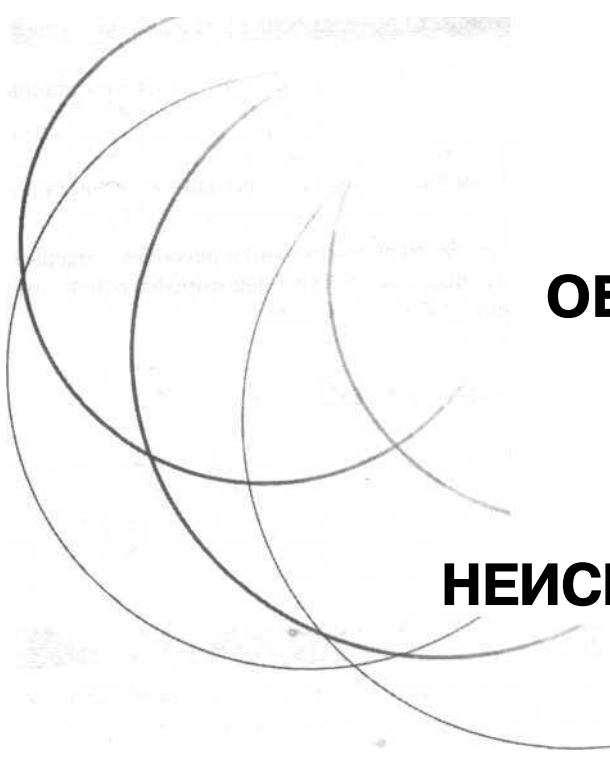
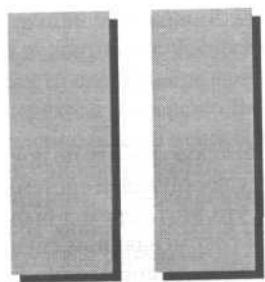
Одновременно в поле **Start in** (Запуск) должна находиться запись:

`c:\lotus\joedoaks`

В соответствии с третьим способом устанавливается лишь одна копия клиента системы Notes, однако формируется несколько файлов идентификационных данных для всех пользователей, которые заносятся в одну папку данных. Создается также набор документов местоположения в базе данных *Personal Address Book*. Каждому документу местоположения придается имя, указывающее на того пользователя, который будет его применять. Так, записи полей сервера в каждом документе местоположения должны указывать на определенные серверы. Поле **Mail file** (Файл почтовых сообщений) каждого документа местоположения должно содержать сведения о базе данных почтовой службы соответствующего пользователя. В поле **Only for user** (Только для пользователя) необходим подстановочный символ «звездочка». В противном случае документы местоположения будут исключены из списков и станут недоступными. Однако в записи поля **User ID to switch to** (Переключение на идентификационные данные) следует помещать путь к файлу идентификационных данных пользователя. При обращении пользователя к собственному документу местоположения система Notes будет автоматически запрашивать указанный в документе файл идентификационных данных.

Для применения четвертого способа необходимо создать идентификационные данные обобщенного пользователя, после чего настроить рабочую станцию системы Notes с помощью файла этих данных. Поскольку вряд ли получится идентифицировать пользователя по такому файлу, нельзя будет отслеживать работу каждого пользователя в отдельности. В этом случае придется весьма тщательно анализировать права доступа для такого «обобщенного» пользователя и разрешать ему применение лишь ограниченного числа баз данных.

ЧАСТЬ

Abstract graphic element consisting of several thin, dark gray curved lines that sweep across the lower-left portion of the page, creating a sense of motion or a stylized 'C' shape.

**ОБЕСПЕЧЕНИЕ
ПОДДЕРЖКИ
И ПОИСК
НЕИСПРАВНОСТЕЙ**

ГЛАВА

7



ОБНОВЛЕНИЕ СЕРВЕРА DOMINO ВЕРСИЙ 4.x И 5.x И ПЕРЕХОД К ВЕРСИИ 6.0

В целом специалисты компании Lotus проделали гигантскую работу по документированию тех операций, которые необходимы для обновления существующей системы Notes/Domino и перехода к версии 6.0. Можно смело утверждать, что этот переход был документально оформлен наилучшим образом. Если следовать всем рекомендациям специалистов Lotus, обновление домена и переход к версии 6.0 осуществляется достаточно быстро. Поэтому в настоящей главе не тратится время на повторение рекомендаций компании Lotus, а просто перечислена соответствующая документация и представлены необходимые пояснения и предупреждения, о которых специалисты Lotus в спешке, видимо, забыли. Предлагаемый материал, дополняющий их рекомендации, поможет провести обновление в весьма короткие сроки и с гарантированным успехом.

Вся процедура обновления домена Notes или Domino до версии 6 состоит из трех этапов:

- О планирование и подготовка к обновлению;
- О установка нового программного обеспечения;
- О обновление различных компонентов, в том числе каталогов, баз данных, средств поиска и безопасности.

Компания Lotus обеспечивает своих пользователей замечательным пособием, содержащим материалы по всем трем этапам, поэтому ниже мы обсудим некоторые нюансы этой процедуры, которые, несомненно, заслуживают особого внимания.

Планирование и подготовка к обновлению

Из практики хорошо известны три аспекта, связанных с планированием или подготовкой обновления и заслуживающих отдельного обсуждения: проверка возможностей аппаратных средств для того, чтобы гарантировать увеличение информационной нагрузки, которая ожидается от версии 6.0, проведение моделирования перед осуществлением реального обновления, а также обучение администраторов и пользователей.

Проверка аппаратных средств

Прежде всего необходимо хорошо себе представлять, что система Notes/Domino R6 имеет более широкие возможности, чем версии 4.x и 5.x. Поэтому нет ничего удивительного в том,

что она нуждается и в больших вычислительных ресурсах. В наши дни многие компании стараются задавать характеристики для своих серверов с существенным запасом, так что данные вопросы могут оказаться просто рутинными. Однако, если сервер Domino (текущая версия) конфигурировался вручную, настоятельно рекомендуется сравнить его характеристики с теми требованиями, которые предъявляются к аппаратным средствам в рамках версии 6.0.

Даже в том случае, если используемые серверы позволяют применение нескольких процессоров, располагают сотнями мегабайт оперативной памяти и терабайтами памяти на жестком диске, следует внимательно проверить конфигурацию жесткого диска, установленного для сервера. Напомним, что версии 5 и 6 предусматривают выполнение новой функции регистрации транзакций, которая способствует объединению данных и повышению степени их целостности, ускорению операций ввода/вывода данных диска и увеличению эффективности операций резервирования. Эта функция вводится по желанию пользователя, и при переходе на версию 6.0 имеет смысл рассмотреть вопрос о ее применении, так как она весьма полезна в некоторых ситуациях. Однако возможно, что сначала потребуются реконфигурировать файлы на жестком диске, поскольку данные регистрации транзакций лучше хранить на независимом жестком диске или в своем дисковом массиве (отдельно от файлов данных). Если в системе имеется только один дисковод (или массив), придется добавить как минимум еще один. Если же в системе уже есть несколько накопителей, следует реконфигурировать файлы данных так, чтобы один из дисководов высвобождался для занесения на диск данных регистрации транзакций.

Проведение моделирования

Рекомендуется, кроме того, перед началом обновления провести предварительное моделирование ситуации. Советуем ни в коем случае не пренебрегать этим этапом, поскольку он позволяет провести необходимые исследования и получить большой объем ценной информации. К тому же администраторам не придется волноваться, если ситуация выйдет из-под контроля, и вместе с тем у них будет возможность приобрести полезные навыки.

Если для обновления домена создается группа администраторов, стоит привлечь ее всю к проведению моделирования. Для этих целей можно выбрать очередную субботу, желательно холодный и дождливый день (чтобы не было поводов отвлекаться от дел и ничто не мешало полностью сосредоточиться на работе). По мере того как администраторы будут осваивать одну новую функцию версии 6.0 за другой, они, несомненно, увлекутся процессом и получат от него истинное удовольствие.

Потребуется настроить по меньшей мере два сервера и две рабочие станции сети, а также подготовить идентификационные данные пользователей с административными и стандартными правами доступа. Настройку серверов следует произвести для той версии системы Notes/Domino, которая на текущий момент применяется компьютерами, причем идентификационные данные, база данных Personal Address Book и приложения системы Notes, хранящиеся на серверах, также должны оставаться неизменными. Можно воспользоваться другими, скажем созвучными, именами файлов идентификационных данных. Такой подход фактически обеспечит копирование баз данных тестовых серверов и позволит не заботиться о редактировании списков управления доступом для создания новых имен.

В этой ситуации администраторы будут иметь доступ не к их реальным идентификационным данным, а только к специальным данным, созданным на экране **Server Administration** (Администрирование сервера). Следует задать идентификационные данные для

сертифицирующих организации и организационной единицы, а также идентификаторы серверов и пользователей. Идентификационные данные не предназначены для внесения их в реальный домене системы Notes и указываются только для тестового домена. Этим данным нужно присвоить имена файлов, которые определяли бы их временный характер и принадлежность к тестовому домену. Если они случайно затеряются среди реальных идентификационных данных, в дальнейшем не придется ломать голову из-за того, что они не обеспечивают выполнения тех или иных операций.

Контрольные серверы не обязаны быть идеальными аппаратными копиями реально установленных серверов, поскольку им не понадобится иметь дело с реальными объемами информационной нагрузки. Однако они должны, по возможности, обладать теми же самыми программными средствами, так как по завершении обновления с помощью этих средств будет проверяться работоспособность приложений версии 4 и 5 в сервере версии 6.

После подготовки тестовых серверов и рабочих станций и запуска для них текущей версии системы Notes/Domino следует сделать паузу (еще до начала операций обновления) и проанализировать необходимость реорганизации файлов на жестких дисках серверов.

Это нужно по двум причинам. Во-первых, вполне возможно, что при оценке аппаратных средств (см. предшествующий раздел) было решено реконфигурировать файлы на жестких дисках для обеспечения нормальной работы функции регистрации транзакций в рамках версии R6. Во-вторых, не исключено, что даже администратор, отказавшийся от введения функции регистрации транзакций, все же сочтет реорганизацию желательной, так как:

- О в рамках версии 3 процедура установки типового программного обеспечения предусматривает занесение всех файлов программ и данных в папку `c:\notes` (кроме операционной системы Windows, в которой файл `notes.ini` заносится в системную папку Windows);
- О начиная с версии 4.0 процедура установки типового программного обеспечения изменена таким образом, чтобы файлы программ записывались в папку `c:\notes`, а файлы данных соответственно в папку `c:\notes\data`. Для компьютеров, использующих операционную систему Windows, файл `notes.ini` будет располагаться в папке Windows;
- О начиная с версии 4.6 процедура установки предусматривает занесение файлов программ в папку `c:\lotus\domino`, а файлов данных (в том числе и файла `notes.ini`) в папку `c:\lotus\domino\data`;
- О в версиях 5 и 6 по умолчанию предполагается выполнение тех же самых действий, что и для версии 4 (файлы программ помещаются в папку `c:\lotus\domino`, а файлы данных соответственно в папку `c:\lotus\domino\data`). Однако файл `notes.ini` попадает в папку `c:\lotus\domino` серверов без дисковых разделов либо в папку `c:\lotus\domino\data` серверов с уже выделенными разделами.

Сначала следует выяснить конфигурацию тестового сервера, а затем оценить, отвечает ли она текущим требованиям администратора. При отрицательном ответе надо подумать об изменении конфигурации компьютера, ведь ущерб от неправильного конфигурирования тестовой машины будет незначителен.

По этому поводу имеет смысл сделать два замечания. Во-первых, если не сообщить системе Notes/Domino о местоположении файла `notes.ini`, содержащего параметры управляющих команд, она начнет самостоятельно искать его сначала в системной папке, а затем уже в папке установленных программ. Во-вторых, при принятии решения относительно

реконфигурирования файлов на серверах потребуются произвести некоторые изменения существующих записей:

- О в файле notes.ini сервера (его следует открыть в текстовом редакторе и проверить все ссылки на диски);
- О в ярлыках (если сервер работает с операционной системой Windows) или в групповых/командных файлах/сценариях, посредством которых управляется сервер (когда применяется операционная система Windows, ярлыки располагаются в папке Start Menu; а в случае Windows NT - в нескольких папках Start Menu, которые относятся к соответствующим разделам подпапки Profiles папки Windows);
- О в реестре операционной системы Windows (для редактирования следует запустить программу regedit.exe или regedit32.exe и искать слова типа «lotus», «notes» и подобные; но можно обойтись и без изменения реестра). Не исключено, что программа установки сервера Domino не найдет текущую копию этой системы, поэтому ей придется сообщить, где располагается соответствующий файл и инициировать переход в нужную папку. Мы работаем на тестовых серверах, которые предназначены исключительно для контроля, поэтому нет повода для какого-либо беспокойства.

Теперь, когда серверы и рабочие станции полностью подготовлены, можно вернуться к вопросам моделирования. К этому моменту уже проведено (или сознательно не проведено) реконфигурирование файлов на серверах и практически завершена подготовка к обновлению тестовых серверов и рабочих станций. Для осуществления обновления следует воспользоваться пошаговыми инструкциями компании Lotus. Обновить до уровня Lotus Notes/Domino 6 допустимо только серверы версии 4.6 или выше, причем требуется предварительно провести обновление до состояния текущего ежеквартального выпуска/обновления существующей версии Notes/Domino (по крайней мере до версии Maintenance Release 4.6.7a). Затем надо переходить на версию б.х.х, то есть на последнюю версию, существующую на момент обновления (кстати, перед выпуском R6 последней версией R5 была Domino 5.011).

По мере обновления и выполнения предписанных компанией Lotus действий нужно вносить записи на полях технического руководства. В дальнейшем станет ясно, что в некоторых местах специалисты Lotus допустили небольшие неточности (обычно это касается повторного запуска ранее остановленных компонентов). Может также обнаружиться, что реальные ответные сообщения сервера не совпадают с указанными. В таких случаях придется самостоятельно принимать решение о способе возвращения на «основной маршрут». Поэтому администраторы еще не раз порадуются тому, что они остаются на этапе тестирования, работают в дневное время и не испортили почтовый сервер администрации своей компании.

После завершения установки первого сервера б.х и его резервного копирования перед обновлением остальных компьютеров необходимо с помощью клиента системы Notes проверить базу данных Personal Address Book на обновленном сервере. При обновлении версии R4.6 некоторые документы изменят свой формат (если только сотрудники фирмы Lotus не устранили проблему уже после написания настоящей книги). Из этого следует практически важный вывод: нет смысла модифицировать рабочие серверы до тех пор, пока не будут подготовлены к обновлению рабочие станции администраторов, поскольку нельзя администрировать серверы версии 5 и 6 из клиентов системы Notes версии 4.

Далее обновляется рабочая станция системы Notes, программы Domino Administrator и, возможно, программы Domino Designer. Затем можно переходить к обновлению следующего сервера и еще одной рабочей станции. Как и в случае с первым сервером, полезно делать пометки на полях соответствующих пособий фирмы Lotus, поскольку в процессе обновления обязательно возникнут расхождения с текстом, которые необходимо учитывать в дальнейшем.

После завершения обновления тестовые серверы и рабочие станции следует на время передать сотрудникам, обеспечивающим поддержку приложений системы Notes, и попросить их проверить характер реализации различных функций и приложений, чтобы проконтролировать правильность исполнения в рамках версии 6. Все проблемы и замечания в обязательном порядке должны быть отражены в документах.

Итак, моделирование является весьма эффективным способом обнаружения всех недостатков в пределах безопасной санитарной зоны. В данном случае можно позволить себе поэкспериментировать, ничем не рискуя. В ходе такого эксперимента администраторы получают большой объем полезной информации о процессе обновления и отличиях между предыдущей и планирующейся установками. Они действуют в достаточно спокойной обстановке, не опасаясь выставить себя не с лучшей стороны или потерять престижную работу.

Проведение обучения и организация тренингов

Чтобы успешно завершить переход на версию 6, необходимо заблаговременно подготовить администраторов, разработчиков и пользователей. Нельзя экономить на обучении, поскольку чем больше администраторы и пользователи будут знать о возможностях версии 6, тем спокойнее пройдет ее внедрение. Ознакомившись с новыми функциями системы Notes, люди непременно захотят ими воспользоваться. Таким образом, с одной стороны, будет обеспечен быстрый и спокойный переход к версии 6, а с другой - администраторы и пользователи фирмы приобретут богатый опыт применения новой системы.

Начинать обучение надо со знакомства с документацией системы Notes/Domino. В дополнение к этому рекомендуется прочесть первую главу данной книги. Затем необходимо просмотреть последние несколько разделов первой главы пособия фирмы Lotus «Переход к версии 6 системы Notes/Domino» (Moving to Notes and Domino Release 6). Так, разделы «Новые функции сервера Domino», «Новые функции почтовой службы сервера Domino», «Новые возможности клиента системы Notes/Domino», «Новые свойства приложений сервера Domino» и «Новые функции поиска сервера Domino», будучи достаточно краткими, описывают все новые возможности системы Notes/Domino. Эти разделы представлены по адресу www.notes.net; их легко загрузить и направить (с помощью электронной почты) основным сотрудникам для подготовки к процедуре обновления.

Кроме того, аналогичные сообщения электронной почты могут быть посланы другим членам группы, занимающимся вопросами обновления и перехода от версии 4 или 5 к версии 6. Компания Lotus проводит несколько вполне достойных внимания семинаров по этим вопросам, поэтому имеет смысл направить туда представителей разработчиков. В ходе семинаров разработчики приложений получат много полезной информации.

Постарайтесь не упустить шанса поработать с программой Domino Administrator и изучить ее возможности, в частности в условиях выполнения ею различных административных функций. Опытного администратора системы Notes/Domino R4 наверняка будет интересовать содержимое базы данных Domain Directory (в прошлом база данных Personal

Address Book), и он захочет поработать с ее видами и создать (или отредактировать) ее документы. В ходе обучения это оказывается вполне реализуемым (а иногда и просто необходимым). Программа Domino Administrator является весьма мощным интерфейсным средством администрирования, поэтому администраторам, без сомнения, стоит с ней ознакомиться.

И наконец, настоятельно рекомендуется предлагать различные формы обучения пользователям. Так, можно предложить посещение занятий, просмотр видеоматериалов, материалы для самостоятельной проработки и книги по вопросам, связанным с версией 6.

Не следует забывать, что чем большей информацией обладают пользователи и чем мощнее ресурсы, которыми они обладают, тем реже они будут обращаться в службу поддержки с глупыми вопросами.

Процедура установки программного обеспечения R6 поверх программного обеспечения версий 4 и 5

В предыдущем разделе данной главы при описании процедуры моделирования рассматривалось использование административного клиента системы Notes для просмотра базы данных Public Address Book на первом обновленном сервере версии 5 или 6. Если эти рекомендации были выполнены, то администраторы, несомненно, пришли к выводу о невозможности администрирования нового сервера с помощью клиента системы Notes R4. В данном случае ситуация еще более драматична: не удастся администрировать даже один сервер домена с помощью рабочей станции версии 4 сразу после обновления одного из серверов и перехода к версии 5 или 6, поскольку рабочая станция не в состоянии считывать некоторые документы в базе данных Public Address Book версии 5 или 6.

Таким образом, не следует обновлять серверы в рабочем домене системы Notes для экспериментальных целей. При желании провести исследования версии 6 разумнее подготовить тестовые серверы. Ни в коем случае не обновляйте для эксперимента рабочие серверы; к обновлению этих серверов можно приступать только тогда, когда все подготовительные работы в домене уже завершены. Нет необходимости обновлять сразу все серверы в домене, однако уже на первом этапе обновления нескольких серверов требуется предусмотреть обновление как минимум одной рабочей станции администратора.

Обновление серверов Domino и переход от версии 4 к версии 5 или 6 обычно продолжается вполне определенное время. Наряду с другими работами здесь понадобится выполнить операции по резервированию, вручную восстановить некоторые виды базы данных Public Address Book, модифицировать структуру различных баз и проделать множество других операций. Все эти работы лучше производить в часы минимальной активности системы, заранее предупредив пользователей о том, что их серверы будут недоступны в течение нескольких часов. При обновлении административных серверов приходится провести целый ряд дополнительных операций в базе данных Public Address Book. То же самое касается серверов, применяющих программу SMTP MTA, поэтому на их обновление необходимо отводить больше времени.

При обновлении до R6 сначала рекомендуется модифицировать один сервер вместе с каталогом Domino Directory или базой данных Public Address Book, если обновляется сервер Domino 4.6. Специалисты Lotus советуют прежде всего обновить сервер концентратора.

На первом этапе необходимо остановить сервер, произвести резервирование и инициировать собственную процедуру обновления. Один из моментов, о котором специалисты Lotus забыли предупредить своих пользователей и который позволяет заметно облегчить работу в будущем, связан с отменой автоматического запуска сервера, которая может быть активизирована. При использовании Windows NT это сопровождается одновременной отменой автоматического запуска ее служб, а в других операционных системах - удалением соответствующей строки в пакетном файле или файле сценариев. Если какие-либо иные программы (например, антивирусная) автоматически запускаются вместе с компьютером, они **также должны быть временно отменены.**

Цель в данном случае состоит в минимизации числа влияющих факторов при реализации процесса обновления. Так, в ряде случаев может потребоваться перезагрузить компьютер, чему функция автозапуска будет препятствовать. Специалисты советуют отменять эту функцию при обновлении любых систем.

Другая операция, которую следует выполнить на всех серверах еще до начала их обновления, - стирание всех старых и ненужных записей, накопившихся на жестких дисках, на которых можно обнаружить старые, уже не употребляющиеся базы данных системы Notes или другие, не связанные с ней программы. Не забывайте, что удаление старых программ и баз данных позволит высвободить на диске большое пространство, весьма ценное и полезное при обновлении. В процессе обновления придется восстанавливать виды баз данных, а в отсутствие свободной области памяти во время восстановления могут появиться сообщения об ошибках.

После завершения обновления первого сервера полезно провести обновление по крайней мере одной рабочей станции администратора, а уже потом заняться остальными серверами. Что касается рабочих станций пользователей, нет необходимости спешить с их обновлением. Люди, естественно, захотят как можно быстрее воспользоваться преимуществами версии 6, однако все функции версий 4 и 5 будут так же хорошо выполняться и после обновления серверов (в перехода на версию 6). Единственная проблема может возникнуть при условии, что обновление приложений (переход на версию 6) будет инициировано до обновления рабочих станций пользователей, поскольку пользователи просто не смогут применять эти приложения.

Обновление баз данных, каталогов, функций поиска, обеспечения безопасности и контроля

После обновления программного обеспечения на сервере и рабочей станции следует приступить к обновлению других объектов, в том числе формата файлов баз данных, структуры баз данных, каталогов, а также функций поиска и обеспечения безопасности. Большинство из этих задач не являются срочными, поскольку система будет нормально функционировать и в отсутствие обновления. Тем не менее их решение позволит получить доступ к целому ряду новых функций, поэтому неразумно надолго откладывать данные мероприятия. Так, по крайней мере обновление формата файлов баз данных и структуры баз данных почтовой службы лучше не оставлять на будущее.

Обновление баз данных

Существующие базы данных имеют два параметра, соответствующих версии 4 (или даже версии 3): формат представления файлов на диске, который соответствует ODS20 для версии 4 и ODS17 для версии 3, и структура этих файлов. Как правило, требуется как можно быстрее привести данные параметры к новому виду, принятому для версии 6 (формат R6 обеспечивает только обратную совместимость с форматом ODS41 версии R5). Внутренняя структура базы данных не меняется в процессе репликации, поэтому на практике не стоит беспокоиться относительно несовместимости, которая могла бы возникнуть при проведении обновления (если во время тестирования проверялись приложения, то уже известно, какие из них не допускают обновлений). Заметим, что после преобразования базы данных в формат Domino 6 сохраняется возможность отката за счет применения ключа **-R**, создания новой реплики или копирования базы данных в формате Domino 5.

Формат ODS (On-Disk Structure - структура на диске) базы данных может быть обновлен путем уплотнения. После приведения базы данных к новому формату Domino 6 новые ее функции будут недоступны из старых клиентов Notes 4.6 и Notes 5, а после уплотнения нельзя посредством команды **updall** обновлять индексы приложений. Следует иметь в виду, что обновление индексов приложений не является строго обязательным, но если этого не сделать, для каждого очередного пользователя, обращающегося к видам, будет наблюдаться заметная временная задержка, поскольку серверу нужно восстановить индекс вида перед передачей его пользователю.

Если на текущем этапе не требуется модифицировать базу данных, можно ограничиться переименованием ее файла **filename.ns4** (для R4) или **filename.ns5** (для R5). Если же необходимо изменить базу данных и вернуться к формату OSD20 или ODS41, то ее уплотняют с помощью параметра **-R** (но не **-r**). Информация относительно формата файлов базы данных имеется на странице **Files** (Файлы) программы Domino Administrator, где параметры файлов приводятся вместе с другими статистическими сведениями. Если по каким-то причинам нельзя уплотнить базы данных сервера в дневные часы, можно соответствующим образом изменить документ программы и инициировать уплотнение в ночное время.

Структуру баз данных надо менять с большой осторожностью. Следует помнить о том, что пользователи системы Notes R4 и R5 не смогут сразу применить новые функции баз данных системы Notes версии 6, а в ряде случаев вообще не сумеют воспользоваться этими базами без проведения соответствующих обновлений.

Обновление баз данных почтовой службы

Почтовые базы данных пользователей нуждаются в весьма оперативном обновлении, которое необходимо провести как можно быстрее, фактически сразу же по завершении обновления рабочей станции пользователя. Если этого не сделать, пользователь в самое ближайшее время обратится к службе поддержки, поскольку шаблоны почтовой службы для версии 4 не поддерживают все функции, реализуемые в интерфейсе новой версией системы Notes. Например, пользователь может щелкнуть по ярлыку **Inbox** (Входящие) системы Notes, затем перейти в другую папку (или в окно календаря), а на заключительном этапе

закрыть это окно. Однако при повторном обращении к ярлыку **Inbox** (при использовании шаблона почтовой службы версии 4) на экран будет выведено содержимое совсем другой папки.

С другой стороны, при обновлении почтовой службы пользователя в рамках системы Notes R4 ему практически запрещается доступ к почтовой службе, так как эта система не распознает все функции шаблонов почтовой службы версии 5 и 6. Не исключено, что, если обновление базы данных почтовой службы будет выполнено на сервере версии 4, но шаблонами версии 5 или 6, база данных окажется просто не в состоянии обеспечивать нормальное функционирование. Такая проблема в основном возникает в случае применения кластера серверов почтовой службы, когда один сервер модифицируется до версии 5 или 6, а другие остаются в прежнем состоянии. В связи с этим не рекомендуется обновлять почтовые службы пользователей до тех пор, пока не обновлены все серверы (а также рабочие станции пользователей).

При проведении обновления для пользователя (переход на версию 6) необходимо предусмотреть выполнение двух действий. Во-первых, по возможности предупредить пользователей о том, что их интерфейс почтовой службы может вести себя несколько необычно (до момента обновления структуры базы данных почтовой службы). Во-вторых, не терять время и не откладывать обновление шаблонов почтовой службы пользователей после завершения обновления их рабочих станций (а также не оставлять на будущее обновление остальных серверов кластера почтовой службы).

Структуру баз данных почтовой службы пользователей можно обновить двумя способами. Во-первых, выполнить эту операцию вручную через интерфейс системы Notes. Такой способ удобен на последнем этапе процедуры обновления системы Notes. При этом следует активизировать систему Notes, предложить пользователю ввести пароль, а затем шелкнуть по ярлыку пользовательской почты и в контекстном меню выбрать команду **Database => Replace Design** (База данных => Изменение структуры). В открывшемся диалоговом окне **Replace Database Design** (Изменение структуры базы данных) надо шелкнуть по строчке **Template Server** (Шаблон сервера) и выбрать сервер почтовой службы пользователя и шаблон **Mail (R6.0)** (Почтовая служба, версия 6.0), то есть файл mail6.ntf. Заметим, что аналогичным образом выполняется преобразование шаблонов iNotes Web Access (R6.0) (файл iNotes60.ntf) и пользовательского почтового шаблона.

Во-вторых, можно одновременно обновить весь кластер баз данных почтовой службы с утилитой преобразования convert. Эта же программа использовалась на этапе перехода от версии 3 к версии 4, поэтому не исключено, что администраторы с ней хорошо знакомы. Программа позволяет одновременно обновить одну или несколько баз данных почтовой службы. Она может применяться совместно с текстовым перечнем имен файлов почтовых служб. При проведении обновления, скажем для двадцати пользователей в конце рабочей смены, можно запустить команду:

```
load convert -f имя_пути_к текстовому_файлу * MAIL6 .NTF
```

Эта команда обращается ко всем файлам с именами имя_пути_к текстовому_файлу, которые базируются на любом из шаблонов почтовой службы (*), и преобразует их в шаблоны почтовой службы версии 6 (файл mail6.ntf).

Для подготовки перечня файлов можно воспользоваться командой вида

```
load convert -l c: \temp\masterlist.txt
```

Эта команда позволяет создать текстовый файл, содержащий сведения об основных файлах почтовой службы. *Основной файл почтовой службы* соответствует файлу почтовой

службы для сервера почтовой службы пользователя. Имейте в виду, что некоторые пользователи могут сформировать реплики (копии) файлов почтовой службы на других серверах, которые, однако, не будут рассматриваться как основные файлы почтовой службы.

В таком случае файл `c:\temp\masterlist.txt` следует использовать в качестве *файла главного перечня*. В конце каждого рабочего дня администратор может открыть этот файл в текстовом редакторе, вызвать пустой файл в другом редакторе, а затем вырезать и вставить из главного перечня имена обновляемых файлов и перенести их в новый файл. Затем надо сохранить и закрыть старый файл, сохранить новый файл с именем `c:\temp\list.txt` и, наконец, выполнить вышеупомянутую команду для тех пользователей, для которых запланировано текущее обновление.

При ежедневном переносе файлов размер главного перечня будет сокращаться постепенно, и по его уменьшению администратор сможет отследить результаты своей работы.

Однако при обновлениях нельзя забывать об одном весьма существенном моменте. Перед запуском процедуры обновления файлов надо остановить устройство маршрутизации, чтобы оно не инициировало пересылку сообщения в ходе этого процесса. По его завершении функция маршрутизации возобновляется. На практике время, требуемое для обновления файлов почтовых сообщений, иногда превышает один час. Администратору вряд ли захочется заниматься этим делом в конце рабочего дня и задерживаться только для того, чтобы снова запустить маршрутизацию, но и уйти с работы он не сможет.

Решить проблему поможет создание нескольких документов программы. Первый из них послужит для выключения маршрутизатора. Второй предназначен для проведения загрузки утилиты `convert`, а третий должен спустя несколько часов после действия первого и второго документов повторно активизировать маршрутизацию. Для корректного применения этих документов необходимо правильно заполнить в них два первых поля: **Program name** (Имя программы) и **Command line** (Командная строка). В табл. 7.1 приведены варианты записей для указанных полей, используемых в рамках трех документов программы.

Таблица 7.1. Записи полей для документов программы, используемых при преобразовании почтовых файлов

Документ программы	Имя программы	Командная строка
Первый документ программы	nserver	-c "tell router quite"
Второй документ программы	nconvert	-f c:\temp\list.txt * mail50.ntf
Третий документ программы	nrouter	Это поле заполнять не следует

Момент запуска для второго документа программы следует задать на одну минуту позже, чем для первого. Третий документ нужно запустить значительно позже второго. На полное преобразование каждой базы данных необходимо выделить примерно пять минут. Реальная длительность этого временного интервала зависит от быстродействия компьютера и от характера операций, одновременно выполняемых сервером Domino. Чтобы точно определить время, можно сначала преобразовать один почтовый файл вручную. Если задать моменты запуска документов в ночные часы, то не придется отключать функцию маршрутизации в периоды сильной загруженности сервера.

Формирование обратного адреса сети Internet

Если планируется предоставить пользователям электронной почты доступ к сети Internet и для этих целей понадобятся серверы Domino версии 6 (вместо серверов R4, работающих

с агентом SMTP MTA), нужно убедиться в том, что все персональные документы (Personal document) снабжены соответствующими адресами электронной почты Internet (в полях адреса сети Internet). В рамках версии 4 эти поля разрешалось заполнять произвольно, а программа SMTP MTA пользовалась параметрами, указанными в документе глобального домена (Global Domain document) при формировании корректного обратного адреса сети Internet для исходящих почтовых сообщений. В техническом плане можно и далее использовать указанный документ для формирования адреса. Однако специалисты Lotus настоятельно советуют формировать корректный обратный адрес для всех исходящих почтовых сообщений путем изменения параметров по умолчанию, задаваемых с помощью документа глобального домена, и назначения корректного адреса в разделе **Internet address** (Адрес сети Internet) каждого персонального документа.

В малых по размерам доменах эту операцию можно выполнять вручную, но при больших объемах работ ее стоит автоматизировать. Компания Lotus разработала программный инструмент, позволяющий автоматически формировать корректные адреса сети Internet и заносить их в персональные документы пользователей. Этот программный инструмент доступен из программы Domino Administrator на вкладке **People & Groups** (Сотрудники и группы). Следует выбрать те персональные документы, которым нужно присвоить адреса сети Internet; в противном случае адреса сети Internet будут добавлены всем существующим персональным документам, не имеющим таких адресов. На панели **Tools** (Программные инструменты) задается **People => Set Internet Address** (Сотрудники => Задание адреса сети Internet) или в меню **People** (Сотрудники) отмечается пункт **People => Set Person's Internet Address** (Сотрудники => Задание адреса сети Internet для сотрудника).

В диалоговом окне **Set Internet Address** (Задание адреса сети Internet) устанавливается шаблон адреса и вносится имя домена. После этого требуется щелкнуть по кнопке OK - и программный инструмент сформирует соответствующий адрес с учетом указанных данных и данных, присутствующих в персональном документе. Если шаблон адреса подходит нескольким пользователям с одинаковым адресом Internet, программный инструмент предоставит альтернативный шаблон или просто откажется от формирования дублирующихся адресов и запишет сообщение об ошибке в журнал Notes Log (Журнал Notes).

Обновление поддержки каталога и каскадных книг адресов

При использовании Directory Assistance, также известной под названием Master Address Book (Главная книга адресов) в рамках версии 4, приходится модифицировать структуру базы данных Directory Assistance. Эту операцию можно выполнить в Domino Administrator на вкладке **Files** (Файлы). Выделите базу данных одного из серверов (предпочтительно имеющего право передавать результаты обновления на другие серверы) и откройте ее. Выберите **File => Database => Replace Design** (Файл => База данных => Изменение структуры) и задайте установленный сервер в качестве шаблона сервера (**Template Server**), затем укажите **Directory Assistance** (Поддержка каталога) в перечне шаблонов (имя соответствующего файла имеет вид da60.ntf). На заключительном шаге выполните команду **Inherit future design changes** (Запоминание будущих изменений структуры) и щелкните по кнопке **Replace** (Замена).

При работе с базой данных Cascading Address Books (Каскадные книги адресов) в рамках версии 4 специалисты Lotus рекомендуют перейти на базу данных Directory Assistance и работать с перечнем каталогов (Directory Catalogs), появившихся в версии 5 (см. главу 11).

Функции просмотра домена и перечня базы данных

Функция **Domain Search** (Просмотр домена) появилась в серверах Domino R5. Она заметно изменилась в лучшую сторону по сравнению с функцией **Site Search** (Поиск сайта), которая присутствовала в серверах версии 4. **Domain Search** позволяет индексировать весь домен системы Notes посредством единой полнотекстовой системы индексации, к которой могут обратиться любые клиенты системы Notes или Web-пользователи. Кроме того, с ее помощью легко индексировать некоторые файловые системы. Функция **Domain Search** демонстрирует ряд преимуществ перед функцией **Site Search**, например обеспечивает фильтрацию результатов поиска за счет привлечения соответствующих списков управления доступом, так что пользователи в состоянии найти только документы, на которые им предоставлено право доступа на уровне **Reader** (Читатель). Данный принцип не всегда целесообразно применять в файловых системах, поэтому на практике не стоит индексировать файловые системы, содержащие файлы с конфиденциальной информацией.

Функцию **Domain Search** следует устанавливать на мощном сервере, входящем в состав соответствующего домена. Поскольку серверу придется выполнять множество операций индексирования, специалисты Lotus рекомендуют выбирать для этой цели быстродействующий, мощный сервер с внушительными объемами дисковой памяти (и несколькими процессорами) и оперативной памяти (и несколькими накопителями). Функция **Domain Search** обычно запрашивает большое количество информации из баз данных и файлов, расположенных на других серверах, поэтому другие серверы также должны характеризоваться высоким быстродействием (тактовой частотой 100 МГц и выше) и подключаться по высокоскоростным локальным сетям.

Подобно функции **Site Search** версии 4, **Domain Search** формирует систему индексации на основе одной базы данных, однако здесь для этого служит база данных Catalog (Каталог, файл catalog.nsf). Она является своего рода преемником базы данных Catalog версии 4, с которой администраторы должны быть хорошо знакомы. Для активизации функции **Domain Search** необходимо проделать следующее:

1. Откройте в режиме **Edit Mode** (Режим редактирования) документ сервера (Server document) на вкладке **Server Tasks** => **Domain Indexer** (Операции сервера => Индексация домена).
2. Задайте в поле **Domain wide indexer** (Широкомасштабная индексация домена) значение **Enabled** (Разрешено).
3. Введите нужное расписание индексирования (если к данному моменту требования еще не сформулированы, что вполне допустимо, можно назначить параметры по умолчанию).
4. Добавьте имена серверов в поле **Limit domain wide indexing to the following servers** (Ограничения при широкомасштабной индексации домена для следующих серверов). Если это поле останется незаполненным, программа индексации Domain Indexer проиндексирует базы данных всех серверов домена, у которых установлено свойство **Include in multi database indexing** (Включение в индексирование нескольких баз данных). На практике рекомендуется ограничиться индексированием только тех серверов, доступ к которым осуществляется с помощью достаточно быстродействующих и надежных сетевых соединений.
5. Сохраните и закройте документ сервера (Server document).
6. Запустите операцию загрузки каталога на сервере Domain Search (он же сервер Domain Catalog), введя на консоли сервера команду load catalog.

При загрузке каталога соответствующей функции придается статус Domain Cataloger (Каталогизатор домена). Одновременно отменяется применение существующей базы данных Catalog и иницируется формирование новой базы данных.

Для включения в индекс базы данных следует установить ее свойство **Include in multi database indexing**. Индексируемые в рамках домена базы могут храниться на любых серверах, указанных на шаге 4 предыдущего упражнения.

Выбирать базы данных для индексирования надо весьма тщательно, добавляя только те из них, которые содержат часто требуемую информацию. В противном случае существует опасность истратить пустую весьма ценные вычислительные ресурсы системы. Например,

не стоит индексировать *mailto:* данные у почтовой службы пользователей, поскольку в дальнейшем никто, кроме самих пользователей, не будет работать с записями этих баз.

Для выполнения индексирования файловой системы надо создать в базе данных Catalog один или несколько документов файловой системы (File System document). Обычно для каждого сервера Domino формируется один такой документ, который может обслуживать одну или большее число файловых систем.

Файловые системы должны соответствовать подпапкам папки данных сервера Domino. Чтобы проиндексировать файловые системы, не относящиеся к таким подпапкам, придется создавать новые ссылки каталога или формировать соответствующие документы отображения/перенаправления (Mapping/Redirection document).

Ссылки каталога формируются в программе Domino Administrator на вкладке **Files**. Для этого выберите вариант **New Link** (Новая ссылка) на панели **Tools** (Программные инструменты) под разделом **Folder** (Папка).

Документ отображения/перенаправления можно сделать следующим образом:

1. В программе Domino Administrator откройте документ сервера для соответствующего сервера.
2. Укажите Web на панели **Toolbar** (Панель программных инструментов), после чего выполните команду **URL Mapping/Redirection** (Отображение/перенаправление адреса URL).

Следует отметить, что документы отображения/перенаправления адреса URL не располагаются в базе данных Domino Configuration (Конфигурация сервера Domino). Начиная с версии 5 они находятся в документах ответов серверу (Responses to Server document), то есть попадают в базу данных Domain Directory (в прошлом база данных Personal Address Book). То же самое относится и к документам виртуального сервера (Virtual Server document). Надо также иметь в виду, что теперь появляется возможность для создания документов защиты файла и области (File Protection and Realm document). Более подробно о функциях, связанных с применением службы Domino HTTP, рассказывается в главе 15.

Чтобы провести настройку поиска по индексу домена (Domain Index) для пользователей системы Notes, необходимо добавить имя сервера Domain Search/Catalog (Сервер поиска/каталога) в соответствующие документы местоположения, в частности в поле **Catalog/Domain Search server** (Сервер поиска в каталоге/домене) на вкладке **Servers** (Серверы). После этого пользователь системы Notes сможет производить поиск в домене, щелкнув на раскрывающейся части кнопки **Search navigation** (Навигация поиска), расположенной в правой верхней части экрана, и выполнив команду **Domain Search** (Поиск в домене).

Вместо того чтобы модифицировать документы местоположения пользователей поочередно (на рабочих станциях), как в версии 4, достаточно добавить имя сервера поиска

в поле **Catalog/Domain Search server** профиля настройки пользователей (User Setup Profiles). Там же можно обновить рабочую станцию пользователя до версии 6 (см. главы 5 и 13).

Для реальной настройки функции **Domain Search** нужны определенные дополнительные сведения. На практике для баз данных и систем файлов лучше ввести категории, чтобы пользователи могли просмотреть базу данных Catalog и получить необходимую информацию, а не искать ее с помощью полнотекстового поиска. Допустимо настроить число индексных потоков и тем самым увеличить скорость индексирования за счет снижения скорости поиска или повысить скорость поиска в ущерб скорости индексирования (см. главу 14).

Завершая обсуждение функции **Domain Search** и базы данных Catalog, можно посоветовать обращаться к базе данных Catalog даже в случае, когда не планируется активизировать функцию **Domain Search**. Здесь содержится гораздо больший объем полезной информации о каталогизированных базах данных, чем в предшествующих каталогах. К тому же эта информация будет реально востребована в процессе последующей работы.

Обновление системы безопасности

В документации Lotus по версии 5 отмечается, что можно использовать для идентификационных данных системы Notes сертификаты X.509 (наряду с сертификатами самой системы Notes или вместо них). С момента появления документации многие специалисты пытались проверить возможность реализации в рамках версии 5.0.x второго варианта (применение сертификатов X.509 вместо сертификатов системы Notes), но ни к каким положительным результатам это не привело. Есть подозрение, что специалисты компании Lotus в последний момент исключили данную функцию из так называемой золотой (Gold) версии системы Notes R5, но не отразили это в документации. В версии R6 сертификаты X.509 используются вместе или вместо аутентификации по имени/пароллю.

Однако пользователи имеют возможность одновременно работать с сертификатами системы Notes и сертификатами X.509 (и запоминать их в идентификационных данных). В системе Notes/Domino R5 допускается считывание, запись и хранение документов в формате MIME/MHTML. В системе Notes можно в формате S/MIME подписывать сообщения, пересылаемые пользователями в сеть Internet (для соответствующих абонентов почтовой службы), и дешифровать сообщения, получаемые из Internet от других пользователей. Правда, для применения формата S/MIME пользователи должны располагать сертификатом X.509 (см. главу 10).

Следует также хорошо представлять себе те ограничения, которые появляются в условиях одновременного использования в среде Notes версий 3/4/5/6. Эти ограничения в основном связаны с изменениями в структуре идентификаторов системы Notes R5:

- О файлы идентификационных данных версии 5 и 6 не могут применяться устройствами клиента системы Notes R3. При необходимости создания идентификационных данных системы Notes, совместимых с версией 3, требуются службы администрирования системы Notes R4;
- О при наличии в рамках идентификационных данных системы Notes R5 и R6 альтернативных имен/языков общения они не смогут применяться совместно с устройствами клиента системы Notes (версия 4/5) или серверами Notes/Domino (см. главу 6);

- О программа Domino Administrator из версии 5 не обеспечивает создания плоских, неформатированных файлов идентификационных данных. При необходимости подобные файлы формируются соответствующими клиентами администрирования системы Notes R4. Если для организации до сих пор не заданы иерархические идентификационные данные, придется обратиться к специалистам или консультантам;
- О только клиенты системы Notes, относящиеся к версии 4.5 и более поздним, осуществляют нормальную аутентификацию серверов, реализующих функцию проверки пароля. Кроме того, лишь на серверах Domino версии 4.5 или более поздних может быть установлена эта функция. Если требуется с помощью идентификаторов провести аутентификацию на сервере, выполняющем проверку пароля, идентификационные данные должны соответствовать версии системы Notes не ниже 4.5;
- О файлы идентификационных данных содержат сертификаты X.509, но клиенты системы Notes R3 работать с ними не могут, а клиенты системы Notes R4 - могут;
- О в версии 5 появилась возможность усилить защиту для Web-имен/паролей. В документе сервера в разделе **Security** (Безопасность) имеется поле **Web server authentication** (Аутентификация Web-сервера), где следует указать вариант **More name variations with lower security** (Большое разнообразие имен при снижении уровня защиты) для Web-аутентификации в версиях ниже пятой или вариант **Fewer name variations with higher security** (Небольшие изменения имен при увеличении уровня защиты). При выборе второго варианта пользователям приходится вводить более сложные имена, чем в первом варианте.

Программные средства мониторинга

Если в версиях 4 и 3 были установлены программные средства мониторинга сервера, например функции **Reporter and Event Dispatcher** (Диспетчеризация отчетов и событий) и **Statistic, File and Event Monitor** (Мониторинг статистических данных, файлов и событий), то эти привычные программы нельзя вводить в рамках версии 5. К сожалению, если не уделить этим вопросам должного внимания, при переходе на версии 5 или 6 перестанут формироваться уведомления о потенциальных проблемах в системе, о которых сообщала версия 4 (поэтому рекомендуется внимательно изучить представленный ниже материал).

Специалисты Lotus отказались от функции **Reporter** (Формирование отчетов) и исключили ее из состава параметров переменной ServerTasks в файле notes.ini сервера. В то же время специалисты не предлагают пользователям самостоятельно заменять ее функцией **Collector** (Сбор данных). Причина в том, что функция **Reporter** обеспечивала только вывод статистических данных и статистических событий, генерировавшихся исполняющим эту функцию сервером, и потому должна была запускаться на всех серверах.

Функция **Collector** (Сбор данных; она же **Statistics Collector** - Сбор статистики) может иницироваться на одном сервере, а собирать статистические данные на других. Нет необходимости иметь эту функцию на каждом сервере. Обычно ее запускают на одном или двух специально выделенных компьютерах. Можно проявить инициативу и добавить параметр collect в переменную ServerTasks файла notes.ini одного или нескольких серверов, которые предназначены для сбора статистических данных с других серверов, хотя в документации Lotus об этом ничего не сказано.

Кроме того, в базе данных Monitoring Results (Мониторинг, файл statrep.nsf) для R6 или базе данных Statistics & Events (Статистические данные и события, файл events4.nsf) для R5, хранящейся на специально выделенном сервере, следует добавить один или

большее число документов набора статистики сервера (Server Statistic Collection document), чтобы функция **Collector** располагала информацией о тех серверах, для которых следует производить сбор статистических данных. В программе Domino Administrator базу данных Monitoring или Statistics & Events можно найти в разделе **Configuration** (Конфигурирование).

Накапливающие данные серверы не должны пытаться собирать статистические данные на серверах, подключенных по медленным соединениям (например, по коммутируемым телефонным линиям). Для этих серверов рекомендуется предусмотреть сбор статистических данных в индивидуальном порядке. Базы данных Statistics Reports (Отчеты по статистическим данным, файл statrep.nsf), хранящиеся на всех серверах домена, реплицируются между серверами, поэтому статистику удастся получить на ближайшем к пользователю сервере.

Обратившись к виду **Alarms and Events** (Аварийные сигналы и события) базы данных Statistics Reports, например с помощью команды **Server => Analysis** (Сервер => Анализ) программы Domino Administrator, легко убедиться в том, что функция **Statistic Monitors** (Мониторинг статистических данных) не обеспечивает формирования документов сигнализации (Alarm document) в рамках версии 5. Однако в R6 не только накапливается статистическая информация, но и регистрируются события. Кроме того, функции контроля **Monitor replication** (Мониторинг репликаций) и **Monitor ACL Changes** (Мониторинг изменения списков управления доступом) больше не информируют пользователей (с помощью сообщений электронной почты) при обнаружении отказов в процессе репликации и при несанкционированных изменениях списков ACL.

Если проверить всю базу данных Statistics & Events, нетрудно заметить, что функция, которая известна в рамках версий 3 и 4 под названием **Monitors** (Мониторинг), теперь получила название **Event Notification** (Уведомление о событиях). К тому же в R6 появился специальный документ Event Notification Method (Метод уведомления о событии), который назначает способ уведомления для определенного обработчика события.

В данном случае специалисты Lotus пришли к логическому разрешению давно назревшей проблемы, касающейся переименования функций. Теперь функции мониторинга (Monitors) не отправляют уведомления о событиях - эта операция передана функции **Event Notification** (Уведомление о событиях). Для получения уведомлений относительно событий (статистических, репликационных или событий безопасности), которые раньше формировались функцией мониторинга, в рамках версий 5 и 6 необходимо активизировать функцию **Event Notification**, поскольку функции **Monitors** в одиночку справиться с такой задачей не удастся.

Любопытно, что причина, по которой компания Lotus отказалась от направления уведомлений посредством функции **Monitors**, так и не была внятно объяснена. В документации версии 5 ясно указано, что функция мониторинга по-прежнему обеспечивает формирование аварийных сигналов (Alarms). Но если это так, то сервер, скорее всего, функционирует некорректно, поскольку функция **Monitors** создает сообщения электронной почты и подобные только в ситуациях, когда требуется обращаться к функции **Event Notification** (Уведомление о событиях). Можно предположить, что в стремлении побыстрее опубликовать версию 5 и не допустить дальнейших проволочек разработчики просто не имели достаточно времени для редактирования документации. В версии R6 прекрасно описаны все компоненты (события, обработчики, виды, документы) функций уведомления о событиях. Однако в любом случае пользователи должны помнить о возможности установки режима уведомления.

Другие новые функции

В версии 5 и 6 появилось большое число новых функций, которые могут оказаться весьма полезными в работе, однако данная глава не может вместить в себя сведения относительно всех нововведений.

Пользователи, несомненно, захотят поближе ознакомиться с функцией **Probes** (Зонды) и способами ее применения. Она позволяет контролировать уровень качества обслуживания на сервере по мере нарастания информационной нагрузки.

Кроме того, удобны функции **Message Tracking** (Отслеживание сообщений) и **Mail Reports** (Подготовка отчетов о почтовых сообщениях), которые помогают получить информацию о действиях пользователя со своей электронной почтой (см. главу 8).

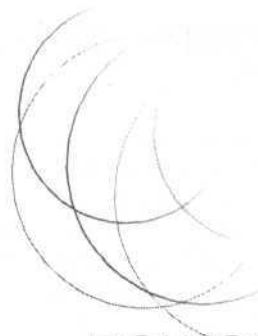
Пользователи, естественно, интересуются функциями, связанными с регистрацией транзакций, наличием кластеров Web-серверов, применением перечня каталогов (отличных от каталога баз данных), а также новыми функциями обеспечения безопасности при работе с сетью Internet и многими другими. Если читатели пропустили главу 1, они могут вернуться к ней, чтобы прочесть об этих функциях. Рекомендуется также ознакомиться с обзорными рекомендациями (Reviewer's Guides), представленными на Web-сайте компании Lotus (www.lotus.com и www.notes.net).

В настоящей главе (равно как и в предшествующих главах) предполагается, что читатели имеют достаточно обширные знания о системе Notes и серверах Domino (поскольку обычно именно администраторы системы версии 4 осуществляют переход на версии 5 и 6). Поэтому цель данной главы заключается в анализе тех нюансов, которые отличают системы Notes R5 и R6 от Notes R4, и привлечении внимания к потенциальным проблемам, тонкостям и возможностям, возникающим в процессе обновления. Здесь опущены подробности настройки большей части функций, поскольку полную информацию по этим вопросам можно найти в исходной документации компании Lotus.

Если сравнивать процедуры установки или обновления сервера Domino 6 и Domino 5, то основное различие состоит в применении для дистрибутива системы формата пакетов MSI установщика Windows Installer (разумеется, речь идет только об операционных системах Windows NT и Windows 2000). Что касается администрирования, то в R6 появились три новые функции: **Smart Upgrade** (Централизованное распространение обновлений клиентских систем), использование политик (хорошо знакомых по операционным системам Windows NT/2000) и клиент Web Administration, дополняющий обычный клиент администрирования Domino Administrator.

ГЛАВА

8



НАСТРОЙКА И ПОДДЕРЖКА ПРОЦЕДУРЫ МАРШРУТИЗАЦИИ ПОЧТОВЫХ СООБЩЕНИЙ

Маршрутизация почтовых сообщений - самая значимая услуга, предоставляемая сервером Domino. В то же время эта служба создает и наибольшее число проблем для администраторов. Маршрутизатор почты представляет собой компонент сервера Domino, который обеспечивает передачу документов между базами данных системы Notes. Процедура репликации также предусматривает подобную пересылку, однако это касается лишь соответствующих реплик баз данных, тогда как процедура маршрутизации предполагает обмен сообщениями между любыми базами. Процедура маршрутизации, реализуемая серверами Domino, создает основу не только для организации электронной почты системы Notes, но и для передачи системой Notes информационных потоков применяемых приложений.

Для администраторов серверов Domino всегда было важно понимать, каким образом выполняется процедура маршрутизации почтовых сообщений, чтобы быть в состоянии оптимально ее осуществлять. Начиная с версии 5 данная процедура превращается в более мощное и одновременно более сложное программное средство. Более мощной она становится потому, что специалисты компании Lotus придали ей возможности маршрутизации почтовых сообщений почтовой службы SMTP и в то же время отказались от агента SMTP Message Transfer Agent (Агент передачи сообщений SMTP). Специалисты также предоставили администраторам дополнительные способы управления процессом маршрутизации почтовых сообщений, например функции предотвращения информационных заторов и задания ограничений на размеры вложений в почтовые сообщения. Однако все эти новые опции, к сожалению, ведут и к усложнению процесса маршрутизации почтовых сообщений.

Маршрутизация почты в версии R6 ничем не отличается от R5, за исключением ввода нового алгоритма сжатия (архивирования) сообщений LZ1, который может заменять применявшийся ранее алгоритм Хаффмана. Следует подчеркнуть, что алгоритм LZ1 не является обязательным и служит для пересылки сжатых сообщений только в операционной среде R6.

В данной главе рассмотрены процедура настройки функции маршрутизации почтовых сообщений, возможности настройки и поддержки совместно используемой почтовой службы и топологии маршрутов, а также оценка производительности этой службы.

Планирование процедуры маршрутизации почтовых сообщений

Для настройки процедуры маршрутизации почтовых сообщений сначала следует принять ряд организационных решений, в частности относительно маршрутов и времени передачи таких сообщений, а уже затем воплощать эти решения в жизнь. В дальнейшем, по мере изменения обстановки или в результате морального старения первоначальных решений, может возникнуть необходимость в изменении характера маршрутизации почтовых сообщений. Решения, связанные с маршрутизацией почтовых сообщений, состоят в определении:

- числа доменов системы Notes и характера взаимосвязей между ними;
 - числа именованных сетей системы Notes и характера взаимосвязей между ними;
 - характера и степени участия домена системы Notes в передаче и приеме почтовых сообщений, которые поступают из других доменов, относящихся или не относящихся к системе Notes, в частности доменов сети Internet;
 - принадлежности к определенному домену и сети системы Notes для каждого сервера, а также объема тех функциональных обязанностей, который он должен выполнять при маршрутизации почтовых сообщений в пределах сети и домена;
 - характера применения функций маршрутизации почтовых сообщений SMTP и NRPC для каждого сервера;
 - для доменов Notes, а также для каждого сервера в отдельности - тех ограничений, которые требуется накладывать на процедуру маршрутизации почтовых сообщений;
 - необходимости применения совместно используемых почтовых служб для каждого сервера;
 - для доменов системы Notes, а также для каждого сервера в отдельности - необходимости введения функции **Message Tracking** (Отслеживание сообщений) и других программных средств мониторинга (контроля).
- >

Большая часть названных проблем обсуждалась в предыдущих главах, остальные рассмотрены в последующих разделах данной главы. Ниже внимание в основном будет сосредоточено на двух вопросах: уяснении взаимосвязей между доменами системы Notes, сетями этой системы и процедурой маршрутизации почтовых сообщений.

Домены системы Notes

Домен системы Notes представляет собой группу серверов, обращающихся к одной и той же базе данных Domino Directory, причем каждый сервер Domino является членом только одного домена системы Notes. Пользователи являются членами того домена, к которому относится соответствующий домашний/почтовый сервер. Необходимо четко определить принадлежность каждого сервера и пользователя на момент их создания. Следует также помнить о том, что перемещение пользователя или сервера из одного домена в другой - дело весьма непростое.

Наличие доменов Notes связано с тем, что серверы, осуществляющие маршрутизацию почтовых сообщений NRPC, не обеспечивают передачу сообщений за границы домена в отсутствие документа соединения (Connection document). В результате имя домена

системы Notes должно так или иначе присутствовать в адресе почтовой службы, причем этот адрес принято задавать в виде почтовый_адрес@домен. Пользователи далеко не всегда обязаны указывать адрес так и в ряде случаев могут ограничиться только компонентом почтовый_адрес. Тогда система Notes сама будет добавлять адреса доменов, чтобы привести к виду почтовый_адрес@домен.

Большинство организаций настраивают все серверы Domino в рамках одного домена. Однако для решения различных административных задач может потребоваться сформировать несколько подобных областей (см. главу 2). Несколько доменов в организации способны образоваться также в результате слияния или поглощения компаний. В этом случае следует планировать маршруты передачи почтовых сообщений между доменами. Кроме того, необходимо проработать маршруты передачи почтовых сообщений между собственными доменами и другими областями системы Notes. И наконец, на практике часто приходится заниматься вопросами взаимосвязи своих доменов с доменами сети Internet.

Именованные сетевые системы Notes

Именованные сетевые системы Notes позволяют задавать маршруты передачи почтовых сообщений в соответствии с характером сетевой топологии. Серверы Domino, принадлежащие к одной и той же сетевой системе Notes, обеспечивают передачу почтовых сообщений друг другу без каких-либо временных задержек и без использования документов соединения (Connection document). А обмен почтовыми сообщениями между серверами Domino, находящимися в различных сетях, происходит только при наличии соответствующих документов соединения.

Если серверы имеют постоянное соединение и применяют один и тот же сетевой протокол (TCP, SPX или NetBEUI), то они, скорее всего, принадлежат к одной и той же сетевой системе Notes. Серверы с различными сетевыми протоколами не могут принадлежать к одной сетевой системе Notes, поскольку используют разные «языки общения». Серверы, связанные с помощью телефонной линии (модем или сеть ISDN), не считаются имеющими постоянное соединение и не могут принадлежать к одной сети. Серверы, связанные между собой с помощью медленного, дорогостоящего или постоянно занятого соединения региональной сети могут относиться к одной и той же сетевой системе Notes, однако их применение далеко не всегда оказывается оправданным. Кроме того, на практике имеются причины, помимо необходимости маршрутизации почтовых сообщений, для формирования множества небольших по размеру сетей системы Notes, причем даже в том случае, когда на первый взгляд кажется, что одной большой именованной сетью вполне достаточно (см. главу 2).

Серверы Domino могут иметь несколько сетевых протоколов и несколько сетевых портов, предназначенных для работы с одним или более протоколами. Такие серверы должны находиться в разных именованных сетях Notes. Вопросы, связанные с установкой сетевых протоколов и способов добавления, переименования и удаления сетевых портов серверов Domino, подробно обсуждались в главах 3 и 4.

Для каждого используемого порта сервер Domino приписывается к определенной сети, что обеспечивается на виде **Server/Networks** (Сервер/сети) базы данных Domino Directory. Характер работы портов и соответствующих именованных сетей сервером можно проследить на вкладке **Ports => Notes Network Ports** (Порты => Сетевые порты системы Notes) в документе сервера (Server document).

Для каждого заданного порта можно переносить сервер из одной сети в другую путем изменения в документе сервера записи в поле **Notes Network** (Сеть системы Notes) для этого порта.

При установке сервер Domino получает имена по умолчанию для каждого разрешенного к применению порта. На практике, однако, не рекомендуется выбирать имена, которые присваиваются в режиме по умолчанию, поскольку в дальнейшем придется менять их на другие. Проблема, связанная с употреблением имен, которые задаются системой Notes по умолчанию, состоит в том, что серверы по ошибке могут оказаться отнесенными к одной и той же сети системы, что совершенно недопустимо. В результате нарушится передача почтовых сообщений.

Например, серверы, связанные только с помощью телефонной линии связи, могут быть по ошибке отнесены к одной сети системы Notes. При этом они будут многократно и безрезультатно пытаться установить связь друг с другом с помощью несуществующего сетевого соединения и станут использовать телефонное соединение только по истечении весьма заметного временного интервала.

Если ни один из серверов не удален от других, такая проблема не обязательно возникнет. Однако при необходимости работать с удаленными серверами она может нивелировать все прочие усилия администраторов. Поэтому пользователям настоятельно рекомендуется присваивать портам другие имена, соответствующие именам эксплуатируемых сетей системы Notes.

Осуществление маршрутизации почтовых сообщений серверами Domino

Еще совсем недавно, в версии 4, механизмы маршрутизации почтовых сообщений серверами Domino были весьма простыми: между пользователями почтовой службы системы Notes предусматривалось применение почтовых маршрутизаторов сервера Domino. Начиная с версии R5 маршрутизатор передает сообщения посредством протокола (функции) NRPC, или Notes RPC (Notes Remote Procedure Call – удаленный вызов процедур системы Notes). Для пересылки почтовых сообщений пользователям почтовой службы других систем (отличных от системы Notes) или пользователям Internet предусматривается применение агента Lotus MTA (Message Transfer Agent – агент пересылки сообщений), также разработанного специалистами компании Lotus, или стороннего шлюза.

Начиная с версии 5, возможности системы Notes заметно расширяются, поскольку специалисты компании Lotus добавили в маршрутизатор функцию передачи почтовых сообщений SMTP. Это заметно усложняет процесс настройки маршрутизации, поскольку теперь приходится определять характер использования протокола SMTP для передачи почтовых сообщений системы Notes (наряду с применением функции NRPC). В серверах Domino версии 5 или 6 появляется возможность выбирать следующие варианты:

- О активизация функции NRPC для передачи почтовых сообщений пользователям системы Notes и протокола SMTP для передачи почтовых сообщений пользователям сети Internet. Подобный вариант обеспечивался и в рамках предшествующих версий системы Notes/Domino;

- О применение протокола SMTP для передачи почтовых сообщений всем пользователям (системы Notes и других систем) - только в случае использования сервера Domino R5 или R6 и сетевого стека TCP/IP;
- О совместное использование NRPC и SMTP для маршрутизации почтовых сообщений при автоматическом выборе подходящего варианта.

Третий вариант, естественно, оказывается наиболее сложным. В этом случае допустимо воспользоваться параметрами режима по умолчанию, однако это далеко не всегда обеспечивает оптимальный выбор характеристик сервера Domino. И, как упоминалось выше, задаваемая по умолчанию именованная сеть потенциально может привести к нарушениям в маршрутизации почтовых сообщений.

Для лучшего понимания установки маршрутизации почтовых сообщений в серверах Domino следует подробнее с ними познакомиться (это касается как функций маршрутизации системы Notes, так и применения протокола SMTP). Затем нужно разобраться в вопросах одновременного использования этих функций сервером Domino, что, конечно же, является более сложной задачей.

Маршрутизация почтовых сообщений по протоколу NRPC

Ниже описаны процедуры, с помощью которых функция NRPC обеспечивает передачу почтовых сообщений:

1. Пользователь (программа или агент) может адресовать документ одному или нескольким получателям (адресатам) и после этого инициировать передачу сообщения. Процесс пересылки предусматривает занесение документа в базу данных Outgoing Mail (Исходящие почтовые сообщения), хранящуюся на всех серверах Domino, управляющую работой маршрутизатора и представленную файлом mailbox:
 - начиная с версии 5 сервер может взаимодействовать с несколькими базами данных Outgoing Mail. В этом случае им ставятся в соответствие файлы mainn.box, где n - целое число. Например, при наличии двух баз данных Outgoing Mail на одном сервере файлы будут иметь имена mail1.box и mail2.box;
 - мобильный пользователь, работающий в режиме отключения от сервера, может заносить документ в локальную базу данных Outgoing Mail. В дальнейшем при восстановлении соединения с сервером и вводе соответствующей команды системы Notes передаст этот документ в базу данных Outgoing Mail сервера. Пользователь считается работающим в режиме отключения, если в поле **Mail file location** (Местоположение файла почтовых сообщений) документа местоположения задается вариант **Local** (Локально);
 - при пересылке сообщения пользователем система Notes будет перед занесением сообщения в базу данных Outgoing Mail пытаться проверить адрес для тех получателей, имена которых не содержат имени домена. Если система Notes не может обнаружить документ группы (Group document) или персональный документ (Personal document) адресата, она будет направлять запрос пользователю и просить его скорректировать имя или исключить адресата из перечня адресатов.
2. После этого маршрутизатор почтовых сообщений, который является загружаемой/незагружаемой серверной задачей Domino, проверяет локальные базы данных

Outgoing Mail. При обнаружении сообщения в одной из подобных баз данных маршрутизатор читает имена адресатов, а потом обращается к документам в базе данных Domino Directory для определения своих последующих действий.

3. Затем маршрутизатор почтовых сообщений формирует для каждого адресата (абонента) копию сообщения, при этом возможны нижеперечисленные варианты:
 - если база данных почтовой службы абонента расположена на текущем сервере, маршрутизатор направляет сообщение непосредственно туда. Если почтовая служба используется совместно, маршрутизатор может передавать сообщение в базу данных почтовой службы абонента только частично, сохраняя оставшуюся часть в общей базе данных (см. ниже). На этом шаге маршрутизатор может преобразовывать формат сообщения, например из расширенного текстового формата системы Notes в формат MIME и наоборот, в зависимости от значения параметров, присутствующих в персональном документе абонента. После выполнения описанных операций процедура маршрутизации считается завершенной;
 - если база данных почтовой службы абонента располагается на другом сервере Domino, маршрутизатор определяет путь (маршрут) к серверу, после чего передает сообщение в базу данных Outgoing Mail первого сервера маршрута. Если сообщение представлено в формате MIME, а у адресата используется сервер R4 или более ранняя версия системы, маршрутизатор преобразует формат сообщения в расширенный текстовый формат системы Notes. Маршрутизатор принимающего сообщения сервера повторяет процесс маршрутизации и направляет сообщение в базу данных адресата (если она расположена на этом сервере) или на следующий сервер маршрута;
 - если адресат расположен вне домена сети Notes, маршрутизатор почтовых сообщений определит путь к серверу Domino, служащему в качестве почтового шлюза для почтовой системы абонента, после чего перешлет сообщение на первый сервер маршрута. Шлюз (граничный шлюзовой сервер) в свою очередь будет передавать сообщение в следующую систему почтовой связи. Маршрутизатор почтовых сообщений может судить о необходимости передачи почтовых сообщений в другую систему почтовой связи по формату адреса абонента или по данным его персонального документа (при наличии этого документа);
 - если по какой-либо причине сервер не обеспечивает передачи сообщения, он может попытаться вернуть его отправителю и добавить запись в базу данных Delivery Failure Report (Отчеты об отказах при пересылке почтовых сообщений). Эти действия могут выполняться незамедлительно или по истечении 24 часов;
 - незамедлительный возврат сообщения инициируется маршрутизатором в том случае, когда ему не удастся отыскать путь к адресату или же кратчайший маршрут превышает заданное максимальное число промежуточных участков;
 - возврат сообщения по истечении 24 часов предусматривается при условии, что требуемые маршруты существуют, но сервер не в состоянии корректно передать сообщение на первый сервер одного из этих маршрутов в течение 24 часов. Тогда маршрутизатор инициирует возврат сообщения отправителю. Путь считается корректным, если он не превышает по длине максимального числа промежуточных участков. По умолчанию максимальное число таких участков равно 25, однако для серверов версии 5 и 6 можно изменять это число в поле **Maximum hop count** (Максимальное число переходов) в документе конфигурации (Configuration document).

Данное поле находится ниже **Router/SMTP => Restrictions** (Маршрутизатор SMTP=> Ограничения) и **Controls => Transfer Controls** (Управление => Задача управления);

- если по какой-либо причине сервер не имеет возможности доставить сообщение ни адресату, ни отправителю, он присваивает сообщению статус **Dead** (Потерянное) и оставляет его в базе данных Outgoing Mail (Исходящие почтовые сообщения). После этого администратор должен решить, что делать с подобным сообщением. Следует также отметить, что сервер способен принять подобное решение незамедлительно или подождать 24 часа (в этом случае используются те же критерии, что и в предшествующем разделе).

Роль системы Notes

При необходимости направления почтового сообщения пользователем системы Notes эта система должна решать следующие задачи:

- О заменять любые имена локальных групп именами их членов. Система получает требуемые имена из документов локальных групп, которые она находит в базе данных Personal Address Book или других локальных каталогах. Если пользователь выбирает имена групп, заданные сервером, системе Notes не приходится расширять их до имен членов групп;
- О проверять все адреса за исключением тех, которые содержат имя домена (например, в виде адресат@домен). При этом система Notes просматривает параметры в текущем документе местоположения (Location document), принимает решение относительно применения подобных компонентов и руководствуется несколькими общими правилами:
 - если в поле **Mail file location** задается вариант **Local**, а для поля **Mail addressing** (Адресация почтовых сообщений) - вариант **Only Local** (Только локально), система Notes будет проверять те имена, которые она сможет обнаружить в соответствующих документах базы данных Personal Address Book. Если система не в состоянии проверить имя, она формирует соответствующее сообщение, но в то же время сохраняет адрес без изменения. Если в дальнейшем системе не удастся идентифицировать некорректный адрес, сервер будет возвращать копию такого сообщения пользователю и одновременно заносить запись в базу данных Delivery Failure Report (Отчеты об отказах при доставке сообщений);
 - если в поле **Mail file location** задан вариант **Server** (Сервер) или в поле **Mail addressing** - вариант **Local and Server** (Локально и сервер), система Notes сначала проверит базу данных Personal Address Book и другие локальные каталоги, указанные в поле **User Preferences** (Предпочтения пользователя), а затем каталоги, хранящиеся на сервере. Это может быть база данных Domino Directory, база данных Directory Catalog и другие каталоги, перечисленные в базе данных Directory Assistance (Поддержка каталога). В этом режиме система Notes будет производить проверку всех адресов. Если системе не удастся проверить адрес в процессе просмотра каталога, она предоставит пользователю возможность исключить этот адрес из соответствующих полей адреса или исправить имя вручную;
- О для каждого адресата формат сообщений задается в виде расширенного текстового формата системы Notes или формата MIME (только для версий R5 и R6). Система

Notes предусматривает применение расширенного текстового формата для сообщений, направляемых пользователям системы, а формат MIME - для сообщений пользователям сети Internet. По формату сообщения система всегда в состоянии сделать вывод относительно местоположения пользователя;

- О если отправляющий сообщение пользователь выбирает вариант с подписью и/или шифрованием сообщений, система Notes задействует стандартные открытые и закрытые ключи для шифрования его данных. Система Notes версии 5 и 6 предусматривает применение открытых и закрытых ключей (если они доступны) стандарта X.509 для тех абонентов, которые являются пользователями почтовой службы сети Internet. В тех случаях, когда нет возможности воспользоваться для шифрования открытым ключом абонента (например, по причине временного отключения пользователя от сервера Domino), системы Notes R5 и R6 будут маркировать сообщение таким образом, чтобы сервер почтовой службы отправителя зашифровал сообщение сразу по его получении;
- О направлять сообщение на сервер почтовой службы. Если для поля **Mail file location** текущего документа местоположения задан вариант **on Server** (На сервере), система Notes постарается сформировать соединение с сервером почтовой службы, указанным в поле **Home/mail server** (Домашний/почтовый сервер), и занесет сообщение в базу данных Outgoing Mail этого сервера. Если для поля **Mail file location** текущего документа местоположения указан вариант **Local**, система Notes будет заносить сообщение в локальную базу данных Outgoing Mail. В дальнейшем пользователь сможет переслать сообщение на сервер. Если сообщение все еще остается в базе данных Outgoing Mail на момент выхода из клиента Notes или изменения местоположения пользователя, система Notes напомнит о том, что в базе данных Outgoing Mail остались ожидающие отправки сообщения, и предложит передать их на сервер.

Роль клиентов других почтовых служб

Клиенты других почтовых служб, поддерживаемых сервером Domino (например, IMAP, POP3 и HTTP), выполняют точно такие же операции, как и клиенты системы Notes. Конечно, не каждый из этих клиентов оказывается способным решать все задачи, например зашифровать или подписывать почтовые сообщения.

Основное различие между клиентами системы Notes и другими клиентами состоит в том, что первые обеспечивают взаимодействие с сервером базы данных (Database server), при занесении сообщений в базу данных Outgoing Mail, а другие клиенты подобного взаимодействия не обеспечивают. С другой стороны, клиенты почтовых служб POP3 и IMAP взаимодействуют с задачей SMTP Listener (Контроль SMTP), а клиенты HTTP - с задачей HTTP. Поэтому, если такая задача не исполняется сервером, сервер не сможет принять почту от соответствующего клиента.

Роль базы данных Domino Directory

Маршрутизатор почтовых сообщений в процессе маршрутизации обычно использует многочисленные документы из каталога Domino Directory и просто не может обойтись без них. Перечислим хранящиеся в базе данных Domino Directory документы, предоставляющие данные маршрутизатору:

- О персональный документ (если сообщение направлено человеку), документ базы данных Mail-In Database (база данных входящих почтовых сообщений, если адресатом является база данных) и документ ресурса (если адресатом является ресурс, например помещение для проведения конференций). Эти документы требуются для определения местоположения и имени базы данных почтовой службы абонента. При необходимости с их помощью можно получить открытые ключи абонента, чтобы зашифровать исходящие сообщения. Поля, содержащие записи о местоположении: **Domain**, **Mail server** (Домен, сервер почтовой службы) и **Mail file** (Файл почтовых сообщений). Если пользователь не применяет почтовую службу системы Notes, его персональный документ не включает подобных сведений, однако в документе присутствуют аналогичные поля, записи которых указывают на ту систему почтовой связи, которой отдает предпочтение пользователь;
- О документ группы (Group document). Если адресат представляет собой группу, сервер имеет возможность получить имена индивидуальных абонентов из документа , группы;
- О документ сервера (Server document). Наличие этих документов позволяет определить принадлежность серверов к конкретным именованным сетям;
- О документ соединения (Connection document) и домена (Domain document). Такие документы позволяют выявлять маршруты к серверу почтовой службы адресата;
- О документ конфигурации (Configuration document). Этот документ определяет используемые правила и ограничения для маршрутизации почтовых сообщений. Кроме того, в рамках версии 5 и 6 такие документы выявляют необходимость в применении традиционных способов маршрутизации почтовых сообщений или протокола SMTP.

Сценарии маршрутизации почтовых сообщений сервером Domino

Сервер почтовой службы определяет адресата для каждого сообщения, выбирает оптимальный путь до него и пересылает сообщение по этому маршруту. Данные адресата обычно содержат имя базы данных почтовой службы абонента, имя сервера почтовой службы, на котором хранится эта база данных, а также имя домена Domino, к которому относится сервер почтовой службы. Вся информация находится в персональном документе пользователя, базе данных входящих почтовых сообщений (Mail-In Database) или документе ресурса (Resource document) при его наличии. Для адресатов других доменов Domino или внешних систем почтовой службы маршрутизатор может не иметь доступа к подобным документам. В таких случаях маршрутизатор выделяет сведения о домене адресата из самого адреса.

Для маршрутизатора почтовых сообщений, которому требуется переслать письмо, допустимы следующие сценарии направления сообщения:

- О в базу данных того же самого сервера;
- О другому серверу Domino той же именованной сети;
- О на сервер Domino другой именованной сети;
- О на сервер Domino соседнего домена Domino;
- О в соседний домен Domino, который в свою очередь перешлет сообщение в другой домен, соседний по отношению ко второму (но не к исходному) домену;

- во внешнюю систему почтовой связи, не отвечающую стандартам системы Notes или сети Internet;
- в сеть Internet.

Случаи использования документов соединения и домена

Перечисленные выше сценарии будут подробно рассмотрены в дальнейшем, но сначала следует подвести итог и сформулировать требования, предъявляемые к документам соединения и домена:

- если маршрутизатор почтовых сообщений должен передать сообщение в базу данных того же самого сервера или отправить его на другой сервер в этой же именованной сети, он может при выполнении данных действий обойтись без документа соединения;
 - все остальные сценарии предполагают применение документа соединения для поддержки передачи почтовых сообщений;
- 1Q почтовые сообщения могут передаваться в другие домены Domino, расположенные непосредственно по соседству или вдалеке от исходного домена, без помощи документа домена. Единственное требование в данном случае связано с наличием соответствующих документов соединения, позволяющих определить маршрут передачи сообщений к серверу другого домена. Документы соседнего домена (Adjacent Domain document) и удаленного домена (Non-adjacent Domain document) позволяют ограничить передачу определенных сообщений в другие домены. Кроме того, документы удаленного домена могут использоваться при определении маршрутизатором почтовых сообщений пути через промежуточные домены;
- для передачи почтовых сообщений в домен не-Domino (например, в домен сети Internet или домен сторонней почтовой службы) требуется в обязательном порядке применение как документов соединения, так и документов домена.

Маршрутизация сообщений сервером Domino

Маршрутизация почтовых сообщений может проводиться немедленно или по расписанию - в зависимости от таких факторов, как адрес доставки сообщения, приоритет передачи и число отложенных сообщений в базе данных Outgoing Mail. При маршрутизации сервер пользуется следующими правилами:

- всегда незамедлительно передаются почтовые сообщения, предназначенные для базы данных, которая относится к тому же серверу, что и маршрутизатор;
- если следующий участок на пути доставки является сервером той же именованной сети, маршрутизатор обеспечивает незамедлительную передачу почтовых сообщений с нормальным или высоким уровнем приоритета. Отправка сообщений с низким уровнем приоритета также выполняется немедленно, но только в часы наименьшей нагрузки сервера (время с низким приоритетом);
- почтовые сообщения, имеющие высокий приоритет **Delivery** (Доставка), передаются немедленно;
- в ситуациях, когда требуется применение документа соединения, почтовые сообщения с нормальным уровнем приоритета (задается в режиме по умолчанию) отправляются в соответствии с расписанием, заданным в конкретном документе соединения;

- О маршрутизатор передает отложенные сообщения с нормальным уровнем приоритета, как только их число достигает значения, указанного в поле **Route at once if ... message pending** (Отправка разом по достижении ... отложенных сообщений) соответствующего документа соединения;
- О почтовые сообщения с низким уровнем приоритета передаются на другие серверы только при наступлении времени доставки почты с низким приоритетом. По умолчанию это время между полуночью и шестью часами утра. В этом временном интервале правила для почтовых сообщений с высоким уровнем приоритета действуют также и на сообщения с низким уровнем приоритета;
- О можно изменить часы доставки почтовых сообщений с низким уровнем приоритета в поле **Low priority mail routing time range** (Временной интервал маршрутизации почтовых сообщений с низким приоритетом) соответствующего документа конфигурации (Configuration document). К этому полю можно обратиться командой **Messaging Settings** (Параметры режима передачи сообщений) или **Router/SMTP** (Маршрутизатор SMTP), а затем выполнить **Restrictions and Controls => Transfer Controls** (Ограничения и управление => Управление передачей сообщений).

Доставка сообщений в базу данных на том же сервере

Этот сценарий является наиболее простым и понятным из всех описанных ниже. Он предусматривает направление сообщения в базу данных Outgoing Mail, причем маршрутизатор проверит соответствующий документ (Person, Mail-In Database или Resource), обнаружит, что доставка происходит на тот же самый сервер, и незамедлительно передаст сообщение в базу данных почтовой службы абонента без привлечения документов соединения и домена (рис. 8.1).

Доставка сообщений на другой сервер Domino той же именованной сети

Данный сценарий также достаточно прост для понимания и реализации. Сообщение адресуется пользователю, сервер почтовой службы которого относится к той же именованной сети, что и сервер маршрутизатора (рис. 8.2).

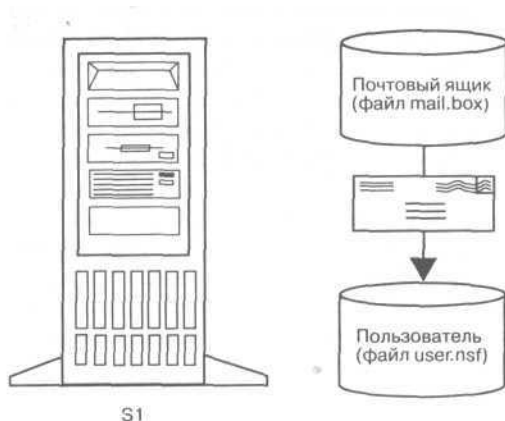


Рис. 8.1. Если база данных адресата располагается на том же сервере, маршрутизатор немедленно доставит туда сообщение



Рис. 8.2. Сервер S1 располагает сообщением, адресованном пользователю сервера S2. Начинается немедленная доставка сообщения с сервера S1 на сервер S2 без привлечения документа соединения

Маршрутизатор будет передавать сообщение на сервер S2 незамедлительно без использования документов соединения и домена, причем сообщение попадет в базу данных Outgoing Mail сервера S2, а сервер S2 в свою очередь перешлет это сообщение в базу данных почтовой службы абонента.

Следует отметить, что серверы располагают информацией о членстве в именованной сети домена Domino, поскольку соответствующие данные хранятся непосредственно на каждом сервере в документе сервера (Server document). Нужная информация находится в разделе **Ports => Notes Network Ports** (Порты => Сетевые порты системы Notes) столбца **Notes Network** (Сети системы Notes). При первом запуске сервер формирует в своей памяти таблицу маршрутизации на основе имеющихся документов сервера, соединения и домена, хранящихся в каталоге Domain Directory, а в процессе работы модифицирует ее, чтобы учесть все изменения, дополнения и коррективы, которые вносятся в эти документы.

Доставка сообщения через общий сервер в другой именованной сети

В этом случае сообщение от сервера S1 адресуется абоненту, база данных почтовой службы которого хранится на сервере S3, относящемся к другой сети. Так, в данном случае сервер S1 находится в сети Marsh Creek TCP, а сервер S3 - в сети Marsh Creek SPX. Эти серверы не могут взаимодействовать напрямую, поскольку используют различные сетевые протоколы (соответственно TCP и SPX). Сервер S2 поддерживает несколько сетевых протоколов (в том числе и указанные) и относится к обоим рассматриваемым именованным сетям (рис. 8.3).

Сервер S1 пошлет сообщение серверу S2 незамедлительно и не будет обращаться к документам соединения и домена, поскольку оба сервера находятся в одной именованной сети Marsh Creek TCP. Сервер S2 в свою очередь передаст сообщение серверу S3 (также незамедлительно) без помощи документов соединения, поскольку эти серверы из одной именованной сети Marsh Creek SPX. На заключительном этапе сервер S3 доставит сообщение абоненту.

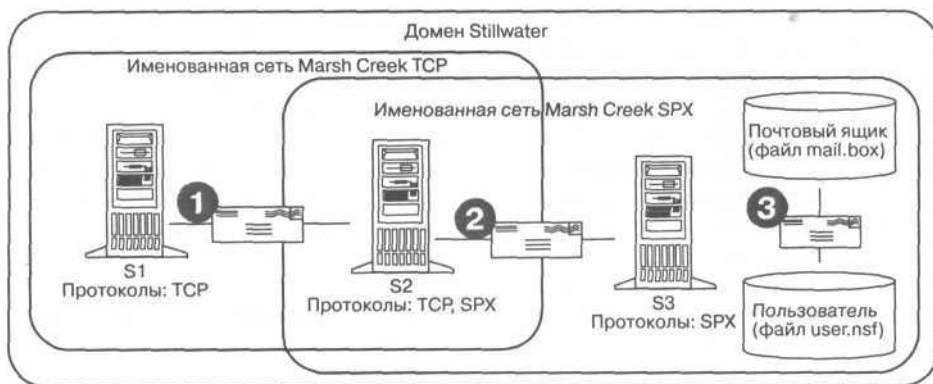


Рис. 8.3. Если сервер S1 направляет сообщение пользователю сервера S3, но не имеет возможности передать его непосредственно, сообщение доставляется на сервер S2, который пересылает его серверу S3, не прибегая к документам соединения

Доставка сообщений между двумя именованными сетями, не имеющими общего сервера

Если сервер почтовой службы адресата располагается не в сети исходного сервера и эти сети не имеют общего сервера, при передаче сообщений может потребоваться один или больше документов соединения, описывающих маршрут между серверами именованных сетей. На рис. 8.4 серверы S1 и S2 относятся к сети Marsh Creek TCP, а серверы S3 и S4 принадлежат к сети Philly TCP.

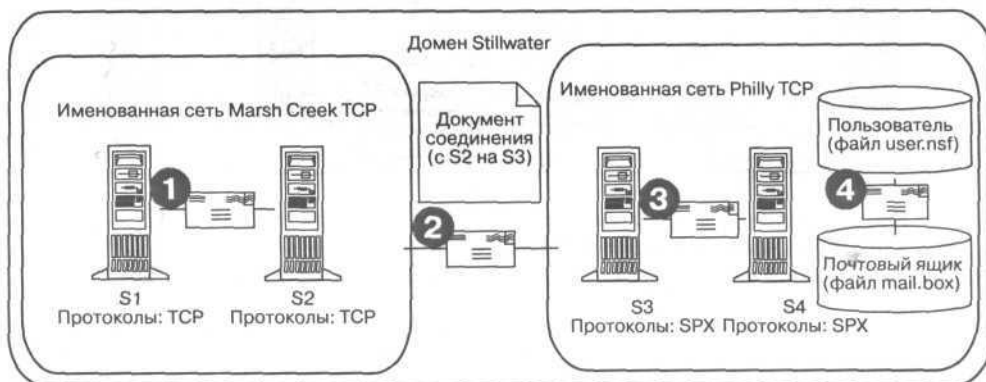


Рис. 8.4. Серверу S2 требуется документ соединения для направления почтовых сообщений на сервер S3. При наличии подобного документа серверы S1 и S2 получают возможность взаимодействовать с серверами S3 и S4

Для передачи почтовых сообщений в этом случае обязательно следует использовать документ соединения (Connection document). В примере, показанном на рис. 8.4, документ соединения информирует систему о том, каким образом сервер S2 подключается к серверу S3, когда следует инициировать соединение и сколько сообщений необходимо накопить перед началом передачи. При наличии документа соединения сервер S1 получит возможность пересылать почтовые сообщения на сервер S4 путем первоначальной передачи на сервер S2, затем на сервер S3 и на заключительной стадии собственно на сервер S4.

Однако серверы сети Philly TCP не обеспечивают пересылку почтовых сообщений на серверы сети Marsh Creek TCP. Чтобы осуществить такую передачу, приходится создавать еще один документ соединения, извещающий систему о том, каким образом и когда сервер сети Philly TCP (например, S3) должен соединяться с серверами сети Marsh Creek TCP (например, с сервером S2).

Отправка почтовых сообщений в другие домены Domino

Для пересылки почтовых сообщений в другие домены Domino необходимо сначала создать документы соединения (как для связи между именованными сетями в предыдущем случае). Например, при пересылке данных непосредственно из домена Stillwater в домен PlanetNotes требуется документ соединения в каталоге домена Stillwater, определяющий маршрут между сервером почтовой службы домена Stillwater и сервером почтовой службы домена PlanetNotes. Если подобные сообщения необходимо передавать и в обратном направлении, должен создаваться документ соединения, описывающий подключение сервера из домена PlanetNotes к серверу в домене Stillwater. Обычно одна и та же пара серверов обеспечивает передачу сообщений в обоих направлениях (рис. 8.5).

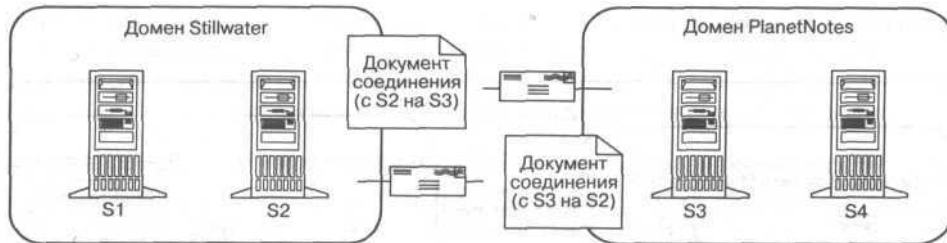


Рис. 8.5. Наличие документа соединения позволяет передавать почтовые сообщения из домена Stillwater в домен PlanetNotes. Наличие второго документа соединения дает возможность пересылать почтовые сообщения в обратном направлении

Конечно, при наличии двух доменов Domino взаимосвязи оказываются простыми, а создание документов соединения не вызывает особых проблем. Однако с увеличением числа доменов ситуация заметно усложняется. Так, при наличии трех доменов может отсутствовать документ соединения для пересылки почтовых сообщений между серверами любых двух доменов, поэтому придется выполнять доставку через промежуточный домен. На рис. 8.6 проиллюстрирована ситуация с тремя доменами, когда пары доменов Stillwater и PlanetNotes, а также PlanetNotes и Raptor имеют по одному документу соединения, что позволяет посылать сообщения из домена Stillwater в домен Raptor.

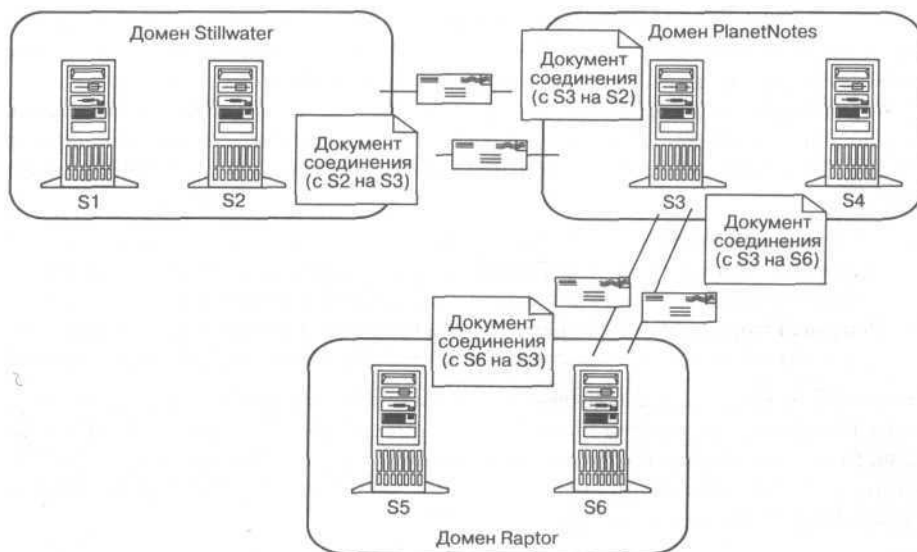


Рис. 8.6. Почтовые сообщения, пересылаемые из домена Stillwater, адресуются абоненту домена Raptor (или наоборот) и могут передаваться с привлечением домена PlanetNotes

Так, сообщение сервера S2 на адрес Joe Doaks@Raptor нельзя отправить, поскольку в домене Stillwater не существует документов соединения, которые проинформировали бы систему о маршруте к домену Raptor. Однако сообщение с адресом Joe Doaks@Raptor@PlanetNotes удастся послать, так как сервер S2 может быть соединен с сервером S3 в домене PlanetNotes, а сервер S3 в свою очередь - с сервером S6 в домене Raptor.

Конечно, пользователи никогда не применяют адресов типа Joe Doaks@Raptor@PlanetNotes, но администратору домена Stillwater ничто не мешает предусмотреть это и выполнить необходимые действия. Например, он вправе создать документ несмежного домена (Non-adjacent domain document), который будет уведомлять систему о том, что любое почтовое сообщение, адресованное в домен Raptor, должно быть послано через домен PlanetNotes. После создания подобного документа пользователи домена Stillwater смогут указывать адрес в виде Joe Doaks@Raptor.

Кроме того, если три домена связаны между собой (а так часто и бывает на практике), они способны совместно использовать каталоги всех доменов. В этом случае любым из трех способов администраторы могут предварительно подготавливать каталоги так, чтобы пользователям было достаточно ввести адрес в виде Joe Doaks. Указанные способы предусматривают использование каскадных адресных книг (правда, такой метод морально устарел), поддержку каталогов и применение перечня каталогов (см. главу 11).

Тот факт, что можно передавать почтовые сообщения из одного домена в другой с помощью третьего домена, в ряде случаев создает проблемы для самих администраторов. Так, для передачи необходима дорогостоящая полоса пропускания, и не исключено, что администратор в промежуточном домене своевременно не выделит ее для сквозной пересылки почты. Кроме того, промежуточный домен должен оплачивать отправку почтовых сообщений в третий домен. Однако администратор домена PlanetNotes вряд ли будет в восторге,

если пользователи домена Stillwater начнут направлять почтовые сообщения с помощью домена PlanetNotes в общественный домен CompuServe, когда за эти соединения домену PlanetNotes придется платить службе CompuServe поминутно.

Для предотвращения подобных ситуаций создаваемые документы домена позволяют ограничить типы сообщений, которые допускается передавать через промежуточные домены. Большая часть документов доменов имеет два поля для задания соответствующих параметров:

- **Allow mail only from domains** (Разрешение на прием почтовых сообщений только из указанных доменов) - сервер Domino пропускает через домен только те почтовые сообщения, имена доменов которых оговариваются в данном поле;
- **Deny mail from domains** (Запрет на прием сообщений из доменов) - сервер Domino не принимает сообщения, которые поступают из доменов, указанных в данном поле.

На рис. 8.7 изображено, как почтовые сообщения могут передаваться из домена Stillwater в домен PlanetNotes, из домена PlanetNotes в домен Raptor и из домена Raptor в домен Firesign (а также в противоположном направлении). Администратор домена PlanetNotes хочет предотвратить пересылку пользователями домена Stillwater почтовых сообщений через домен PlanetNotes в домены Raptor и Firesign.

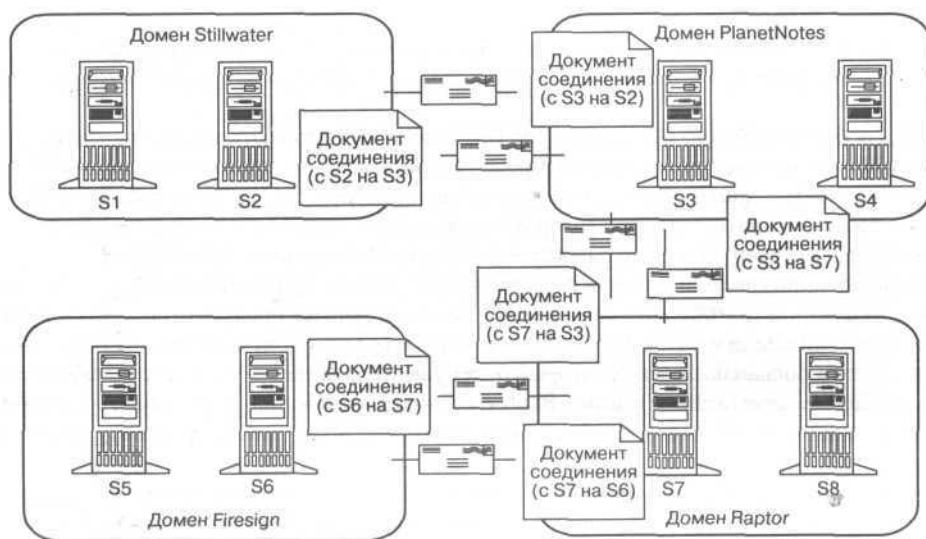


Рис. 8.7. Почтовые сообщения из домена Stillwater в домен Firesign могут доставляться через домены PlanetNotes и Raptor

На практике администратор имеет возможность выполнить следующие действия:

- если в домене PlanetNotes создан документ несмежного домена (Non-adjacent Domain document) для домена Firesign, который содержит запись типа **Route mail addressed to Firesign via Raptor** (Маршрутизация почтовых сообщений, адресованных домену Firesign через домен Raptor), администратор может добавить имя Stillwater в поле **Deny mail from domains** (Запрет на передачу почтовых сообщений из доменов). В результате

- будут блокироваться почтовые сообщения, поступающие из домена Stillwater и имеющие адреса типа Ralph Spoilsport@Firesign или Ralph Spoilsport@Firesign@PlanetNotes;
- О сформировать документ смежного домена (Adjacent Domain document), указывающий на домен Raptor как на соседний, и внести имя Stillwater в поле **Deny mail from domains**. Это позволит заблокировать почтовые сообщения, приходящие из домена Stillwater с адресами типа Ralph Spoilsport@Firesign@Raptor@PlanetNotes. Одновременно будут блокироваться почтовые сообщения с такими адресами, как Joe Doaks@Raptor и Joe Doaks@Raptor@PlanetNotes.

Совместное применение этих подходов обеспечивает передачу почтовых сообщений домена Stillwater в домен PlanetNotes и блокировку сообщений, предназначенных для других доменов. При этом маршрутизатор домена PlanetNotes будет возвращать письма отправителям и заносить в базу данных Delivery Failure Report (Отчеты об отказах при доставке сообщений) запись, информирующую об отсутствии маршрута для пересылки сообщений из домена PlanetNotes в домен х.

Возникает вопрос, почему документ несмежного домена не может послужить для блокирования почтовых сообщений домена Stillwater с адресами типа Ralph Spoilsport@Firesign@Raptor@PlanetNotes. Причина в данном случае состоит в том, что необходимо явно указать имена всех доменов по пути следования сообщения. В отличие от других адресов, здесь не применяется документ несмежного домена, поэтому маршрутизатор домена PlanetNotes не привлекает к формированию маршрута документ несмежного домена и не просматривает его поле.

Отправка почтовых сообщений внешней системе почтовой связи

Если адресат располагается во внешней системе почтовой связи, не относящейся к домену Domino, следует выделять по крайней мере один шлюз на основе одного из серверов Domino. Компьютер будет исполнять роль шлюза, обеспечивающего пересылку почтовых сообщений во внешнюю систему почтовой связи и обратно. Перечень документов, которые потребуются для передачи сообщений с помощью шлюза (граничного шлюзового сервера), будет зависеть от типа сервера. В общем случае для этих целей могут понадобиться следующие документы:

- О документ соединения (Connection document), который должен задавать тип соединения между сервером Domino (шлюзом) и компьютером внешней системы, обеспечивающим прием почтовых сообщений для пользователей. Подобный документ может быть специальным и добавляться в виде отдельной формы в базу данных Domino Directory самим шлюзовым сервером;
- О один или несколько документов домена (Domain document), которые должны содержать данные о внешнем домене. В частности, в подобный документ должно входить имя этого домена, которое могли бы применять пользователи системы Notes при адресации почтовых сообщений во внешнюю систему. Например, систему почтовой службы cc:Mail домена Stillwater допустимо назвать Stillwater ccmail, при этом пользователи обращались бы к ней с помощью адреса C.C.Rider@Stillwater ccmail.

Отправка почтовых сообщений в сеть Internet

Поскольку серверы Domino версии 5 и 6 могут использоваться в качестве хостов SMTP, каждый подобный сервер способен выступать в качестве шлюза SMTP для тех доменов Domino, которые имеют обыкновение направлять почтовые сообщения во внешние сети.

Разрешается также применять сервер R4 с агентом SMTP MTA (см. раздел в конце данной главы).

Топологии маршрутизации почтовых сообщений по протоколу NRPC

В компаниях, располагающих большим числом именованных сетей или доменов Domino, может потребоваться тем или иным образом оптимизировать топологию маршрутизации почтовых сообщений, например посредством концентратора. Если сетей или доменов больше четырех, то минимизировать число документов соединения, а также число проходимых участков допустимо за счет *концентратора почтовой службы*. Если подобный концентратор является членом одной или нескольких сетей, число создаваемых документов соединения существенно уменьшится. Для большей наглядности можно сравнить рис. 8.7 и 8.8, причем безразлично, используются именованные сети или домены (принцип в данном случае остается тем же самым).

На рис. 8.7 домены связаны последовательно, при этом требуется шесть соединений, а для связи между конечными доменами нужно пройти три участка. На рис. 8.8 показана структура с концентратором, роль которого играет домен PlanetNotes. Здесь также предусмотрено шесть соединений, однако для любых двух доменов число проходимых участков не превышает двух. На рис. 8.7 к структуре может быть добавлена еще одна пара соединений, обеспечивающая связь между серверами S2 и S6. Это приводит к формированию *кольцевой топологии*, в которой отсутствуют конечные домены, число участков сокращается до двух, но в то же время требуется восемь документов соединения.

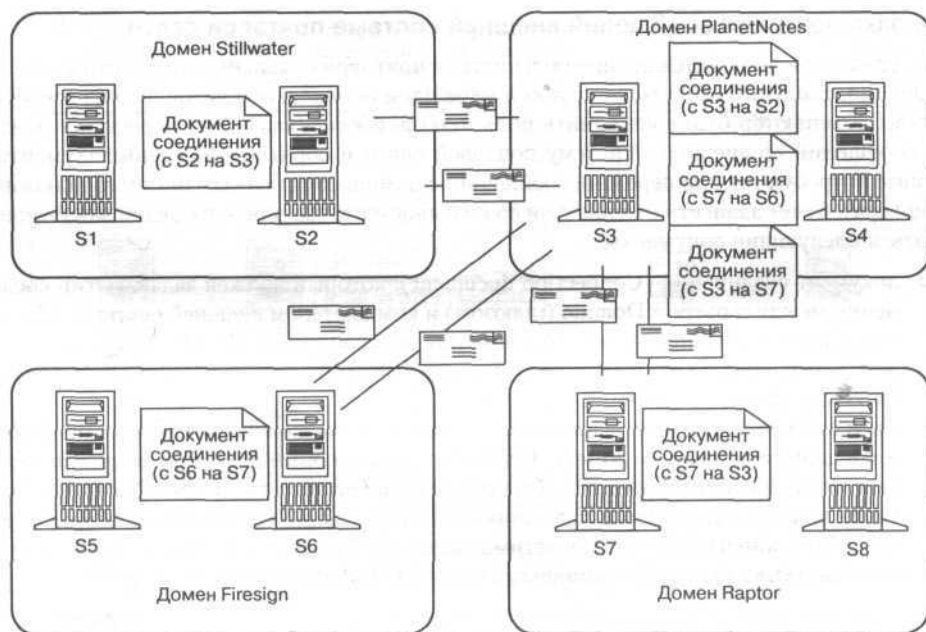


РИС. 8.8. Сервер S3 в домене PlanetNotes выполняет функцию концентратора почтовой службы. Маршрутизация почтовых сообщений между любыми двумя доменами предполагает переход только через один промежуточный домен. То же самое справедливо и для именованных сетей системы Notes

Хотя в приведенном примере различия не столь очевидны, они будут усиливаться с увеличением числа доменов или именованных сетей. В любом случае тщательное планирование не столь важно для почтовой маршрутизации по протоколу SMTP (см. ниже).

Маршрутизация почтовых сообщений по протоколу SMTP

Протокол SMTP (Simple Mail Transfer Protocol - упрощенный протокол передачи почтовых сообщений) является стандартным для пересылки почтовых сообщений в сети Internet и сетях, использующих протоколы TCP/IP. Именно протокол TCP позволяет организовать соединения SMTP, что невозможно в сетях не-TCP/IP. Подробное описание протокола SMTP приводилось в двух запросах на комментарии (Request for Comments, документы RFC 821 и RFC 822), но это описание в дальнейшем многократно менялось (каждое изменение оформлено в виде отдельного документа RFC) и модифицируется по сей день. В документе RFC 821 специфицирован способ передачи почтовых сообщений хостами SMTP, а в документе RFC 822 определен их формат. При желании познакомиться с документами RFC можно прибегнуть к любой поисковой системе сети Internet. Результатом поиска обязательно станет ссылка на службу каталогизации документов RFC, которая поможет получить нужную спецификацию по ее индексу.

Процедура маршрутизации почтовых сообщений с помощью протокола SMTP предусматривает выполнение следующих операций:

1. Отправитель почтового сообщения, являющийся клиентом почтовой службы SMTP, должен сформировать соединение с локальным, специально выделенным хостом SMTP (обычно это обеспечивается с помощью порта 25) и передать одно или несколько сообщений такому хосту. Переданные сообщения должны быть в определенном формате, в соответствии с требованиями документа RFC 822 (с учетом более поздних изменений). В документе RFC 822 содержатся требования по форматированию адреса, по заданию полей заголовка сообщения и по структуре сообщения в целом.
2. Адреса сообщений должны указываться в виде локальная_часть@домен или (фраза) локальная_часть@домен. Хост SMTP выделяет в каждом подобном адресе имя домена, после чего обращается к службе DNS (Сервер доменных имен) за информацией о хосте SMTP, который отвечает за получение почтовых сообщений, адресуемых в соответствующий домен. Сервер DNS хранит такую информацию в записях Mail exchanger (MX).
3. Если сервер DNS не имеет требуемой информации, он передает запрос хоста SMTP серверу DNS более высокого уровня либо самостоятельно обращается к нему. Процесс ссылок и просмотров продолжается до тех пор, пока не будет найден сервер DNS, хранящий необходимую информацию, и пока эта информация не будет передана на хост SMTP.
4. Сервер DNS должен передавать все имеющиеся у него записи MX, а также сопутствующие записи A (от Alias - псевдоним). Каждая запись MX включает в себя имя хоста и уровень предпочтения, согласно которому хост SMTP будет принимать почтовые сообщения для соответствующего домена. Запись A содержит IP-адреса хостов SMTP.
5. Если существует несколько записей MX, хост должен выбирать запись с наименьшим значением предпочтения. Если таких записей несколько, то хост должен произвольным образом выбрать одну из них. После этого передающий сообщения хост

SMTP вступает в контакт с принимающим хостом, организует сеанс связи и направляет ему необходимые сообщения. Если инициирующий взаимодействие хост не может организовать сеанс связи или передать сообщения, но имеются другие записи MX, пересылающий хост SMTP должен предпринять еще одну попытку. Таким образом, процесс может продолжаться до тех пор, пока сообщения не будут успешно переданы (или до момента завершения соответствующего временного интервала). Тайм-аут задается произвольным образом, но, как правило, устанавливается равным 24 часам. (В том случае, если для домена адресата записи MX отсутствуют, служба Domino SMTP предпримет последнюю попытку и попытается отыскать запись A для самого домена (например, для адреса example.com, а не имя_хоста.example.com.) При наличии такой записи служба Domino SMTP попробует организовать сеанс связи с хостом SMTP по найденному IP-адресу.

6. Если принимающий хост SMTP является сервером почтового офиса адресата, этот сервер должен обработать сообщения и сделать их доступными для адресата. Если же принимающий хост является лишь промежуточным, он повторяет всю описанную выше процедуру и направляет сообщения на другой хост SMTP нужного домена, но с более низким значением предпочтения. Таким образом, сообщения неизбежно попадут на сервер почтового офиса нужного домена и затем к адресату.

Формат сообщений SMTP

Сообщения, передаваемые с помощью серверов SMTP, должны иметь вполне определенную структуру, которая оговаривается в документе RFC 822. Обычно такие сообщения представлены набором текстовых строк и подразделяются на *заголовок* и *тело* (информационный раздел). Заголовок имеет информационные поля, каждое из которых находится на отдельной строке и должно удовлетворять определенным требованиям. Заполнение части этих полей обязательно, а остальные поля могут не заполняться. Тело сообщения не регламентируется документом RFC 822, однако должно быть представлено текстом в кодировке US-ASCII.

Поскольку пользователи не ограничиваются пересылкой текстовых сообщений, был разработан ряд способов, позволяющих передавать с помощью стандартных сообщений (отвечающих документу RFC 822) различные наборы символов, сведения о форматировании и нетекстовую информацию. Для этих целей служит протокол MIME (Multipart Internet Messaging Extensions - многофункциональные расширения сообщений сети Internet), текущая версия которого описана в документе RFC 2045. Протокол MIME стал стандартным способом привнесения символов, не соответствующих формату ASCII, в сообщения, отвечающие требованиям документа RFC 822. Кроме того, существует способ MHTML (инкапсуляция формата HTML в формате MIME), описанный в документе RFC 2110, который стал стандартным способом, позволяющим осуществлять форматирование и добавлять гипертекстовые ссылки в тело сообщений, отвечающих требованиям документа RFC 822.

Различия почтовой маршрутизации SMTP и Notes

Маршрутизация почтовых сообщений системы SMTP заметно отличается от маршрутизации сообщений (RPC) в системе Notes. Во-первых, эта процедура является децентрализованной, какой, впрочем, и должна быть общедоступная система передачи информации. В системе SMTP не предусмотрено выделение концентраторов или специальных *узлов передачи данных*. Скорее наоборот, в системе SMTP любой хост может вступать

в контакт с любым другим хостом и передавать ему почтовые сообщения. В этом смысле почтовая служба SMTP аналогична серверу почтовой службы Domino в пределах именовой сети Domino, в рамках которой каждый сервер способен напрямую общаться с другим сервером.

После разрешения маршрутизации SMTP на сервере Domino удастся заметно расширить возможности системы Notes, например запрашивать у службы DNS адреса назначенных хостов SMTP, затем обращаться к этим хостам и пересылать им почтовые сообщения. Если сервер Domino способен подключиться к сети Internet и серверу DNS, располагающему необходимой записью MX, он в состоянии принимать почтовые сообщения от любого другого хоста SMTP сети Internet.

Если каждый используемый сервер Domino отвечает подобным требованиям, можно вообще отказаться от маршрутизации системой Notes и применять для пересылки почты маршрутизацию системы SMTP. Однако на практике это далеко не всегда реально и не всегда дает оптимальный результат.

Почтовая служба SMTP предусматривает применение стека TCP/IP, включая службу DNS, чтобы обеспечить свою работу. Если в сети используются другие протоколы, почтовые клиенты и серверы не смогут работать с почтовой службой SMTP.

Кроме того, модель сети Internet предусматривает достаточно универсальное взаимодействие между хостами SMTP. В то же время администраторы, скорее всего, захотят отгородиться от той анархии, которая царит в сети Internet, и защититься по меньшей мере одним брандмауэром. Возможна также ситуация, в которой далеко не все сети системы Notes будут связаны с сетью Internet и между собой. Могут также потребоваться специальные *контрольные узлы*, через которые почтовые сообщения должны проходить в обязательном порядке, чтобы попасть на другую группу серверов, либо придется выделить специальный брандмауэр (сквозной сервер или сервер коммутируемого доступа) в качестве такого контрольного узла. Следовательно, системы Notes и SMTP (равно как и их процедуры маршрутизации), скорее всего, придется использовать совместно. Здесь уместно отметить, что система SMTP вполне заменяет NRPC, а почтовая служба системы Notes успешно конфигурируется и перенастраивается. При необходимости, конечно, можно работать лишь с одной почтовой службой SMTP, однако не стоит упускать шанс расширить возможности своей системы, поскольку протокол NRPC позволяет решать самые разные проблемы маршрутизации.

Назначение формата почтовой службы SMTP в документах системы Notes

Другим заметным различием между системами SMTP и Notes является формат сообщений. Система Notes во все времена применяла для почтовой службы расширенный текстовый формат, а специалисты компании Lotus предложили лицензированный способ форматирования Notes CD (Notes Compound Document - формат составных документов системы Notes, или расширенный текстовый формат системы Notes). Этот способ позволяет легко формировать и запоминать тексты (содержащие форматирование, вложения, встроенные объекты, гиперссылки и т.д.), а его разработка была завершена задолго до появления соответствующего стандарта сети Internet.

Почтовая служба SMTP, напротив, требует представления своих сообщений в формате US-ASCII, следовательно, приходится преобразовывать текстовый формат в формат US-ASCII с использованием кодирования MIME и MHTML. MHTML является в данном случае тем эквивалентом, который соответствует расширенному текстовому формату системы Notes.

Для поддержки стандартов сети Internet специалисты компании Lotus адаптировали формат сообщений по спецификации RFC 822 (включая MIME и MHTML) и создали на его основе альтернативный формат для почтовых сообщений систем Notes R5 и R6. Компании Lotus пришлось пойти на подобные излишества для того, чтобы обеспечить полномасштабную поддержку протокола SMTP. В версии 4.6 сервер Domino мог хранить сообщения RFC 822 в качестве вложений в поля расширенного текстового формата системы Notes. Начиная с версии 5 сервер Domino запоминает компоненты RFC 822 без выполнения каких-либо дополнительных преобразований или инкапсуляции, то есть в виде объектов системы Notes. Компания Lotus назвала этот формат «родным MIME» (несмотря на то, что сообщение RFC 822 может и не быть в формате MIME). Подобный подход не только позволяет серверу Domino полностью соответствовать стандартам SMTP, но и расширяет возможности почтовых служб POP3 и IMAP по сравнению с версией 4.6.

Серверы Domino способны обеспечивать передачу и хранение сообщений в расширенном текстовом формате системы Notes или в формате MIME. Выбор того или иного формата определяется параметрами в документах Person и Mail-In Database абонентов почтовой службы.

Начиная с версии R5 серверы Domino совершают, при необходимости, преобразование сообщений из одного формата в другой. Например, если такой сервер получает сообщение в формате MIME и должен направить его на другой сервер Domino, не поддерживающий этот формат (например, на сервер Domino версии 4), пересылающий сообщение сервер автоматически преобразует сообщение в расширенный текстовый формат Notes. Кроме того, сервер Domino, получающий сообщение для локального пользователя, будет автоматически преобразовывать его в тот формат, который указывается этим пользователем (расширенный текстовый или MIME).

Совместное использование сервером Domino маршрутизации SMTP и Notes

Основная цель разработчиков процедуры маршрутизации заключалась в том, чтобы обеспечить оптимальные показатели функциональной гибкости для серверов Domino и системы Notes в целом. Так, они постарались добиться полной совместимости со стандартами форматирования и передачи сообщений сети Internet и в то же время сохранить максимальную преемственность по отношению к собственным стандартам форматирования и пересылки сообщений. Это было призвано обеспечить максимальную совместимость системы Notes и сети Internet и устранить необходимость постоянного преобразования передаваемых между ними сообщений. Возможно, именно стремление максимально уменьшить объем преобразований сыграло в данном случае решающую роль, поскольку такие преобразования отвлекали заметные ресурсы системы в прошлом.

Системы Notes/Domino версии 5 и 6 поддерживают свободное преобразование форматов сообщений (расширенный текстовый формат и формат MIME), однако при осуществлении подобного преобразования не обеспечивается полного сохранения сообщения в его исходном виде. Дело в том, что текстовый формат системы Notes поддерживает целый ряд операций форматирования, которые не поддерживаются в MIME/MHTML. При преобразовании сообщения и переходе от текстового формата к MIME все компоненты, связанные с использованием подобных операций, будут исключаться, а при обратном преобразовании (в формат системы Notes) эти исходные компоненты не могут быть восстановлены.

Как и в случае преобразования, нет никакой гарантии того, что форматирование, корректно выполненное в рамках одной процедуры преобразования, будет так же корректно осуществлено и в рамках последующей процедуры. Таким образом, основная цель состоит в том, чтобы максимально уменьшить число переходов от одного формата к другому.

Сообщение не требуется преобразовывать, когда пересылающая его программа почтовой службы, маршрутизирующие серверы, сервер абонента и почтовая служба в целом поддерживают один и тот же формат представления документов (например, расширенный текстовый формат или формат MIME). Если это условие не выполнено, сообщение придется преобразовывать хотя бы один раз. В случае, когда отправитель и получатель сообщения не поддерживают один и тот же формат, сообщение должно быть преобразовано только один раз, однако если и промежуточный сервер не поддерживает требуемый формат, число преобразований увеличится.

Ниже перечислены различные программы, используемые в процессе выполнения процедуры маршрутизации системы Notes, а также операции, связанные с преобразованием форматов:

- О система Notes версии 4 - для чтения и записи сообщений только в расширенном текстовом формате. Сообщение, полученное системой в формате MIME, надо предварительно преобразовать в текстовый формат одним из промежуточных серверов;
- О сервер Domino версии 4 - для маршрутизации и хранения сообщений только в расширенном текстовом формате. Любой сервер, направляющий ему сообщения в формате MIME, должен предварительно преобразовать их в текстовый формат;
- О агент SMTP MTA из состава сервера Domino версии 4 - в качестве маршрутизатора SMTP на сервере Domino R4 для преобразования форматов сообщений (текстовый формат и формат MIME);
- О системы Notes/Domino R5 и R6 - для чтения, записи и хранения сообщений в текстовом формате или формате MIME;
- О маршрутизатор NRPC сервера Domino R5 и R6 - для передачи сообщений в формате MIME и текстовом формате;
- О маршрутизатор почтовой службы SMTP (на сервере Domino) - для маршрутизации сообщений только в формате MIME;
- О почтовые программы сети Internet - для чтения, записи и хранения сообщений в формате MIME или в виде обычного текста.

В общем случае, чтобы сервер Domino обеспечивал эффективную маршрутизацию почты Notes и SMTP (NRPC/SMTP), необходимо выполнить следующие действия:

1. Убедиться (по возможности) в том, что промежуточные серверы почтовой службы (серверы Domino) обновлены до текущей версии. Кроме того, удостовериться, что сообщения будут претерпевать не более одного преобразования формата.
2. В персональном документе (Personal document) пользователя для поля **Format preference for incoming mail** (Предпочтение формата для входящих почтовых сообщений) необходимо правильно задать формат. Это поле специально предназначено для определения формата (расширенный текстовый формат системы Notes или формат MIME) сообщений, поступающих в базу данных почтовой службы пользователя. При необходимости работы в смешанной среде (с версией 4) специалисты компании Lotus рекомендуют задавать здесь вариант **Prefers Notes rich text** (Предпочтителен расширенный текстовый формат системы Notes), что позволяет

улучшить функциональную гибкость и другие характеристики системы. Для сред, состоящих из версий 5 и 6, специалисты советуют выбрать вариант **No preference** (Без предпочтений) для пользователей системы Notes или **Prefers MIME** (Предпочтителен формат MIME) для пользователей других систем, например почтовых служб POP и IMAP.

Настройка процедуры маршрутизации почтовых сообщений

Для проведения настройки маршрутизации почтовых сообщений необходимо подготовить следующие документы базы данных Domino Directory:

- документ сервера (Server document) для каждого сервера;
- документ конфигурации сервера (Server Configuration document) для каждого сервера или группы серверов;
- два или больше документов соединения (Connection document), если маршрутизация почтовых сообщений производится в именованной сети системы Notes или в домене системы Notes, а также, при необходимости, документ домена (Domain document);
- если маршрутизация распространяется на домены не-Notes, необходимы документы соответствующих соединений и документы внешних доменов, а также другие документы (в зависимости от требований программного обеспечения шлюза);
- если маршрутизация почтовых сообщений выполняется в сети Internet, нужны записи в документах серверов и конфигурации либо документы внешнего домена SMTP (Foreign SMTP Domain document) и соединения SMTP (SMTP Connection document) - в зависимости от того, какой из внутренних серверов (SMTP или NRPC) используется для маршрутизации почты в сеть Internet.

Настройка маршрутизации почтовых сообщений по протоколу NRPC

При настройке сервера, предназначенного для маршрутизации почтовых сообщений по протоколу NRPC, практически не требуется выполнять никаких операций, поскольку этот вариант задается по умолчанию. Уже при первом запуске сервера стартует маршрутизатор, который создает базу данных Outgoing Mail (файл mailbox) для записи сообщений почтовыми клиентами и другими маршрутизаторами. Маршрутизатор контролирует базу данных Outgoing Mail (Исходящие почтовые сообщения) на предмет поступления сообщений, требующих обработки. В отсутствие других конфигураций маршрутизатор обеспечит только прием и передачу почтовых сообщений по протоколу NRPC.

Для настройки сервера и приведения его в соответствие с используемой топологией маршрутизации почтовых сообщений понадобится провести настройку портов сервера и указать членство в именованных сетях системы Notes. Для проверки активизированных портов можно обратиться на вкладку **Server => Status** (Сервер => Статус) программы Domino Administrator. Имеется также возможность создать новые порты и переименовать или удалить

существующие порты с помощью команд **Tools => Server => Setup Ports** (Программные инструменты => Сервер =Ф Установка портов) той же самой вкладки (см. главы 3 и 4).

Проверку принадлежности сервера к именованной сети системы Notes производят на виде **Networks** (Сети) базы данных Domino Directory, которую, правда, достаточно трудно открыть в программе Domino Administrator. Для этого надо сначала загрузить базу данных Domino Directory, а уже только после этого переключиться на вид **Networks**. Имеется также возможность просмотреть и изменить сети системы Notes сервера, воспользовавшись вкладкой **Ports => Notes Network Ports** (Порты => Сетевые порты системы Notes) в соответствующем документе сервера.

Подготовка документа соединения для маршрутизации почтовых сообщений

В этом случае может потребоваться подготовить документы соединения, разрешающие маршрутизацию почтовых сообщений для любого из перечисленных ниже условий:

- О если серверы NRPC относятся к нескольким именованным сетям системы Notes, нужно создать два или большее число документов соединения (Connection document) для обеспечения нормального обмена сообщениями между этими серверами. Если сервер одновременно относится к двум именованным сетям, создания документов соединения для маршрутизации между сетями вообще не потребуется. Серверы одной сети будут автоматически направлять почтовые сообщения серверам другой сети с помощью подобного общего сервера;
- О если предусматривается применение нескольких доменов системы Notes и надо организовать передачу сообщений между этими доменами, необходимо создать два или большее число документов соединения;
- О если серверы должны взаимодействовать по телефонной линии связи (модем или сеть ISDN) или обращаться в сеть по телефонным линиям коммутируемого доступа, необходимо создать два или большее число документов соединения.

Для перечисленных выше ситуаций следует создавать не менее двух документов соединения. Дело в том, что процедура маршрутизации почтовых сообщений является процедурой однонаправленного типа. Каждый передающий сервер должен направлять свои почтовые сообщения на соответствующий принимающий сервер. Поэтому, если требуется организовать передачу сообщений в обоих направлениях, подготавливают документ соединения для каждого из направлений. Сервер Domino позволяет сформировать соединение «вытягивания/выталкивания», с помощью которого один сервер вступает в контакт с другим и инициирует передачу почтовых сообщений в обоих направлениях. Но даже в этом случае требуется создавать два документа соединения, если отвечающим хостом является сервер Domino (но не хост SMTP на сервере не-Domino). Для получения дополнительной информации по этому вопросу обратитесь к следующим разделам данной главы.

Если нужно организовать процедуру репликации для двух серверов, достаточно заготовить один документ соединения для обеспечения маршрутизации и репликации, то есть один из документов соединения удастся исключить. Тем не менее специалисты рекомендуют создавать отдельные документы соединения для выполнения маршрутизации и репликации. Как показывает накопленный опыт, в этом случае заметно упрощается характер связей между двумя взаимодействующими серверами (см. главу 9).

Для создания документа соединения, обеспечивающего взаимодействие двух серверов (NRPC) при обмене почтовыми сообщениями, необходимо убедиться в том, что соответствующий сервер выбран в программе Domino Administrator. Сервер адресата должен находиться в том же домене, что и иницилирующий взаимодействие сервер (для которого готовится документ). Затем на вкладке **Configuration** (Конфигурация) следует раскрыть пункт **Messaging** (Передача сообщений) и выбрать **Connections** (Соединения). После этого надо задать вариант **Add Connection** (Добавление соединения) и заполнить поля, указанные в табл. 8.1.

Таблица 8.1. Поля формы **Connection**, связанные с передачей сообщений

Поле	Назначение
Вкладка Basics (Основные параметры)	
Connection type (Тип соединения)	В этом поле может быть задан один из следующих вариантов: ☐ Local Area Network (Локальная сеть) - когда иницилирующий взаимодействие сервер соединен с сервером адресата по сети; ☐ Notes Direct Dialup (Прямой коммутируемый доступ Notes) — когда иницилирующий взаимодействие сервер соединен с сервером адресата по коммутируемой телефонной линии (с помощью модема); ☐ Network Dialup (Сетевой коммутируемый доступ) — когда иницилирующий сервер соединен с сетью сервера адресата с помощью модема, а с самим сервером адресата - по этой сети; ☐ Passthru server (Сквозной сервер) - когда иницилирующий взаимодействие сервер соединен с сервером адресата с помощью третьего сервера
Source server (Исходный сервер)	Данное поле предназначено для ввода полного различающегося имени иницилирующего взаимодействие сервера
Source domain (Исходный домен)	Здесь указывается имя домена исходного сервера
Use the port(s) (Использование портов)	Щелкните по кнопке Choose ports (Выбор портов), а затем укажите необходимый порт. Если требуется более одного порта, исходный сервер будет обращаться к ним в той последовательности, в которой они занесены в данное поле. Когда поле остается незаполненным, сервер последовательно опрашивает все свои порты вплоть до получения положительного результата
Usage priority (Приоритет использования)	В поле следует задавать вариант Normal (Нормальный), если только данное соединение не планируется использовать в качестве резервного, когда надо указывать вариант Low (Низкий). Сервер при попытке связаться с другим сервером, не относящимся к его сети Domino, сначала обратится к соединениям с уровнем приоритета Normal , затем к стекам протоколов, а уже после этого - к соединениям с уровнем приоритета Low
Destination server (Сервер адресата)	В данное поле помещается полное различающееся имя сервера, иницилирующего взаимодействие
Destination domain (Домен адресата)	Поле служит для внесения имени домена, иницилирующего взаимодействие сервера
Optional network address (Необязательный сетевой адрес)	В случае применения порта TCP/IP в этом поле указывается имя хоста или IP-адрес сервера адресата

Таблица 8.1. Поля формы **Connection**, связанные с передачей сообщений (окончание)

Поле	Назначение

Вкладка **Replication/Routing** (Репликация/маршрутизация)

Routing task (Задача маршрутизации)	Для маршрутизации почтовых сообщений по протоколу NRPC здесь выбирается вариант Mail Routing (Маршрутизация почтовых сообщений)
Route at once if x messages pending (Немедленная маршрутизация при накоплении x сообщений)	По умолчанию в данном поле установлено число 5, причем на практике совсем не обязательно его изменять. Сообщения с уровнем приоритета Normal (Нормальный) обычно передаются в соответствии с расписанием, заданным на вкладке Schedule (Расписание). Тем не менее при накоплении сообщений с нормальным приоритетом в количестве, оговоренном в этом поле, сервер, не дожидаясь очередного планового срока, создаст необходимое соединение. Имеется также возможность задать здесь число 1, что предусматривает формирование соединения для каждого очередного сообщения с уровнем приоритета Normal , однако при анализе подобного подхода подумайте о последствиях, в частности о сетевой стоимости такой маршрутизации
Routing cost (Стоимость маршрутизации)	По умолчанию в поле вносится число 1 для сетевых соединений и число 5 для модемных соединений. Допускается изменять эти числа в интервале от 1 до 1С. Более подробная информация представлена ниже в данной главе
Router type (Тип маршрутизатора)	По умолчанию в этом поле выбирается вариант Push Only (Только выталкивание), подходящий во многих случаях. Сведения о других возможных вариантах заполнения данного поля приведены ниже в настоящей главе
Вкладка Schedule (Расписание)	
Schedule (Планирование)	По умолчанию здесь установлен режим Enabled (Разрешено). При задании варианта Disabled (Отмена) исходный сервер никогда не обратится к данному документу соединения
Call at times (Вызовы в определенное время для R5 или -)	В поле указываются моменты времени, в которые сервер будет пытаться сформировать соединение с помощью данного документа. О возможных вариантах заполнения речь пойдет в настоящей главе
Connect at times (Подключение в определенное время) для R6	ниже
Repeat interval of x minutes (Временной интервал повторения в минутах)	По умолчанию в этом поле определено значение 360 (360 минут, или шесть часов). Число минут можно задавать от 0. Сведения о возможных вариантах заполнения данного поля приведены ниже
Days of week (Дни недели)	Здесь надо перечислить те дни недели, в которые должно использоваться расписание. По умолчанию оно применяется ежедневно

После заполнения полей следует сохранить и закрыть документ соединения. Если документ создается на сервере, отличном от исходного, документ нельзя использовать до тех пор, пока он не будет реплицирован на исходный сервер. Если документ сразу формируется на исходном сервере, он может быть применен без всяких задержек.

Поле Routing Cost (Стоимость передачи)

Если сервер обнаруживает два или больше маршрутов к серверу адресата, он суммирует стоимость всех участков каждого маршрута, после чего выбирает путь с наименьшей суммарной стоимостью. В том случае, если маршрут является единственным, сервер просто проигнорирует запись в поле. Если два маршрута имеют одинаковые показатели стоимости, сервер будет выбирать путь с наименьшим числом участков. И наконец, если два маршрута характеризуются одинаковыми показателями стоимости и одинаковым числом участков, сервер станет использовать тот, для которого первый из участков ведет к серверу, имя которого стоит выше в алфавитном перечне.

При отказе соединения сервер будет увеличивать стоимость соответствующего участка на единицу. Повторные отказы приведут к возрастанию стоимости маршрута, которая может достичь такого уровня, что данный маршрут перестанет считаться оптимальным. При этом сервер перейдет к применению *альтернативного маршрута*.

Поле Router Type (Тип маршрутизатора)

Обычно для этого поля по умолчанию задается вариант **Push Only** (Только выталкивание). При этом исходный сервер будет устанавливать контакт с сервером адресата, передавать на него накопленные почтовые сообщения и инициировать отмену соединения. При необходимости передачи почтовых сообщений в обоих направлениях следует создавать два документа соединения - по одному на каждый сервер.

Другие типы маршрутизации возможны в следующих ситуациях:

- О один из серверов не в состоянии быстро сформировать соединение с другим;
- О один из серверов должен принять на себя стоимость передачи по всем участкам.

Ситуация, в которой один сервер не может быстро сформировать соединение с другим, может возникать при сетевом коммутируемом доступе. Не исключено, что сервер адресата вообще не имеет возможности установить контакт с исходным сервером. Другой пример связан с использованием сервера, не имеющего постоянного соединения с сетью Internet, но пытающегося установить контакт с сервером SMTP этой сети и инициирующего пересылку оттуда всех отложенных почтовых сообщений. Другие допустимые значения в поле **Router Type** (Тип маршрутизатора):

- О **Pull Push** (Вытягивание и выталкивание) - исходный сервер формирует соединение с сервером адресата, «выталкивает» в соединение почтовые сообщения, а затем предлагает серверу адресата «вытолкнуть» собственные почтовые сообщения и после их приема отменяет соединение;
- О **Pull Only** (Только вытягивание) - исходный сервер формирует соединение с сервером адресата, предлагает ему «вытолкнуть» почтовые сообщения и после их приема отменяет соединение;
- О **Push Wait** (Ожидание выталкивания) - исходный сервер ожидает вызова от сервера адресата на «выталкивание» почтовых сообщений, а после передачи сообщений отменяет соединение.
- О **Pull Pull** (Вытягивание и вытягивание), доступен в R6 - исходный сервер «вытягивает» (инициирует) процесс «вытягивания» на сервере адресата.

При использовании этих типов маршрутизации для протокола NRPC и передачи почтовых сообщений между двумя серверами Domino необходимо создать два документа соединения - один для исходного сервера, а второй для сервера адресата:

- О для исходного сервера следует создать соединение типа **Pull Push** или **Pull Only** и указать в соответствующем документе исходный сервер (в поле исходного сервера) и сервер адресата (в поле сервера адресата);
- О для сервера адресата требуется сформировать соединение типа **Push Wait** и задать в соответствующем документе сервер адресата (в поле исходного сервера) и исходный сервер (в поле сервера адресата).

Соединения типа **Pull Push** или **Pull Only** применяются для того, чтобы не имеющий постоянного соединения с сетью Internet сервер Domino мог отправлять и принимать почту от сервера SMTP сети Internet, при этом достаточно одного документа соединения. Если сервер SMTP не является сервером Domino, сервер адресата (сервер SMTP) должен обеспечивать поддержку управляющей команды ETRN (см. ниже в этой главе).

Поля вкладки **Schedule (Расписание)**

Поле **Call at times** (Время вызова) или **Connect at times** (Время подключения) может содержать одно значение (например, в виде 8:00 a.m., 8 часов утра), временной интервал (например, в виде 8:00 p.m.-10:00 p.m., с 8 часов утра до 10 часов вечера), а также несколько значений и/или временных интервалов (например, в виде 8:00 a.m., 11:00 a.m.; 2:00 p.m.-4:30 p.m., 8 часов утра, 11 часов утра; с 2 часов вечера до 4 часов 30 минут вечера). При наступлении указанного времени исходный сервер будет пытаться сформировать соединение с сервером адресата и выполнить те задачи, которые указаны в поле **Replication/Routing** (Репликация/маршрутизация).

Если при формировании соединения происходит отказ, исходный сервер выжидает в течение определенного времени, а затем предпринимает еще одну попытку. При повторном отказе сервер выжидает дольше и делает очередную попытку. С каждым следующим отказом интервал ожидания увеличивается. Для подсчета временных интервалов исходный сервер пользуется алгоритмом Randomized Exponential Backoff Algorithm (Алгоритм случайного экспоненциального отката). Этот алгоритм указывает на необходимость увеличения времени ожидания приблизительно вдвое после очередного отказа.

Если соединение создается для указанного момента времени (например, для 8 часов утра) и происходит отказ, исходный сервер продолжит попытки формирования соединения в течение 60 минут (или вплоть до получения положительного результата), а при отсутствии положительного результата прекращает действия и ожидает следующего намеченного сеанса связи.

Если возникает отказ при формировании соединения для определенного временного интервала (например, с 8 часов утра до 10 часов вечера), сервер будет продолжать попытки вплоть до получения положительного результата или вплоть до завершения оговоренного временного интервала.

В случае успешного создания соединения и превышения указанного временного интервала исходный сервер будет выжидать в течение временного интервала, заданного в поле **Connection interval** (Интервал соединения), а затем предпримет еще одну попытку. Отсчет

интервала ожидания начинается от момента прерывания соединения. Сервер игнорирует параметр, присутствующий в поле **Connection interval**, в том случае, если соединение формируется для конкретного момента времени (например, для 8 часов утра), указанного в документе соединения.

Настройка маршрутизации почтовых сообщений SMTP

Серверы Domino имеют возможность использовать процедуру маршрутизации почтовых сообщений SMTP любым из трех способов:

- О прием почтовых сообщений SMTP. В этом случае рассматриваемая процедура позволяет серверу принимать почтовые сообщения, передаваемые с помощью протокола SMTP;
- О пересылка почтовых сообщений за пределы локальных доменов сети Internet. С помощью данной процедуры сервер применяет протокол SMTP для пересылки почтовых сообщений на хосты SMTP, которые расположены в доменах сети Internet, не относящихся к домену сервера Domino, или для отправки почтовых сообщений сети Internet на промежуточные хосты;
- О передача почтовых сообщений в пределах локальных доменов сети Internet. В таких условиях процедура предоставляет серверу возможность посредством протокола SMTP доставлять сообщения на другие серверы Domino SMTP. Эта процедура обеспечивает передачу сообщения SMTP в пределах именованных сетей системы Notes или в пределах локальной доменной области системы Notes. Ее также можно использовать для создания локального *интеллектуального хоста*, если некоторые локальные пользователи почтовой службы SMTP относятся к серверу почтовой службы, не являющемуся сервером Domino.

В данном случае термин «локальные домены сети Internet», присутствующий в приведенном выше списке, указывает на домены сети Internet, заданные в документах глобального домена (Global Domain document) каталога Domain Directory. Иначе адреса могут оговариваться в поле **Fully qualified Internet host name** (Полное различающееся имя хоста в сети Internet).

На практике пользователь в состоянии принять любое из предложенных выше решений для каждого сервера R5/6 домена. К сожалению, не существует четких правил, позволяющих сформулировать требования по настройке сервера. На этот процесс обычно влияет большое число факторов, которые, кстати, способны изменяться со временем. Но даже после тщательного анализа этих факторов решение может оказаться совершенно неочевидным. Ниже приводится перечень таких факторов:

- О применение протокола SMTP предполагает принадлежность всех хостов SMTP к одной и той же сети. Следовательно, не предусматривается маршрутизации из домена *A* в домен *C* через домен *B*, поскольку всегда можно связаться с *C* непосредственно из *A*, что позволяет минимизировать число транзитных участков (переходов), а также исключает необходимость заранее намечать маршруты между хостами;
- О система Notes предусматривает возможность прямого подключения между серверами только в пределах именованных сетей. За границами этих сетей, доменов и систем почтовой связи серверы Domino далеко не всегда могут установить контакт друг с другом, причем им требуются документы соединения, в которых описываются пути для передачи сообщений через существующие границы;

- О процедура маршрутизации почтовых сообщений SMTP основана на применении протокола TCP/IP. Система Notes, напротив, допускает работу с различными протоколами, включая другие сетевые протоколы и протоколы коммутируемого доступа;
- О при обновлении серверов и пользователей во время перехода от версии 4 к версии 5 или 6 нет необходимости сразу активизировать процедуру маршрутизации почтовых сообщений SMTP. К тому моменту, когда эта процедура реально потребуется, существующая система почтовой связи будет уже хорошо отлажена (так же хорошо, как в версии R4, или даже лучше). При желании можно продолжить применение сервера R4 с агентом SMTP MTA, которые используют формат сообщений версии 4, но обновить остальные серверы;
- О серверы R4 не предусматривают применения протокола SMTP и соответствующей процедуры маршрутизации почтовых сообщений на другие серверы Domino, поэтому обязаны пользоваться маршрутизацией почтовых сообщений системы Notes;
- О маршрутизаторы почтовых сообщений SMTP применяют записи MX, полученные с сервера DNS, для определения идентификационных данных и адресов хостов SMTP. Любой маршрутизатор почтовой службы Domino, использующий протокол SMTP для передачи почтовых сообщений во внешний мир, должен иметь доступ к службе DNS. Серверы, поддерживающие маршрутизацию сообщений SMTP только с хостами Domino, интеллектуальными или промежуточными хостами, могут обойтись без службы DNS. Серверы, выделенные для приема сообщений SMTP из внешнего мира, обязаны иметь записи MX в базе данных сервера DNS, которая должна быть доступной извне. С другой стороны, допустимо установить внутреннюю маршрутизацию почтовых сообщений по протоколу NRPC без привлечения сервера DNS или какой-либо другой службы каталогов, не относящейся к системе Notes.

Для каждого конкретного сервера следует принимать решение о необходимости и характере использования маршрутизации почтовых сообщений SMTP. Проведение в жизнь принятых решений не представляет никакой сложности.

Настройка сервера для приема почтовых сообщений по протоколу SMTP

Такая настройка сервера позволяет принимать почтовые сообщения посредством их маршрутизации по протоколу SMTP. Для проведения настройки надо установить флажок в поле **SMTP listener task** (Задача контроля SMTP) в документе сервера на вкладке **Basics**, а затем перезапустить сервер. Это позволит активизировать серверную задачу SMTP, причем в данном случае добавлять параметр SMTP в переменную ServerTasks в файле notes.ini не рекомендуется.

Указанная задача «прослушивает» протокол TCP в порте 25 (или в другом порте, заданном в документе сервера), чтобы узнать о подключениях других серверов SMTP. При формировании соединения с подобным сервером задача контроля SMTP будет обеспечивать прием сообщений и занесение их в файл mailbox, после чего маршрутизатор займется обработкой полученных сообщений.

Серверы, для которых нужно запускать задачу SMTP Listener (Контроль SMTP):

- О любой сервер, выделенный для получения почтовых сообщений от внешнего хоста SMTP. Например, серверы, принимающие почтовые сообщения из сети Internet, из других доменов сети intranet или от промежуточного хоста;
- О любой сервер, выделенный для маршрутизации внешних и внутренних почтовых сообщений SMTP.

Настройка сервера для отправки почтовых сообщений за пределы локальных доменов Internet по протоколу SMTP

Серверы, которые настроены на протокол SMTP для пересылки сообщений, адресованных нелокальным доменам сети Internet, обычно применяют один из двух способов передачи: пересылку сообщений непосредственно адресатам сети Internet или направление их посредством протокола SMTP на локальный промежуточный хост SMTP. Промежуточный хост в этом случае обычно представляет собой серверный брандмауэр и может быть сервером SMTP не-Domino или другим сервером Domino, способным отправлять почтовые сообщения за пределы локального домена сети Internet.

Для настройки такого сервера необходимо выполнить следующие операции:

1. Создать документ конфигурации (Configuration document) для сервера или использовать уже существующий документ. Если присутствуют несколько документов конфигурации, надо объединить их.
2. В документе конфигурации на вкладке **SMTP/Router => Basics** (SMTP/маршрутизатор => Основные параметры) указать в поле **SMTP used when sending messages outside the local Internet domain** (Использовать SMTP для отправки сообщений за пределы локального домена сети Internet) вариант **Enabled** (Разрешено), после чего сохранить документ конфигурации.
3. Если сервер планируется в качестве промежуточного хоста для Domino R4 или сервера Domino R5/6, не работающего с протоколом SMTP, выбрать **SMTP Mail Routing** (Маршрутизация почтовых сообщений SMTP) в поле **Routing Tasks** (Задачи маршрутизации) на вкладке **Basics** документа сервера, подготовленного ранее для этого промежуточного хоста.

Настройка сервера пересылки почтовых сообщений по протоколу SMTP в пределах локального домена сети Internet

Данный сервер обеспечивает маршрутизацию почтовых сообщений системы Notes или SMTP для передачи на другие серверы Domino в пределах локальной именованной сети системы Notes или локальной доменной области системы Notes.

При настройке подобного сервера следует создать для него документ конфигурации и заполнить два поля на вкладке **SMTP/Router => Basics: The server will only use Notes routing to route mail internally** (Сервер использует только маршрутизацию системы Notes для передачи внутренних сообщений) и **Servers within the local domain are reachable through SMTP over TCP/IP** (Доступ к серверам в пределах локального домена обеспечивается с помощью протокола SMTP поверх TCP/IP).

Поле **The server will only use Notes routing to route mail internally** допускает выбор из трех следующих вариантов:

- **Disabled** (Отмена) - установлен в режиме по умолчанию. В этом случае сервер будет пользоваться только маршрутизацией системы Notes для внутренней передачи почтовых сообщений;
- **MIME messages only** (Только сообщения в формате MIME) - задается для разрешения маршрутизации почтовых сообщений SMTP, однако не все внутренние серверы

смогут принимать почтовые сообщения SMTP. Каждый из серверов задействует наиболее подходящую процедуру маршрутизации для каждого почтового сообщения (NRPC или SMTP);

- О **All messages** (Все сообщения) - выбирается только при условии, что все внутренние серверы Domino и все пользователи почтовой службы системы Notes могут принимать почтовые сообщения с помощью протокола SMTP. При этом серверы преобразуют расширенный текстовый формат системы Notes в формат MIME. Если сервер адресата не обеспечивает прием почтовых сообщений, передаваемых с помощью протокола SMTP, пересылка не производится.

Поле **Servers within the local domain are reachable through SMTP over TCP/IP** допускает выбор из двух вариантов:

- О **Only if in same Notes named network** (Только в той же именованной сети системы Notes) - сервер с помощью протокола SMTP будет передавать почтовые сообщения в пределах именованных сетей (поддерживающих также протоколы TCP/IP) к тем серверам, которые допускают применение протокола SMTP. Сервер также станет использовать маршрутизацию NRPC для направления почтовых сообщений на те серверы, которые не поддерживают протокол SMTP и расположены за границами именованной сети и домена системы Notes;
- О **Always** (Всегда) - сервер посредством протокола SMTP будет передавать почтовые сообщения всем серверам Domino в локальном домене сети Internet, работающим с протоколом SMTP. Под «локальным доменом» в данном случае понимается локальный домен сети Internet, который определен в поле **All the Internet domains listed in this Notes domain** (Все домены сети Internet, перечисленные в данном домене Notes) документа глобального домена (Global Domain document). В этом случае сервер имеет возможность направлять почтовые сообщения с помощью протокола SMTP за границы именованной сети и домена системы Notes.

Подключение доменов системы Notes к сети Internet

Для доменной области системы Notes имеется три варианта формирования соединения с сетью Internet:

- О **Inbound/Outbound Gateway Server** (Использование входящих/исходящих шлюзов). Небольшая группа серверов может совместно выполнять функции шлюза для остальных серверов домена Domino. Шлюзовые серверы доставляют в сеть Internet сообщения, поступающие от внутренних серверов, а также из сети Internet на внутренние серверы. Достаточно одного шлюза, но для обеспечения резервирования лучше установить два шлюзовых сервера. Подобная конфигурация оказывается весьма удобной для системы Notes/Domino, в которой внутренние серверы не могут использовать протокол SMTP или требуется полностью изолировать внутренние серверы за брандмауэром. Кроме того, эта конфигурация активно применяется серверами Domino R4 с агентами SMTP Message Transfer Agent (Агент передачи сообщений SMTP) для доставки почты в Internet;

- О **Inbound Gateway Servers Only** (Использование только входящих шлюзовых серверов). Все или большая часть серверов способны маршрутизировать почтовые сообщения непосредственно в сеть Internet и лишь несколько выделенных серверов используются в качестве шлюзов. Такие серверы получают входящие почтовые сообщения и направляют их на внутренние серверы. Если все или большая часть серверов Domino связаны непосредственно с сетью Internet, можно разрешить им маршрутизацию собственной исходящей почты в сеть Internet. Это позволяет исключить транзитный участок для исходящей почты и освободить шлюзовые серверы для маршрутизации входящих сообщений;
- О **No Gateway Servers** (Без использования шлюзов). Все серверы передают свои почтовые сообщения непосредственно в сеть Internet и получают сообщения также непосредственно из сети Internet. Этот подход, возможно, является оптимальным для организаций, имеющих небольшое число серверов и не заботящихся о безопасности своих данных (и хакерских атаках из сети Internet).

При формировании связей между доменами системы Notes и сетью Internet серверы Domino в состоянии выполнять три различные функции:

- О маршрутизатора исходящих почтовых сообщений (Outbound Mail Router), который получает почтовые сообщения от внутренних серверов Domino и направляет их на хосты SMTP сети Internet;
- О маршрутизатора входящих почтовых сообщений (Inbound Mail Router), принимающего почтовые сообщения от внешних хостов сети Internet и пересылающего их на внутренние серверы Domino;
- О маршрутизатора внутренних почтовых сообщений (Internal Mail Router), обеспечивающего маршрутизацию почтовых сообщений только на другие локальные серверы Domino. Кроме того, он передает исходящую почту для сети Internet на шлюзовой сервер исходящей почты и получает почтовые сообщения сети Internet от шлюзового сервера входящей почты. Такой сервер может допускать или не допускать применение протокола SMTP.

Для настройки сервера каждого типа необходимо ознакомиться с материалами последующих разделов.

Настройка шлюза исходящей почты

Для настройки шлюзового сервера исходящей почты нужно выполнить следующие операции:

1. Разрешить в документе конфигурации сервера применение протокола SMTP для пересылки сообщений за границы локального домена сети Internet.
2. Убедиться в том, что данный сервер способен подключиться к сети Internet, при этом наилучшим вариантом является соединение по локальной сети, что, конечно, не исключает возможности работы с модемом или сетью ISDN.
3. Если сервер используется в качестве промежуточного хоста для серверов Domino 4, 5 или 6, которые не допускают применения протокола SMTP, следует добавить запись **SMTP Mail Routing** (Маршрутизация почтовых сообщений SMTP) в поле **Routing Tasks** (Задачи маршрутизации) на вкладке **Basics** документа сервера, подготовленного для промежуточного хоста.

Настройка шлюза входящей почты

Для настройки шлюзового сервера входящей почты выполните следующие действия:

1. Разрешить исполнение задачи SMTP Listener (Контроль SMTP).
2. Создать запись MX для сервера в базе данных сервера DNS, допускающего обращение из сети Internet (сервер может принадлежать компании или провайдеру услуг сети Internet).

Настройка внутренних серверов

Внутренние серверы обеспечивают передачу почтовых сообщений только на локальные серверы Domino. Сообщения для сети Internet пересылаются на шлюзовые серверы, выполняющие функцию промежуточных хостов. Шлюзы должны точно знать сервер или серверы, выделенные для этой цели. Способ получения такой информации зависит от выбранного для взаимодействия с сетью Internet варианта маршрутизации (SMTP или NRPC). Так, сервер, использующий протокол SMTP, получает подобную информацию из записей полей документа конфигурации, а сервер NRPC - из нескольких источников. В данном случае проще всего установить сервер SMTP, на котором легче настроить маршрутизацию исходящих почтовых сообщений сети Internet.

Серверы, применяющие протокол SMTP

Для разрешения серверу Domino использовать протокол SMTP при маршрутизации почтовых сообщений (сообщений сети Internet, передаваемых на шлюз) требуется заполнить перечисленные ниже поля документа конфигурации сервера, находящиеся на вкладке **Router/SMTP => Basics**:

- в поле **SMTP used when sending messages outside of local Internet domain** (Использовать SMTP для отправки сообщений за границы локального домена сети Internet) следует задать вариант **Enabled** (Разрешено);
- в поле **Relay host for messages leaving the local Internet domain** (Промежуточный хост для пересылки сообщений, покидающих локальный домен сети Internet) надо отметить один из двух вариантов:
 - когда имеется один шлюз исходящей почты, необходимо задать его имя хоста или IP-адрес (причем лучше имя хоста, поскольку вероятность изменения для него меньше, чем для IP-адреса). Тогда внутренние серверы будут направлять все исходящие почтовые сообщения именно на этот сервер;
 - если для исходящей почты запланировано несколько шлюзовых серверов, следует создать для них соответствующие записи MX на сервере DNS текущего домена, а затем в поле **Relay host for messages leaving the local Internet domain** указать имя шлюзового сервера в домене сети Internet. При этом внутренние серверы будут пересылать почтовые сообщения на данный шлюз с учетом приоритета DNS (для серверов с одинаковым приоритетом выбор будет случайным).

Серверы NRPC

На практике существует несколько способов разрешения действия только протокола NRPC на сервере Domino, маршрутизирующем почту сети Internet на шлюзовой сервер. Речь в данном случае идет о способе, рекомендуемом специалистами компании Lotus, и о двух других

способах. Выбор того или иного способа зависит от двух факторов: находится ли сервер Domino в том же самом домене системы Notes, что и шлюзовой сервер, и сколько имеется шлюзовых серверов.

Все способы предполагают создание по крайней мере одного документа внешнего домена SMTP (Foreign SMTP Domain document) и одного или нескольких документов соединения (Connection document). Основное назначение документа внешнего домена SMTP состоит в предоставлении серверу Domino с протоколом NRPC информации о том, какие сообщения должны быть направлены в домен или на сервер, указанный в этом документе (Foreign SMTP Domain document). В поле **Internet Domain** (Домен Internet) задается имя домена (например, в виде example.com) или подстановочный шаблон (например, в виде *.uk, *.us, ".example.com, *."). После того как сервер NRPC найдет адрес, совпадающий с именем домена или подстановочным шаблоном, он инициирует пересылку сообщения с учетом данных из документа внешнего домена SMTP.

Документ соединения в данном случае представляет собой обычный документ подобного типа и информирует передающий сервер о необходимости формирования соединения, о времени соединения и о действиях, предпринимаемых сразу после создания соединения. Единственное отличие связано с реализацией первого подхода, описанного в следующем разделе, когда документ соединения не может предоставить передающему серверу NRPC имя сервера, маршрутизирующего почту сети Internet. В этой ситуации передающий сервер получает необходимую информацию о сервере адресата косвенным образом.

Сервер NRPC и шлюзовые серверы одного домена системы Notes: способ, рекомендуемый компанией Lotus

Если сервер NRPC находится в том же домене, что и шлюзовой сервер, можно настроить его для маршрутизации почтовых сообщений сети Internet с помощью способа, официально предлагаемого специалистами компании Lotus. Этот способ является достаточно сложным по сравнению с другими, но в то же время имеет определенное преимущество: в случае построения шлюза на основе нескольких серверов сервер NRPC обеспечит передачу почтовых сообщений сети Internet на любой из этих серверов. Для настройки сервера необходимо выполнить следующие действия:

1. В документе сервера (Server document) каждого шлюзового сервера, с помощью которого сервер NRPC будет передавать почтовые сообщения сети Internet, добавьте запись **SMTP Mail Routing** в поле **Routing tasks** (Задачи маршрутизации), чтобы проинформировать сервер NRPC о маршруте передачи почтовых сообщений сети Internet.
2. В программе Domino Administrator выберите **Configuration => Messaging => Domains** (Конфигурирование => Передача сообщений => Домен) и создайте документ внешнего домена SMTP (Foreign SMTP Domain document) с учетом рекомендаций, приведенных в табл. 8.2. Для этого щелкните по кнопке **Add Domain** (Добавить домен) и укажите нужный тип документа в поле **Domain type** (Тип домена) на вкладке **Basics**.
3. В программе Domino Administrator выберите **Configuration => Messaging => Connections** (Конфигурирование => Передача сообщений => Соединения) и создайте документ соединения SMTP (SMTP Connection document) с учетом рекомендаций, представленных в табл. 8.3.

Таблица 8.2. Перечень полей на форме внешнего домена SMTP

Поле	Назначение
Вкладка Basics (Основные параметры)	
Domain Type (Тип домена)	В этом поле задается вариант Foreign SMTP Domain (Внешний домен SMTP)
Вкладка Routing (Маршрутизация)	
Internet Domain (Домен сети Internet)	В поле вносится имя домена сети Internet, куда будут направляться почтовые сообщения в соответствии с данным документом (для маршрутизации во все домены Internet надо ввести *.*). Если данный документ обеспечивает пересылку почтовых сообщений в определенный домен SMTP, следует указать имя этого домена
Domain name (Имя домена)	Поле предназначено для записи имени домена, куда будут передаваться почтовые сообщения в соответствии с данным документом. Это имя может соответствовать имени домена в системе Notes или быть описательным названием, например The Internet (Сеть Internet)
Internet host (Хост сети Internet)	Поле не требует заполнения

Таблица 8.3. Перечень полей на форме соединения SMTP

Поле	Назначение
Вкладка Basics (Основные параметры)	
Connection type (Тип соединения)	В этом поле указывается SMTP
Source server (Исходный сервер)	В поле вводится полное имя сервера NRPC. Можно также воспользоваться подстановочными символами для указания группы серверов (например, */Servers/Stillwater). В этом случае может неправильно действовать кнопка Choose record (Выбор записи), см. ниже
Source domain (Исходный домен)	Поле предназначено для внесения имени домена системы Notes для исходного сервера
Connect via (Соединение с помощью)	Для данного поля следует выбирать вариант Direct connection (Непосредственное соединение), если исходный сервер взаимодействует со шлюзом по локальной сети. Вариант Dial-up connection (Коммутируемое соединение) удобен, если исходный сервер взаимодействует со шлюзовым по коммутируемому сетевому подключению или коммутируемому подключению системы Notes
Dial using connection record (Коммутируемое подключение с помощью записи соединения)	Это поле появляется в том случае, если в предшествующем поле задан вариант Network Dialup connection (Коммутируемое сетевое соединение). Если исходный сервер использует сетевой коммутируемый доступ к шлюзу, а документ соединения такого

Таблица 8.3. Перечень полей на форме соединения SMTP (окончание)

Поле	Назначение
Dial using connection record	подключения уже существует, можно просто нажать кнопку Choose record и выбрать соответствующую запись соединения из предлагаемого списка. Формула выбора записей этой кнопки обеспечивает поиск требуемых записей соединения, для которых исходный сервер указан в документе соединения. При использовании подстановочных символов формула найдет только записи с тем же подстановочным шаблоном. Если исходный сервер использует прямой коммутируемый доступ системы Notes для подключения к шлюзу, в поле следует вводить полное имя шлюзового сервера
Destination server (Сервер адресата)	В данном случае сервер Domino не обращается к этому полю, однако требуется внести в него какую-нибудь информацию, поскольку нельзя сохранить документ с незаполненными полями. Вид Connections (Соединения) обеспечивает сортировку по содержимому этого поля, поэтому следует поместить в него описательное название. Например, если символы *.* вводились в поле Internet Domain (Домен сети Internet) документа внешнего домена SMTP, следует выбрать здесь вариант All Internet Servers (Все серверы сети Internet). Если в указанном документе задавались определенные домены сети Internet (например, в виде example.com), надо ввести Internet Servers in example.com (Серверы сети Internet из домена example.com) или аналогичный вариант
Destination domain (Домен адресата)	В это поле помещается тот же самый текст, что и в поле Domain name (Имя домена) документа внешнего домена SMTP. Например, если в документе вводилась запись The Internet (Сеть Internet), аналогичная запись должна быть занесена в данное поле. Именно использование одного названия позволяет связать два документа между собой. Запись в поле информирует сервер Domino о необходимости обращаться к данному документу соединения для передачи почтовых сообщений, адресованных доменам сети Internet, которые перечислены в документе внешнего домена SMTP
Поля на вкладке Replication/Routing (Репликация/маршрутизация)	Поля заполняются так же, как в любом документе соединения. Если требуется передавать на шлюзовую сервер с помощью исходного сервера только почтовые сообщения сети Internet, задача репликации в поле Replication task отменяется, а в поле Routing task (Задача маршрутизации) указывается SMTP Mail Routing (Почтовая маршрутизация SMTP). Если разрешены обе задачи, исходный сервер будет осуществлять маршрутизацию отложенных почтовых сообщений, не принадлежащих сети Internet, вместе с почтой этой сети
Поля на вкладке Schedule (Расписание)	Исходный сервер будет передавать почтовые сообщения в соответствии с расписанием, помещенным на данной вкладке

При использовании нескольких шлюзовых серверов для связи с почтовой службой сети Internet требуется создать по два документа для каждого подобного сервера. Например,

один из шлюзов может обеспечивать связь с самой сетью Internet, другой - с частным доменом сети intranet, а третий - со всеми доменами сети Internet, имена которых заканчиваются на *.uk. При этом необходимо создавать документ внешнего домена SMTP и документ соединения SMTP для каждого шлюзового сервера. Первый документ обеспечит передачу почтовых сообщений для адресов, соответствующих шаблону *, второй - для определенных адресов, например example.com, а третий документ - для адресов с шаблоном *.uk. В таком случае почтовые сообщения с адресами example.co.uk или example.com будут автоматически задействовать специально созданный документ, а не документ общего типа (*.*).

Сервер NRPC и шлюз в одном домене системы Notes: простой способ

Данный способ проще описанного выше, но годится лишь при условии, что для любого шлюза имеется только один шлюзовой сервер. В таком случае достаточно создать документ внешнего домена SMTP, в котором поле **Domain name** (Имя домена) останется незаполненным, и задать имя шлюзового сервера в поле **Internet host** (Хост сети Internet).

Теперь все серверы NRPC, которые передают почтовые сообщения на шлюзовой сервер, будут направлять на него предназначенные для сети Internet сообщения с помощью созданного документа. Конечно, в отсутствие маршрута для почты к этому серверу придется создать и типовые документы соединения (Connection document).

Серверы NRPC и шлюзовые серверы в разных доменах системы Notes

Если сервер NRPC находится в ином домене Domino, чем шлюзовой сервер или серверы, можно применять не шлюзовой домен (см. два рассмотренных выше примера), а сформировать дополнительный документ внешнего домена SMTP в домене сервера NRPC. В таком документе в поле **Domain name** (Имя домена) должно указываться имя домена системы Notes для шлюзового сервера, при этом сервер NRPC будет направлять почтовые сообщения сети Internet, а также другие почтовые сообщения в шлюзовой домен.

Предполагается, что все типы почтовых сообщений можно свободно направлять в домен шлюзового сервера. В противном случае потребуются создать стандартные документы соединения для указания маршрутов. Если нужно направлять в домен шлюзового сервера только почтовые сообщения сети Internet (а не почтовые сообщения системы Notes), можно указать **SMTP Mail Routing** (Маршрутизация почтовых сообщений SMTP) в поле **Routing tasks** (Задачи маршрутизации) любого созданного документа соединения. Если требуется направлять почтовые сообщения сети Internet с учетом различных расписаний системы Notes, допустимо создать один документ соединения для маршрутизации почтовых сообщений SMTP (SMTP Mail routing), а другой - для маршрутизации обычных почтовых сообщений (Mail routing). В подобных документах соединения при необходимости следует предусмотреть возможность репликации.

Взаимосвязи между доменами

Когда сообщение с адресом jdoaks@planetnotes.com попадает в домен системы Notes из сети Internet, сервер, получивший сообщение, должен принять решение относительно способа передачи его адресату addressee.jdoaks. На практике компонент адреса jdoaks может быть связан с сервером четырьмя различными способами:

- О адрес jdoaks@planetnotes.com принадлежит домену самого сервера, при этом сервер без труда обнаружит компонент адреса jdoaks в базе данных Domino Directory;

- компонент адреса jdoaks принадлежит другому домену системы Notes, при этом сервер распознает домен с помощью документа глобального домена (Global Domain document);
- компонент адреса jdoaks не принадлежит домену системы Notes, однако компонент адреса planetnotes соответствует локальному домену сети Internet, которому сервер должен направлять сообщение. При этом сервер передает на интеллектуальный хост (не базирующийся на сервере Domino) сообщение, которое обеспечит распознавание компонента адреса jdoaks и определение способа передачи сообщения;
- компоненты адреса jdoaks и planetnotes никак не соотносятся с сервером, и сервер вынужден вернуть сообщение отправителю.

Документ глобального домена

Документ глобального домена (Global Domain document) информирует сервер о взаимосвязи между локальными доменами сети Internet и локальными доменами системы Notes. Например, если передающий сервер принадлежит к домену с адресом roskteam.com, а принимающий сервер - к домену с адресом jdoaks@planetnotes.com, документ глобального домена уведомит сервер о том, что компонент адреса относится к тому же самому домену системы Notes (несмотря на то, что компонент адреса jdoaks может соответствовать другому домену сети Internet). Либо документ глобального домена укажет серверу, что компонент адреса соответствует соседнему домену системы Notes.

Документ глобального домена следует создавать в тех случаях, когда приходится организовывать взаимодействие с несколькими доменами сети Internet или с несколькими доменами системы Notes. В этом случае подобный документ служит для установления взаимосвязей между доменами сети Internet и системы Notes, а также решает ряд других проблем, поэтому поля документа содержат разнообразную информацию:

- **Notes domains and aliases** (Домены системы Notes и псевдонимы). Здесь надо задать имена всех доменов системы Notes, которые взаимодействуют с доменами сети Internet, присутствующими в двух приводящихся ниже полях. При указании нескольких доменов Domino следует копировать этот документ глобального домена для каждого домена системы Notes или создавать аналогичные документы в соответствующих базах данных Domino Directory;
- **Local primary Internet domain** (Локальный основной домен сети Internet). В этом поле следует ввести имя домена сети Internet для соответствующего сервера;
- **Alternate Internet domain aliases** (Дополнительные псевдонимы для домена сети Internet). В данном поле нужно указывать имена других доменов сети Internet, объекты которых одновременно являются объектами доменов Domino, упомянутых в документе глобального домена.

При поступлении в домен сообщения из сети Internet принимающий сервер с помощью документа глобального домена получает информацию о том, принадлежит ли адресат к домену системы Notes для данного сервера или к иному домену системы. Доставка сообщения осуществляется согласно полученным данным.

Задание адресов сети Internet для пользователей

Другое назначение документа глобального домена (Global Domain document) состоит в том, чтобы задавать (в режиме по умолчанию) обратные адреса сети Internet для пользователей системы Notes, которые направляют свои почтовые сообщения в сеть Internet. В персональном документе (Personal document) версий R5 и R6 присутствует специальное поле для

указания обратного адреса сети Internet. При регистрации нового пользователя заполнение этого поля производится автоматически. Однако для более ранних версий в упомянутом документе не предусматривалось подобного поля. Поэтому те организации, которые осуществляют обновление до новых версий системы, могут получить большое число документов, в которых поле **Internet address** (Адрес сети Internet) осталось пустым. Для таких пользователей документ глобального домена позволяет задать формулу, обеспечивающую генерацию обратных адресов.

Вместо создания документа глобального домена можно самостоятельно заполнить поля **Internet address** во всех персональных документах домена, и совсем не обязательно вручную. Domino Administrator содержит необходимый программный инструмент для осуществления таких операций. Следует лишь перейти на вкладку **People & Groups** (Сотрудники и группы) и выполнить **Tools => People => Set Internet Address** (Программные инструменты => Сотрудники => Задание обратных адресов сети Internet).

Появится диалоговое окно **Set Internet Address** (Задание адреса сети Internet). В нем можно воспользоваться стандартным форматом для преобразования имен системы Notes в адреса сети Internet. После щелчка по кнопке OK адрес сети Internet формируется на основе тех правил, которые были заданы раньше, и заносится в поля **Internet Address** документов выбранного каталога. Программа также проверит уже занесенные адреса и определит степень их соответствия требованиям документа RFC 822, а также их уникальность для заданного каталога.

Интеллектуальный хост

Многие организации не ориентируются только на стандарты системы Notes, работая с пользователями системы Notes и других почтовых служб, не связанных непосредственно с системой Notes. Тем не менее все пользователи могут быть отнесены к одному домену, скажем с адресом planetnotes.com. В этом случае из сети Internet на сервер Domino будет передано сообщение, не адресованное пользователю, который указан в базе данных Domino Directory. Серверу придется направить сообщение на интеллектуальный хост, который не относится к системе Notes, но имеет информацию относительно нужного адресата и потому передаст адресату полученное сообщение.

Чтобы сервер мог взаимодействовать с подобным интеллектуальным хостом, необходимо заполнить два поля на вкладке **Basics** документа конфигурации сервера (табл. 8.4).

Таблица 8.4. Поля документа конфигурации для направления сообщений на интеллектуальный хост

Поле	Назначение
Local Internet domain smarthost (Интеллектуальный хост локального домена сети Internet)	В это поле вводится имя хоста сервера, который обеспечивает управление каталогом для абонентов почтовой службы, не использующих почтовую службу Notes
Smart host is used for all local Internet domain recipients (Интеллектуальный хост для всех абонентов локального домена сети Internet)	Здесь задается вариант Enable (Разрешено) или Disable (Отмена — установлен в режиме по умолчанию). Когда эта функция разрешена, сервер посылает все сообщения на интеллектуальный хост и не пытается выяснить, кому они направлены — пользователям системы Notes или другим пользователям. При отмене функции сервер передает сообщения на интеллектуальный хост только после неудачной попытки обнаружить адресата в локальной базе данных Domino Directory

Настройка календаря и расписания

Несмотря на тот факт, что функции поддержки календаря и расписания в системе Notes не связаны непосредственно с передачей почтовых сообщений, они тем не менее косвенно участвуют в пересылке. Так, календари пользователей обычно являются разделами базы данных почтовой службы. При организации встреч, направлении приглашений и резервировании ресурсов пользователи неизбежно пересылают почтовые сообщения. Поэтому целесообразно рассмотреть функции поддержки календаря и расписания в контексте работы функции передачи почтовых сообщений.

Применение функций поддержки календаря и расписания не предполагает активного участия администраторов. При первом формировании домена Domino требуется создать базу данных Resource Reservations (Резервирование ресурсов) и провести ее конфигурирование. Кроме того, если планируется использование большого числа доменов системы Notes и большого числа пользователей, которые будут приглашать на встречи сотрудников, относящихся к другим доменам, требуется создать документ смежного домена (Adjacent Domain document) и, возможно, документ несмежного домена (Non-adjacent Domain document). Это позволит беспрепятственно производить поиск необходимых ресурсов в других доменах. Имеется также возможность организовать поиск свободных ресурсов в доменах почтовых служб cc:Mail и OfficeVision, но здесь необходим документ внешнего домена (Foreign Domain document). И наконец, можно сформировать документы выходного дня (Holiday document), предназначенные для различных неофициальных событий в жизни компании или необычных выходных дней, о которых следует проинформировать сотрудников. Для типичных выходных дней подобные документы создаются автоматически.

Принцип работы календаря и расписания

В системе Lotus Notes предусмотрен полномасштабный календарь, встроенный в стандартный шаблон базы данных почтовой службы. Эта функция обеспечивает организацию встреч, поиск свободных часов для них, рассылку приглашений и резервирование ресурсов (например, помещений для встреч). Пользователи могут получать с помощью календаря информацию о выходных днях компании, которая передается непосредственно в их базы данных почтовой службы.

Серверы Domino при поддержке этих функций используют две основные программы:

- О менеджер Schedule Manager (Менеджер календаря) проводит опрос баз данных пользователей и базы данных Resource Reservations, а также получает сведения о дате и времени для составления расписания. Программа запоминает полученную информацию в базе данных Free Time (Свободное время; файл busytime.nsf для автономного сервера или clubusy.nsf для сервера кластера), которая создается при первом запуске программы. При поиске одним пользователем свободных часов другого пользователя (или ресурса) Schedule Manager обеспечивает извлечение сведений о уже распределенном времени из файлов busytime.nsf/clubusy.nsf и передачу их в систему Notes. При этом система Notes будет показывать занятые часы в графическом виде, чтобы производящий поиск пользователь мог ознакомиться со свободными часами (или ресурсами) другого пользователя;
- О программа Calendar Connector (Коннектор календаря) применяется в тех случаях, когда требуется просмотреть свободные часы другого пользователя или ресурсы

другого сервера почтовой службы. Calendar Connector имеет возможность получать информацию от серверов почтовой службы других доменов системы Notes, а также доменов почтовых служб cc:Mail и Office Visual.

Программы Schedule Manager и Calendar Connector загружаются (в режиме по умолчанию) в память при запуске сервера и отмечены в файле notes.ini каждого сервера (параметры sched и calconn переменной ServerTasks). Они могут запускаться вручную с консоли сервера командами load sched и load calconn. Выгрузка этих программ из памяти производится с помощью команд tell sched quit и tell calconn quit соответственно.

Имеется также возможность загружать и выгружать упомянутые программы в Domino Administrator. Следует отметить, что программа Schedule Manager поддерживает и другие команды типа tell, которые можно запустить командами консоли или в программе Domino Administrator - см. вкладку **Server => Status** (Сервер => Статус).

Программы Schedule Manager и Calendar Connector способны исполняться непосредственно на серверах почтовой службы, на любом сервере, обеспечивающем поддержку базы данных Resource Reservations или приложения с функциями календаря и расписания системы Notes, а также серверами концентраторов и серверами, обеспечивающими связь между доменами. Эти программы свободно выгружаются из памяти любого сервера, который не управляет приложениями с функциями календаря и расписания, или сервера, не связанного с другими серверами или доменами.

Запросы на использование ресурсов, например помещения для встреч или проектора, хранятся в одной или нескольких базах данных Resource Reservations. Каждый ресурс представлен документом в базе данных Resource Reservations, а также документом ресурса (Resource document) в каталоге Domain Directory. Документ ресурса в базе данных Resource Reservations содержит описание ресурса и позволяет организовать его резервирование (бронирование). Этот специализированный документ базы данных входящих почтовых сообщений (Mail-In Database document) информирует маршрутизатор о передаче запросов на резервирование из базы данных пользователя в базу данных Resource Reservations. Документ ресурса должен создаваться непосредственно в базе данных Resource Reservations, однако при правильной настройке процесса Administration Process он может использоваться для автоматического создания документа ресурса в каталоге Domain Directory.

Формирование базы данных Resource Reservations

Можно создавать одну или большее число баз данных Resource Reservations, однако организации, как правило, ограничиваются одной подобной базой. В ряде случаев^ может потребоваться создать дополнительные базы данных Resource Reservations, например при наличии весьма удаленных и управляемых независимым образом офисов или при связи одной группы серверов с другой группой серверов только с помощью модемных соединений. Если планируется использовать несколько подобных баз данных, они не должны содержать одинаковых записей, касающихся одних и тех же ресурсов.

Обычно у пользователей не возникает желания реплицировать базы данных Resource Reservations и передавать их на большое число серверов, поскольку копии баз данных могут быстро устаревать. Кроме того, программа Calendar Connector позволяет быстро направить запрос по сети и получить все необходимые данные о ресурсах.

После создания базы данных Resource Reservations командой **File Database => New** (База данных файлов => Новый) следует сохранить ее на сервере. База данных ресурсов основана на шаблоне проектирования Resource Reservations (5.0), файл resrc50.nsf на сервере, или

Resource Reservations (6.0), файл resrc60.nsf на сервере. Имя для базы данных может задаваться произвольным образом (обычно ее называют Resource Reservations). Имя файла также может быть произвольным (но, как правило, оно соответствует resource.nsf). Необходимости шифровать, индексировать или ограничивать размеры данных нет. Тем не менее в диалоговом окне **Advanced Database Options** (Дополнительные параметры базы данных) допустимо задать **Don't montain unread marks** (Не поддерживать нечитаемые метки) и **Don't overwrite Free space** (Не перезаписывать свободное пространство).

При создании базы данных следует открыть список ACL командой **File => Database => Access Control** (Файл => База данных => Управление доступом). Проследите за тем, чтобы сервер, на котором создается база данных, и группа **LocalDomainServers** (Серверы локального домена) имели уровень доступа **Manager** (Менеджер). По умолчанию уровень доступа равен **Author** (Автор), что вполне подходит для большей части пользователей. Для некоторых пользователей может быть задан уровень доступа **Manager**, однако всем, кто будет участвовать в создании записей относительно ресурсов, следует присвоить статус **[CreateResource]** (Создание ресурсов) - тогда другим лицам создавать ресурсы будет запрещено.

База данных упорядочена по сайтам, ресурсам и резервированию ресурсов. На первом шаге создается один или несколько сайтов, а затем - ряд ресурсов, связанных с каждым сайтом. Для создания сайтов и ресурсов необходимо обладать статусом **[CreateResource]**, поэтому обычные пользователи имеют возможность только резервировать их.

Для создания сайта следует обратиться к любому виду, который содержит операцию **New site** (Новый сайт), и щелкнуть по соответствующей кнопке. Затем нужно ввести имя сайта и сохранить созданный документ. Если новый сайт не появляется на виде, нажмите функциональную клавишу F9 для обновления вида. Если после щелчка по кнопке **New site** появляется сообщение **You have insufficient access to perform this operation** (Недостаточный уровень доступа для выполнения данной операции), это может свидетельствовать о невозможности идентификации базой данных статуса **[CreateResource]** пользователя. Если на самом деле этот статус имеется в наличии, следует закрыть базу данных и сделать еще одну попытку.

После создания сайта можно переходить к формированию ресурсов, связанных с этим сайтом. Щелкните по кнопке **New Resource** (Новый ресурс), заполните открывшуюся форму **Resource** (Ресурсы), а затем сохраните и закройте ее. Поля формы и рекомендации по их заполнению приведены в табл. 8.5.

Таблица 8.5. Перечень полей для формы Resource

Поле	Назначение
Вкладка Type (Тип)	
Resource type (Тип ресурса)	В этом поле задается вариант Room (Помещение) или Other (Другие ресурсы)
Вкладка Resource Information (Информация о ресурсе)	
Name (Имя)	Поле предназначено для ввода информативного названия ресурса, которое позволило бы специалисту быстро его идентифицировать
Site (Сайт)	В данном поле из списка выбирается сайт, на котором хранится ресурс

Таблица 8.5. Перечень полей для формы **Resource** (окончание)

Поле	Назначение
Capacity (Производительность)	Это поле присутствует в том случае, если выбран вариант Room для поля типа ресурса. В нем указывается число сотрудников, которые могут эффективно работать в данном помещении
Category (Категория)	Поле появляется, если установлен вариант Other при выборе типа ресурса. Изначально категорий может не быть, однако после создания они будут отображаться в списке при формировании ресурсов на более поздних этапах. В качестве категорий могут выступать следующие варианты: Audio/video equipment (Аудио/видеооборудование), Transport (Транспортные средства), Computer equipment (Вычислительное оборудование) и т.п.
Description (Описание)	В поле следует помещать информативное описание, позволяющее идентифицировать ресурс для сотрудников, которые пытаются его зарезервировать
Вкладка Resource Owner Options (Характеристики владельца ресурса)	
Ownership type (Тип владельца)	В данном случае возможны следующие варианты: None (Отсутствует) - любой пользователь вправе зарезервировать данный ресурс, Only owner can book resource (Только владелец может резервировать ресурс), Others have to book it through the owner (Другие сотрудники могут резервировать ресурс через владельца), Only select list of people can book resource (Только сотрудники из списка могут резервировать ресурс), Only select list of people can book resource via autoproccessing (Только сотрудники из перечня могут резервировать ресурс в автоматическом режиме, другим сотрудникам потребуется получить подтверждение владельца). Temporarily disable reservations (Временное прекращение резервирования)
Owner's name (Имя владельца)	Поле открывается при выборе второго или четвертого варианта для предыдущего поля. При этом допускается ввести или выбрать имя из перечня
List of names (Список имен)	Поле выводится в том случае, когда выбирается третий или четвертый вариант для поля Ownership type . Имена можно вносить или отмечать в предлагаемом перечне

На вкладке **Availability Settings** (Параметры доступности) следует задать дни недели и время суток, в которые можно резервировать ресурс. В режиме по умолчанию временной интервал устанавливается от 9 часов утра до 5 часов вечера (в рабочие дни).

Когда документ ресурса сохранен, система Notes формирует запрос **Add resource** (Добавление ресурса) для службы Administration Process. После репликации и передачи запроса на административный сервер каталога Domino Directory процесс Administration Process, используемый сервером, создаст документ ресурса в каталоге Domain Directory. Этот документ подобен документу базы данных входящих почтовых сообщений (Mail-In Database document), но нужен не для почты, а для ресурсов. Сотрудники получают возможность резервировать ресурс с помощью собственных баз данных почтовой службы. После появления запроса на резервирование ресурса соответствующее почтовое сообщение будет передано в базу данных Resource Reservations.

Разрешение междоменного группового расписания в документе домена

Если предусматривается применение нескольких доменов, в них можно активизировать функцию просмотра свободных часов сотрудников. При этом необходимо создать (для каждого домена) соответствующие документы домена. Для смежных доменов потребуются документы смежного домена (Adjacent Domain document), а для несмежных - документы несмежных доменов (Non-adjacent Domain document). Области почтовых служб cc:Mail и OfficeVision нуждаются в документах внешнего домена (Foreign Domain document).

В любом случае - вне зависимости от типа создаваемых документов домена - придется заполнять одно весьма важное поле, которое может иметь различные названия и предназначено для задания имени поддерживающего функцию календаря сервера:

- в документах смежного и внешнего домена это поле называется **Calendar server name** (Имя сервера, поддерживающего функцию календаря), причем в нем вводится имя сервера календаря в другом домене;
- в документе несмежного домена поле имеет имя **Route requests through calendar server** (Маршрутизировать запросы через сервер календаря), и в нем указывается имя сервера для сквозного домена маршрута. Такой домен должен граничить с текущим доменом и несмежным доменом, для которого создается документ. Другими словами, на практике нельзя вводить более одного промежуточного домена между текущим и несмежным доменами.

Сервер, поддерживающий функцию календаря в домене, должен предоставлять доступ другим серверам (соседних доменов) с помощью соединений локальной сети, характеризующихся относительно высокими показателями быстродействия. В этом качестве может выступать практически любой сервер, исполняющий программы Schedule Manager и Calendar Connector.

Документы выходного дня

Вид **Holiday** (Выходные дни) базы данных Domino Directory обеспечивает хранение документов, связанных с выходными днями. Стандартные документы выходного дня (Holiday document) уже существуют и связаны с теми праздниками, которые отмечаются в разных странах мира, причем учитываются и религиозные праздники. Просмотреть существующие документы выходного дня можно в программе Domino Administrator, выполнив команду **Configuration => Miscellaneous => Holiday** (Конфигурирование => Вспомогательные данные => Выходные дни).

Чтобы задать на этом виде новые выходные дни, надо щелкнуть по кнопке **Add Holiday** (Добавление выходных дней). При задании выходного дня следует ввести его название, данные о времени проведения, число дней, число повторений и т.д. Кроме того, необходимо классифицировать выходные дни по странам и/или по религиозному признаку. Для событий или выходных дней самой компании допустимо придерживаться собственной классификации.

Пользователи могут импортировать информацию о выходных днях из базы данных Domino Directory и передавать ее в свои базы данных почтовой службы командой **Tools => Import Holidays** (Программные инструменты => Импорт выходных дней) на виде **Calendar** (Календарь). Появится диалоговое окно, в котором разрешается выбрать определенные

классы выходных дней (по странам, по религиозному принципу и т.д.) для переноса в собственную базу данных.

Проверка базы данных Free Time

Каждый раз в два часа ночи программа Schedule Manager проверяет базу данных свободного времени. Она делает это и при перезапуске сервера. Кроме того, проверку (на предмет наличия ошибок) можно выполнить управляющей командой `tell sched validate`. Если в ходе проверки обнаруживаются ошибки, тому имеются две причины:

- О есть база данных почтовой службы, но персонального документа для нее нет. Такую базу данных необходимо удалить;
- О существующий персональный документ информирует о наличии базы данных почтовой службы, но на самом деле она отсутствует. В этом случае следует создать базу данных и отредактировать или удалить персональный документ.

Настройка и поддержка совместно используемой почтовой службы

По умолчанию каждое сообщение почтовых служб системы Notes, POP и ШАР запоминается в базе данных системы Notes независимо от других сообщений. Этот подход имеет несколько заметных преимуществ по сравнению с применяемым многими почтовыми службами и системами хранением почтовых сообщений в одной большой базе. Главное достоинство первого способа заключается в том, что разрушение базы данных отразится только на одном пользователе, второе состоит в возможности разработать и применять более гибкие процедуры резервного копирования, а третье связано с относительной простотой процедуры переноса пользователя почтовой службы с одного сервера почтовой службы на другой.

В то же время подход, предусматривающий хранение на сервере Domino большого числа баз данных пользователей, имеет один существенный недостаток - необходимость репликации почтовых сообщений. Когда сообщение требуется скопировать для десяти сотрудников, эти десять копий хранятся на одном жестком диске, но в разных базах данных. Принцип совместного использования почтовой службы позволяет заметно экономить пространство на жестком диске за счет исключения копий сообщений и одновременно преодолеть недостатки единой базы данных.

В прошлом большая часть администраторов серверов Domino не решалась переходить на совместную почтовую службу в основном по двум причинам. Во-первых, при этом существенно усложняется работа самого администратора. Во-вторых, администраторы не верили, что в версии R4 удастся обеспечить хорошие показатели целостности больших баз данных системы Notes и надежное хранение многочисленных почтовых сообщений пользователей в одной базе. И наконец, не стоит забывать о том, что пространство на жестком диске весьма дешево. Поэтому администраторам нет смысла усложнять себе жизнь настройкой совместной почтовой службы, когда удастся решить все текущие проблемы за счет увеличения дисковой памяти.

Начиная с версии 5 по крайней мере один недостаток совместной почтовой службы был эффективно устранен. Так, введение функции регистрации транзакций и другие

усовершенствования заметно улучшили показатели целостности баз данных системы Notes (по сравнению с версией 4). Кроме того, мощная служба Administration Process позволила избавиться от некоторых проблем администрирования, связанных с применением совместной почтовой службы. Тем не менее прежде чем переходить к созданию такой службы, необходимо понять механизмы ее функционирования и ту роль, которая отводится самому администратору.

Принципы работы совместной почтовой службы

При применении совместной почтовой службы на сервере может располагаться одна или несколько совместно используемых баз данных почтовой службы. Эти базы данных называются Single Copy Object Stores (Хранение объектов с одной копией), или SCOS. Передавая сообщение в локальную базу данных почтовой службы, маршрутизатор разделяет его на две части. Заголовок сообщения, содержащий поля **To** (Кому), **From** (От кого) и подобные, направляется в базу данных почтовой службы абонента, а информационный раздел (тело) сообщения отсылается в совместно используемую базу данных почтовой службы. Маршрутизатор добавляет необходимые указатели в заголовок и информационный раздел. Назначение заголовка определяется его местоположением. Если сообщение адресуется нескольким абонентам сервера, информационный раздел будет снабжен несколькими указателями, по одному на каждую базу данных почтовой службы абонента.

При открытии пользователем сообщения сервер, на котором хранится база данных, выводит заголовок из базы данных почтовой службы пользователя, затем указатель для поиска информационного раздела и раздел из совместно используемой базы данных почтовой службы, после чего направляет абоненту объединенное сообщение. В этом случае пользователь даже не подозревает о том, каким образом хранится и формируется его сообщение.

В деталях механизм действия системы зависит от того, какое число (1 или 2) присутствует в поле **Shared_Mail** (Совместная почтовая служба). Для значения 1 информационный раздел хранится в совместно используемой базе данных почтовой службы только в том случае, когда сообщение адресуется двум или большему числу пользователей почтовой службы. Если в поле указано число 2, информационный раздел всегда будет заноситься в совместно используемую базу данных - независимо от числа абонентов.

Приведенное выше описание позволяет в первом приближении понять механизм взаимодействия, хотя его принципы, естественно, оказываются более сложными. Так, при выборе для поля **Shared_Mail** числа 1 маршрутизатор извлекает сообщение из файла mail.box и помещает его копию в базу данных почтовой службы первого абонента. Когда абонент всего один, процедура завершается. Если же абонентов несколько, то маршрутизатор направляет информационный раздел сообщения в совместно используемую базу данных почтовой службы, а копию заголовка - в базу данных почтовой службы каждого абонента, в том числе и первого. При этом предусматривается исключение полной копии того сообщения, которое было внесено на первом шаге в базу данных почтовой службы первого абонента.

При задании в указанном поле числа 2 маршрутизатор извлекает сообщение из файла mail.box и вводит его в информационный раздел совместно используемой базы данных почтовой службы. Затем он просматривает перечень абонентов. Если абоненты являются резидентами данного сервера почтовой службы, устройство помещает копию заголовка

сообщения в базу данных почтовой службы каждого из них. При условии, что среди абонентов нет резидентов данного сервера, маршрутизатор передаст сообщение на другие серверы, после чего удалит информационный раздел сообщения из совместно используемой базы данных почтовой службы.

Вывод о том, что первый подход более эффективен, кажется вполне закономерным. Однако на самом деле более плодотворным является второй вариант, поскольку он реализуется по умолчанию (при активизации функции использования совместной почтовой службы) и позволяет серверу самому выбирать способ хранения почтовых сообщений (см. следующий раздел).

Следует также отметить, что совместно используемая база данных почтовой службы хорошо защищена. Обычно ее данные шифруются с помощью открытого ключа сервера, а в самой базе наличие видов не предполагается. В этой ситуации сервер хоста является единственным объектом в списке ACL, а его имя отсутствует в диалоговом окне **Open Database** (Открытие базы данных).

Когда один из абонентов удаляет копию своего сообщения, указатель заголовка для этого абонента исключается из информационного раздела сообщения. В том случае, когда все абоненты исключают свои копии сообщения, предусматривается полное удаление информационного раздела (тела) сообщения из совместно используемой базы данных почтовой службы.

На практике можно создавать и применять несколько совместно используемых баз данных почтовой службы. Этот подход оказывается весьма полезным, поскольку он позволяет реализовать как все достоинства совместной почтовой службы (экономия пространства на жестком диске), так и преимущества, связанные с хранением сообщений в независимых и относительно небольших по размеру базах данных почтовой службы (более простое восстановление информации, меньший ущерб в случае ее повреждения). Считается, что наилучший способ хранения почтовых сообщений на сервере Domino состоит именно в создании нескольких совместно используемых баз данных почтовой службы с дальнейшим применением одной из них (по принципу ротации) для реальной записи сообщений.

При наличии большого числа подобных баз данных одна из них обычно бывает активной: маршрутизатор обращается к ней для записи вновь поступающих сообщений. Другие базы становятся архивными, поскольку в них хранятся предыдущие сообщения. Сервер всегда осведомлен о том, которая из баз данных активна, так как эта информация хранится в специальном файле базы данных (в текстовом файле mailobj.nsf), который содержит всего одну строку, указывающую имя активной в текущий момент базы данных.

Передавая поступившее сообщение локальным пользователям, маршрутизатор сначала просматривает содержимое файла mailobj.nsf, определяет активную на текущий момент базу данных и заносит в нее сообщение. При направлении на маршрутизатор данных, указывающих на необходимость применения другой базы, устройство поместит имя этой базы в файл mailobj.nsf и в дальнейшем будет обращаться именно к ней.

Путем периодического управления маршрутизатором (замены активной базы данных) можно распределять нагрузку между несколькими используемыми базами данных почтовой службы. Если какая-либо из них разрушится, отрицательный эффект окажется не таким значительным, поскольку в этой базе хранится только часть почтовых сообщений.

- Видимо, объем мероприятий, необходимых для внедрения и поддержки рассматриваемого подхода (особенно в версии 4), заставляет администраторов относиться к нему весьма прохладно. На практике администраторам и без того приходится выполнять достаточно

много работы и решать неотложные проблемы с пользователями, а этот способ требует заметных усилий с их стороны при переносе пользователей с одного сервера на другой или при полном удалении пользователя из нескольких баз данных. Тем не менее в версии 5 и 6 появляется возможность автоматизировать большинство этих операций с помощью документов программы (Program document). Кроме того, весьма мощная служба Administration Process берет на себя существенную часть операций по переносу и удалению пользователей. Таким образом, специалисты компании Lotus постарались устранить препятствия на пути внедрения совместной почтовой службы.

Настройка совместной почтовой службы

Разрешение на применение совместной почтовой службы может быть дано путем добавления в файл notes.ini переменной Shared_Mail=1, соответствующей варианту **Delivery Only** (Разрешение только доставки), или переменной Shared_Mail=2, отвечающей варианту **Transfer and Delivery** (Разрешение передачи и доставки). При наличии в этом файле переменной вида Shared_Mail=0 или в отсутствие переменных совместная почтовая служба просто отменяется. Активизировать данную службу можно непосредственно, например отредактировав файл notes.ini и перезапустив сервер. Но допустимо сделать это и косвенно, скажем добавив переменную в документ конфигурации (Configuration document). Последний способ предпочтительнее, поскольку отпадает необходимость повторного запуска сервера.

Для активизации совместной почтовой службы:

1. Откройте документ конфигурации, где указано имя сервера, для которого планируется активизировать совместную почтовую службу. Если такого документа нет, придется его создать.
2. На вкладке **NOTES.INI Settings** (Параметры файла notes.ini) выберите **Set/Modify Parameters** (Установка/модификация параметров).
3. В открывшемся диалоговом окне щелкните по небольшой вспомогательной кнопке, расположенной справа от поля **Item** (Пункт).
4. В диалоговом окне **Select a Standard Parameter** (Выбор стандартного параметра) отметьте **SHARED_MAIL** (Совместная почтовая служба), после чего щелкните по кнопке OK.
5. В поле **Value** (Значение) введите число 1 или 2, после чего выполните **Next** (Далее) или **Add** (Добавить) и щелкните по OK. При этом в документе конфигурации появится запись **SHARED_MAIL=n** 0
6. Сохраните и закройте документ конфигурации. В течение нескольких минут документ будет передан на соответствующий сервер, а сервер добавит переменную в файл notes.ini, создаст совместно используемую базу данных почтовой службы (файл mailobjl.nsf) и начнет активно обращаться к ней.

Поскольку переменная Shared_Mail добавляется в файл notes.ini сервера, этот сервер будет переходить в режим совместного использования почтовой службы при каждом своем запуске.

Разрешить совместную почтовую службу можно еще двумя способами. Так, управляющая команда консоли сервера tell router use shared.nsf позволяет сформировать требуемую базу данных (если она еще не создана) и разрешает применение совместной почтовой службы (если это не было сделано ранее). То же самое относится и к управляющей

команде `load object create shared.nsf`. В данных примерах и в приведенных ниже файл `shared.nsf` соответствует совместно используемой базе данных почтовой службы, а файл `usermail.nsf` - базе данных почтовой службы пользователя или каталогу почтовой службы.

Преимущество этих подходов состоит в том, что они позволяют сразу задать имя совместно применяемой базы данных почтовой службы. Не требуется указывать тип создаваемой и совместно используемой базы данных, поскольку сервер автоматически введет переменную `Shared_Mail=2` в файл `notes.ini`.

Когда планируется применение на сервере совместно используемой базы данных почтовой службы, необходимо руководствоваться следующим:

- если сервер не является сервером почтовой службы, задействовать подобную базу данных не рекомендуется, поскольку это не дает никаких преимуществ;
- если сервер играет роль сервера почтовой службы и концентратора почтовых сообщений (или по какой-либо иной причине обеспечивает передачу большого числа почтовых сообщений на другие серверы), лучше задавать для совместной почтовой службы режим **Delivery Only** (Только доставка), что соответствует записи `Shared_Mail=1`;
- если сервер служит окончательным или радиальным, который передает весьма небольшое число сообщений на другие серверы, имеет смысл для совместной почтовой службы назначить режим **For transfer and delivery** (Передача и доставка), что соответствует записи `Shared_Mail=2`.

Операции поддержки совместно используемой почтовой службы

Ниже представлен перечень операций, которые могут быть выполнены для совместной почтовой службы:

- создание новых совместно используемых баз данных почтовой службы;
- ротация существующих совместно используемых баз данных почтовой службы;
- создание, изменение и удаление связей файлов почтовых сообщений пользователей с совместно используемыми базами данных почтовой службы;
- исключение или включение файлов в процесс совместной почтовой службы;
- исключение ненужных файлов из совместно используемых баз данных почтовой службы;
- перенос файлов почтовых сообщений пользователей с одного сервера почтовой службы на другой;
- удаление файлов почтовых сообщений пользователей с сервера;
- удаление совместно используемых баз данных почтовой службы.

Создание совместно используемых баз данных почтовой службы

Сформировать такие базы данных можно посредством одной из двух упомянутых выше команд. Во-первых, командой вида

```
load object create scared.nsf
```

В память будет загружена задача `Object`, которая создаст новую базу данных. После этого задача удаляется из памяти, поскольку ее работа закончена. Однако созданная база данных еще не является активной, а маршрутизатор не может заносить в нее сообщения,

поскольку указанные действия не предусматривают редактирования файла mailobj.nsf. Такая команда оказывается весьма полезной при задании плана ротации совместно используемых баз данных почтовой службы (см. следующий раздел).

Во-вторых, создать базу данных и перевести ее в активное состояние допустимо с помощью управляющей команды

```
tell router use schared.nsf
```

В этом случае задача маршрутизации сформирует новую базу данных, а затем изменит файл mailobj.nsf так, чтобы он непосредственно указывал на новую базу. Теперь маршрутизатор будет направлять все сообщения в созданную базу данных.

Осуществление ротации для существующих совместно используемых баз данных почтовой службы

Для назначения совместной базы данных в качестве активной (то есть той, в которую маршрутизатор помещает вновь поступающие сообщения) предназначена следующая управляющая команда:

```
tell router use shared.nsf
```

Чтобы ту же самую операцию провести посредством документа программы, следует задать вариант nserver для поля **Program name** (Имя программы) и вариант -с 'tell router use shared.nsf' для поля **Command line** (Управляющая команда). При занесении записи в документ программы надо ввести фразу (команду) tell router quit с помощью двойных кавычек.

Для применения документов программы при формировании плана ротации баз данных почтовой службы необходимо создать:

- О от пяти до семи совместно используемых баз данных почтовой службы (по одной на каждый день недели) и поставить им в соответствие файлы mailobj1.nsf, mailobj2.nsf, mailobj3.nsf и т.д.;
- О по одному документу программы в расчете на каждую базу данных почтовой службы. Каждый из этих документов будет запускаться соответствующей управляющей командой в определенный день недели (в 4 часа утра): для файла mailobj1.nsf - в понедельник (командой tell router use mailobj1.nsf), для файла mailobj2.nsf - во вторник (командой tell router use mailobj2.nsf) и т.д.

В результате маршрутизатор будет добавлять новые сообщения в файл mailobj1.nsf в понедельник, в файл mailobj2.nsf во вторник, в файл mailobj3.nsf в среду - и так всю неделю. Эта схема соответствует варианту *еженедельной ротации* и позволяет весьма просто создавать документы программы. Другой план ротации (более динамичный) предусматривает обращение ко всем документам программ в течение одного дня, но в различные часы, например в 8 часов утра, в 9 часов утра, в 10 часов утра и т.д. Интересным следствием этих схем ротации является то, что относительный размер совместно используемых баз данных почтовой службы может указывать на объем почтовых сообщений, которые поступают в соответствующие дни недели (для первой схемы ротации) или ежедневно в определенные часы (для второй схемы ротации).

Связывание совместных баз данных

Скорее всего, первой управляющей командой после активизации базы данных почтовой службы на сервере Domino будет команда

```
load objectlinkusermail.nsf shared.nsf
```

Она разбивает на части имеющиеся сообщения базы данных почтовой службы пользователя и передает информационные разделы этих сообщений в новую базу данных почтовой службы. Если сервер перед этим работал достаточно долго, операция позволит высвободить значительную область памяти на жестком диске. Далее указанную команду надо будет исполнять лишь эпизодически. Взаимосвязи устанавливаются такими управляющими командами:

- О команда `load object link usermail.nsf schared.nsf` служит для установления связи между файлом почтовых сообщений пользователя и заполненным файлами почтовых сообщений каталогом с совместно используемым файлом почтовых сообщений;
- О команда `load object unlink usermail.nsf I schsred.nsf` отменяет взаимосвязи между пользовательской или совместно используемой базой данных почтовой службы и всеми файлами, с которыми она ранее была связана. Все информационные разделы снова переносятся в файлы почтовых сообщений пользователя. Команду можно применить перед переносом файла почтовых сообщений пользователя с сервера, например непосредственно перед удалением совместно используемого файла почтовых сообщений;
- О команда `load object link -relink usermail.nsf schared.nsf` ликвидирует существующие взаимосвязи с файлом почтовых сообщений пользователей, а затем восстанавливает необходимые связи файла почтовых сообщений пользователя с совместно используемым файлом почтовых сообщений.

Включение и исключение баз данных

На практике можно исключить базу данных почтовой службы пользователя (или папку, заполненную подобными базами данных) из совместной почтовой службы следующей управляющей командой:

```
load object set -never usermail.nsf
```

Чтобы снова вставить предварительно исключенную базу данных почтовой службы (или папку с подобными базами данных), надо ввести управляющую команду вида

```
load object reset -never usermail.nsf
```

Рекомендуется пользоваться управляющей командой `set -never` перед отменой взаимосвязей для файла (перед его переносом или удалением).

На практике можно также включить реплики файлов почтовых сообщений (или папку с подобными файлами) в совместно используемую базу данных почтовой службы посредством управляющей команды

```
load object set -always usermail.nsf shared, nsf
```

Кроме того, пользователи вправе исключать ранее включенные реплики файла почтовых сообщений (или папки с подобными файлами) из совместной почтовой службы с помощью управляющей команды

```
load object reset-alwaysusermail.nsf
```

Как правило, маршрутизатор переносит сообщения из файла mailbox в соответствующие базы данных и обеспечивает разделение сообщений на части после запуска совместно используемой базы данных почтовой службы. Следовательно, если база данных почтовой службы будет заполнена в процессе репликации, а не самим маршрутизатором, она не сможет активно участвовать в процессе применения совместной почтовой службы. Этот нюанс не следует упускать из виду (если маршрутизатор не работает с сообщением, оно не разделяется на две части).

Файл почтовой службы может заполняться в процессе репликации данных и в том случае, если он располагается на другом сервере (не на сервере почтовой службы пользователя). Допустим, например, что Джо Доакс находится в Нью-Йорке вместе со своим сервером почтовой службы. Если Джо тратит много времени на работу в Лондоне, у него наверняка есть реплика его базы почтовой службы на сервере в Лондоне, чтобы он мог читать письма, поступающие в его лондонский офис, без периодического переключения на сервер почтовой службы в Нью-Йорке.

Предназначенные для Джо письма направляются на сервер в Нью-Йорке, поскольку он является официальным офисным сервером. После этого сообщения реплицируются и направляются в реплику базы данных Джо на сервере в Лондоне. Поскольку маршрутизатор в Нью-Йорке обрабатывает сообщения Джо, они разделяются на две части, а информационные разделы заносятся в совместно используемую базу данных почтовой службы. В то же время, поскольку маршрутизатор в Лондоне не обрабатывает сообщения Джо, поступающие в лондонский офис, сообщения не разбиваются на две части на сервере почтовой службы в Лондоне. Управляющая команда `set -always`, исполняемая для базы данных почтовой службы Джо в Лондоне, заставляет маршрутизатор преобразовать сообщения и передать их в совместно применяемую базу данных почтовой службы, хранящуюся на сервере, причем даже в том случае, если сервер ранее эту базу не использовал.

Удаление ненужных файлов из совместно используемой базы данных почтовой службы

Весьма важной операцией по обслуживанию совместной почтовой службы является операция по удалению указателей и информационных разделов из совместно используемых баз данных почтовой службы в тех случаях, когда пользователи исключают заголовки из собственных баз такого типа. Эти операции выполняются автоматически для активной совместной базы данных почтовой службы. Однако следует убедиться в том, что они успешно проведены и для архивных совместно используемых баз данных почтовой службы.

Удаление можно провести вручную с помощью следующей управляющей команды на консоли сервера:

```
load object collect schared.nsf
```

Ту же операцию удастся автоматизировать. Имеется два способа инициирования функции автоматического сбора данных. Во-первых, можно добавить параметр `collection task` в переменную `ServerTasksAtn` файла `notes.ini`. Именно таким образом специалисты

компании Lotus советуют автоматизировать процедуру сбора данных для активной совместно используемой базы данных почтовой службы.

Если обратиться к переменной `ServerTasksAt2` в файле `notes.ini` любого сервера Domino, нетрудно увидеть, что одна из операций, которую сервер выполняет в два часа утра, соответствует команде `Object Collect mailobj.nsf`. Файл `mailobj.nsf` служит для задания взаимосвязей и указывает на активную (на текущий момент) совместно используемую базу данных почтовой службы и именно к нему обычно обращается команда `Object Collect`. На практике можно определить (в файле `notes.ini`) и другие параметры команды `Object Collect`, причем они добавляются к существующим переменным `ServerTasksAtn` или образуют новые переменные.

Во втором способе автоматизации операции сбора данных для неактивной совместно используемой базы данных почтовой службы требуется документ программы (Program document), обеспечивающий работу практически любой программы, которая в нем указана. Эти программы могут исполняться в конкретный день недели или в определенное время суток в зависимости от желания пользователя. Последнее придает документу программы заметную функциональную гибкость и делает его более эффективным средством, чем переменные `ServerTasksAtn`, которые запускают операции ежедневно в указанные часы.

Для создания документа программы необходимо запустить Domino Administrator и открыть вкладку **Configuration** (Конфигурация), затем раскрыть **Server** (Сервер) и выбрать **Programs** (Программы). После этого надо щелкнуть по кнопке **Add Program** (Добавление программы) и заполнить поля появившейся формы в соответствии с рекомендациями, приведенными в табл. 8.6.

Таблица 8.6. Перечень полей формы программы

Поле	Назначение
Вкладка Basics (Основные параметры)	
Programname (Имя программы)	В этом поле вводится имя файла для программы (без расширения имени файла). В рассматриваемом примере следует набрать имя <code>object</code> (Объект)
Command line (Управляющая команда)	В данном поле можно задавать любые аргументы (параметры) команды. В рассматриваемом примере нужен параметр <code>collect shared.nsf</code> , где <code>shared.nsf</code> соответствует имени файла для одной из совместно используемых баз данных почтовой службы
Server to be run on (Используемый сервер)	В поле вносится полное различающееся имя сервера <code>Domir>o</code>
Comments (Комментарии)	Здесь следует помещать описательную информацию о документе, так чтобы в будущем пользователь или его преемник могли без труда определить назначение документа и причину его создания
Вкладка Schedule (Расписание)	Здесь определяется расписание, в соответствии с которым будет исполняться программа

Рекомендуется создавать один документ программы на каждую совместно используемую базу данных почтовой службы. После этого разрешается удалить параметр `object collect mailobj.nsf` из переменной `ServerTasksAt2` в файле `notes.ini`, поскольку созданный документ программы сам позаботится об активной базе данных, а также об архивных

базах. Однако в ряде случаев можно управлять всеми совместно используемыми базами данных почтовой службы с помощью всего одного документа программы, что требует, правда, применения управляющей команды в виде `object collect` (без указания имени базы данных). Исполнение команды `Object Collect` без указания имени базы инициирует проведение работы по сбору информации для всех существующих баз данных упомянутого типа. Тем не менее пользователи могут предпочесть собирать сведения из различных баз и в разные дни и часы, чтобы обеспечить равномерное распределение информационной нагрузки во времени. Иногда информационные разделы сообщений теряются в совместно используемых базах данных почтовой службы - например, если они содержат указатель базы данных пользователя, которая уже не существует. Такая ситуация возникает при удалении или переносе базы данных почтовой службы с сервера без предварительной отмены взаимосвязей с совместно используемой базой данных почтовой службы. Как правило, команда `Object Collect` не обращается к таким потерянным сообщениям, а для удаления их из базы данных предназначена управляющая команда

```
load object collect-forcedatabase.nsf
```

Другой вариант команды `Object Collect` имеет вид

```
load object collect-nodelete
```

С помощью этой команды можно заранее просмотреть документы, которые будут исключены из базы данных, и увидеть, какой объем пространства на жестком диске удастся освободить. Пользователь, хорошо владеющий языками программирования C++ или Java, в состоянии написать программу, позволяющую предварительно проверять характер воздействия команды `Object Collect` на базу данных, и только потом запускать ее реально. Это дает возможность правильно оценить эффект от применения указанной команды, в частности в плане высвобождения памяти на жестком диске. Если такая программа будет составлена и даст положительные результаты, автор данной книги очень хотел бы ее получить, поскольку сам он не силен в программировании.

Перенос баз данных почтовой службы пользователей с одного сервера на другой

В версии 5 и 6 можно посредством процесса `Administration Process` перенести базы данных почтовой службы с одного сервера на другой. В том случае, когда требуется сделать это вручную;

1. Управляющей командой `load object set -never usermail .nsf` запретите внесение входящих почтовых сообщений в совместно используемую базу данных почтовой службы.
2. Управляющей командой `load object unlink usermail .nsf` переместите все информационные разделы сообщений из совместно используемой базы данных обратно в базу данных почтовой службы пользователя.
3. Создайте реплику базы данных почтовой службы пользователя на новом сервере почтовой службы, после чего реплицируйте в нее копии нужных сообщений.
4. Измените персональный документ (`Personal document`) пользователя в базе данных `Domino Directory`, назначив новый сервер почтовой службы.
5. Выполните репликацию изменений в персональном документе на все серверы домена.
6. Отредактируйте документы местоположения (`Location document`) пользователя и укажите новый сервер почтовой службы.

7. Реплицируйте две базы данных почтовой службы (в последний раз), чтобы гарантировать перенос всех сообщений в новую копию базы данных.
8. Удалите старую копию базы данных почтовой службы.
9. Если новый сервер почтовой службы применяет совместную почтовую службу, дайте управляющую команду `load object link usermail.nsf` для включения существующих сообщений в совместно используемую базу данных почтовой службы на новом сервере.

Удаление баз данных почтовой службы с сервера

В версии 5 и 6 процесс Administration Process позволяет выполнить подобную операцию автоматически. В том случае, когда требуется удалить базу данных вручную:

1. Управляющей командой `load object set -never usermail.nsf` запретите размещение входящих почтовых сообщений в совместно используемой базе данных почтовой службы.
2. Управляющей командой `load object unlink usermail.nsf` переместите все информационные разделы сообщений из совместно используемых баз данных в базу данных почтовой службы пользователя.
3. Введите адрес пересылки (при его наличии) в персональный документ пользователя, чтобы обеспечить нормальное перенаправление почтовых сообщений в будущем.
4. Реплицируйте изменения в персональном документе на все серверы домена.
5. Удалите старую базу данных почтовой службы.

Удаление совместно используемых баз данных почтовой службы

Перед удалением совместно используемой базы данных почтовой службы следует отменить ее связи с другими базами. Для этого требуется исполнить управляющую команду вида `load object unlink shared.nsf`. Затем можно перейти к удалению совместной базы данных почтовых сообщений.

Перед началом операции имеет смысл выждать в течение непродолжительного времени. Если число связей базы данных было достаточно большим, возможно, понадобится заметное время для их отмены и переноса информационных разделов сообщений обратно в базы данных почтовой службы пользователей. О продолжении активной стадии операции отмены связей можно судить по управляющей команде `show tasks`. Пока процесс остается активным, соответствующая операция присутствует в списке операций сервера, а по завершении процесса будет удалена из него.

Прежде чем применять эту команду в отношении большой совместно используемой базы данных почтовой службы, необходимо убедиться, что пользователь располагает нужным объемом памяти жесткого диска для хранения файлов почтовой службы пользователей, чьи сообщения связаны с удаляемой базой данных. Не следует забывать об основном назначении совместно используемой базы данных почтовой службы, которое состоит в экономии пространства на жестком диске за счет хранения только одной копии информационного раздела сообщений, адресованных нескольким пользователям. При отмене соответствующих связей число хранящихся на жестком диске копий может заметно возрасти.

В общем случае трудно дать четкий совет относительно методики определения объема пространства на жестком диске, которое потребуется для выполнения этой операции. Тем не менее ниже приводится ряд общих рекомендаций. Во-первых, если переменная

Shared_Mail равна 1 (совместная почтовая служба реализует только доставку), то для добавления сообщений в базу данных при отмене связей потребуется больше памяти на диске, чем когда переменная равна 2 (совместная почтовая служба с передачей и доставкой сообщений). Дело в том, что в первом варианте хранящиеся в совместно используемой базе данных почтовой службы информационные разделы сообщений обычно предназначены для множества пользователей. Во втором варианте в совместно используемой базе данных почтовой службы хранятся все информационные разделы сообщений, вне зависимости от числа пользователей. Поэтому можно ожидать, что в первом варианте при отмене связей появится большее число копий для большего числа пользователей.

Получить приблизительную информацию о требуемом объеме жесткого диска можно также с помощью управляющей команды `show start object`, позволяющей выводить статистические данные о содержимом всех совместно используемых баз данных почтовой службы. В частности, удастся узнать количество сообщений в базе данных, совместно применяемых различным числом пользователей. При этом становится ясно, какое число сообщений связано с одним файлом почтовых сообщений пользователя, какое - с двумя и т.д. Те же самые статистические данные содержатся в программе Domino Administrator на вкладке **Server => Statistics** (Сервер => Статистические данные).

Предположим, что все сообщения в первом приближении одинаковы по размеру. Тогда в результате несложных арифметических операций можно получить ответ на вопрос о том, насколько увеличится объем дисковой памяти после отмены связей. Например, простая совместно используемая база данных почтовой службы может занимать 6000 байт и содержать шесть сообщений со следующими параметрами:

- три сообщения для одного пользователя;
- два сообщения для двух пользователей;
- одно сообщение для трех пользователей.

Если предположить, что все сообщения одинаковы по размерам, то на одно сообщение приходится приблизительно 1000 байт памяти. При отмене связей три сообщения практически не изменятся по размеру, два сообщения увеличатся примерно вдвое, а одно сообщение потребует трехкратного увеличения памяти на диске. Картина в результате будет следующей:

- три сообщения для одного пользователя - каждое $\times 1 = 3000$ байт;
- два сообщения для двух пользователей - каждое $\times 2 = 4000$ байт;
- одно сообщение для трех пользователей - каждое $\times 3 = 3000$ байт.

Если теперь сложить все три значения, получится 10000 байт. Это и есть грубая оценка объема памяти на жестком диске, который понадобится для размещения сообщений.

Тонкая настройка маршрутизации почтовых сообщений в документах конфигурации

После завершения установки процедуры маршрутизации почтовых сообщений можно предусмотреть для нее тонкую (точную) настройку. Сервер Domino позволяет использовать большое число программных инструментов для настройки и совершенствования системы маршрутизации в целом. Эти инструменты связаны с наличием различных полей в документе конфигурации (Configuration document) и весьма удобно расположены на

соответствующих формах. Ниже инструменты подробно обсуждаются в последовательности, отвечающей их размещению на форме конфигурации.

Причина, по которой специалисты компании Lotus занесли эти поля в форму конфигурации, а не в форму сервера, состоит в том, что форма конфигурации в дальнейшем может послужить при создании документа конфигурации для всего домена, для группы серверов или для одного сервера.

Такой подход избавляет администраторов от большого объема ручной работы, но одновременно таит в себе целый ряд опасностей. Например, при формировании двух или большего числа документов конфигурации, управляющих работой одного сервера, система Notes может неверно распознавать ситуацию и неправильно задавать параметры сервера, что приведет к совершенно непредсказуемым результатам.

Не вызывает трудностей создание документа конфигурации для домена, группы серверов и одного сервера, но все эти документы могут так или иначе влиять на один конкретный сервер (именно так, кстати, и должны заполняться подобные документы). Параметры специальных документов конфигурации будут иметь более высокий приоритет по отношению к параметрам общих документов конфигурации (исключением является ситуация, подробно обсуждаемая в главе 11). Однако при создании нескольких документов конфигурации на одном уровне следует проявлять большую осторожность, чтобы они не были предназначены для управления одной и той же группой серверов, а в случаях, когда это необходимо, содержали параметры, не противоречащие друг другу. Указанная ситуация на практике чревата серьезными проблемами, поэтому рекомендуется по возможности ее избегать.

Параметры формы конфигурации, представляющие наибольший интерес (в данной главе книги), присутствуют в основном на вкладках **Router/SMTP** (Маршрутизатор/SMTP) и **MIME**. Ниже основное внимание будет сосредоточено на следующих параметрах этой вкладки:

- **Basics** (Основные параметры);
- **Restrictions and Controls** (Ограничение и управление);
- **Advanced** (Дополнительные параметры),

а также на целом ряде параметров вкладки **MIME**:

- **Basics** (Основные параметры);
- **Conversion Options** (Параметры преобразования);
- **Character Set Groups** (Параметры набора символов);
- **Advanced** (Дополнительные параметры).

Здесь не рассматриваются параметры вкладки **Message Tracking** (Отслеживание сообщений), поскольку данная тема подробно обсуждается в следующих главах. Если ранее в режиме по умолчанию был создан документ конфигурации для всего домена, придется заполнить дополнительную вкладку **LDAP** или **LDAP Settings** (Параметры протокола LDAP) в зависимости от того, каким образом открывается этот документ. Параметры вкладки будут в деталях проанализированы в главе 11.

Некоторые из упомянутых выше полей предусматривают задание вариантов разрешено/запрещено (**Allow/Deny**). Один из вариантов в этой паре разрешает выполнение операции или функции, называемой обычно по имени самого поля, а другой запрещает.

Поля с разрешением (**Allow**) имеют свои ограничения: имя пользователя должно быть занесено в определенные разделы, чтобы он мог инициировать выполнение той или иной функции. Если поле разрешения не заполнено, любой пользователь вправе применить

данную функцию. Если в поле разрешения присутствует только одна запись, другие пользователи не смогут активизировать эту функцию. Поля запрета (**Deny**), как правило, носят нестрогий характер. Если имя пользователя здесь отсутствует, он в состоянии задействовать функцию (с учетом тех ограничений, которые приведены в поле **Allow**). Если записи в поле отмены отсутствуют, фактически каждый пользователь имеет возможность применить данную функцию (также с учетом ограничений поля **Allow**).

Обычно достаточно делать записи в одном из указанных полей (а не в двух сразу). Рекомендуется заполнять поле **Allow** в тех случаях, когда планируется ввод небольшого числа записей, а поле **Deny** – если намечается применение функции для большей части пользователей. При внесении имен в оба поля поле **Deny** может быть выбрано только в части тех записей, которые присутствуют также и в поле **Allow**, поскольку поле **Deny** имеет более высокий приоритет.

Настройка основных параметров

Ниже приводятся перечень и основные функции полей подвкладки **Basics** (Основные параметры) вкладки **Router/SMTP** (Маршрутизатор/SMTP):

- **Number of mailboxes** (Число почтовых ящиков). По умолчанию в это поле заносится число 1, а для почтового ящика задается файл mailbox. При большой загруженности сервера почтовой службы, многочисленные пользователи которого пересылают сообщения одновременно, доступ к такому почтовому ящику может стать «узким местом» всей системы, что отрицательно скажется на показателях быстродействия сервера. Если задать в данном поле число 2 или большее, а затем перезапустить сервер, маршрутизатор создаст несколько почтовых ящиков с именами mail1.box, mail2.box и т.д., а пользователи почтовой службы будут получать быстрый доступ к одному из этих ящиков;
- **SMTP used when sending messages outside of the local internet domain** (Протокол SMTP используется при отправке сообщений вне локального домена сети Internet). Назначение этого поля подробно обсуждалось в начале главы. Оно служит для разрешения или запрета применения протокола SMTP при передаче сообщений, направляемых в сеть Internet;
- **SMTP allowed within the local internet domain** (Использование протокола SMTP разрешено в пределах локального домена сети Internet). Назначение этого поля также обсуждалось в начале данной главы. Оно предназначено для разрешения или запрета применения протокола SMTP в сообщениях, адресованных локальным пользователям;
- **Servers within the local Notes domain are reachable via SMTP over TCP/IP** (Доступ к серверам локального домена системы Notes обеспечивается с помощью протокола SMTP поверх TCP/IP). Назначение этого поля подробно обсуждалось в начале данной главы. Использовать его следует для разрешения протокола SMTP на сервере при передаче сообщений всем локальным серверам SMTP или только одному из серверов, относящемуся к соответствующей сети системы Notes;
- **Address lookup** (Поиск адреса). Поле служит для формирования сервером адресов сети Internet из адресов в базе данных Domino Directory. Вариант **Fullname only** (Только полное имя) предполагает обеспечение адекватного соответствия адресов сети Internet, формируемых для сообщений, адресам сети Internet, появляющимся в виде \$Users. Если не удастся обнаружить требуемый адрес, он считается некорректным.

Вариант **Local Part only** (Только локальный компонент) означает соответствие на уровне компонентов имени, располагающихся слева от значка @. Вариант **Fullname than Local Part** (Полное имя, а затем локальный компонент) предписывает проведение проверки сначала для варианта **Fullname only**, а затем - при неудачном поиске - для варианта **Local Part only**;

- **Exhaustive lookup** (Тщательный просмотр). При разрешении применения этой функции маршрутизатор будет производить поиск имен пользователей во всех доступных для него каталогах, а в отсутствие нужных имен попытается найти схожие с ними. Когда доступны несколько каталогов, гарантируется выявление всех совпадений. Описанный подход требует заметного увеличения времени поиска;
- **Relay host for messages leaving the local internet domain** (Промежуточный хост для сообщений локального домена сети Internet). Если сервер передает почтовые сообщения в сеть Internet через промежуточный хост, здесь следует указать имя этого хоста. Если же сервер имеет возможность доставлять почтовые сообщения непосредственно в домен адресата, поле заполнять не надо;
- **Local Internet domain smart host** (Интеллектуальный хост локального домена сети Internet). Когда в локальном домене сети Internet имеются пользователи почтовой службы, не относящиеся к доменам системы Notes, в этом поле вводится имя или IP-адрес хоста SMTP, не принадлежащего серверу Domino и выполняющего обработку почтовых сообщений для указанных пользователей почтовой службы;
- **Smart host is used for all local internet domain recipients** (Интеллектуальный хост для всех абонентов локального домена сети Internet). К данной функции приходится обращаться в тех случаях, когда все почтовые сообщения, поступающие из сети Internet (даже сообщения, адресованные пользователям системы Notes), должны проходить через интеллектуальный хост для специальной обработки;
- **Host name lookup** (Поиск имени хоста). Эта функция обеспечивает динамичный просмотр базы данных DNS (локальный просмотр осуществляется в файле локального хоста).

Установка ограничений

Вкладка **Router/SMTP => Restrictions and Controls => Restrictions**. Первые четыре поля этой вкладки связаны с получением почтовых сообщений от других доменов и организаций системы Notes. Остальные поля действуют на все входящие почтовые сообщения:

- **Allow mail only from domains** (Разрешение на получение почтовых сообщений только от доменов) - указывает на другие домены системы Notes, причем сообщения, поступающие от иных доменов, будут возвращаться отправителям;
- **Deny mail from domains** (Запрет на получение почтовых сообщений от доменов) - также указывает на другие домены системы Notes; почтовые сообщения, принимаемые из этих доменов, тоже будут возвращаться отправителям;
- **Allow mail from the folloing organizations and organizational units (* /Acme, * /Sales /Acme)** (Разрешение на получение почтовых сообщений от следующих организаций и организационных единиц). Почтовые сообщения, приходящие из организаций и организационных единиц, не внесенных в данное поле, будут возвращаться отправителям;

- **Deny mail only from the following organizations and organozational units (*Acme, */Sales/Acme)** (Запрет на получение почтовых сообщений от следующих организаций и организационных единиц). Почтовые сообщения, передаваемые перечисленными в поле организациями и организационными единицами, будут возвращаться отправителям;
- **Maximum message size** (Максимальный размер сообщения). В режиме по умолчанию в этом поле задается число 0 (КБ), что обозначает отсутствие каких-либо ограничений на размер сообщения. Если указать другое число, большие по размеру сообщения будут возвращаться отправителям;
- **Send all messages as low priority if message size is between** (Пересылка всех сообщений с низким уровнем приоритета, если размер сообщения соответствует указанному диапазону). При использовании этой функции появятся два других поля - в первом из них задается минимальный, а во втором - максимальный размер сообщения, которое должно пересылаться с низким уровнем приоритета. Если во второе поле ввести число 0, все почтовые сообщения, которые имеют размер, превышающий минимальный показатель, будут пересылаться с низким уровнем приоритета. Почта с низким приоритетом передается только в специально определенное нерабочее время;
- **Obey database quotas during message delivery** (Исполнение рекомендаций и квот базы данных при доставке сообщений, только версия R5). По умолчанию квоты базы данных действуют лишь при сохранении новых документов, а не их почтовой пересылки. Однако параметры режима по умолчанию могут быть изменены. Не исключено, что при превышении квоты сообщения не будут приниматься и вернутся обратно отправителям.

Блокирование сквозной почты через домен

Вкладка **Router/SMTP=>Restrictions and Controls=>SMTP Inbound Controls=>Inbound Relay Controls**. Поля этой вкладки позволяют запретить внешним хостам или доменам пересылать почтовые сообщения через данный домен в другие домены системы Notes или сети Internet. Одна из целей формирования такого запрета - блокирование сквозной почты через домен, что иногда предпринимается для сокрытия реального источника той или иной информации. Другой причиной подобного запрета является экономия весьма дорогостоящей полосы пропускания.

В двух описанных ниже полях могут быть указаны имена доменов системы Notes или сети Internet. В этом случае именам системы Notes должен предшествовать символ %, а запись асмехот обеспечит блокирование почты из доменов асмехот и sales.асмехот. Выбор варианта записи @асме.com позволит блокировать поступление сообщений от домена с именем асмехот, но не sales.асмехот. Итак:

- **Allow messages from external internet domains to be sent only to the following internet domains** (Разрешить сообщениям из внешних доменов Internet поступать на следующие домены сети Internet) - почтовые сообщения будут передаваться только в перечисленные здесь домены;

- **Deny messages from external internet domains to be sent to the following internet domains** (Запретить сообщениям из внешних доменов Internet поступать на следующие домены сети Internet) - почтовые сообщения не будут доставляться в домены, имена которых внесены в это поле. Имеется также возможность вводить звездочку (*) для блокирования всех транзитных сообщений.

В следующие два поля надо вписать полностью квалифицированные имена домена или хоста (или соответствующие IP-адреса). При вводе asme.com блокируется передача сообщений, поступающих от всех хостов домена asme.com. IP-адреса принято заключать в квадратные скобки и использовать звездочки для отмены целых подсетей. Например, запись [10.0.0*] может использоваться для блокирования каждого хоста, IP-адрес которого начинается с 10.0.0. Вот эти поля:

- **Allow messages only from the following external internet hosts to be sent to external internet domains** (Разрешить сообщениям от следующих внешних хостов поступать на следующие внешние домены сети Internet) - только те хосты, чьи имена присутствуют здесь, смогут обращаться к данному домену как к промежуточному;
- **Deny messages from the following external internet hosts to be sent to external internet domains** (Запретить сообщениям от следующих внешних хостов поступать на следующие внешние домены сети Internet). Тем хостам, имена которых здесь указаны, запрещено пользоваться данным доменом для транзитных целей.

Контроль соединений хостов

Вкладка **Router/SMTP=>Restrictions and Controls=>SMTP Inbound Controls=>Inbound Connection Controls**. Три поля этой вкладки позволяют отменять соединения хостов (их целесообразно сравнить с тремя полями следующей вкладки, в которых можно запретить получение почтовых сообщений, направляемых определенными пользователями):

- **Verify connecting hostname in DNS** (Проверка в базе данных DNS имен подключающихся хостов). При активизации этой функции сервер запретит формирование соединения с любым хостом, имя которого не обнаруживается в системе DNS.

Два следующих поля предназначены для ввода полностью квалифицированных имен домена или хоста либо соответствующего IP-адреса. При вводе asme.com блокируется передача сообщений, поступающих от всех хостов домена asme.com. IP-адреса принято заключать в квадратные скобки и использовать звездочки для отмены целых подсетей. Например, запись [10.0.0*] заблокирует все хосты, IP-адрес которых начинается с 10.0.0.

- **Allow connections only from the following SMTP internet hostnames/IP addresses** (Разрешить подключения SMTP только для следующих имен хостов/IP-адресов). Хосты, чьи имена отсутствуют в этом поле или чьи адреса отсутствуют в соответствующем списке, не подключатся к данному серверу. Следовательно, они не смогут передать ему почтовые сообщения;
- **Deny connections from the following SMTP internet hostnames/IP addresses** (Запретить подключения SMTP только для следующих имен хостов/IP-адресов). Хосты,

чьи имена приводятся в данном поле или чьи IP-адреса содержатся в соответствующем списке, не смогут подключиться к данному серверу. Следовательно, они не вправе передавать ему почтовые сообщения.

Блокирование входящих почтовых сообщений

Вкладка **Router/SMTP => Restrictions and Controls => SMTP Inbound Controls => Inbound Sender Controls**. Ниже перечислены поля, которые предоставляют возможность блокировать почтовые сообщения на основе анализа параметров отправителя (рекомендуется сравнить эти поля с тремя предыдущими, служащими для блокирования подключений к хостам- SMTP):

- **Verify sender's domain in DNS** (Проверка домена отправителя в базе данных DNS). При активизации данной функции сервер откажется от приема почтовых сообщений, поступающих от отправителя, имя которого не найдено в системе DNS.

В двух следующих полях можно вводить имена доменов или адреса электронной почты. Домен в таком случае играет роль подстановочного шаблона, причем запись `acme.com` подразумевает адрес `*.acme.com`. Адреса должны быть заданы точно, так что запись `doaks@acme.com` не подразумевает адрес `jdoaks@acme.com`;

- **Allow messages from the following external internet addresses/domains** (Разрешение на прием сообщений только от следующих внешних адресов/доменов Internet). Сообщения, поступающие от не указанных в этом поле объектов, будут блокироваться;
- **Deny messages from the following external internet addresses/domains** (Запрет на прием сообщений, поступающих от следующих внешних адресов/доменов Internet). Сообщения, поступающие от объектов, которые перечислены в данном поле, также будут блокироваться.

Ограничение приема почтовых сообщений из сети Internet

Вкладка **Router/SMTP => Restrictions and Controls => SMTP Inbound Controls => Inbound Intended Recipients Controls**. Следующие два поля служат для ограничения приема абонентами почтовых сообщений, поступающих из сети Internet:

- **Allow messages intended for the following internet addresses** (Разрешение на прием¹ сообщений только для следующих адресов сети Internet). Если адресат сообщения не указан здесь, сообщение будет блокироваться; *
- **Deny messages intended for the following internet addresses** (Запрет на прием сообщений, предназначенных для следующих адресов сети Internet). Если адресат сообщения указан в поле, сообщение также будет заблокировано.

Управление исходящими почтовыми сообщениями

Вкладка **Router/SMTP => Restrictions and Controls => SMTP Outbound Controls => Outbound Sender Controls**. Первые два поля позволяют управлять почтовыми сообщениями с учетом адреса сети Internet, данного отправителю. Остальные поля дают возможность управлять почтовыми сообщениями с учетом адреса системы Notes, присвоенного отправителю. В обоих случаях указываются локальные адреса Internet и системы Notes:

- **Allow messages only from the following Internet addresses to be sent to the Internet** (Разрешение на отправку сообщений в Internet, поступающих только от следующих адресов сети Internet). Только те отправители, которые указаны в этом поле, имеют возможность направлять почтовые сообщения в сеть Internet;
- **Deny messages only from the following Internet addresses to be sent to the Internet** (Запрет на отправку сообщений в Internet, поступающих только от следующих адресов сети Internet). Тем отправителям, которые здесь названы, не будет разрешено направлять почтовые сообщения в сеть Internet;
- **Allow messages only from the following Notes addresses to be sent to the Internet** (Разрешение на отправку сообщений в Internet, поступающих только от следующих адресов системы Notes). Только отправители, которые перечислены в данном поле, имеют возможность направлять почтовые сообщения в сеть Internet;
- **Deny messages from the following Notes addresses to be sent to the Internet** (Запрет на отправку сообщений в Internet, поступающих только от следующих адресов системы Notes). Отправителям, указанным в этом поле, запрещено направлять почтовые сообщения в сеть Internet.

Управление доставкой почтовых сообщений

Вкладка **Router/SMTP => Restrictions and Controls => Delivery Controls**. Ниже приводится перечень полей, позволяющих управлять процессом доставки почтовых сообщений:

- **Maximum delivery threads** (Максимальное число потоков доставки). По умолчанию маршрутизатор задает это число с учетом доступного объема памяти. Специалисты компании Lotus рекомендуют вводить числа в интервале от 1 до 25 в зависимости от характера информационной нагрузки сервера;
- **Encrypt all delivered mail** (Шифрование всех доставляемых почтовых сообщений). При активизации данной функции сервер обеспечивает шифрование всех доставляемых ему сообщений, а при ее отмене шифрует только сообщения, специально помеченные отправителями и абонентами;
- **Pre-delivery agent timeout** (Тайм-аут агента предварительной доставки). В этом поле указывается временной интервал для выполнения агентом предварительной доставки своей работы. По умолчанию интервал равен 30 с.

Управление пересылкой почтовых сообщений

Вкладка **Router/SMTP => Restrictions and Controls => Transfer Controls**. Поля этой вкладки обеспечивают управление процессом пересылки сообщений:

- **Maximum transfer threads** (Максимальное число потоков пересылки). По умолчанию маршрутизатор назначает число потоков пересылки с учетом доступного объема памяти. Можно изменять значение, указанное маршрутизатором. Специалисты компании Lotus рекомендуют задавать это число в диапазоне от 1 до 25 в зависимости от реальной информационной нагрузки сервера;
- **Maximum concurrent transfer threads** (Максимальное число одновременных потоков пересылки) - максимальное число потоков, выделяемых сервером Domino для

Ф

передачи сообщений одному адресату. По умолчанию здесь указывается число, соответствующее половине максимального потока пересылки;

- О **Maximum hop count** (Максимальное число переходов). В данном поле определяется максимально допустимое число переходов перед формированием отказа в доставке сообщения. По умолчанию оно равно 25;
- О **Low priority mail routing time range** (Временной интервал для передачи почтовых сообщений с низким уровнем приоритета). По умолчанию назначается временной интервал с 12 часов дня до 6 часов утра, причем допускается по своему усмотрению менять его границы;
- О **Initial transfer retry interval** (Исходный временной интервал повторной пересылки) - временной интервал в минутах, в течение которого сервер будет оставаться в режиме ожидания после первого отказа при попытке передачи сообщения (до второй попытки). По умолчанию здесь установлено 15 минут, причем после каждого очередного отказа сервер увеличивает это значение;
- О **Expired message purge interval** (Временной интервал для удаления сообщений) Здесь указывается, как часто маршрутизатору надлежит проверять просроченные сообщения. По умолчанию задается временной интервал, равный 15 минутам.

Использование входящих команд протокола SMTP

Вкладка **Router/SMTP => Advanced => Commands and Extensions => Inbound SMTP Commands and Extensions**. По прошествии нескольких лет с момента публикации документов RFC 821 и RFC 822 был осуществлен целый ряд расширений и изменений, утвержденных в других документах RFC. Представленные ниже поля соответствуют специальным командам, благодаря которым сервер Domino способен удовлетворить требованиям документов RFC 821 и RFC 822, а также более поздних документов RFC. Пользователи могут применять или отменять соответствующие функции по своему усмотрению:

- О **SIZE extension** (Расширение размера). Эта функция установлена по умолчанию. Сервер будет отменять входящие сообщения, которые по размеру превышают максимальный оговоренный размер, заданный на странице **Router/SMTP => Restrictions and Controls => Restrictions**;
- О **Pipelining extension** (Расширение конвейерного режима). Данная функция активируется по умолчанию. Разрешается пересылка нескольких команд SMTP в одном сетевом пакете для ускорения передачи сообщений SMTP;
- О **DSN extension** (Расширение DSN). Функция отменяется по умолчанию. При ее активизации сервер Domino будет реагировать на запросы о статусе доставки и отвечать соответствующими уведомлениями;
- О **8 bit MIME extension** (Расширение восьмиразрядного формата MIME). Функция отменяется по умолчанию. При ее активизации сервер Domino будет пытаться пересылать восьмиразрядные сообщения. Если другой сервер или хост примет сообщение в восьмиразрядном формате, сервер Domino вернется к использованию кодирования семью разрядами. Данная функция оказывается весьма полезной для кодировок с поддержкой символов нескольких языков;

- **HELP command** (Команда HELP). Функция активизируется по умолчанию. При ее отмене сервер Domino не будет исполнять команды **HELP** (Справка);
- **VRFY command** (Команда VRFY). Функция отменяется по умолчанию, при этом сервер Domino не исполняет команды, требующие проверки имен пользователей;
- **EXPN command** (Команда EXPN). Функция отменяется по умолчанию. Сервер Domino не исполняет команды, связанные с рассылочными почтовыми списками;
- **ETRN command** (Команда ETRN). Функция отменяется по умолчанию. Сервер Domino не принимает запросы **PULL** (Вытягивание), поступающие от других хостов SMTP. Возможно, данную функцию потребуется активизировать на сервере Domino, который вынужден ожидать формирования соединения с другим сервером прежде, чем он сможет передать почтовые сообщения на вызывающий сервер;
- **SSL negotiated over TCP/IP port** (Согласование режима SSL с помощью порта протокола TCP/IP). Функция отменяется по умолчанию. При ее активизации появляется возможность применять защищенное соединение SMTP.

Использование исходящих команд протокола SMTP

Вкладка **Router/SMTP => Advanced => Commands and Extensions => Outbound SMTP Commands and Extensions**. Ниже приводится перечень полей, позволяющих улучшить использование исходящих команд протокола SMTP:

- **SIZE extension** (Расширение размера). Функция активизируется по умолчанию. Сервер откажется передавать исходящие сообщения, размер которых превышает максимально допустимый уровень и которые заданы на странице **Router/SMTP => Restrictions and Controls => Restrictions**;
- **Pipelining extension** (Расширение конвейерного режима). Данная функция активизируется по умолчанию и позволяет другому серверу пересылать несколько команд в одном сетевом пакете;
- **DSN extension** (Расширение DSN). Эта функция по умолчанию отменяется. При ее активизации сервер Domino получает возможность отвечать на запросы о статусе доставки;
- **8 bit MIME extension** (Расширение восьмиразрядного формата MIME). По умолчанию данная функция отменяется. При ее активизации сервер Domino получает возможность принимать восьмиразрядные сообщения.

Настройка функций вспомогательного управления

Вкладка **Router/SMTP => Advanced => Controls => Miscellaneous Controls**. Это поле предназначено для улучшения функций вспомогательного управления:

- **Logging level** (Уровень регистрации). По умолчанию в поле задан вариант **Normal** (Нормальный). Другие возможные варианты: **Minimal** (Минимальный), **Informational** (Информационный) и **Verbose** (Полный). Варианты **Informational** и **Verbose** следует применять только в режимах поиска неисправностей.

Управления передачей сообщений

Вкладка **Router/SMTP => Advanced => Controls => Advanced Transfer Controls**. Следующие два поля позволяют улучшить управление передачей сообщений:

- **Ignore message priority** (Игнорирование приоритета сообщения). При активизации этой функции сервер будет игнорировать параметры приоритета сообщения отправителя и преобразовывать все сообщения по приоритету **Normal**;
- **Dynamic cost reset interval** (Временной интервал для динамического изменения стоимости) - временной интервал, по истечении которого маршрутизатор изменяет стоимость маршрута, постоянно возрастающую за последний период времени, и возвращает ее к исходному значению. По умолчанию этот временной интервал задается равным 60 минутам. Следовательно, если стоимость маршрута увеличилась из-за отказа соединения, например, с 1 до 2, то по истечении 60 минут она снова будет равна 1.

Настройка режима передачи/доставки сообщений

Вкладка **Router/SMTP => Advanced => Controls => Additional Controls (Delivery and Transfer)**. Представленные ниже поля также дают возможность улучшить режим передачи/доставки сообщений:

- **Restrict name lookups to primary directory only** (Ограничение на поиск имен только в пределах основного каталога). По умолчанию эта функция отменяется. Пользователи способны производить поиск имен как в основном каталоге, так и в дополнительных каталогах, помещенных в базу данных Directory Assistance (Поддержка каталога). При активизации функции выполняется поиск только в основных каталогах (без учета дополнительных);
- **Cluster failover** (Преодоление последствий отказа кластера). Поле может быть использовано лишь в том случае, когда домен содержит серверный кластер Domino. При активизации функции доставка почтовых сообщений обеспечивается даже при отказе некоторых серверов этого кластера. Предусмотрены следующие варианты: **Disabled** (Отмена), **Enabled for last hop only** (Разрешено только для последнего перехода; задается по умолчанию) и **Enabled for all transfers in this domain** (Разрешено для всех пересылок в данном домене). Второй вариант связан с передачей сообщения другому серверу кластера (если сервер почтовой службы абонента отказывает), который должен принять на себя управление в случае отказа данного сервера. Третий вариант предлагает пересылать сообщения другим серверам кластера в случае отказа любого из серверов (этого кластера) на маршруте передачи сообщения;
- **Hold undeliverable** (Хранение без доставки). По умолчанию данная функция отменяется. При ее активизации не переданные ранее почтовые сообщения будут храниться в файле mailbox, а не возвращаться отправителям.

Указание пути к файлу описания события

Вкладка **Router/SMTP => Advanced => Controls => Failure Messages**. В каждом из перечисленных ниже полей задают путь к текстовому файлу, который содержит дополнительное

описание, выводимое для пользователя вместе со стандартным текстом сообщения об определенном событии. В этих полях допускается добавлять текст на иностранном языке, указывать телефонный номер для обращения за помощью в ситуации, определяемой данным событием, и подобную информацию. Разрешено выделять специальные файлы для событий следующих типов (файлы указываются в одноименных полях):

- **Transfer failure** (Отказ при передаче сообщений);
- **Delivery failure** (Отказ при доставке сообщений);
- **Message expiration** (Завершение срока действия сообщений);
- **Domain failure** (Отказ в домене);
- **Server failure** (Отказ сервера);
- **Username failure** (Отказ при использовании имени пользователя);
- **Size failure** (Отказ при превышении размера сообщения);
- **Restriction failure** (Отказ при нарушении ограничений).

Использование формата MIME серверами Domino и системой Notes

Если только пользователь не начал чтение книги именно на этой странице, он уже должен знать о том, что для поддержки стандартов сети Internet серверы Domino и система Notes версий 5 и 6 предусматривают применение формата MIME (Multipurpose Internet Mail Extensions - многоцелевые почтовые расширения сети Internet). В данном формате подготавливаются сообщения электронной почты, он является альтернативным по отношению к расширенному текстовому формату самой системы Notes и поддерживается намного шире, чем в предыдущих версиях системы Notes/Domino. Так, версия 4.6 ограничивалась поддержкой форматирования сообщений, получаемых от программ почтовой службы сети Internet, преобразованием их текстовой части в расширенный текстовый формат системы Notes и представлением содержимого сообщения (в формате MIME) в виде одного или нескольких вложений. Начиная с версии 5 система Notes обеспечивает распознавание и работу с форматом MIME в форматах внутренних документов.

В результате появился целый ряд возможностей, позволяющих различным образом задавать параметры работы с форматом MIME. Для серверов Domino эти параметры указаны в основном на форме **Configuration** (Конфигурация), но как минимум один параметр присутствует на форме **Person** (Сотрудник). В системе Notes такие параметры имеются на форме **International MIME Settings** (Параметры международного формата MIME) базы данных Personal Address Book, а также на страницах **International** (Международный), **Mail** (Почтовая служба) и **News** (Новости) вкладки **User Preferences** (Предпочтения пользователя). Более подробная информация относительно задания предпочтений для формата MIME в системе Notes содержится в главе 13, а использование формата MIME в серверах Domino обсуждается ниже.

Принципы действия формата MIME

Для лучшего понимания роли формата MIME в сервере Domino и системе Notes следует разобраться в механизме функционирования самих протоколов MIME и SMTP, с которым и знакомит данный раздел.

Сообщение, удовлетворяющее требованиям протокола SMTP (документ RFC 822), обычно содержит заголовок и информационный раздел (тело сообщения). В документе RFC 822 весьма подробно описывается заголовок сообщения, тогда как информационному разделу внимание практически не уделяется. Заголовки сообщений обычно включают в себя ряд полей, каждое из которых занимает одну строку. *Синтаксис поля* соответствует варианту `fieldname: value; comment` (Имя поля: параметр; комментарии), причем комментарии допускается приводить в произвольном виде. Пример заголовка сообщения (в заголовках сообщений могут применяться и другие поля):

Date (Дата) : 22 Aug99 0932 EST
From (От) : rkirk
Subject (Предмет) : (описаниетемы)
Sender(Отправитель) :Rkirk@example1.com
Reply-To (Вответна) : Rkirk@example1.com
To (Кому) : JDoaks@example2.com
Message ID (Идентификационные данные сообщения) : (идентификатор сообщения)

В то же время документ RFC 822 не предъявляет практически никаких требований к информационному разделу сообщения, который может быть сформирован произвольно, подготовлен с помощью кодировки US-ASCII и не имеет ограничений на размер.

Естественно, пользователям достаточно часто приходится передавать сообщения, которые содержат символы, отличные от символов кодировки US-ASCII, например форматированный текст, текст в иной кодировке или нетекстовые данные. Протокол MIME (документы RFC 2045-2049) предлагает стандартное решение подобных вопросов, в частности допускает отступления от требований документа RFC 821, состоящие в использовании:

- О наборов символов, отличных от символов кода US-ASCII, в заголовках и информационных разделах сообщений (документ RFC 822);
- О расширяемого набора форматов для нетекстовых компонентов информационного раздела сообщений;
- О многокомпонентных информационных разделов сообщений (например, совместное использование обычного текста, вложенного файла, вложенного изображения и т.д.).

Информационный раздел сообщения (в формате MIME) может содержать один или большее число компонентов. При наличии нескольких компонентов каждый из них отделяется от остальных с помощью декларированного разделительного символа. В сообщении формат MIME указывается путем включения в заголовок определенных полей. Кроме того, каждый компонент информационного раздела сообщения (в формате MIME) может иметь специальные поля.

Стандартные поля в заголовке сообщения формата MIME:

- О **MIME-Version** (Версия протокола MIME). В этом поле указывается версия протокола MIME, которой соответствует данное сообщение. По умолчанию задается вариант 1.0, причем данное поле должно быть расположено в верхней части заголовка, а не между компонентами информационного раздела;
- О **Content-Type** (Тип содержимого). Здесь определяется тип содержимого для информационного раздела сообщения. Синтаксис поля: `Content-Type: type/subtype; [parameter=value]` (Тип содержимого: тип/подтип; [параметр=величина]). В настоящее время существует семь типов содержимого: текст, изображение, аудио- и видеoinформация, приложение, многокомпонентный раздел и сообщение. В каждом

типе имеется один или несколько подтипов. Например, в типе «текст» есть два подтипа: обычный текст и HTML. Некоторые типы содержимого предусматривают использование параметров или могут задаваться в произвольном виде. Скажем, тип «текст» (text) предполагает применение параметра charset (charset=cТроKa). В отсутствие этого параметра набор символов полагается соответствующим коду US-ASCII. Другая возможная величина для такого параметра (в соответствии с документом RFC 2046 и в дополнение к кодам US-ASCII) представлена ISO 8859-X, где X соответствует числу в диапазоне от 1 до 10 и определенному набору символов, оговоренному в документе ISO 8859 (на момент опубликования документа RFC 2046). Наборы символов документа ISO 8859 служат в настоящее время в качестве официальных наборов символов сети Internet. Тип «многокомпонентный раздел» (multipart), Boиnбaгy=строка, требует обязательного параметра boundary, который ограничивает компоненты многокомпонентного информационного раздела и отделяет их друг от друга;

- О **Content-Transfer-Encoding** (Кодирование передаваемого содержимого). В этом поле указывается способ кодирования для содержимого информационного раздела сообщения MIME. Если такого поля в сообщении нет, то полагается (по умолчанию), что информационный раздел закодирован посредством семиразрядного формата согласно документу RFC 811. Другие возможные варианты: **Shit** (Восемь разрядов), **Binary** (Двоичный), **Quoted-printable** (С кватированием при печати) и **Base64**;
- О **Content-ID** (Идентификационные данные содержимого). Обычно это поле появляется в начале информационного раздела сообщения MIME. Оно позволяет идентифицировать данный раздел, чтобы на него можно было ссылаться в компонентах других информационных разделов сообщений MIME с помощью соответствующих идентификационных данных;
- О **Content-Description** (Описание содержимого). Поле может появляться в начале каждого компонента информационного раздела сообщения MIME. Здесь вводится информация относительно соответствующего компонента информационного раздела или информационного раздела в целом.

В дополнение к названным полям протокол MIME (документ RFC 2045) предусматривает использование других полей. Единственным ограничением для дополнительных полей в данном случае является наличие в их именах компонента **Content** (Содержимое).

Протокол MIME также позволяет использовать «частные» (private, введенные пользователями) типы и подтипы содержимого. Другими словами, отправитель и адресат вправе выбирать типы или подтипы содержимого и способы кодирования передаваемых сообщений, которые не соответствуют общеизвестным стандартам. Единственным¹ требованием при этом является применение в качестве метки обозначения x-tokens (для типов/подтипов/способов). Например, домены PlanetNotes и Stillwater могут совместно использовать подтип текста, имеющий имя PigLatin. Протокол MIME требует метки x-piglatin, которая привносится в сообщения MIME.

Если пользователю когда-нибудь доводилось работать с сообщениями MIME в текстовом редакторе (способном интерпретировать формат MIME), он, вероятно, знает, что они выглядят так, как показано ниже (пример заимствован из документа RFC 2046):

From (От) : Whomever

To (Для) : Someone

Date (Дата) : Whomever

Subject (Тема) : Whomever

MIME Version (Версия MIME) : 1.0

Content type (Тип содержимого) : multipart/mixed; boundary="simple boundary"

Это преамбула. Ее можно проигнорировать, хотя она оказывается полезной при размещении агентов и пояснений для программ чтения, не использующих формат MIME.

- simple boundary-

Данная часть соответствует обычному тексту US-ASCII. Текст не заканчивается символом перевода строки.

-'simple boundary-

Content type (Тип содержимого):text/plain; charset=us-ascii

Эта часть соответствует обычному тексту типа US-ASCII. Текст не заканчивается символом перевода строки.

- simple boundary-

Это завершающая часть. Ее также можно проигнорировать.

Следует отметить, что сообщение содержит поле MIME Version (Версия протокола MIME) в основном заголовке, а также поле Content Type (Тип содержимого), в котором указывается на характер информации, приводящейся в последующих компонентах информационного раздела. Эти компоненты разделены строками simple boundary (Простой разделительный). Строка multipart/mixed (Многокомпонентный/смешанный) означает присутствие нескольких компонентов информационного раздела сообщения MIME с собственным типом содержимого. В сообщении также присутствует преамбула и заключительная часть, которые располагаются за пределами разделительных компонентов. Эти части являются необязательными и указывают на те позиции, в которых должны вводиться комментарии и другая подобная информация.

В многокомпонентном сообщении **MIME** разделителем (в приведенном выше примере) является строка simple boundary. Разделители, ограничивающие компоненты информационного раздела MIME, представлены такой же строкой с парой символов «тире» (-). Последний граничный разделитель также содержит пару символов «тире» с соответствующей строкой.

Параметры формата MIME для сервера Domino

Параметры формата MIME, задаваемые в системе Notes/Domino, могут быть разделены на две основные категории: для доменов системы Notes, которые поддерживают обмен сообщениями с сетью Internet, и для организаций, поддерживающих несколько языков общения (так называемые параметры International MIME).

Параметры International MIME (Международный формат MIME) позволяют информировать систему Notes/Domino о порядке преобразования сообщений формата MIME в расширенный текстовый формат системы Notes и о тех наборах символов и шрифтов, которые должны применяться при воспроизведении сообщений, создаваемых на языках, отличных от английского. Если организация никогда в прошлом не принимала сообщений или документов, написанных на других языках, кроме английского, нет никакой необходимости переживать относительно задания параметров International MIME, поскольку серверу Domino они вообще не потребуются.

Если же организация постоянно сталкивается с корреспонденцией не только на английском языке, параметры International MIME приобретают большое значение. В зависимости

от используемых языков параметры могут быть более или менее простыми. К сожалению, здесь невозможно уделить данным вопросам должного внимания. Впрочем, в этом нет и особой необходимости, поскольку один из разработчиков формата MIME для версии R5, Джефф Эйсен (Jeff Eisen) из компании Iris Associates, опубликовал пространную статью «Передача сообщений в глобальной сети с помощью международного формата MIME версии R5» (см. интерактивное обозрение «Компания Iris Associates в наши дни», июль 1999 г., www.notes.net/V Для пользователей системы, применяющих исключительно английский язык, эта статья представляет лишь академический интерес, однако в том случае, когда предполагаются различные языки общения, она сможет заметно облегчить жизнь администраторам.

Параметры формата MIME для сервера Domino заносятся в форму конфигурации сервера. Если для одного сервера сформировано несколько документов конфигурации, сервер Domino воспользуется параметрами формата MIME из специально подготовленного документа. Например, если существуют созданный в режиме по умолчанию документ конфигурации для всего домена, а также аналогичные документы для группы серверов Mail Servers (Серверы почтовой службы) и для группы серверов MailOl/Servers/Stillwater, будут применяться параметры формата MIME только этого последнего документа, поскольку он специально создан для сервера MailOl. Когда для одного и того же сервера имеется два или большее число специально подготовленных документов конфигурации, рекомендуется оставить лишь один из них или ограничить принадлежность сервера только одной группой серверов. Следует отметить, что параметры MIME в документе конфигурации не оказывают никакого влияния в том случае, если не установлено разрешение в поле **International MIME Settings** (Параметры международного формата MIME) на вкладке **Basics** соответствующего документа. И наконец, после изменения параметров формата MIME следует перезапустить сервер Domino. Специалисты компании Lotus обещали устранить перезапуск, поэтому в сервере Domino R6 можно обойтись без него, хотя и не всегда.

Основные параметры формата MIME на форме конфигурации сервера подробно описаны в табл. 8.7. Некоторые из этих параметров, однако, не рассматриваются, поскольку выше уже сделана ссылка на статью Джеффа Эйсена.

Таблица 8.7. Параметры формата MIME на форме конфигурации

Поле	Назначение
Вкладка Basics (Основные параметры)	
Primary character set group (Группа основного набора символов)	По умолчанию для этого поля задается английский язык. Следует определить донный набор символов в качестве основного языка в домене
Secondary character set groups (Группы дополнительных наборов символов)	По умолчанию дополнительные группы не вводятся. Необходимо указать наборы символов для всех других языков общения, используемых в домене, при этом число языков обычно не ограничивается
Вкладка MIME => Conversion Options => General (MIME => Параметры преобразования => Общие)	
Return receipts (Ответные сообщения)	По умолчанию устанавливается вариант Disabled (Отменено), который может быть заменен вариантом Enabled (Разрешено), если требуется возвращать ответные сообщения вместе с почтовыми сообщениями сети Internet

Таблица 8.7. Параметры формата MIME на форме конфигурации (продолжение)

Поле	Назначение
Return receipt mapping (Адресация ответного сообщения), только R5	В этом поле выбирается используемое поле заголовка SMTP. По умолчанию обычно задается вариант Disposition-Notification-To (Направление уведомления в). В альтернативном случае может быть установлен вариант Return-Receipt-To (Направление обратного сообщения в), который предусматривает применение поля более старого, нестандартного заголовка. Изменение следует производить только в том случае, если приходится работать с абонентами, программы чтения которых не допускают применения варианта Disposition-Notification-To
Вкладка MIME => Conversion Options => Inbound (MIME => Параметры преобразования => Входящие)	
Line length (Размер строки, R5) или Use character set auto-detection if message has no character set information (Использовать	По умолчанию в поле задается 75 символов. Следует указать, где планируется использовать символы CRLF (возврат каретки/перевод строки) для преобразования сообщений MIME в обычные текстовые сообщения. Если пользователи планируют просмотр сообщений сети Internet,
Attachmentencoding method (Способ кодирования дополнения)	строками, возможные проблемы могут быть устранены путем предварительного указания этого параметра. В случае, когда сообщение не имеет данных относительно набора символов, поле предназначено для определения способа кодирования. По умолчанию задается вариант Base64 , который рекомендуется использовать функцией автоматического преобразования сообщения (вариант Base64 является наиболее часто применяемым для формата MIME. Этот способ обеспечивает весьма эффективное кодирование данных. Другие возможные варианты: QuotedPrintable , UUencode , BinHex . Если предполагается получать сообщения на языках, отличных от английского, и эти сообщения не содержат данных относительно набора символов, следует задать вариант Yes (да). Вариант QuotedPrintable связан с использованием менее эффективного способа кодирования (по сравнению с вариантом Base64), однако вполне подходит для кодирования сообщений. Вариант UUencode соответствует способу кодирования, непосредственно не относящемуся к стандарту MIME, однако широко используется для других целей. Вариант BinHex соответствует способу кодирования, позволяющему эффективно кодировать двоичные данные
Message content » (Содержимое сообщения)	В этом поле следует указать, каким образом программа Domino преобразует расширенный текстовый формат системы Notes в формат MIME. По умолчанию обычно задается вариант Convert from Notes to Internet message format

Таблица 8.7. Параметры формата MIME на форме конфигурации (продолжение)

Поле	Назначение
Message content	(Преобразование из формата системы Notes в формат сообщений сети Internet, R5). В версии R6 по умолчанию обеспечивается преобразование в неформатированный текст (from Notes to Plain Text). В альтернативном случае может использоваться вариант Create multi-part alternative including conversion and encapsulation (Создание многокомпонентного формата, предусматривающего преобразование и инкапсуляцию), который преобразует сообщение в формате MIME при инкапсуляции в нем формата системы Notes. При применении такого варианта происходит фактическое удвоение размера исходящего сообщения, поэтому его следует применять только в тех случаях, когда пользователи направляют большое количество сообщений абонентам, использующим систему Notes 4.x в сети Internet. Указанные абоненты будут получать правильно отформатированные сообщения вне зависимости от того, в каком формате они вводились. В этом случае абоненты будут получать полные текстовые сообщения с дополнением MIME, которое может быть считано с помощью Web-браузера
Convert tabs to spaces (Преобразование символов табуляции в пробелы)	По умолчанию в этом поле выбран вариант No (Нет). Вариант Yes (Да) следует использовать в тех случаях, когда программа чтения почтовых сообщений у пользователей не обеспечивает распознавания символов табуляции
Outbound line length (Размер внешней строки)	По умолчанию в поле задано 75 символов. Следует определить положения символов CRLF (возврат каретки/перевод строки) при преобразовании сообщений из расширенного текстового формата системы Notes в неформатированный текст. Если корреспонденты сети Internet воспринимают сообщения пользователя в виде попеременно следующих длинных и коротких строк, возможные проблемы устраняются при указании этого параметра
Lookup Internet address for all Notes address when Internet address is not defined in document (Искать адреса Internet для всех адресов Notes, когда в документе не определен адрес Internet)	Все адреса в сообщениях, представленных в формате MIME, должны форматироваться с учетом требований документа RFC 821, причем даже в случае, когда адресатом является пользователь системы Notes в том же домене Notes. При выборе варианта Enabled (Разрешено) программа Domino будет производить поиск адреса сети Internet для пользователя системы Notes в его персональном документе. При отмене этой функции (в режиме по умолчанию) программа Domino будет формировать адрес сети Internet на основе имени пользователя и имени домена системы Notes. Например, для Joe Doaks@Stillwater из домена planetnotes.com адрес будет выглядеть так: Joe_Doaks%stillwater@planetnotes.com
Perform exhaustive lookups when converting [Тщательный поиск в процессе преобразования]	Определяет адрес Notes для адресата в сети Internet. Появляется, если в предыдущем поле задан вариант Enabled (Разрешено). По умолчанию эта функция отменяется, что предполагает прекращение программой Domino поиска

Таблица 8.7. Параметры формата MIME на форме конфигурации (продолжение)

Поле	Назначение
Perform exhaustive lookups when converting	адреса сети Internet при обнаружении персонального документа с именем, соответствующим имени адресата. При разрешении использования функции программа Domino будет просматривать все каталоги для обнаружения всех документов с именами, соответствующими имени адресата. При обнаружении нескольких подобных имен программа будет формировать запрос и просить пользователя сделать выбор

Вкладка **Settings by Character Set Group** (Параметры для групп набора символов)

MIME setting by character set group (Параметры MIME для определенной группы набора символов)	Для каждой группы набора символов следует определить шрифт, наборы символов и способ кодирования, принятый программой Domino. В поле надо сначала указать первую группу набора символов, а уже затем заполнить все остальные поля формы. После этого можно перейти к другой группе набора символов и т.д. Как правило, не приходится изменять предварительно заданные параметры. Если планируется несколько языков общения, рекомендуется обратиться к статье Джеффа Эйсена за более подробной информацией, которая требуется для правильного задания параметров

Вкладка **Advanced => Advanced Inbound Message Options**
(Дополнительно => Дополнительные параметры входящих сообщений)

Resent headers take precedence over original headers (Использовавшиеся ранее заголовки имеют приоритет по отношению к исходным заголовкам)	По умолчанию использование функции отменяется. Согласно документу RFC 822, в перенаправляемые сообщения могут быть добавлены введенные ранее заголовки (с сохранением исходных заголовков). При обращении к стандарту MIME пересылаемое сообщение кодируется и превращается в новое сообщение в формате MIME, причем прежних заголовков здесь не будет. Разрешение на применение данной функции следует давать только в том случае, если пользователи получают почтовые сообщения сети Internet, в которых находятся ранее принятые заголовки, а ответные сообщения адресуются исходному отправителю по ошибке (вместо адресата)
Remove group names from headers (Исключение имен групп из заголовков)	По умолчанию данная функция отменяется. Разрешить ее применение можно только в том случае, если наличие имен групп в заголовках создает проблемы при пересылке ответных сообщений. Введение этой функции повлияет на применение других функций
If each recipients's does not appear in any address header, then add their address to the BCC list (Если адрес каждого абонента не появляется ни в одном заголовке адреса, следует добавить адрес в список BCC)	По умолчанию эта функция отменяется. Разрешение на ее применение следует давать только в том случае, если отсутствие имен абонентов в заголовках вызывает определенные проблемы при пересылке ответных сообщений. Использование функции может сказываться на применении других функций

Таблица 8.7. Параметры формата MIME на форме конфигурации (продолжение)

For non-MIME messages or MIME messages with an unknown character set, 8-bit character set is assumed to be (Для сообщений не-MIME или сообщений MIME с неизвестным набором символов предполагается использование восьмиразрядного кодирования)	По умолчанию предусматривается кодировка Windows-1252, которая допускает применение всех символов, используемых в западноевропейских языках. Возможен также выбор варианта Primary of interest (Основной представляющий интерес) в случае, когда пользователи получают сообщения на языках, отличных от английского. Более подробная информация по данному вопросу содержится в статье Джеффа Эйсена
Character set name aliases (Псевдоним для имени набора символов)	В этом поле следует задавать вариант Primary of interest (Основной представляющий интерес) в том случае, если пользователи получают сообщения на языках, отличных от английского (см. статью Джеффа Эйсена)

Вкладка **Advanced** ⇒ **Advanced Outbound Message Options**
(Дополнительно => Дополнительные параметры исходящих сообщений)

Macintosh attachment conversion (Преобразование вложений Macintosh)	В версии R5 информация по заполнению этого поля отсутствовала, но в R6 можно выбрать кодирование AppleDouble или BinHex 4.0
RFC822 phrase handling (Обработки фраз согласно RFC 822)	В данном случае фраза RFC 822 соответствует необязательной части адреса сети Internet. Фразой может быть любой отрывок текста, приводящегося в скобках, и предшествующий компоненту адреса локальная_часть@домен. Фраза часто используется для включения в адрес сети Internet полных имен и фамилий сотрудников. Поле служит для задания параметра управления процедуры обработки фраз сервером Domino при формировании обратных адресов сети Internet для пользователей системы Notes. В данном случае возможны следующие варианты: Do not add phrase (Не добавлять фразу, вариант по умолчанию), Use DN as phrase (Использовать в качестве фразы доменное имя) - позволяет привносить полное различающееся имя отправителя системы Notes в формируемую фразу, Use alt. Name if available - otherwise DN (Использование альтернативного имени, если существует, либо доменного имени) - дает возможность задавать альтернативное имя отправителя при его наличии или полное различающееся имя отправителя системы Notes, а также Remove phrase (Исключение фразы) - можно исключать уже используемые фразы, которые присутствуют в полях Internet address (Адрес сети Internet) пользователей. Для версии R6 имеется еще один вариант: Use CN as phrase (Использование в качестве фразы общего имени)
Internet Mail server sends Notes private items in messages (Сервер почтовой службы сети Internet пересылает частные элементы системы Notes в сообщениях)	По умолчанию эта функция не используется. Разрешение на ее применение можно давать только в том случае, если предусматривается пересылка сообщений с помощью конкретных приложений на другие клиентские программы системы Notes

Таблица 8.7. *Параметры формата MIME на форме конфигурации (окончание)*

Поле	Назначение
Notes fields to be removed from headers (Поля системы Notes, которые удаляются из заголовков)	В поле рекомендуется добавлять имена полей системы Notes, которые не должны присутствовать в сообщениях, пересылаемых пользователям сети Internet
When converting multilingual message to MIME (При преобразовании многоязычного сообщения к формату MIME)	Чтобы правильно заполнить это поле, стоит посмотреть статью Джеффа Эйсена
Character set name aliases (Псевдоним для имени набора символов)	Для правильного заполнения этого поля также рекомендуется ознакомиться со статьей Джеффа Эйсена

Мониторинг и диагностика работы почты

Обмен почтовыми сообщениями является весьма важной обязанностью сервера Domino, поэтому система почтовой связи должна работать устойчиво и без сбоев. У сервера Domino есть много программных инструментов, помогающих при контроле системы почтовой связи и отслеживании причин возникающих проблем. Набор инструментов содержит следующие программы и функции:

- О программу Domino Administrator;
- О базу данных Notes Log (Журнал системы Notes);
- О базу данных Outgoing Mail (Исходящие почтовые сообщения);
- О программы для сбора статистических данных почтовой службы, формирования отчетов и осуществления контроля;
- О вкладку **Messaging** (Передача сообщений) программы Domino Administrator;
- О почтовые зонды;
- О отслеживание почтовых сообщений;
- О программу Mail Tracking (Отслеживание почтовых сообщений);
- О отчет Mail Usage Reports (Отчеты по использованию почтовых сообщений).

Некоторые из этих программных инструментов, в том числе база данных Notes Log и программы сбора статистических данных, формирования отчетов и контроля, более подробно обсуждаются в последующих главах. В данном разделе будут рассмотрены только те аспекты программ, которые непосредственно связаны с процедурой передачи сообщений.

Программа Domino Administrator

Вкладки программы Domino Administrator обеспечивают доступ к параметрам, связанным с функциями передачи сообщений сервером Domino. Основная вкладка в данном случае - **Messaging** (Передача сообщений), в которой можно активизировать большую часть вышеуказанных программных инструментов (рис. 8.9). Параметры, связанные с передачей почтовых сообщений, присутствуют также на вкладках **Files** (Файлы), **Server** (Сервер) и **Configuration** (Конфигурация).

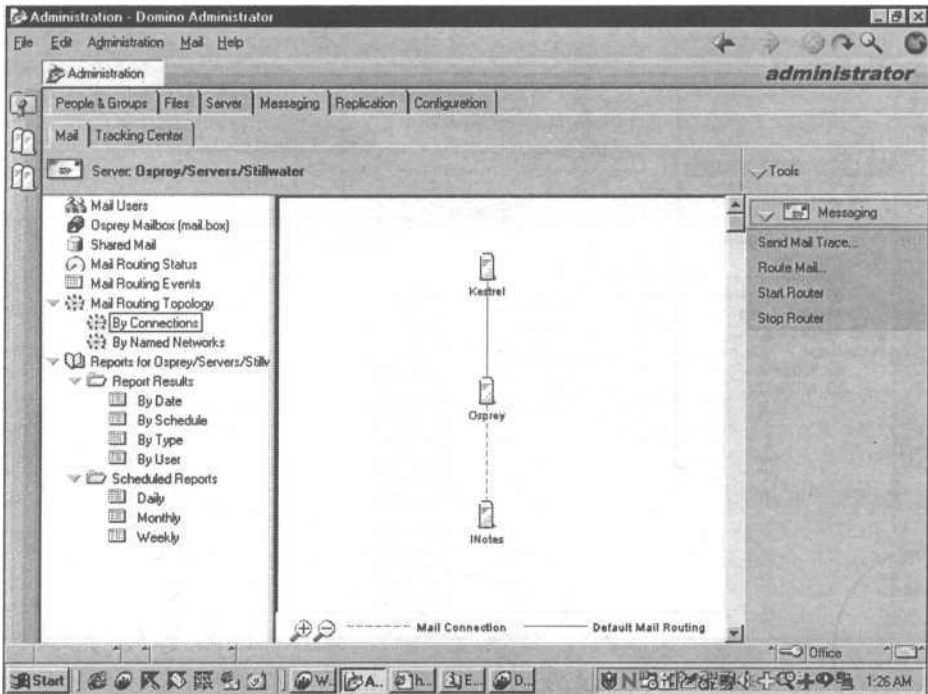


Рис. 8.9. На вкладке **Messaging** можно определить статус сообщений.
Разделы вкладки **Configuration** обеспечивают задание конфигурации для самих сообщений

База данных Notes Log

База данных Notes Log (Журнал системы Notes; файл log.nsf) представляет собой базу данных, хранящуюся на каждом сервере Domino и на каждом клиенте системы Notes. Сервер Domino обеспечивает регистрацию в этой базе больших объемов информации, связанной с исходящими сообщениями сервера. Две вида этой базы данных представляют особый интерес, в частности для поиска неисправностей. Так, вид **Mail Routing Events** (События при маршрутизации почтовых сообщений) определяет регистрацию событий, которые имеют место на сервере. Этот вид организован по хронологическому принципу, причем можно просматривать события или производить поиск событий, содержащих определенные ключевые слова, с помощью программного инструмента **Log Analysis** (Анализ журнала) - рис. 8.10.

Кроме того, вид **Object Store Usage** (Использование данных об объектах) обеспечивает ежедневную регистрацию данных относительно применения активной совместно используемой базы данных почтовой службы (рис. 8.11). Регистрируемые данные указывают на характер взаимосвязей этой базы с другими, число присутствующих в ней документов и объем памяти, занимаемый каждой базой данных почтовой службы.

Обратиться к этим видам можно путем непосредственного открытия базы данных Notes Log на вкладке **Messaging => Mail** (Передача сообщений => Почта) или на вкладке **Server => Analysis** (Сервер => Анализ) программы Domino Administrator.

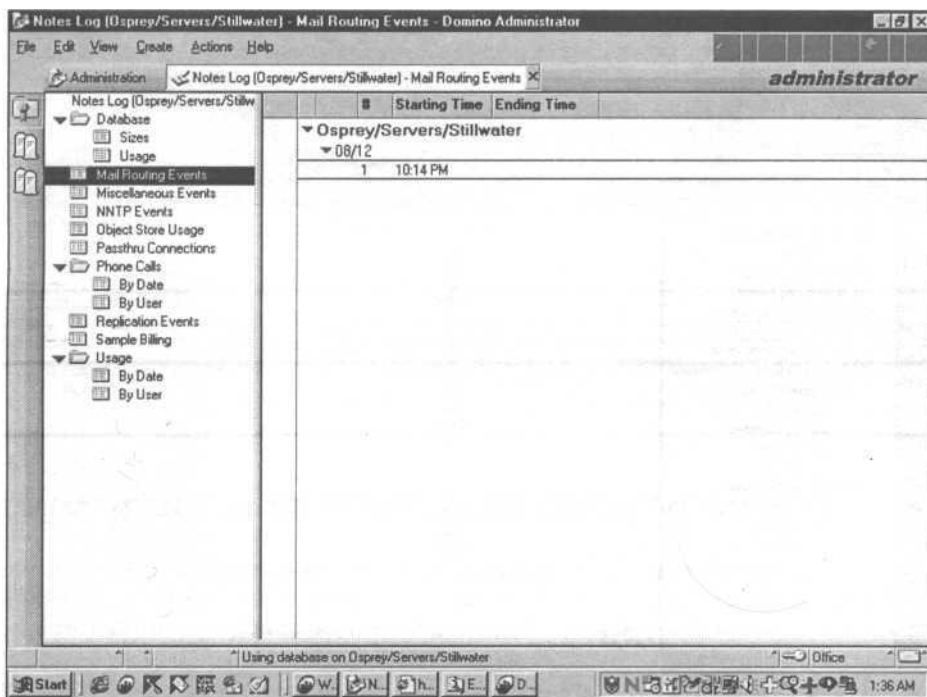


Рис. 8. 10. База данных Notes Log содержит вид **Mail Routing Events** и вид **Object Store Usage**

База данных Outgoing Mail

Если в системе возникают проблемы с передачей почтовых сообщений, которые приводят к их потере, эти потерянные письма можно обнаружить в базе данных Outgoing Mail (Исходящие почтовые сообщения, файл mail.box). Подобные сообщения присутствуют в ней в виде дополнений к отчетам, которые формулируют причины прекращения передачи сообщений. Таким образом, именно к этой базе данных следует обращаться при анализе причин сбоев при передаче сообщений.

Сообщения приобретают указанный статус только в том случае, если они **НЕ** могут быть доставлены адресату или возвращены отправителю. Большая часть писем, которые не удается переслать адресату, обычно возвращаются их отправителям (в файл почтовых сообщений) вместе с отчетами об отказе при передаче сообщения (Delivery Failure Report). Невозможность возвращения сообщения отправителю указывает на наличие достаточно простой или, наоборот, весьма серьезной проблемы. Поэтому рекомендуется во всех случаях определять причину появления подобных сообщений.

Большая часть потерянных почтовых сообщений является следствием либо формирования одним из серверов сообщений, которые не представляется возможным отправить адресатам, либо появления в домене ошибочных сообщений. Такие причины обычно считаются достаточно простыми и не связаны с возникновением серьезных нарушений в маршрутизации почтовых сообщений. Например, серверы Domino не в состоянии принимать

Object Store Filename	Mail Database Filename	Mail Database Title	Number of Documents Referenced in Object Store	Total Size of Documents in Object Store
▼ Osprey/Servers/Stillwater				1,635,886
▼ 08/23/99				1,635,886
▼ mailobj1.nsf				817,943
	mail\bcherry.nsf	Bing Cherry	1	167
	mail\bdbobbs.nsf	Bob Dobbs	133	401,180
	mail\cwagon.nsf	Chuck Wagon	10	64,109
	mail\dburke.nsf	Dorothy Burke	8	136,159
	mail\hdoody.nsf	Howdy Doody	2	1,085
	mail\ispy50.nsf	ISpy on Osprey	87	11,365
	mail\janereal.nsf	Jane Calabria (Real)	132	19,272
	mail\jcalab.nsf	Jane Calabria	25	9,416
	mail\jdoaks.nsf	Joe Doaks	6	4,448
	mail\pthree.nsf	Pop Three	3	561
	mail\rkiklan.nsf	Rob Kikland	84	168,606
	mail\rburke.nsf	Tom Burke	2	982
	mail\zorro.nsf	Don Diego	1	573
▼ mailobj.nsf				817,943
	mail\bcherry.nsf	Bing Cherry	1	167
	mail\bdbobbs.nsf	Bob Dobbs	133	401,180
	mail\cwagon.nsf	Chuck Wagon	10	64,109
	mail\dburke.nsf	Dorothy Burke	8	136,159
	mail\hdoody.nsf	Howdy Doody	2	1,085
	mail\ispy50.nsf	ISpy on Osprey	87	11,365
	mail\janereal.nsf	Jane Calabria (Real)	132	19,272

Рис. 8.11. Вид Object Store Usage обеспечивает вывод важной статистической информации относительно объектов системы

почтовые сообщения, поскольку они не имеют баз данных почтовой службы. Поэтому каждый раз сформированное сервером почтовое сообщение переводится в разряд потерянных. Все, что требуется сделать в данном случае, - это понять, почему сервер направляет сообщения с некорректным адресом, и устранить несоответствие.

Некорректные почтовые сообщения обычно теряются в том случае, когда они адресуются пользователю, уже не относящемуся к данному домену. В некорректных сообщениях, как правило, указан обратный адрес, который не допускает возврата сообщения, так что при отсутствии в домене требуемого адресата эти сообщения переводятся в разряд потерянных. Если таких сообщений, адресованных, например, одному и тому же давно уволившемуся сотруднику, много, заблокируйте их поступление в домен путем добавления имени адресата в поле **Deny messages intended for the following internet addresses** (Запрет на прием сообщений, предназначенных для следующих адресов сети Internet) в соответствующем документе конфигурации. Данное поле расположено на вкладке **SMTP => Restrictions and Controls => SMTP Inbound Controls => Inbound Intended Recipients Controls** (SMTP => Ограничения и управление => Управление входящими сообщениями SMTP => Управление входящими сообщениями определенного адресата). При этом надо обращаться к тому документу конфигурации, который управляет серверами, получающими почтовые сообщения из сети Internet, то есть входными шлюзовыми серверами.

Если сообщения, формируемые пользователем системы Notes или базой данных входных почтовых сообщений домена, переводятся в разряд потерянных, не исключено, что

проблема окажется гораздо более сложной. Такая ситуация может указывать на наличие ошибки в персональном документе, в имени файла базы данных почтовой службы пользователя или в документе соединения. Нужно обязательно выяснить причину возникновения проблемы и устранить ее.

Программные инструменты для сбора статистических данных, формирования отчетов и осуществления контроля

Сервер Domino располагает целым набором программных инструментов для сбора данных, формирования отчетов и вывода статистических показателей. Среди них - консольная команда `show statistics`, серверные задачи `Stat`, `Collect` и `Event`, а также почтовые зонды. Большая часть этих инструментов может быть запущена в программе Domino Administrator.

Команда консоли для вывода статистических данных

Команда консоли для вывода статистических данных, `sh st`, позволяет отобразить на экран длинный список статистических данных для конкретного сервера. Особый интерес представляют команды `sh st mail` и `sh st mailbydest`, которые предназначены для вывода статистических данных, касающихся только почтовых сообщений. Отдельные статистические показатели вызываются на экран и при указании полного имени статистического параметра. Например, при вводе команды `st st mail.dead` отображается число потерянных сообщений, присутствующих в базе данных Outgoing Mail сервера. Команду консоли можно инициировать как непосредственно с консоли сервера, так на вкладке **Server => Status** (Сервер => Статус) программы Domino Administrator щелчком по кнопке **Console** (Консоль) в R5 или **Server Console** (Серверная консоль) в R6.

Задача статистических данных сервера

Задача статистических данных сервера запускается по умолчанию (каждый раз при старте сервера) и позволяет пользователям выполнять ряд действий. Во-первых, можно выводить статистические показатели удаленного сервера посредством команды `load stats имя_сервера`. Для вывода статистических данных о почтовых сообщениях следует воспользоваться командой `load stats имя_сервера mail` или `load stats имя_сервера mailbydest`. Для отображения конкретного статистического показателя почтовых сообщений следует использовать команду вида `load stats имя_сервера mail .dead`.

Во-вторых, допустимо запросить статистические данные и получить их с помощью почтовой службы. При первом запуске задача статистических данных сервера создает базу данных входных почтовых сообщений, а также документ базы данных входных почтовых сообщений (Mail-In Database document). Имя файла для базы данных в этом случае соответствует `statmail.nsf` (в случае нового сервера версии 5 или 6) либо `statsxxx.nsf` (где xxx - то или иное число) для старых серверов версии 4. Имя сервера (а также имя базы данных входящих почтовых сообщений) представляется в виде `общее_имя_сервера Stats/HMN_организации` (например, `Osprey Stats/Servers/Stillwater`).

Не пытайтесь сразу открыть эту базу, поскольку в первый момент данных в ней просто нет. Однако в дальнейшем можно направлять туда подписанные сообщения, а операция формирования статистических данных в ответ перешлет статистические данные с помощью

электронной почты. Если сообщение не подписано, операция не выполняется. Когда в сообщении остается незаполненным поле **Subject** (Тема), операция формирования статистических данных направляет в ответ все статистические показатели - тот же перечень, который может быть получен путем ввода команды `st st` на консоли сервера. Однако при наличии в поле **Subject** записи типа **mail**, **mailbydest** или **mail.dead** операция будет посылать только требуемые статистические показатели.

Задачи сбора данных и контроля события

Имеется возможность воспользоваться серверной задачей сбора данных (Collect), которая направляет статистические данные в соответствии с установленным расписанием (по умолчанию задается почасовой режим подготовки статистических данных), а эти данные заносятся в базу Statistics Reports (Статистические отчеты, файл `statrep.nsf`) - Кроме того, пользователи могут запустить серверную задачу контроля событий (Event), которая уведомляет о том, что определенные статистические данные превышают установленные пороговые значения. Статистические данные, связанные с почтовыми сообщениями, собираются на виде **Statistics Reports\Mail & Database** (Отчеты по статистическим данным, почтовая служба и база данных), а статистические данные для совместно используемой базы данных почтовой службы - на виде **Single Copy Object Store Statistics** (Статистические данные для объектов с одной копией).

Если в базе данных Statistics and Events (Статистические данные и события, файл `events4.nsf`) созданы монитор статистики и уведомление о событиях, задача Collect обеспечит формирование события в том случае, когда контролируемые статистические данные превысят заданные для них предельные значения. На практике можно организовать контроль за потерянными и накапливаемыми сообщениями, за процессом их передачи, за отказами в процессе .передачи, а также за множеством других статистических показателей, связанных с почтовыми сообщениями. При использовании задачи Event на сервере появляется возможность формировать упомянутые выше уведомления, например направлять сигнальные сообщения программам сетевого управления или на пейджер пользователя.

Задача сбора данных Collect предусматривает задание параметров на вкладках **Monitoring** (Мониторинг) и **Statistics** (Статистические данные) программы Domino Administrator. Параметры вкладки **Monitoring** позволяют набирать и формировать статистические данные относительно отдельных задач и событий. При этом допускается создавать любые статистические показатели для почтовых сообщений. Параметры вкладки **Statistics** соответствуют другому виду статистических данных сервера, который, по существу, аналогичен консольной команде **Show Statistics** (Показ статистических данных) и серверной задаче Stat.

Почтовые зонды

Пробное почтовое сообщение (зонд), с которым работает функция отслеживания почтовых сообщений, инициируется серверной задачей ISpy в ответ на создание документа пробного почтового сообщения (Mail Probe document) в базе данных Statistics & Events. Почтовый зонд позволяет определить время (в секундах), затрачиваемое на прохождение маршрута почтовой службы, и сформировать соответствующий статистический параметр, `QOS.Mail.RecipientName.ResponseTime=n`, где `n` равно числу затраченных секунд. При возникновении отказа в процессе пересылки зонда величина указанного параметра задается

равной - 1, а серверная задача ISpy формирует событие типа **Mail** (Почтовая служба) с важностью **Warning (high)** - Предостережение (высокий уровень).

После запуска задачи Collect отчет по статистическим данным направляется в базу данных Statistics Reports. При использовании задачи Event можно формировать уведомления об отказе в процессе передачи зонда (пробного почтового сообщения).

Для создания пробных почтовых сообщений необходимо запустить задачу ISpy. Следует напомнить, что серверная задача ISpy написана на языке программирования Java и ее имя должно быть задано с учетом регистра. Так, для загрузки задачи вручную надо ввести команду load runjava ISpy с консоли сервера. Закрывается программа вручную командой tell runjava quit или tell ISpy quit. Для исполнения задачи в автоматическом режиме (каждый раз при запуске сервера) требуется добавить параметр runjava ISpy в переменную ServerTasks файла notes.ini сервера.

Запущенная на сервере задача ISpy автоматически направляет пробные почтовые сообщения в файл mailbox самого сервера (с периодичностью 15 минут). Для проверки маршрутов почтовой службы (связь с другими серверами) создаются почтовые зонды. Чтобы сформировать пробное почтовое сообщение в программе Domino Administrator R5 перейдите на вкладку **Configuration** (Конфигурация), откройте подвкладку **Statistics & Events** (Статистические данные и события), после чего выполните **Probes** (Пробные почтовые сообщения). Затем выберите вариант **Mail** (Почтовая служба) - появится вид **Mail Probes** (Пробные почтовые сообщения) базы данных Statistics & Events. В версии R6 создание зондов (в том числе и почтовых) приравнено к событиям, поэтому на вкладке **Configuration** требуется щелкнуть по значку **Monitoring Configuration** (Конфигурация мониторинга) и выбрать **Mail** (Почтовая служба). Далее щелкните по кнопке **New Mail Routing Event Generator** (Создать генератор событий почтовой маршрутизации) и перейдите на вкладку **Probe** (Зонд). В любом случае почтовый зонд запускается с помощью Мастера, если выбрать пункт **Setup Wizard => Probe** (Программа установки => Зонд) в меню **Actions** (Операции). Перечень полей документа пробного почтового сообщения (Probe document) приведен в табл. 8.8.

Таблица 8.8. Список полей для формы пробного почтового сообщения

Поле	Назначение
Вкладка Basics (Основные параметры)	
All Domino servers in the domain will probe themselves (Все серверы Domino области будут направлять друг другу пробные сообщения)	Не следует обращаться к данному полю, поскольку пробные почтовые сообщения такого типа уже существуют
Recipient (Абонент)	В поле задается или выбирается имя пользователя почтовой службы для целевого почтового сервера. С помощью пробных почтовых сообщений будет проверяться маршрут к этому серверу
Server(s) (Серверы)	Здесь следует вводить или задавать имена для одного или нескольких серверов, которые будут формировать пробные почтовые сообщения. Для каждого выбираемого сервера должна в обязательном порядке выполняться функция ISpy

Таблица 8.8. Список полей для формы пробного почтового сообщения (окончание)

Поле	Назначение
Вкладка Probe (Зонд)	
Send interval (Временной интервал отправки)	В этом поле указывается число минут между направлением пробных почтовых сообщений. По умолчанию временной интервал устанавливается равным 15 минутам
Timeout threshold (Максимальный временной интервал)	Пробное почтовое сообщение должно формироваться в течение заданного числа минут. В противном случае генерируется сообщение об отказе. По умолчанию на эту операцию выделяется одна минута
Вкладка Other (Другие параметры)	
On timeout, generate a Mail event of severity (По истечении тайм-аута генерировать почтовое событие, имеющее заданную важность)	В данном поле следует указывать уровень важности. По умолчанию задан вариант Warning (high) - Предупреждение (высокий уровень)
Disable this probe (Отменить зонд)	После установки этого флажка задача ISpu не будет генерировать пробных почтовых сообщений

Отслеживание маршрутов почтовой службы

Функция отслеживания маршрута почтовой службы позволяет проверять наличие и корректность пути к точке назначения. Данные об отслеженных маршрутах представляют собой весьма ценный материал, особенно в тех случаях, когда направляемые другим пользователям системы Notes сообщения попадают в разряд потерянных.

При контроле маршрута пробное сообщение может быть отправлено и прослежено вплоть до конкретного сервера почтовой службы. В ответ сервер почтовой службы пользователя (или промежуточный сервер) возвращает отчет о прохождении пробного сообщения (Trace Report). Для каждого сервера задаются два момента. Первый информирует о времени получения сервером пробного сообщения, а второй - о времени пересылки сервером соответствующего отчета. Подобные отчеты удобны не только для проверки корректности маршрута почтовой связи, но и для проведения хронометража.

Администратор имеет возможность направлять пробные сообщения (для проверки маршрута) путем задания соответствующих параметров на вкладке **Messaging => Mail** (Передача сообщений => Почта) программы Domino Administrator, например воспользовавшись кнопкой **Send Mail Trace** (Передача пробного почтового сообщения) на панели **Tools** (Программные инструменты). Предварительно администратору рекомендуется убедиться в том, что регистрация была осуществлена не для сервера. В противном случае все направляемые в ответ отчеты разделят судьбу потерянных сообщений.

Пользователи также вправе направлять пробные почтовые сообщения (с помощью услуг электронной почты) посредством команды **Trace entire path** (Проверка всего маршрута) в разделе **Delivery Options => Delivery Reports** (Параметры доставки => Отчеты о результатах доставки). Различия между двумя описанными выше типами пробных

сообщений состоят в том, что пробные сообщения администраторов никогда реально не попадают к адресатам, а предназначены только для возвращения отчетов с проводящих маршрутизацию серверов. Те же сообщения электронной почты, которые передаются пользователями, носят, по существу, статус обычных сообщений и доставляются по возможности конечным адресатам.

Пробные почтовые сообщения и пробные сообщения для проверки маршрута выполняют практически одну и ту же функцию, а небольшие различия между ними описаны в табл. 8.9.

Таблица 8.9. Различия между пробными почтовыми сообщениями и почтовыми сообщениями, предназначенными для проверки маршрутов

	Отслеживание почтовых маршрутов	Пробные почтовые сообщения
Режим отправки	По требованию	зния
Способ отправки	Сообщения электронной почты	Периодическая, автоматическая
Формат при представлении результатов	Отчет по результатам отслеживания сообщений электронной почты	Задача ISpy Обеспечивающая мониторинг статистика QOS Statistics (Сбор статистических данных относительно параметров качества обслуживания)

Отслеживание обычных/почтовых сообщений

Функция отслеживания сообщений (иногда называемая функцией отслеживания почтовых сообщений - в зависимости от конкретного назначения) позволяет определять, что происходит с индивидуальными сообщениями, посланными в режиме почтовой связи. Здесь удастся получить ответ на целый ряд вопросов, в частности о характере доставки сообщений, о способе хранения их в базе данных адресата (или уничтожения), а также о фактах просмотра адресатом после доставки, придания им статуса потерянных, наличия этих сообщений на маршруте и т.д. Функция отслеживания почтовых сообщений отличается от функций отслеживания маршрутов почтовой связи и передачи пробных почтовых сообщений. Последние функции не дают возможности охарактеризовать индивидуальные сообщения, а служат лишь для анализа состояния маршрута почтовой службы (допустимо оценить корректность этого маршрута и время, необходимое для его прохождения).

Настройкаотслеживаниясообщений

Функция отслеживания сообщений не выполняется автоматически, а требует настройки на каждом сервере, который планируется для целей контроля. На практике приходится производить такую настройку практически для всех серверов и концентраторов почтовой службы, а иногда и для серверов, обеспечивающих передачу почтовых сообщений в другие домены. После настройки функции отслеживания сообщений администраторы и пользователи получают возможность контролировать прохождение своих писем. При этом администраторы способны отслеживать все почтовые сообщения, а пользователи - лишь собственные.

Функцию отслеживания сообщений необходимо активизировать с помощью соответствующего документа конфигурации. В каждом документе конфигурации выберите

Router/SMTP => Message Tracking (Маршрутизатор/SMTP => Отслеживание сообщений) на вкладке **Basics**, а затем укажите **Enabled** (Разрешено) в поле **Message tracking** (Отслеживание сообщений). При работе в режиме редактирования имеется также возможность занести записи в другие поля, указанные в табл. 8.10.

Таблица 8.10. Поля **Message Tracking** формы конфигурации

Поле	Назначение
Don't track messages for (Запрет на отслеживание сообщений для)	В поле следует указывать имена сотрудников, баз данных и групп, сообщения которых не должны отслеживаться. Если поле остается незаполненным, все сообщения будут отслеживаться. Когда серверная задача ISpy используется для пересылки пробных почтовых сообщений, добавьте в это поле ISpy on имя_сервера , чтобы избежать заполнения базы данных ненужными записями о почтовых зондах
Log message subjects (Регистрация темы сообщений)	По умолчанию в поле установлен вариант No (Нет). При изменении записи на Yes (Да) текстовая запись поля Subject (Тема) каждого сообщения будет занесена в базу данных слежения, что позволит отследить сообщения в соответствии с характером их назначения. В результате увеличится размер записей слежения и нарушится безопасность, поскольку администраторы, которые до этого не могли знакомиться с содержанием частных почтовых сообщений, теперь будут информированы о предмете переписки
Don't log subjects for (Запрет регистрации темы для)	В поле указываются имена сотрудников, баз данных и групп, для которых не будут регистрироваться темы сообщений. Это поле имеет смысл только в том случае, если для поля Log message subjects (Регистрация темы сообщений) задан вариант Yes
Message tracking collection interval (Временной интервал для сбора данных относительно отслеживания сообщений)	По умолчанию в данном поле установлено значение 15 минут. Эта запись указывает, как часто программа MT Collector будет инициировать сбор данных. Определение более короткого временного интервала может привести к замедлению работы сервера, поэтому следует проявлять известную осторожность
Allowed to track messages (Разрешение на отслеживание сообщений)	Когда данное поле остается незаполненным, всем пользователям разрешается отслеживать собственные сообщения, а администратором — все сообщения пользователей. Если сюда помещен список имен, только лица из этого списка будут вправе отслеживать все сообщения. Остальные сотрудники и администраторы смогут отслеживать только свои сообщения. При добавлении имен необходимо также дополнительно вносить имена серверов. В противном случае не будет возможности отследить сообщения, проходящие через несколько серверов
Allowed to track subjects (Разрешение на отслеживание темы сообщений)	Запись этого поля имеет смысл только в случае, если в поле Log messages subjects задан вариант Yes . Если поле не заполнено, то все пользователи получают возможность отслеживать тему собственных сообщений, а администраторы — тему любых сообщений. При добавлении в данное поле списка имен только лица из этого списка будут отслеживать темы всех сообщений. Остальные пользователи смогут отслеживать тему только своих сообщений. При добавлении имен следует вносить и имена серверов, иначе не удастся отслеживать предмет тех сообщений, которые проходят через несколько серверов

Программа MT Collector может загружаться в память вручную, например командой `load mtc`, задаваемой с консоли сервера, или в программе Domino Administrator на вкладке **Server** (Сервер). Для выгрузки этой программы можно воспользоваться командой `tell mtc quit`, задаваемой с консоли сервера, или обратиться к Domino Administrator для удаления программы.

При первом запуске на сервере программа Mail Tracking Collector создает базу данных MailTracking Store (Результаты отслеживания почтовых сообщений, файл `mtstore.nsf`) в подпапке `mtdata`. Кроме того, предусматривается проведение для этой базы данных полнотекстовой индексации.

Использование функции отслеживания сообщений

Администраторы, уполномоченные контролировать передаваемые сообщения, могут осуществлять эту операцию в программе Domino Administrator, например воспользовавшись подвкладкой **Tracking Center** (Центр слежения) вкладки **Messaging** (Передача сообщений). Надо щелкнуть по кнопке **New Tracking Request** (Новый запрос на слежение), а в диалоговом окне **New Tracking Request** (Новый запрос на слежение) ввести максимальный объем информации, чтобы упростить идентификацию отслеживаемых сообщений. При нажатии на кнопку ОК программа Domino Administrator перешлет сформированный запрос на указанный в запросе сервер. Этот сервер в дальнейшем будет накапливать данные обо всех сообщениях, соответствующих ранее введенной информации. Таким образом, чем точнее сформулирован запрос, тем меньшее число сообщений будет учтено в ответе.

Данные относительно сообщений выводятся в верхней части окна **Tracking Center** (Центр слежения) с указанием для каждого сообщения его отправителя, адресата и, по возможности, назначения и даты и времени доставки.

Выберите (на экране) любое сообщение и выполните **Track Selected Message** (Отслеживание заданного сообщения). Программа Domino Administrator получит с соответствующих серверов данные относительно сообщения, хранящегося в базе данных MailTracker Store сервера. Есть возможность указать в нижней части экрана сервер для передачи дополнительных сведений (слева) и вывести данные по результатам слежения (справа) в разделе **Mail Transfer Details** (Результаты отслеживания почтового сообщения).

Пользователи в состоянии отслеживать сообщения в базах данных почтовой службы путем выбора любого направляемого им сообщения и ввода команды **Actions => Tools => Send Tracking Request** (Операции => Программные инструменты => Направление запроса на слежение) из соответствующего меню. В диалоговом окне **Message Tracking** (Отслеживание сообщения) указывают абонентов, копии сообщений которых нужно отследить. Кроме того, пользователь должен отметить необходимость определения текущего статуса сообщений или отслеживания его полного маршрута, после чего щелкнуть по кнопке ОК. Запрос на отслеживание будет передаваться с помощью средств электронной почты на серверы почтовой службы, связанные с контролируруемыми абонентами. В дальнейшем домашние серверы и, возможно, сквозные серверы будут пересылать ответ обратно направившему запрос пользователю (Также с помощью средств электронной почты). Передаваемые пользователю данные информируют его относительно самого факта и срока доставки сообщения, относительно факта и срока ознакомления с ним абонента, а также относительно факта и срока удаления сообщения абонентом.

Ниже приводится перечень возможных статусов доставки сообщения:

- О **Delivered** (Сообщение доставлено) - сообщение было передано в базу данных почтовой службы абонента;
- О **Delivery failed** (Отказ при доставке сообщения) - сервер не смог послать сообщение в базу данных почтовой службы абонента;
- О **In queue** (В очереди) - маршрутизатор все еще занимается обработкой сообщения;
- О **Transferred** (Сообщение передано) - сообщение отправлено на следующий сервер маршрута;
- О **Transfer failed** (Отказ при передаче сообщения) - маршрутизатору не удалось переслать сообщение на следующий сервер маршрута;
- О **Group expanded** (Расширение группы) - сообщение было адресовано группе, а данный сервер перевел группу в разряд составляющих ее пользователей;
- О **Unknown** (Нераспознанное состояние) - сервер не располагает данными относительно статуса сообщения.

Сообщению, успешно доставленному абоненту, также придается статус почтового ящика, который может быть представлен одним из следующих значений: **Read** (Прочитанное), **Unread** (Не прочитанное), **Deleted** (Удаленное), **Unknown** (Нераспознанное).

Управление отслеживанием обычных/почтовых сообщений

В общем случае не требуется предпринимать никаких специальных действий для поддержания нормальной работы системы отслеживания сообщений. Соответствующая база данных (файл `mtstore.nsf`) предварительно конфигурируется так, чтобы документы по истечении 30 дней удалялись, однако пользователям разрешается при необходимости сократить этот временной интервал. Возможно, потребуется также сформировать для базы данных список управления доступом ACL, чтобы группа **Administrators** (Администраторы) получила право **Manager** (Менеджер). Такое право доступа в пределах группы **LocalDomainServers** (Серверы локального домена Domino) на первый момент получает тот пользователь, который запустил функцию отслеживания сообщений.

Не следует забывать о возможности применения перечисленных в табл. 8.11 команд типа `tell`, позволяющих выполнять различные функции.

Таблица 8.7 / Команды `tell` для реализации функции *Message Tracking*

Команда	Назначение
<code>tell mtc process</code>	Данная команда заставляет программу MT Collector незамедлительно приступить к сбору данных относительно доставки сообщений
<code>tell mtc interval</code> минуты	В данном случае параметр минуты соответствует количеству минут. Эта команда обеспечивает изменение временного интервала сбора данных, который ранее был задан в документе конфигурации
<code>tell mtc compact</code> -	Команда уплотняет соответствующую базу данных (файл <code>mtstore.nsf</code>)
<code>tell mtc reindex</code>	Эта команда обеспечивает модификацию полнотекстового индекса соответствующей базы данных (файл <code>mtstore.nsf</code>)
<code>tell mtc purge</code> дни	В данном случае параметр дни равен числу дней. Команда исключает все документы, которые отстоят на указанное число дней от момента создания базы данных

Подготовка отчетов об использовании почтовых сообщений

После активизации отслеживания сообщений (см. предшествующий раздел) можно обеспечить подготовку отчетов об использовании почтовой службы. Следует отметить, что база данных MailTracker Store сервера Domino накапливает большие объемы информации, которая полезна при составлении таких отчетов. Отчеты для почтовых сообщений формируются в специально создаваемой базе данных Reports (Отчеты). Подготовка отчетов производится по запросу или по расписанию. Хранить подготовленные отчеты допускается как в упомянутой базе данных, так и в базах соответствующих абонентов. На практике формированием отчетов в базе данных занимается несколько высокоэффективных агентов, а администратору остается заполнить формы с указанием требуемых типов отчетов.

Настройка функции подготовки отчетов об использовании почтовых сообщений

Для настройки функции подготовки отчетов об использовании почтовых сообщений необходимо сначала настроить функцию отслеживания сообщений (этот вопрос подробно обсуждался выше), затем создать базу данных Reports, а потом задать параметры обеспечения безопасности таким образом, чтобы процесс формирования отчетов проходил без сбоев.

Для создания базы данных Reports выполните **File => Database => New** (Файл => База данных => Новый) в соответствующем меню, а затем заполните поля, указанные в табл. 8.12, и щелкните по кнопке ОК.

Таблица 8.12. Список полей новой базы данных, требующих заполнения при создании базы данных Reports

Поле	Назначение
Server (Сервер)	База данных должна храниться на том же сервере, что и база данных в файле mtstore.nsf, которая используется в качестве исходной при подготовке отчетов
Title (Заголовок)	Для данного поля должен выбираться вариант Reports (Отчеты)
Filename (Имя файла)	В этом поле должно присутствовать имя файла reports.nsf
Template (Шаблон)	В поле следует задавать для шаблона сервера те параметры сервера, которые указывались в поле Server , затем выбрать Reports (Отчеты, файл reports.nsf)

Ф

Для завершения формирования базы данных необходимо выполнить следующие действия:

1. В списке ACL базы данных Reports проверьте имена администраторов, отвечающих за подготовку отчетов, и убедитесь в том, что и они, и сервер имеют уровень доступа **Manager**. По умолчанию доступ для других пользователей будет запрещен.
2. Разрешите все агенты, связанные с процедурой планирования. В меню **View** (Вид) выберите **Agents** (Агенты) и установите флажки слева от планируемых отчетов. После этого закройте вид.
3. Предоставьте всем администраторам, которые будут создавать отчеты, неограниченный доступ к агентам сервера - откройте документ сервера и перейдите на вкладку **Security** (Безопасность). В разделе **Agent Restrictions** (Ограничения для агентов)

введите имена администраторов в поле **Run unrestricted LotusScript/Java** (Запуск без ограничений для сценариев LotusScript/Java).

Формирование отчетов об использовании почтовых сообщений

Эта задача является достаточно простой. Для ее решения откройте базу данных Reports и щелкните по кнопке **Run Report** (Формирование отчета). Затем заполните поля появившейся на экране формы и щелкните по кнопке ОК. В форме следует задавать тип отчета, перекрываемый им временной диапазон и временной интервал исполнения, оговаривать необходимость сохранения отчета, пересылки его с помощью почтовой службы (можно указать выполнение обеих операций), а также задавать специальные параметры.

На практике можно создавать отчеты следующего типа:

- ☐ первые 25 пользователей по порядку;
- ☐ первые 25 пользователей по размеру сообщения;
- ☐ первые 25 отправителей сообщений по порядку;
- ☐ первые 25 отправителей по размеру сообщения;
- ☐ первые 25 принимающих сообщения пользователей по порядку;
- ☐ первые 25 принимающих сообщения пользователей по размеру сообщения;
- ☐ первые 25 наиболее часто используемых «очередных участков»;
- ☐ первые 25 наиболее часто используемых «предшествующих участков»;
- ☐ первые 25 наибольших по размеру сообщений;
- ☐ суммарный объем сообщений;
- ☐ результирующий статус сообщений.

Каждый тип отчета может перекрывать несколько временных диапазонов (например, сутки, одну неделю, две недели, один месяц) или конкретный временной диапазон, указанный в базе данных (файл mtstore.nsf). Допускается формировать отчеты однократно, ежедневно, еженедельно или ежемесячно.

ГЛАВА

9

ПРОЦЕДУРА РЕПЛИКАЦИИ ДАННЫХ



Репликация является одной из наиболее значимых процедур сервера Domino. Эта процедура, по существу, является ключевой для всей *архитектуры распределения данных*, предусматривающей хранение многочисленных копий баз данных на многих серверах Domino и рабочих станциях пользователей. Такой подход позволяет пользователям осуществлять доступ к любой базе данных, применяемой в системе. Пользователи получают возможность читать и вносить информацию в любые копии баз данных с учетом предоставленных им прав доступа. По прошествии короткого времени процедура репликации осуществит копирование сделанных дополнений, изменений и исключений и передаст их в другие копии баз данных.

С появлением каждой новой версии системы Notes/Domino репликация приобретает все большее значение. В наши дни благодаря ей малое число мощных серверов в состоянии обеспечить работу множества пользователей. Дешевые региональные сети позволяют перенести серверы ближе к пользователям. Вдобавок к своим первоначальным функциям репликация стала (по счастливой случайности) весьма ценным дополнением для различных функций сервера Domino, число которых увеличивается с переходом к каждой новой версии.

Например, репликация (наряду с процедурой поддержки рабочего процесса) облегчает создание, разработку и поддержку различных Web-приложений. Разработчики имеют возможность модифицировать приложения на одном сервере, а затем по мере готовности передавать их копии на другие объекты системы. Кроме того, авторы информационного содержимого теперь в состоянии распространять свои изменения в одну или большее число копий баз данных, располагающихся за брандмауэром.

В таких условиях руководители могут утверждать информационное содержимое (с помощью соответствующей процедуры системы Notes) и санкционировать его передачу во внешние организации. В результате избирательной и плановой репликации утвержденное информационное содержимое передается на один или большее число Web-серверов, расположенных за границами брандмауэров, и к ним обеспечивается свободный доступ общественности.

Значимость репликации данных для нормального функционирования доменов системы Notes не уменьшается с появлением новых версий системы. Следует отметить, что корректное осуществление репликации необходимо для поддержания жизнеспособности

структуры серверов Domino. В данной главе подробно рассмотрен механизм репликации, порядок ее настройки, а также способы поддержки и оптимизации этой процедуры.

Описание механизма репликации данных

Многие программы посредством репликации распределяют данные между многочисленными серверами. Большая часть реализует данную процедуру в режиме управления «главный/подчиненный» (ведущий/ведомый), когда одна копия базы данных играет роль главной и используется для проведения необходимых изменений, а все остальные копии выполняют функцию подчиненных и допускают только чтение данных. Возможно также существование большого числа главных копий, однако обычно базы делят между собой зоны ответственности за различные сегменты данных, чтобы для каждого сегмента предназначалась только одна главная копия.

Такой принцип организации баз данных призван в первую очередь улучшить показатели их связности и целостности с целью устранения независимых и произвольных изменений копий баз. Большая часть систем поддержки данных не допускает возникновения подобных изменений, поскольку они не в состоянии в дальнейшем выявить возникшие различия между массивами данных.

В этом смысле (как, впрочем, и во многих других отношениях) сервер Domino заметно отличается от других программных продуктов обработки данных. Копии (реплики) баз данных сервера Domino полностью соответствуют друг другу. В отсутствие ограничений на разработку все реплики выполняют функции главных баз данных, допускающих привнесение изменений. Это означает, что в разных копиях баз данных могут инициироваться различные изменения, которые затем будут перенесены во все остальные копии баз данных. Сервер Domino предусматривает применение ряда встроенных механизмов для решения подобных задач, в том числе:

- несколько способов предотвращения редактирования существующих документов и устранение конфликтов при репликации;
- ручные и автоматические (программные) способы устранения возникающих конфликтных ситуаций при репликации.

Для получения более подробной информации относительно конфликтов, возможных в процессе репликации данных, обратитесь к разделам в конце настоящей главы.

Другой аспект, отличающий операцию репликации сервера Domino от операций, выполняемых другими программными продуктами, связан с ее дискретным выполнением. Так, в процессе репликации сервером Domino дублирование всего документа предусматривается только в том случае, если этот документ является новым. При репликации изменений в уже существующем документе дублируются только измененные поля. Это позволяет заметно повысить эффективность процесса репликации.

В системе Notes/Domino возможны две базовые операции репликации данных: типа Pull и типа Push. При осуществлении *репликации по принципу Pull* (Вытягивание) инициирующий дублирование объект запрашивает новые документы и измененные поля существующих документов с сервера Domino, проводящего репликацию. При *репликации по принципу Push* (Выталкивание) инициирующий дублирование объект пересылает собственные документы и измененные поля существующих документов на сервер Domino, обеспечивающий репликацию.

На практике репликация может инициироваться между двумя серверами Domino или между сервером Domino и клиентом системы Notes. Когда репликация выполняется для двух серверов, все операции реализуются с помощью специальных служб одного или обоих серверов. При осуществлении репликации для сервера Domino и клиентов системы Notes все указанные операции выполняет сама система Notes, а служба сервера Domino к этой работе не привлекается.

Система Notes в ходе репликации производит чтение и регистрацию записей на сервере практически так же, как это делает пользователь в режиме интерактивного взаимодействия с сервером, то есть путем формирования запросов на чтение и запись данных и направления этих запросов на сервер базы данных (Database Server), построенный на основе сервера Domino. При осуществлении репликации система Notes выполняет все операции автоматически и вместо вывода соответствующих запросов на экран дисплея заносит их в свою локальную копию базы данных.

Операции Pull и Push на практике могут комбинироваться четырьмя различными способами:

- О вариант Pull-Pull возможен только в условиях плановой репликации данных для двух серверов, когда первый сервер получает данные со второго, а второй - с первого. В этом случае оказываются задействованными обе серверные службы, и каждый сервер самостоятельно регистрирует результаты инициированных им операций репликации. Если репликация осуществляется с помощью сетевого соединения, сервер 1 будет получать данные первым, а сервер 2 - вторым. При использовании соединения на основе модема оба сервера получают данные одновременно (что позволяет повысить производительность для медленных соединений);
- О вариант Pull-Push допустим в случае взаимодействия как двух серверов Domino, так и сервера Domino и клиентов системы Notes. Первый сервер (клиент системы Notes) получает данные от второго, а затем передает ему данные. Служба первого сервера (клиента системы Notes) в этом случае выполняет все необходимые действия, а сам первый сервер регистрирует данные относительно всей транзакции;
- О вариант Pull Only предусматривает получение данных первым сервером (клиентом системы Notes) от второго. При этом служба первого сервера выполняет все необходимые действия, а сам первый сервер регистрирует данные относительно всей транзакции;
- О вариант Push Only предусматривает передачу первым сервером (клиентом системы Notes) данных на второй. При этом служба первого сервера выполняет все необходимые действия, а сам первый сервер регистрирует данные относительно всей транзакции.

Как уже отмечалось выше, вариант репликации Pull-Pull допускается только при взаимодействии двух серверов и активизируется лишь с помощью соответствующего документа соединения (Connection document). Как правило, к такому варианту приходится прибегать в единственной ситуации - когда серверы взаимодействуют через модем или какое-либо иное медленное соединение. Вариант репликации Pull-Push на практике считается более предпочтительным, поскольку данные целого сеанса связи регистрируются всего одним сервером. В случае варианта Pull-Pull каждый сервер регистрирует данные для тех действий, которые выполняет его собственная служба, поэтому записи одного сервера позволяют получить лишь приблизительное представление о сеансе связи. Последнее иногда бывает крайне неудобным, особенно при поиске неисправностей.

Тем не менее, когда два сервера взаимодействуют с помощью модема, вариант **Pull-Pull** может оказаться более подходящим, поскольку службы серверов выполняют операции репликации практически одновременно. Это позволит эффективнее использовать медленное соединение и заметно уменьшить время, затрачиваемое на репликацию.

При плановой репликации возможны три варианта:

- О **On a schedule** (По расписанию) - разрабатывается специальный план реализации процедуры репликации между серверами Domino, который описывается в документе соединения (Connection document). Как правило, подобные процедуры для двух серверов осуществляются именно таким образом, поскольку репликацию данных приходится выполнять достаточно часто и регулярно. Аналогичную плановую процедуру репликации для сервера Domino и клиента системы Notes можно оговорить в документе местоположения (Location document). Для большей части подобных случаев плановая репликация не предусматривается, поскольку пользователи, поддерживающие локальные реплики баз данных, не нуждаются в частом или периодическом проведении этих операций;
- О **On demand** (По требованию) - администратор имеет возможность потребовать (с помощью соответствующей команды) у сервера продублировать конкретные данные и передать их на другой сервер. Аналогичную команду может инициировать и пользователь системы Notes. Обычно репликация в режиме по требованию проводится только в специальных случаях, поскольку плановая репликация позволяет передать весь объем накопленных изменений между двумя серверами Domino. В то же время при взаимодействии сервера Domino с клиентом системы Notes репликация по требованию является наиболее типичной;
- О **Event driven** (При появлении события). Серверы в кластере Domino часто применяют процедуру *кластерной репликации*, в процессе которой сервер одновременно передает все накопленные в его базе данных изменения на другие серверы группы. Процедура кластерной репликации производится с помощью службы Cluster Replicator (Кластерный репликатор), а не обычной службы Replicator (Репликатор), и в некоторых отношениях заметно отличается от стандартной процедуры репликации (см. главу 20).

Операции, выполняемые в процессе репликации данных

При реализации варианта **Pull-Pull** и репликации данных для двух серверов возникает необходимость в совершении целого ряда операций (которые в случае взаимодействия сервера Domino и клиента системы Notes оказываются практически теми же самыми):

1. Служба Replicator сервера S1 пребывает в режиме ожидания до тех пор, пока он не получит команду (с консоли сервера или из документа соединения) вступить во взаимодействие с сервером S2.
2. Затем сервер S1 инициирует формирование соединения с сервером S2 и серверы аутентифицируют друг друга, подтверждая тем самым факт взаимодействия именно серверов S1 и S2.
3. После этого каждый сервер создает список локальных баз данных, к которым другой сервер имеет доступ на уровне **Reader** (Читатель) или выше и для которых репликация ранее не была запрещена. Сервер S1 выявляет в списке базы данных, характеризующиеся однотипными идентификационными данными (и, следовательно, являющиеся репликами одной и той же базы).

4. После выбора первой реплики базы данных сервер S1 запрашивает у сервера S2 перечень новых документов или претерпевших изменения после последнего успешного взаимодействия этих серверов. Момент последнего взаимодействия в данном случае хорошо известен, поскольку он отмечается в каждой копии *журнала репликации* базы данных. Если в журнале отсутствует указание на момент последней репликации, сервер S1 запросит у сервера S2 перечень всех документов этой базы данных. Для просмотра журнала репликации базы данных следует использовать команду **Replication => History** (Репликация => Журнал) в меню **File** (Файл).
5. В ответ на это сервер S2 направляет перечень универсальных идентификационных данных (Universal ID - UNID) на сервер S1. В соответствии с запросом, он посылает идентификационные данные UNID только новых документов или документов, подвергшихся модификации с момента последней репликации данных. При этом сервер S2 не сообщает о тех документах, к которым сервер S1 не имеет доступа на уровне **Reader**. Кроме того, сервер S2 пересылает на сервер S1 *временной указатель*, который при условии успешного завершения текущего сеанса связи будет запоминаться сервером S1 в журнале репликации вместо предшествующего временного указателя.
6. Сервер S1 формирует собственный перечень идентификационных данных UNID (с использованием своей реплики базы данных) и сравнивает эти два списка (последовательно, документ с документом).
7. Затем сервер S1 инициирует получение документов с сервера S2 и занесение их в собственную базу данных, руководствуясь рядом установленных правил. Так, например, идентификационные данные UNID, имеющиеся в списке сервера S2, но отсутствующие в списке сервера S1, соответствуют документу либо совершенно новому, либо недавно модифицированному сервером S2 (но не сервером S1); если список ACL в базе данных сервера S1 указывает на то, что сервер S2 имеет право занести документ в базу данных сервера S1, сервер S1 получает документ с сервера S2 и помещает его в собственную реплику базы данных; при этом сервер S2 должен обладать правом доступа на уровне **Manager** (Менеджер) для пересылки измененного списка ACL на сервер S1, на уровне **Designer** (Разработчик) для передачи измененного документа проектирования и на уровне **Editor** (Редактор) для пересылки измененного информационного документа:
 - если идентификационные данные UNID появляются в списке сервера S2, но их нет в списке сервера S1, это означает, что они отвечают новому или недавно измененному на сервере S2 (но не на сервере S1) документу. В случае, когда список ACL для копии базы данных сервера S1 указывает на наличие у сервера S2 достаточных прав для записи документа в базу данных сервера S1, сервер S1 получит документ с сервера S2 и внесет его в свою реплику базы данных. Серверу S2 необходимо право доступа на уровне **Manager** для пересылки на сервер S1 измененного списка ACL, право доступа на уровне **Designer** для отправки на этот сервер измененных документов проектирования и право доступа на уровне **Editor** для передачи измененных информационных документов;
 - наличие идентификационных данных UNID в списках серверов S1 и S2 иногда приводит к конфликтной ситуации. Поэтому сервер S1 анализирует ситуации для определения факта наличия конфликта и при его обнаружении намечает план действий. Ситуация может не быть конфликтной, если, например, документ был продублирован с сервера S2 на более раннем этапе, но попытка репликации прервалась в результате аварийной остановки;

- если возникает конфликтная ситуация, сервер S1 пытается совместить свою версию документа с версией документа сервера S2. Он сможет выполнить эту операцию только в том случае, если форма, которая использовалась для создания документа, предусматривала активизацию функции **Merge Replication Conflicts** (Совмещение конфликтов при репликации), а измененные поля в копиях документа различны. Когда поле оказывается модифицированным в обеих копиях документа, сервер S1 не пытается совместить документы;
 - если сервер S1 не сможет устранить конфликтную ситуацию, он определит, которая из версий документа имеет больший порядковый номер, а при равенстве номеров - какой из документов позднее претерпел изменения. Данная версия будет объявлена своего рода «победителем», а тот сервер, на котором находится другая версия, создает *конфликтный документ*. Этот документ, содержащий другую версию, будет в дальнейшем рассматриваться в качестве «дочернего» по отношению к документу-победителю. Конфликтный документ появляется на виде с меткой **<Save or Replication Conflict>** (Конфликт при сохранении или репликации) и располагается непосредственно под документом-победителем. Тем не менее, поскольку процесс репликации остается в режиме **Pull** (Вытягивание), конфликтный документ может не сразу попасть в обе копии баз данных.
8. После получения сервером S1 нового или измененного документа с сервера S2 он пересылает серверу S2 временной указатель, который сервер S2 запоминает в журнале репликации. Если процесс репликации прерывается до получения сервером S1 документов, пересылка временного указателя производиться не будет. Следовательно, при следующем взаимодействии серверов процесс начнется с тех же самых действий, с которых он начался в этот раз.
 9. Сервер S1 повторяет рассматриваемый процесс репликации (с шага 4 по 8) для всех имеющихся реплик баз данных.
 10. После окончания приема всех необходимых документов сервер S1 переходит к передаче собственных (новых и модифицированных) документов на сервер S2.

Вариант репликации **Pull-Pull** во многом напоминает описанный выше, хотя имеет два характерных отличия. Во-первых, при повторном обращении к копиям баз данных (шаг 10) сервер S2 берет на себя инициативу и запрашивает получение необходимых документов. Во-вторых, если серверы соединены между собой с помощью модема, процесс получения ими документов будет протекать одновременно, а не последовательно.

Вариант репликации **Pull Only** предусматривает завершение действий после прихода документов на сервер S1 (шаг 9), равно как и вариант **Push Only**, однако в последнем случае на более ранних этапах (шаги с 4 по 8) сервер S1 «выталкивает» (а не «вытягивает») новые и измененные документы на сервер S2.

Расписание репликации для двух серверов

Для организации плановой репликации между двумя серверами необходимо создать документ соединения, обеспечивающий поддержку такого взаимодействия. Один из серверов в этом случае будет инициировать начало сеанса связи, а другой - соответствующим образом реагировать. Перечень полей в документе соединения сервера (Server Connection document), подлежащих заполнению при репликации по расписанию, представлен в табл. 9.1.

Таблица 9.1. Перечень полей документа соединения, используемых при организации процедуры репликации по расписанию

Поле	Назначение
Вкладка Basics (Основные параметры)	
Source server (Исходный сервер)	В это поле вводится имя сервера, инициирующего сеанс связи. При выполнении репликации методом Pull-Pull указанный сервер первым начинает «вытягивание», а во время репликации Pull-Push сервер сначала выполняет «вытягивание», а затем «выталкивание» измененных данных второму серверу
Destination server (Сервер адресата)	В поле помещается имя сервера, который будет отвечать на запрос исходного сервера. В ходе репликации по принципу Pull-Pull этот сервер «вытягивает» данные вторым. В поле можно ввести подстановочный шаблон, чтобы указать сразу несколько серверов
Source domain (Исходный домен) и Destination domain (Домен адресата)	Поле служит для ввода названия домена для серверов. Когда оба сервера относятся к одному домену, заполнять его необязательно
Вкладка Replication/Routing (Репликация/маршрутизация)	
Replication task (Задача репликации)	По умолчанию предусматривается активизация этой задачи
Replicate databases of x priority (Дублирование баз данных с уровнем приоритета)	По умолчанию задается вариант Low & Medium & High (Низкий, средний, высокий), что соответствует случаю использования всех уровней приоритета. В других случаях допускается выбирать варианты Medium & High (Средний, высокий) или High (Высокий). Обычно репликацию баз данных следует производить с использованием параметров по умолчанию, когда разрешены все уровни приоритета. Другие варианты применяют только в тех случаях, когда требуется конкретизировать план репликации, чтобы базы данных с более высоким уровнем приоритета дублировались чаще других
Replication Type (Тип репликации)	По умолчанию в этом поле установлен вариант Pull-Push, отвечающий самому распространенному режиму передачи данных. Альтернативный вариант Pull-Pull назначается только в том случае, когда соединение формируется с помощью модема. Допускаются также варианты Pull Only и Push Only
Files/Directories to Replicate (Реплицируемые файлы/каталоги) в R5 или Files/Directories Paths to Replicate (Файлы и пути к каталогам для репликации) в R6	Это поле следует оставлять незаполненным, чтобы реплицировать все базы данных. Другая возможность: ввести в поле имена одной или нескольких баз или папок данных. Использование символа «звездочка» не допускается
Replication Time Limit (Ограниченный временной интервал репликации)	По умолчанию репликация разрешена в течение необходимого временного интервала. Если потребуется ограничить величину этого интервала для конкретного сеанса связи, укажите здесь максимальное число минут, выделяемых на процедуру репликации для заданного документа соединения. Данные надо изменять весьма осторожно, поскольку при заметном уменьшении временного интервала они вообще могут перестать реплицироваться. См. об этом подробнее в материалах настоящей главы

Таблица 9.1. Перечень полей документа соединения, используемых при организации процедуры репликации по расписанию (окончание)

Поле	Назначение
	Вкладка Schedule (Расписание)
Schedule (Расписание)	По умолчанию эта функция активизируется. Отмена функции планирования приводит к полной отмене соединения
Call at times (Периодичность направления вызова)	В поле указывается число попыток сформировать соединение, предпринимаемых сервером для данного документа соединения. Более подробная информации относительно возможных записей поля содержится в последующих разделах настоящей главы
Repeat Interval of (Временной интервал повторения вызова)	По умолчанию здесь установлен вариант 360 minutes (360 минут, 6 часов). Допустимы любые положительные значения. О записях данного поля речь пойдет в последующих разделах
Days of week (Дни недели)	В поле перечислены дни недели, в которые будет активизирована репликация. По умолчанию эту функцию предполагается активизировать ежедневно

Поле **Call at times** (Периодическое направление вызовов) может содержать момент времени (например, в виде 8:00 a.m., 8 часов утра), временной интервал (скажем, 8:00 a.m. - 10:00 p.m., с 8 часов утра до 10 часов вечера) или последовательность моментов времени и/или временных интервалов (8:00 a.m.; 11:00 a.m.; 2:00 p.m. - 4:30 p.m., 8 часов утра; 11 часов утра; с 2 часов дня до 4 часов 30 минут вечера). При наступлении времени сеанса связи исходный сервер попытается сформировать соединение с сервером адресата и выполнить задачи, указанные в полях раздела **Replication/Routing** (Репликация/маршрутизация).

Если соединение установить не удастся, исходный сервер выжидает в течение определенного временного интервала, а затем предпринимает очередную попытку. При повторном отказе он ждет дольше, после чего вновь пытается сформировать соединение. Начальный временной интервал ожидания невелик, однако его длительность быстро растет по мере увеличения числа отказов. Для расчета длительности интервала ожидания исходный сервер применяет алгоритм случайного экспоненциального отката - Randomized Exponential Backoff Algorithm, который предусматривает увеличение его продолжительности приблизительно вдвое после каждого очередного отказа.

При отказе в ходе формирования соединения для определенного момента времени (например, в виде 8:00 a.m., 8 часов утра) исходный сервер постарается организовать сеанс связи еще в течение 60 минут (или вплоть до формирования соединения), после чего прекратит попытки и будет ожидать следующего заданного момента.

Если отказ получен при установке соединения для временного интервала (скажем, в виде 8:00 a.m. - 10:00 p.m., с 8 часов утра до 10 часов вечера) исходный сервер продолжит попытки организовать сеанс связи вплоть до формирования соединения или до истечения этого интервала.

При успешном создании соединения для временного интервала исходный сервер будет выжидать в течение определенного времени, длительность которого указывается в поле **Connection interval** (Интервал для формирования соединения), после чего будет снова инициировать формирование соединения. Отсчет интервала ожидания в этом случае начинается в момент завершения установки соединения. При том сервер будет игнорировать параметры поля **Connection interval** для соединения на определенный момент времени (например, для 8:00 a.m., 8 часов утра), указанный в соответствующем документе соединения.

Сравнение соединений репликации и маршрутизации

Соединения, предназначенные для репликации данных и для маршрутизации почтовых сообщений, различаются по крайней мере несколькими аспектами. Во-первых, для репликации всегда требуется документ соединения, а для маршрутизации почтовых сообщений он обязателен только в тех случаях, например, когда серверы располагаются в различных сетях или доменах системы Notes.

Во-вторых, на практике можно организовать двунаправленный процесс репликации данных с помощью всего одного документа соединения, а чтобы реализовать двунаправленную маршрутизацию почтовых сообщений, всегда нужны два документа соединения (естественно, если вообще необходимо их использовать).

И наконец, при формировании документов соединения для репликации нет нужды создавать *конкурирующие соединения*. Такими соединениями в данном случае являются соединения, которые для осуществления репликации предусматривают взаимодействие двух серверов на одном и том же временном интервале. Сервер Domino обычно предполагает, что лишь один сервер из пары будет инициировать формирование соединений для репликации данных на каждом конкретном временном интервале. И этот сервер наверняка откажется инициировать запланированный процесс репликации в том случае, если два сервера будут пытаться организовать (на конфликтной основе) соединение для осуществления репликации, причем причину отказа бывает достаточно сложно обнаружить. Если возникают какие-либо обстоятельства, по которым два сервера практически одновременно инициируют операции репликации, для них можно предусмотреть варианты типа **Pull Only** или **Push Only** или попытаться разнести инициируемые сеансы связи на различное время суток.

Осуществление репликации для двух серверов по требованию

Репликация по требованию выполняется соответствующей командой на консоли сервера или в программе Domino Administrator. Для этих целей обычно используются три управляющие команды: replicate, pull и push.

Управляющая команда replicate обеспечивает репликацию в варианте **Pull-Push**, при этом сервер, на который направляется команда, выполняет все необходимые действия и регистрирует все результаты транзакций. Команда может вводиться в двух вариантах:

```
replicate имя_сервера
```

Первый вариант информирует сервер о необходимости репликации для всех баз данных на сервере имя_сервера, второй - о требовании реплицировать определенную базу данных на указанном сервере.

Допускается вводить управляющую команду на консоли сервера в сокращенной форме, скажем в виде rep. Обычно в подобном случае необходимо указывать полное имя второго сервера (например, rep Kestrel/Servers/Stillwater). Тем не менее эта команда вполне корректно исполняется и для сокращенного имени сервера (например, в виде rep kestrel).

Управляющая команда pull обеспечивает репликацию в варианте **Pull-Only**, причем тот сервер, на который направляется команда, получает данные с другого сервера и регистрирует все результаты транзакций. Эта команда также может вводиться в двух вариантах:

pull имя_сервера

pull имя_сервера имя_базы_данных

Управляющая команда push служит для репликации в варианте **Push-Only**. В этом случае сервер, на который поступает команда, передает документы на другой сервер и регистрирует все результаты транзакций.

Команду push, как и команды replicate и pull, допускается применять в двух вариантах. Указанные команды можно ввести на вкладке **Server => Status** (Сервер => Статус) программы Domino Administrator. Для этого на панели **Tools** (Программные инструменты) следует выбрать пункт **Server => Replicate** (Сервер => Репликация), в соответствующем диалоговом окне задать имя сервера, к которому планируется обратиться в процессе репликации, и тип репликации (**Push-Pull**, **Push** или **Pull**), а затем выполнить команду **All databases in common** (Все базы данных в целом) или указать конкретную базу данных.

Выполнение репликации для сервера и рабочей станции

Как и в случае двух серверов, репликация для сервера Domino и рабочей станции системы Notes может быть проведена в режиме по требованию или плановым образом (в соответствии с расписанием документа), причем не предусматривается варианта инициирования репликации какими-либо событиями, как для кластерной репликации. Репликация по требованию возможна в *приоритетном* или в *фоновом режиме*. При репликации в фоновом режиме можно использовать систему Notes для любых других целей, а в приоритетном - нельзя.

Чтобы выполнить репликацию в приоритетном режиме:

1. Откройте локальную базу данных системы Notes или щелкните правой кнопкой по закладке этой базы.
2. Если предусматривается непосредственное открытие базы данных, выполните команду **Replication => Replicate** (Репликация => Реплицировать) в меню **File** (Файл). Если обращение к базе данных производится с использованием закладки, отметьте **Replication => Replicate** в контекстном меню.
3. В диалоговом окне выберите вариант **Replicate with options** (Репликация с указанием параметров), после чего щелкните по кнопке ОК.
4. Во втором диалоговом окне должна отобразиться запись вида **Replicate: Local with servername** (Репликация: локальная на сервере имя_сервера). При появлении записи вида **Replicate: servername with servername** (Репликация: с имя_сервера на имя_сервера) справедлив вывод о том, что не было обращения к локальной копии базы данных (вместо этого обращались к первому названному в записи серверу). В данном случае следует отменить репликацию и заново начать операцию. Если все пройдет успешно, можно выбрать режим отправки, получения или обмена документами. Если принимается решение относительно приема документов, необходимо указать, следует принимать эти документы в полном виде или в виде резюме, после чего щелкнуть по кнопке ОК.

На практике процедуру фоновой репликации допустимо инициировать несколькими способами. Во-первых, можно воспользоваться описанной выше последовательностью действий, а на шаге 3 выбрать **Replicate via background Replicator** (Репликация в фоновом режиме), что позволит осуществить репликацию всей базы данных.

Во-вторых, запуск процедуры репликации разрешается выполнить на странице **Replicator** (Репликатор). Для этого следует выбрать закладку **Replicator** на панели **Bookmarks** (Закладки) и запустить репликацию одной базы данных, указав ее на экране **Replicator**, либо выполнить **Actions => Replicate selected database** (Операции => Репликация указанной базы данных). Предпочтительнее, однако, сначала щелкнуть по кнопке для самой базы данных, а уже затем отметить пункт **Replicate Selected Database** (Репликация указанной базы данных) в контекстном меню.

Репликация всех или некоторых баз данных инициируется также щелчком по кнопке операции **Start** (Запуск), расположенной в верхней части экрана. При этом базы данных, помеченные в левом столбце, будут реплицироваться с привлечением домашнего сервера, если только в списке баз данных не появляется запись вызова, информирующая систему Notes о необходимости обращения к конкретному серверу. На практике достаточно щелкнуть по кнопке **Start** для запуска репликации с несколькими серверами. В таком случае следует либо ввести записи **Call** (Вызов) и **Hangup** (Отключение) в соответствующие поля списка баз данных на экране **Replicator**, либо (если один вызов может быть передан на несколько серверов с помощью, скажем, сквозного сервера) просто указать те базы данных, реплики которых хранятся на нескольких серверах.

Для планирования репликации из клиента системы Notes необходимо разрешить эту операцию в документе местоположения (Location document), а не в документе соединения (Connection document). На вкладке **Replication** каждого документа местоположения надо оговорить два расписания репликации. Во-первых, следует предусмотреть возможность плановой репликации всех баз данных и, во-вторых - дополнительную (и, возможно, более частую) плановую репликацию для баз данных, имеющих высокий уровень приоритета.

Для задания баз данных с высоким уровнем приоритета следует командой **File => Replication => Settings** (Файл => Репликация => Параметры) открыть окно **Replication Properties** (Приоритет репликации), перейти на вкладку **Other** (Другие параметры) и выбрать **Low, Medium or High** (Низкий, средний или высокий).

Для указания репликации в документе местоположения нужно ввести в поля ее расписание в соответствии с рекомендациями, представленными в табл. 9.2.

Таблица 9.2j Список полей планирования репликации в документе местоположения

Поле	Назначение
Schedule (Расписание) и High priority replication (Репликация с высоким приоритетом)	Для обоих полей по умолчанию задан вариант Disabled (Отмена). Вариант Enabled (Разрешено) следует указать в поле Schedule , чтобы выводить на экран перечисленные ниже поля. Это позволяет также увидеть на экране поле High priority replication . Вариант Enabled выбирается для открытия дополнительных полей расписания репликации
Call at times (Периодичность направления вызова)	В поле устанавливается временной интервал, в течение которого система Notes пытается выполнить задачи, назначенные на экране Replicator . Допускается указывать здесь момент времени (например, в виде 8:00 a.m., 8 часов утра), временной интервал (8:00 a.m. — 10:00 p.m., с 8 часов утра до 10 часов вечера), а также последовательность моментов времени и/или временных интервалов (8:00 a.m.; 11:00 a.m.; 2:00 p.m. - 4:30 p.m., 8 часов утра; 11 часов утра; с 2 часов вечера до 4 часов 30 минут вечера). При наступлении оговоренного момента система Notes попытается выполнить операцию, заданную на экране Replicator

Таблица 9.2. Список полей планирования репликации в документе местоположения (окончание)

Поле	Назначение
Repeat interval of x minutes (Временной интервал повторения соответствует x минутам)	Если в поле Call at times (Периодичность направления вызовов) указывается временной интервал, в данном поле определяется периодичность проведения системой Notes попыток (на заданном временном интервале) выполнить операции, представленные на экране Replicator . Если в данном поле имеется несколько моментов времени, записи будут игнорироваться
Days of week (Дни недели)	В этом поле следует задавать дни недели, в которые будет выполняться репликация. По умолчанию данная функция будет активизирована ежедневно

Топологии репликации

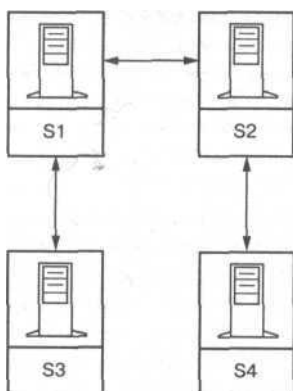
Как правило, каждый сервер Domino в домене обеспечивает регулярную репликацию для других серверов этого домена. Поэтому изменения основных совместно используемых баз данных, в том числе базы данных Domino Directory (файл names.nsf), базы данных Administration Requests (файл admin4.nsf) и некоторых других - в зависимости от конкретно реализуемых служб, происходят своевременно. Необязательно, чтобы сервер реплицировал данные непосредственно со всеми остальными серверами домена. Тем не менее каждый сервер домена должен взаимодействовать по меньшей мере с одним сервером этого домена, а тот, в свою очередь, - с еще одним и т.д., чтобы все серверы домена вовремя вносили изменения в свои копии баз данных.

При работе с приложениями, нуждающимися в частых модификациях реплик баз данных, можно увеличить *частоту репликации* для некоторых серверов. С другой стороны, выполнение такой процедуры требует привлечения большого объема ресурсов и существенно загружает процессор и сетевую полосу пропускания. На практике рекомендуется соблюдать некий баланс между необходимостью частого обновления баз данных и объемом занимаемых при этом ресурсов. (Если репликацию надо проводить незамедлительно, то имеет смысл сформировать кластер серверов Domino, для которого репликация будет осуществляться сразу по завершении изменений в одной из копий базы данных - см. главу 20.)

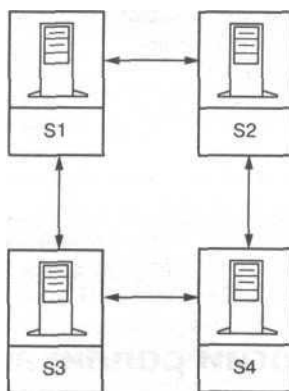
Другими словами, при добавлении серверов в домен надлежит принять решение о том, какие копии баз данных будут храниться на каждом сервере, а также каким образом и как часто они будут обновляться. Естественно, на начальном этапе этот вопрос больше похож на академический. Если предусматривается применение небольшого числа серверов, способ репликации для них допускается выбирать произвольно. При этом возможно использование одной из следующих хорошо известных топологий (рис. 9.1):

- О Hub-and-spoke (Концентратор и радиальные компоненты) - один сервер выбирается в качестве концентратора, а все другие выполняют функции радиальных компонентов;
- О Peer-to-peer (Одноранговое взаимодействие) - каждый сервер домена в состоянии непосредственно взаимодействовать (в части приема или передачи данных) с любым другим сервером домена;
- О End-to-end (Взаимодействие последовательного типа) - сервер S1 может непосредственно взаимодействовать с сервером S2, сервер S2 - с сервером S3 и т.д., вплоть до сервера Sn;

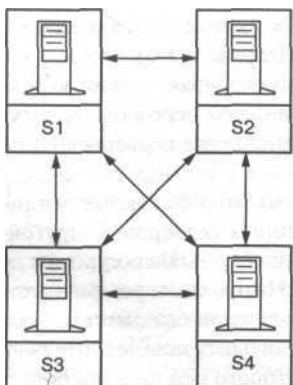
Последовательное соединение



Кольцевая структура



Одноранговое соединение



Концентратори радиальные серверы

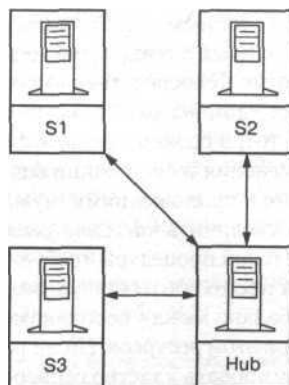


Рис. 9.1. Если в домене используются четыре сервера, следует задуматься о топологии репликации данных и определить связи между серверами. При увеличении числа серверов до пяти наилучшим выбором считается топология с концентратором и радиальными компонентами (внизу справа)

О Ring (Кольцевая структура) - образуется в том случае, когда удастся замкнуть структуру, принятую в предыдущем варианте (путем реализации непосредственного взаимодействия серверов S_i и S_n).

Если имеется от трех до пяти серверов, одноранговая топология обеспечивает целый ряд преимуществ. Она позволяет быстро передавать данные на все серверы и мало чувствительна к отказам и сбоям, поскольку отказ одного сервера не нарушает связей других серверов. Тем не менее при увеличении числа серверов число требуемых документов соединения возрастает экспоненциальным образом ($= n(n-1)/2$), что создает заметные трудности при работе с этой топологией.

При большом числе серверов рекомендуется топология с концентратором и радиальными компонентами, благодаря которой удастся минимизировать число необходимых документов соединения, а также сократить доступ к серверам, используемым в качестве периферийных компонентов структуры в условиях, когда уровень доступа обычно соответствует уровням Editor (Редактор) или Reader (Читатель). И, что самое главное, в этой структуре удастся централизовать регистрацию всех результатов репликации в рамках одного сервера.

На практике уже начиная с четырех или пяти серверов имеет смысл попробовать выделить один из них в качестве концентратора и использовать его в основном для целей репликации. Если предполагается применение многих серверов, этот сервер может сосредоточиться исключительно на задачах репликации данных и не заниматься другими проблемами (например, как сервер почтовой службы, сервер приложений или сервер каталогов), оставив их решение остальным серверам структуры.

В больших доменах (специалисты компании Lotus рекомендуют не менее 25 радиальных серверов на один концентратор) или территориально разнесенных доменах (когда группы серверов разбросаны по разным уголкам планеты) может потребоваться структура с несколькими концентраторами (рис. 9.2) или структура с концентраторами и одноранговыми связями (рис. 9.3). В структуре с несколькими концентраторами *основной концентратор* обеспечивает взаимодействие с вторичными, или *региональными, концентраторами*, а те, в свою очередь, - со своими периферийными компонентами. В структуре с концентраторами и одноранговыми связями концентраторы взаимодействуют попарно, а каждый концентратор - еще и с собственными периферийными компонентами. Поскольку концентраторы также подвержены отказам, на практике желательно применять ту или иную *технология кластеризации*, например создавать кластеры на уровне операционной системы, чтобы минимизировать влияние отказа концентратора на работу всей структуры.

Указанные топологии, естественно, можно рассматривать лишь в качестве базовых. Они призваны облегчить жизнь администраторам в наиболее простых ситуациях, когда соблюдение основных правил позволяет всегда совершенно точно знать, какие из серверов структуры должны взаимодействовать друг с другом, а какие нет. Тем не менее, если *пара радиальных серверов* предназначена для выполнения каких-либо специальных операций и требуется обеспечить между ними непосредственную связь, это должно быть сделано. При необходимости следует сформировать подгруппу серверов, отличающуюся от остальных серверов домена. Например, на рис. 9.3 концентратор Hub1 и серверы S1, S2 и S3 могут взаимодействовать друг с другом попарно, тогда как концентратор Hub1 обеспечивает взаимодействие с указанными серверами и другими концентраторами. Основные цели в данном случае должны состоять в упрощении управления, улучшении предоставляемых пользователям услуг и минимизации используемых ресурсов. При этом следует в обязательном порядке документировать изменения в структуре, чтобы в дальнейшем специалисты могли понять причины произведенных изменений.

Репликация и списки ACL баз данных

Осуществление репликации, а также характер этой процедуры зависят от параметров, содержащихся в списке ACL базы данных, хранящейся на любом типе объектов (серверов и рабочих станций), которые участвуют в процессе репликации. В списке ACL пересылающего данные объекта следует указать, что принимающий данные объект имеет на это

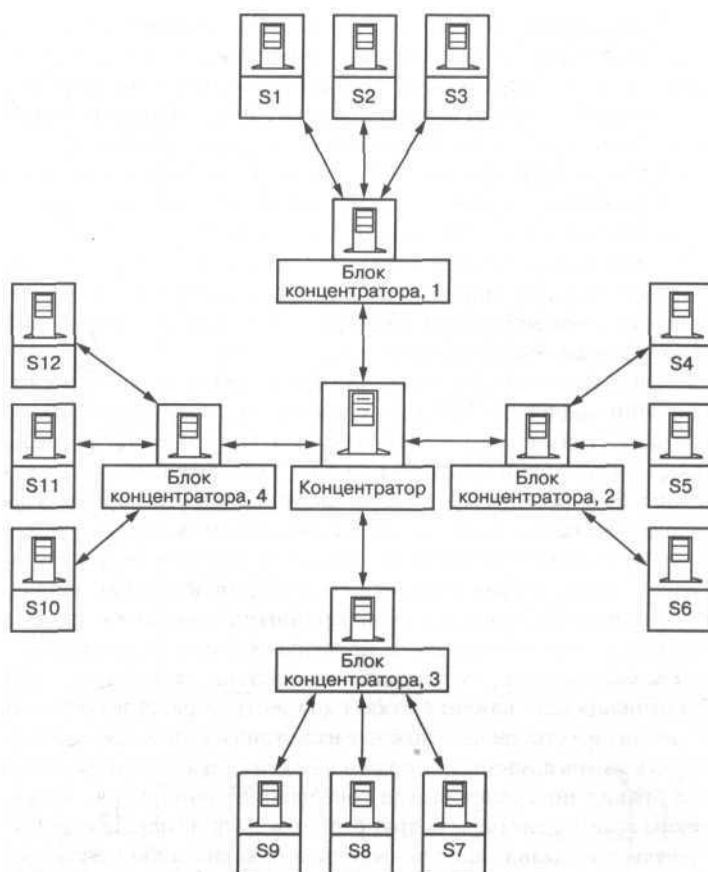


Рис. 9.2. Структура с каскадным соединением концентраторов
(на практике число радиальных серверов значительно больше)

право, а в списке ACL принимающего объекта должно быть оговорено, что передающему объекту разрешено пересылать такие данные. Здесь действуют следующие правила:

- О принимающий документы объект должен обладать (в списке ACL базы данных пересылающего объекта) правом доступа на уровне не ниже **Reader** (Читатель). Кроме того, если для передаваемого документа процедура считывания имеет ограничения, принимающий объект должен иметь специальное разрешение на чтение документа;
- О для отправки документа пересылающая рабочая станция системы Notes обязана обладать (в списке ACL базы данных принимающего сервера) правом доступа на уровне не ниже **Author** (Автор). В частности, если пересылающий объект представлен сервером, этот уровень должен обеспечиваться не ниже **Editor** (Редактор). Либо он может указываться в поле **Author** каждого документа базы данных;
- О для отправки документов проектирования пересылающий их объект должен обладать правом доступа на уровне не ниже **Designer** (Разработчик) и этот уровень обязан быть в списке ACL базы данных принимающего объекта;

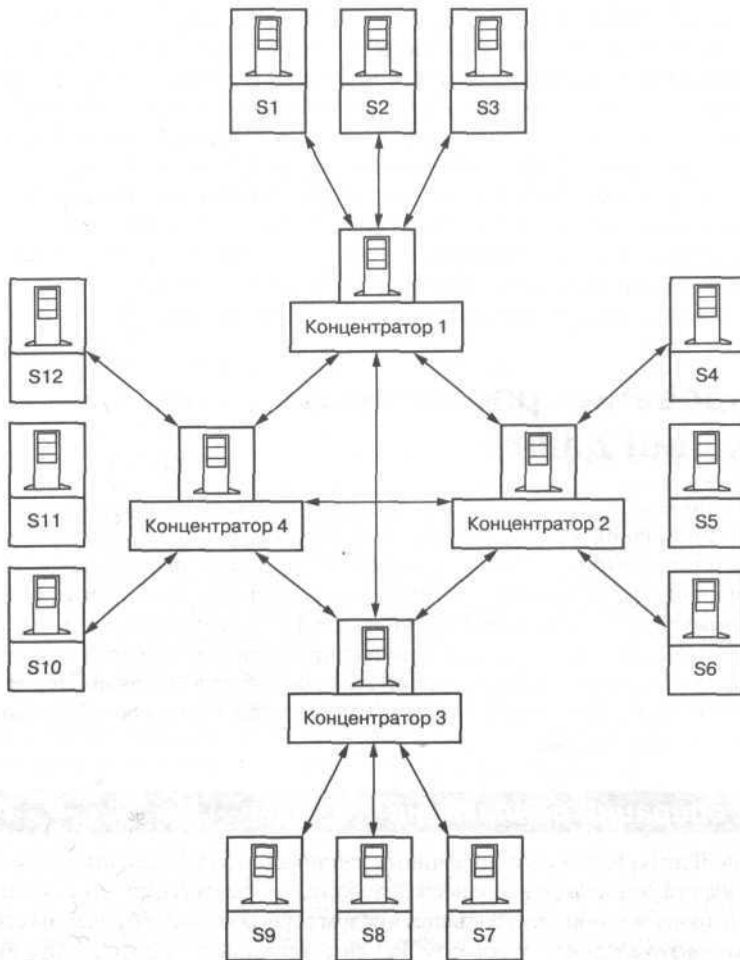


Рис. 9.3. Структура с несколькими концентраторами и одноранговыми связями
(на практике число радиальных серверов значительно больше)

О для отправки скорректированного списка ACL базы данных пересылающий объект должен обладать правом доступа на уровне не ниже Manager (Менеджер) и этот уровень обязан быть в списке ACL базы данных принимающего объекта.

Многие администраторы баз данных решают проблему, связанную с назначением соответствующих прав доступа в списке ACL, посредством придания всем серверам в локальном домене прав доступа на уровне Manager ко всем базам данных. Обычно это реализуется путем предоставления указанного уровня доступа группе LocalDomainServers (Серверы локального домена). В домене, в котором репликация не организована по принципу взаимодействия концентратора и радиальных объектов (см. выше), такой подход оказывается просто необходимым.

Другие администраторы значительно более жестко контролируют процессы репликации и разрешают права доступа на уровне **Manager** и/или **Designer** только определенным серверам, а права доступа с уровнем **Editor** и/или **Reader** - большей части серверов домена. Подобный подход оказывается целесообразным в топологии с концентратором и радиальными компонентами (см. выше). В этой топологии только серверы концентраторов (и, возможно, серверы разработчиков) требуют права доступа на уровне **Manager**, а периферийные серверы вполне могут обойтись правами на уровне **Editor** или **Reader**. Право доступа на уровне **Editor** нужно в том случае, когда пользователи хотят внести изменения в ту или иную базу данных, а на уровне **Reader** - когда пользователи обладают подобным уровнем доступа. Для получения более подробной информации относительно списков ACL баз данных, а также уровней доступа **Editor** и **Reader** обратитесь к главе 10.

Формирование расписания репликации данных

Плановые репликации могут создавать проблемы в двух различных ситуациях. Во-первых, при обслуживании одним концентратором большого числа радиальных компонентов следует убедиться в том, что он не пропускает запланированные операции репликации из-за отсутствия необходимого времени. Во-вторых, если сервер обеспечивает обслуживание (в режиме коммутируемого доступа) пользователей и других серверов, то не исключено, что придется уменьшить объем репликации на определенных интервалах времени, чтобы сервер не монополизировал использование телефонной линии связи. Первая проблема обычно возникает при работе в больших доменах, а вторая - у компаний с ограниченными финансовыми возможностями.

Пропуск операций репликации

Если временной интервал между операциями репликации задается слишком малым, а число серверов, участвующих в этом процессе, наоборот, оказывается слишком большим, можно разрешить пропуск одним или большим числом серверов запланированных сеансов связи. Организуется это следующим образом. Репликатор данных концентратора обеспечивает взаимодействие одновременно только с одним сервером и допускает постановку в очередь до пяти запросов на репликацию. Предположим, что концентратор должен обслуживать 20 серверов, а соответствующие документы (Connection document) информируют концентратор о том, что он должен производить репликацию для каждого сервера с периодичностью в два часа во временном интервале с 8 часов утра до 10 часов вечера ежедневно. Концентратор начинает процедуру репликации с сервера *A* и завершает ее, скажем, за пять минут, после чего переходит к серверу *B* и затрачивает на него также пять минут. В дальнейшем концентратор начинает взаимодействовать с серверами *C*, *D* и другими, репликация для которых занимает время, соответствующее также пяти минутам. В результате концентратор завершает циклический опрос серверов в 9 часов 40 минут утра.

После этого концентратор выжидает в течение двух часов для возобновления взаимодействия с серверами, причем отсчет интервала ожидания начинается с момента завершения взаимодействия с каждым конкретным сервером. Например, концентратор возобновит взаимодействие с сервером *L* в 10 часов 5 минут утра, причем в 10 часов 10 минут он уже должен перейти к обслуживанию сервера *B*, в 10 часов 15 минут - сервера *C* и т.д.

Следует отметить, что информационная нагрузка на базу возрастает по мере активизации различных пользователей, поэтому со временем для проведения репликации может потребоваться не пять, а, скажем, десять минут. В итоге весь цикл репликации будет возрастать до 3 часов 20 минут, при этом репликация для сервера *A* будет завершаться в 10 часов 15 минут и должна снова производиться в 12 часов 15 минут.

В 12 часов 15 минут завершится репликация для сервера *M*, при этом серверы *5* и *Г* будут пытаться занять место на обслуживание в очереди. Сервер *A* в алфавитном порядке располагается перед серверами *5* и *Г*, поэтому в 12 часов 15 минут концентратор перейдет к взаимодействию именно с сервером *Л*, а не с серверами *5* и *Г*. В 12 часов 25 минут он начнет взаимодействовать с сервером *B*, а не с серверами *5* и *Г*, и т.д. Следовательно, два последних сервера могут остаться заблокированными в течение всей рабочей недели или даже нескольких недель.

Подобная ситуация наблюдалась в версии 3, однако теперь такие проблемы возникают относительно редко. Репликация данных в версиях 4, 5 и 6 стала существенно эффективнее по сравнению с версией 3, поэтому пользователям без особых затруднений удастся инициировать репликацию больших объемов данных за весьма короткие интервалы времени. Важным событием стала организация репликации на уровне полей (в версии 4). В дополнение к этому серверы обеспечивают обслуживание большего числа пользователей, чем в версии 3. В результате уменьшилась вероятность возникновения вышеуказанной проблемы из-за роста числа радиальных серверов в организации. И наконец, компания Lotus в наши дни предлагает целый набор программных инструментов, позволяющих быстро устранить данную проблему при ее появлении. В частности, следующие:

- несколько задач репликации, причем допускается загружать два экземпляра в расчете на один процессор (но всего не более восьми). Каждый репликатор (задача репликации) позволяет одновременно взаимодействовать с одним сервером и поддерживать в очереди на обслуживание до пяти запросов. В рассмотренном примере репликатор *R1* обеспечивает обслуживание сервера *Л*, репликатор *R2* - сервера *B* и т.д. Для обеспечения загрузки нескольких репликаторов при очередном запуске сервера необходимо добавить переменную `Replicators=n` в файл `notes.ini`, при этом параметр `n` соответствует числу *задан репликации*, которые будут использоваться сервером. Каждая задача в режиме ожидания занимает объем памяти порядка 3 Мб, поэтому без необходимости излишние репликаторы добавлять не рекомендуется;
- поле **Replicate databases of** (Репликация баз данных) дает возможность задать *расписание репликации* таким образом, чтобы базы данных с более высоким уровнем приоритета обслуживались чаще, чем имеющие более низкие уровни приоритета;
- поле **Files/Directories to Replicate** (Репликация файлов/каталогов) также позволяет установить такой план репликации данных, в соответствии с которым более значимые базы данных смогут чаще других обновлять свои информационные массивы;
- поле **Replication Time Limit** (Ограничение временного интервала репликации). В особых случаях следует организовывать репликацию таким образом, чтобы каждый сервер получал необходимое обслуживание. Это достигается путем ограничения временного интервала, выделяемого каждому серверу на выполнение репликации. Однако данным полем следует пользоваться весьма аккуратно. При заметном уменьшении временного интервала репликации появляется риск, что серверы не будут успевать возобновлять информацию баз данных, а требующие репликации изменения начнут накапливаться и, в конце концов, заблокируют работу всей системы. На практике поле служит совсем иным целям, которые обсуждаются в следующем разделе данной главы.

Монополизация телефонной линии связи

Если имеется ограниченное число модемов (совместно применяемых многими пользователями и серверами), может потребоваться поле **Replication Time Limit** (Ограничение временного интервала репликации) документа соединения для того, чтобы ограничить время, отводящееся серверу на использование телефонной линии связи (для целей репликации данных). Из практики известен клиент сервера Domino с двумя модемами. Сервер обслуживал до 40 пользователей (в режиме коммутируемого доступа) и несколько других серверов. При правильной и ритмичной организации работы сигналы «занято» в этой структуре были достаточно редким явлением. Однако иногда возникали ситуации, когда один из внешних серверов получал большой массив измененных данных, репликация которого (на сервер клиента) требовала от двух до двенадцати часов и полного отвлечения одного из модемов. При этом остальным клиентам приходилось бороться за одну оставшуюся телефонную линию связи, а качество обслуживания неизбежно снижалось.

Клиенту было предложено увеличить число телефонных линий связи (в долгосрочной перспективе планируется использовать линию T-1 для связи с сетью Internet). Однако с точки зрения ближайших потребностей пришлось перенастроить сервер и применить двухкомпонентный план репликации для учета нюансов взаимодействия внешнего (создающего проблемы) сервера с сервером коммутируемого доступа. Один из документов соединения в этом случае оговаривал, что в дневные и вечерние часы (рабочие дни) внешний сервер имел возможность обращаться для репликации лишь несколько раз в день, причем каждый раз репликация осуществлялась только для баз данных с высоким уровнем приоритета и в течение временного интервала продолжительностью не более десяти минут. Второй документ соединения оговаривал, что в ночные часы (рабочие дни) и в выходные дни внешний сервер мог обращаться достаточно часто и выполнять репликацию для всех баз данных, но в условиях, когда продолжительность одного временного интервала репликации не превышала 90 минут.

Было подсчитано, что все жизненно необходимые данные будут передаваться в дневные часы, а большие объемы второстепенных данных - в менее загруженные ночные. В таких условиях сервер не будет долго занимать модем (даже в ночное время). На практике этот вариант дал весьма хорошие результаты, так что в дальнейшем аналогичные подходы были предложены и для других серверов клиентов.

у

Избирательная репликация данных

В целом ряде случаев не требуется дублировать всю информацию, которая содержится в базе данных, помещенной на сервере или на рабочей станции. Например, приложение, связанное с автоматизацией продаж, может иметь копии, хранящиеся в главном офисе компании и в локальных офисах. Копия, находящаяся в главном офисе, должна включать в себя все данные, формируемые указанным приложением и относящиеся как к самому главному офису, так и к локальным офисам. В то же время копии локальных офисов могут ограничиться теми данными, которые касаются продаж в окружающем их регионе. Объем каждой подобной копии может быть заметно уменьшен, в частности, по сравнению с объемом копии, используемой главным офисом. Одновременно появляется возможность снизить продолжительность процедуры репликации для подобных локальных копий приложения и ограничить доступ сотрудникам локальных офисов к конфиденциальной информации, подготавливаемой в главном офисе компании.

Если развить эту идею и дальше, то, возможно, каждый менеджер отдела продаж сумеет обойтись собственной базой данных и репликацией необходимой информации на свой персональный компьютер. Подобный подход позволил бы достичь тех же самых целей: сократить объем реплицируемых данных, снизить время репликации и ограничить доступ к конфиденциальной информации.

Ограничения на репликацию данных можно задавать в диалоговом окне **Replication Settings** (Параметры репликации), причем подход оказывается одинаковым как для самого сервера Domino, так и для системы Notes в целом. Для открытия диалогового окна **Replication Settings** загрузите соответствующую базу данных, а затем выполните команду **Replication => Settings** (Репликация => Параметры) в меню **File** (Файл). Либо щелкните по вкладке для базы данных правой кнопкой мыши, после чего выберите **Replication => Settings** в контекстном меню. В открытом диалоговом окне **Database Properties** (Свойства базы данных) можно также щелкнуть по кнопке **Replication Settings** (Параметры репликации) на вкладке **Database Basics** (Основные параметры базы данных).

Диалоговое окно **Replication Settings** содержит четыре вкладки:

- **Space Savers** (Экономия пространства) - позволяет несколькими способами ограничить число и тип документов в заданной копии базы данных. Поля экрана представляют определенный интерес для пользователей системы Notes, выражающих желание уменьшить размер локальной реплики базы данных;
- **Send** (Пересылка) - дает возможность ограничить объем данных, пересылаемых локальной репликой в другие копии базы данных; интересен для пользователей системы Notes (но не для самих администраторов);
- **Other** (Другие параметры) - здесь можно определить вспомогательные параметры, связанные с процедурой репликации данных. При этом допускается временно прервать репликацию, установить уровень приоритета для дублируемой базы данных, а также указать даты, ограничивающие время существования документов, которые данная реплика получает от других копий баз данных. Экран очень важен для администраторов серверов и баз данных;
- **Advanced** (Дополнительно) - этот экран позволяет задать формулу выбора базы данных и представляет особый интерес для администраторов серверов и баз данных.

Таблица 9.3. Перечень полей диалогового окна **Replication Settings**

Поле	Назначение
Вкладка Space Savers (Экономия пространства)	
Remove documents not modified in the last x days (Удаление документов, неизменявшихся в течение x последних дней)	Это поле на практике соответствует двум полям, причем второе поле имеет два назначения. Во-первых, при установке флажка в первом поле система Notes/Domino будет автоматически удалять и очищать документы, которые не изменялись в течение последних x дней с момента создания базы данных. Большая часть баз данных по умолчанию к этому полю не обращается, однако в некоторых шаблонах баз данных предусмотрено изменение параметров режима по умолчанию. Во-вторых, число дней (x) может меняться. Для большинства баз данных по умолчанию задается число 90, но существуют шаблоны, для которых оно в режиме по умолчанию указывается заметно меньшим. Поле с числом дней может служить и для других целей, например для определения периода очистки базы данных и вывода исключенных документов. Более подробная информация по данному вопросу приводится ниже

Таблица 9.3. Перечень полей диалогового окна **Replication Settings** (продолжение)

Поле	Назначение
Include (Включая)	Поле появляется только в том случае, если используемая база данных соответствует адресной книге или каталогу. Для этого поля возможны следующие варианты: All Fields (Все поля), Minimal Address Book (Краткая адресная книга), Minimal Address Book => Encryption (Краткая адресная книга => Шифрование), Minimal Address Book => Person Info (Краткая адресная книга => Данные о сотрудниках) или Minimal Address Book => Encryption => Person Info (Краткая адресная книга => Шифрование => Данные о сотрудниках). В версии R6 добавлены Configuration document only (Только документы конфигурации) и Custom (Пользовательская настройка). Каждая запись, связанная с обращением к краткой адресной книге, предусматривает задание определенной формулы репликации в нижнем поле, которая позволяет ограничить перечень реплицируемых полей и документов. Данное поле оказывается весьма полезным в тех случаях, когда предварительно не была активизирована функция Directory Catalog. В такой ситуации поле позволяет пользователям быстро реплицировать базу данных Domino Directory в память портативных компьютеров, чтобы в дальнейшем была возможность производить поиск адресов даже после отключения от сервера
Receive summary and 40kb of rich text only (Прием только резюме и расширенного текстового сообщения объемом не более 40 Кб)	Поле появляется только в том случае, когда производится проверка параметров репликации (Replication Settings) для конкретной базы данных сервера. Пользователь системы Notes имеет возможность проверить указанные параметры, чтобы ограничить число и типы реплицируемых массивов данных. Усеченные текстовые материалы можно дублировать в объеме не более 40 Кб, причем репликация дополнений не допускается. В этом случае слово «Truncated» (усеченный) появляется в заголовке выводимого усеченного документа. Пользователь, конечно, способен вывести документ целиком командой Retrieve Entire Document (Извлечение всего документа) в меню Actions (Операции)
Replicate a subset of documents (Репликация подмножества документов) в R5 или Documents in specified views and folders (Документы в указанных видах или папках) в R6	После установки флажка появляется возможность отметить в списке один или большее число видов либо папок. Только те документы, которые относятся к выбранным видам и папкам, будут реплицироваться в этой копии базы данных \$
Select by formula (Выбор по формуле) в R5 или Documents that meet selection formula (Документы, удовлетворяющие формуле выделения) в R6	После установки флажка открывается диалоговое окно, в котором имеется возможность вводить и редактировать формулу выбора (о формулах выбора рассказывается в справке Designer Help - Справка программы Domino Designer)

Таблица 9.3. Перечень полей диалогового окна **Replication Settings** (продолжение)

Поле	Назначение
Fields & Functions (Поля и функции)	Эта кнопка появляется в том случае, если установлен рассмотренный выше флажок. Следует щелкнуть по кнопке для вывода окна Fields and function (Поля и функции), где можно выбрать объект для вставки в формулу (см. в данном окне справку о каждом объекте)
Formula Window (Окно формулы)	Эта кнопка присутствует на экране, если установлен флажок выбора по формуле. При ее нажатии открывается окно редактирования выбранной формулы Вкладка Send (Пересылка)
Do not send deletions made in this replica to other replicas (Не пересылать сведения об удалениях в данной реплике другим репликам)	Пользователь системы Notes, установивший этот флажок для локальной копии базы данных, получает возможность окончательно удалять документы для высвобождения области памяти на жестком диске. Удаляемые документы в таком случае не будут копироваться в базу данных сервера
Do not send changes in database titles & catalog info to other replicas (Не пересылать изменения в заголовке базы данных и данных каталога в другие реплики)	После установки этого флажка изменения заголовка локальной базы данных и параметров каталога Database Catalog не будут реплицироваться в другие копии баз данных
Do not send changes in local security property to other replicas (Не пересылать изменения в локальных свойствах безопасности в другие реплики)	Следует установить этот флажок для того, чтобы блокировать дублирование локальных параметров шифрования базы данных в другие реплики базы данных Вкладка Other (Другие параметры)
Temporarily disable replication (Репликация временно прекращена)	Флажок устанавливается при необходимости временно приостановить репликацию базы данных. Если пользователь сомневается в целостности этой или какой-либо другой реплики базы данных и хочет избавить себя от проблем, в частности от распространения ошибок на другие базы, имеет смысл воспользоваться таким флажком
Scheduled replication priority (Приоритет плановой репликации)	В поле могут задаваться варианты Low (Низкий), Medium (Средний) и High (Высокий). Документы соединения, в поле Replicate databases of priority (Репликация баз данных с приоритетом) которых задается вариант High (Высокий) или High & Medium (Высокий, средний), используют этот параметр для определения необходимости репликации базы данных. Не следует путать данный уровень приоритета с низким, средним и высоким уровнями приоритета в процедуре передачи почтовых сообщений (эти параметры совершенно не связаны между собой)

Таблица 9.3. Перечень полей диалогового окна **Replication Settings** (продолжение)

Поле	Назначение
Only replicate incoming documents saved or modified after (Репликация только входящих документов, сохраненных или измененных после)	Система автоматически устанавливает в данном поле значение, однако пользователь всегда имеет возможность его изменить. Только документы, созданные или измененные по истечении даты/времени, определенных в этом поле, могут быть применены при репликации
CD-ROM publishing date (Дата публикации диска CD-ROM)	Некоторые базы данных весьма объемны, поэтому представляется целесообразным формировать их копии на диске CD-ROM. Пользователь может скопировать базу данных с компакт-диска на сервер (в папку данных), а затем ввести дату публикации диска CD-ROM в это поле. При первом формировании копии исходной базы данных репликация будет выполнена только в отношении документов, которые создавались и изменялись после даты, назначенной в данном поле
Вкладка Advanced (Дополнительно)	
When computer (При использовании компьютера)	Здесь указывается, какой компьютер из соответствующего списка будет выполнять функцию сервера адресата
Receivers from (Прием с)	В этом поле задается другой компьютер из списка, который будет служить исходным сервером
Replicate a subset of documents (Репликация подмножества документов) в R5 или	Элемент управления, действует аналогично одноименному элементу на вкладке Space Savers (Экономия пространства)
Documents in specified views and folders (Документы в указанных видах или папках) в R6	
Select by formula (Выбор по формуле) в R5 или	Элемент управления, действует аналогично одноименному элементу на вкладке Space Savers
Documents that meet selection formula (Документы, удовлетворяющие формуле выделения) в R6	
Fields & Functions (Поля и функции)	Элемент управления, действует аналогично одноименному элементу на вкладке Space Savers л
Formula Window (Окно формулы)	Элемент управления, действует аналогично одноименному элементу на вкладке Space Savers
Флажки Replicate (Реплицировать)	В расположенных ниже полях можно выбрать типы объектов базы данных (отличных от документов), которые будут реплицированы со второго компьютера на первый
Replicate: Forms, views, etc (Формы, виды и т.д.) в R5 или Replicate: Design elements (Элементы проектирования) в R6	Эта функция активизируется в режиме по умолчанию. Если исходный сервер имеет уровень доступа Designer к базе данных, он сможет пересылать все документы проектирования в базу данных адресата. При отмене данной функции блокируется пересылка всех документов проектирования, за исключением агентов

Таблица 9.3. Перечень полей диалогового окна **Replication Settings** (окончание)

Поле	Назначение
Replicate: Agents (Агенты)	Функция активизируется в режиме по умолчанию, а при ее отмене блокируется пересылка агентов
Replicate: Replication formula (Формула репликации)	Функция отменяется в режиме по умолчанию. При ее активизации исходный сервер получает возможность пересылать формулу репликации, заданную в поле Replicate a subset of documents (Репликация подмножества документов) на сервер адресата
Replicate: Access control list (Список управления доступом)	Функция активизируется в режиме по умолчанию. При ее отмене блокируется пересылка списков ACL, причем даже в тех случаях, когда исходному серверу придан уровень доступа Manager в списке ACL сервера адресата
Replicate: Deletions (Удаленные данные)	Функция активизируется в режиме по умолчанию. При ее отмене сервер адресата принимает удаленные ранее данные с исходного сервера. Это поле эквивалентно полю исходного сервера Do not send deletions made in this replica to other replicas (Не пересылать удаления в данной реплике другим репликам) - см. подробнее в начале таблицы
Replicate: Fields (Поля)	Функция отменяется в режиме по умолчанию. При необходимости ее активизации следует щелкнуть по кнопке Define (Определение) для открытия диалогового окна Replicate Selected Fields (Репликация заданных полей). В этом окне можно выбрать те же варианты, что и в поле Include вкладки Space Savers - см. подробнее в начале данной таблицы

Интересной особенностью экрана **Advanced**, описанного в последнем разделе табл. 9.3, является то, что на практике можно задавать различные комбинации компьютеров для полей **When computer** (При использовании компьютера) и **Receives from** (Прием с), а также выбирать индивидуальную формулу для любой такой комбинации. В дальнейшем при обращении к полю **Replicate: Replication formula** (Репликация: формула репликации) на той же вкладке выбранная формула репликации будет пересылаться в каждый документ сервера (Server document). Это позволяет однократно ввести формулу репликации (для исходной копии базы данных), а затем распространить ее по другим репликам баз данных.

Существует еще три важных замечания о параметрах указанного диалогового окна. Во-первых, это в основном специальные параметры, относящиеся исключительно к той реплике базы данных, для которой они задаются. За небольшим исключением, они не будут реплицироваться в другие копии базы данных. Исключение в данном случае связано с самой формулой репликации, но только в том случае, если установлен флажок **Replicate: Replication formula** (Репликация: формула репликации), и только для той формулы, которая оказывается приемлемой для сервера адресата.

Во-вторых, использование формулы репликации не способствует обеспечению безопасности. На практике формулой можно ограничить данные, получаемые сервером с сервера главного офиса компании, причем соответствующая формула может быть создана на сервере главного офиса, а затем передана на сервер локального офиса. Однако в этом случае не удастся помешать лицам, имеющим доступ к серверу локального офиса или доступ на уровне **Manager** к базе данных, изменить формулу и тем самым получать больший объем

информации. (Если требуется воспользоваться безопасным подходом и кардинально ограничить репликацию документов, можно ограничить доступ для чтения данных, но это уже больше относится к разработчикам приложений, а не к администраторам.)

В-третьих, на практике требуется уровень доступа не ниже **Designer** к той базе данных, для которой планируется изменить формулу репликации и поле **Replication** (Репликация), а также уровень доступа не ниже **Manager** для изменения параметров репликации. Однако любой сотрудник вправе ознакомиться с параметрами репликации для определенной базы данных, в том числе и пользователь с уровнем доступа **No Access** (Без доступа) в списке **ACL** (например, если он имеет доступ к закладке базы данных). В этой ситуации необходимо выполнить следующие действия: создать закладку для базы данных, к которой имеется право доступа на уровне **Manager**. Затем добавить пользователя в список **ACL**, задать для него уровень доступа **No Access** и указать на этот факт в идентификационных данных пользователя, после чего щелкнуть по закладке базы данных и выбрать **Replication => Settings**.

Конфликтные ситуации, возникающие при репликации и сохранении документов

Поскольку система Notes является системой с распределенными базами данных, в ней нельзя запретить *конфликтное редактирование* одних и тех же документов (никто этого делать и не пытается, по крайней мере в режимах по умолчанию). Зато система предусматривает применение программных инструментов и процедур, направленных на минимизацию конфликтных ситуаций и быстрое их разрешение. Для баз данных системы Notes на практике могут возникать конфликты двух типов:

- О конфликтные ситуации при сохранении документов. Когда сотрудники одновременно редактируют информационный документ одной и той же реплики базы данных, тот из них, кто первым выполнит сохранение, сможет корректно завершить операцию. Однако в дальнейшем, когда сохранение попытается выполнить другой сотрудник, система Notes выведет на экран предупреждение **Another copy of this document was saved while you were editing it. Save your changes also as a Save Conflict document?** (Другая копия данного документа была сохранена в процессе вашего редактирования. Следует ли запомнить вашу копию в виде сохраняемого конфликтного документа?), на которое следует дать утвердительный или отрицательный ответ. Во избежание возникновения конфликтной ситуации второму сотруднику рекомендуется отказаться от продолжения редактирования;
- О конфликтные ситуации при репликации документов. Когда документ изменяется в двух различных репликах базы данных (в период между сеансами репликации), также возможна конфликтная ситуация. При следующей репликации двух баз данных репликатору придется так или иначе разрешать этот конфликт или переводить один из документов в разряд конфликтных.

Когда в вышеуказанных ситуациях принимается решение о формировании конфликтного документа, этот документ появляется на виде в качестве дочернего по отношению к основной версии документа и снабжается заголовком **[Replication or Save Conflict]** (Конфликт при сохранении или репликации). Основной документ считается победителем, а конфликтный переводится в разряд второстепенных, что способствует успешному разрешению конфликтной ситуации в системе (рис. 9.4).

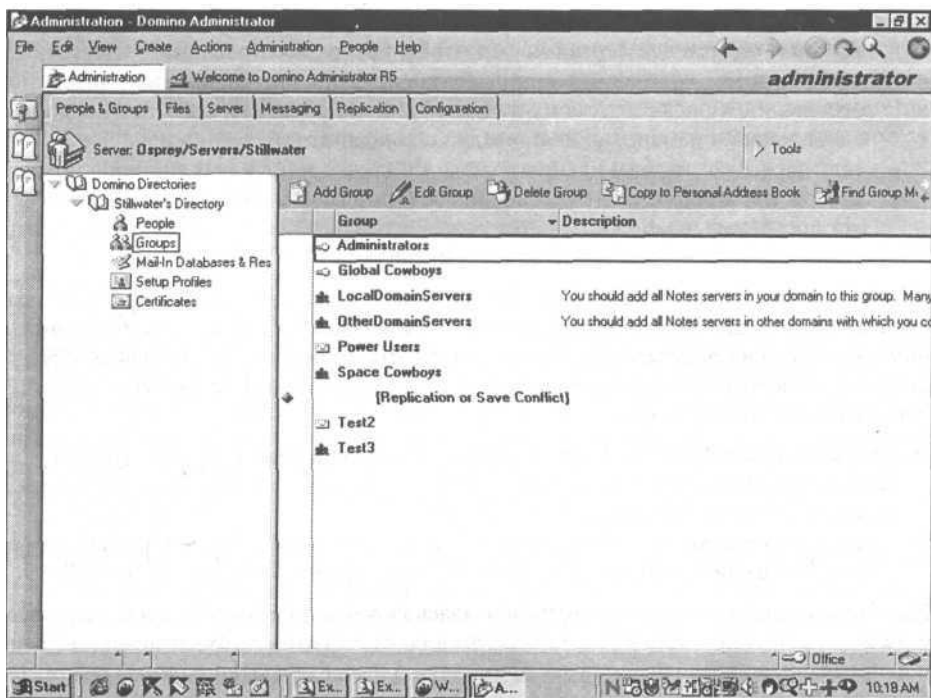


Рис. 9.4. Документы Space Cowboys и [Replication or Save conflict] конфликтуют друг с другом. В соответствии с принятым компанией Lotus подходом Space Cowboys является победителем, а [Replication or Save Conflict] - проигравшей стороной

Правила разрешения конфликтных ситуаций

Сервер Domino обеспечивает разрешение различных конфликтных ситуаций при сохранении и репликации документов. Разрешаемыми обычно бывают следующие конфликты:

- если два сотрудника независимо друг от друга редактируют один и тот же список ACL, превалирует первое изменение;
- когда два сотрудника независимо один от другого редактируют документ проектирования (Design document), превалирует первое изменение;
- если один сотрудник редактирует информационный документ, а другой его удаляет, превалирует первое изменение;
- если два сотрудника редактируют один и тот же информационный документ на двух разных серверах (в интервале между операциями репликации), конфликтной ситуации можно избежать в следующих случаях:
 - когда функция **Merge replication conflicts** (Слияние конфликтов при репликации) активизирована для той формы, с помощью которой создается данный документ, и два редактора работают с различными полями, программа репликации (Replicator) обеспечит совмещение двух версий документа;

- если для формы, посредством которой формировался документ, активизирована *функция управления версиями*, так чтобы при редактировании существующего документа мог создаваться новый документ (дополнительный или дочерний по отношению к редактируемому документу, но не родительский), два проводимых одновременно изменения не приведут к конфликтной ситуации;
- если разработчик базы данных создал в свое время управляющий заголовок LotusScript для разрешения конфликтов (например, в виде специального агента), эта программа, возможно, сумеет разрешить конфликтную ситуацию в соответствии с собственными критериями и правилами.

Существующие правила удаления одного из списков ACL, документов проектирования (Design document) или информационных документов (Data document) и определения среди них победителя и проигравшей стороны могут быть применены в том случае, когда репликатор оказывается не в состоянии справиться с возникшей конфликтной ситуацией. Эти правила заключаются в следующем:

- О *правило наиболее частой повторяемости*. В конфликтной ситуации (при осуществлении репликации) победителем считается та версия конфликтного документа, которая редактировалась большее число раз;
- О *правило более позднего редактирования*. Если обе версии редактировались одинаковое число раз, победителем признается версия, сформированная последней.

Если одна копия документа модифицировалась между двумя сеансами репликации, скажем дважды, а другая - только единожды, то в соответствии с первым правилом первая копия, признанная победителем, будет применяться в ходе очередного сеанса репликации.

Если же обе копии документа модифицировались одинаковое число раз между сеансами репликации, то согласно второму правилу копия, которая модифицировалась последней, считается победителем и может быть, например, исключена из базы данных в ходе очередного сеанса репликации.

Разрешение конфликтных ситуаций вручную

Если, несмотря на все предпринятые усилия, конфликтный документ не появляется в базе данных, администратору придется самостоятельно разрешить возникшую конфликтную ситуацию. Для этого ему потребуется выполнить следующие действия:

1. Проанализировать оба документа и определить наличие между ними конфликта.
2. Скопировать (при необходимости) данные одного документа в другой, чтобы привести их к приемлемому виду.
3. Удалить из рассмотрения немодифицированный документ.

Простейший способ устранения конфликтной ситуации такого типа состоит в использовании документа-победителя и отбрасывании другого документа. В этом случае все, что требуется сделать после копирования данных из отбрасываемого документа, - это удалить его из рассмотрения.

Если все же принимается решение сохранить проигравший документ и отбросить документ-победитель, следует сначала преобразовать первый документ к его обычному виду. Ниже описывается один из возможных приемов выполнения этой операции:

1. Пометьте документ-победитель в качестве исключаемого.
2. Затем откройте в режиме редактирования проигравший документ, сохраните его и снова закройте. (Для этого требуется последовательно нажать клавиши Ctrl+E,

Ctrl+S, Ctrl+W, причем можно просто не отпускать клавишу **Ctrl** и последовательно нажимать клавиши для указанных букв). Упомянутый документ появиться на виде в качестве обычного документа, возможно непосредственно под документом победителем, и будет иметь точно такой же заголовок. (Однако, в зависимости от произведенных в документе изменений, эти два документа могут поменяться местами - по данной причине документ победитель должен помечаться на шаге 1). Следует отметить, что указанный документ может появляться на виде и в другой позиции, а также иметь свой индивидуальный заголовок.

3. Нажмите клавишу F9 для обновления вида, в результате чего документ-победитель будет удален.

Поскольку анализ конфликтных документов представляет собой достаточно трудоемкую процедуру, старайтесь избегать их формирования. Выше было показано, каким образом администратор базы данных может исключать конфликтные ситуации - например, с помощью функции **Merge replication conflicts** (Слияние конфликтов при репликации), функции управления версиями и специальной программы разрешения конфликтов на языке программирования LotusScript. Ниже приводится перечень приемов, с помощью которых администратор базы данных способен в значительной степени сократить число возникающих конфликтов:

- О уменьшение числа пользователей, имеющих право редактировать существующие документы в базе данных. Это достигается за счет придания большей части пользователей права доступа на уровне не выше **Author**. Таким способом удастся снизить вероятность возникновения конфликтных ситуаций;
- О создание администраторами баз данных лишь необходимого для них числа реплик. Пользователи часто сами понимают, когда они рискуют вызвать конфликтную ситуацию, а когда в состоянии избежать ее появления. Однако они не могут удалять конфликты в ходе репликации. Поэтому при сокращении числа реплик баз данных снижается и вероятность создания самими пользователями конфликтных ситуаций. Дополнительное преимущество в этом случае состоит в том, что для обслуживания меньшего числа реплик требуется и меньший объем ресурсов;
- О задание предельного уровня для свойства базы данных **Limit entries in SRevisions field** (Ограничение записей в поле Изменения), например не меньше 10 записей. При уменьшении предельного уровня появляется опасность того, что задача репликации (которая обращается к указанному полю в процессе анализа и разрешения конфликтных ситуаций) сделает вывод относительно наличия конфликта в тех случаях, когда на самом деле его нет.

Создание новых реплик

В предыдущем разделе одна из рекомендаций касалась минимизации числа реплик базы данных, что позволяет уменьшить вероятность возникновения конфликтных ситуаций и ту нагрузку, которая связана с сетевой репликацией. Из этой рекомендации можно сделать вывод о том, что увеличение числа реплик нежелательно. Однако подобный вывод в целом, конечно же, неверен, поскольку продуманное создание и использование реплик баз данных приводит к заметному положительному результату. Преимущества, связанные с использованием дополнительных реплик баз данных, заключаются в следующем:

- О информационная нагрузка распределяется между большим числом серверов, что способствует улучшению характеристик самих серверов;

- О локализуются *сетевые информационные потоки*, а данные становятся более доступными для удаленных пользователей, поскольку реплики баз данных располагаются на серверах, являющихся локальными по отношению к этим пользователям;
- О появляется возможность отделить рабочую версию базы данных от версий разработчика, претерпевающих последующие изменения;
- О обеспечивается доступность базы данных даже в случае отказа резидентного сервера;
- О можно выполнять операции избирательной репликации, направлять на рабочие станции лишь необходимые наборы данных и предоставлять деловым партнерам, поставщикам, клиентам и общественным организациям только информацию, предназначенную специально для них;
- О удаленные пользователи, не имеющие связей с сервером (например, владельцы, использующие переносной компьютер в самолете), смогут нормально работать с локальной репликой базы данных.

Некоторые реплики создаются сервером Domino практически автоматически, например реплики баз данных Domain Directory и Administration Requests. Но большая часть реплик должна быть сделана администраторами. Начиная с версии R5 формировать реплики баз данных на серверах можно с помощью процесса Administration Process (Процесс администрирования) или совершать все операции вручную. Для создания реплик баз данных на рабочих станциях необходимо произвести соответствующую настройку или выполнить все процедуры вручную.

При формировании реплик баз данных на серверах обычно возникает большое желание воспользоваться процессом Administration Process, поскольку он заметно облегчает дело, обеспечивая быстрое создание различных реплик баз данных на многочисленных серверах, причем большая часть операций выполняется автоматически. При этом процесс формирует реплики-заглушки (не наполненные информацией базы данных). Поскольку процесс Administration Process делает такие реплики автоматически, они иногда называются *заготовками баз данных по умолчанию*, что указывает на возможность заполнения их любым сервером в процессе репликации.

Реплика базы данных может быть сформирована и вручную - например, в том случае, когда не удастся применить процесс Administration Process или необходима какая-либо специальная реплика. Так, иногда требуется ограничить объемы репликации данных или шифровать информацию локальной базы данных.

Создание реплик баз данных на серверах: предварительные замечания

Перед созданием новой реплики базы данных на другом сервере следует убедиться в самой возможности подобных действий. Для этого предварительно выполните следующее:

1. Убедитесь, что исходный сервер допустимо подключить к серверам адресата. Для этого может потребоваться создание нескольких документов соединения (Connection document). В этом случае удобен программный инструмент Trace Connections (Отслеживание соединений) в диалоговом окне **User Preferences => Ports** (Предпочтения пользователя => Порты) для проверки соединений и поиска неисправностей. Для получения более подробной информации о программе Trace Connections обратитесь к главам 4 и 6.

2. Удостоверьтесь, что администратор и исходный сервер имеют все необходимые права доступа для создания реплик баз данных на серверах адресата. При этом необходимо проверить поле **Create replica databases** (Создание реплик баз данных) вкладки **Security** (Безопасность) в документе сервера (Server document) для каждого сервера адресата. При необходимости в поле следует занести имена групп, членами которых являются администратор и исходный сервер.
3. Проверьте, обладают ли администратор и серверы адресата правом доступа по меньшей мере на уровне **Reader** к соответствующим базам данных. Если нет, то исходный сервер будет отклонять все запросы на создание новой реплики базы данных.

Использование процесса Administration Process для создания новых реплик баз данных

Для создания новой реплики базы данных в программе Administration Process нужно убедиться в том, что удовлетворены все предварительные условия (см. предшествующий раздел), и только после этого предпринять следующие действия:

1. Запустите программу Domino Administrator и перейдите на экран **Files** (Файлы).
2. Укажите сервер, на котором хранятся текущие реплики баз данных.
3. Выберите одну или несколько баз данных, используя клавиши **Shift** и **Ctrl** для выбора второй и последующих баз данных.
4. Для выбранных баз данных выполните **Database => Create Replica(s)** (База данных => Создание реплик) на панели **Tools** (Программные инструменты), появится диалоговое окно **Create Replica** (Создание реплики).
5. Укажите имена серверов адресата в поле **Create replicas on these servers** (Создание реплик для этих серверов).
6. Для редактирования имен файлов (баз данных) каждого сервера адресата служит кнопка **File Names** (Имена файлов). Надо в диалоговом окне **Edit Destination Path** (Редактирование имени файла адресата) отметить (по очереди) все серверы поля **Destination database and server** (База данных и сервер адресата), после чего отредактировать имена в поле **Destination file path** (Имя файла сервера адресата). В версии R6 кнопка **File Names** отсутствует, но остальные поля находятся непосредственно в диалоговом окне **Create Replica** (Создание реплики).
7. Щелчком по кнопке **OK** закройте соответствующие диалоговые окна, при этом появится сообщение, формируемое программой Domino Administrator и информирующее о том, сколько баз данных обработано и сколько ошибок обнаружено.

После этого процесс Administration Process создаст заготовки баз данных, которые выполняются в течение последующих сеансов репликации. Такие сеансы в дальнейшем будут инициироваться между серверами адресата и сервером, располагающим заполненной записями копией реплицируемых баз данных.

Создание новых реплик баз данных вручную

Существует два способа создания реплик баз данных на новом сервере вручную, причем ни один из этих способов нельзя назвать предпочтительным. Во-первых, администратор

может выполнить команду **Replication => New replica** (Репликация => Новая реплика) в меню **File**. Во-вторых, администратор способен использовать программные инструменты операционной системы для копирования базы данных на другой сервер. Следует отметить, однако, что на практике не представляется возможным сформировать новую копию с помощью команды **Database => New Copy** (База данных => Новая копия) меню **File**.

Две базы данных считаются репликами в том случае, если они применяют одни и те же идентификационные данные реплики. Командой **New replica** (Новая реплика) обеспечивается копирование идентификационных данных реплики в новую базу данных. Использование команды **New copy** (Новая копия) не приводит к такому же результату, поскольку ведет к созданию новой базы данных с новыми идентификационными данными реплики, при этом новая база данных будет похожа на исходную, но не сможет взаимодействовать с ней в процессе репликации. При выполнении операции копирования с помощью операционной системы идентификационные данные исходной реплики сохраняются без изменений (поскольку операционная система не изменяет содержимого копируемого файла), поэтому в данном случае новая копия является реальной репликой исходной базы данных.

Для создания новой реплики базы данных вручную (на сервере R5 или R6) следует выполнить те же предварительные операции, что и для процесса Administration Process. Исходный сервер и сервер адресата должны формировать соединения, администратор и исходный сервер обязаны располагать необходимыми правами доступа для создания новой реплики на сервере адресата, а администратор и сервер адресата должны располагать необходимыми правами доступа (не ниже **Reader**) к соответствующей базе данных.

Эти требования несколько отличаются от аналогичных требований, имевших место в версии 4, причем в тех случаях, если предусматривается работа в смешанной среде (с версиями 4), необходимо хорошо представлять себе существующие различия. Так, для создания новой реплики на сервере R4 администратор и исходный сервер должны обладать правами доступа не ниже уровня **Designer** к исходной базе данных. В противном случае процесс создания новой реплики базы данных завершится отказом, а сервер адресата R4 сформирует сообщение об ошибке.

Формирование заготовки реплики может пройти вполне успешно, однако при поступлении в эту базу данных списка ACL (в процессе очередной операции репликации) сервер адресата обнаружит, что администратор или исходный сервер не обладают правом доступа на уровне **Designer**, и откажется принимать какие-либо документы проектирования. В результате репликация прервется и работать с этой базой можно будет лишь после того, как к ней обратится исходный сервер с правом доступа на уровне **Designer**, указанным в списке ACL сервера адресата. Только тогда появится возможность передавать документы проектирования и заполнять созданную базу данных.

Такой подход является традиционным и соответствует стандартным правилам обеспечения безопасности в системе Notes, причем вариант получения сервером R5 или R6 полной реплики базы данных с сервера, располагающего правами доступа (к этой базе данных) лишь на уровне **Reader**, является исключением из правил.

Чтобы создать новую реплику базы данных вручную (с помощью системы Notes или программы Domino Administrator) выполните следующие операции:

1. В меню **File** выберите **Replication => New replica** (Репликация => Новая реплика). Если база данных уже была открыта, подойдет вариант **New replica** (Новая реплика), при этом появится диалоговое окно **New Replica [заголовок_базы_данных]**

(Новая реплика базы данных, с указанием названия). Если база данных ранее не была открыта, будет выведено диалоговое окно **Choose Database** (Выбор базы данных).

2. При отображении подобного диалогового окна следует использовать его для выбора исходного сервера и базы данных. Сначала рекомендуется выбирать сервер, а уже затем базу данных. В случае, если имя базы данных не появляется в списке **Database** (База данных), нужно указать имя файла в поле **File name** (Имя файла), затем воспользоваться кнопкой **Open** (Открыть) или **Select** (Выбор).
3. После этих действий на экран выводится диалоговое окно **New Replica for [заголовок базы данных]**. Выберите имя сервера адресата в поле **Server** (Сервер). При необходимости измените имя файла в поле **File name** в **R5** или **File path** (Путь к файлу) в **R6**.
4. Установите другие параметры, а затем щелкните по кнопке **OK**. Указанные параметры соответствуют следующим полям (только в **R5**, поскольку в **R6** эти параметры получают значения по умолчанию, которые могут быть изменены в дальнейшем):
 - **Create** (Создание). Возможные варианты - **Immediately** (Незамедлительно) или **Next scheduled replication** (При следующем запланированном сеансе репликации). Если база данных достаточно объемна, рекомендуется второй вариант, поскольку опция **Immediately** приостановит рабочую станцию на время осуществления репликации;
 - **Encryption** (Шифрование). При нажатии этой кнопки открывается диалоговое окно **Encryption for [заголовок базы данных]** (Шифрование базы данных, с указанием названия). В нем можно задать варианты с усиленным, средним и упрощенным шифрованием, а новая реплика базы данных будет шифроваться с помощью идентификационных данных сервера адресата;
 - **Size Limit** (Ограничение размера базы данных). Этот параметр применяется только в отношении баз данных, созданных на серверах версии 4 или в формате баз данных этой версии. Варианты связаны с введением ограничений на уровне 1,2,3 или 4 Гб, а для баз данных версий 5 и 6 (формат ODS41) - только с ограничениями используемой операционной системы;
 - **Replication Settings** (Параметры репликации). Кнопка открывает одноименное диалоговое окно, которое достаточно подробно описано в начале данной главы. Здесь можно изменить различные параметры, а затем щелкнуть по кнопке **OK**;
 - **Copy Access Control List** (Копирование списка управления доступом). При отмене этой функции новая копия базы данных будет обращаться к обновленному списку ACL, в котором для администратора и сервера оговариваются права доступа на уровне **Manager** или просто используются параметры режима по умолчанию. Наряду с другими возможностями, функция позволяет администратору просматривать структуры базы данных, доступ к которой отсутствует на уровне **Designer**. При этом администратор не получит права доступа на уровне **Designer** к реплике базы данных на сервере, но будет располагать правами доступа на уровне **Manager** к ее локальной реплике;
 - **Create full text index for searching** (Создание полнотекстового индекса для проведения поиска). При задании этого параметра для новой реплики базы данных будет незамедлительно выполнена операция полномасштабной индексации.

Формирование новой реплики на рабочей станции системы Notes

В предыдущем разделе отмечалось, что с рабочей станции можно обратиться практически к любой базе данных, хранящейся на другом сервере, и инициировать ее репликацию для третьего сервера. Для этого необходимо лишь обладать соответствующими правами доступа. Подобный подход на практике позволяет создать новую базу данных для рабочей станции системы Notes. Но в таком случае придется провести все действия на самой рабочей станции, а не удаленно. Если требуется удаленно сформировать одну или несколько реплик базы данных для рабочей станции пользователя, надо выполнить **Setup Profile** (Установка профиля). В этом случае, однако, реплики баз данных будут формироваться на всех рабочих станциях, управляемых с помощью указанного профиля.

Для применения команды **Setup Profile** при создании реплики баз данных для рабочих станций системы Notes необходимо выполнять следующие действия:

1. Откройте базу данных, которую планируется реплицировать, - она будет служить источником данных для новых реплик.
2. В открытой базе данных выполните **Copy As Link => Database Link** (Копирование в виде ссылки => Ссылка базы данных) в меню **File**.
3. Закройте исходную базу данных, обратитесь к форме **Setup Profile** (Установка профиля) в каталоге Domain Directory и перейдите в режим редактирования (**Edit mode**).
4. На вкладке **Database** (База данных) установите текстовый курсор в позиции поля **Create As new replica on user's machine** (Создание в качестве новой реплики на компьютере пользователя) и щелкните по кнопке **Paste** (Вставка). В результате на экране появится значок для ссылки базы данных.
5. Сохраните и закройте форму **Setup Profile**.

В дальнейшем каждый раз при регистрации в системе Notes пользователя, применяющего форму **Setup Profile**, локальная программа Dynamic Configuration (Динамичное конфигурирование, файл ndyncfg.exe) будет просматривать форму **Setup Profile**, определять произошедшие в ней изменения и передавать новую реплику базы данных с исходного сервера. Более подробно методика применения формы **Setup Profile** описана в главе 13.

Удаленные документы, заготовки удаления и очистка баз данных

Что же происходит с теми документами, которые исключаются из базы данных в процессе репликации? Можно предположить, что, поскольку документ больше не существует (после удаления) в реплике базы данных сервера S1, репликация должна предусматривать пересылку сервером S2 новой реплики исключенного документа на сервер S1, чтобы одинаковые реплики документа хранились на обоих серверах. Подобное случается, хотя и весьма редко, так как определенные характеристики системы Notes способствуют заметному уменьшению вероятности такого события.

Например, документ в момент удаления его пользователем не исчезает из базы данных: пропадают поля, однако заготовка удаления остается в базе. (Это соответствует так

называемому процессу быстрого удаления. Если же в базе данных инициируется мягкий вариант удаления, информационные поля не исключаются до завершения заданного временного интервала. Затем они пропадают, а документ превращается в заготовку удаления.)

При инициировании очередного сеанса репликации заготовка удаления, отвечающая последней редактировавшейся версии документа, будет реплицирована и передана на другой сервер, способствуя удалению реплики документа. Именно таким образом процесс удаления распространяется в сети.

Периодически Notes, Domino или Updall (консольная команда очистки) исключают заготовки (и, возможно, другие документы - в зависимости от заданных параметров репликации) из базы данных. Эта процедура позволяет убирать документы полностью, причем после удаления в базе данных не остается никаких признаков их присутствия.

Исключенные документы могут появляться в репликах баз данных в двух случаях: в результате разрешения той или иной конфликтной ситуации или вследствие попытки удалить заготовки до того момента, когда они будут применены для репликации.

При условии, что между сеансами репликации в одной из реплик базы данных инициируется удаление документа, а в другой производится его редактирование, существует вероятность, что отредактированная версия возобладает и при очередном сеансе репликации ранее исключенный документ вновь будет помещен в базу данных.

В соответствии с правилом наиболее частой повторяемости, если отредактированная версия документа ранее модифицировалась большее число раз (между сеансами репликации), чем исключаемая версия, отредактированный документ получит преимущество перед удаляемым при осуществлении очередной операции репликации. Сама операция удаления в данном случае будет рассматриваться в качестве операции модификации.

Согласно правилу наиболее позднего редактирования, если обе версии документа модифицировались одинаковое число раз (между сеансами репликации), но редактирование имело место после удаления, отредактированный документ также получит определенное преимущество перед исключенным в процессе выполнения очередной операции репликации.

Другой случай появления исключенного документа в базе данных возможен при попытке удаления заготовок прежде, чем они будут реплицированы и переданы в другие реплики базы данных. В этой ситуации при некоторых обстоятельствах не исключенные корректным образом реплики могут вновь оказаться в подвергшихся очистке копиях баз данных. К счастью, на практике подобные события происходят достаточно редко, поскольку журнал репликации и параметр репликации **Only replicate incoming documents saved or modified after** (Репликация только входящих документов, сохраненных или измененных после) стремятся их предотвратить.

Неисключенная версия документа, не модифицировавшегося позднее определенных дат, не может служить кандидатом для репликации. Однако в том случае, когда производится стирание журнала репликации и записи в поле **Only replicate incoming documents saved or modified after**, все такие документы становятся кандидатами для репликации. Серверу достаточно обнаружить исключенный документ всего в одной реплике, чтобы обеспечить его репликацию для других копий базы данных.

Если же в реплике редактируется неисключенный документ, отредактированная версия становится кандидатом для репликации в процессе очередного сеанса и будет передаваться в другие копии базы данных.

Итак, необходимо предварительно убедиться в том, что репликация выполняется чаще, чем процедура очистки баз данных от заготовок. На практике такая ситуация вполне тривиальна, поскольку плановая репликация должна проводиться по крайней мере один раз в неделю, тогда как исключаемые документы хранятся (в режиме по умолчанию для большей части баз данных) в течение 90 дней, прежде чем их преобразуют в кандидаты на удаление. Тем не менее в ряде случаев процедура очистки выполняется чаще, чем процедура репликации:

- если в поле Remove documents not modified in the last [x] days (Удаление документов, не модифицированных в течение последних x дней) на экране Replication Settings задается небольшое число дней, например три, а репликация производится с периодичностью, скажем, в семь дней, процедура очистки будет заметно более частой, чем процедура репликации;
- если база данных не участвует в плановой репликации в течение длительного периода времени, например вследствие установки флажка Temporarily disable replication (Временная приостановка репликации), документы окажутся исключенными и удаленными до повторной активизации функции репликации;
- если пользователь формирует локальную реплику базы данных, но в дальнейшем продолжительное время не инициирует операции репликации для сервера, документы могут быть исключены и удалены до возобновления этой операции.

Журнал репликации, поле Remove documents not modified in the last [x] days и список ACL призваны защищать систему от возникновения подобных событий. Однако при стирании журнала репликации и записи в указанном поле и наличии у пользователя, инициировавшего удаление, соответствующих прав на удаление (оговоренных в списке ACL) для данной реплики базы данных следует быть готовым к самым неожиданным результатам.

Для предотвращения несанкционированных очисток/удалений документов из базы данных до того момента, когда процесс удаления распространится на все ее реплики, придерживайтесь следующих рекомендаций:

- не устанавливайте короткие периоды очистки баз данных, имеющих реплики на других серверах. Задавайте значение в поле Remove documents not modified in the last [x] days таким образом, чтобы периодичность очистки базы данных превышала периодичность плановой репликации;
- не стирайте журнал репликации одновременно со сбросом флажка в поле Only replicate incoming documents saved or modified after без крайней необходимости. Многие сотрудники стирают эту информацию практически автоматически при возникновении каких-либо трудностей с репликациями. Следует напомнить, что отказ "от подобной привычки позволит избежать куда более серьезных проблем;
- если все-таки принято решение о стирании журнала репликации, следует стирать лишь определенные записи, а не весь журнал. Для этого выберите команду Zoom (Увеличение), а затем Remove (Удаление);
- максимально урежьте права на удаление для обычных пользователей совместно применяемых баз данных. Большая часть пользователей должна располагать правами удаления только для документов, созданных ими самими, а может быть, и этих прав для них будет слишком много. Не исключено, что самой приемлемой окажется ситуация, когда лишь редакторы или администраторы получают право удалять все документы из большей части баз данных.

Мониторинг репликации

На практике следует контролировать процесс репликации, чтобы гарантировать его корректное исполнение. Этот процесс, конечно, надежен, однако появление сбоев, приводящих к отказам при репликации, указывает на наличие реальных неполадок, например на некорректные действия самих пользователей. Сотрудники и пользователи обычно полагаются на сведения, хранящиеся в базах данных системы Notes, но, получив отказ при репликации, могут предположить, что руководствовались неверными сведениями. В результате у них начнутся проблемы, они перестанут доверять сведениям баз данных, а система Notes потеряет для них всякую привлекательность.

Сервер Domino предусматривает применение целого набора программных инструментов для постоянного информирования администратора относительно состояния процесса репликации. К этим программным инструментам относятся:

- О база данных Notes Log (Журнал системы Notes);
- О статистические данные процесса репликации;
- О мониторы процесса репликации и уведомления о событиях (Event);
- О инструменты графического мониторинга программы Domino Administrator.

База данных Notes Log

Отчеты программы Replicator информируют о результатах выполнения процесса репликации и заносятся в базу данных Notes Log. Информация в данном случае появляется на видах **Miscellaneous Events** (Дополнительные события) и **Replication Events** (События при репликации). Вид **Replication Events**, в частности, позволяет выяснить причину тех или иных событий в ходе сеанса репликации. Надо только не забывать обращаться к базе данных Notes Log, хранящейся на соответствующем компьютере и выполняющей основной объем работы. На сервере, чья программа репликации совершает необходимые действия, как раз и находится информация.

Для просмотра базы данных Notes Log можно открыть ее непосредственно или в программе Domino Administrator, где удастся отобразить все виды этой базы, воспользовавшись вкладкой **Server => Analysis** (Сервер => Анализ). Для перехода на вид **Replication Events** следует обратиться к вкладке **Replication** (Репликация).

Статистические данные процесса репликации

Сервер Domino обеспечивает сбор следующих статистических данных относительно процесса репликации: Replica.Docs.Added (Репликация, добавленные документы), Replica.Docs.Deleted (Репликация, удаленные документы), Replica.Docs.Updated (Репликация, модифицированные документы), Replica.Failed (Репликация, отказы) и Replica.Successful (Репликация, успешное завершение). На практике можно отображать статистические данные самыми различными способами. Можно применить управляющую команду Show Statistics (shst replica), вводимую на консоли сервера. В программе Domino Administrator сделать это позволяет вкладка **Server =Ф Statistics** (Сервер => Статистические данные) или база данных Statistics Reports (Отчеты постатистическим данным), к которой обращаются с помощью вкладки **Server => Analysis** (Сервер => Анализ). В базе данных Statistics Reports данные относительно репликации присутствуют в документах на видах **Statistics Reports\ Mail & Database**

(Отчеты по статистическим данным/почтовая служба и база данных) и **Statistics Reports\System** (Отчеты по статистическим данным/система).

Имеется возможность обратиться к журналу репликации (**Replication History**) соответствующей базы данных, для чего следует открыть базу и отметить **Replication History** (Журнал репликации) в меню **File**. Либо допустимо выбрать **Replication => History** (Репликация => Журнал) в окне **Database Properties** (Свойства базы данных). Обратитесь к диалоговому окну **Replication Settings** (Параметры репликации) базы данных и проверьте, что планируется реплицировать в ходе очередного сеанса репликации.

Мониторы процесса репликации и уведомления о событиях

Система формирования отчетов о статистических данных (**Statistics**) и событиях (**Events**) позволяет контролировать индивидуальные базы данных на предмет возникновения отказов при репликации. Разрешается пользоваться системой уведомлений по поводу возникших отказов в процессе репликации и взаимодействия с другими серверами (в течение специально оговариваемого временного интервала).

Такой режим может быть задан с помощью базы данных **Statistics & Events** (Статистические данные и события, файл **events4.nsf**), которая выполняет функцию базы данных конфигурации для систем сбора статистических данных и событий сервера **Domino**. Для доступа к ней служит значок **Statistics & Events** (Статистические данные и события) в **R5** или значок **Monitoring Configuration** (Мониторинг конфигурации) в **R6** на вкладке **Configuration** (Конфигурация) программы **Domino Administrator**. При этом следует создавать два документа:

- О документ мониторинга репликации (**Replication Monitor**) - позволяет программе **Event Dispatcher** (Диспетчер событий) регистрировать полученные отказы при репликации и формировать соответствующие события (**Replication event**);
- О документ уведомления о событиях (**Event Notification**) - дает возможность информировать программу **Event Dispatcher** о необходимости уведомления (тем или иным образом) администратора при возникновении событий, указанных в документе мониторинга репликации, например о типе события или о серьезности возникшей ошибки.

Администратор имеет возможность подготовить документ мониторинга репликации путем его создания вручную или в программе, которая будет направлять запросы относительно всей требующейся информации, а затем сама создаст этот документ. Для создания документа вручную следует перейти на вид **Monitors => Replication** (Мониторы => Репликация) в базе данных **Statistics & Events**, а затем выполнить **New Replication Monitor** (Новый монитор репликации) на панели **Action** (Операции) и заполнить поля, перечень которых приведен в табл. 9.4.

Таблица 9.4. Перечень полей для формы мониторинга репликации

Поле	Назначение
Вкладка Basics (Основные параметры)	
File name (Имя файла)	В это поле следует вводить имя файла для контролируемой базы данных (допускается только одно имя)
Servers (Серверы)	Поле позволяет указать несколько серверов для мониторинга всех отказов репликации. Контроль может осуществляться для любой группы серверов в домене, от одного до всех серверов

Таблица 9.4. Перечень полей для формы мониторинга репликации (окончание)

Поле	Назначение
Servers) with which the database must replicate (Серверы, для которых должна реплицироваться база данных)	Здесь задается мониторинг ошибок репликации между серверами, указанными в предшествующем поле, и любой другой группой серверов домена, от одного до всех серверов
Replication timeout; Timeout x hours (Тайм-аут репликации; временной интервал соответствует x часам)	По умолчанию в поле присутствует значение 24 часа. Разрешается изменять это значение в соответствии с имеющимися требованиями
Вкладка Other (Другие параметры)	
Event: Generate a Replication event of severity (Событие: генерация события репликации со статусом серьезной ошибки)	Для данного поля есть следующие варианты: Fatal (Фатальный отказ), Failure (Отказ), Warning (high) (Предупреждение, высокий уровень приоритета), Warning (low) (Предупреждение, низкий уровень приоритета) и Normal (Нормальный). На практике рекомендуется выбирать вариант Fatal по причинам, о которых речь пойдет в последующих разделах
Enablement: Disable this monitor (Разрешительная функция: отмена использования этого монитора)	Это поле позволяет прекратить формирование событий (без реальной отмены функции)

Примечание для администраторов системы R4

В версии 4 можно создавать только документ мониторинга репликации (Replication Monitor), а в версии 5 и 6 - также и документ уведомления о событиях (Event Notification), однако документ мониторинга репликации не формирует уведомления относительно отказов в ходе репликации, а просто фиксирует эти отказы в качестве событий с соответствующим кодом серьезности ошибки (Replica events of x severity). Для получения уведомлений о событиях следует проинформировать программу Event Dispatcher о том, каким образом их направлять с помощью документа уведомления о событиях. Тем не менее подобная проблема может возникнуть только в ранних версиях сервера Domino. Начиная с версии 5.0.1 база данных Statistics & Events по умолчанию содержит набор документов уведомления о событиях, который позволяет формировать документы о событиях (Event document) для базы данных Statistics Reports (Отчеты по статистическим данным) при возникновении событий любого типа и с любым кодом серьезности ошибки, например типа **Warning (high)** или более серьезной.

Для использования Мастера создания этого документа следует открыть тот же вид командой **Setup Wizards => Monitor** (Мастера установки => Монитор) в меню **Actions** (Операции). Мастер поможет заполнить поля, которые соответствуют полям формы, перечисленным в табл. 9.4.

При сохранении (или очередной репликации) документа мониторинга для серверов их функция **Event** (Событие) обеспечит мониторинг отказов в процессе репликации для указанной базы данных. Если по истечении временного интервала, указанного в документе мониторинга репликации, процесс репликации не завершается успешно (для двух участвующих серверов), функция **Event** будет формировать (для осуществляющего репликацию сервера) событие типа **Replica** (Реплика), а также указывать код серьезности ошибки, который ранее был задан в документе мониторинга репликации.

Это, безусловно, является хорошим признаком, однако требуется получить информацию о произошедшем событии. Следует создать документ уведомления о событиях путем перехода на вид Event Notification (Уведомление о событиях). Документ может формироваться непосредственно, например командой New Event Notification (Новое уведомление о событиях) на панели Action (Операции), или косвенным образом, с помощью соответствующего Мастера, который запускается командой Setup Wizards => Event Notification (Мастера установки => Уведомление о событиях) в меню Actions (Операции). После этого нужно заполнять поля, указанные в табл. 9.5.

Таблица 9.5. Перечень полей для формы уведомлений о событиях

Поле	Назначение
Вкладка Basics (Основные параметры)	
	В данном поле выбирается первое значение, если требуется направлять уведомление при возникновении определенных событий и известен вид формируемого для этого события сообщения. На вкладке Event (Событие) отмечается событие переключения. Второй предлагаемый вариант применяется в том случае, когда нужно уведомление о событиях определенного класса или изначально не известен вид сообщения, которое должно формироваться для такого события. При этом необходимо определить тип события и серьезности ошибки
Server(s) monitor (Контролируемые серверы)	Уведомление будет направляться в том случае, если для любой подгруппы серверов (от одного до всех серверов области), указанных в этом поле, произойдет оговоренное событие
Вкладка Event (Событие)	
Built-in/Add-in task event (Встроенное/добавленное событие)	Если флажок указан на вкладке Basics (Основные параметры), будут появляться последующие поля (кнопки)
Select Event (Выбор события)	Воспользуйтесь этой кнопкой для вывода списка сообщений, которые могут формироваться событием. Перечень может получиться объемным, поэтому в отсутствие сведений о сообщениях, которые формируются событием, следует вернуться на вкладку Basics и выбрать Any event that matches a criteria (Любое событие, соответствующее критерию)
Events can have any message (События могут сопровождаться любыми сообщениями)	Эта кнопка удобна в том случае, если обобщенное ^общение, выбранное для поля Select Events , является весьма специфическим
Events must have this text [in] the event message (События должны сопровождаться сообщением с данным текстом)	Посредством данной кнопки можно при необходимости привнести какие-либо переменные в сообщение, выбранное в поле Select Events
Criteria to match (Критерий соответствия)	При Any event that matches a criteria на вкладке Basics будут появляться нижеследующие поля

Таблица 9.5. Перечень полей для формы уведомлений о событиях (продолжение)

Поле	Назначение
Event... type (Событие... тип)	Если надо направлять уведомления о событиях любого типа, здесь указывается вариант Events can be any type (Сообщения могут соответствовать любому типу), а если о событиях только одного типа - то вариант Events must be this type (События должны соответствовать данному типу), после чего задается определенный тип событий. В данном случае, когда требуется направлять сообщения при отказе в ходе выполнения операции репликации, следует определить тип события Replica (Реплика)
Event... severity (Событие ... серьезность ошибки)	При необходимости направления уведомлений для всех уровней серьезности ошибки следует выбирать для этого поля вариант Events can be any severity (События могут соответствовать любому уровню серьезности ошибки). Если требуется направлять уведомления не для всех уровней серьезности . ошибки (эта ситуация часто используется на практике), нужно отметить вариант Events must be one of these severities (События должны соответствовать одному из данных уровней серьезности ошибки), после чего выбирать уровень серьезности ошибки, для которого направляется уведомление. В данном случае, когда требуется направлять сообщения в случае отказа при выполнении операции репликации, можно указать уровень серьезности ошибки соответствующим тому уровню, который задавался для функции Replication Monitor (Мониторинг репликации)
Event... message (Событие... сообщение)	При необходимости получать уведомления для событий и уровней серьезности ошибки; заданных в предшествующих полях, или в отсутствие информации относительно тех сообщений, которые будут формироваться для данного события, следует выбрать вариант Events can have any message (События могут сопровождаться любыми сообщениями). Если требуется получать уведомления только для событий, содержащих определенный текст в сообщениях события, нужно выбрать вариант Events must have this text [in] the event message (События должны сопровождаться сообщением с данным текстом), после чего ввести текст. В данном случае, когда надо направлять сообщения в случае отказа при выполнении операции репликации, выберите следующий вариант текста: filename.nsf has not replicated with (Файл filename.nsf не был реплицирован). Следует заменять имя «filename.nsf» именем реального файла и при необходимости использовать метки кватирования На вкладке Action (Операции) нужно определить способ уведомления и категорию разрешения: Enable/Disable/Enabled only during these times (Разрешено/отменено/разрешено только в заданном временном интервале). Список появляющихся при этом полей зависит от сделанного выбора. Ниже приводится перечень возможных способов уведомления

Таблица 9.5. Перечень полей для формы уведомлений о событиях (окончание)

Поле	Назначение
Broadcast (Широковещательное сообщение)	В этом поле указывают получателя сообщения, передаваемого в широковещательном сетевом режиме
Log to database (Регистрация в базе данных)	В поле нужно задать имя базы данных и тот сервер, на котором она хранится. По умолчанию будет происходить обращение к файлу statrp.nsf для того сервера, на котором имело место соответствующее событие
Mail (Почтовое сообщение)	В поле следует ввести адрес электронной почты для администраторов из числа тех, которые должны получить уведомление
Log to NT Event Viewer (Регистрация в базе данных Event Viewer системы NT)	Для этого поля значения отсутствуют
Pager (Пейджинговое сообщение)	В поле нужно задавать адрес электронной почты для владельца пейджеров из числа тех, которые должны получить уведомление
Run Program (Запуск программы)	В поле следует вводить имя программы, параметры управляющей команды, а также имя сервера, на котором эта программа должна исполняться
Relay to other server (Передача на другой сервер)	В этом поле нужно определить имя сервера, который принимает на себя управление
SNMP Trap (Ловушка SNMP)	В поле следует указать имя сервера SMTP
Log to Unix System Log (Регистрация в базе данных System Log системы Unix)	Для этого поля значения отсутствуют

Необходимо проявлять осторожность при определении события, для которого планируется получать уведомления. Если описать событие лишь в общих чертах, то в дальнейшем будет поступать 10,100 или даже 1000 уведомлений по поводу каждого вполне законного действия. Для уменьшения числа таких малоинформативных сообщений относительно отказов при репликации событие должно быть определено одним из следующих способов:

- выберите в качестве уровня серьезности ошибки вариант **Failure** (Отказ) и задавайте этот вариант в документе мониторинга репликации. Установите тип события - вариант **Replica** (Реплика), в качестве уровня серьезности ошибки **Failure**, а также **Events can have any messages** (События могут сопровождаться любыми сообщениями) в документе уведомления о событиях. На практике происходит очень мало событий, соответствующих вариантам **Replica** и **Failure**, поэтому число приходящих уведомлений будет относительно небольшим;
- в документе уведомления о событиях поместите запись filename.nsf has **not replicated with** (Файл filename.nsf не реплицирован с), появляющуюся одновременно с текстом сообщения (в данном случае слово «filename.nsf» должно быть заменено реальным именем файла). После этого можно воспользоваться вариантами **Events can be any type** (События могут быть любого типа) и **Events can be any severity** (События могут иметь любой уровень серьезности ошибки).

Программные инструменты для графического мониторинга

Программа Domino Administrator позволяет использовать несколько графических инструментов для того, чтобы быстро и доступно проинформировать администратора относительно состояния процесса репликации в его домене. С помощью вкладки **Replication** может быть проиллюстрирован каждый план репликации сервера и выбранная топология репликации. С помощью вкладки **Server => Monitoring** (Сервер => Мониторинг) легко контролировать текущий статус программы Replicator для заданных серверов.

План репликации исследуют путем анализа соответствующих документов соединения, к которым обращается сервер при репликации. В версии 5.0.0 не предусматривается вывод статуса репликации в соответствии с планом, но в последующих версиях эта возможность реализована. Администраторам также следует знать о том, что в версии 5.0.0, к сожалению, имеет место ошибка. Так, при задании нескольких моментов времени или временных интервалов в документе репликации (Replication document) только первый момент времени будет графически отображаться на экране и показывать характер исполнения плана репликации.

Если определить топологию репликации на основе соответствующих документов соединения (Connection document), будут показаны все соединения, которые данный сервер способен формировать сам или совместно с другими объектами при осуществлении репликации. Иногда топологию репликации для данного сервера не удастся вывести в графической форме. Это означает, что не инициирована операция **Maps** (Карты адресации). Для исправления ситуации следует ввести управляющую команду load maps с консоли сервера и добавить параметр Maps (Карты адресации) в список параметров переменной SerberTasks в файле notes.ini сервера.

И наконец, на экране **Server => Monitoring** (Сервер => Мониторинг) можно отследить текущий статус задачи Replicator (Репликатор) для заданных серверов. Различные значки используются для проверки факта нормального исполнения этой программы, прекращения ее исполнения или отсутствия реакции с ее стороны. Кроме того, могут быть получены данные относительно уровня серьезности ошибки: **Warning** (Предупреждение), **Failure** (Отказ) или **Fatal** (Фатальный отказ).

ГЛАВА 10

ЗАЩИТА ИНФОРМАЦИИ



Большинство организаций, работающих с системой Notes, рано или поздно начинают применять ее для хранения и управления информацией, которая рассматривается как секретная, конфиденциальная или имеет ценность для конкурентов. К такой информации должен иметь доступ только определенный круг людей. Специалисты компании Lotus изначально предполагали, что их продукт будет использоваться именно так, поэтому в Notes сразу были встроены разнообразные возможности для защиты данных. Средства защиты Notes/Domino настолько сильно сконцентрированы в данном программном продукте, что до конца понять систему администрирования Notes/Domino без четкого знания процедур защиты не удастся.

Для изучения системы защиты сначала необходимо разобраться, как работает сервер Domino. Это сторож информации, хранящейся в базах данных. Он должен воспринимать информацию только от тех источников (компьютеров, программ, людей), которые имеют право на внесение изменений, а предоставлять информацию лишь потребителям, имеющим доступ к ней. Система защиты Domino выполняет все названные функции.

Существуют также другие взгляды на защиту. Людям, обращающимся к серверу Domino, надо уметь идентифицировать сервер, с которым они будут работать. Тем, кто хранит локальные реплики баз данных в Notes, следует обеспечить защиту данных от несанкционированного доступа. Все пользователи обязаны защищать и подтверждать сообщения, передаваемые по электронной почте. Всем нужна защита от компьютерных вирусов и «червей», которые могут скрываться в данных системы Notes.

Сейчас, когда все больше и больше компаний стали подключаться к анархичной всемирной сети Internet, чтобы облегчить связь с потребителями, деловыми партнерами, поставщиками и всем остальным миром, вопросы обеспечения безопасности встали очень остро. Компания Lotus предусмотрела это, встроив в Notes и Domino средства обеспечения безопасности SSL и S/MIME.

В этой главе рассмотрены средства аутентификации, защита серверов Domino, защита баз данных и рабочих станций Notes. В конце главы более детально описано, как Domino и Notes используют защиту SSL.

Аутентификация

Аутентификация - это процесс идентификации другой стороны перед проведением некоторой транзакции (операции). Аутентификация является ядром системы безопасности

Domino. Если сервер не в состоянии установить личность пользователя, то степень доступа к информации не может быть установлена. Конечно, не во всех случаях серверу нужно проводить аутентификацию. Степень и тип аутентификации зависит от типа программного клиента, применяемого пользователем.

Серверы Domino и их клиенты используют четыре типа аутентификации:

- Notes proprietary (Лицензированная аутентификация Notes). Серверы Domino и клиенты Notes идентифицируют друг друга как обычно. Этот тип основывается на сертификатах и очень надежен;
- SSL (Secure Sockets Layer - уровень защищенного сокета). Необязательный тип аутентификации, который можно установить для клиентов, не использующих Notes. Как и Notes proprietary, этот тип основывается на сертификатах и очень надежен. Так можно аутентифицировать серверы Domino или сервер Domino и клиент, не работающий с Notes;
- Name and password (Имя и пароль). Также необязательный тип аутентификации, который можно установить для клиентов, не применяющих Notes. Это самый слабый тип аутентификации. Так можно аутентифицировать только пользователей, но ни в коем случае не серверы;
- None (Нет). Это не аутентификация, а, скорее, ее отсутствие. Пользователи без аутентификации остаются для сервера неизвестными. А вот сервер без аутентификации не остается для клиента неизвестным, точнее, клиенты считают, что работают именно с определенным сервером, не проверяя его подлинность. Клиенты HTTP, LDAP, NNTP, SMTP и POP по умолчанию неизвестны для сервера. Можно разрешить неизвестным клиентам пользоваться Notes. Анонимные клиенты остаются анонимными только до тех пор, пока получают доступ к серверу в объеме, разрешенном анонимному клиенту. Например, Web-клиент пытается откорректировать документ в базе данных, к которому анонимному клиенту разрешен доступ только для чтения. Чтобы получить большие права доступа к этому документу, он должен быть идентифицирован либо с помощью SSL, либо с помощью имени и пароля.

Возможные варианты аутентификации клиентов и сервера Domino приведены в табл. 10.1. Первая комбинация в каждом случае задана по умолчанию. Для примера рассмотрим первую строку. Клиент Notes может идентифицировать сервер только одним способом - способом Notes proprietary, а сервер - идентифицировать пользователя с помощью Notes proprietary или допустить его к работе без аутентификации. Notes proprietary (первый вариант выбора в третьем столбце) установлен по умолчанию.

Таблица 10.1. Параметры аутентификации

Тип клиента	Клиент аутентифицирует сервер с помощью	Сервер аутентифицирует клиент с помощью
Notes	Notes proprietary	Notes proprietary Без аутентификации
НИР, IMAP, NNTP	Без аутентификации	Без аутентификации
	SSL	Имя и пароль Без аутентификации Имя и пароль SSL

Таблица 10.1. Параметры аутентификации (окончание)

Тип клиента	Клиент аутентифицирует сервер с помощью	Сервер аутентифицирует клиент с помощью
POP3, IMAP	Без аутентификации SSL	Имя и пароль Имя и пароль SSL
SMTP, POP	Без аутентификации или SSL	Без аутентификации Имя и пароль

Принцип работы аутентификации по имени и паролю

Это самый простой тип аутентификации. Domino так идентифицирует пользователей, не применяющих Notes. Клиент передает серверу свое имя и пароль, а сервер исследует каталоги в поисках записи с таким же именем и паролем. Пароль обычно является секретным, поэтому предполагается, что объект, представляющий пароль, обозначен в записи сервера.

Достоинством данного метода (в сравнении с системами на основе сертификата) можно считать его простоту - сервер и пользователь принимают заранее установленные имя пользователя и пароль, которые впоследствии служат пользователю постоянно. К его недостаткам относятся следующие:

- О пароль на самом деле может не быть секретным. Люди вводят пароль, который легко угадать, куда-нибудь записывают его или говорят другим;
- О имя и пароль передаются от пользователя к серверу через сеть. Если они не зашифрованы, кто-нибудь может перехватить их. А если пересылать их в зашифрованном виде, то либо необходимо иметь заранее оговоренный секретный ключ шифрования, который сам способен быть альтернативой имени и пароля, либо применять систему аутентификации на основе сертификата;
- О нет защиты против программ подбора паролей;
- О сначала пользователь должен зарегистрироваться, чтобы на сервере была запись, с которой будут сравниваться имя и пароль, предоставленные пользователем.

Аутентификация на основе сертификата устраняет все названные недостатки.

Принцип работы аутентификации на основе сертификата

Аутентификации Notes proprietary и SSL являются системами на основе сертификата. Идея такой системы состоит в том, что ни одна из сторон перед операцией не знает другую, но они имеют общую дружественную сторону, которая может поручиться за них. Стороны доверяют друг другу на основании отношения доверия дружественной стороны.

В электронном виде одна сторона предоставляет другой стороне имеющийся сертификат, который можно рассматривать как рекомендательное письмо, подписанное дружественной

стороной. В сущности, сертификат говорит, что открытый ключ данного сертификата принадлежит объекту, заявленному в сертификате. Все это «подписывается» третьей стороной, которая на языке Notes называется *сертификатор (заверитель)* или *орган (авторизатор) сертификации (Certifying Authority - CA)*.

Сертификат связывает открытый ключ с именем. Если получатель сертификата доверяет подписи заверителя, то он доверяет и сути заверения - что ключ принадлежит указанному объекту. Все это делается для того, чтобы выяснить, действительно ли сторона, предоставившая сертификат, имеет открытый ключ, соответствующий ключу, который представлен в сертификате. В таком случае сторона, предъявившая сертификат, теоретически является объектом, указанным в сертификате. Идентификация прошла успешно.

Ключи шифрования: шифрование, подписи и идентификация

Возможно, предшествующее объяснение не совсем понятно, потому что не ясно, какие ключи имеются в виду. Речь идет о ключах шифрования. Как и обычные ключи, они закрывают и открывают что-либо, в данном случае - информацию. Вы берете информацию и изменяете ее, применяя к ней математические преобразования с помощью своего ключа. Скажем, вы умножаете число в поле «Заработная плата» на ключ шифрования (немного проще, чем реальные преобразования информации). Информация теперь зашифрована. Чтобы ее расшифровать, вы должны произвести обратные преобразования. В данном примере для получения исходного значения следует разделить полученные сведения на ключ.

В сущности, ключ шифрования работает так: вы шифруете информацию посредством ключа и дешифруете ее тоже с его помощью. Чтобы расшифровать данные, вам необходимо знать, каким ключом они закрыты. В противном случае вы потратите очень много времени, чтобы вычислить используемый ключ. Для шифрования применяются такие ключи, что даже на очень быстрых компьютерах процесс вычисления ключа занимает очень много времени. Даже если удастся вычислить ключ, попытка может оказаться настолько дорогой, что у человека, пытающегося угадать шифр, не хватит денег либо сама информация не будет стоить этих усилий.

Когда для шифрования и дешифрования служит один ключ, это называют *шифрованием с одним ключом*. Аутентификация основывается немного на другом типе шифрования - с двойным ключом. Как подразумевает само название метода, *шифрование с двойным ключом* требует наличия двух ключей - уникального набора из двух ключей, математически связанных друг с другом так, что один ключ может открыть только то, что было закрыто другим ключом. Это означает, что если вы шифруете информацию одним ключом, то для ее дешифрования вам нужен другой ключ.

Данная схема устраняет огромный недостаток схемы шифрования с одним ключом, который заключается в следующем: для использования одного ключа шифрования при связи друг с другом два объекта сначала должны получить копии этого ключа. Однако, когда ключ создает один объект, он передает ключ другому объекту через сеть. Во время передачи ключ может быть перехвачен злоумышленником, то есть перестанет быть секретным. Любое сообщение, зашифрованное этим ключом, в состоянии расшифровать стороннее лицо. Конечно, при передаче ключ можно зашифровать. Но чем? Другим ключом? А как две стороны получают копии этого «другого» ключа? По телефону? По электронной почте?

По почте? Ни один из способов не исключает возможности перехвата ключа во время передачи. Кроме того, это неудобные и устаревшие способы доставки. Современная компьютерная система связи предназначена для переноса битов, а не атомов.

Шифрование с двойным ключом решает данную проблему. Происходит это так. Один ключ делается открытым, а другой держится в секрете. Вы спокойно любым известным вам способом отправляете открытый ключ. Если даже третья сторона сумеет его перехватить, вам не о чем беспокоиться, ведь расшифровать сообщения можно лишь одним ключом - секретным, который находится у вас. Вторая сторона может зашифровать сообщение открытым ключом и послать вам. Третья сторона не сможет расшифровать его. На самом деле даже вторая сторона не сможет расшифровать его. Расшифровать сообщение сможете только вы с помощью вашего секретного ключа, который находится только у вас.

Но это не единственная особенность такой пары ключей. Вторая особенность состоит в том, что они позволяют идентифицировать источник сообщения и удостовериться в целостности сообщения. Рассмотрим сказанное подробнее. Секретного ключа не имеет никто, кроме вас, и вы - единственный человек, который способен расшифровать сообщение. Если вы зашифруете сообщение, воспользовавшись своим секретным ключом, и пошлете его второй стороне, то лишь вторая сторона сумеет расшифровать посланное сообщение с помощью открытого ключа. А это будет означать, что оно зашифровано и отправлено именно вами. По сути, шифрование сообщения вашим закрытым ключом можно рассматривать как вашу электронную подпись.

На самом деле, подписывая сообщение, вы не должны полностью шифровать его. Это займет очень много времени. Достаточно применить к сообщению *алгоритм хеширования* математическое преобразование, которое превращает длинное сообщение в короткую свертку. Затем вы шифруете свертку. Получатель сообщения использует такой же алгоритм хеширования для получения свертки, идентичной вашей, а потом расшифровывает вашу свертку вашим открытым ключом. Тот факт, что последовательность расшифрована, гарантирует, что она зашифрована именно вами, - и это является вашей подписью. Если две последовательности совпадают, получатель знает: после того, как вы подписали сообщение, его не изменяли.

Как вторая сторона получает копию вашего открытого ключа? Вы его просто пересылаете. Если у вас долгосрочные отношения, то, возможно, вы отослали копию ключа уже очень давно и вторая сторона хранит ее. А если это ваш первый контакт, то допускается посылать открытый ключ в самом тексте сообщения. Таково третье преимущество шифрования с двойным ключом.

Рассмотрим его подробнее. Вы приняли сообщение от незнакомца. Сообщение подписано им, но оно также содержит открытый ключ. Таким образом, можно расшифровать подпись и определить, что сообщение действительно принадлежит этому незнакомцу. Имя незнакомца - Джордж Буш. Великолепно! Сообщение от президента!

Однако стоп! Откуда вы знаете, что сообщение действительно от президента? На основании чего вы сделали такой вывод? Пару ключей может сгенерировать кто угодно. Алгоритм генерации ключей является открытым, а программы свободно распространяются в Internet.

Теперь предположим, что вы и я имеем определенные взаимоотношения: мы знакомы еще с детского сада или с колледжа (что, собственно, одно и то же). В этом случае я могу предоставить вам свой открытый ключ на дискете, скажем при очередной встрече в теннисном клубе. В этом ключе вы уже не будете сомневаться. Отлично! А как насчет тех

многочисленных незнакомцев по всему миру, с которыми вы никогда не встречались, кроме как по электронной почте? Как удостовериться, что сообщение, которое должно быть от Джорджа Буша, на самом деле от Джорджа Буша, а не от «Джорджа Буша» по имени Роб Кирклэнд? Вот здесь вступают в силу сертификаты.

Если мы с вами договоримся, что какая-то третья сторона заслуживает доверия, то алгоритм наших действий может быть приблизительно таким: я генерирую пару ключей и отправляю открытый ключ третьей стороне. Она убеждается, что отправленный мною открытый ключ действительно принадлежит Робу Кирклэнду. Третья сторона создает сертификат с моим именем, открытым ключом, а также определенным сроком действия. Третья сторона подписывает сертификат, добавляет свой открытый ключ и отправляет все это мне. Одновременно вы можете сделать то же самое. Или - если вы не хотите подобных трудностей - просто возьмите копию открытого ключа третьей доверенной стороны.

Теперь, отправляя сообщение, я добавляю к нему свой сертификат. Можно использовать открытый ключ третьей, доверенной, стороны для расшифровки подписи. Вы доверяете ключу - у вас есть его копия. Поэтому вы идентифицируете доверенную сторону. Вы сравниваете хеш-последовательности, которые получились в результате генерации и дешифрования. Они одинаковые. Значит, ни имя, ни ключ не могли быть изменены после их подписания доверенной стороной. Теперь у вас есть заверение третьей стороны (заверителя) в том, что открытый ключ, указанный в сертификате, принадлежит Робу Кирклэнду. Допустимо зашифровать некоторый объем информации с помощью моего открытого ключа, отправить мне, попросить расшифровать его и доложить о результатах. Если я возвращаю ту же информацию, которую вы зашифровали, вы знаете, что я, некоторый анонимный отправитель потока битов по электрическим проводам, на самом деле Роб Кирклэнд. Идентификация прошла успешно.

Еще одна деталь, которую следует иметь в виду. Чтобы описанный механизм работал надлежащим образом и обеспечивал такую же степень защиты (чтобы его было так же сложно расшифровать), как и одиночный ключ, открытый и закрытый ключи должны быть гораздо длиннее одиночного ключа - от 768 до 2048 бит, в то время как одиночный ключ может составлять порядка 56 разрядов. Разница состоит в том, что одиночный ключ основывается на одном большом простом числе, а двойной строится на базе двух больших простых чисел. В результате компьютеру потребуется гораздо больше времени, чтобы зашифровать и расшифровать информацию с помощью открытого и закрытого ключа, чем в случае одиночного ключа.

По этой причине системами аутентификации с двойным ключом обычно пользуются на начальном этапе аутентификации. Но потом одна из сторон генерирует случайный ключ шифрования (называемый сеансовым ключом, поскольку в конце сеанса он анулируется) и посылает его, зашифровав посредством открытого ключа получателя. Теперь обе стороны имеют ключ, который во время передачи не подвергается риску перехвата. При необходимости для передачи последующих сообщений они могут применять менее длинные ключи. Для подписи сообщений стороны все же используют закрытые ключи.

Так работает шифрование почтовых сообщений. Отправитель генерирует ключ и шифрует им сообщение. Затем он шифрует ключ открытым ключом получателя, прикрепляет его к сообщению и отправляет. Получатель расшифровывает сеансовый ключ своим закрытым ключом и с помощью сеансового ключа расшифровывает само сообщение.

И последнее. Как решить, доверять ли третьей стороне? Только вы сами можете сделать выбор. Все зависит от того, что представляет собой третья сторона.

В системе аутентификации Notes proprietary заверителем выступает ваша собственная организация¹. Это самый простой случай. Организация сертифицирует ваш открытый ключ. Когда кто-нибудь предоставляет вам свой сертификат, подписанный тем же заверителем, вы доверяете подписи и, следовательно, доверяете сертификату. В Notes это делается автоматически. В таком случае ни вы, ни я не можем ничего возразить.

В открытых системах, представленных стандартом SSL, органом сертификации (CA) может быть ваша организация, доверенная третья сторона или сторонняя компания, сертифицирующая открытые ключи. В этой ситуации существует две меры доверия:

- О целостность открытых ключей, применяемых для подписи сертификатов;
- О процедуры, используемые CA для идентификации объектов, которым выдаются сертификаты, и для аннулирования сомнительных ключей.

От названных факторов зависит целостность открытого и закрытого ключей. Во-первых, закрытые ключи CA должны быть всячески защищены от воров, несанкционированного использования, утери и других неприятностей. Если, например, ключ CA украден, то сертификатам, подписанным этим ключом, доверять уже нельзя, поскольку они могут быть подписаны краденой копией.

Во-вторых, авторизатор CA должен стараться не выдавать сертификаты мошенникам. Если CA выдал сертификат Робу Кирклэнду, который говорит, что прикрепленный ключ принадлежит Джорджу Бушу, то вызывает сомнение достоверность любого сертификата, подписанного данным CA. Кроме того, у CA должны быть процедуры аннулирования сертификатов, подписанных этим органом и вызвавших сомнения.

Обычно коммерческие CA, такие как Verisign (www.verisign.com). EnTrust (www.entrust.com) и Thawte (www.thawte.com) публикуют свои процедуры выдачи сертификатов. Они также предлагают сертификаты, предоставляющие различные степени заверения. Разумно платить за ту степень доверия, которая вам подходит. Такие CA выдают различные сертификаты для разных типов объектов за разную плату. Вы получаете один сертификат для Web-сервера, другой - для разработчиков и третий - для индивидуальных пользователей.

Допустим, сертификаты, которые можно получить для Web-сервера, имеют тип X и Y. Пусть сертификат типа X основывается на письменном заверении, что ваш сервер принадлежит вашей компании. С другой стороны, тип Y базируется на том, что вы предъявляете подписанное корпоративное решение, определенное обязательство, стоящее в заголовке. В данном случае требуется больше подтверждений достоверности и это стоит дороже, но предъявляются более весомые доказательства подлинности вашего сертификата. Для некоторых целей, например для заказа лимонада по электронной почте, может быть достаточно сертификата класса X. Но при расчетах с банками потребуются сертификат класса Y.

Все, что сейчас говорилось, имеет целью объяснить основные принципы работы схемы аутентификации на основе сертификатов. Чтобы узнать об этом больше, стоит обратиться к лучшему источнику информации о системах электронной криптографии - к Web-сайту RSA Data Security Incorporated (www.rsa.com). RSA - обладатель патента (закончившегося в 2000 г.) на систему шифрования с двойным ключом, описанную выше. Криптосистема RSA образует основу почти всех коммерческих систем защиты информации с двойным ключом, существующих на сегодняшний день, в том числе Notes proprietary, SSL и S/MIME. Ответы на наиболее распространенные вопросы (FAQ) компании RSA Laboratories можно прочитать в Internet (www.rsa.com/rsalabs/faq) или загрузить оттуда все, что требуется знать не только о RSA, но и о любой другой открытой криптографической системе, известной в наши дни.

¹ Как логическое понятие иерархической системы Notes, но не как конкретная компания. - *Прим. ред.*

Принцип работы системы Notes proprietary

В целом система Notes proprietary работает так, как описано в предыдущем разделе. В частности, все серверы и пользователи Notes входят в одну организацию с именем /Имяорганизации, которая представлена одним маленьким, на первый взгляд ничем не интересным файлом Organization Certifier ID (Идентификационные данные сертификатора или заверителя организации). По умолчанию этот файл называется cert.id. Он защищен паролем и включает в себя следующие элементы:

- О имя организации (может быть на нескольких языках);
- О открытый и закрытый ключи организации;
- О самоподписанный сертификат (выданный организацией самой себе) в двух версиях: североамериканской и международной (международная версия учитывает экспортные законы США);
- О срок действия сертификатов. По умолчанию составляет 100 лет со дня его выдачи. В версии R5 и R6 можно изменить и повторно сертифицировать идентификационные данные заверителя организации. В таком случае по умолчанию срок действия нового сертификата равен всего двум годам (думаю, что это получилось неумышленно и будет устранено в последующих версиях);
- О ключи шифрования (необязательный параметр);
- О комментарии (необязательный параметр).

Доступ в файл идентификации (файл идентификационных данных) ограничен паролем. Можно еще сильнее защитить этот файл, установив на доступ к нему несколько паролей. Как и все ID-файлы, он защищен от подбора пароля с помощью ограниченной временной задержки между неудачными попытками ввода пароля. И наконец, имеется средство защиты от программ подбора паролей, которое последовательно генерирует все возможные комбинации, чтобы подобрать правильный пароль. Идея метода состоит в том, что очень сложно написать программу, подставляющую множество вариантов паролей скрытно от пользователя.

При регистрации организационной единицы, сервера или лица, имеющего ID-файл организации, программа Domino Administrator генерирует ID-файл для нового объекта, а также открытый и закрытый ключи. Она создает сертификат, подписанный закрытым ключом заверителя, и помещает его вместе с копией собственного сертификата заверителя в новый ID-файл.

Если вы зарегистрировали новую организационную единицу (OU первого уровня, или OU1), она будет иметь имя /имя_ОШ/имя_организации. При последующем*использовании этого идентификатора заверителя организационной единицы для создания идентификаторов низшего уровня (других OU, серверов или лиц) программа Domino Administrator с помощью закрытого ключа заверителя подписывает сертификат нового объекта. Она помещает новый сертификат в новый ID-файл вместе с копиями сертификатов OU и сертификата исходного заверителя организации.

Особенность здесь в том, что ID-файл объекта (лица, сервера или OU) содержит не только собственный сертификат, подписанный родительским заверителем, но и все сертификаты его предков. Во время аутентификации пользователь или сервер отправляет другому объекту копии всех сертификатов данного ID-файла. Этот объект сравнивает их с сертификатами своего ID-файла и может доверять любому сертификату, который происходит от любого его родительского заверителя. Например, сервер S1 (рис. 10.1) доверяет

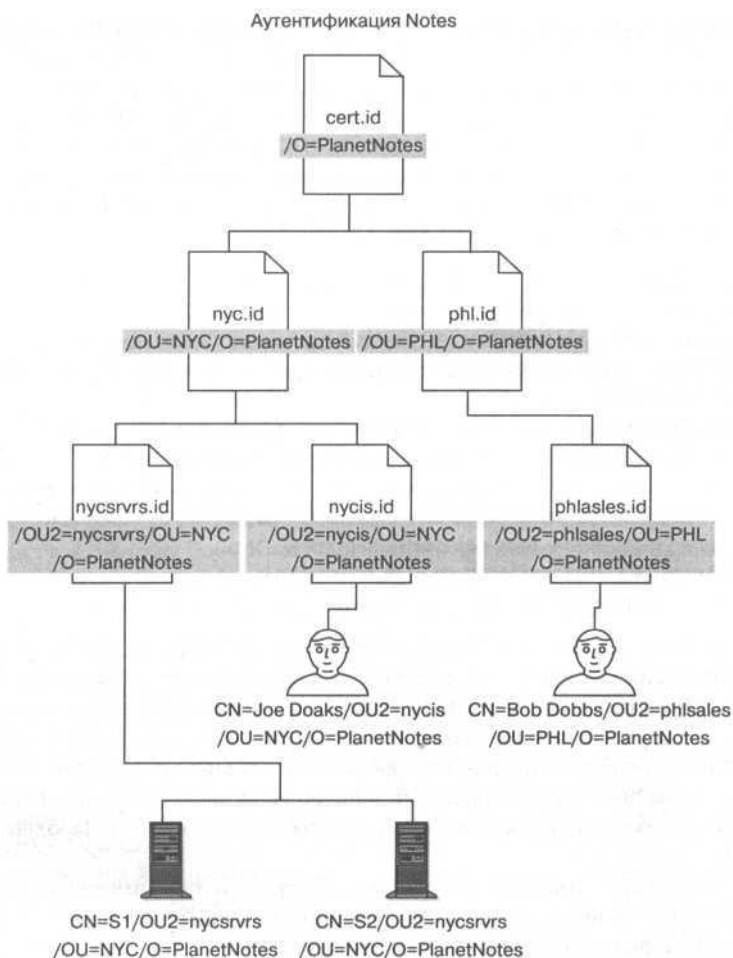


Рис. 10.1. Серверы S1 и S2 могут доверять друг другу, поскольку они оба происходят от nycsrvrs, S1 и Joe Doaks - так как оба они потомки NYC, а S1 и Bob Dobbs - потомки PlanetNotes

открытым ключам сервера S2 и пользователей U1 и U2, поскольку их ключи заверены потомками одного и того же родительского заверителя.

Принцип кросс-сертификации Notes

В системе аутентификации Notes есть одно замечательное свойство: два объекта, имеющие дочерние сертификаты от одного и того же заверителя, доверяют этим сертификатам безоговорочно. Однако, если два объекта принадлежат различным организациям, то такая схема уже не работает. Поскольку они не могут быть потомками одного и того же заверителя данной организации, их сертификаты друг для друга уже не являются достоверными. Им требуется другой способ проверки подлинности.

Способ состоит в следующем. Каждый объект издает специальный сертификат (мы назвали его кросс-сертификатом) в пользу другого объекта. Для аутентификации объект должен найти подписанный доверенным объектом сертификат, заверяющий имя другого объекта, и открытый и закрытый ключи. В кросс-сертификате указано именно это. Однако такой сертификат не передается в ID-файле в процессе аутентификации, а хранится в собственном каталоге проверяющей стороны. Когда возникает необходимость в аутентификации объекта, вторая сторона уже имеет сертификат в пользу данного объекта - кросс-сертификат - и на основании этого аутентификация проходит успешно.

Кросс-сертификаты замечательны тем, что их могут формировать аутентифицирующая сторона (сервер или пользователь) и ее потомки. Поскольку аутентифицирующая сторона доверяет своим предкам, она будет доверять и сгенерированным ими сертификатам. Кроме того, создатель кросс-сертификата вправе сформировать его в пользу (то есть для исключительного и монопольного применения) другой аутентифицирующей стороны (сервера или пользователя) или в пользу любого из ее потомков. Поскольку вторая сторона в состоянии отследить происхождение кросс-сертификата вплоть до объекта, для которого предназначен сертификат, этой стороне можно доверять.

Подведем итоги: я или любой мой предок можем создать сертификат для вас или любого вашего предка. На основании такого сертификата я могу аутентифицировать вас. Аналогично, если вы или любой ваш предок формируете сертификат для меня или любого моего предка, то можно аутентифицировать меня. Отлично, раз мы способны аутентифицировать друг друга, давайте работать!

В описанном мною случае очень важно, что для успешных взаимных операций вы должны аутентифицировать меня, а я - вас. Если хоть один из нас аутентифицирует другого, можно действовать. Когда хотя бы один из нас создает сертификат в пользу другого, мы оба в состоянии аутентифицировать друг друга. Я или мой предок должны сформировать сертификат для вас или вашего предка, а вы или ваш предок - для меня или моего предка.

Остался только один вопрос: на каком уровне в своей организации мне следует делать кросс-сертификат? И для какого уровня в вашей организации? Общее правило заключается в том, что создатель и получатель сертификата должны быть в иерархии как можно ниже - в соответствии с целями кросс-сертификации. Другими словами, если для ваших целей достаточно кросс-сертификации серверов, не нужно сертифицировать OU этих серверов или организации.

Правила кросс-сертификации на заданном уровне:

- если сервер или пользователь создает кросс-сертификат, только этот объект будет ему доверять; #
- когда кросс-сертификат формируется организацией или заверителем организационной единицы OU, то все дочерние единицы доверяют данному кросс-сертификату, поскольку они доверяют подписи издающего органа;
- если кросс-сертификат предназначен для сервера или пользователя, то с его помощью можно аутентифицировать только эти объекты;
- если кросс-сертификат создается для организации или заверителя (сертификатора) OU, то с его помощью можно аутентифицировать все дочерние организационные единицы, поскольку создатель сертификата доверяет сертификатам, созданным организацией-получателем или OU-получателем, а также их дочерним единицам. Если сам создатель является организацией или OU, то все его дочерние организационные единицы будут доверять сертификатам, созданным организацией-получателем или OU-получателем, а также их дочерним единицам.

Когда понятны названные правила, нетрудно в любой ситуации и для любых обстоятельств правильно указать, на каком уровне необходимо создавать кросс-сертификат и для какого уровня организации-получателя этот сертификат предназначен. Рассмотрим несколько примеров.

Пусть две организации намерены переписываться по электронной почте. Им следует аутентифицировать два сервера и маршрутизировать через них почтовые сообщения. В пределах указанных организаций достаточно аутентифицировать только серверы. Значит, надо, чтобы серверы создали кросс-сертификаты друг для друга. Так как нет необходимости сертифицировать ни один из вышележащих уровней иерархии, это и не делается.

Теперь предположим, что Joe Doaks/PlanetNotes должен взаимно распознаваться всеми серверами в /Servers/Stillwater. Больше никому в /PlanetNotes не нужно работать с серверами Stillwater, а в /Stillwater никому не нужно обращаться к серверам PlanetNotes. Таким образом, Joe Doaks следует создать кросс-сертификат для /Servers/Stillwater, а /Servers/Stillwater - для Joe Doaks/PlanetNotes. Joe будет доверять сертификатам, сформированным /Servers/Stillwater, а следовательно - Osprey/Servers/Stillwater и Kestrel/Servers/Stillwater. Названные серверы соответственно доверяют сертификатам, созданным /Servers/Stillwater, и на этом основании могут доверять Joe. Но они не должны доверять Bob Dobbs/PlanetNotes, поскольку от его имени нет достоверных сертификатов. Аналогично Bob Dobbs не доверяет этим серверам по той же причине; то, что Joe создал сертификат, не имеет значения, потому что Bob не является дочерним объектом по отношению к Joe.

И наконец, предположим, что PlanetNotes и Stillwater объединились. В этом случае нужно, чтобы все пользователи и серверы одной организации могли идентифицировать пользователей и серверы другой организации. /PlanetNotes подготавливает кросс-сертификат для /Stillwater и наоборот. Теперь все объекты в каждой организации имеют основание для аутентификации любого объекта в другой организации.

Если все сказанное понятно, осталось только научиться создавать кросс-сертификаты. Существует пять способов:

- О по электронной почте. Предполагаемый получатель отправляет по электронной почте безопасную копию своего ID-файла кому-нибудь, кто сможет создать для него кросс-сертификат. Безопасная копия ID-файла содержит точное имя получателя и открытый ключ, то есть минимальную информацию для создания сертификата. Сертификатор берет эту информацию, создает сертификат и, поскольку ему больше не нужен безопасный ID-файл, уничтожает его;
- О через курьера. Единственное отличие данного метода состоит в том, что безопасный ID-файл копируется на дискету и передается представителю другой организации через курьера;
- О по телефону. Администраторы каждой организации связываются по телефону и точно, без ошибок, диктуют друг другу имена и открытые ключи получателей сертификатов;
- О из персонального документа. Если есть доступ к каталогу Domino, в котором хранятся персональные документы (Person document) объектов другой организации Notes, можно подготовить кросс-сертификат на основании информации открытых ключей, содержащихся в персональном документе сотрудника;
- О по требованию. Иногда Notes не может аутентифицировать объект (пользователя или сервер) другой организации. Когда такое происходит, Notes выводит диалоговое окно **Create Cross Certificate** (Создать кросс-сертификат), в котором предлагается создать кросс-сертификат для этого объекта. Если есть абсолютная уверенность, что

он/она именно тот, за кого себя выдает, можно сформировать кросс-сертификат для него/нее, просто нажав Yes (Да) или Advanced (Дополнительно). Если же возникают сомнения в достоверности объекта, нажмите No (Нет).

Из всех перечисленных методов чаще всего используются «по электронной почте» и «по требованию», как самые простые. К методу «по телефону» прибегают реже, потому что необходимо вводить информацию вручную и к тому же многие точно не знают, какой ключ надо диктовать (совет: нужен ключ, указанный в поле Primary Key (Основной ключ) на вкладке Basics (Основные параметры) в диалоговом окне идентификационных данных).

Кросс-сертификация по электронной почте

Для кросс-сертификации по электронной почте вы инициируете операцию, отправляя по электронной почте безопасный ID-файл сертифицируемого объекта представителю другой организации, который способен создать требуемый сертификат. Для формирования электронного сообщения:

1. Выберите File => Tools => User ID (Файл => Программные инструменты => Идентификационные данные пользователя) и введите пароль. Появится ваш ID-файл.
2. Задайте вариант Certificates (Сертификаты), затем Request Cross Certificate (Запросить кросс-сертификат). Отобразится диалоговое окно Choose ID by Cross-Certified (Выберите идентификационные данные для кросс-сертификации).
3. Отметьте сертификат заверителя пользователя, сервера, организации или OU и щелкните по Open (Открыть). Откроется окно Mail Cross Certificate Request (Отправить почтовый запрос на кросс-сертификат).
4. Введите адрес электронной почты объекта, который создаст кросс-сертификат, например адрес администратора другой организации. Можно отметить адрес в каталоге, щелкнув по Address (Адрес), или добавить текст в поле Subject (Тема). По окончании нажмите на Send (Отправить). Закройте диалоговое окно идентификационных данных пользователя.

Если получено такое сообщение, можно создать кросс-сертификат, открыв сообщение и выбрав Actions => Cross Certify Attached ID File (Операции => Кросс-сертификация вложенного ID-файла). Открывается диалоговое окно Choose Certifier ID (Выбрать файл идентификационных данных сертифицируемого объекта), где нужно указать ID-файл объекта, создающего кросс-сертификат. Это может быть ваш ID-файл, ID-файл сервера, организации или заверителя OU вашей организации. Выберите Open и введите пароль сертифицирующего ID-файла. Появится окно Issue Cross Certificate (Выдать кросс-сертификат - рис. 10.2. Можно заполнить поля, как указано в табл. 10.2, и затем щелкнуть по Cross Certify (Сертифицировать).

Таблица 10.2. Поля диалогового окна Issue Cross Certificate

Поле	Описание
Certifier (Сертификатор)	Щелкните по этой кнопке, если неверно выбран ID заверителя (сертификатора), и укажите нужный файл идентификационных данных
Server (Сервер)	» Задайте каталог или адресную книгу, где будет храниться сформированный кросс-сертификат. Если вы создаете сертификат от своего имени (используя ваш собственный ID-файл), выберите Local (Локально), а если нет - то имя сервера в домене Notes заверителя

Таблица 10.2. Поля диалогового окна **Issue Cross Certificate** (окончание)

Subject name (Имя объекта)	Здесь нужно указать получателя сертификата. Это может быть объект, которому принадлежит безопасный ID-файл, или любой из его родительских объектов. Например, вы получили безопасный ID-файл от Joe Doaks/MarshGreek/Stillwater. Вы можете сформировать сертификат для Joe Doaks/MarshGreek/Stillwater или для /Stillwater
Subject alternate name list (Список альтернативных имен объекта)	Это поле нельзя редактировать. Оно показывает альтернативные имена объекта. Кросс-сертификат будет создан для объекта под любым из указанных имен
Expiration date (Срок действия)	По умолчанию равен 10 годам со дня создания; данный срок можно изменить

После щелчка по кнопке **Cross Certify** клиент Notes (или программа Domino Administrator) создает кросс-сертификат и сохраняет его в каталоге Domino на указанном сервере или в персональной адресной книге, если в поле **Server** указано **Local**.

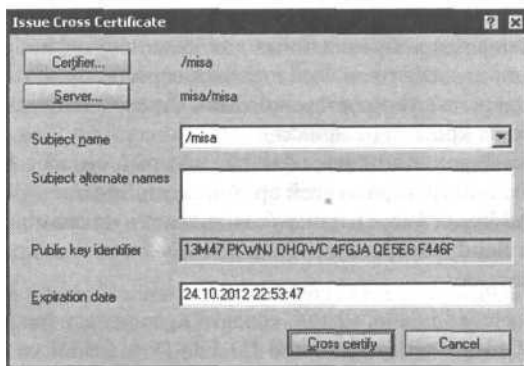


Рис. 10.2. Данное диалоговое окно позволяет выбрать объект, создающий кросс-сертификат, и сертифицируемый объект

Кросс-сертификация через курьера

#

Под словом «курьер» здесь подразумевается физическое лицо, а не электронное средство. Сторона, запрашивающая кросс-сертификат, доставляет сертифицируемый безопасный ID-файл на дискете. Если вы представляете сертифицируемую сторону, то вы инициируете операцию, формируя безопасный ID-файл из своего ID-файла. Для этого необходимо:

1. Если вы запрашиваете кросс-сертификат для себя, выберите **File => Tools => User ID** и введите пароль. Если же нужен сертификат для заверителя сервера, организации или OU, откройте вкладку **Configuration** в окне Domino Administrator и выберите **Tools => Certification => ID Properties** (Программные инструменты => Сертификация => Свойства файла идентификационных данных) или выполните **ID Properties Configuration** в меню **Certification => ID Properties** (Сертификация => Свойства файла идентификационных данных). Затем выберите ID-файл и введите пароль.

2. Укажите **More Options** (Дополнительные параметры), затем **Create Safe Copy** (Создать безопасную копию). Появится диалоговое окно **Enter Safe Copy ID File Name** (Введите имя безопасной копии ID-файла).
3. Выберите каталог, в котором будет создана безопасная копия (например, A:\). Задайте имя файла или оставьте установленное по умолчанию (safe.id) и щелкните по **Save** (Сохранить).
4. Отправьте безопасную копию в другую организацию сотруднику, который выдаст кросс-сертификат.

Если получена дискета, содержащая безопасную копию сертифицируемого ID-файла, сделайте следующее:

1. Вставьте дискету в устройство чтения рабочей станции. Запустите Domino Administrator, перейдите на вкладку **Configuration** и выберите **Tools => Certification => Cross Certify** (Программные инструменты => Сертификация => Сертифицировать) или **Configuration => Certification => Cross Certify** (Конфигурация => Сертификация => Сертифицировать).
2. Откроется диалоговое окно **Choose Certifier ID**. Здесь следует указать ID-файл объекта (пользователя, сервера, организации или организационной единицы), который создаст кросс-сертификат. Многие делают ошибку и вводят в этом окне безопасный ID-файл получателя. Прочтите имя окна. В нем ведь написано, какой ID-файл необходимо выбрать - это ID-файл сертифицирующего, а не сертифицируемого объекта. Нажмите на **Open**. Введите пароль выбранного ID-файла.
3. На экране откроется диалоговое окно **Choose ID to be Certified** (Выберите сертифицируемый файл идентификационных данных). Теперь укажите безопасный ID-файл и щелкните по **Open**.
4. Появится диалоговое окно **Issue Cross Certificate**. Заполните поля, как указано в табл. 10.2, и щелкните по **Cross Certify**.

Клиент Notes (или программа Domino Administrator) создает кросс-сертификат и сохраняет его в каталоге Domino на указанном сервере или в персональной адресной книге, если в поле **Server** установлено **Local**.

Кросс-сертификация по телефону

Для кросс-сертификации по телефону необходимо следующее:

1. Администратор, запрашивающий кросс-сертификацию, открывает ID-файл сертифицируемого объекта (пользователя, сервера или организационной единицы).
2. Администратор, создающий кросс-сертификат, переходит на вкладку **Configuration** в окне Domino Administrator и выбирает **Tools => Certification => Cross Certify Key** (Программные инструменты => Сертификация => Сертифицировать ключ). Открывается окно **Choose Certifier ID**. Администратор выбирает сертифицирующий ID-файл, щелкает по **Open** и вводит пароль выбранного файла. Появляется окно **Issue Cross Certificate**.
3. Сертифицирующий администратор может изменить поля **Certifier**, **Server** и **Expiration**
 - » **Date** (см. табл. 10.2). Поля **Subject Name** и **Public Key** заполняются со слов запрашивающего администратора по телефону.
4. Запрашивающий администратор диктует имя объекта, записанное в поле **Names** на вкладке **Basics** диалогового окна **User ID**. Сертифицирующий администратор вводит информацию в поле **Subject Name**.

5. Запрашивающий администратор диктует открытый ключ объекта, записанный в поле **Primary Key** на вкладке **Basics** диалогового окна **User ID**. Сертифицирующий администратор вводит эту информацию в поле **Public Key**.
6. Запрашивающий администратор закрывает окно **User ID**. Сертифицирующий администратор щелкает по кнопке **Cross Certify**. Клиент Notes генерирует кросс-сертификат.
7. Стороны могут поменяться ролями и повторить процесс.

Кросс-сертификация из персонального документа

Если есть доступ к персональному документу пользователя, для которого нужно создать кросс-сертификат (данный метод не годится для серверов и заверителей), можно открыть этот документ и указать **Actions => Create Cross Certificate** (Операции => Создать кросс-сертификат). Если сертифицируемый пользователь имеет североамериканскую лицензию, вас предупредят, что можно выбрать североамериканский или международный ключ. Появится диалоговое окно **Issue Cross Certificate**. Заполните необходимые поля (см. табл. 10.2). По умолчанию в качестве заверителя указывается ваш ID-файл. В качестве сервера по умолчанию указана ваша адресная книга. Щелкните по кнопке **Cross Certify**. Клиент Notes сгенерирует кросс-сертификат.

Кросс-сертификация по требованию

Администратор одной организации в качестве пользователя пытается аутентифицировать сервер другой организации. В процессе аутентификации сервер отправляет администратору сертификаты. Если у администратора еще нет сертификатов этого сервера в адресной книге, Notes открывает диалоговое окно **Create Cross Certificate**. В нем предлагается создать требуемый кросс-сертификат (рис. 10.3). Notes может сформировать кросс-сертификат, поскольку при попытке аутентификации сервер отправил свое имя и открытый ключ. Данный метод работает только для пользователей. Сервер на другом конце тоже имеет открытый ключ и имя пользователя, но не может принять решения о выдаче

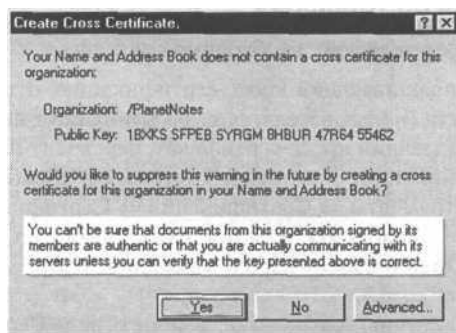


Рис. 10.3. Если клиент Notes не в состоянии аутентифицировать сервер или подпись, открывается диалоговое окно, в котором предлагается создать кросс-сертификат. Подпись может быть в сообщении, документе или элементе проектирования базы данных

сертификата, поскольку он - всего лишь компьютер. Поэтому он просто отказывает в аутентификации.

В указанном окне выведено следующее сообщение: «Следует ли создать в адресной книге кросс-сертификат для этой организации, чтобы больше не выводить данное предупреждение?» (см. рис. 10.3). Администратор может выбрать **Yes** (Да), **No** (Нет) или **Advanced** (Дополнительно).

Если администратор щелкнет по **Yes**, он создаст кросс-сертификат для организации, которой принадлежит сервер, а не для самого сервера. Кросс-сертификат сохраняется в персональной адресной книге администратора. Если администратор хочет создать кросс-сертификат для всей организации, то все в порядке. Но если он намерен предоставить кросс-сертификат только для сервера или от имени свой организации, необходимо выбрать **Advanced**.

Если администратор щелкнет по **No**, появится сообщение, в котором запрашивается подтверждение на отказ в выдаче кросс-сертификата и предлагается соединение с сервером без аутентификации. Если теперь администратор щелкнет по **Yes**, то сервер аутентифицируется и администратор сможет работать с ним, но лишь в текущем сеансе. Когда в следующий раз он попытается соединиться с данным сервером, ему придется повторить все описанные выше операции.

Если администратор выбирает **No**, то клиент Notes отказывает в установлении связи с сервером. Если администратор отмечает **Yes** и в первом, и во втором случае, а сервер не может аутентифицировать пользователя, то сервер отказывает в установлении связи с ним.

Указав **Advanced**, администратор открывает стандартное диалоговое окно **Issue Cross Certificate** (см. рис. 10.2). Здесь он может изменить следующие значения:

- О объект (он сам, сервер, заверитель организации или OU), создающий сертификат;
- О объект (сервер или любой из его родительских заверителей), которому выдается кросс-сертификат;
- О сервер, на котором первоначально будет храниться кросс-сертификат;
- О срок действия сертификата.

Значения полей диалогового окна **Issue Cross Certificate** приведены в табл. 10.2.

Принцип работы аутентификации SSL

В то время как основное назначение аутентификации Notes заключается в том, чтобы правильно идентифицировать каждую взаимодействующую сторону, для SSL это только второстепенная цель. Основная задача защиты SSL - предоставить двум сторонам закрытую связь через сеть общего пользования. Соответственно сеанс SSL отличается от Сеанса Notes. Он начинается с запроса сеанса клиентом. При этом клиент связывается с сервером через SSL-порт. Сервер отправляет клиенту сертификат и предпочитаемые варианты шифров - поддерживаемые сервером типы шифрования.

Клиент принимает сертификат или утверждает его, определяя возможность доверять подписавшему объекту. Если клиент не может утвердить сертификат, он имеет право отменить сеанс или отложить утверждение. Если же клиент принимает сертификат без утверждения, он, по сути, не нуждается в аутентификации сервера. Сервер инициирует второй этап аутентификации и сообщает, что у него есть соответствующий закрытый ключ, что само по себе не подтверждает аутентификацию.

Клиент генерирует главный ключ, шифрует его открытым ключом сервера (взятым из сертификата) и отправляет серверу. Сервер расшифровывает главный ключ, аутентифицирует

(подписывает) им сообщение и пересылает сообщение клиенту. Фактически сервер способен уже сейчас завершить свою аутентификацию клиентом, то есть он подтверждает, что имеет закрытый ключ, который соответствует открытому ключу, предъявленному в сертификате. С этого момента все сообщения, передаваемые во время сеанса, шифруются и подписываются с помощью ключа, полученного из главного ключа шифрования.

Следующий шаг, аутентификация клиента, производится на выбор сервера. Серверу может быть безразлично, что собой представляет клиент. В таком случае начинается сеанс. Если серверу необходимо идентифицировать клиента и определить его права на доступ, он может либо принять только имя и пароль, предоставленные клиентом, либо потребовать сертификат. При этом сервер отправляет клиенту запрос, клиент подписывает его и возвращает вместе с сертификатом. Сервер устанавливает подлинность сертификата и с помощью открытого ключа проверяет подпись клиента.

В целом для использования SSL объект (сервер или клиент) должен сгенерировать пару ключей и предъявить неподписанный сертификат (содержащий имя объекта и открытый ключ) СА для сертификации. Это можно сделать многими способами, но любой из них обычно подразумевает фазу предоставления информации для авторизатора СА, то есть заполнение стандартизированной формы на Web-сайте авторизатора СА. Авторизатор (заверитель) СА подписывает сертификат и возвращает его объекту по электронной почте или добавляет его на свой сайт, чтобы объект загрузил его самостоятельно. Если сертифицируемым объектом является сервер Domino, он забирает сертификат и вставляет его в *ключевой файл* (filename.kyr), который является аналогом ID-файла Notes. Если сертификат выдается определенному пользователю, то он может храниться во многих местах - в одном или нескольких Web-браузерах, почтовой программе или, если человек является пользователем Notes, в ID-файле среди других сертификатов.

Как и сертификат Notes, сертификат SSL содержит имя объекта, копию открытого ключа и срок действия, а также информацию о порядке использования сертификата. Например, это может быть другой сертификат, предназначенный для сертификации открытых ключей (такой вариант аналогичен созданию сертификата организационной единицы в системе Notes), либо сертификат сервера или разработчика, применяемый для подписи программ, либо сертификат отдельного пользователя, служащий для аутентификации серверами SSL и/или для подписи и шифрования электронной почты с помощью стандарта S/MIME. Все указанные сертификаты имеют формат, соответствующий международному стандарту X.509. Их иногда называют сертификатами X.509.

Ниже мы подробно рассмотрим управление SSL на серверах Domino и на рабочих станциях Notes. Но сначала речь пойдет о средствах защиты информации Domino и Notes.

Защита сервера

Если сервер Domino правильно настроить, то получится самая защищенная платформа, которую можно приобрести за деньги. Но защищенность определяется безопасностью нижележащей операционной системы. Поэтому необходимо охранять не только Domino, но и операционную систему. Защита сервера Domino подразумевает:

- физическую защиту;
- сетевую защиту;
- защиту операционной системы;
- управление доступом к серверу Domino.

Физическая защита, сетевая защита и защита операционной системы

Первые три элемента предыдущего списка являются наиболее важными способами обеспечения защиты Domino от взлома внутренних защитных барьеров, то есть от незаконного доступа в базы данных Notes. Существует два способа обхода защитных средств Domino на незащищенном сервере. Первый: если сервер работает под управлением Windows и есть физический доступ к серверу Domino, то обойти большинство барьеров Notes и Domino позволяет локальная копия клиента Notes. Удается обойти все барьеры, кроме унифицированного списка управления доступом к базе данных и шифрования данных. То же самое можно сделать и в операционных системах OS/2 и UNIX с Notes версии 4.5 или еще более ранней версии. Второй: если есть доступ к файловой системе, в которой Domino хранит базы данных, можно скопировать их на локальную рабочую станцию и получить к ним локальный доступ. Поэтому обязательно при физической защите серверов Domino защищать сеть и операционную систему компьютеров.

Физическая защита

В общем случае физическая защита означает, что сервер необходимо блокировать и закрывать на замок. Также следует блокировать или убрать клавиатуру либо заблокировать консоль Domino. Команда `set secure` пароль делает невозможным ввод команд с консоли сервера, в том числе `load`, `tell`, `exit`, `quit` и `set configuration`.

Команды `exit` и `quit` разрешается задать с паролем, то есть `exit` пароль или `quit` пароль. Для выбора других команд надо еще раз ввести `set secure` пароль, чтобы снять блокировку консоли.

Допустимо изменить пароль блокировки командой `set secure старый_пароль новый_пароль`. И наконец, можно взломать пароль:

1. Откройте файл `notes.ini` в текстовом редакторе, найдите переменную `SERVER_CONSOLE_PASSWORD` и удалите ее. Сохраните и закройте файл.
2. Выключите Domino с помощью средств операционной системы. В Windows или OS/2 можно просто отключить питание. В UNIX допустимо использовать команду `kill`. Интересно, что только NetWare, которую Lotus отказалась поддерживать с версии R5, не позволяет отключить программный сервер Domino, поэтому нельзя обойти защиту консоли сервера.
3. Перезапустите Domino. Консоль не будет заблокирована. #

Сетевая защита

Сетевая защита предусматривает защиту сети от злоумышленников и вредоносных программ. Чтобы защитить частную сеть от внешних пользователей, следует установить брандмауэр (межсетевой экран), который может включать в себя такие средства, как разрешение ответных звонков на сервер удаленного доступа. Для защиты сети от вредоносных программ необходимо установить современные антивирусные программы. Нужно использовать все стандартные средства сетевой операционной системы для обеспечения надежной защиты. Можно потребовать, чтобы все пользователи применяли пароли и периодически их меняли, а также установить программы контроля защиты, поставляемые вместе с сетевой операционной системой. ..

Рекомендуется нанять консультантов по проверке системы защиты. И наконец, надо объяснить пользователям, что некоторые мошенники могут обманом и хитростью выведать у них пароль.

Если есть подозрение, что сервер особенно уязвим хотя бы на одном из указанных уровней, имеет смысл применить несколько средств защиты на уровне базы данных. Во-первых, можно установить дополнительное средство управления доступом к базе данных - Enforce consistent Access Control List (Установка согласованного списка управления доступом) для всех реплик этой базы. Во-вторых, легко зашифровать данные.

Установка согласованного списка ACL в Notes ограничивает доступ локальных пользователей к базе данных. Если согласованный ACL не установлен, то только ACL сервера Domino ограничивает доступ. Пользователи Notes будут иметь доступ к локальным базам данных на уровне **Manager**. Однако режим Enforce consistent Access Control List - достаточно сложное средство Notes. Его не всегда удастся корректно установить, но даже если все сделано правильно, оно вызывает много проблем. Более детально мы рассмотрим возникающие затруднения чуть позже.

Шифрование данных на сервере более эффективно и реализовать его гораздо проще. Существует два способа шифрования.

Можно зашифровать отдельные поля с помощью ключа, специально разработанного для таких целей. Доступ к данным в этих полях будет предоставлен только пользователям, имеющим копию соответствующего ключа. Чтобы подобное средство сокрытия информации было эффективным, его следует встроить в базу данных. Поэтому для администратора Domino оно, скорее всего, недоступно.

Допустимо шифровать всю базу данных. Это называется *шифрованием локальной базы данных*. Если есть доступ к базе данных на уровне **Manager**, можно зашифровать ее. Администратор вправе пользоваться указанным способом.

Лучше всего для наших целей (для защиты данных от хакеров) подходит шифрование локальной базы данных (более подробно это объяснено ниже).

Даже если администратор локально зашифрует базу данных сервера, хакеры все же смогут получить доступ к данным, войдя в Notes с помощью ID-файла сервера. Известны два способа защиты сервера от подобного вторжения. Во-первых, установить пароль для ID-файла сервера. В таком случае для доступа к открытому ключу сервера придется подбирать пароль. Во-вторых, ввести список ACL базы данных так, чтобы доступ к ней нельзя было получить с помощью ID-файла сервера. Здесь необходимо присвоить элементу списка ACL для сервера тип пользователя (User type) равный **Server** (Сервер) или **Server Group** (Группа серверов). При этом ID-файл сервера в клиенте Notes уже не действует.

Защита операционной системы

Обычно защита нижележащей операционной системы подразумевает выполнение двух условий. Прежде всего надо в операционной системе запретить доступ к программе Domino и папкам с данными. Доступ к папкам Domino должна иметь сама система Domino или учетная запись пользователя, работающего с данной системой. Для обычных пользователей доступ к этим папкам локально или через сеть следует заблокировать. Не все операционные системы, совместимые с Domino, можно заблокировать от локального доступа (например, это нельзя сделать в файловой системе FAT операционных систем OS/2, Windows 9x и Windows NT). Однако все равно заблокируйте пользователей, насколько возможно.

Кроме того, необходимо максимально ограничить административный доступ к компьютеру, на котором работает сервер Domino. Административный пароль для компьютера Domino должен знать только персонал, которому действительно нужен такой доступ. Также важно постоянно обновлять операционную систему, особенно если выпускаются какие-либо «заплатки» для устранения брешей в системе защиты. Поскольку сейчас существует множество программ для открытия потайных ходов администратора к операционной системе, таких как Back Office, требуется бдительно следить за слабыми местами системы защиты, «дырами» в ней и их устранением.

Управление доступом к серверу Domino

Сама система Domino имеет множество функций управления на уровне сервера, которые ограничивают доступ к данным. Они разработаны не столько для противостояния хакерам, сколько с целью защиты от несанкционированного доступа клиентов Notes и не-Notes. Необходимо проверить каждый элемент и решить, подходит ли он в данной ситуации. Большинство элементов управления находятся в документах Server, Server Configuration и Web Configuration. Остальные элементы управления определены в файле notes.ini на сервере.

Элементы управления доступом обычно представлены в документе сервера (Server document) - см. табл. 10.3. Многие поля предполагают ввод имен серверов, людей и/или групп. В общем случае рекомендуется вместо отдельных имен серверов или людей использовать имена групп или подстановочные шаблоны, например */Stillwater, что позволяет ограничивать пользователей и серверы, добавляя или удаляя их из составляющих групп, а не из полей документа сервера. Хотя сервер Domino R5 и R6 гораздо лучше предыдущих версий обеспечивает открытие документа сервера для редактирования, компания Lotus не разрабатывала новые версии только для этого. Другими словами, нельзя заранее знать, что новый документ сервера Server начал действовать, пока не произведена перезагрузка. Все-го этого можно избежать, если просто вносить имена групп и подстановочные символы в поля документа сервера. Описания основных полей приведены в табл. 10.3.

Таблица 10.3. Поля управления доступом к серверу в документе сервера

Поле	Описание
Вкладка Basics (Основные параметры)	
Administrators (Администраторы)	Введите одно или несколько имен групп либо подстановочные шаблоны, которые определяют организационную единицу (например, */IT/Stillwater). Можно указать индивидуальные имена администраторов, разделяя их запятыми. Администраторы, чьи имена есть в списке, вправе выполнять на сервере следующие функции: вводить команды с удаленной консоли сервера; определять сервер как административный сервер для баз данных; уплотнять базы данных; использовать полнотекстовые индексы; управлять каталогами и связями базы данных
Вкладка Security (Параметры защиты)	
Compare Notes public keys against those stored in Directory (Сравнение открытых ключей Notes с хранящимися в каталоге)	По умолчанию No (Нет). Для уточнения значений в этом поле прочтите разъяснения, приведенные после таблицы

Таблица 10.3. Поля управления доступом к серверу в документе сервера (продолжение)

Поле	Описание
Allow anonymous Notes connections (Разрешил» анонимные соединения Notes)	По умолчанию No (Нет). Установка Yes (Да) позволяет пользователям Notes обращаться к серверу без аутентификации
Check passwords on Notes Ids (Проверка паролей ID-файлов Notes)	По умолчанию отключен. Для уточнения значений в этом поле воспользуйтесь разъяснениями, приведенными после таблицы
Вкладка Security => Server Access => Who Can (Параметры защиты => Доступ к серверу => Кто имеет право)	
Only allow server access to users listed in this Directory (Доступ к серверу разрешен только пользователям, перечисленным в данном каталоге) в R5	По умолчанию No . Если этот параметр разрешен, то доступ к серверу получают только те пользователи, которые имеют персональные документы в каталоге Domino. Поэтому после ввода варианта Yes проверьте, что поле Access server заполнено, чтобы люди, которые должны иметь доступ к серверу, получили его
Access server (Доступ к серверу)	Если поле пустое, то доступ к серверу разрешен всем пользователям. Если это поле заполняется, доступ имеют только пользователи, перечисленные в данном списке. Используйте имена групп или подстановочные символы (например, */Stillwater) или индивидуальные имена, разделяя их запятыми. Учтите, что, если предыдущий параметр (Only allow server access to users listed in this Directory) получил значение Yes , необходимо заполнить и это поле, иначе ни один сервер не сможет обратиться к данному
Not access server (Нет доступа к серверу)	По умолчанию поле пустое. Если введены какие-нибудь имена, этот параметр отменяет действие всех остальных параметров и указанные объекты не получают доступ к серверу. Создайте одну или несколько групп типа Deny List (Список запрещения) и внесите в него имена. Чтобы при необходимости заблокировать пользователя, просто поместите его в одну из этих групп
Create new databases (Создание новых баз данных) в R5 или Create databases & template (Создание баз данных и шаблонов) в R6	Когда поле пустое, любой пользователь может создавать новые базы данных на сервере. Большинство администраторов предпочитают контролировать процесс и задают здесь имена групп. Если добавлены имена, убедитесь, что указаны и имена групп серверов, таких как LocalDomainServers
Create replica databases (Создание реплики баз данных) в R5 или Create new replicas (Создание новых реплик) в R6	При пустом поле никто не сможет создать реплику базы данных на сервере. Обычно это неудобно. Добавьте имена групп администраторов и серверов
Allowed/Not allowed to use monitors (Разрешить/запретить использование мониторов)	В первом поле по умолчанию установлено значение *, а второе - пустое. Это значит, что любой человек может использовать мониторы на сервере. Мониторы представляют собой документы, отображающие подписи баз данных пользователей. Если в подписанной базе данных что-либо изменяется, монитор извещает пользователя. Монитор находится в базе данных Headlines на каждой рабочей станции Notes. Если базы данных на сервере будут подписывать много пользователей, то общая

Таблица 10.3. Поля управления доступом к серверу в документе сервера (продолжение)

Поле	Описание
Allowed/Not allowed to use monitors	производительность сервера сильно ухудшится. Названные поля можно применять для ограничения числа пользователей, имеющих право на подпись баз данных сервера. Запись в поле Allowed блокирует остальных пользователей. Запись в поле Not allowed блокирует только указанных там пользователей
Administer the server from a browser (Администрирование сервера через браузер) в R5	Пустое поле (по умолчанию) показывает, что никто не имеет такого права. Введите имена групп администраторов, чтобы разрешить им обращаться к базе данных Domino Web Administrator в R5 (webadmin.nsf) для администрирования сервера из браузера
Вкладка Security => Agent Restrictions =* Who Can (Параметры защиты => Ограничения для агентов =* Кто имеет право)	
Run personal agents (Запуск персональных агентов) в R5 или Run unrestricted methods and operations (Запуск неограниченных методов и операций) в R6	При пустом поле (по умолчанию) любой пользователь может запускать собственные программы-агенты на этом сервере. Добавление каких-либо имен заблокирует остальных пользователей
Runrestricted/unrestricted LotusScript/Java agents (Запуск ограниченных/неограниченных агентов LotusScript/Java)	Эти два поля по умолчанию пустые: ни у кого нет права запускать такие программы на сервере. Введите групповые символы (например, */Stillwater), группы или индивидуальные имена. При добавлении каких-либо имен убедитесь, что указаны также имена групп серверов (например, LocalDomainServers). Объекты, которым разрешено применять неограниченные агенты, могут также работать и с ограниченными агентами - независимо от того, внесены ли их имена в поле Restricted . Ограниченные агенты не в состоянии управлять системным временем, осуществлять ввод/вывод файлов и не имеют доступа к операционной системе. Точный список ограниченных операций имеется в справке Designer Help
Web server authentication (Аутентификация Web-сервера), в R6 называется Internet authentication (Аутентификация Internet) и находится в собственном разделе	Значение, установленное по умолчанию (More name variations) со слабой защитой, следует правилам Web-аутентификации версии R4, а Fewer name variations с сильной защитой — правилам Web-аутентификации версий R5 и R6. Задавайте второй вариант только в том случае, если все каталоги, которые исследует данный сервер, применяют шаблон каталогов версии R5/6. Оба варианта позволяют пользователям Web аутентифицироваться с помощью своего иерархического имени или любого псевдонима, указанного в поле User name персонального документа. Первый вариант дает возможность вводить только имя пользователя, только фамилию, сокращенное имя или созвучное значение
Вкладка Security => Passthru Use => Who Can (Параметры защиты => Использование сквозного режима => Кто имеет право)	
Access this server (Доступ к данному серверу)	Пустое поле (по умолчанию) означает, что никто не имеет права доступа к серверу транзитом

Таблица 10.3. Поля управления доступом к серверу в документе сервера (окончание)

Поле	Описание
Route through (Маршрутизация через данный сервер)	Пустое поле (по умолчанию) означает, что никто не может получить доступ к другому серверу через этот
Cause calling (Инициирование сквозного соединения)	Пустое поле (по умолчанию) означает, что никто не может заставить данный сервер связаться с другим для сквозной пересылки
Destinations allowed (Разрешенные адресаты)	Пустое поле (по умолчанию) означает, что любой пользователь, имеющий право сквозного обращения через этот сервер, имеет право транзита через любой доступный сервер. Если нужно ограничить сквозные соединения, введите имена серверов (или групп, содержащих их имена), к которым разрешен доступ через данный сервер. Сквозной доступ к другим серверам будет закрыт
Вкладка Security => HOP Restrictions => Who Can (Параметры защиты => Ограничения ПОР => Кто имеет право)	
Run restricted/unrestricted Java/JavaScript (Запуск ограниченных/неограниченных сценариев Java/JavaScript). В версии R6 находится в другом разделе, а данный раздел отсутствует	Для указанных полей применяются те же правила, что и для полей Restricted/unrestricted LotusScript/Java agents

Блокировка подозрительных ID-файлов

Два поля в документе сервера имеют особое значение – **Compare Notes public keys against those stored in Directory** (Сравнение открытых ключей Notes с хранящимися в каталоге) и **Check passwords on Notes Ids** (Проверка паролей ID-файлов Notes), которые заслуживают более подробного обсуждения.

Как и при аутентификации на основе сертификата, в этом случае существует один недостаток – закрытые ключи не всегда остаются закрытыми. Пользователю достаточно взять ID-файл другого пользователя и применить его для несанкционированного доступа. Администраторы многих организаций могут злоупотреблять ID-файлами заверителей организации или организационной единицы. На самом деле, если в большинстве организаций нет случаев злоупотребления, то только потому, что в основном люди в этих организациях честные, а мошенники просто не представляют себе, какой ущерб можно нанести, завладев чужим ID-файлом.

Указанные поля в документе сервера изначально предназначены для борьбы с последствиями применения подложных ID-файлов. Из них я бы посоветовал использовать второе и не трогать первое.

Сравнение открытых ключей Notes с хранящимися в каталоге

В нормальном режиме сервер при аутентификации другого сервера или пользователя принимает и использует открытый ключ, который он получает от другого объекта. Если сертификат, в котором хранится открытый ключ, подписан доверенной стороной и вторая сторона может подтвердить, что у нее есть соответствующий закрытый ключ, сервер доверяет этой стороне. Но если ID-файл кем-то скопирован или украден, то можно

аутентифицировать самозванца. Данное поле позволяет заблокировать доступ к серверу известным мошенникам.

Если активизировать поле **Compare Notes public keys against those stored in Directory**, то сервер не станет просто так принимать открытые ключи в присланных сертификатах, а будет сравнивать их с ключами, хранящимися в каталоге Domino. Если они не совпадут, сервер откажет в доступе.

Таким образом, если у пользователя украли ID-файл, можно сгенерировать этому пользователю новый открытый ключ. Копию нового ключа следует поместить в персональный документ пользователя. Затем разрешается соответствующее поле. Потом, когда самозванец пытается получить доступ к серверу с помощью старого открытого ключа, сервер блокирует доступ.

Однако данный способ обладает некоторыми недостатками. Во-первых, он не работает, если не сформированы новые ключи для пользователей, чьи ключи скомпрометированы. Это на самом деле проблема, поскольку не всегда известно, что ключ скомпрометирован, и, кроме того, создать новый ключ достаточно сложно. Во-вторых, такое поле одинаково действует на всех потенциальных пользователей и серверы, которые не имеют персональных или серверных документов в каталоге Domino. Если преследуется подобная цель, то гораздо проще использовать поле **Access server** (Доступ к серверу).

Из-за описанной проблемы компания Lotus начала исследования и нашла лучшее решение - поле **Check passwords on Notes IDs**.

Проверка паролей ID-файлов Notes

Если разрешено данное поле, то также можно заблокировать сомнительные ID-файлы, но эффективнее и проще, чем с помощью сравнения ключей. При активизации этого поля пользователь Notes (начиная с версии R5) создает свертку пароля своего ID-файла (файла идентификационных данных) и отправляет серверу вместе с сертификатом.

Сервер сохраняет свертку пароля в персональном документе пользователя. Теперь каждый раз, когда пользователь соединяется с сервером, сервер сверяет вновь полученную свертку пароля с уже имеющейся в персональном документе. Если они одинаковые, сервер аутентифицирует пользователя. Если пользователь меняет пароль ID-файла, сервер сохраняет новую свертку пароля, а также оставляет старую версию. Всего сервер может хранить до 50 паролей, поэтому пользователь вправе повторно применять пароли достаточно долгое время.

Если пользователь пытается ввести старый (не текущий) пароль, сервер не принимает его и предлагает ввести текущий пароль. Если пользователь, который ввел старый пароль, не является тем человеком, который сменил пароль на текущий, то он не знает нового пароля, не сможет его ввести и, следовательно, не будет аутентифицирован. Если пользователь на самом деле является санкционированным, а злоумышленник сменил его пароль, администратор удалит свертку пароля из персонального документа, пользователь установит новый пароль и соединится с сервером. В следующий раз при попытке соединения с сервером несанкционированный пользователь будет заблокирован.

Еще одно свойство проверки паролей заключается в том, что можно установить интервал смены паролей (**Required change interval**) и время отсрочки (**Grace period**). Перед окончанием интервала смены паролей сервер напомнит пользователю, что необходимо поменять пароль. По истечении такого интервала сервер блокирует пользователя до тех пор, пока он этого не сделает. Пользователь, не сменивший пароль до окончания времени

отсрочки, будет полностью заблокирован даже после смены пароля. В подобном случае потребуются вмешательство администратора.

Данный способ имеет два важных достоинства. Во-первых, если кто-либо скомпрометирует ID-файл, а вы об этом не будете знать, данный пользователь окажется заблокированным по окончании интервала смены паролей и времени отсрочки, а возможно, и раньше (когда санкционированный пользователь сам меняет пароль). Во-вторых, не работающие с системой пользователи автоматически будут заблокированы по окончании времени отсрочки.

Для активизации проверки паролей необходимо установить указанный параметр в серверных документах всех серверов, которые должны проверять пароли и во всех персональных документах, чьи пароли должны проверяться. Для установки проверки паролей в персональном документе выделите необходимое их количество на виде **People** (Сотрудники). Затем выберите **Actions => Set Password Fields** (Операции => Установка полей паролей). В появившемся диалоговом окне отметьте поле **Check password**, установите значение поля **Required change interval** и **Grace period** и щелкните по ОК. При этом в базе данных **Administrator Requests** (Административные запросы) генерируется запрос **Change User Password in Address Book** (Изменить пароль пользователя в адресной книге). Административный сервер каталога Domino выполнит запрос, как только документ запроса ему ответит.

Интересно, что кроме значений **Check password** (Проверять пароль) и **Don't check password** (Не проверять пароль), можно установить значение **Lockout ID** (Заблокировать ID-файл). В последнем случае указанный пользователь не получит доступ к любому серверу домена, на котором проверяются пароли. Это еще один способ блокирования пассивных пользователей (другой способ заключается в помещении их имен в группу **Inactive Users** (Неактивные пользователи), которая заносится в поле **Not access server** (Доступ к серверу запрещен) в документе сервера).

Lotus рекомендует действовать именно так, если вы беспокоитесь относительно активности пользователей. Однако следует соблюдать осторожность при работе с полем **Not access server** по двум причинам. Во-первых, таким образом для пользователей блокируется доступ к любому серверу домена, а не только к серверам, проверяющим пароли. Во-вторых, блокируется доступ для всех пользователей, не имеющих персональных документов в каталоге Domino. И наконец, можно скрыть данную группу от взора обычного пользователя, присвоив ей тип **Deny List**.

Такая группа будет отображаться только на виде **Deny Access** Стоир^двступном администратору. Конечно, пользователь может создать собственные виды, в которых будет показана данная группа, но лишь наиболее опытные пользователи Notes сумеют сделать это.

Защита базы данных

После того как пользователь преодолест барьеры на уровне защиты сервера, ему придется обходить препятствия на уровне защиты базы данных, включающей в себя несколько аспектов:

- О список управления доступом к базе данных;
- О защиту форм, видов и документов;
- О защиту разделов и полей;
- О локальное шифрование базы данных.

Самый полный перечень прав доступа пользователей к содержимому базы данных находится в списках управления доступом ACL в каждой базе. Другие указанные здесь средства служат для ограничения этих прав, а не для их расширения.

Список управления доступом к базе данных

Список управления доступом (ACL) к базе данных является основным элементом управления доступом в Notes. Все остальные элементы управления доступом просто усиливают ограничения ACL. Чтобы получить доступ в список ACL базы данных, откройте ее и выберите **File = Ф Database => Access Control** (Файл => База данных => Управление доступом). Можно также щелкнуть правой кнопкой мыши по значку базы данных и выбрать **Database => Access Control** (База данных => Управление доступом) в контекстном меню. ACL делится на четыре части: **Basics** (Основные параметры), **Roles** (Роли), **Log** (Регистрация) и **Advanced** (Дополнительно). Большая часть элементов перечислена на вкладке **Basics** (рис. 10.4).

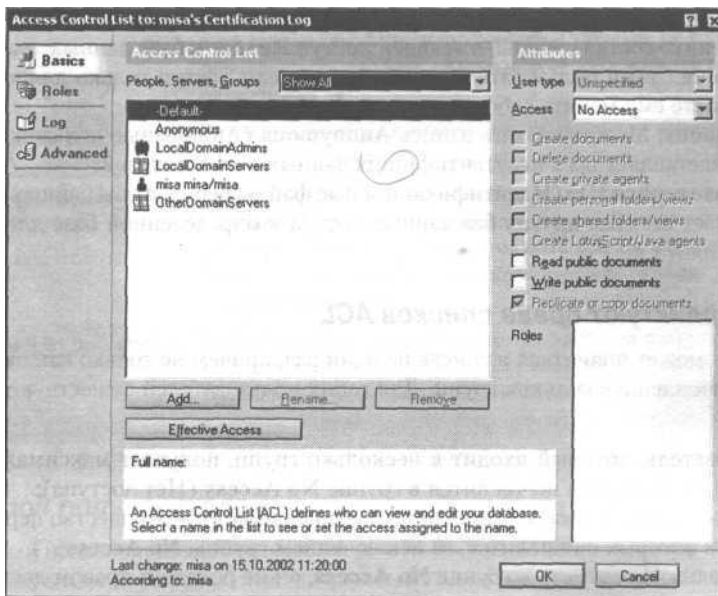


Рис. 10.4. Когда пользователь отмечен в списке, другие поля показывают все его права доступа к серверу. Здесь выбрано значение -Default- (По умолчанию)

Список пользователей

Центральный элемент вкладки **Basics** - список пользователей. Можно выбрать любого пользователя в списке, и остальные поля покажут его права доступа. Первым в списке

пользователей идет значение **-Default-**, которое определяет права пользователей, отсутствующих в списке. В список могут входить только следующие категории пользователей:

- О **People**. Люди (сотрудники) могут быть занесены в список по иерархическому имени, общему имени, если они являются членами одной иерархической организации, или по псевдониму. Компания Lotus рекомендует применять иерархические имена или псевдонимы. Конечно, некоторые пользователи (например, пользователи Internet) не имеют полных иерархических имен;
- О **Servers**. Серверы можно заносить по их иерархическим именам или общим именам, если они входят в одну иерархическую организацию, как сервер-хост. Lotus рекомендует применять иерархические имена;
- О **Wildcard entries**. Разрешено записывать целые организации или организационные единицы с помощью символов подстановки (например, */Stillwater или */MarchGreek/Stillwater);
- О **Groups**. Допускается задавать имена групп, перечисленных в локальном каталоге Domino или каталогах LDAP, которые были установлены для расширения полномочий групп в базе данных Directory Assistance. Введение групп позволяет гибко управлять правами ACL. Например, пользователю, которому предоставлено право изменять состав группы, имеющей доступ **Reader** к базе данных, вы даете право управления теми пользователями, которые имеют доступ только для чтения, но не разрешаете ему менять соответственно список ACL;
- О **Anonymous**. Можно создать запись **Anonymous** (Анонимные пользователи), которая представляет всех неаутентифицированных пользователей;
- О **Database replica IDs** (Идентификационные файлы реплик базы данных). Эта запись открывает агентам других баз данных доступ к определенной базе для поиска, обновления и т.д.

Когда конфликтуют права списков ACL

Пользователь может появиться в списке не один раз, причем не только как отдельный человек, но и как член нескольких групп. Для таких пользователей существуют следующие правила:

- О пользователь, который входит в несколько групп, получает максимальный набор прав, если только он не числится в группе **No Access** (Нет доступа);
- О если пользователь указан отдельно, эта запись имеет преимущество перед записями групп, в которых он числится, за исключением группы **No Access**;
- О если пользователь есть в группе **No Access**, он не обладает правом доступа независимо от того, в каких еще группах он присутствует.

Семь уровней доступа к базе данных

Основной уровень прав доступа пользователя появляется в поле **Access** в верхнем правом углу диалогового окна. Всего существует семь уровней доступа, а именно (от максимального до минимального): **Manager, Designer, Editor, Author, Reader, Depositor** и **No Access**. Назначение этих уровней объяснено в табл. 10.4. Права доступа на каждом уровне в общем случае совокупные; они включают в себя все права нижних уровней, кроме специально исключенных (см. **Reader**), и не содержат прав высших уровней, кроме специально включенных (см. **Editor**).

Таблица 10.4. Права доступа к базе данных Lotus Notes

Уровень доступа	Разрешенные действия
Manager (Менеджер)	Может вносить изменения в ACL, шифровать базу данных, изменять параметры репликации и удалять базу данных. Кроме того, обладает всеми правами, которые имеют пользователи нижних уровней
Designer (Разработчик)	Разрешено читать, создавать и изменять проектные документы, создавать полнотекстовые индексы и изменять формулу репликации. Кроме того, есть все права, которые имеют пользователи нижних уровней
Editor (Редактор)	Допустимо создавать новые документы, читать и редактировать существующие документы. Можно дать право создавать совместно используемые виды и папки (право, принадлежащее пользователям уровня Manager и Designer)
Author (Автор)	Способен создавать новые документы (если ему дано право Create document) и читать существующие. Не может редактировать документы, даже если сам был их автором, за исключением случаев, когда автор занесен в поле Authors в документе либо как пользователь, либо в составе группы. Если автор занесен в это поле, он вправе редактировать документ независимо от того, является его автором или нет
Reader (Читатель)	Разрешено читать существующие документы, но не редактировать и создавать документы, кроме документов со свойством Public (Общие)
Depositor (Вкладчик)	Может создавать новые документы, но не в состоянии читать и редактировать существующие документы. Однако вкладчику иногда дают право просмотра элементов базы данных, имеющих свойство Public, а также создавать и редактировать документы со свойством Public
No Access (Нет доступа)	В общем случае такому пользователю даже не разрешено открывать базу данных. Однако можно дать право просмотра элементов базы данных, имеющих свойство Public, а также создавать документы с этим свойством

Пять типов пользователей

Когда новый пользователь добавляется в список ACL базы данных, необходимо указать его тип. Это закрывает потенциальные «дыры» в системе безопасности. Всего существует пять типов пользователей: Person (Сотрудник), Server (Сервер), Mixed group (Смешанная группа), Person group (Группа сотрудников) и Server group (Группа серверов). Смешанная группа - группа, состоящая из серверов и людей. Если вы не укажете тип пользователя, он может получить большие права доступа, чем ему положено. Существует две потенциальные проблемы:

- О ID-файл пользователя и группа имеют одинаковые имена. Если общее имя в ID-файле пользователя совпадает с именем группы, сервер по ошибке может предоставить пользователю права, соответствующие ID-файлу группы. Если группе присвоить один из групповых типов пользователей, этого не произойдет, поскольку сервер будет знать, что данная запись в списке ACL соответствует группе, а не пользователю,

и не предоставит пользователю с таким же именем права группы. Но если тип пользователя не определен, то сервер не будет знать, к чему относится запись - к пользователю или к группе, и предоставит права того объекта, который первый встретится в списке;

- О пользователь регистрируется в системе с помощью ID-файла сервера. Серверы обычно имеют высокий уровень доступа к базам данных. Если сервер записан в ACL и для него не определен тип пользователя, то пользователь может соединиться с помощью ID-файла сервера и получить все его права. Сервер предоставит пользователю права другого сервера, потому что не знает, кто записан в ACL - сервер или человек. Если серверу в списке ACL присвоить тип Server, этого не произойдет, поскольку хост сервера будет знать, что соединившийся пользователь не способен быть сервером, потому что сервер не может использовать клиент Notes для соединения с другими серверами. А так как сервер теперь не знает, что собой представляет пользователь, он предоставит ему права, назначенные по умолчанию, но не права сервера.

Если список ACL базы данных уже содержит множество записей, для которых не определен тип пользователя, допустимо установить его для всех записей сразу, щелкнув по кнопке **Look Up User Types for 'Unspecified' User** (Задать тип пользователя для «неопределенных» пользователей) на вкладке **Advanced** окна **ACL**. Сервер для каждой записи ищет тип пользователя в каталоге Domino. Сервер не может определить принадлежность для групп пользователей, поэтому он присваивает всем группам тип **Mixed group**.

Дополнительные полномочия

В правой части вкладки **Basics** окна ACL указаны восемь дополнительных полномочий (в версии R6 добавлено еще одно полномочие), которые разрешено предоставлять пользователю. Вопрос о возможности их предоставления определенным категориям пользователей зависит от уровня их доступа. Для заданного уровня доступа некоторые полномочия можно автоматически установить и нельзя снять (флажки есть, но недоступны). Некоторые права могут быть автоматически назначены, но их можно снять (флажки установлены, но доступны), либо не назначены, когда флажка нет, но он доступен. В целом указаны следующие дополнительные полномочия:

- О **Create document** (Создание документов). Затрагивает только пользователей с уровнем доступа **Author**. Когда этот флажок снят, пользователь не вправе создавать новые документы, но может редактировать существующие, в которых в поле **Author** указано имя данного пользователя. В каталоге Domino по умолчанию пользователям предоставлен именно такой доступ. Пользователь способен редактировать свой персональный документ, но не может редактировать ни один другой документ в базе данных;
- О **Delete document** (Удаление документов). Это право предоставляют или снимают с пользователей с уровнем доступа **Author** и выше. Администратор должен собственноручно снять это право у самого себя, чтобы защититься от ошибочного массового удаления документов;
- О **Create personal agents** (Создание персональных агентов). Агенты - это программы, автоматизирующие работу баз данных. Они бывают очень мощными и полезными, могут функционировать и на рабочих станциях Notes, и на серверах Domino, но требуют очень много ресурсов процессора и оперативной памяти. Неактивный агент нередко занимает много дискового пространства. Персональные агенты предназначены

для использования исключительно их создателем. Администраторы и разработчики автоматически получают право создавать как общие, так и персональные агенты. Редакторам, авторам и читателям можно предоставить возможность создавать персональные агенты. Поскольку агенты потребляют много ресурсов, необходимо хорошо подумать, прежде чем давать право их создания кому-либо;

- О **Create personal folder/views** (Создание персональных папок/видов). Все пользователи с уровнем доступа **Reader** и выше способны формировать собственные папки и виды. Персональные папки и виды вместе с их индексами занимают много дискового пространства. Поэтому у редакторов, авторов и читателей можно отнять это право, разрешив создавать и использовать собственные папки и виды, но хранить не в самой базе данных, а на рабочих станциях пользователей в файле `desktop.dsk`. Это экономит огромное количество дискового пространства сервера, но персональные папки и виды теряют свою мобильность. Если пользователь запускает Notes на другой рабочей станции, его папки и виды будут недоступны;
- О **Create shared folder/views** (Создание общих папок/видов). Затрагивает только редакторов: разработчикам и администраторам это право предоставлено постоянно, а пользователи с уровнем доступа **Author** и ниже не обладают им никогда;
- О **Create LotusScript/Java agents** (Создание агентов LotusScript/Java). Относится к разработчикам, редакторам, авторам и читателям - они получают это право по умолчанию, но его можно снять. Агенты LotusScript и Java являются более мощными, чем обычные агенты, применяющие простые действия и формулы. И конечно, они требуют еще больших ресурсов компьютера. Поэтому необходимо еще тщательнее продумывать перечень пользователей, которым можно предоставить указанное право;
- О **Read public documents** (Чтение общих документов). Общие (совместно используемые) документы - это специальный тип документов, которые могут читать и создавать любые пользователи, даже если им присвоен статус **No Access**. Программисты создали этот класс документов для формирования групповых планов и календарей IB Notes. Персональная информация календаря каждого пользователя хранится в его почтовой базе данных, которая по умолчанию доступна только для этого пользователя. Чтобы групповое планирование имело определенную силу, необходимо предоставить другим пользователям хотя бы частичный доступ к персональным календарям. Такой цели служат общие документы. Пользователи разрешают другим пользователям доступ к некоторым документам (записям календаря), но закрывают его к другим документам (записям почтового ящика). Это право касается только вкладчиков и пользователей без доступа, поскольку лишь они вообще не могут читать документы;
- О **Write public documents** (Запись общих документов). Данное право затрагивает читателей, вкладчиков и пользователей без доступа;
- О **Replicate or copy documents** (Репликация или копирование документов - только в R6). Это право позволяет пользователям копировать и реплицировать как саму базу данных, так и ее документы. Распространяется на любой уровень доступа, за исключением **Depositor** (Вкладчик) и **No access** (Нет доступа).

Роли

Роли - это специальные функции, которые разрешено определять разработчику в базе данных. Например, в базе данных Resource Reservation (которая является частью функции Calendaring and Scheduling) есть роль для создания организационного ресурса, которая называется [CreateResource]. Большинству пользователей достаточно уметь только

резервировать ресурсы (конференц-зал, аудио/видеоаппаратура и т.д.). но кто-то должен распределять их и управлять ими. База данных настроена так, чтобы это могли делать только люди, которым назначена роль [CreateResource]. Вид **Site**, форма **Resource** и действия, необходимые для создания документа Resource, невидимы для всех пользователей - кроме тех, кому назначена роль [CreateResource].

Роли вправе создавать, переименовывать и удалять лишь администраторы (уровень **Manager**). Это делается на вкладке **Roles** диалогового окна **Access Control List**. Однако на практике разработчики тоже создают роли, когда имеют доступ администратора к базе данных. Имя роли может включать до 15 символов и содержать пробелы, символы верхнего и нижнего регистров и числа. Notes автоматически заключает имя роли в квадратные скобки. Существующие роли отображаются в квадратных скобках. Имя роли в любом поле или в формуле следует писать в скобках.

После создания роли ее имя (заключенное в квадратные скобки) появляется в списке **Roles** (Роли) на вкладке **Basics** диалогового окна **Access Control List**. Чтобы назначить роль пользователю (или снять назначение), необходимо отметить пользователя в списке и затем щелкнуть по имени роли, устанавливая или снимая флажок у этого имени.

Роли в каталоге Domino

В то время как большинство ролей полезны только для администраторов и разработчиков, некоторые роли, такие как [CreateResource] в базе данных Resource Reservation, представляют интерес для администраторов Domino. Наиболее важные роли, появляющиеся в каталоге Domino. Всего существует восемь ролей, разбитых по парам. Пользователи, которым назначены перечисленные ниже роли, могут создавать и изменять определенные документы:

- О [UserCreator] и [UserModifier] - персональные документы;
- О [ServerCreator] и [ServerModifier] - документы сервера;
- О ~tGroupCreatpr и [GroupModifier] - документы групп;
- О [NetCreator] и [NetModifier] - все остальные типы документов в каталоге домена.

На самом деле способность пользователя соответствовать назначенным ролям зависит от основного уровня его доступа. Пользователи с уровнем доступа **Author** и выше могут их выполнять, а читатели и ниже - нет.

Еще одно важное уточнение: роли **Creator** применяются для всех уровней доступа от автора и выше, а роли **Modifier** - только для авторов. Таким образом, чтобы создать какой-нибудь документ в каталоге Domino, пользователь должен иметь уровень доступа **Author** или выше, право **Create document** и соответствующую роль **Creator**. Для редактирования документа необходимо быть администратором, разработчиком либо редактором или же автором с ролью **Modifier**.

Предназначение ролей состоит в том, чтобы более эффективно распределять административные функции. Например, администратору, в чьи обязанности входит только управление существующими учетными записями пользователей, достаточно редактировать имеющиеся персональные и групповые документы. Для подобного человека лучшим уровнем доступа к каталогу Domino будет авторский основной доступ плюс роли [UserModifier] и [GroupModifier]. Пользователь с таким правом доступа сможет лишь читать другие типы документов.

И последнее: роли класса **Creator** более удобны, чем средства защиты, поскольку они не разрешают применять интерфейс Notes для создания документов пользователям, не имеющим статуса создателя. Для формирования документов, которые нельзя создать без роли **Creator**, служит агент LotusScript. С другой стороны, роли класса **Modifier** составляют основу защиты. Отсутствие соответствующей роли полностью блокирует автора списка ACL, и он уже не сможет создать запрещенный документ.

Журнал списка ACL и мониторы изменений ACL

Третья вкладка в окне **ACL** - это вкладка **Log** (Журнал). Здесь хранятся дата и время всех изменений, внесенных в список ACL базы данных, а также идентифицируются пользователи, которые производили изменения, и основные свойства этих изменений.

Поскольку изменения в ACL баз данных влекут за собой серьезные последствия, очень важно иметь инструмент для отслеживания такой информации. Можно установить **ACL Change Monitors** (Мониторы изменений ACL) в базе данных Statistics & Events (events4.nsf). Эти документы заставляют серверную задачу Event фиксировать случаи изменения ACL в определенных базах данных. Такие изменения становятся событиями безопасности (Security) с уровнем важности, заданным в мониторе. Можно создать в базе данных Statistics & Events документ Event Notification (Извещение о событии), который будет всеми возможными способами (электронная почта, пейджер или запись в базу данных) извещать о произошедшем событии.

Дополнительные возможности списков ACL

Вкладка **Advanced** содержит несколько инструментов, которые позволяют дополнительно защитить доступ к базе данных. Эти инструменты определяются полями для назначения административного сервера, установки защиты базы данных, определения максимального уровня доступа через Internet и массового обновления поля **User type** (Тип пользователя). Последний параметр мы рассматривали выше, поэтому остановимся на первых трех.

Назначение административного сервера

Во-первых, в поле **Administration server** (Административный сервер) можно назначить административный сервер и определить его функции. Большинство баз данных Notes требуют наличия административного сервера, чтобы изменения имени пользователя автоматически обновлялись в списке ACL базы данных и полях **Author** и **Reader**.

Введение согласованного списка ACL

Во-вторых, можно выбрать вариант **Enforce a consistent Access Control List across all replicas** (Установить согласованный список управления доступом для всех реплик) определенной базы данных. Это основной шаг, который предпринимается с целью усиления защиты базы данных. Но это также и проблемный шаг, приводящий к ряду побочных эффектов. Поэтому прежде чем задать такой параметр, необходимо понять, как он работает.

По умолчанию только Domino (сервер) устанавливает защиту ACL. Notes (клиент) этого не делает. Потенциально здесь защита не работает: если пользователь может получить физический доступ к серверу (только в операционных системах Windows), то он сумеет получить прямой (локальный) доступ к базе данных, не пользуясь доступом к базе данных

через сервер. Таким образом, пользователь обходит все средства защиты на уровне сервера и большинство средств защиты на уровне базы данных. На рис. 10.5 описанная ситуация изображена графически.

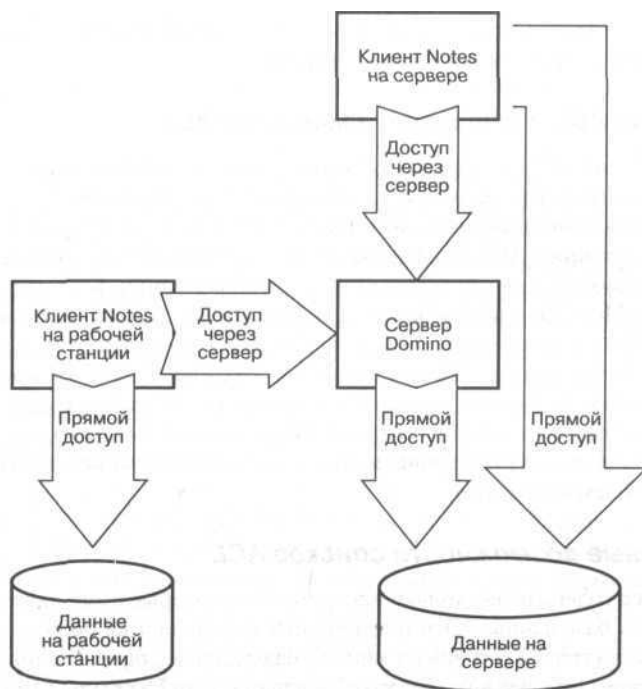


Рис. 10.5. Клиент Notes на рабочей станции имеет прямой доступ к локальным базам данных, но для получения доступа к серверным базам данных необходимо пройти через защитные барьеры сервера Domino. Если клиент Notes работает на сервере, то доступ можно получить напрямую (поскольку база данных локальная) или через программное обеспечение сервера

То, что Notes не имеет средств обеспечения защиты ACL, может смутить пользователя, потому что при попытке получить доступ к локальной базе данных у него не будет ограничений, которые есть при доступе к базе данных на сервере.

Основная цель выбора согласованного списка ACL для всех реплик базы данных заключается в том, чтобы установить список ACL в клиенте Notes. Если пользователь после этого запустит Notes на сервере, он уже не обойдет ограничения доступа, поскольку в клиенте Notes установлены свои ограничения. И пользователь с уровнем доступа Reader не сможет редактировать документы в локальной реплике базы данных, так как система Notes назначила для него доступ «только чтение», как всегда делает сервер и как уже ожидает пользователь.

Второй эффект наличия* согласованного списка ACL, который обычно удивляет администраторов баз данных, состоит в том, что можно изменить ACL только в главной реплике базы данных. После внесения определенных изменений в реплики ACL на сервере S1

и других изменений в реплики ACL сервера S2 две реплики оказываются несогласованными. В результате два сервера больше не способны обращаться друг к другу из-за несогласованности их списков ACL. Приходится вручную согласовывать реплики ACL. Если вы не отслеживаете ошибки репликации серверов, то рискуете не заметить нарушения взаимодействия серверов в течение дней, недель или даже месяцев со всеми вытекающими последствиями.

Побочный эффект такой установки недостаточно хорошо описан в документации Lotus и не до конца понимается большинством администраторов. Они пробуют данное средство, получают все неприятности и зарекаются от повторного его применения.

Кроме того, возникают сложности, если устанавливать согласованные списки ACL для баз данных, которые используются несколькими независимыми доменами Notes. Это случается, когда администраторы вторичных доменов создают реплики базы на одном из своих серверов и затем меняют ACL так, как нужно для их домена. В описанном случае они больше не смогут поддерживать реплики баз данных исходного домена. Если требуется ввести согласованный список ACL для нескольких доменов, администратор исходного домена должен быть источником всех изменений ACL и должен добавлять записи групп, удовлетворяющие требованиям других администраторов. Для администратора это не такая уж сложная задача.

Еще одна проблема с установлением согласованного списка ACL заключается в том, что такой ACL потенциально опасен. Есть вероятность навсегда заблокировать кого-нибудь в ACL базы данных, удалив всех несерверных администраторов из списка ACL. Если это произойдет, то единственный способ решить проблему - создать новую реплику базы данных, потеряв список ACL. В подобной ситуации необходимо иметь уровень доступа **Reader** или выше. Вы не сумеете скопировать или реплицировать в новую базу данных элементы, если у вас нет к ним доступа «для чтения». Это могут быть персональные папки, виды, агенты и документы других пользователей, к которым вы не имеете доступа. Вывод: помните обо всех последствиях установки согласованного списка ACL и будьте осторожны.

Установка максимального уровня доступа через Internet

И наконец, допустимо задать максимальный уровень доступа к базе данных, который пользователь может получить через Internet, применяя аутентификацию с помощью имени и пароля. По умолчанию определен уровень доступа **Editor**, но разрешается установить любой.

Другие способы просмотра и управления полями списка ACL,

Диалоговое окно **Access Control List** позволяет просматривать список ACL выбранной базы данных и управлять им. Можно просматривать список, если есть уровень доступа ниже **Manager**, а управляют ACL только с уровнем доступа **Manager**. Но что будет, если вам нужно просмотреть или изменить права доступа в нескольких базах данных?

Для просмотра состояния нескольких баз данных следует открыть Database Catalog (Каталог баз данных) - имя Catalog (5.0) или Catalog (6); имя файла catalog.nsf. Эта база данных имеет три вида для списков ACL. Их допустимо сортировать по базе данных, по уровню доступа или по имени пользователя. Таким способом невозможно просмотреть только те базы данных, которые были исключены из каталога посредством установки собственных свойств.

Для управления сразу несколькими базами данных предназначен программный инструмент **Multi ACL Management** (Управление несколькими списками ACL) в окне Domino Administrator. Перейдите на вкладку **Files** (Файлы), выберите сервер, на котором находятся нужные базы данных, и выделите их. После этого выполните **Tools => Database => Manage ACL** (Программные инструменты => База данных => Управление ACL). Откроется диалоговое окно **Multi ACL Management** (Управление несколькими ACL) в R5 или **Manage Multiple ACLs** (Управление несколькими ACL) в R6. Поскольку Domino Administrator не может предполагать, что все выбранные базы данных имеют одинаковые текущие записи ACL, текущие параметры ACL не отображаются. Фактически даже если вы выберете одну базу данных, ее текущие параметры ACL выводиться не будут. Мы надеемся, что подобные недоработки будут устранены.

Разрешается добавлять пользователей, переименовывать и удалять их (это относится только к тем пользователям, которых вы сами добавили). Можно добавлять, переименовывать и удалять роли, но нельзя распределять их между пользователями. Допустимо изменить значения в полях **Administration Server** (Административный сервер), **Consistent ACL** (Согласованный список ACL) и **Internet name and password** (Имя и пароль для доступа из Internet). При щелчке по ОК процесс Administration Process обновляет ACL во всех выбранных базах данных (или в тех, к которым вы имеете уровень доступа **Manager**).

Рекомендации по установке списков ACL для баз данных

Система Notes требует, чтобы в каждой базе данных был хотя бы один администратор (она не позволит удалить полный административный доступ). Однако Lotus советует иметь несколько администраторов. Идея такого решения заключается в том, что, если один человек не может выполнять администраторские задачи, это сделает другой. Кроме того, рекомендуется назначать административный доступ не группам, а отдельным людям. Так будет точно известно, кто является администратором. Однако многие предпочитают предоставлять административный доступ группам.

Если вы устанавливаете согласованный список ACL, обязательно предоставьте административный доступ хотя бы одному пользователю и одной несерверной группе. Так вы минимизируете риск блокирования своего доступа после удаления всех администраторов (имеются в виду люди, которым предоставлены права администратора). В качестве дополнительной меры предосторожности можно обозначить любую серверную группу с административным доступом как смешанную группу и получить доступ к серверу с помощью идентификатора сервера. Но это в состоянии сделать и несанкционированный пользователь.

Советуем предоставлять пользователям минимальные права доступа. Чем меньше администраторов, разработчиков и редакторов в базе данных, тем меньше вероятность конфликтов реплик.

И наконец, устанавливайте уровень доступа серверов максимально низким. Для правильного копирования базы данных серверу (в списке ACL другого сервера) необходимы следующие уровни доступа:

- **Manager**, если сервер должен записывать изменения ACL на указанные серверы;
- **Designer**, если сервер должен записывать изменения дизайна на указанные серверы;
- **Editor**, если сервер должен записывать изменения данных на указанные серверы;
- **Reader**, если сервер должен воспринимать изменения от исходных серверов.

Некоторые организации, особенно применяющие топологию сетей с концентратором и радиальными серверами (hub-and-spoke), определяют для баз данных сервера-концентратора уровень доступа **Manager**, но не людям, а другим объектам системы. Если имеется несколько концентраторов или они расположены каскадом, необходимо всем им предоставить доступ на уровне **Manager**, чтобы концентраторы могли передавать изменения ACL радиальным серверам. Любые дизайнерские серверы должны иметь уровень доступа **Designer** и иногда **Manager**. Подчиненные серверы обладают уровнем доступа **Editor** к базам данных, в которых их пользователям дан доступ для записи (**Depositor**, **Author** и выше), и уровень доступа **Reader** к базам данных «только чтение», таким как справочные базы данных или руководства пользователей.

Почтовые базы данных пользователей являются особенно сложной проблемой, потому что по умолчанию (во многих существующих конфигурациях) полный доступ к базе данных имеет только собственник и его почтовый сервер. Начиная с версии R5.0 можно установить собственнику базы данных уровень доступа к своим почтовым базам ниже **Manager**. Начиная с версии R5.0.1 допускается в качестве дополнительного администратора новых почтовых баз данных пользователя добавить группу администраторов. В зависимости от политики компании в отношении конфиденциальности почты, допустимо по-разному воспользоваться этой возможностью.

Просмотр списков доступа

Разработчикам видов достаточно ограничить доступ только к их собственным видам. Для этого в окне **View Properties** (Свойства вида) на вкладке **Security** (Защита) установите параметр **May be used by...** (Может использоваться...) в значение ниже **All readers and above** (Всеми читателями и выше). Это более удобное средство, чем опции собственно защиты, поскольку любой пользователь в состоянии создать собственный вид, который будет отображать тот же документ, выводимый на виде с ограниченным доступом. Но есть несколько особенностей, которых необходимо остерегаться.

Списки доступа формы

Формы могут иметь два различных списка доступа: **Default read access for documents created with this form** (Доступ «только чтение» для документов, созданных с помощью данной формы) и **Who can create document with this form** (Кто может создавать документы с помощью этой формы). Оба списка доступны разработчику форм в окне **Form Properties** (Свойства формы) на вкладке **Security**.

Когда разработчик устанавливает в поле **Default read access for documents created with this form** значение ниже **All readers and above**, программа Domino Designer создает внутри формы поле, называемое **SReaders**. Это поле типа **Names** (Имена), содержащее имена людей, серверов и групп, которые отмечены в поле **Default read access**. Все документы, созданные с помощью данной формы, будут наследовать указанное поле и его параметры. Окончательные документы смогут читать только те пользователи, которые указаны здесь и в любом поле документа с типом данных **Author** или **Reader**.

Если разработчик задает поле **Who can create document with this form** значение ниже **All authors and above**, то форма становится недоступной для пользователей, не указанных

в данном поле. Таким способом каталог Domino ограничивает права создания документов людям, которым назначены различные роли класса **Creator**, - используются только роли, присутствующие в поле **Who can create** соответствующей формы.

Усилить защиту форм можно также и другими способами. В частности, разработчик вправе установить, что документ, созданный с помощью данной формы, нельзя распечатать, переслать или скопировать. Это устраняет все способы неправильного использования информации в документах, созданных посредством данной формы.

Поля \$Readers, Readers и Authors

Разработчики, а также авторы и редакторы документов способны ограничить доступ к индивидуальным документам данными различными способами. В предыдущем разделе мы рассказали о том, как можно использовать параметр формы **Default read access...** для ограничения числа читателей документа, созданного с помощью этой формы. Авторы и редакторы документа вправе ограничивать число читателей, управляя параметром **Who can read this document** (Кто может читать документ). Указанный параметр наследует значение параметра формы **Default read access...** Другими словами, он наследует и использует значение поля **SReaders** документа, который создан с помощью данной формы. Изменения, которые пользователь вносит в поле **Who can read this document**, автоматически отображаются в поле **SReaders**.

Допустимо еще больше ограничить круг читателей документа в поле с типом данных **Readers**. К документу с таким полем доступ для чтения получают только пользователи, серверы и группы, упомянутые в этом поле (из тех пользователей, серверов и групп, которые перечислены в полях **SReaders** и **Authors**). Если поле существует, но в нем ничего не записано, доступ предоставляется любым пользователям.

И наконец, разработчики могут ограничить права на редактирование документа посредством поля с типом данных **Authors**. Эти поля касаются только пользователей с уровнем доступа **Author**. Такие пользователи могут редактировать документы только в случае, когда их имена (или имена групп, членами которых они являются) перечислены в поле **Authors** данного документа; иначе они могут только читать этот документ.

Ограничение доступа к частям документа

Разработчики в состоянии ограничивать доступ на редактирование отдельных разделов документа. Раздел - это определенная часть формы или документа, созданного с помощью такой формы. Любой, кому разрешено читать документ, вправе читать все разделы. Но если ограничена возможность редактирования, то изменить определенный раздел способны только те пользователи, которые перечислены в списке редакторов данного раздела.

И наконец, авторы и редакторы могут подписывать и/или шифровать отдельные поля документа. Пользователь, подписывая поле, обозначает, что именно он последним редактировал документ. Подпись, кроме того, заверяет читателя, что подписанное значение с момента подписи не изменялось. Время подписи поля также указано. Если поле находится в разделе документа, то подпись затрагивает все поля данного раздела. В документе с несколькими разделами каждый раздел разрешается подписывать отдельно.

Автор или редактор, который зашифровывает поле, может сделать это либо одним или несколькими открытыми ключами, либо специально созданным ключом шифрования. Если поле зашифровано открытым ключом, то расшифровать его сумеет только владелец

соответствующего закрытого ключа. Поле, зашифрованное определенным ключом, в состоянии расшифровать только пользователь, располагающий копией этого ключа. Различные поля документа допустимо шифровать различными ключами. Но один ключ шифрования позволяет дешифровать все поля.

Хотя любой автор или редактор в состоянии зашифровать любое поле по своему усмотрению, чаще поля шифруются автоматически, поскольку так было задано разработчиком базы данных. В этом случае разработчик или администратор базы данных создает ключи шифрования во время проектирования. Затем, когда база данных вводится в эксплуатацию, разработчик должен передать ключ шифрования администратору, который в свою очередь распространяет ключи среди пользователей. Эти ключи хранятся в ID-файле каждого пользователя. Ключи, применяемые пользователем, можно увидеть в ID-файле на странице Encryption Keys (Ключи шифрования).

Шифрование локальной базы данных

В отличие от полей, в локальной базе данных шифруется все ее содержимое. База данных шифруется с помощью ключа, который в свою очередь шифруется открытым ключом отдельного пользователя или сервера (в зависимости от расположения базы). Чтобы получить доступ к этой базе из Notes, необходимо войти в систему с помощью идентификатора пользователя или сервера, который сможет расшифровать ключ. Для блокирования доступа к зашифрованной локальной базе данных не из Notes, необходимо использовать среднее или стойкое шифрование, но не нестойкое (см. ниже).

Целью локального шифрования является предотвращение несанкционированного локального доступа к базе данных, размещенной на сервере или на рабочей станции. Опасность в случае с сервером заключается в том, что пользователь с помощью вокальной копии Notes может обойти защиту ACL и получить административный доступ к базе данных, а в случае с рабочей станцией - доступ к базе данных для чтения. Он сумеет открыть ее, даже не зная пароля ни к одному ID-файлу системы Notes.

Для шифрования базы данных необходимо иметь административный доступ к ней. Обычно пользователи обладают таким доступом к базам данных на своих рабочих станциях, поэтому могут шифровать их самостоятельно с помощью собственных ID-файлов. Но если в локальной базе данных установлен согласованный список ACL, то пользователь должен попросить администратора базы данных зашифровать ее. Администратор переключается на свой ID-файл, а затем шифрует базу данных с помощью ID-файла пользователя, блокируя таким образом свой доступ к локальной реплике базы данных. Предупреждение: убедитесь, что данная локальная копия - не единственная копия базы данных.

Для шифрования существующей базы данных откройте диалоговое окно **Database Properties** (Свойства базы данных). На вкладке **Basics** выберите **Encryption Settings** (Параметры шифрования). Если эта кнопка недоступна, значит, у вас нет административного доступа к базе, то есть доступа на уровне **Manager**. Появляется диалоговое окно **Encryption for имя_базы^данных** (Шифрование указанной базы данных).

Выберите **Locally encrypt this database using...** (Локально шифровать базу данных с помощью...) и задайте стойкость шифрования: стойкое, среднее и простое. Если вы имеете доступ к базе данных через сервер Domino, то появится запись **For имя_сервера**, указывающая, что для шифрования базы данных будет использован открытый ключ сервера. Если вы получили локальный доступ к базе данных (непосредственно на сервере либо на рабочей станции), слово **For** будет кнопкой, а имя пользователя - это имя, под которым вы

вошли в систему. Щелкнув по кнопке **For**, можно выбрать имя другого пользователя или сервера из каталога. Если открытый ключ заданного пользователя доступен в каталоге, из которого выбран пользователь или сервер, Notes шифрует базу этим открытым ключом, блокируя доступ всем остальным пользователям. При выборе стойкости шифрования имеет смысл воспользоваться следующими рекомендациями:

- в большинстве случаев применяйте шифрование средней стойкости (**medium encryption**). При этом относительно сложно вскрыть ключ и не увеличивается время доступа к данным;
- прибегайте к стойкому шифрованию (**strong encryption**) только для особенно важных данных. Такой шифр очень сложно взломать, но он сильно замедляет доступ к данным;
- простое шифрование (**simple encryption**) следует назначать исключительно в тех случаях, когда сокрытие данных не является основной целью и вам достаточно сжать файлы. Такой шифр защищает данные только от случайного «бродяги».

При простом шифровании информация на самом деле не шифруется. Notes всего лишь не показывает данные пользователям, которые не имеют закрытого ключа для их расшифровки. Файлы позволяет прочитать программа, обладающая соответствующим интерфейсом прикладного программирования API.

Можно зашифровать базу данных при ее создании. В диалоговых окнах **New Database** (Новая база данных), **New Copy** (Новая копия) и **New Replica** (Новая реплика) есть кнопка **Encrypt** (Шифровать), которая открывает описанное выше диалоговое окно.

Защита рабочей станции

Защита рабочей станции включает в себя следующие направления:

- защиту от вирусов, «червей» и троянских коней;
- защиту локальных данных от несанкционированного доступа.

Для защиты от вредоносного программного обеспечения Notes предлагает список ECL (Execution Control List - список управления исполнением программ), а для защиты от несанкционированного доступа - целый ряд инструментов, в том числе средства защиты ID-файлов пользователя и индивидуальных баз данных.

Список управления исполнением программ

Для выполнения задач, обозначенных первым пунктом в предыдущем списке, можно использовать стороннее программное обеспечение. Но нас больше интересует встроенное средство Notes - Execution Control List (ECL). ECL - это двойник списка ACL баз данных, который ограничивает доступ объектов к системе. Как и в списке ACL базы данных, в списке ECL перечисляются объекты (здесь - объекты, подписывающие программы), и для каждого объекта указываются права на выполнение программ (рис. 10.6). Допустимо определить различные наборы прав для каждого типа программ: агентов LotusScript/Formula Language, Java-апплетов и внедренных JavaScript-кодов.

Чтобы открыть список ECL на рабочей станции, запустите клиент Notes и выполните **File => Preferences => User Preferences** (Файл => Предпочтения => Предпочтения

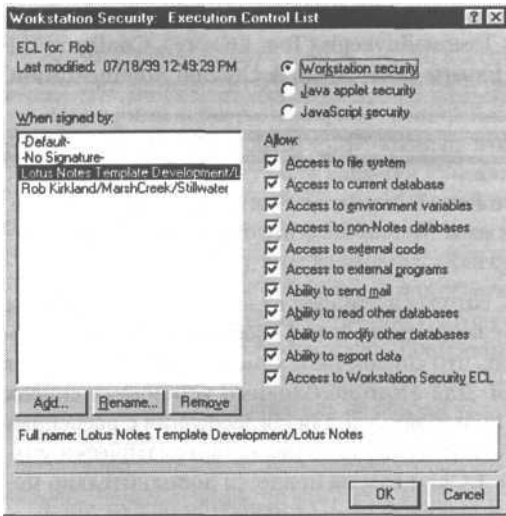


Рис. 10.6. Для каждого из подписывающихся пользователей можно определить уровень доступа его программ к системе

пользователя). В окне **User Preferences** на вкладке **Basics** выберите **Security Options** (Параметры защиты). Откроется окно **Workstation Security: Execution Control List** (Защита рабочей станции: Список управления исполнением программ). В версии R6 все рассмотренные ниже параметры находятся на самой вкладке **Basics** в разделе **Additional Options** (Дополнительные параметры).

Это окно имеет три вкладки: **Workstation Security** (Защита рабочей станции), **Java applet security** (Защита Java-апплетов) и **JavaScript security** (Защита сценариев JavaScript), их выбирают в правом верхнем углу диалогового окна. На каждой вкладке можно добавлять, переименовывать и удалять подписывающихся пользователей. Для любого пользователя допускается выбирать и снимать различные типы доступа или права на исполнение программ.

Есть небольшой подвох, на который автор наткнулся много раз, пока не разобрался, как работает это окно: при добавлении пользователя на одной вкладке Notes не вносит его автоматически на остальных двух вкладках. Поэтому, если нужно, чтобы имя пользователя появилось на нескольких вкладках, необходимо вписывать его дополнительно.

По умолчанию защита рабочей станции отключена. Следовательно, все указанные по умолчанию пользователи имеют полный набор прав на выполнение программ. В списке по умолчанию названы следующие пользователи: **-Default-** (По умолчанию), **-No Signature-** (Без подписи), **Lotus Notes Template Development/Lotus** (Разработка шаблона проектирования Lotus Notes/Notes) и основной пользователь данной рабочей станции. Интересно, что на незащищенной системе Notes любая программа, подписанная кем угодно или не подписанная вообще, в состоянии выполнять любые функции, которые позволяет реализовать язык программирования.

На сегодняшний день это очень опасно. Не составляет особого труда, например, создать почтовое сообщение, которое форматирует жесткий диск получателя. Такое сообщение может похитить конфиденциальную информацию из баз данных Notes и отправить ее на другой компьютер или сформировать путь, через который хакер впоследствии проникнет

в систему и будет делать там все, что ему заблагорассудится. Приведем пример создания подобного сообщения (пример предоставлен Томом Лоувери (Tom Lowery), *Configure the ECL to Thwart Trojan Horse Attacks*, Advisor Expert: Lotus Notes & Domino Administration, Premiere 1999, с 13):

1. Измените форму **Мемо** (Памятка) в базе данных Notes Mail, чтобы автоматически выполнять вложения.
2. Установите в документе свойство **Store form** (Форма хранения) для формы **Мемо**,
3. В сообщение, созданное с помощью формы **Мемо**, вложите троянского коня и отправьте его.

В большинстве систем единственная вещь, которая защищает от выполнения подобных программ, - это беспечность и/или незнание получателя таких сообщений. Но есть возможность настроить систему пользователя так, что список ECL клиента Notes тоже будет предотвращать выполнение троянских коней. Для этого необходимо установить список Administration ECL и обновить списки ECL пользователей для согласования с введенными параметрами (пользователи, которые устанавливали Notes позже, автоматически наследуют параметры настройки Administration ECL, и вам не придется дополнительно менять индивидуальные значения).

Настройка административного списка ECL

Список Administration ECL расположен в каталоге Domino. Для настройки административного ECL откройте каталог Domino на сервере. Выполните **Actions => Edit Administration ECL** (Операции => Редактировать административный список ECL). Выберите тип защиты и измените записи в списке. Обратите внимание на подвох, о котором я говорил ранее: когда вы добавляете пользователя, он вносится только на текущую вкладку.

Если вы, скажем, хотите настроить несколько ECL, у каждого из которых будут разные конфигурации для различных типов пользователей, то допускается настроить несколько баз данных Directory и затем модифицировать отдельно списки ECL в каждой базе. Каждая база данных будет основываться на шаблоне каталога Domino (pubnames.ntf) и, конечно, будет иметь уникальное имя файла.

Компания Lotus разрешила создавать несколько административных списков ECL в одном каталоге. Но в версии R5.0 это не было сделано, и полная реализация такой возможности предусмотрена только в версии R6.

Обновление списков ECL пользователей

#

Чтобы распространить действие списка Administration ECL на пользователей, необходимо послать им сообщение электронной почты, где будет кнопка, при нажатии на которую выполнится обновление. Для этого:

1. Создайте сообщение, адресованное всем пользователям, чьи ECL нужно обновить.
2. Добавьте в сообщение кнопку, при нажатии на которую будет выполняться команда **@RefreshECL** (имя_сервера:имя_файла; имя_ECL).
3. Опишите назначение сообщения, проинструктируйте пользователя, что он должен щелкнуть по кнопке, и отправьте сообщение.

В указанной формуле:

- О имя_сервера: имя_файла - путь к административному списку ECL, из которого будет производиться обновление ECL пользователей. Первая часть выражения - полное имя сервера, а вторая - имя файла каталога Domino, где находится ECL. Чтобы обратиться к каталогу Domino на локальном сервере пользователя, вместо всего выражения поставьте кавычки (""") или напишите слово NULL;
- О имя_ЕСБ - это имя административного списка ECL, из которого производится обновление. В версии R5.0 нельзя было создавать несколько списков ECL в одном каталоге, поэтому вместо имени файла ставились кавычки (""") или слово NULL, указывающее на безымянный административный список ECL. В версии R6 допускается создание нескольких административных списков ECL, настроенных на определенные группы пользователей. Такие списки селективно действуют на разные группы за счет определения каждого списка ECL в собственной политике безопасности. Как и прежде, пользователь не обязан указывать имя файла, но может получить индивидуально настроенный список ECL, который применяется к нему в рамках наследования определенной политики безопасности.

Если нужно обновить ECL на локальном сервере пользователя из административного списка ECL, расположенного в каталоге Domino (names.nsf), реализующую формулу можно записать следующим образом:

```
@RefreshECL ("";""")
```

Первая пара кавычек сообщает Notes, что необходимо обратиться к базе данных names.nsf, расположенной на локальном сервере пользователя. Вторая пара кавычек отправляет к безымянному ECL в этой базе.

Если требуется обновить ECL из административного ECL, находящегося в специально созданном каталоге, выражение может выглядеть так:

```
@RefreshECL("Osprey/Servers/Stillwater":"ECL1.nsf";""")
```

или так:

```
@RefreshECL ("";"ECL1.nsf";""")
```

В первом примере конкретно указано, какие сервер и базу данных необходимо использовать. Во втором примере определена база данных, но показано, что она расположена на локальном сервере пользователя. Обратите внимание, что имя сервера и имя файла базы данных заключены в кавычки. Это важно, поскольку формула без кавычек работать не будет.

Безопасное использование ECL

Компания Lotus по умолчанию отключает ECL, потому что при неправильной настройке он может работать непредсказуемо. Чтобы изначально список ECL функционировал корректно, Lotus рекомендует разобраться в правилах использования ECL и настроить его так, как нужно.

Перед выполнением какой-либо программы (внедренного кода, LotusScript, JavaScript или Java-апплета) Notes проверяет ECL, чтобы определить, какие действия способна

реализовать эта программа. Notes находит подпись программы, аутентифицирует ее и затем ищет имя объекта в ECL. Если такого пользователя в списке нет, Notes устанавливает для него параметры по умолчанию, то есть **-Default-**. Если программа вообще не подписана, указывается значение «не подписано» (**-No signature-**).

Если теперь программа пытается произвести какое-либо действие, которое не разрешено подписавшему ее пользователю, появляется предупреждающее диалоговое окно **Execution Security Alert** (Предупреждение системы защиты) - рис. 10.7.

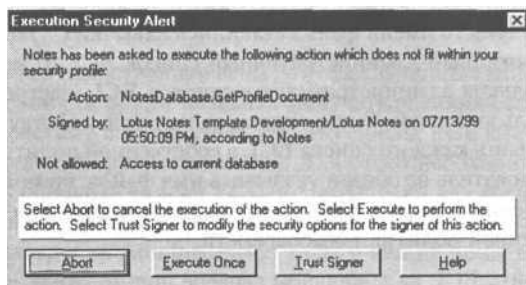


Рис. 10.7. Предупреждение системы защиты выводится, когда программа пытается выполнить запрещенные ей действия

Это диалоговое окно - явная недоработка защиты ECL. Оно непонятно для большинства пользователей Notes: они либо не знают, что с ним делать (и обращаются в службу технической поддержки), либо знают, что можно нажать **Trust Signer** (Доверять подписавшему пользователю) и программа продолжит работу. Но, поступая таким образом, они делают список ECL все менее и менее полезным, поскольку впоследствии они разрешат программам, подписанным этим же пользователем (или вообще без подписи) выполнять любые действия в системе, что может нанести серьезный вред. Если они часто обращаются в службу технической поддержки компании, то консультант вскоре устанет и скажет, что достаточно щелкнуть по кнопке **Trust Signer**, чтобы программа выполнялась дальше.

В качестве альтернативного варианта список ECL пользователя блокируется таким образом, чтобы кнопка **Trust Signer** была недоступна и пользователь мог нажать только на **Abort** (Заккрыть) или на **Execute Once** (Выполнить один раз). После нескольких повторений этой операции пользователь начинает ненавидеть Notes, ненавидеть вас, ненавидеть свою работу и свою жизнь в целом. В утешение вы отключаете ECL и предоставляете всем пользователям полные права на выполнение программ.

Существует решение, которое минимизирует возможность открытия окна **Execution Security Alert** и тем самым делает его появление более значимым:

- О ограничьте число пользователей, способных создавать новые базы данных на вашем сервере;
- О создайте фиктивного пользователя, у которого будет единственная задача - подпись внутренних баз данных. Предоставьте ему права администратора, достаточные для получения доступа к файлам на сервере Domino из программы Domino Administrator. Например, компания Lotus подписывает свои шаблоны и базы данных с помощью ID пользователя, названного Lotus Notes Template Development/Lotus Notes. Для этой цели создана и организация (/Lotus Notes), и пользователь (Lotus Notes Template Development);

- О обновите ECL пользователей так, чтобы все пользователи, подписывающие базы данных на ваших серверах, имели те права, которые им требуются для выполнения своей работы;
- О прежде чем поместить новую базу данных на серверы, убедитесь, что она подписана известным объектом. Кроме того, удостоверьтесь, что подписаны все существующие базы. Можно подписывать шаблоны или сами базы данных. Базы будут наследовать подписи из шаблонов, на основе которых они формируются;
- О объясните пользователям вашей компании и персоналу технической поддержки важность и значение оперативной реакции на появление окна **Execution Security Alert**.

Это большая и сложная работа. Но в нашем растущем компьютеризированном мире такие средства защиты становятся все более и более важными. Хотя можно просто сидеть и ждать, когда придет беда.

Предупреждение: компания Lotus обычно подписывает базы данных и шаблоны с помощью ID, названного Lotus Notes Template Development/Lotus Notes. Однако в спешке при выпуске версии R5.0 они забыли подписать многие шаблоны и базы данных, поставляемые вместе с этой версией. Перед развертыванием любого приложения на основе таких шаблонов и баз данных убедитесь, что они подписаны, и, если подписи нет, самостоятельно подпишите их. Иначе ваши пользователи столкнутся с выбором - либо не работать с приложением, либо позволить объектам без подписи совершать разрушительные действия на своих компьютерах.

Подпись базданныхишаблонов

Чтобы подписать базы данных или шаблон:

1. Переключитесь на ID-файл пользователя, который вы будете использовать для подписи базы данных или шаблона.
2. Откройте вкладку **Files** окна Domino Administrator. Выберите сервер, на котором находятся подписываемые базы данных и шаблоны.
3. Отметьте базы данных и/или шаблоны и выполните **Tools => Database => Sign** (Программные инструменты => База данных => Подпись). Откроется диалоговое окно **Sign Database** (Подпись базы данных).
4. Выберите нужные параметры и щелкните по ОК.

Существуют следующие параметры: подписывать все проектируемые документы (**all design documents**); только документы определенного типа (**all documents of type**) - тип документа выбирается из списка; только определенные документы (**this specific Note ID**) - документы с определенным файлом идентификационных данных, который необходимо знать. Кроме того, в версии R6 можно подписывать все документы данных (**all data documents**). Допустимо также задавать только обновление существующих подписей (**update existing signatures only**).

Чтобы найти Note ID разрабатываемого документа:

1. Откройте нужную базу данных в Domino Designer.
2. На панели **Bookmark** выберите тип документа, чей Note ID вам нужен. Появится список документов указанного типа, содержащихся в базе данных.
3. Щелкните правой кнопкой мыши по требуемому документу и в контекстном меню выберите **Design Properties**. Откроется диалоговое окно **Design Document Properties**.

4. Выберите вкладку **Document IDs**.
5. **Note ID** - это последняя строка, начинающаяся с букв «NT». Вам нужны только крайние правые символы, перед которыми стоят нули.

Защита данных на рабочей станции

Еще одна проблема безопасности данных заключается в том, что рабочие станции часто располагаются в местах, где они могут подвергаться несанкционированному доступу. Это, в частности, относится к портативным компьютерам, которыми пользуется руководство компаний. Если вы еще не слышали страшных историй о том, как в аэропортах, гостиничных номерах или даже прямо со стола руководителей воровали портативные компьютеры, где хранилась информация о пятилетних планах компаний, то это просто вопрос времени.

Для защиты таких компьютеров от посторонних глаз можно предпринять следующие меры:

- О установить согласованные списки ACL, что усиливает ACL в локальной копии клиента Notes;
- О зашифровать локальные базы данных;
- О убедить пользователей, чтобы они блокировали свои ID, если оставляют рабочие станции без присмотра;
- О установить в клиенте Notes автоматическую блокировку после определенного периода бездействия;
- О запрашивать необычно сложные пароли на открытие ID-файлов;
- О требовать несколько паролей при открытии ID-файлов;
- О в особо важных базах данных запретить печать, пересылку и копирование документов.

Установка согласованных списков ACL

Мы уже рассматривали установку согласованных ACL. В данном случае преимущество согласованных списков ACL заключается в том, что пользователь, просматривающий локальную копию базы данных, обладает уровнем доступа локального пользователя к этой базе. Но если вы хотите полностью скрыть информацию от несанкционированного доступа, это средство не поможет, поскольку локальный пользователь имеет доступ минимум «только чтение».

Шифрование локальной базы данных

Эти вопросы тоже уже обсуждались. Здесь вся база данных шифруется определенным ключом, который в свою очередь шифруется с помощью открытого ключа какого-либо пользователя. В результате, чтобы получить доступ к базе данных, вам необходимо войти в систему с помощью ID-файла того же пользователя, поскольку для расшифровки содержимого базы данных нужен закрытый ключ из этого ID-файла. Не зная пароля для ID-файла, вы не сумеете открыть ни его, ни базу данных. Эффективно защитить от несанкционированного доступа сможет только стойкое шифрование или шифрование средней стойкости.

Блокировка ID-файла пользователя

По умолчанию, после того как ID-файл открыт, он остается открытым до завершения работы с Notes. Однако можно заблокировать доступ к нему в любой момент. Если вы блокируете ID, вам придется вводить пароль при попытке получения доступа к закрытому ключу (для аутентификации с сервером, подписи сообщения или чтения зашифрованного входящего сообщения). Допустимо также установить блокировку ID после определенного времени бездействия.

Можно вручную заблокировать ID-файл, нажав клавишу F5 или выбрав **File => Tools => Lock ID** (Файл => Программные инструменты => Блокировать ID-файл). Чтобы установить автоматическую блокировку, выполните **File => Preferences => User Preferences** (Файл => Предпочтения => Предпочтения пользователя) и введите число в поле **Lock ID after x minutes of inactivity** (Блокировать ID после x минут бездействия) на вкладке **Basics**.

Сложные пароли

При регистрации новых или повторной сертификации существующих пользователей можно установить для них минимальное качество паролей. Этим вы фактически сообщаете пользователю, что пароль его ID-файла должен иметь качество не ниже заданного вами. По умолчанию для пользователя указано качество 8 по шкале качества паролей, которая градуирована от 0 (не требуется) до 16 (крайне сложный).

Шкала качества паролей приблизительно соответствует количеству символов пароля, но не точно. Пароль качества 8 может содержать 9 символов, если состоит из одного или больше словарных слов, а может иметь всего 6 символов, если включает случайные числа, буквы (в верхнем и нижнем регистре) и знаки препинания.

На ID-файл, с помощью которого зашифрована особо важная база данных, лучше установить максимально сложный пароль, сделав его как можно длиннее, введя в него неудобочитаемые слова и неалфавитные символы. Кроме всего прочего, советуем написать несколько слов, разделенных пробелами. Как правило, такой пароль проще запомнить, чем бессмысленный одиночный пароль.

Несколько паролей

Любой ID-файл можно настроить так, чтобы для его открытия потребовалось несколько паролей. Это средство применяется только для закрытия ID-файлов заверителей и иногда для ID-файлов серверов. ID-файлы пользователей, содержащие несколько паролей, несовместимы с проверкой паролей, поэтому вам придется отключать проверку, если пользователь предъявляет несколько паролей. Но если вы действительно очень хотите закрыть данные от несанкционированного доступа, можно локально зашифровать базу с помощью многопарольного ID-файла.

В многопарольном ID-файле допускается написать сколько угодно паролей и потребовать для открытия определенный их набор. Например, ввести пять паролей так, чтобы пять пользователей знали по одному из них, а для открытия потребовать любые три.

Чтобы установить несколько паролей на доступ к ID-файлу, запустите Domino Administrator. Откройте вкладку **Configuration**. Выберите **Tools => Certification => Edit**

Multiple Passwords (Программные инструменты => Сертификация => Редактирование нескольких паролей). Выберите ID-файл, на который нужно установить несколько паролей. Введите имя человека, который должен знать один из паролей, соответствующий пароль и щелкните по **Add** (Добавить).

Запрет печати, пересылки и копирования

Выше в настоящей главе обсуждалось, как запретить печать, пересылку и копирование документов, созданных с помощью определенной формы: для этого разработчик формы устанавливает свойство **Disable printing/forwarding/copying to clipboard** (Запретить печать/ пересылку/копирование в буфер).

Кроме того, можно запретить печать и копирование отдельных абзацев текста в полях расширенного текстового формата. Поместите курсор в блокируемый абзац и выберите **Text => Text Properties** (Текст => Свойства текста). На вкладке **Hide When** (Скрыть, когда...) отметьте флажки **Printed** (Напечатано) и **Copied to clipboard** (Скопировано в буфер).

Защита SSL в Domino и Notes

Серверы Domino применяют протокол SSL в нескольких случаях:

- О общий Web-сервер Domino, на котором работает приложение электронной коммерции, должен уметь доказать свою достоверность всем пользователям, которые хотят приобрести ваши продукты на сайте. Этому серверу нужен сертификат, подписанный коммерческим заверителем (авторизатором). Сервер, как правило, не требует аутентификации покупателя (ему нужно просто получить с покупателя деньги);
- О другой сервер Domino может разрешить вашим потребителям, поставщикам или деловым партнерам использовать Web-браузер для отслеживания состояния своих счетов или различных финансовых транзакций. Такому серверу необходим сертификат, подписанный либо коммерческим заверителем, либо заверителем Domino (то есть вами). Клиентам, обращающимся к этому серверу, вероятно, тоже следует доказать свою достоверность. В зависимости от важности данных, к которым получает доступ клиент, сервер может либо потребовать имя и пароль, либо провести аутентификацию на основе сертификата, причем сертификат должен быть подписан вами или коммерческим заверителем;
- О еще один сервер способен поддерживать почтовые учетные записи для сотрудников, работающих с почтовыми серверами не Notes, а POP3 и IMAP. Или *еще* он обеспечивает работу закрытого дискуссионного форума, поддерживаемого по протоколу NNTP. Или же этот сервер предоставляет доступ к каталогам для избранных внешних клиентов. Он также вправе разрешить некоторым отправителям сообщений SMTP обращаться к серверу через брандмауэр компании или работать с доверенным LDAP-сервером, чтобы аутентифицировать Internet-клиентов. Все эти серверы могут потребовать от клиентов работать с ними посредством соединения, защищенного по протоколу SSL. Сервер запрашивает аутентификацию с помощью либо имени и пароля, либо сертификата. Обычно частные (некоммерческие) заверители создают сертификаты, которые удовлетворяют этим условиям.

По последнему и, возможно, второму сценариям в списке вам необходимо стать частным заверителем - точно так же, как при регистрации пользователей и серверов системы

Notes. Вы будете формировать сертификаты для своих серверов и некоторых потребителей, поставщиков, деловых партнеров и служащих. В соответствии со всеми сценариями один или несколько ваших серверов должны иметь сертификаты X.509. И наконец, не исключено, что вам придется либо создавать сертификаты X.509 для своих служащих, либо помогать им получать сертификаты от коммерческих заверителей, чтобы они могли шифровать или подписывать почтовые сообщения согласно протоколу S/MIME.

Получение статуса заверителя

Если требуется формировать сертификаты для серверов, пользователей или сторонних лиц, таких как деловые партнеры или поставщики, вам следует получить статус заверителя. Для этого можно использовать приложение Domino Certificate Authority, которое есть на каждом сервере Domino как дополнительный шаблон проектирования. Шаблон называется Domino R5 Certificate Authority в версии R5 и Domino Certificate Authority (6) в версии R6 (в обоих случаях имя файла - csa50.ntf).

Используйте указанный шаблон для создания базы данных Domino Certificate Authority на сервере Domino с поддержкой Web, то есть на сервере, на котором действует серверная задача HTTP. Он станет СА-сервером (сервером авторизатора сертификации). Клиенты будут запрашивать и получать от вас сертификаты через этот сервер. Можно присвоить базе данных и файлу любое имя. После создания базы данных ее необходимо модифицировать следующим образом:

1. Настройте список ACL базы данных.
2. Создайте файл ключей СА и основной сертификат.
3. Заполните профиль заверителя (**Certificate Authority Profile**).
4. Создайте сертификат для СА-сервера. *
5. Настройте на СА-сервере протокол SSL.

Можно снять флажок **Show** (Показывать) в окне **Open Database** (Открыть базу данных), чтобы база не была видна случайным пользователям.

Настройка параметров ACL

Настройте список ACL приложения Certificate Authority так:

- **Default access** (Доступ по умолчанию) - автор с правом создания документов;
- **Administrators who will issue certificates** (Администраторы, которые будут создавать сертификаты) - минимум редактор с правом удаления документов *и назначенной ролью [CAPrilegedUser].

Создание файла ключей СА и основного сертификата

Файл ключей содержит основной сертификат СА и закрытый ключ. Будьте готовы защитить его так же сильно, как вы защищаете ID-файл заверителя своей организации.

Когда вы открываете приложение Certificate Authority, появляется **CASetup navigator** (Навигатор настройки СА). Выберите **Certificate Authority Configuration** (Настройка СА) - на экране слева, затем **Create Certificate Authority Key Ring & Certificate** (Создать файл ключей СА и сертификат) - в центре экрана. Заполните форму в соответствии с табл. 10.5.

Таблица 10.5. Поля формы *Create Certificate Authority Key Ring*

Поле	Комментарии
Key Ring File Name (Имя файла ключей)	По умолчанию присвоено имя CAKey.kyr. Notes сохраняет его в локальной папке данных Notes, если не определен другой путь. Рекомендуется хранить в защищенной папке
Key Ring Password and Password Verify (Пароль файла ключей и проверка пароля)	Компания Lotus рекомендует использовать пароли длиной не менее 12 символов
Key Size (Размер ключа)	Для североамериканской версии Notes или при наличии файла идентификационных данных Verisign Global Server ID (www.verisign.com) длина ключа может быть 512 или 1024 бита. В противном случае она равна 512 бит (средней стойкости)
Common Name (Общее имя)	Выбирайте имя, которое ясно описывает заверителя, например Stillwater CA
Organization (Организация)	Введите имя организации в иерархической системе Notes или что-либо подобное
Organizational Unit (Организационная единица)	Необязательный параметр. Если этот заверитель принадлежит к организационной единице в пределах организации системы Notes либо является заверителем для отдела или подразделения компании, укажите имя организационной единицы, а если оно отсутствует, то название отдела или подразделения компании
City or Locality (Город или район)	Необязательный параметр. Город, в котором расположен авторизатор (заверитель) CA
State or Province (Штат или область)	Полное название штата или области, в которой расположен CA. Минимум три символа
Country (Страна)	Двухбуквенный код ANSI для страны, где располагается CA (например, US для Соединенных Штатов, CA для Канады или UK для Великобритании)

По окончании щелкните по кнопке **Create Certificate Authority Key Ring** (Создать файл ключей CA). Система Notes создаст файл ключей и основной сертификат (подписанный и созданный ею самой) и затем откроет диалоговое окно с итоговыми результатами. Обратите внимание, что срок действия сертификата - 10 лет.

Если после закрытия этого окна вы захотите снова просмотреть файл ключей, выберите **View Certificate Authority Key Ring** (Просмотреть файл ключей CA) на экране слева и затем на панели **Actions** (Операции) приложения Certificate Authority щелкните по **Display CA Key Ring** (Показать файл ключей CA).

Профиль CA

Профиль CA (авторизатора сертификации) - это форма, которая содержит параметры по умолчанию для создания сертификата. Для настройки формы выберите **Certificate Authority Configuration** - на экране слева, затем **Configure Certificate Authority Profile** (Настроить профиль CA) и заполните форму в соответствии с табл. 10.6.

Таблица 10.6. Поля формы *Certificate Authority Profile*

Поле	Комментарии
CA Key File (Ключевой файл CA)	По умолчанию установлено исходное местоположение файла ключей CA. Если вы меняете размещение файла, обновите это поле
Certificate Server DNS Name (Имя DNS сервера)	Введите полное квалифицированное имя домена или псевдоним, зарегистрированный в службе DNS
Use SSL for certificate transactions? (Использовать во время сертификации защиту SSL?)	По умолчанию установлено значение Yes (Да). Если вы не планируете для сертификации применять соединения, защищенные по протоколу SSL, отключите этот параметр
Certificate Server Port Number (Номер порта сервера сертификации)	Если поле пустое, используется порт 80. Если на CA-сервере вы задействуете другой порт, введите его номер
Mail confirmation of signed certificate to requestor? (Подтверждать по электронной почте подпись сертификата)	Устанавливает режим отправки подтверждений на запросы сертификатов. По умолчанию Yes
Submit signed certificates to AdminP for addition to the Directory? (Отправлять подписанные сертификаты процессу администрирования дополнительно к отправке в каталог Domino?)	Определяет поведение, касающееся добавления подписанных сертификатов в каталог Domino. По умолчанию Yes
Default validity period (Срок действия сертификата по умолчанию)	Задаёт срок действия сертификата. По умолчанию 2 года

Создание сертификата для CA-сервера

Приложение Certificate Authority предполагает, что объекты, получающие от него сертификаты, работают с сервером с помощью соединения, защищенного по протоколу SSL. Чтобы это стало возможным, заверитель должен создать сертификат для собственного сервера хоста. Допустимо воспользоваться такой последовательностью действий

В приложении Certificate Authority выберите **Certificate Authority Configuration** - на экране слева, затем **Create CA Server Key Ring & Certificate** (Создать файл ключей CA-сервера и сертификат). Заполните форму в соответствии с табл. 10.7.

Таблица 10.7. Поля формы *Create CA Server Key Ring*

Поле	Комментарии
Key Ring File Name (Имя файла ключей)	По умолчанию присвоено имя keyfile.kyr. Можно назвать его CAserver.kyr или server.kyr. Убедитесь, что используется расширение .kyr для сохранения единообразия

Таблица 10.7. Поля формы **Create CA Server Key Ring** (окончание)

Поле	Комментарии
Key Ring Password and Password Verify (Проверка пароля файла ключей и проверка пароля)	Компания Lotus рекомендует использовать пароли длиной не менее 12 символов
Key Size (Размер ключа)	Для североамериканской версии Notes или файла идентификационных данных от Verisign Global Server ID (www.verisign.com) длина ключа может быть 512 или 1024 бита. В противном случае длина ключа равна 512 бит (средней стойкости)
CA Certificate Label (Метка заверителя сертификата)	Введите описательное название заверителя сертификата сервера. Оно будет отображаться при последующих просмотрах файла ключей сервера
Common Name (Общее имя)	По умолчанию установлено полное квалифицированное имя домена. Некоторые браузеры не могут соединиться, если общее имя сертификата сервера не соответствует имени сервера в DNS. Разрешается воспользоваться любым псевдонимом, для которого имеется запись DNS, например www.stillwater.com
Organization (Организация)	Укажите название организации в иерархии Notes или что-либо подобное
Organizational Unit (Организационная единица)	Необязательный параметр. Если заверитель организационной единицы находится в пределах организации Notes либо обслуживает отдел или подразделение компании, задайте имя организационной единицы или название отдела либо подразделения
City or Locality (Город или район)	Необязательный параметр. Город, в котором расположен CA
State or Province (Штат или область)	Полное название штата или области, где находится CA. Минимум три символа
Country (Страна)	Двухбуквенный код ANSI для страны, где располагается CA (например, US для Соединенных Штатов, CA для Канады или UK для Великобритании)

По окончании заполнения щелкните по **Create Server Key Ring** (Создать файл ключей сервера). Notes предложит ввести пароль на файл ключей CA, так что система сможет использовать закрытый ключ CA, чтобы подписать сертификат сервера. Затем States создаст файл ключей сервера, содержащий сертификат сервера и откроет окно результатов.

Запомните полное имя файла ключей. Следующий необходимый шаг - сделать копию этого файла (и его скрытую копию) для CA-сервера.

Настройка протокола SSL на CA-сервере

На последнем шаге настройки откройте и настройте SSL-порт для протокола HTTP:

1. Скопируйте файл ключей CA-сервера (filename.kyr) и соответствующую скрытую кпию (filename.sth) с рабочей станции, на которой они были созданы, в папку данных сервера Domino.

2. Настройте SSL-порт CA-сервера для HTTP так, чтобы аутентифицировался только CA-сервер. Откройте серверный документ CA-сервера в каталоге Domino. Установите поля на вкладке **Ports => Internet Ports => Web** (Порты => Порты Internet => Web) в соответствии с табл. 10.8.

Таблица 10.8. Некоторые поля на форме **Server => Notes Network Ports => Web**

Поле	Комментарии
SSL key filename (Имя файла ключа SSL)	По умолчанию имя файла keyfile.kyr. При использовании другого имени файла укажите его в этом поле. Если файл находится не в папке данных сервера Domino, задайте полный путь
TCP/IP port number (Номер порта TCP/IP)	По умолчанию применяется порт 80. Этот номер должен соответствовать номеру порта, записанному в профиле заверителя, а также номеру, которым пользуется служба HTTP сервера Domino
TCP/IP port status (Состояние порта TCP/IP)	Установлено значение Enabled (Открыт)
Name & Password (Имя и пароль)	Можно выбрать либо Yes , либо No . Приложение Certificate Authority не требует, чтобы значение было обязательно Yes
Anonymous (Анонимные пользователи)	Если пользователи для соединения с этим сервером будут применять браузер Internet Explorer, то для приложения Certificate Authority необходимо установить значение Yes . В остальных случаях можно задать либо Yes , либо No
SSL port number (Номер порта SSL)	По умолчанию указано значение 443. Этот номер должен соответствовать номеру порта, который использует служба HTTP SSL сервера Domino. Номер не равен 443 только в том случае, когда данный порт применяет прокси-сервер
SSL port status (Состояние порта SSL)	Установлено значение Enabled (Открыт)
Client certificate (Сертификат клиента)	Можно задать либо Yes , либо No . Приложение Certificate Authority не требует, чтобы было установлено значение Yes
Name & Password (Имя и пароль)	Допустимо либо Yes , либо No . Приложение Certificate Authority не требует значения Yes
Anonymous (Анонимные пользователи)	Задается значение Yes . Приложение Certificate Authority требует, чтобы было установлено именно это значение

3. Запустите на CA-сервере службу HTTP. Если она уже запущена, обновите службу с помощью команды `tell http restart`, набрав ее на консоли сервера или в программе Domino Administrator. При необходимости добавьте параметр `http` в список задач в переменной `ServerTasks` файла `notes.ini`.
4. Если клиенты для доступа к приложению Certificate Authority не будут применять браузер Internet Explorer версии 4.0 или более ранней версии, то можно установить свойство базы данных **Web Access: Require SSL connection for the Certificate Authority application** (Доступ через Web: требовать SSL соединения для приложения Certificate Authority).

Последний шаг заставит пользователей для доступа к указанному приложению использовать соединение, защищенное по протоколу SSL. Пользователи, которые применяют IE 4.0 или более ранние версии браузера, не смогут получить доступ, поскольку не в состоянии принимать сертификаты сайта от серверов, для которых у них нет доверенных корневых сертификатов. Сертификата сайта от сервера не будет, пока пользователи не получат его от приложения. А для этого они могут задействовать только порт 80 протоколов TCP/IP - другого выбора нет.

Выполнив все описанные шаги, не забудьте сделать еще одну вещь. Люди и серверы будут обращаться к вам для создания сертификатов. Вам необходимо разработать политику безопасности, чтобы можно было решать - стоит создавать запрашиваемый сертификат или нет. Помните: сертификат служит для других объектов - серверов или пользователей - заверением в том, что объект, указанный в сертификате, является владельцем открытого ключа, заявленного в сертификате. Он также подразумевает, что вы положительно идентифицировали объект, который получил от вас сертификат, и предприняли все необходимые шаги, чтобы убедиться, что предоставляете сертификат не мошеннику. Обязательно учтите все эти положения при разработке порядка выдачи сертификатов.

Помните также, что вы не являетесь коммерческим заверителем. Сертификация объектов - не ваша основная работа. Вы это делаете скорее для удобства своих коллег или поставщиков, деловых партнеров и потребителей своей компании. Вы легко можете отклонить кандидатуру, которая не удовлетворяет вашим требованиям и профилю объектов, установленному для предоставления сертификатов.

И наконец, вам нужна достоверная информация о пользователе, чтобы однозначно идентифицировать его. Если кандидат не предъявляет необходимой информации, можно отказать ему. Когда он соберет запрашиваемые сведения, то снова обратится за сертификатом.

*

Работа авторизатора сертификации

Если вы завершили настройку приложения Domino Certificate Authority, можно заняться сертификацией. Вашими клиентами будут серверы Domino, клиенты Notes, различные типы Internet-клиентов и, возможно, различные типы серверов, не относящихся к Domino. Серверы будут запрашивать серверные сертификаты и забирать их, когда они будут готовы. Клиенты начнут запрашивать клиентские сертификаты и тоже потом их получают. Клиенты Notes могут предоставлять сертификаты, выданные другим заверителем, и запрашивать регистрацию (здесь нужно просто добавить открытый ключ в его персональный документ). Все запросы поступают через базу данных Domino Certificate Authority, запущенную в браузере. Окно базы данных, открытой в браузере, представлено на рис. 10.8.

Получив запрос, вы должны решить, выдавать сертификат этому кандидату или нет. Здесь вступает в силу ваша политика безопасности. Если вы отклоняете запрос, следует объяснить причину отказа. Если вы принимаете запрос, необходимо подписать сертификат и установить срок его действия. Чтобы получить закрытый ключ, надо ввести пароль файла ключей CA.

По умолчанию база данных отправляет сообщение по электронной почте о вашем решении относительно запроса на сертификацию - отказ либо согласие. Положительный ответ включает в себя Pickup ID (ID-файл для получения сертификата). Теперь пользователь может вернуться в базу данных и получить подписанный сертификат.

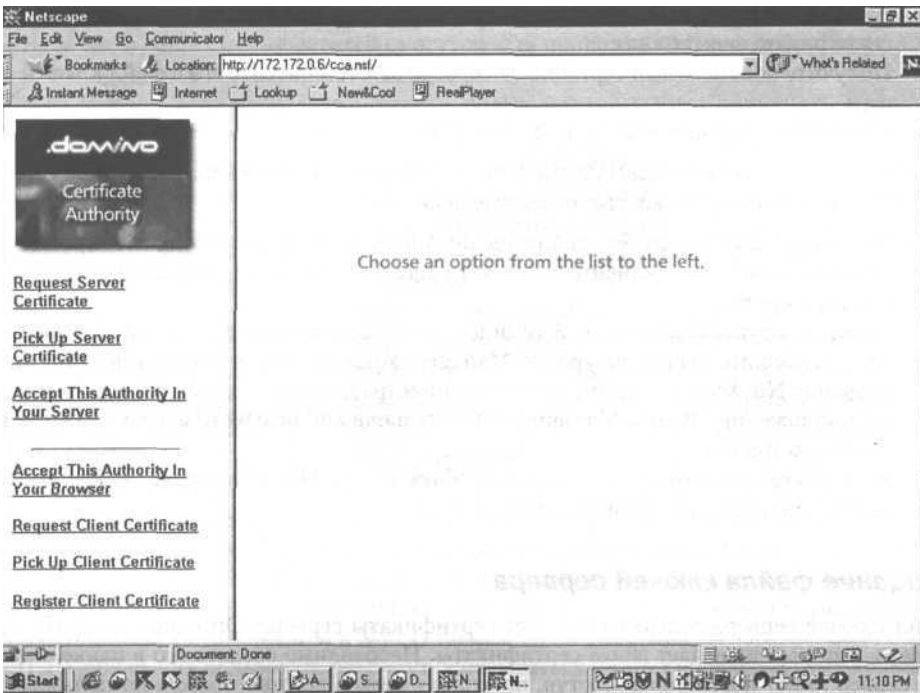


Рис. 10.8. Серверы могут выбирать любой из трех верхних элементов управления, а пользователи - любой из четырех нижних элементов. Самый нижний элемент управления предназначен для клиентов, не использующих Notes

Доступные вам виды отображают обрабатываемые, отклоненные и выполненные серверные запросы на сертификацию, клиентские запросы на сертификацию и клиентские запросы на регистрацию.

Можно также проверить и внести изменения в ваш файл ключей CA.

Настройка сервера Domino для использования протокола SSL

Чтобы использовать протокол SSL на любом сервере Domino, необходимо получить один или более серверных SSL-сертификатов. На сервере нужно открыть один или несколько SSL-портов. В целом процесс подразумевает выполнение следующих шагов:

1. Запустите на сервере процесс HTTP.
2. Установите базу данных Server Certificate Admin на сервере так, чтобы она была настроена для SSL.
3. Создайте файл ключей сервера, который будет хранить SSL-сертификаты сервера.
4. Запросите у авторизатора CA серверный SSL-сертификат.

5. Внесите собственный сертификат CA в файл ключей сервера в качестве основного сертификата заверителя.
6. Получите подписанный сертификат сервера от CA и внесите его в файл ключей сервера.
7. Настройте один или несколько SSL-портов.

База данных Server Certificate Admin (certsrv.nsf) существует на каждом сервере Domino. Ее настройка включает нижеперечисленные действия:

1. Откройте базу данных Server Certificate Admin из Notes или Domino Administrator. Если вы работаете с клиентом Notes, то сделайте закладку, чтобы было легко вернуться в систему.
2. Отредактируйте список ACL. Администраторам, которые будут отвечать за базу данных, разрешите доступ на уровне Manager. Установите для доступа по умолчанию значение No Access - никто, кроме администраторов, не должен обращаться к этому приложению. В поле Maximum Internet name and password access укажите значение No Access.
3. При необходимости снимите флажок Show в окне Open Database, чтобы эту базу данных не видели остальные пользователи.

Создание файла ключей сервера

Файл ключей сервера содержит Internet-сертификаты сервера. Он напоминает ID-файл сервера, который включает Notes-сертификаты. Необходимо создать его в папке, к которой сервер имеет постоянный доступ, поскольку сервер должен постоянно пользоваться ею при обращении к своему ID-файлу. Проблема заключается в том, что можно запустить приложение на своей рабочей станции. Необходимо открыть папку данных на сервере и перенести туда данные со своей рабочей станции. Это достаточно рискованно с точки зрения безопасности. Убедитесь, что никто (кроме вас) не обладает доступом к названной папке.

Применение SSL и S/MIME пользователями Notes

Пользователи клиентов Notes R5 и Notes R6 вместе со своими Notes-сертификатами в ID-файл могут записать сертификаты X.509. Существует две причины, по которым требуются сертификаты X.509. Во-первых, процесс аутентификации с некоторыми Internet-серверами происходит с помощью SSL. Во-вторых, с помощью S/MIME они в состоянии подписывать исходящие сообщения электронной почты и расшифровывать входящие.

Допускается, чтобы пользователи Notes получали сертификат X.509 самостоятельно или чтобы вы как заверитель Domino автоматически выдавали их. Для самостоятельного получения сертификата пользователь должен запросить его у сертифицирующего авторизатора, у стороннего заверителя либо у заверителя Domino. Если пользователю сертификат предоставляет сторонний заверитель, ему надлежит снова зарегистрироваться у вас как заверителя Domino. Чтобы автоматически обеспечивать своих пользователей Notes сертификатами X.509, вам требуется статус заверителя Domino.

Основная идея здесь состоит в том, что если ваши Notes-пользователи захотят прибегнуть к SSL или S/MIME, то вам придется стать заверителем Domino. На самом деле это не совсем так. Пользователь Notes может получить сертификат у стороннего заверителя и затем просто скопировать открытый ключ из сертификата в свой персональный документ

в каталоге Domain. Но если вам присвоят статус заверителя компании, то большую часть работы за вас и ваших пользователей смогут делать приложение Domino Certificate Administrator и процесс Administration Process.

Таким образом, если несколько активных пользователей захотят применять протоколы SSL и S/MIME, то можно им разрешить или помочь получить сертификаты самостоятельно. Но если нужно, чтобы у всех пользователей была возможность работы с SSL и S/MIME, то вам все же лучше приобрести статус заверителя. Необходимо решить один вопрос: будете вы заверителем Domino, создающим сертификаты на основе собственного корневого сертификата¹, или же вы станете сторонним заверителем, создающим сертификаты на основе общепринятого корневого сертификата.

Причина, по которой имеет смысл стать сторонним заверителем, заключается в том, что вы тем самым упростите жизнь своим пользователям. Они будут предоставлять сертификаты либо SSL-серверу для аутентификации, либо пользователям для подписи сообщений. Второй стороне (серверу или пользователю) придется решать, сможет ли она доверять сертификату вашего пользователя. Это значит, что вторая сторона должна установить ваш сертификат заверителя как доверенный корневой сертификат. Для почтовых пользователей это не столь серьезная проблема: их почтовые программы в первый раз просто спрашивают, стоит ли доверять полученному сертификату. Пользователю достаточно ответить утвердительно - и процесс сертификации начнется от данной точки. Но, по всей вероятности, у них уже есть список известных корневых сертификатов коммерческих заверителей, которые определены как доверенные корневые сертификаты - в большинстве программ клиентов Internet (в том числе и в Notes) такие списки установлены заранее. Если сертификаты X.509 ваших пользователей будут основываться на этих общеизвестных корневых сертификатах, то получатели их сообщений никогда не столкнутся с дилеммой относительно истинности сертификатов ваших пользователей.

Если ваши пользователи аутентифицируются на Internet-сервере SSL, у них может возникнуть еще одна большая проблема. Сам сервер не в состоянии принять решение об истинности корневого сертификата вашего заверителя - требуется вмешательство администратора. Он должен обратиться к серверу вашего заверителя, получить ваш корневой сертификат и установить его как доверенный сертификат для этого сервера. Поскольку решение относительно возможности доверия одновременно является и проблемой, и необходимостью, администратору проще отказать. Пользователю остается только обратиться к стороннему заверителю, получить сертификат у него и зарегистрировать его у вас.

Все описанные проблемы будут устранены, если вы сделаете так, чтобы все сертификаты, которые вы выдаете, основывались на сертификатах общеизвестных коммерческих сертифицирующих органов. Другими словами, необязательно быть заверителем организации, достаточно стать, к примеру, заверителем организационной единицы. Вместо того чтобы самому создавать корневой сертификат своего заверителя, вы можете получить его у коммерческого заверителя, а затем применять для создания сертификатов X.509 для своих пользователей с помощью либо СА-приложений, поставляемых коммерческим заверителем, выдавшим вам сертификат, либо собственно приложения Domino Certificate Administrator. (Автор не тестировал ни одно из названных приложений, но нет оснований полагать, что они не будут работать.)

¹ Корневым (root) называется самовыданный сертификат, от имени которого выдаются все остальные сертификаты, действующие в определенной области доверия. - *Прим. ред.*

Например, компания Thawte, один из трех крупнейших коммерческих заверителей (два других - VeriSign и EnTrust), продает так называемые связанные сертификаты. Этот термин соответствует заверителю организационной единицы (OU) в Notes. Компания Thawte предлагает два вида связанных сертификатов. Один - очень дорогой - позволит вам стать коммерческим заверителем с собственными правами. Другой тип стоит чуть дешевле и дает возможность выдавать ограниченное число сертификатов для определенных нужд.

Вам подходит второй тип сертификатов. Вы устанавливаете этот сертификат в Domino Certificate Administrator и затем выдаете своим пользователям и серверам сертификаты, которые сторонними организациями и пользователями будут расцениваться как потомки доверенных коммерческих корневых сертификатов. За дополнительной информацией о программах, которые предлагают коммерческие заверители, обращайтесь на сайты www.thawte.com, www.verisign.com и www.entrust.com.



Службы каталогов используются для предоставления (публикации) пользователям информации об объектах, перечисленных в этих каталогах. Они играют центральную роль в Notes и Domino. В версии R5 компания Lotus усовершенствовала существующие службы каталогов и добавила новые. Для настройки и администрирования эффективно функционирующего домена Notes необходимо понимать роль каждой службы и принципы их совместной работы. Чем больше система Domino, тем важнее эти службы.

Полный список служб каталогов Domino включает в себя:

- О *первичный каталог Domino* (primary Domino directory) - база данных с именем names.nsf, которая имеется в каждом сервере Domino домена Notes и определяет сам домен Notes. Каталог Domino содержит информацию двух типов: о конфигурации сервера, которую использует локальный сервер, и о каталоге для всех серверов и пользователей;
- О *вторичный каталог Domino* (secondary Domino directory). Любой сервер может поддерживать каталоги Domino, отличающиеся от первичного. Всего существует два типа возможных вторичных каталогов:
 - каталоги других доменов. Сервер способен хранить реплики каталогов Domino, которые определяют один или более доменов, отличающихся от собственного домена сервера. Сервер должен поддерживать каталоги других доменов таким образом, чтобы пользователям этих доменов было легко адресовать почту в другие домены;
 - каталоги, не относящиеся к домену. Можно создать каталоги для других целей (не для описания домена Notes). Например, каталог для хранения имен пользователей сети Internet, обращающихся к этому серверу (то есть аутентифицируемых им). Или вторичный каталог для хранения имен пользователей вне Notes-домена, с которыми часто работают пользователи домена. Идея создания таких каталогов заключается в том, чтобы не засорять первичные каталоги информацией о пользователях, не являющихся членами домена;
- О *служба LDAP* сервера Domino. Lightweight Directory Access Protocol (Облегченный протокол службы каталогов) - набор Internet-стандартов, определяющих способы установок, управления и доступа к каталогам по сети TCP/IP. Служба LDAP сервера Domino позволяет клиентам, не использующим Notes, получать с помощью LDAP доступ, осуществлять поиск и обновлять каталоги Domino;

- О *перечень каталога* (Directory Catalog). Эта служба появилась в версии R5. Directory Catalog - сильно сжатый сборник каталогов Domino. Он создан для того, чтобы у каждого пользователя был маленький, но полный список, удобный для быстрого поиска при работе с почтовыми и другими приложениями, когда нужно найти много адресов пользователей. Такое факультативное средство Domino наиболее полезно для больших организаций или для организаций, в которых пользователи не всегда подключены к серверам. Если вы применяете перечень каталога, компания Lotus рекомендует определять два перечня:
 - *серверный перечень каталога* (Server Directory Catalog) - для пользователей, соединенных с сервером;
 - *мобильный перечень каталога* (Mobile Directory Catalog) - для отключенных пользователей;
- О *поддержка каталога* (Directory Assistance). Служба, предоставляющая серверам Domino возможность делать вторичные каталоги Domino и LDAP-каталоги доступными для пользователей при поиске по имени;
- О *каскадные адресные книги* (Cascade Address Book). Устаревшая служба, которая в версии R5 и R6 включена только из соображений обратной совместимости. Через нее пользователи при поиске какого-либо имени получают доступ к вторичным каталогам Domino. Поддержка каталогов обеспечивает большие возможности. Если вы все еще используете каскадные адресные книги, Lotus рекомендует перейти на каталоги;
- О *серверы каталогов* (Directory Server). В Domino R5/6 можно назначить сервер, который предлагает службы каталогов Notes- и LDAP-клиентам. Тем самым эта нагрузка снимается с остальных серверов, чтобы они могли более эффективно предоставлять другие службы. Например, почтовый сервер, не занимающийся службами каталогов, будет более эффективно работать с приложениями электронной почты. В будущих версиях Lotus может расширить серверы каталогов так, чтобы они обеспечивали службы каталогов для других серверов Domino. Если это произойдет, то только серверы каталогов будут хранить реплики первичных каталогов Domino; другие же серверы Domino, если им потребуется информация из каталога Domino, будут обращаться к серверу каталогов.

Кроме того, Lotus Notes поддерживает еще две службы каталогов. Во-первых, каждая копия Notes имеет Personal Address Book (Персональная адресная книга, файл names.nsf), предоставляющую локальной копии Notes и локальному пользователю Notes те же службы, которые каталог Domino (names.nsf) предлагает локальному серверу Domino и всем пользователям домена. Другими словами, эта служба обеспечивает Notes информацией, необходимой для корректной работы, и допускает локального пользователя^ локальному каталогу для хранения собственной контактной информации. Во-вторых, Notes имеет встроенные возможности поддержки LDAP-клиентов, то есть рабочая станция может обращаться к серверам каталогов LDAP.

Службы каталогов Notes рассматриваются в главе 12, а в данной главе детально описана каждая из служб каталогов Domino. Особое внимание уделено их совместной работе и службам, которые вы будете использовать.

Каталог Domino

Каталог Domino является центром системы Notes. Каждый сервер Domino имеет первичный каталог Domino (names.nsf), в котором перечислены члены локального домена Notes.

Каталог Domino - это база данных Notes. Он основан на шаблоне каталога домена (pubnames.ntf).

В версии R4 каталог Domino известен как Public Address Book (Общая адресная книга). В версии R3 и более ранних он носит имя Public Name and Address Book (Общая книга имен и адресов). Поскольку от старых привычек очень трудно избавиться, многие люди, особенно в Lotus, до сих пор обращаются к каталогу с помощью этих имен или акронимов, таких как NAB, PAB и PNAB. Но весь компьютерный мир недавно открыл значение «каталог-ориентированных» приложений. А поскольку Lotus хочет, чтобы мир точно знал истинную функцию общей адресной книги, она начиная с версии R5 называется Domino Directory (Каталог Domino). Мы иногда ссылались на него как на каталог домена (Domain Directory), чтобы подчеркнуть его роль в определении рамок домена и отделить от вторичных каталогов Domino.

Первичный каталог Domino (names.nsf) выполняет две функции. Во-первых, в нем хранятся параметры каждого сервера. Во время работы серверы постоянно обращаются к нему для получения «приказа на марш». Сервер не сможет даже запуситься, если не найдет реплику каталога. Первичный каталог, наряду с текстовым файлом конфигурации notes.ini, указывает серверам, какие службы запускать, как и когда необходимо остановить выполнение этих служб.

Вторая функция, которая представляет для нас основной интерес, - службы каталогов. Первичный каталог домена хранит информацию о каждом сервере, пользователе, локальном почтовом адресате, группе, заверителе и ресурсах локального домена; о том, как и когда передавать почту и реплицировать базы данных; о выходных днях и о соседних доменах. Кроме того, его можно настраивать, поэтому в каталоге домена можно хранить любые данные.

Настройка первичного каталога Domino

При установке первого сервера в домене автоматически создается первичный каталог Domino, и когда в домен добавляется новый сервер, он автоматически получает новую реплику каталога Domino. Таким образом, не требуется создавать реплики каталогов в домене. В предыдущих версиях Notes пользователи часто формировали локальные реплики общей адресной книги, чтобы было проще отправлять почту пользователям своего домена Notes. Сейчас в этом нет необходимости, если настроен мобильный перечень каталога (см. ниже).

Однако, поскольку первичный каталог Domino очень важен для корректной работы домена Notes, нужно правильно его настроить. Во-первых - как главное правило - следует ограничить доступ к каталогу. Во-вторых, обеспечить частую репликацию каталога на серверы домена. В-третьих, убедиться, что документы профилей настроены верно. И наконец, требуется отслеживать изменения в списках ACL и отказы при репликации.

Настройка списка ACL

Как правило, надо ограничить права доступа пользователей к первичному каталогу Domino. С помощью шаблона каталога Domino это сделать очень легко. По умолчанию большинство пользователей имеют уровень доступа **Author** (Автор), но не могут создавать и удалять документы - им разрешено только редактировать определенные поля «персональной информации» в собственных персональных документах. Создавать и удалять документы в состоянии лишь те пользователи, которым это поручено. Если нужно минимизировать вероятность сбоев системы защиты и возникновения ошибок в результате работы

неопытного пользователя, стоит ограничить права отдельных администраторов на внесение изменений в каталог Domino, настроив их права в списке ACL.

Чтобы создавать документы, пользователю требуется иметь уровень доступа **Author** и выше к списку ACL и право **Create Documents** (Создание документов), а также обладать одной или несколькими ролями **Creator** (Создатель) - см. главу 10. Редактировать документы можно, если выполняются следующие условия:

- О для создания только определенных классов документов (персональных, групп, серверных и всех остальных) установите в ACL уровень доступа пользователя **Author** с правом **Create document** и выберите соответствующие роли **Creator**;
- О если планируется редактировать только определенные классы документов, задайте в ACL уровень доступа пользователя **Author** и выберите соответствующие роли **Modifier**. Если пользователю разрешено удалять такие же типы документов, предоставьте ему право **Delete document** (Удаление документов);
- О чтобы редактировать лишь выбранные документы, укажите в ACL уровень доступа пользователя **Author** и добавьте имя пользователя в поле **Administrators** (Администраторы) редактируемых документов. Если пользователю разрешено удалять такие же типы документов, предоставьте ему право **Delete document**.

Дополнительно можно ограничить распространение изменений по сети, понизив в ACL права ваших серверов: например, установить только для серверов-концентраторов уровень доступа **Manager**, а для остальных серверов - уровень **Editor**. Тогда все изменения ACL или вида каталога Domino на радиальном сервере будут локализованы, поскольку сервер-концентратор заблокирует их. Единственная проблема заключается в том, что существует риск не узнать о произошедшем изменении, как в случае их репликации на другие серверы.

И наконец, можно настроить серверы таким образом, чтобы они выдавали уведомления о внесении любых изменений в списки ACL каталога Domino. Для этого нужно создать монитор изменений ACL и уведомление о событии (Event Notification) в базе данных Statistics & Events. Монитор изменений ACL запустит на выбранных серверах задачу Event для отслеживания изменений в ACL базы данных names.nsf и для немедленного сообщения о возникновении события типа Security (Безопасность) в случае такого рода изменений. Event Notification сообщает установленным вами способом о возникновении выбранных событий. Более детальное рассмотрение этих вопросов вы найдете в главе 18.

Настройка репликации

Что касается первичного каталога Domino, то компания Lotus рекомендует выполнять его репликацию (и репликацию базы данных Administration Requests) не реже, чем раз в 30 минут. Поскольку необязательно так часто реплицировать остальные базы данных, можно настроить специальные документы соединения для репликации этих двух баз (и любых других баз, которым нужно часто реплицировать изменения).

Предусмотрены два способа. Во-первых, можно сформировать документы соединения (Connection document), указывающие на эти две базы данных (names.nsf и admin4.nsf), в поле **Replicate** (Реплицировать) окна **Files/Directories** (Файлы/каталоги) или установить в параметрах репликации (Replication Settings) уровень приоритета таких баз как **High Priority** (Высокий приоритет) и затем настроить документы соединения на репликацию только тех баз данных, которые имеют приоритет **High Priority**.

Можно также задать, чтобы в случае отказа при репликации каталога Domino через определенные интервалы времени выдавалось сообщение. Для этого создайте Replication

Профиль каталогов Domino

Domino Directory Profile - Domino Administrator

File Edit View Create Actions Test Help

Administration Stillwater's Directory - Server/Mail Users Domino Directory Profile X

administrator

Save and Close

DOMINO DIRECTORY PROFILE

Basics

Domain defined by this Domino Directory: Stillwater

Directory Catalog database name for domain:

Sort all new groups by default: No

Use more secure Internet Passwords: No

Allow the creation of Alternate Language Information documents: Yes

List of administrators who are allowed to create Cross Domain Configuration documents in the Administration Process:

Requests database:

Таблица 11.1. Поля профиля каталогов

Поле	Комментарии
Domain defined by this Domino Directory (Домен, определяемым данным каталогом Domino)	Для вторичных каталогов, которые не определяют домены, оставьте данное поле пустым
Directory Catalog database name for domain (Имя базы данных перечня каталогов домена) в R5 или Condensed server directory catalog for domain (Сжатый серверный перечень каталогов домена) в R6	Это имя перечня каталогов на сервере, заданное по умолчанию (см. ниже в настоящей главе). В версии R6 явно указано на сжатие данных в перечне каталогов

Таблица 11.1. Поля профиля каталогов (окончание)

Поле	Комментарии
Sort all new groups by default (Сортировать новые группы по умолчанию)	По умолчанию установлено значение No. Если его оставить, можно сортировать группы, открывая их в режиме редактирования и выбирая сортировку. Если вы предпочитаете сортировать группы по вхождению в тот или иной список, укажите Yes
Use more secure Internet Passwords (Использовать более защищенные пароли Internet)	Если служба HTTP работает на серверах, на которых установлена версия Domino R4.5 или более ранняя, можно оставить значение No. В остальных случаях поменяйте на Yes
Allow the creation of Alternate Language Information documents (Разрешить создание документов с информацией об альтернативных языках)	Этот параметр имеет значение, когда на одном или нескольких серверах домена работает поддержка LDAP. Если определено значение Yes , то возможен поиск информации на разных языках (см. ниже)
List of administrators who are allowed to create Cross Domain Configuration documents in Administration Process Requests database (Список администраторов, которым разрешено создавать документы междоменной конфигурации в базе данных запросов процесса администрирования)	В документы междоменной конфигурации (Cross Domain Configuration), которые вы создаете в базе данных административных запросов Administration Requests - admin.nsf, перечисляются запросы от других доменов Notes, которые примет на обработку процесс Administration Process. Внесите в этот список всех, кто имеет право создавать документы междоменной конфигурации. Пользователи с уровнем доступа Manager в любом случае могут создавать такие документы, поэтому их не нужно заносить в список

Вторичные каталоги Domino

Администраторы часто обращаются к вторичным каталогам Domino по двум причинам.

Во-первых, некоторые компании применяют несколько доменов Notes. Чтобы пользователям каждого домена было проще адресовать почту своим коллегам в других доменах, администраторы в таких компаниях создают реплики всех каталогов одного домена на серверах других доменов. Более подробно это обсуждается ниже в настоящей главе. •

Во-вторых, администраторы иногда формируют каталоги, которые не определяют домены Notes, а просто хранят информацию о каталоге. Рассмотрим два случая. Первый - когда компания обслуживает Web-сайт, где пользователю надо должным образом зарегистрироваться. Каждый зарегистрированный пользователь имеет персональный документ. Второй случай чаще всего касается маленьких компаний, создающих персональные документы для всех пользователей, с которыми они работают (поставщики, деловые партнеры, потребители и т.д.).

В обоих случаях нужен персональный документ для людей, которые на самом деле не являются членами домена. Чтобы такие документы не попали в каталог домена, администраторы с помощью шаблона pubnames.nsf формируют вторичные каталоги и вносят в них персональные документы. Потом они настраивают поддержку каталогов и перечень каталога, чтобы членам данного домена были доступны имена сотрудников компании. Более подробно это описано ниже в данной главе.

При создании вторичных каталогов Domino убедитесь, что они имеют уникальные имена (например, Webnames.nsf или othernames.nsf)- Кроме того, необходимо присвоить им описательные заголовки (скажем, Web Users или Other Users), чтобы потом было легко понять, что представляет собой тот или иной каталог.

LDAP-службы каталогов

Начиная с версии R4.6 компания Lotus сделала каталог Domino (в версии 4.6 он известен как общая адресная книга) доступным для пользователей не-Notes, встроив в сервер Domino Internet-стандарт LDAP (Lightweight Directory Access Protocol - облегченный протокол службы каталогов). Domino R4.6 поддерживает LDAP версии 2, а Domino R5/6 - LDAP версий 2 и 3.

Если на сервере Domino функционирует служба LDAP, вы передаете выбранные составляющие одного или более каталогов Domino клиентам LDAP и другим серверам LDAP. При этом ваши пользователи имеют некоторые преимущества. Приведем несколько примеров:

- допустимо предоставить службы каталогов Domino своим пользователям почты протоколов POP3 и ШАР таким образом, что подобно коллегам, применяющим Notes, они смогут просматривать адреса людей и баз данных, которым нужно отправить сообщения;
- люди (не имеющие отношения к вашему домену), которые хотят отправить сообщение пользователю вашего домена, вправе просматривать почтовые адреса пользователей и баз данных в каталоге вашего домена;
- LDAP-совместимые приложения могут просматривать информацию в ваших каталогах;
- сторонние серверы (такие, как Netscape Enterprise Web Server) способны применить информацию каталога вашего домена для аутентификации ваших пользователей. Например, сервер сравнивает имя и пароль или имя и сертификат, полученные от одного из ваших пользователей, с информацией, имеющейся в персональном документе этого пользователя, чтобы удостовериться в истинности предоставленных сведений.

Domino поддерживает следующие средства LDAP:

- расширенный поиск и перенаправление. Когда LDAP-клиент запрашивает сервер Domino, он сначала производит поиск в первичном каталоге Domino, после чего при необходимости предпринимает расширенный поиск во вторичных каталогах Domino Directory. Кроме того, если сервер Domino определяет, что информация, которую ищет клиент LDAP, возможно, находится на стороннем сервере LDAP, то сервер LDAP Domino вправе обратиться к клиенту на этом стороннем сервере. Оба эти средства, известные как «расширенный поиск» и «перенаправление», являются стандартными средствами LDAP-сервера. Чтобы их настроить, следует разрешить работу службы Directory Assistance (Поддержка каталога) на сервере (см. ниже);
- параметры аутентификации. Если вы не хотите, чтобы анонимные пользователи просматривали ваши каталоги Domino, потребуйте аутентификацию клиента с помощью имени и пароля или на основе сертификата SSL. Кроме того, можно настроить LDAP так, чтобы клиент LDAP при подключении к серверу сам аутентифицировал сервер

- с помощью SSL. И наконец, Domino поддерживает протокол SASL (Simple Authentication Security Layer - простой уровень аутентификации и защиты) - RFC 2222;
- О доступ для добавления, изменения и удаления. Можно позволить LDAP-клиентам добавлять, изменять и удалять записи каталога. Например, пользователь способен самостоятельно изменять свой пароль, или разрешено использование клиента LDAP для удаленной поддержки;
 - О публикация, проверка и расширение схем. Если говорить простыми словами, то схема Domino - это список документов и полей в каталоге Domino, к которым предоставлен доступ LDAP-пользователю, но только для чтения либо для чтения/записи. Публикация и проверка схем позволяет клиентам определять, к какой информации они имеют доступ и каковы права доступа, а расширение схемы - изменять документы и поля, которые публикуются. Есть возможность задавать новые формы, подформы и поля непосредственно в каталогах, и если делать это должным образом, то не надо беспокоиться, что все изменения будут удалены при обновлении версии Domino;
 - О выбор языковой поддержки. Если вы создадите документы Alternate Language Information (Информация об альтернативном языке), то служба LDAP сервера Domino будет выполнять поиск на указанном вами языке. Документы выбора языка относятся к персональным документам и имеют тот же набор полей, а поля содержат такую же информацию, как и их эквиваленты в персональном документе, но на других заданных языках. Имейте в виду - это не равносильно поддержке выбора имени/языка в ID-файле пользователя. Допускается установить одну или несколько служб. Существенная разница заключается в том, что для ID-файла пользователя назначается только один альтернативный язык, а документов Alternate Language Information для каждого персонального документа можно создать множество (все они будут соответствовать разным языкам).

Domino также поддерживает некоторые службы LDAP, которые не требуют установки на сервере поддержки LDAP. Все серверы Domino R5/6 в состоянии работать со следующими LDAP-службами:

- О серверы Domino могут использовать сторонние каталоги LDAP для аутентификации Web-пользователей, необходимо лишь настроить службу Directory Assistance (Поддержка каталога);
- О в списке ACL баз данных допустимо обращаться к группам из сторонних LDAP-каталогов. Для этого также требуется настройка службы Directory Assistance;
- О серверы Domino включают специальную утилиту командной строки (ldapsearch.exe для Windows), с помощью которой осуществляется LDAP-поиск; #

СГ-с помощью LDIF-формата файлов можно импортировать объекты из другого каталога LDAP в каталог Domino (см. главу 6).

В дополнение к этому серверы Domino R6 обеспечивают следующие службы LDAP:

- О Central Directory Architecture (Архитектура центрального каталога), которая позволяет сформировать селективную реплику основного каталога Domino, содержащую только сведения о серверах домена;
- О расширенные списки ACL (Extended ACL - xACL), предоставляющие дополнительные возможности управления в каталогах Domino Directory и Extended Directory Catalog;
- О пользовательские фильтры для поиска в удаленных каталогах LDAP.

Добавим, что Lotus Notes является LDAP-клиентом. Можно установить в Lotus Notes для LDAP-каталогов учетные документы (Account document). Несколько таких документов для коммерческих LDAP-каталогов уже существуют в дистрибутиве Notes (см. главы 5, 6 и 13).

Что такое LDAP

Lightweight Directory Access Protocol определяет набор стандартных методов и правил доступа к службам каталогов X.500 без (по словам его авторов) «выполнения требований протокола DAP (Directory Access Protocol - протокол доступа к каталогу) к ресурсам». Протокол службы каталогов, X.500, был разработан в конце 80-х годов с огромными надеждами и перспективами на стандартизацию служб каталогов. Но он не нашел широкого распространения, в частности из-за большой стоимости реализации.

LDAP предназначен для сокращения расходов, связанных с реализацией X.500, благодаря (кроме всего прочего) передаче данных между службами X.500 и клиентом LDAP с помощью семейства протоколов TCP/IP. LDAP версии 1 увидел свет в 1993 году (далее - RFC 1487). Версия 2 появилась в 1995 году (далее RFC 1777). Текущая, третья версия была выпущена в 1997 году (далее RFC 2251).

Чтобы понять, что такое LDAP, необходимо разобраться в принципах служб каталогов X.500. Это не должно вызвать трудностей, поскольку Notes приняла все требования X.500 еще в версии R3, когда были сформированы иерархическая организация и различающееся именование. X.500 требует, чтобы объекты каталогов располагались в соответствии с иерархией, а их имена уникально идентифицировали объект и отличали его от других объектов каталога. Система Notes показывает хороший пример реализации этих требований, поскольку применяет иерархическую систему организации пользователей и серверов и отображает иерархическое положение в полном различающемся имени пользователей и серверов. Другой хороший пример - служба каталога NDS компании Novell. Если вам ясны правила организации и присвоения имен в Notes и NDS Novell, то вы на полпути к пониманию принципов X.500.

Для полного понимания X.500 следует выучить специфический жаргон. Ни Notes, ни NDS Novell не прибегают к жаргону X.500, хотя обе системы отвечают требованиям X.500. LDAP употребляет терминологию X.500, поэтому надо уметь сопоставлять термины X.500 и Notes.

Каталоги X.500 известны как DIT (Directory Information Trees - деревья информации о каталогах). Они включают в себя объекты, являющиеся членами классов объектов, и атрибуты, задаваемые классом объекта. Атрибуты объекта содержат определенные значения.

Каталог Domino - это, по сути, DIT в X.500. Формы в каталоге Domino соответствуют классам объектов. Например, форма **Person** определяет класс **Person**.

Документы Notes, создаваемые с помощью форм Notes, фактически являются объектами, членами класса. Персональные документы - это объекты класса **Person**; документы группы - объекты класса **Group** и т.д.

Поля эквивалентны атрибутам. Значения поля - это значения, которые Domino предоставляет LDAP-клиенту, когда тот запрашивает атрибуты всех объектов, имеющих заданные свойства.

В табл. 11.2 показаны соответствия объектов LDAP и Notes.

Таблица 11.2. Соответствия терминов LDAP/DAP и Notes

Термин LDAP	Термин Notes
Directory Information Tree (Дерево информации о каталоге)	Domino Directory (Каталог Domino)
Object class (Класс объекта)	Form (Форма)
Object (Объект)	Document (Документ)
Attribute (Атрибут)	Field (Поле)
Attribute value (Значение атрибута)	Field value (Значение поля)

Соответствие между формой и классом LDAP не является взаимно однозначным. Более того, в каталоге Domino только персональные, групповые, серверные документы и документы почтовой базы данных изначально соответствуют классам объектов и лишь некоторые поля этих документов - атрибутам LDAP. Но спецификация протокола LDAP не требует, чтобы внутренняя структура каталога Domino была организована аналогично структуре каталога LDAP. Этому стандарту достаточно, чтобы сервер Domino отвечал на LDAP-подобные запросы известным образом. И Domino удовлетворяет данному требованию.

Настройка службы LDAP сервера Domino

Чтобы настроить сервер для поддержки службы LDAP, необходимо сначала установить следующие элементы:

- О протоколы TCP/IP. Служба LDAP основана на этих протоколах, а значит, на любом сервере Domino, на котором включена поддержка LDAP, должна работать поддержка протоколов TCP/IP;
- О регистрация DNS. LDAP-клиенты будут обращаться к службе DNS для получения адреса LDAP-сервера, поэтому необходимо зарегистрировать LDAP-сервер на локальном DNS-сервере. Если запросы могут поступать от пользователей и через Internet, следует подключить сервер к сети Internet и зарегистрировать его на DNS-сервере провайдера. В качестве имени сервера допускается выбирать любые псевдонимы, например ldap.planetnotes.com;
- О полнотекстовый индекс. Создайте на LDAP-сервере полнотекстовый индекс первичного каталога Domino и всех вторичных каталогов, которые должны быть доступны LDAP. В противном случае поиск будет идти очень долго;
- О глобальный документ домена. Если домен определяет несколько глобальных документов домена (Global Domain document), то службы определяют один из них как документ, применяемый по умолчанию. Откройте его в режиме редактирования и установите в поле **Use as default Global Domain** (Использовать по умолчанию как глобальный домен) значение **Yes**.

Если вы выполните указанные выше требования (а также некоторые факультативные, о которых речь пойдет позже), то можете включать службу LDAP. Чтобы запустить ее вручную, введите команду load ldap с консоли сервера или выберите **Server Status => Tools => Task => Start => LDAP Server** (Сервер => Состояние => Программные инструменты => Задачи => Запустить => LDAP-сервер) в окне Domino Administrator. Для выключения LDAP можно воспользоваться командой tell ldap quit или в окне Domino Administrator указать

Server => Status, отметить службу и выполнить **Tools => Task => Stop** (Программные инструменты => Задачи => Остановить). А чтобы служба LDAP запускалась при включении сервера и работала постоянно, необходимо записать в переменную ServerTask файла сервера notes.ini значение LDAP.

После того как вы настроили и запустили службу LDAP, можно тестировать, настраивать ее дополнительно и устанавливать клиентские программы для доступа к этой службе. Для тестирования LDAP необходимо обратиться к серверу с помощью либо клиентской программы LDAP, либо утилиты ldapsearch, которая поставляется вместе с сервером Domino и программой Domino Administrator.

Утилита ldapsearch

На начальном этапе сложно освоить утилиту ldapsearch по двум причинам. Во-первых, она корректно работает только в том случае, когда правильно указаны все параметры. Во-вторых, компания Lotus в версии R5 не предоставила документацию по ней (в справочном файле Domino Administrator R6 утилита описана очень подробно). Документированная утилита называется lsearch и имеет имя файла lsearch.exe, где ? означает различные начальные символы для разных операционных систем сервера. Но кажется, что программисты забрали у разработчиков документации современную версию. В последнюю минуту они вставили в версию R5 Domino для Windows NT файл ldapsearch.exe, а во всех остальных версиях до R5.0.1, в которой снова работает утилита ldapsearch, вообще нет средств поиска.

Команда ldapsearch имеет следующий синтаксис:

LDAPsearch[параметры] Filter [атрибуты]

[параметры] - всего существует свыше 20 параметров. Для тестирования сервера необходимо знать только один —h hostname, где hostname - либо имя хоста LDAP-сервера (или его псевдоним), либо (если еще не задано имя хоста в DNS) его IP-адрес. При введении нескольких параметров они разделяются двоеточием (:).

Filter (Фильтр) - это любое выражение, которое распознает LDAP. Он указывает каталог, который вы ищете. Например, sn=surname, где surname - фамилия пользователя, которого вы ищете (во время тестирования можно указать свою фамилию).

[атрибуты] - список значений полей, которые нужно получить. Элементы списка разделены пробелами. Если параметр не указывать, то в результате поиска (в случае удачного его выполнения) будут выведены все поля, которым присвоены свойства LDAP.

Таким образом, чтобы протестировать LDAP-сервер пользователя Kirkland, запускается следующая команда:

ldapsearch -h osprey.planetnotes.comsn=kirkland

Можно записать эту команду так:

ldapsearch-h 192.168.0.6 sn=kirkland

В любом случае, если все работает правильно, возвращается следующий список пар атрибут=значение:

```
CN=Rob Kirkland,OU=MarchGreek,O=Stillwater
o=Stillwater
ou=MarchGreek
cn=Rob Kirkland
```

```

mail=Rob_Kirkland@planetnotes.com
objectclass=top
objectclass=person
objectclass=organizationalPerson
objectclass=inetOrgPerson
objectclass=dominoPerson
certificate=03005302 3672FEOElAG0162AG0020DD71CEDEF03G0030200 01208600
67061100 516725G0 024FG002 6D061100 50672500 08D310002B6A2585 01A07700
67061100 516725G0 024FG002 6D061100 50672500 08D31000 2B6A2585 4F553D4D
61727368437265656B2F4F3D5374696C6C776174657
publickey=0200526F 62204B69 726B6C616E64G043
givenname=Rob
sn=Kirkland
fullname=CN=RobKirkland,OU=MarchGreek,O=Stillwater
fullname=CN=RobKirkland
shortname=rKirklan
maildomain=Stillwater

```

Здесь команда `ldapsearch` не рассматривается детально. Если в документации Lotus заменить `ldapsearch` на `lsearch`, все остальное будет работать так, как написано (в версии R6 не осталось никаких упоминаний о `lsearch`). Создание формул для фильтров аналогично спецификации поиска в Notes. Можно использовать стандартные операторы сравнения: равно (=), приблизительно равно (~=), больше (>), меньше (<), больше или равно (>=), меньше или равно (<=) и т.д., а также некоторые логические операторы: И (&), ИЛИ (||) и НЕ (!).

КонфигурированиеLDAP

Если оставить параметры по умолчанию, LDAP работает достаточно хорошо во многих случаях. Однако существует набор переменных, которые можно изменить в документах параметров по умолчанию, серверных документах и в `notes.ini`, чтобы задать режим работы LDAP.

Основные параметры, действующие в пределах домена, определяют конфигурацию домена по умолчанию. Если вы еще не сформировали такой документ, сделайте это сейчас следующим образом. В окне Domino Administrator на вкладке **Configuration** выделите сервер и выберите **Server => Configurations => Add Configuration** (Сервер => Конфигурации => Добавить конфигурацию). Установите в поле **Use this settings as the default settings for all servers** (Использовать эти параметры по умолчанию для всех серверов) вкладки **Basics** значение **Yes**. Если такого поля нет, значит, документ уже создан. Domino позволяет создавать только один подобный документ. Появляется вкладка **LDAP**. Теперь можно занести требуемые значения в появившиеся поля.

Но сначала сохраните и закройте документ. Если теперь вы откроете окно **Directory** в клиенте Notes или вкладку **Files** в окне Domino Administrator, то увидите новый документ конфигурации в разделе **All servers** (Все серверы). Если вы создали новый документ в Domino Administrator, то на виде **Server => Configurations** и **Messaging => Configurations** он не будет показан. Он появляется только на виде **Directory => Directory Settings**, причем выводится только вкладка **LDAP** (отмеченная здесь как **LDAP Settings**).

Элементы вкладки **LDAP Settings** и их применение описаны в табл. 11.3.

Таблица 11.3. Настройка ШАРВ в рамках домена

Поле	Комментарии
Anonymous users can query (Анонимные пользователи могут запрашивать)	Состоит из списка полей, значения которых могут возвращаться по запросам пользователей без аутентификации. Разрешается добавлять и удалять имена полей
Allow LDAP users write access (Разрешить LDAP-пользователям доступ для записи)	По умолчанию установлено значение No. Чтобы разрешить LDAP-пользователям добавлять, изменять и удалять записи, надо поменять на Yes
Timeout (Время ожидания)	Время тайм-аута (в секундах) для поиска. По истечении этого времени поиск автоматически прекращается. По умолчанию задано значение 0: поиск продолжается до тех пор, пока не будут просмотрены все каталоги
Maximum number of entries returned (Максимальное число возвращаемых записей)	По умолчанию 0, то есть максимальное значение не установлено. Поиск возвращает все найденные записи
Minimum characters for wildcard search (Максимальное число символов при поиске по подстановочному шаблону)	По умолчанию 1. Это означает, что для поиска достаточно одного символа, перед которым стоит звездочка (*). Другими словами, записи sn=* для поиска недостаточно. В очень больших каталогах данное число лучше увеличить
Allow Alternate Language Information (Разрешить многоязыковую поддержку)	Разрешает поиск сведений в документах информации об альтернативных языках (Alternate Language Information). Если указано значение Yes , автоматически активизируется свойство Optimize LDAP queries (Оптимизировать запросы LDAP), которое в свою очередь активизирует набор скрытых видов каталогов
Rules to follow when this directory is the primary directory, and there are multiple matches on the distinguished name being compared/modified (Правила действия в случае, если каталог является первичным и присутствует несколько совпадающих различающихся имен при операции сравнения или изменения)	Применяется только к запросам, заставляющим Domino изменять совпадающие записи. По умолчанию задано значение Don't modify any (Не изменять). Можно установить также Modify first match (Изменить первую найденную запись) и Modify all matches (Изменить все записи)

Можно сделать так, чтобы параметры из табл. 11.3 действовали в рамках всего домена. Они будут влиять на LDAP-серверы только внутри одного домена. Один из параметров (который является исключением из общего правила) перекрывает значения в отдельных документах конфигурации. Если в поле **Allow Alternate Language Information** установить значение Yes, то поле **Optimize LDAP queries** на вкладке Basics документа конфигурации становится доступным. Это правило распространяется на документы конфигурации всех серверов

Установка значения **Yes** заставляет LDAP обращаться к четырем скрытым видам для каталога: \$LDAPS, SLDAPG, SLDAPCN и SLDAPHIER. Последняя буква (или сочетание букв) в имени вида (S, G, CN и HIER) отображает порядок сортировки в каждом из видов.

То есть \$LDAPS применяет сортировку по фамилии (S - surname), SLDAPG - по имени (G - given name), SLDAPCN - по общему имени (CN - common name) и SLDAPHIER - по иерархическому имени (**HIER** - hierarchical name, полное различающееся иерархическое имя). Эти виды ускоряют обработку LDAP-запросов, разрешают поддержку поиска на разных языках и экспорт объектов, не являющихся пользователями и группами.

В каждом серверном документе допустимо установить порты LDAP и требования аутентификации. Можно выбрать **Ports => Internet Ports => Directory** и открыть или закрыть порт LDAP TCP/IP либо порт LDAP SSL. Разрешается изменить номера портов и задать требуемый тип аутентификации. Поля и доступные значения для них приведены в табл. 11.4.

Таблица 11.4. Поля LDAP Port и Authentication

Поле	Комментарии
TCP/IP port number (Номер порта TCP/IP)	По умолчанию указан номер 389, то есть общеизвестный порт для LDAP поверх TCP/IP. Если вы изменяете номер порта, ваши клиенты тоже должны будут изменить его. В противном случае они не смогут его найти
TCP/IP port status (Состояние порта TCP/IP)	По умолчанию задано Enabled (Открыт). Это значит, что пользователи могут делать запросы серверу без точной идентификации с помощью SSL. Допускается установить значение Disabled (Закрыт). При этом все запросы через данный порт будут отклоняться. Если задать Redirect to SSL (Направить на SSL), то сервер отправит пользователя к порту, указанному в поле SSL port number
Authentication options: Name & password (Параметры аутентификации: имя и пароль)	По умолчанию установлено значение Yes : пользователи могут аутентифицироваться по имени и паролю. Если поменять на No, имени и пароля будет недостаточно
Authentication options: Anonymous (Параметры аутентификации: для анонимного доступа)	По умолчанию - No. Это значит, что LDAP-пользователи могут запрашивать сервер без аутентификации. Если пользователь попытается сделать что-либо, запрещенное для анонимных пользователей, сервер потребует аутентификации или откажет пользователю - в зависимости от значений остальных параметров данной формы
SSL port number (Номер порта SSL)	По умолчанию указан номер 636, то есть общеизвестный порт для LDAP поверх SSL. Если вы меняете номер порта, ваши клиенты тоже должны будут изменить его. В противном случае они не смогут его найти
SSL port status (Состояние порта SSL)	По умолчанию задано Disabled . Это значит, что пользователи перед запросом не могут аутентифицировать сервер с помощью SSL. Можно установить Enabled , предварительно настроив протокол SSL на сервере (см. главу 10)
Authentication options: Client certificate (Параметры аутентификации: сертификат клиента)	По умолчанию указано No: после того как сервер аутентифицирован, он не будет требовать аутентификации пользователя на основе сертификата. Чтобы активизировать аутентификацию пользователя, установите значение Yes . Если вы активизируете это поле и отключите следующие два, то

Таблица 11.4. Поля *LDAP Port* и *Authentication* (окончание)

Поле	Комментарии
Authentication options: Client certificate	пользователь для аутентификации должен будет предоставить заверенный сертификат. Если активизировано данное поле и одно или оба следующих, то пользователь аутентифицируется с помощью сертификата. Если такая попытка оказывается неудачной, сервер предоставляет ему доступ как анонимному пользователю до тех пор, пока пользователь не захочет сделать что-нибудь запрещенное. В этом случае сервер запросит имя и пароль
Authentication options: Name & password (Параметры аутентификации: имя и пароль)	По умолчанию - No: когда сам сервер аутентифицирован, он не будет требовать аутентификации пользователя с помощью имени и пароля. Чтобы активизировать аутентификацию пользователя, установите значение Yes. Необходимость такой аутентификации зависит от значений в двух других полях
Authentication options: Anonymous (Параметры аутентификации: для анонимного доступа)	По умолчанию — Yes. Это значит, что, после того как сам сервер аутентифицирован, он предоставит клиенту доступ без аутентификации. Если определить значение No, пользователю придется обратиться к порту SSL и пройти аутентификацию одним из вышеописанных способов

И наконец, в файле `notes.ini` каждого сервера можно записать следующую переменную:

```
LDAP_Strict_RFC_Adherence=1
```

При этом LDAP-клиентам придется проходить аутентификацию с помощью полного различающегося имени пользователя. Если же переменную удалить или задать для нее значение 0 (установлено по умолчанию), то пользователи смогут аутентифицироваться посредством своих уникальных имен, отображаемых в поле **FullName** или **ShortName** персонального документа.

Расширение и мониторинг служб LDAP

Мы не станем рассматривать вопросы расширения схемы Domino. На это нет ни времени, ни свободного места в книге. Желаящим изучить эти темы рекомендуем обратиться к книге Кендры Боукер (Kendra Bowker) «Exploring LDAP Features in Domino R5», издательства Iris Today, представленной на www.notes.net. июль 1999 (надеемся, что не менее подробное издание появится и для версии R6).

Для отслеживания статистики LDAP можно использовать набор команд консоли управления сервером Domino. Например, команда `show tasks` отображает количество текущих активных сеансов LDAP. Команда `show port portname`, где `portname` - это имя порта TCP/IP, который применяет служба LDAP, показывает статистику о трафике и количестве ошибок порта. Команда `show stat ldap` выводит список примерно 30 параметров производительности LDAP-сервера. Статистику о работе LDAP можно также просмотреть в базе данных Statistics Reports и в окне Domino Administrator, выбрав **Server => Statistics** (Сервер => Статистика).

Несколько каталогов

Как уже отмечалось, вместе с первичным каталогом Domino домен может иметь несколько вторичных каталогов Domino. Чтобы эти каталоги были полезны, необходимо сделать их доступными для пользователей, серверов и программ поиска. В Domino есть три варианта: Directory Catalog (Перечень каталога), Directory Assistance (Поддержка каталога) и Cascaded Address Books (Каскадные адресные книги). Появились они в разное время: Directory Catalog - только в версии R5, Directory Assistance - начиная с версии R4, а служба Cascaded Address Books осталась еще с версии R3 и поддерживается в R5/6 лишь из соображений обратной совместимости. Directory Catalog и Directory Assistance имеют больше функциональных возможностей, чем Cascaded Address Books, и требуют меньше системных ресурсов. Lotus рекомендует прекратить использование Cascaded Address Books и перейти на Directory Catalog или Directory Assistance либо на оба средства одновременно. Эти рекомендации следует признать вполне разумными.

Остается вопрос: стоит ли устанавливать одновременно Directory Catalog и Directory Assistance? Ответ зависит от того, почему вы обращаетесь к нескольким каталогам.

Для работы с простым доменом Notes (если только он не совсем маленький) будет по-видимому достаточно Directory Catalog, даже если у вас есть только первичный каталог Domino. Основная задача перечня каталогов состоит в том, чтобы сократить просматриваемый каталог до минимально возможного размера и ускорить адресный поиск. Directory Catalog отлично выполняет обе задачи. Если организация маленькая, скажем менее 200 человек, и среди них нет мобильных пользователей, то Directory Catalog принесет мало пользы. Но чем крупнее фирма, тем больше нужен Directory Catalog. А если в организации есть мобильные пользователи, то Directory Catalog - лучшее решение проблемы поддержания современной мобильной адресной книги.

С другой стороны, Directory Assistance выполняет ряд функций, с которыми не справляется Directory Catalog. Каталог Directory Assistance может расширить адресный поиск пользователей Notes для объектов LDAP и направлять LDAP-клиентов к другим каталогам LDAP, что позволяет аутентифицировать Web-пользователей на основании сертификатов, хранящихся в других каталогах LDAP. Если вам нужны такие средства, то следует применять Directory Assistance.

Кроме того, если вы храните вторичные каталоги пользователей, которым другие пользователи отправляют почту, то можно удалить их из Directory Catalog и включить в Directory Assistance. Например, у вас есть вторичный каталог, предназначенный только для аутентификации Web-пользователей, к которым не часто обращаются постоянные пользователи вашей организации. В таком случае нет смысла включать этот каталог в Directory Catalog, поскольку целью создания Directory Catalog является ускорение адресного поиска и, следовательно, необходимо, чтобы он был как можно меньше. Но допустимо включить его в Directory Assistance, чтобы такие пользователи, как администраторы Web-приложений, были вправе при необходимости задействовать этот каталог для поиска нужного адреса.

И наконец, если вы все еще сомневаетесь в том, какую службу лучше выбрать, вот совет компании Lotus: установите обе службы. Они работают вместе, чтобы предоставить все возможности поиска. Если ваш Directory Catalog по некоторым причинам становится недоступен, Directory Assistance полностью заменит его, так что пользователи даже не заметят его отсутствия (если, конечно, они не знали, что он должен быть на первом месте).

В табл. 11.5 сравниваются возможности Mobile Directory Catalog, Server Directory Catalog и Directory Assistance.

Таблица 11.5. Сравнительные возможности *Mobile Directory Catalog*, *Server Directory Catalog* и *Directory Assistance*

Задача	Mobile Directory Catalog	Server Directory Catalog	Directory Assistance
Поиск адреса для пользователей почты Notes во вторичных каталогах Domino	Да	Да	Да
Поиск адреса для пользователей почты Notes в каталогах LDAP	Нет	Нет	Да
Поиск адреса для LDAP-клиентов во вторичных каталогах Domino	Нет	Да	Да
Перенаправление LDAP-клиентов в другие каталоги LDAP	Нет	Нет	Да
Аутентификация Web-клиентов, зарегистрированных во вторичных каталогах Domino	Нет	Да	Да
Аутентификация Web-клиентов, зарегистрированных в других каталогах LDAP	Нет	Нет	Да
Проверка принадлежности к группе, зарегистрированной в другом каталоге LDAP	Нет	Нет	Да
Адресация с помощью имени получателя	Да	Да	Да
Предоставление мобильным пользователям Notes полного списка каталогов	Да	Нет	Нет

Порядок просмотра каталогов

Когда установлены обе службы, поинтересуйтесь, в каком порядке просматриваются каталоги. Если говорить кратко, то Directory Catalog просматривается перед вторичными каталогами, перечисленными в Directory Assistance.

Но какова очередность просмотра всех каталогов? Ответ зависит от того, кто осуществляет поиск - сервер Domino, клиент Notes или LDAP-клиент.

Сервер Domino просматривает каталоги в таком порядке:

#

1. Первичный каталог Domino.
2. Если Доступна служба Cascaded Address Books, то далее следуют каталоги, перечисленные в переменной names файла сервера notes.ini. Обратите внимание, что если доступна служба Cascaded Address Books, то остальные службы недоступны и поиск на этом заканчивается.
3. Если установлен Directory Catalog, исследуется он.
4. В случае, когда в Directory Catalog найден требуемый объект, но сервер не может найти в этом объекте нужный информационный элемент, то изучается вторичный каталог Domino, в котором находится найденный объект.
5. При условии, что доступна служба Directory Assistance, просматриваются перечисленные там вторичные каталоги:

- когда серверу известно полное различающееся имя искомого объекта, он ищет в базе данных Directory Assistance правило для определения вторичного каталога, в котором следует продолжать поиск;
- если сервер знает только общее имя искомого объекта или не может найти правило определения требуемого вторичного каталога, он начинает просматривать все вторичные каталоги в порядке их нумерации, а при наличии нескольких каталогов с одинаковыми порядковыми номерами - в алфавитном порядке.

Очередность просмотра каталогов пользователем Notes следующая:

1. Локальные каталоги в порядке их появления в поле **Local address books** в окнах **User Preferences**, **Mail** и **News**. Если клиент Notes настроен стандартно, то сначала исследуется персональная адресная книга (names.nsf), а потом Mobile Directory Catalog (когда он есть на рабочей станции).
2. Если в поле **Mail file location** выбранного документа местоположения (Location document) пользователя установлено значение **Local**, а в поле **Recipient name type-ahead** - значение **Disabled** или **Local only**, поиск прекращается.
3. Если же в поле **Mail file location** задано значение **Local**, а в поле **Recipient name type-ahead** - значение **Local then server**, то клиент Notes продолжает поиск в доступных ему каталогах или на почтовом сервере, но только после того, как пользователь нажимает F9 или выбирает **Send**.
4. Когда в поле **Mail file location** установлено значение **on Server**, Notes продолжает поиск в каталогах или на почтовом сервере.
5. Если в поле **Recipient name lookup** документа местоположения установлено значение **Exhaustively check all address books**, поиск продолжается до тех пор, пока не будут исследованы все каталоги. Если в этом поле установлено значение **Stop on the first match**, поиск останавливается при обнаружении первого соответствия.
6. Клиент Notes просматривает каталоги на сервере в том же порядке, что и сервер Domino (см. выше).

Службой LDAP каталоги по запросу LDAP-клиентов просматриваются в следующем порядке:

1. Первичный каталог Domino на LDAP-сервере.
2. Server Directory Catalog (Перечень каталогов сервера), если он используется LDAP-сервером.
3. Вторичные каталоги, перечисленные в Directory Assistance, если эта служба применяется LDAP-сервером. Он просматривает их так же, как сервер, то егѣ сначала по правилу, если возможно, и затем в порядке нумерации каталогов:
 - если по правилу предусматривается просмотр вторичных каталогов Domino, то поиск выполняет служба LDAP;
 - если порядок просмотра предполагает просмотр каталога LDAP, который имеется в списке, служба LDAP отправляет клиента к этому каталогу и клиент просматривает его самостоятельно.

Клиенты, не использующие Notes, например клиенты почтовых служб POP3 и ШАР, получают доступ к каталогам Domino только в том случае, если они имеют функции LDAP-клиента.

Перечень каталогов

Directory Catalog (Перечень каталогов) – новое средство, которое появилось в версии R5. Это сильно сжатый сборник наиболее часто используемой информации из одного или нескольких каталогов Domino. Он занимает гораздо меньше места, чем каталог Domino и в нем гораздо быстрее проводится поиск. Если в вашей компании много сотрудников (более 200) или есть мобильные пользователи, необходимо задействовать Directory Catalog.

Всего существует два типа перечней каталогов: Server Directory Catalog (Серверный перечень каталога) и Mobile Directory Catalog (Мобильный перечень каталога). Server Directory Catalog расположен на сервере и предоставляет возможности поиска для серверов и пользователей Notes, подключенных к сети. Mobile Directory Catalog расположен на компьютере мобильного пользователя и позволяет производить поиск без подключения к сети.

Специалисты Lotus рекомендуют создавать оба типа перечней каталогов, хотя не могут четко объяснить, зачем. А причина в следующем. Вы, скорее всего, захотите включить в каталоги различные поля. Например, в зависимости от того, как вы используете Server Directory Catalog, допустимо поместить в него те поля, которые вам не нужны в Mobile Directory Catalog. Даже если при первой установке эти два перечня получаются одинаковыми, вы все равно должны создать разные перечни. Придет день, когда вам понадобится добавить определенные поля в Server Directory Catalog. Если у вас уже есть оба перечня, то вам просто придется добавить выбранные поля в нужный перечень. Если же у вас один перечень выполняет двойную работу, потребуется создать новый перечень и перенастроить домен, чтобы отразить ситуацию использования двух перечней каталогов вместо одного. Поэтому вы сэкономите много времени и сил, если сразу создадите два перечня.

Установка перечня каталогов

Чтобы установить перечень каталогов, выделите один из серверов своего домена для построения исходного перечня каталога. Затем скопируйте Server Directory Catalog на остальные серверы домена. Mobile Directory Catalog копируется либо непосредственно на рабочие станции пользователей, либо на промежуточный сервер, с которого потом можно перенести этот перечень на рабочие станции. Основной момент заключается в том, что создавать перечни каталогов нужно на одном сервере. Создавать их могут разные серверы, но только один сервер вправе иметь определенный перечень.

В целом процесс выглядит следующим образом:

*

1. Назначьте сервер для построения перечня каталогов.
2. Скопируйте вторичные каталоги Domino на «сервер-строитель».
3. Спланируйте регулярную репликацию вторичных каталогов на этот сервер.
4. Создайте и настройте исходные перечни каталогов.
5. Скомпонуйте исходные перечни каталогов.
6. Создайте реплики исходных перечней каталогов на требуемые серверы и/или рабочие станции.
7. Спланируйте регулярную репликацию перечней каталогов.

Далее подробно расписан каждый шаг.

Назначение и подготовка «сервера-строителя»

Сервером для построения исходного перечня каталогов лучше назначить сервер-концентратор или сервер каталогов. При наличии в домене концентратора удастся быстро распространять все изменения среди радиальных серверов. Сервер каталогов - это сервер, назначенный только для предоставления служб каталогов. Такой сервер целесообразно выделять только в очень больших доменах. Если у вас есть один или несколько серверов каталогов, можно построить перечни каталогов на одном из них и затем реплицировать их на остальные серверы каталогов и на почтовые серверы, если сервер каталогов работает с ними.

Если вы строите перечни каталогов для нескольких доменов, допустимо создать их на одном из серверов любого домена и затем реплицировать на серверы остальных доменов. Вместо этого разрешается построить разные перечни каталогов только для пользователей одного домена (даже если перечни каталогов содержат каталоги из других доменов). Выбор способа зависит от множества факторов, включая необходимость наличия одинаковых каталогов в нескольких доменах и возможность договоренности между администраторами, чтобы один из них обеспечивал работу всех каталогов.

Для подготовки сервера, назначенного для построения исходного перечня каталогов, необходимо выполнить следующие операции:

1. Создайте на «сервере-строителе» реплики всех вторичных каталогов, которые должны быть включены в перечень каталога. Присвойте им описательные названия, чтобы их было проще распознавать. В качестве шаблона можно использовать `???names.nsf`, где `???` - любые символы, указывающие, что это за каталог, а `names.nsf` означает, что данный файл является каталогом. Обратите внимание: даже если сервер в состоянии формировать перечень каталога из каталогов, расположенных на других серверах, лучше так не делать, поскольку это сильно замедляет процесс (в зависимости от возможностей сети) и напрасно расходует пропускную способность сети.
2. Настройте документы соединения (Connection document), чтобы спланировать регулярную репликацию вторичных каталогов Domino и их исходных реплик. Вам нужно, чтобы они своевременно модифицировались и обновленная информация включалась в перечень каталога.
3. Создайте два исходных перечня каталогов: один для Server Directory Catalog, другой для Mobile Directory Catalog. Для этого выберите **File => Database => New** (Файл => База данных => Новая). В поле **Server** (Сервер) выберите **build server** («сервер-строитель»). В поле **Title** (Имя) введите любое имя. Советуем использовать названия, указывающие на назначение каждого списка, например Server Dirgptory Catalog и Mobile Directory Catalog. В поле **File Name** (Имя файла) задайте имя файла. Компания Eotus предлагает применять имена файлов `sdn.nsf` и `mdn.nsf` - просто, коротко и ясно. Выберите **Create full text index for searching** (Создать полнотекстовый индекс для поиска). В поле **Template Server** (Сервер шаблона) отметьте **build server**. Укажите шаблон перечня каталогов: файл `dircat5.ntf` для R5 или `dc.ntf` для R6 (хотя в документации версии R6 все еще обсуждается файл `dircat5.ntf`) - Не следует выбирать шаблон Catalog (5.0) или Catalog (6). Щелкните по OK.
4. Внесите необходимые изменения в список ACL. Уровень доступа по умолчанию можно оставить **Reader**. Подумайте над тем, чтобы группе администраторов предоставить уровень доступа **Manager**, а для групп **LocalDomainServers** (Серверы локального домена) и **OtherDomainServers** (Серверы других доменов) установить уровень

доступа ниже Designer. Ни одному из серверов, кроме главного и «сервера-строителя», не нужен доступ к базам данных выше Reader. Главному серверу требуется доступ **Manager**, чтобы он мог передавать все обновления на другие серверы.

5. Создайте документ Configuration (Конфигурация) в каждом исходном перечне каталогов (см. следующий раздел).

Настройка исходных перечней каталогов

Откройте перечни каталога (Server Directory Catalog и Mobile Directory Catalog) по очереди. В каждом из них создайте документ Configuration. Выберите **Create => Configuration** (Создать => Конфигурация). В появившемся окне отредактируйте следующие поля: **Directories to include** (Включаемые каталоги), **Additional fields to include** (Включаемые дополнительные поля), **Restrict aggregation to this server** (Ограничить обобщение этим сервером), **Send Directory Catalog reports to** (Отправлять отчеты перечня каталогов в) и **Comments** (Комментарии). Описание этих полей приведено в табл. 11.6.

Таблица 11.6. Поля документа *Directory Catalog Configuration*, которые необходимо заполнить

Поле	Комментарии
Вкладка Basics (Основные параметры)	
Directories to include (Включаемые каталоги)	Введите имена файлов каталогов, включаемых в перечень каталогов. Поместите первичный каталог Domino в Mobile Directory Catalog. Если Server Directory Catalog будет использоваться только в вашем домене, то первичный каталог Domino вносить в него необязательно, а если в нескольких доменах - обязательно. Его лучше не помещать в список каталогов: подключенные пользователи и серверы будут сначала просматривать первичный каталог Domino, а потом - перечень каталогов, поэтому если список каталогов применяется только в данном домене, то первичный каталог будет лишним. Если вы (несмотря на приведенное замечание) включите вторичные каталоги Domino, которые не реплицированы на «сервер-строитель», у вас будет возможность ссылаться на них с помощью имени либо следующей записи: portname!!!servername!! filename, где portname - номер порта сервера, через который можно получить доступ к хосту сервера баз данных, servername - полное различающееся имя сервера Notes, а filename - имя файла и путь к базе данных на сервере-хосте
Additional fields to include (Включаемые дополнительные поля)	Можно оставить значения в этом поле как есть. Если вы все же хотите изменить их, обратите внимание на рекомендации Lotus: - О не удаляйте установленный по умолчанию набор полей — это поля, которые просматриваются чаще всего; - О не переусердствуйте при добавлении полей, поскольку каждое новое поле увеличивает размер перечня каталогов и общее время репликации; - О добавляйте поля только из форм Person, Group, Mail-In Database и Resource; - О в серверный перечень каталогов (Server Directory Catalog) добавьте поля AltFullName и AltFullNameLanguage; - О в серверный перечень каталогов внесите поле Members, если пользователи будут применять Server Directory Catalog без ограничения времени (полезно при поиске пользователей других доменов);

Таблица 11.6. Поля документа *Directory Catalog Configuration*, которые необходимо заполнить (окончание)

Поле	Комментарии
Additional fields to include	О в серверный перечень каталогов добавьте поле HTTTPassword, если Server Directory Catalog будет использоваться для аутентификации Web-пользователей; О в мобильный перечень каталогов (Mobile Directory Catalog) введите поля AltFullName и AltFullNameLanguage, только если в Ю-файлах пользователей разрешены альтернативные имена файлов; О в мобильный перечень каталогов добавьте поле Members, если пользователям разрешен поиск без ограничения времени, когда они отключены от сети, и только при условии, что вы в состоянии предоставить дополнительное дисковое пространство и допускаете, чтобы на репликацию тратилось дополнительное время
Restrict aggregation to this server (Ограничить обобщение этим сервером)	Введите имя «сервера-строителя». Это защитит от случайного запуска задачи direct на другом сервере и случайного создания перечня каталогов
Send Directory Catalog reports to (Отправлять отчеты перечня каталогов в)	Укажите в данном поле хотя бы свое имя и имена людей, ответственных за корректную работу перечня каталогов. Если вы заполняете поле, то при сохранении и закрытии документа конфигурации Notes откроет диалоговое окно, в котором будет предложено назначить сервер для работы «этого агента». Под агентом Notes здесь понимается агент Directory Catalog Status Report. Выберите «сервер-строитель». Запланировано, что агент запускается каждое воскресенье в 2 часа утра. Допускается изменить график работы, выбрав View => Agents (Вид => Агенты) при открытой базе данных
Comments (Комментарии)	Обычно рекомендуется свободное комментирование для удобства ваших преемников. Среди всего прочего укажите, какой это перечень каталогов - серверный или мобильный. Также объясните причины включения и исключения определенных полей и каталогов

Остальные поля документа конфигурации содержат некоторые параметры по умолчанию на вкладке Basics (Основные параметры) и некоторые параметры оптимизации производительности на вкладке Advanced (Дополнительно). Можно оставить значения в названных полях так, как они установлены, или настроить их позже. Лучше все сделать сразу, поскольку* если вы будете изменять параметры потом, Domino придется перестраивать весь перечень каталога, что потребует полного копирования базы данных. Если база достаточно большая, а репликация происходит по коммутируемому соединению, это будет продолжаться долго. Стоит потратить некоторое время и сразу оптимально подобрать конфигурацию перечня каталогов, чтобы избежать такой неприятности. Поля вкладки Basics перечислены в табл. 11.7.

Поля на вкладке Advanced управляют параметрами сборки перечня каталогов. В большинстве случаев следует оставить значения по умолчанию до тех пор, пока вас удовлетворяет производительность, перечня каталогов. Подробнее о воздействии на производительность списка каталогов рассказано ниже.

Таблица 11.7. Необязательные для заполнения поля на вкладке *Basics* документа конфигурации перечня каталогов (*Directory Catalog*)

Поле	Комментарии
Sort by (Сортировать по)	По умолчанию сортировка производится по различающемуся имени, то есть сначала по имени, а затем по фамилии. Так установлено, поскольку большинство людей в своих почтовых адресах указывают имена в таком порядке. Если ваши пользователи сначала указывают фамилию, измените порядок сортировки на Last Name , а если они при отправке почты используют альтернативные имена, выберите Alternate Fullname (Альтернативное полное имя)
Use Soundex (Использовать Soundex)	Средство Soundex предоставляет возможность поиска по произношению. По умолчанию задано значение Yes . Если вы изменяете значение и устанавливаете No , вы сэкономите около 4 байт на каталог в окончательном перечне каталогов
Remove duplicate users (Удалять дублированных пользователей)	По умолчанию указано Yes . Это означает, что каталог выбирает первую копию, когда встречаются повторяющиеся записи одного пользователя. Если задано No , каталог просит пользователя отметить нужную копию
Group types (Типы групп)	По умолчанию установлены группы Mail (Почтовые) и Multi-purpose (Многоцелевые). Обычно данные значения можно не менять, поскольку в полях почтового адреса встречаются только эти группы

Запуск каталогизатора

Когда конфигурирование исходного перечня каталогов закончено (см. предыдущий раздел), можно заполнить его нужными каталогами, запустив на «сервере-строителе» Directory Cataloger (Каталогизатор). Каталогизатор помещает данные из каталогов в Directory Catalog. Он обобщает содержимое до 255 документов включаемых каталогов, перенося его в перечень каталога. Группировка производится таким образом, что в обобщенном документе содержатся те поля, которые были перечислены в документе конфигурации, а каждое поле включает данные соответствующих полей из множества исходных документов (до 255).

Процесс можно планировать или запустить вручную. При планировании процесса любое обновление будет происходить автоматически. Настройте расписание Directory Catalog следующим образом:

1. Откройте серверный документ «сервера-строителя», желательно на самом «сервере-строителе».
2. В этом документе выберите **Server Tasks => Directory Cataloger** (Задачи сервера => Каталогизатор) и заполните поля, как указано в табл. 11.8.
3. Сохраните и закройте документ.

Soundex действует только для имен и названий, записанных латинскими буквами, и учитывает правила произношения английского языка. - *Прим. ред.*

Таблица 11.8. Поля в серверном документе на вкладке **Server Tasks => Directory Cataloger**

Поле	Комментарии
DirectoryCatalogfilenames: (Имена файлов перечня каталогов)	Введите имена файлов перечня каталогов, которые будет обобщать данный сервер, разделяя их запятыми или точкой с запятой (например, sdc.nsf, mdcnsf)
Schedule: (Расписание)	Установлено значение Enabled (Разрешено)
Other fields: (Другие поля)	Компания Lotus рекомендует принять график по умолчанию. Естественно, вы можете установить тот график, который реально отражает ваши потребности

Если сервер в назначенный расписанием момент обнаруживает изменения, то запускается Directory Cataloger. В противном случае Directory Cataloger стартует в следующее запланированное время.

Можно компоновать и обновлять перечень каталога вручную, набрав соответствующую команду на консоли сервера или указав ее в программе Domino Administrator.

Перед запуском Directory Cataloger убедитесь, что эта задача еще не выполняется. Когда одновременно работают два экземпляра программы, результаты могут быть непредсказуемыми. В окне Domino Administrator выберите **Server => Status** (Сервер => Состояние) и посмотрите, нет ли в списке выполняемых задач Directory Cataloger. Или наберите на консоли сервера команду `show tasks` и проверьте наличие Directory Cataloger. Если каталогизатор выполняется, прервите его работу, отметив эту задачу в Domino Administrator и выполнив **Tools => Task => Stop** (Программные инструменты => Задача => Остановить). Или введите команду `tell dircat quit` на консоли сервера.

Для запуска Directory Cataloger с консоли управления сервером служит следующая команда:

```
load dircat dc.nsf
```

где `dc.nsf` - имя файла компонуемого списка каталогов.

Первая компоновка списка каталогов может занять некоторое время. Специалисты Lotus посчитали, что на компьютере Pentium с тактовой частотой 200 МГц задача Directory Cataloger способна обработать около 75000 записей в час. Обновления потребуют гораздо меньше времени.

Целиком заполненный перечень каталога можно скопировать на другие серверы и рабочие станции пользователей.

0

Установка Server Directory Catalog на рабочие серверы

Чтобы установить полностью скомпонованный перечень каталога на рабочий (производственный) сервер, выполните следующие действия:

1. Создайте реплики Server Directory Catalog на других серверах, которые будут использовать каталогизатор. Если репликация проводится через серверы-концентраторы, для них тоже создайте реплики. Компания Lotus рекомендует одинаковые имена файлов для всех серверов. Когда вы создаете реплики, Domino автоматически снабжает их полнотекстовыми индексами.
2. Выполните одно или два следующих действия (для дополнительной страховки Lotus советует реализовать оба действия):

- добавьте имя файла перечня каталогов в профиль каталога первичного каталога Domino. Для этого откройте каталог Domino и выберите **Actions => Edit Directory Profile** (Операции => Редактировать профиль каталога). Введите имя файла в поле **Directory Catalog database name for domain** (Имя файла базы данных перечня каталогов для домена);
 - дополните именем файла перечня каталогов серверный документ каждого сервера, который будет его использовать. Задайте имя файла на вкладке **Basics** (Основные параметры) в поле **Directory Catalog database filename for this server** (Имя файла базы данных перечня каталогов для этого сервера). Если имя файла на данном сервере отличается от имени файла, указанного в профиле каталога, то на сервере надо обязательно выполнить это действие.
3. Если перечень каталога будет применяться и на серверах других доменов, то их администраторы также должны проделать второе действие.
 4. Проверьте расписание и топологическую схему репликации, чтобы удостовериться, что все рабочие реплики списка каталогов своевременно обновляются.

Установка Mobile Directory Catalog на рабочие станции

Для установки полностью скомпонованного Mobile Directory Catalog на рабочую станцию Notes R5/R6 (на остальных рабочих станциях он не функционирует) необходимо выполнить две операции. Во-первых, создать реплики Mobile Directory Catalog для каждой рабочей станции Notes. Во-вторых, добавить имя файла мобильного перечня каталогов в поле **Local address books** (Локальные адресные книги) на вкладке **Mail** (Почта) в окне **User Preferences** (Предпочтения пользователя), что, в свою очередь, добавляет имя файла в переменную Names файла notes.ini.

Это можно сделать вручную или автоматизировать с помощью **User Setup Profiles** (Профиль установки пользователя). Для использования **User Setup Profiles** выполните следующие действия:

1. Создайте реплики Mobile Directory Catalog на серверах, к которым имеют доступ рабочие станции пользователей (их почтовые серверы или серверы каталогов). Чем больше серверов имеют такие реплики, тем больше возможностей будет у пользователей при репликации мобильного перечня каталогов на рабочие станции.
2. Откройте любую реплику Mobile Directory Catalog и выберите **Edit => Copy As Link => Database Link** (Правка => Копировать как ссылку => Ссылка на базу данных). При этом ссылка на Mobile Directory Catalog помещается в буфер обмена Windows.
3. Вставьте ссылку в поле **Mobile directory catalogs** (Мобильные перечни каталогов) профиля **User Setup Profile**, предназначенного для ваших мобильных пользователей. Если такой профиль уже существует, откройте его в режиме редактирования (**Edit, mode**), в противном случае создайте его. Когда для разных пользователей назначены разные профили, необходимо вставить ссылку в каждый из них. При создании нескольких профилей **User Setup Profile** заполните остальные поля по необходимости. Сохраните и закройте каждый профиль.
4. Если вы создаете профиль установки пользователя, введите имя данного пользователя в поле **Setup profile(s)** его персонального документа. Когда это нужно сделать для большого числа пользователей, имеет смысл построить агент и автоматизировать процесс (см. ниже).

Затем редактируемый (или новый) профиль установки пользователя и редактируемый персональный документ (если таковой имеется) необходимо реплицировать на почтовые серверы указанных пользователей. В дальнейшем, при подключении такого пользователя к почтовому серверу, его профиль и персональный документ получают шаблон реплики мобильного списка каталогов. Расписание репликации уже настроено, поэтому рабочие станции будут регулярно автоматически обновлять локальные реплики. Кроме того, как уже отмечалось, имя файла локальной реплики каждого пользователя автоматически появляется в поле **Local address books** окна **User Preferences**.

Программа Notes Dynamic Configuration для рабочей станции Notes R5 (ndyncfg.exe) выполняет все указанные действия. Ее можно остановить. Когда вы останавливаете программу, есть возможность все сделать вручную либо вновь запустить программу. В версии R6 программа Notes Dynamic Configuration заменена средством IBM Lotus Notes Smart Upgrade (Интеллектуальное обновление), которое действует на основе политик и позволяет обновлять программное обеспечение не только на рабочих станциях, но и на серверах. Для работы с IBM Lotus Notes Smart Upgrade требуется предварительно установить главную политику обновления (Master upgrade policy), после чего требования этой политики распространяются на всю систему Notes. О данном средстве подробно рассказано в технической документации Notes/Domino R6.

Если пользователи других доменов тоже будут обращаться к Mobile Directory Catalog, его необходимо реплицировать на один или несколько серверов этих доменов. Затем администраторы таких доменов должны выполнить все указанные выше действия.

Использование агента для обновления поля Setup Profile(s)

Чтобы создать агент для автоматизации процесса распространения действия профиля **User Setup Profile** на нескольких пользователей, необходимо:

1. На вкладке **People & Groups** программы Domino Administrator выделить сервер так, чтобы отображались имена людей, для которых создается агент, и выполнить **Create => Agent** (Создать => Агент). Появляется окно для агента без имени. На рис. 11.2 поля изображены уже заполненными, а не так, как они появляются изначально.
2. В поле **Name** (Имя) введите описание агента. Когда вы сохраняете агент, это имя появляется в меню **Actions** (Операции), если открыт текущий каталог.
3. В поле **When should this agent run?** (Когда должен выполняться этот агент?) оставьте значение **Manually From Actions Menu** (Вручную из меню Actions). В R6 это значение указывается в безымянном поле раздела **Runtime** (Время исполнения), причем нужно выбрать значение **Actions menu selection** (При выборе меню Actions).
4. В тьюле **Which document(s) should it act on?** (С какими документами он должен работать?) оставьте значение **Selected documents** (Выделенные документы). В R6 это поле названо **Target** (Целевые документы), причем указать нужно значение **All selected documents** (Все выделенные документы).
5. В поле **Run** (Запуск) оставьте значение **Simple action(s)** (Простое действие). В версии R6 заполнение этого поля происходит уже после закрытия вкладки основных параметров агента.

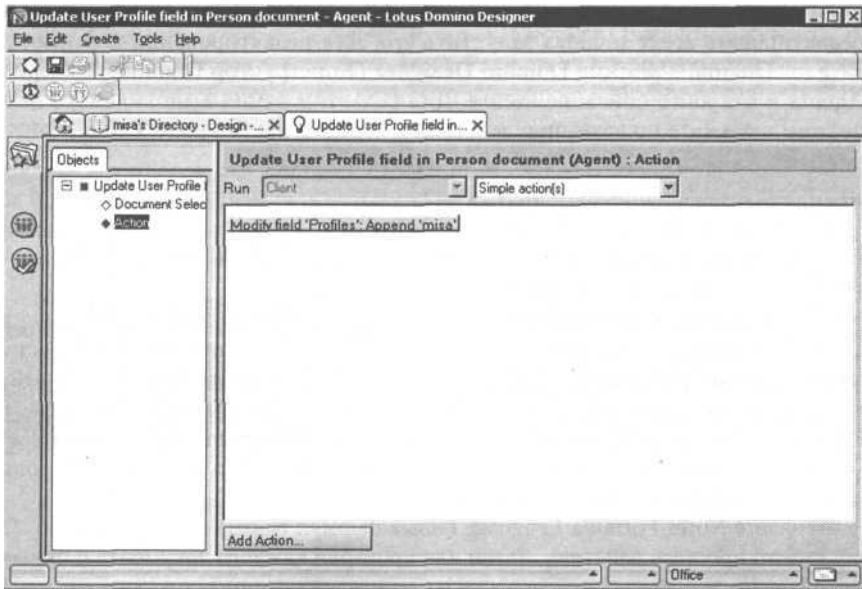


Рис. 11.2. Для определения критерия поиска, по которому агент будет выбирать обновляемые документы, щелкните по кнопке Add Search (Добавление поиска)

6. Щелкните по кнопке Add Action (Добавить действие). Появится одноименное окно, где нужно заполнить поля следующим образом:
 - Action (Действие) - установите значение Modify Field (Изменить поле);
 - Field (Поле) или The value in field (Значение в поле) для R6 - задайте значение Profiles (Профили);
 - Value (Значение) или Whis the new value (На новое значение) - введите имя профиля установки пользователя без кавычек;
 - выберите Replace value (Заменить значение) или Append value (Добавить значение), как считаете нужным, либо Modify by Replacing (Изменение заменой) или Modify by Appending (Изменение дополнением) в R6.
7. Щелкните по ОК, чтобы добавить выбранные действия в описание агента. Сохраните и закройте агент. Обратите внимание, что агент появился в меню Actions.
8. Выделите персональные документы, с которыми будет работать агент. Щелкните мышью по столбцу слева от названия документа, чтобы поставить там метку.
9. Запустите агент из меню Actions. После выполнения проверьте правильность функционирования, просмотрев поле Setup profile(s) в документе, с которым работал агент. Если в этом поле указано имя профиля установки пользователя, которое было задано в агенте, то все в порядке.

10. Если для других пользователей необходимо установить другие профили, можно отредактировать агент и снова запустить его. Для редактирования агента откройте каталог Domino в режиме **Domino Designer** (Конструктор Domino), выберите вид **Agents** и откройте описание агента. Для редактирования выполняемого действия дважды щелкните по названию действия и отредактируйте поле **Value**.

Рассмотренный агент легко создать, и он просто работает. Его недостаток заключается в том, что приходится вручную выбирать персональные документы, с которыми он должен взаимодействовать. В больших доменах это само по себе может быть утомительно. Можно написать агент таким образом, чтобы он сам просматривал вид **People** и правильно выбирал персональные документы, которые необходимо изменить.

Однако сложно определить уникальные свойства документов, которым нужно присвоить профиль установки пользователя. Если удастся выделить такие свойства, достаточно щелкнуть по кнопке **Add Search** (Добавить условие) и определить поиск, который будет находить документы, удовлетворяющие выбранному вами критерию. В этом случае в поле **Which document(s) should it act on?** задайте значение **All Documents in view** (Все документы на данном виде). Будут просматриваться все документы, а изменяться - только те, которые удовлетворяют установленному критерию.

Если вы знаете Notes Formula Language (Язык формул Notes), то можете использовать формулу вместо простого действия. Затем для проверки каждого документа и присвоения соответствующего профиля в зависимости от результатов примените выражение **@if**. Не будем углубляться в детали создания и настройки такого агента. Любая хорошая книга по программированию в Notes содержит необходимую информацию.

Небольшое замечание прежде, чем будет закрыта тема о создании агентов. Если вы создаете агент, который просматривает документы на виде и решает, в какой из них следует внести изменения, проверьте установленный критерий и убедитесь, что выбираются нужные документы. Если вы ошибочно вносите изменения, то единственным способом возврата будет восстановление резервной реплики базы данных, поскольку после применения агента нельзя щелкнуть по кнопке **Undo** (Отмена).

Существует два способа проверить выбранный критерий. Первый - посредством предлагаемого критерия провести ручной перебор на виде **People**. Для этого нажмите на значок **Search** (Поиск) в правом верхнем углу окна Domino Administrator. Когда появится панель **Search**, нажмите на **More** (Дополнительно), затем кнопками **Condition** (Условие) определите условия поиска (рис. 11.3).

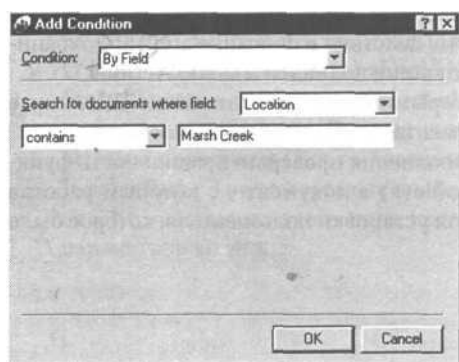
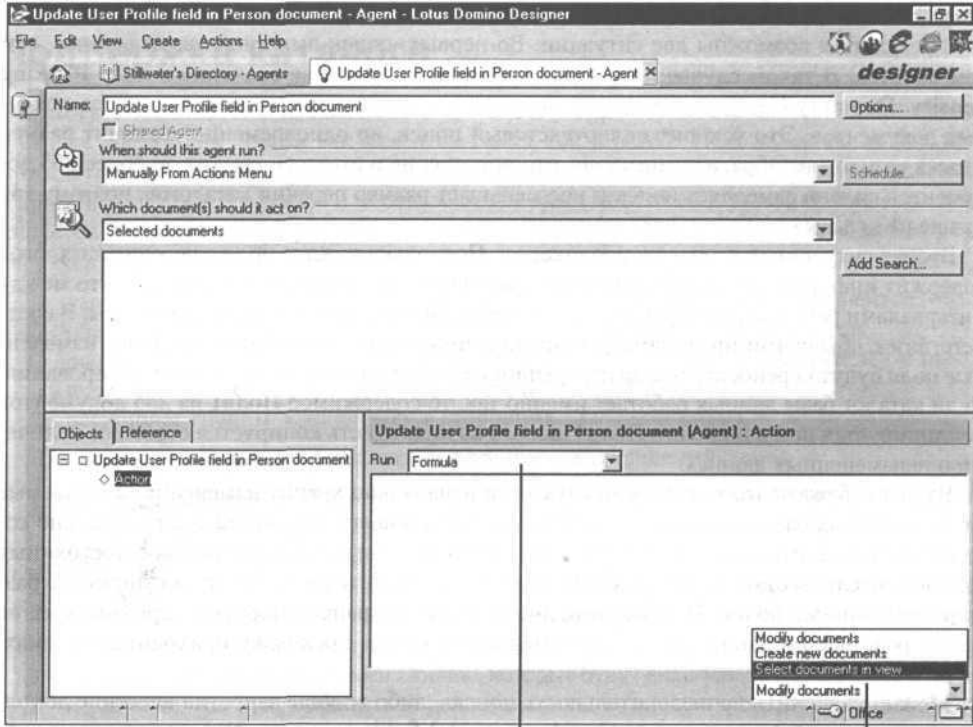


Рис. 11.3. Диалоговое окно **Add Condition** (Добавить условие) открывается любой кнопкой **Condition** на дополнительной панели поиска, которая расположена чуть выше диалогового окна. Окно **Search** загружается щелчком по значку **Search** (на нем изображено увеличительное стекло) в верхнем правом углу экрана

Второй способ: если вы вводите формулу вместо простого действия, можно проверить критерий выбора, указав значение **Select documents in view** (Выбрать документы на виде) в правом нижнем углу окна агента (рис. 11.4). Если агент правильно отмечает персональные документы, то указанное значение можно изменить на **Modify documents** (Изменить документы).



Если в поле Run установлено значение Formula...

...то становятся доступными следующие варианты

Рис. 11.4. Чтобы проверить критерий выбора, укажите вариант **Select documents in view**.

Если выбор осуществляется верно, задайте значение **Modify documents**

Оптимизация производительности серверного перечня каталогов

В процессе работы иногда обнаруживается, что при некоторых условиях поиск в вашем серверном перечне каталогов выполняется неприемлемо медленно. Если возникает такая проблема, она затрагивает перебор вариантов в полнотекстовом индексе перечня каталогов. Можно ускорить поиск, отредактировав одно или несколько полей на вкладке **Advanced** документа **Directory Catalog Configuration**. Перечисленные там поля, такие как **Packing density** (Плотность сжатия), **Incremental fields** (Дополнительные поля) и **Merge factor** (Коэффициент объединения), управляют параметрами сборки перечня каталогов.

Чтобы понять, как эти поля влияют на производительность поиска, необходимо разобраться в устройстве перечня каталога. По умолчанию Directory Cataloger обобщает в одном документе списка каталогов данные из 255 документов. Каталогизатор делает это, перечисляя данные из одинаковых полей всех обобщаемых документов в одном поле общего документа. Другими словами, **Поле1** общего документа содержит список значений **Поля1** всех составляющих документов; **Поле2** - список значений **Поля2** всех составляющих документов - и так для всех включаемых полей.

В результате возможны две ситуации. Во-первых, поиск выполняется медленнее, чем вам хочется. В таком случае попробуйте установить меньшее значение в поле **Packing density**. Directory Cataloger в каждый сводный документ поместит меньшее число исходных документов. Это ускорит полнотекстовый поиск, но одновременно увеличит размер списка каталогов. Обратите внимание, что повышение плотности сжатия до более 255 документов сильно замедляет поиск и не уменьшает размер перечня каталогов, поэтому так лучше не делать.

Вторая ситуация относится к репликации. Поскольку каждое поле в перечне каталогов содержит информацию из 255 исходных документов, велика вероятность того, что между интервалами репликации некоторые поля в исходных документах будут изменены. В соответствии с обычными правилами репликации при одном изменении в поле все измененные поля будут переноситься в другие реплики базы данных при следующем копировании. Если каталог базы данных работает именно так, то содержимое **Поля1** из 255 документов реплицируется при изменении **Поля1** любого из них, то есть копируется огромное количество неизмененных данных.

Чтобы избежать этого, перечень каталогов изначально хранит изменения, получаемые от включаемых баз данных не в постоянных полях общего документа, а в специально созданных дополнительных полях. По умолчанию он объединяет содержимое постоянных и дополнительных полей, когда объем данных в дополнительных полях достигает 5% размера постоянных полей. В результате значительно сокращается объем передаваемых во время репликации данных, но также замедляется поиск, поскольку приходится просматривать оба поля.

Можно увеличить производительность поиска, либо вообще запретив внесение дополнительных полей (установите в поле **Incremental fields** значение No), либо задав коэффициент объединения менее 5% (укажите значение в поле **Merge factor**). Запрет дополнительных полей сильно увеличит объемы копируемых данных, что неприемлемо в случае большого размера перечня каталогов. Однако этот эффект может быть незначительным, когда перечень каталога маленький.

Если ваш перечень каталога содержит тысячи или десятки тысяч записей, то лучше уменьшить коэффициент объединения, в результате чего сократится объем реплицируемой информации. Удастся найти золотую середину, изменяя коэффициент объединения на единицу и сравнивая объем копируемых данных и время поиска.

Мониторинг перечней каталогов

Существует два способа наблюдения за перечнями каталогов. Во-первых, можно добавить в файл notes.ini «сервера-строителя» переменную Log_DirCat=1. При этом в журнале Notes будет регистрироваться время начала и окончания работы перечня каталогов, а также имена обработанных каталогов. Во-вторых, можно еженедельно получать по электронной почте отчеты о деятельности каталогизатора. Следуя предыдущим рекомендациям,

вы сумеете использовать режим получения отчетов в качестве общего правила настройки перечней каталогов. В противном случае допустимо настроить отправку отчетов, добавив свое имя в поле **Send Directory Catalog reports to** (Отправлять перечень каталогов в) каждого документа конфигурации перечня каталогов. Отчет будет содержать ссылки на перечень каталога, включенные базы данных и различные статистические данные о составляющих базы данных.

Поддержка каталога

Directory Assistance (Поддержка каталога) – это служба, которая позволяет Domino предоставлять доступ для поиска как клиентам Notes, так и LDAP. Некоторые, но не все, возможности этой службы продублированы в Directory Catalog. Таким образом, решение о применении данной службы или отказе от нее зависит от того, для каких целей она планируется. Хотя чуть ранее уже обсуждались достоинства Directory Assistance, здесь снова перечислены те функции, которые выполняет только эта служба:

- О дает возможность адресного поиска в сторонних LDAP-каталогах для клиентов Notes;
- О обеспечивает ссылки на сторонние LDAP-каталоги для LDAP-клиентов;
- О позволяет Web-серверам Domino аутентифицировать Web-пользователей с помощью сертификатов, хранящихся в сторонних LDAP-каталогах;
- О расширяет группы, хранящиеся в сторонних LDAP-каталогах.

Для установки Directory Assistance выполните следующие действия:

1. Создайте базу данных Directory Assistance по шаблону Directory Assistance (da50.ntf) и реплицируйте ее на серверы, которые будут работать с названной службой (тот же шаблон установлен и в версии R6).
2. Определите эту базу данных для серверов, которые к ней обращаются, вписав ее имя файла в поле **Directory Assistance database name** (Имя файла базы данных Directory Assistance) серверного документа.
3. Назначьте вторичные каталоги Domino, которые будут включены в Directory Assistance, и укажите, где будут храниться реплики, затем в базе данных Directory Assistance создайте для каждого такого каталога документ Directory Assistance.
4. Отметьте; какие LDAP-каталоги войдут в Directory Assistance, установите доступ к ним и создайте для каждого такого LDAP-каталога документ Directory Assistance в базе данных Directory Assistance.

Выглядит достаточно просто, не так ли? Тонкость заключается в настройке документов Directory Assistance.

Установка, репликация и идентификация базы данных Directory Assistance

Чаще всего администраторы создают одну базу данных Directory Assistance для работы в одном домене – чтобы предоставить пользователям домена (как пользователям Notes, так и LDAP-клиентам) доступ к ресурсам за пределами домена, включая каталоги в других доменах Notes, а также сторонние LDAP-каталоги. Вместо этого можно сформировать несколько баз данных Directory Assistance, каждая из которых будет обслуживать несколько серверов локального домена Notes.

В версии R4 допускалась одна база данных Directory Assistance для нескольких доменов, то есть серверы в разных доменах Notes совместно использовали общую базу данных Directory Assistance. Но в версии R5/6 нельзя создавать документ Directory Assistance для первичного каталога Domino. Хотя в документации Lotus нет ясности относительно этого вопроса, такие намеки есть. Если все действительно так, то каждый домен Notes должен иметь свою базу данных Directory Assistance, в которой перечислены все остальные домены, кроме локального.

Создание базы данных Directory Assistance

Создайте базу данных Directory Assistance на сервере, который будет ее использовать. Выберите **File => Database => New** (Файл => База данных => Создать). В окне **New Database** (Новая база данных) введите значения, перечисленные в табл. 11.9.

Таблица 11.9. Значения полей в окне **New Database** для базы данных Directory Assistance

Поле	Комментарии
Server (Сервер)	Укажите имя сервера, который будет обращаться к базе данных Directory Assistance
Title (Название)	Определите любое название. Если вы создаете только одну базу, можете назвать ее именно Directory Assistance
File Name (Имя файла)	Введите любое имя файла, например da.nsf. Чтобы немного облегчить свою жизнь, по возможности выберите имя, доступное на всех серверах, которые будут работать с этой базой данных
Template Server (Сервер шаблона)	Задайте имя сервера R5/6, лучше из перечисленных в поле Server . Затем выберите шаблон Directory Assistance (da50.ntf)
Inherit future design changes (Наследовать будущие изменения шаблона)	Убедитесь, что это поле отмечено

Щелкните по ОК, чтобы закрыть окно и создать базу данных.

Настройка списка ACL базы данных Directory Assistance

После этого настройте список ACL. Добавьте группу администраторов с правом доступа **Manager**. Серверы-концентраторы репликации и сервер, на котором будут сформированы документы Directory Assistance, должны иметь право доступа **Manager**, а -See остальные серверы - **Reader**. По умолчанию допускается оставить право **Reader**.

Репликация базы данных Directory Assistance на другие серверы

Затем реплицируйте базу данных на все серверы, которые планируют с ней работать. Это могут быть только почтовые серверы или серверы каталогов. Если всю репликацию намерено производить через серверы-концентраторы, необходимо сделать реплики и на них, даже если они сами не намерены обращаться к Directory Assistance. Чтобы быстро создать новые реплики на всех серверах, выполните следующие действия:

1. Откройте вкладку **Files** в окне Domino Administrator.
2. Выберите сервер, на котором расположена база данных Directory Assistance.

3. Выделите базу данных Directory Assistance в списке баз данных.
4. Укажите **Tools => Database => Create Replica(s)** (Программные инструменты => База данных => Создать реплику).
5. Отметьте или введите имена серверов, на которых нужно создать новые реплики.
6. При необходимости измените имена файлов базы данных на серверах-получателях.
7. Щелкните по ОК. Процесс Administration Process сформирует реплики-заглушки. При запланированной репликации они будут постоянно заполнены документами.

Проверка репликации

Для корректной работы Directory Assistance необходимо своевременно обновлять все реплики ее базы данных. Проверьте правильность функционирования расписания репликации и ее топологии, а также убедитесь, что все реплики базы данных действительно своевременно обновляются.

Идентификация базы данных Directory Assistance для серверов, которые будут ее использовать

И наконец, идентифицируйте базу данных Directory Assistance для каждого сервера, который будет к ней обращаться. Процесс Administrative Process позволяет сделать это одновременно для нескольких серверов или по очереди идентифицировать базу вручную.

Чтобы применить Administrative Process, выполните следующие действия:

1. Откройте вкладку **Configuration** в окне Domino Administrator.
2. Если программа Domino Administrator покажет локальные данные, выберите сервер на панели **Server**.
3. На панели **Tasks** раскройте значок **Server** и укажите **All Server Documents** (Все серверные документы).
4. Определите все серверы, на которые реплицируется база данных Directory Assistance. Если вы присваиваете базе данных различные имена файлов на разных серверах, укажите только те серверы, на которых она имеет одинаковые имена файлов. Щелкните по пустому столбцу слева от имени сервера. Появится метка.
5. После этого выберите **Actions => Set Directory Assistance Information** (Операции => Установить информацию о поддержке каталога).
6. В диалоговом окне **Directory Assistance Information** (Информация о поддержке каталога) введите имя файла базы данных Directory Assistance. Щелкните по ОК. Процесс администрирования (Administration Process) получает запрос на обновление поля **Directory Assistance database name** (Имя файла базы данных Directory Assistance) на выбранных серверах.
7. При необходимости повторите процесс для остальных серверов, пока не будут обновлены все требуемые серверы.

Если нужно обновить какой-либо сервер вручную, откройте его серверный документ в режиме редактирования (**Bdit Mode**). Затем на вкладке **Basics** в поле **Directory Assistance database name** введите имя файла реплики базы данных Directory Assistance на этом сервере. Сохраните и закройте документ.

Все готово для создания документов Directory Assistance.

Установка Directory Assistance для вторичных каталогов Domino

Документ Directory Assistance содержит информацию о домене Notes и его каталоге домена или о LDAP-каталоге, который нужен для осуществления поиска серверам, работающим с Directory Assistance. Разные документы устанавливаются неодинаково, в зависимости от типа документа - для домена Notes или для LDAP-каталога.

Перед тем как создавать документ Directory Assistance для Notes-доменов, следует определить, где расположить документы, на которые будут ссылаться документы Directory Assistance. Надо указать хотя бы одно такое место (но лучше несколько) в документе Directory Assistance для каждого домена. Ниже приведено несколько важных суждений на этот счет:

- О серверам, применяющим Directory Assistance, не требуется хранить реплики вторичных каталогов Domino. Во многих случаях это так, но некоторые серверы с постоянным высокоскоростным доступом должны хранить такие реплики;
- О если каналы связи (в рамках региональной сети) между серверами локального домена Notes и серверами вторичного домена Notes обеспечивают слишком маленькие скорости, ненадежны или перегружены, приходится создавать реплики вторичных каталогов Domino на локальных серверах;
- О если каналы между доменами достаточно быстрые и надежные, то вам могут вообще не понадобиться реплики вторичных каталогов на локальных серверах;
- О если вы определили несколько серверов каталогов, создайте на них реплики;
- О если вы планируете также обращаться к Directory Catalog, то серверы, на которых установлен перечень каталога, скорее всего, имеют реплики вторичных каталогов, включенных в этот перечень.

Нужно обязательно сделать еще одну вещь - полнотекстовый индекс для всех вторичных каталогов Domino, которые будут доступны для LDAP-поиска, то есть сформировать индекс для копий тех баз данных, которые будут перечислены в поле **Replica** (Реплика) документа Directory Assistance.

Когда вы решите, где будут располагаться реплики вторичных каталогов Domino, создайте их. При необходимости постройте для них полнотекстовые индексы. После этого можно создавать документы Directory Assistance для всех вторичных каталогов Domino.

Чтобы установить документ Directory Assistance для вторичного каталога Domino, откройте базу данных Directory Assistance на сервере, имеющем уровень доступа к ней как минимум **Editor**. Сервер, на котором вы формируете документы, должен быть способен реплицировать их, поэтому не выбирайте для этого сервер с доступом **Reader**. Щелкните на панели инструментов по кнопке **Add Directory Assistance** (Добавить поддержку каталога). Появится новый документ Directory Assistance. Заполните необходимые поля и сохраните его. Когда при репликации этот документ будет скопирован на остальные серверы, он станет полностью функционирующим.

Документы Directory Assistance для каталогов Domino имеют три вкладки:

- О **Basics** (Основные параметры) - здесь вводится разнообразная информация о домене, который представляет каталог Domino;
- О **Rules** (Правила) - на ней указываются шаблоны заданных имен, которые могут быть найдены в каталоге Domino. Такие шаблоны позволяют заранее определить, в каком

каталоге лучше искать определенное имя. Они также указывают серверу Domino, может ли он посредством реквизитов системы защиты, находящихся в этом каталоге, аутентифицировать пользователя, чье имя соответствует шаблону;

- О **Replicas** (Реплики) - служит для размещения ссылок на вторичные каталоги Domino либо их имен и мест хранения.

Вкладка **Basics**

Поля, расположенные на вкладке **Basics**, перечислены в табл. 11.10.

Таблица 11.10. Поля, расположенные на вкладке **Basics** документа *Domino Directory Assistance*

Поле	Комментарии
Domain type (Тип домена)	Выберите Notes
Domain name (Имя домена)	Если вторичный каталог Domino представляет домен Notes, введите здесь имя домена Notes. Если же вторичный каталог не представляет домен (например, он хранит имена Web-пользователей, зарегистрированных на одном или нескольких Web-серверах Domino), укажите любое выдуманное имя домена. Не задавайте имя реального домена
Company name (Название компании)	Поместите здесь название компании, которая связана с доменом, указанным в предыдущем поле
Search order (Порядок просмотра)	Назначьте порядок просмотра каталогов. Сервер сначала попытается следовать правилам (установленным на вкладке Rules), чтобы определить каталог, в котором нужно искать информацию. Если ему не удастся найти подходящее правило, он будет просматривать все доступные каталоги в порядке, указанном в этом поле. Чем меньше номер, тем раньше будет изучаться каталог. Два каталога с одинаковыми номерами просматриваются в алфавитном порядке
Enabled (Разрешено)	По умолчанию указано Yes . Чтобы временно сделать каталог недоступным для поиска, поменяйте на No

Вкладка **Rules**

Вкладка **Rules** состоит из полей, в которых можно вводить до пяти правил присвоения имен для каталога. Каждое такое правило позволяет задавать допустимые имена для каждого уровня иерархии присвоения имен Notes (организационные единицы разного уровня, организация, затем страна) - OU4, OU3, OU2, OU1, O и C. Допустимо также включать и выключать отдельно каждое правило. Можно отметить, разрешено ли пользователю, чье полное различающееся имя соответствует указанному шаблону, аутентифицироваться с помощью реквизитов, находящихся во вторичном каталоге. Это существенно только для Web-пользователей; пользователи Notes всегда в состоянии обратиться к кросс-сертификату, если он их затрагивает.

Первое правило для каждого уровня иерархии состоит из подстановочного символа «звездочка» (*). Это делает каталог доступным для поиска, если из всей информации об искомом объекте известно только его общее имя. Первое правило обычно установлено сразу и сразу же разрешено для применения.

Для всех остальных правил необходимо ввести иерархические составляющие имени, которые могут находиться в соответствующем вторичном каталоге. Например, если каталог содержит записи о членах организации /PlanetNotes, требуется указывать в поле **Organization** (Организация) значение /PlanetNotes, а во все остальные поля поставить звездочки. Это будет означать, что, если имя объекта в качестве составляющей **Organization** имеет значение /PlanetNotes, сервер должен искать такой объект в данном каталоге.

В больших компаниях может быть одна организация (например, /PlanetNotes), но несколько доменов, каждый из которых предназначен для одного бизнес-подразделения компании. Каждое подразделение в свою очередь представлено уникальным именем OUI. Допустим, что подразделение Variable Annuities (Выплаты дивидендов) имеет уникальное имя /VA/PlanetNotes, а подразделение Funds (Финансирование) - имя /Funds/PlanetNotes. Тогда правило для VA выглядит так: OUI=VA, 0=PlanetNotes, а для Funds - так: OUI=Funds, OPlanetNotes. Сервер, выполняющий поиск, будет знать, что большую часть информации об искомом объекте можно найти в каталоге, обозначенном с помощью этих правил.

Вкладка Replica

Здесь вводится информация о расположении одной или нескольких реплик требуемого каталога. Создание нескольких доступных реплик обеспечивает защиту от сбоев, которую не гарантирует отдельная копия. Обратите внимание, что, если вы формируете реплику на кластерном сервере, автоматического копирования на другой сервер кластера не происходит; необходимо явно указать каждую реплику в группе, которая должна быть доступна.

Можно ввести либо ссылку на каждую реплику в поле **Database links** (Ссылки базы данных), либо имя сервера и имя файла каталога для каждой реплики. Сервер, выполняющий поиск, будет пытаться просматривать реплики в порядке их перечисления. Существует возможность временно запретить доступ к определенной реплике. Это удобно, когда требуется на некоторое время отключить определенный сервер или копию.

Если вы поместите и ссылку на базу данных, и имя сервера и файла базы данных, поле **Replica** будет обладать преимуществом.

Установка Directory Assistance для LDAP-каталогов

Установка Directory Assistance для LDAP-каталогов немного отличается от установки для серверов Domino. Обычно вам не нужно беспокоиться о репликации LDAP-каталога - достаточно соединиться с ним, где бы он ни находился. Вместо вкладки **Replicas** появляется вкладка **LDAP**, на которой указывается информация, касающаяся LDAP.

Вкладка Rules

Как и для вторичных каталогов Domino, в этом поле указываются иерархические составляющие имен, которые могут находиться в определенном вторичном каталоге. Это позволяет серверу, выполняющему поиск, быстро сосредоточиться на базе данных, вероятнее всего содержащей нужную информацию.

Чтобы разрешить аутентификацию в определенном LDAP-каталоге, можно использовать поле **Trusted for Credentials** (Доверять реквизитам) в каждом правиле. Если в данном

поле установлено Yes, то в случае попытки Web-пользователя аутентифицироваться при соответствии имени пользователя указанному правилу Domino сделает это на основании реквизитов (сертификата или пароля), расположенных в каталоге LDAP.

Вкладка Basics

Поля, имеющиеся на вкладке Basics, описаны в табл. 11.11.

Таблица 11.11. Поля, расположенные на вкладке Basics документа ЮAP Directory Assistance

Поле	Комментарии
Domain type (Тип домена)	Выберите LDAP
Domain name (Имя домена)	Введите любое описательное и уникальное имя
Company name (Название компании)	Укажите название компании, которая владеет LDAP-сервером, назначенным данным документом
Search order (Порядок просмотра)	Задайте порядок просмотра каталогов. Сервер сначала попытается действовать по правилам (установленным на вкладке Rules), чтобы определить каталог, в котором нужно искать информацию. Если он не может найти подходящее правило, то просматривает все доступные каталоги в порядке, определенном в этом поле. Чем меньше номер, тем раньше будет просматриваться каталог. Если два каталога имеют одинаковые номера, то они просматриваются в алфавитном порядке
Group expansion (Расширение групп)	Можно установить Yes или No . Задавайте Yes , только если хотите изменять имена членов групп, определенных на данном LDAP-сервере. Это поле допускается активизировать лишь для одного LDAP-каталога
Enabled (Разрешено)	По умолчанию Yes . Чтобы временно сделать каталог недоступным для поиска, поменяйте на No

Вкладка LDAP

Вкладка LDAP содержит поля, в которых записывается информация, позволяющая серверу Domino соединяться и обращаться к LDAP-серверу. Поля описаны в табл. 11.12.

Таблица 11.12. Поля, расположенные на вкладке LDAP документа LDAP Directory Assistance

Поле	Комментарии
Hostname (Имя хоста)	
Base DN for search (Базовое доменное имя для поиска)	серверы) требуют предоставления базы поиска, которая сообщает серверу, какую часть его дерева вы хотите просмотреть. База поиска — это крайняя правая часть различающегося имени (например, O=planetnotes, C=US)
Perform LDAP search for (Выполнять LDAP-поиск для)	Существуют следующие варианты: Notes Clients/Web Authentication и LDAP clients . Укажите один из них или оба
Channel encryption (Шифрование канала связи)	Выберите SSL или None . Lotus настоятельно рекомендует применять SSL, если вы будете обращаться к сторонним серверам для получения реквизитов при аутентификации Web-пользователей

Таблица 11.12. Поля, расположенные на вкладке **LDAP** документа *LDAP Directory Assistance* (окончание)

Поле	Комментарии
Port (Порт)	По умолчанию 389, если предыдущее поле установлено в None ; 636, когда в предыдущем поле задано SSL . Измените это значение, если LDAP-сервер на самом деле пользуется другим портом
Accept expired SSL certificates (Принимать просроченные сертификаты SSL)	Укажите Yes , чтобы игнорировать истечение срока действия сертификата. Для установки сроков действия сертификатов введите No
SSL protocol Version (Версия протокола SSL)	Выберите Negotiated (Согласовывать) или определенную версию. Другие версии указывайте только в случае, когда Negotiated не работает
Verify server name with remote server's certificate (Сравнивать имя сервера с удаленным сертификатом сервера)	Lotus настоятельно рекомендует активизировать данное поле, если вы доверяете LDAP-серверу вопросы аутентификации. Это требует включения имени LDAP-сервера в строку Subject сертификата сервера
Timeout {Тайм-аут}	Время в секундах, в течение которого выполняется поиск. По умолчанию 60 секунд
Maximum number of entries returned (Максимальное число возвращаемых записей)	Введите максимальное число записей, которые удастся получить в результате одного запроса на поиск. По умолчанию 100

Серверы каталогов

Если вы администрируете большой домен с тысячами почтовых пользователей, имеет смысл назначить один или несколько серверов каталогов (Directory server) для предоставления служб каталогов, таких как поиск. Обычно эти службы обеспечивает почтовый сервер. Однако при перенесении службы поиска в другое место почтовый сервер освободится и будет лучше выполнять обязанности, относящиеся к почтовой службе. Таким образом, он сумеет обслуживать большее количество пользователей электронной почты.

Сервер каталогов обычно содержит реплики Server Directory Catalog и иногда Mobile Directory Catalog, может иметь реплики базы данных Directory Assistance И~~ххх~~хх вторичных каталогов Domino. Этот сервер позволяет производить поиск, а также способен быть «сервером-строителем», собирающим перечни каталогов. И наконец, он в состоянии поддерживать службу LDAP, чтобы у LDAP-клиентов была возможность осуществлять поиск.

Для настройки сервера каталогов необходимо сделать одну вещь (кроме выполнения мероприятий, связанных с установкой соответствующих служб каталогов) - информировать своих пользователей, чтобы они отправляли запросы на поиск не на почтовые серверы (как задано по умолчанию), а на назначенный сервер.

Лучше всего это сделать, указав данный сервер в профилях **User Setup Profile**. В поле **Directory Server** вкладки **Basics** профиля **User Setup Profile** введите имя соответствующего

сервера каталогов. Когда после репликации изменений на почтовый сервер пользователь в очередной раз подключится к своему серверу, Notes обнаружит изменения в документе профиля и обновит документ местоположения данного пользователя.

Если нужно вручную изменить параметры пользователя, добавьте имя сервера каталогов в поле **Domino directory server** (Сервер каталогов Domino) в соответствующем документе местоположения.

ГЛАВА 12

ОБСЛУЖИВАНИЕ ПОЛЬЗОВАТЕЛЕЙ И УСТРАНЕНИЕ НЕПОЛАДОК

Жизнь была бы гораздо проще, если бы наша прекрасно работающая система не ломалась. Но пользователи приходят и уходят, изменяют свои имена или просто перемещаются в пределах компании, заставляя нас обновлять записи, переносить их базы данных на другие серверы. Иногда пользователь может даже забыть свой пароль, заставляя администратора использовать программу Password Recovery, чтобы он сумел войти в систему своего компьютера.

Большинство изменений, описанных в этой главе, можно выполнить с помощью либо Domino Administrator, либо каталога Domino, либо Web Administrator или NT User Administration. Обсуждается работа с программой Domino Administrator, поскольку она имеет больше всего средств и ее проще всего применять, но там, где подходят другие способы, рассмотрены и они. Описывается также процесс изменения или удаления одного пользователя, причем почти во всех случаях допустимо, выделив нескольких пользователей, обновить или убрать их одновременно. Удалением, конечно же, является изменение имени пользователя. Изменения нужно делать по очереди.

Термин «переименование пользователя» обычно означает изменение имени человека в его персональном документе. Но в системе Notes заверители, участвующие в процессе создания ID-файлов пользователя, также становятся частью его имени. Таким образом, если мы хотим переместить пользователя из отдела продаж в отдел маркетинга, переименовать и создать новый сертификат для него сможет только заверитель отдела маркетинга. С другой стороны, когда мы перемещаем пользователя с одного сервера на другой, мы действительно перемещаем его почтовый файл на другой сервер.

Переименование пользователей

Существует всего три действия, которые выполняются при переименовании пользователя:

- обновление в иерархии - обновляются данные любого пользователя, который был создан с помощью фиксированного сертификата;
- изменение общего имени - общее имя пользователя меняется при изменении его семейного положения или в случае, если была допущена ошибка в процессе создания ID-файла пользователя;

О запрос перемещения к новому заверителю - перемещение «мысленное», однако пользователь на самом деле переименовывается новым заверителем, который обслуживает какой-либо отдел или местоположение.

Все эти изменения, за исключением общего имени, которое мы рассмотрим при изучении способов изменения по запросу, выполняются с помощью процесса Administration Process (AdminP).

Почему переименование подразумевает не просто изменение имени пользователя в персональном документе или создание нового ID? Открытый ключ пользователя служит для подписи полей и документов. Имя пользователя может содержаться в поле **Reader Names** (Имя читателя) или **Author Names** (Имя автора) в документах, а также в списке ACL и в некоторых группах в каталоге Domino. Поиск и изменение всех экземпляров у администратора иногда занимают дни или недели. Умножьте затраченное время на количество запросов - и вскоре это перестанет казаться очень увлекательной работой. К счастью, AdminP выполняет большую часть описанных действий (если не все), и можно не беспокоиться - все будет сделано правильно. Представьте, что вы изменили имя пользователя в персональном документе и во всех базах данных и ACL, где оно встречается, а пользователь не узнал об этом. Его ID-файл будет содержать исходное имя, и доступ ко всем базам данных, а возможно, и ко всем серверам окажется для него закрытым. Процесс AdminP

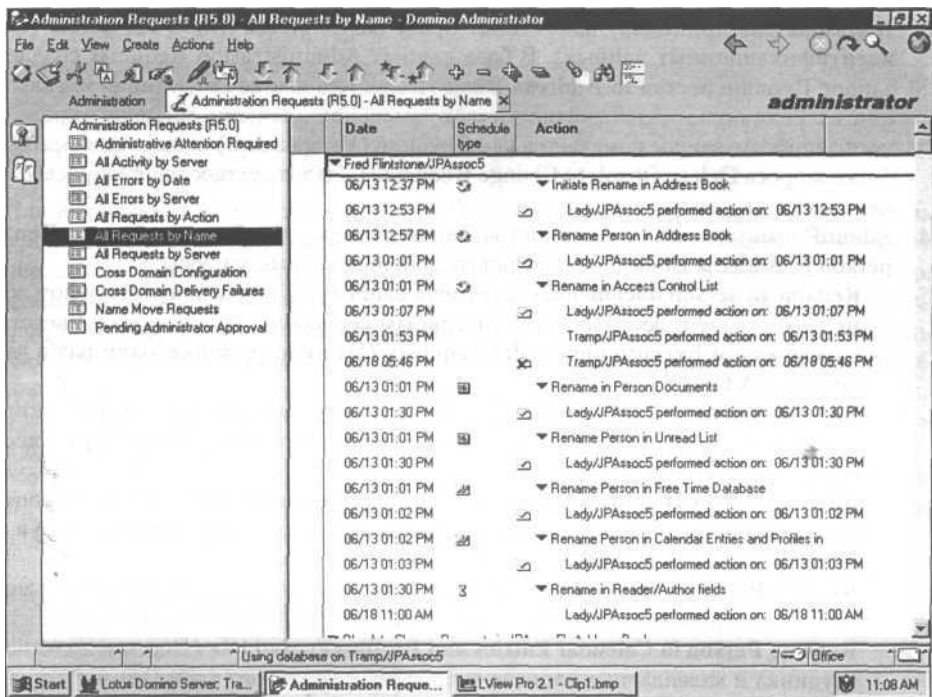


Рис. 12.1. С помощью вида All Requests by name (Все запросы по имени) отображаются все запросы для одного пользователя

гарантирует, что ни такие, ни другие ошибки не лишат пользователя правомерного доступа к его собственным базам данных.

Первым шагом при переименовании пользователя является запрос на переименование. В базе данных Administration Requests (Административные запросы), с которой работает AdminP, создается документ (рис. 12.1). Проследим, что происходит с запросом, а затем рассмотрим, как создавать запросы для различных действий переименования.

Этапы работы AdminP при переименовании пользователя

Различают следующие этапы процесса переименования:

1. Запрос на изменение создает в базе данных Administration Requests запрос **Initiate rename in Address Book** (Инициализация переименования в адресной книге). Процесс AdminP выполняется на сервере, который является административным для каталога Domino, обрабатывает запрос, добавляет новое имя и сертификат, затем меняет запрос на персональный документ пользователя.
2. Пользователь аутентифицируется на сервере. Поскольку создан запрос на изменение, сервер предлагает пользователю принять изменения. Если аутентифицирующий сервер не обрабатывает запрос AdminP к каталогу Domino, то каталог должен быть реплицирован на сервер пользователя, чтобы там был сформирован и представлен пользователю запрос на принятие изменений.
3. Пользователь принимает изменения. Сразу же меняется имя в ID-файле (файл идентификационных данных). В базе данных Administration Requests создается запрос **Rename person in Address Book** (Переименование сотрудника в адресной книге). Если пользователь не принимает изменения в течение времени, определенного запросом, запрос помечается как **Obsolete** (Устаревший) и удаляется при обработке запроса **Delete Obsolete Change Requests** (Удалить устаревшие запросы на изменение).
4. AdminP выполняется на административном сервере, обрабатывает запрос **Rename person in Address Book** и создает новые дополнительные запросы:
 - **Rename in person documents** (Переименование сотрудника в персональном документе) - выполняется административным сервером каталогов в соответствии с параметром **Execute once a day requests** (Исполнять запрос один раз в день) процесса AdminP;
 - **Rename person in Unread Lists** (Переименование сотрудника в списке блокировки чтения) - выполняется каждым сервером в соответствии с параметром **Execute once a day requests** процесса AdminP;
 - **Rename in Access Control List** (Переименование в списке управления доступом) - выполняется каждым сервером в соответствии с параметром **Execute once a day requests** процесса AdminP;
 - **Rename Person in Free Time Database** (Переименование сотрудника в базе данных свободного времени) - выполняется немедленно локальным сервером пользователя;
 - **Rename Person in Calendar Entries and Profiles in Mail File** (Переименование сотрудника в календарных записях и профилях почтового файла) - выполняется немедленно локальным сервером пользователя;
 - **Rename in Reader/Author Fields** (Переименование в полях Reader и Author) - выполняется каждым сервером в соответствии с параметром **Delayed Request** (Отложенный запрос) процесса AdminP.

Если запрос не обработан, он помечается красным знаком X. Откройте запрос и проверьте **Action Message** (Сообщение о выполнении), чтобы узнать, почему это произошло. Разобравшись в проблеме, установите флажок **Run Request Again** (Запустить запрос еще раз), чтобы AdminP снова обработал запрос. Измените запрос, если, к примеру, вы неверно ввели имя пользователя в запросе на смену его имени, что и вызвало отказ.

Не исключена ситуация, когда запрос обработан, но никак не помечен. Возможно, запрос был на изменение всех полей **Reader/Author** в базах данных сервера, но сервер не является административным ни для одной из указанных баз данных, поэтому сообщение о выполнении здесь будет именно таким.

Теперь рассмотрим, что происходит после создания запроса, обсудим различные типы запросов поддержки пользователей и то, как эти запросы формируются.

Обновление в иерархии

Ниже перечислены достоинства иерархического присвоения имен (возможно, в вашей организации оно еще не практикуется):

- О люди с одинаковыми именами будут различаться по организационным единицам;
- О применение средств версии 5 и 6, включая AdminP, упрощает администрирование пользователей;
- О кросс-сертификация облегчает доступ пользователям одной организации к серверам другой организации.

Есть проблемы при выполнении изменений?

Для выполнения изменений необходимо ознакомиться с разделом, посвященным предварительным условиям регистрации, в главе 5.

Для выполнения изменения в каталоге Domino откройте вид **People**, отметьте пользователей, чьи записи необходимо обновить, и выберите **Actions => Rename selected people** (Операции => Переименовать выделенных пользователей), затем щелкните по кнопке **Upgrade to Hierarchical** (Обновить иерархию). Если вы работаете в Domino Administrator, откройте вкладку **People and Groups**, выберите задачу **People** и отметьте имена пользователей, которые необходимо обновить. Откройте инструмент **People** и щелкните по **Rename**. Появится диалоговое окно **Rename Selected Entries** (Переименовать выбранные записи) в версии R5 или **Rename Selected Notes People** (Переименовать выделенных пользователей Notes) - рис. 12.2. #

Можно изменить число дней, установленное для обработки запроса, - это период времени, в течение которого запрос будет находиться в базе данных Administration Requests, ожидая^ чтобы пользователь принял изменения.

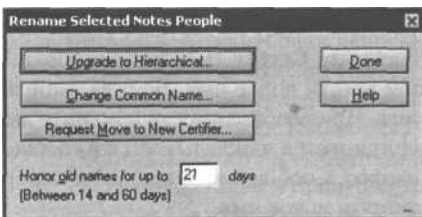


Рис. 12.2. Для обработки запроса на переименование по умолчанию требуется 21 день

Изменение общего имени

Иногда кому-нибудь нужно сменить имя в своем ID-файле. Обычно пользователь обращается в службу технической поддержки или непосредственно к администратору, то есть к вам, и просит изменить его имя. Вы можете начать процесс переименования. Однако существует несколько способов, когда пользователь вправе сам создать запрос на переименование с помощью Notes, поэтому сначала рассмотрим эти способы.

Запрос по инициативе пользователя

Пользователь сам может инициировать запрос на вкладке **More Options** (Дополнительные параметры) в диалоговом окне **User ID**. Выберите **File => Tools => User ID** (Файл => Программные инструменты => Файл идентификационных данных пользователя) - рис. 12.3.

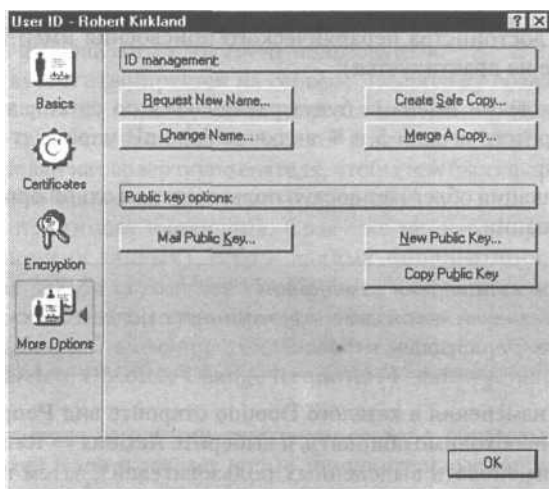


Рис. 12.3. Пользователь может инициировать запрос на переименование с помощью встроенных средств Notes

В вашей папке **Inbox** (Входящие) появится запрос, инициированный пользователем. Тема сообщения дает пояснения о том, как сертифицировать и вернуть ID-файл пользователю. Выполните **Actions => Certify Attached ID file** (Операции => Сертифицировать вложенный ID-файл). Система запросит имя заверителя. Укажите имя того заверителя, который использовался при первом создании ID-файла. Появится другое окно, в котором можно изменить длину пароля, срок его действия или добавить имя пользователя на альтернативном языке. Длина пароля по умолчанию равна 0, поэтому не забудьте установить значение, которое принято в вашей организации. Нажмите **Certify** (Сертифицировать). Откроется еще одно диалоговое окно с предложением ввести новое имя. Во всех записях будет указано то имя, которое запрашивал пользователь. При необходимости измените любые записи и щелкните по **OK**. ID-файл вновь сертифицируется и вкладывается в сообщение, адресованное пользователю, который прислал запрос. Сообщение будет также содержать инструкции, которые помогут пользователю принять новое имя.

Имейте в виду, что если пользователь выйдет из Notes прежде, чем получит вновь сертифицированный ID-файл, то при следующих попытках аутентификации в момент входа в систему появится сообщение об ошибке (рис. 12.4). Пользователь должен щелкнуть по ОК, чтобы обойти его. Ошибка возникает потому, что открытый ключ пользователя в каталоге Domino был изменен, а в ID-файле пользователя остался старый вариант. Пользователь будет получать такое сообщение, пока не примет ответное почтовое сообщение, не откроет его и не обновит свой ID-файл. За более подробной информацией об этой ошибке обратитесь к Technote #147165 «Error Updating Local ID File...Required Parameter in a Subroutine Call...» в базе знаний Lotus Notes (<http://www.lotus.com/support>).

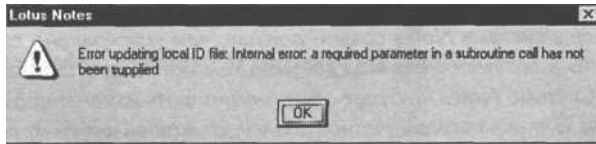


Рис. 12.4. Если пользователь пытается получить доступ к серверу прежде, чем внесет новое имя в ID-файл, выдается сообщение об ошибке

Хотя такой процесс достаточно эффективно меняет имя пользователя, он не затрагивает Administration Process. Поэтому имя пользователя остается прежним в списке ACL, документах групп или полях **Reader/Author**. Вы можете не рассматривать запросы в своем почтовом ящике, а создавать собственные запросы с помощью одного из методов, описанных далее, чтобы реализовать все возможности Administration Process (и впоследствии сэкономить время).

Запрос на переименование по инициативе администратора Notes

Существует два способа инициировать процесс переименования, если пользователь обращается в службу технической поддержки или непосредственно к вам:

- О в каталоге Domino выделите имя пользователя и используйте команду **Rename selected people** (Переименование выделенных сотрудников);
- О в программе Domino Administrator откройте каталог организации, выберите вкладку **People & Groups**, выделите пользователя и выполните **People => Rename** (Сотрудник => Переименовать).

В любом случае на экран будет выведено диалоговое окно **Rename Selected Entries** или **Rename Selected People**, как показано на рис. 12.2. Укажите **Change Common Name** (Изменить общее имя). Запустите процесс изменения имени:

1. Выберите заверителя в диалоговом окне **Choose Certifier ID**, введя, если требуется, пароль.
2. В диалоговом окне **Rename Selected User** внесите необходимые изменения для имени пользователя, срока действия ID-файла и при желании добавьте значение для **Qualifying Organization Unit** (Квалификационная организационная единица). Если вы задали **Synchronizing Notes and Windows NT Users**, как описано в главе 6, то установите флажок **Rename NT User Account** для автоматического переименования учетных записей пользователя в операционной системе NT.
3. Нажмите **Rename** и проверьте базу данных Administration Requests, чтобы убедиться, что в нее занесены новые запросы.

Изменения в NT User Admin по инициативе администратора

Программу NT User Administration не рекомендуется применять для изменения полного имени пользователя Notes. После синхронизации изменений новое полное имя появится только в персональном документе пользователя.

Если имя пользователя изменяется в NT, то при синхронизации пользователя с Notes обновляется поле **Network Account Name** (Имя в сетевой учетной записи) в персональном документе и можно дополнительно установить одинаковые пароли для Domino в сети Internet и системе NT.

«Несинхронизируемая» Molly Brown

Если пользователь в системе Notes создан раньше, чем установлено средство NT User Synchronization, то в его персональном документе может отсутствовать поле **Network Account Name**. Система Notes не будет синхронизировать измененное имя пользователя, у которого нет имени в сетевой учетной записи, служащей для синхронизации. К счастью, если для синхронизации пользователей вы настроили NT User Administration, можно пометить имя **NT User Name** в учетную запись, выполнив в программе NT User Administration команду **Notes => Sync Selected NT Users with Notes**. Если NT не может найти пользователя в Notes, появляется сообщение об ошибке и в NT Event Log (Журнал событий NT) заносится запись о событии.

Запрос на перемещение к новому заверителю

Третий тип переименования - изменение организационной единицы или даже организации в ID-файле пользователя.

Например, заверитель /Marchcreek/Stillwater использовался для сертификации пользователя Боба Доббса (Bob Dobbs), ID-файл и имя Notes которого построены с помощью имени заверителя. Предположим, что Боб переходит в новое место Philly. Чтобы переместить его на новое место/отдел (организационную единицу) мы должны переименовать его, обратившись к другому заверителю.

Для переименования и перемещения в новую организационную единицу выделите имя Боба в каталоге Domino или, если вы работаете в Domino Administrator, откройте вкладку **People & Groups** и отметьте его имя там. В каталоге Domino выберите **Actions => Rename Selected People**. В Domino Administrator используйте **People => Rename**. В обоих случаях появится диалоговое окно **Rename Select People**, в котором нужно щелкнуть по кнопке **Request Move to New Certifier** (Запрос на перемещение к новому заверителю[^] и выполнить следующие действия:

1. Выберите заверителя, который указывался при создании ID-файла пользователя. Возможно, будет запрашиваться пароль.
2. В диалоговом окне **Request Move for Selected Entries** (Запрос на перемещение выделенных записей) введите имя нового заверителя. В данном случае воспользуйтесь сертификатом /Philly/Stillwater, чтобы переместить Боба в новую организационную единицу (рис. 12.5).
- 3. Щелкните по **Submit Request** (Создать запрос) и удостоверьтесь, что запрос появился в базе данных Administration Requests.
4. Время от времени проверяйте базу данных Administration Requests, чтобы в ней не возникало ошибок. Процесс не начнется, пока пользователь не примет новое имя, как описано выше.

<

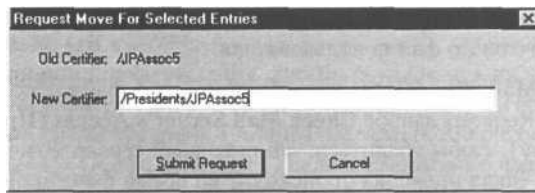


Рис. 12.5. Введите имя заверителя организации. Если вы ошиблись в его написании, откроется окно с сообщением об ошибке, связанной с несуществующим именем заверителя

Перемещение пользователей

В отличие от процесса перемещения пользователя к новому заверителю, рассмотренного только что, процесс перемещения пользователя на новый сервер действительно подразумевает некоторые реальные перемещения. Поскольку пользователь может аутентифицироваться на любом сервере, к которому у него есть доступ, нет смысла в употреблении понятия «домашнего» сервера, кроме как применительно к серверу почтовых файлов. Фактически пользователь соединяется или аутентифицируется со сквозным сервером, а почтовый файл находится на каком-либо другом сервере.

Предположим, что в предыдущем примере необходимо не только переименовать Боба Доббса с помощью заверителя Philly, но и перенести его почтовый файл в офис Philly - «Hagrier». Можно просто переместить файл, но Боб не будет знать об этом. Выполнение нескольких действий облегчит бедному Бобу жизнь после того, как он переберется на новое место, и ему останется только получить там свою почту.

Если все делать вручную, нужно:

1. Поместить реплику почтового файла на новый сервер.
2. Изменить записи **Mail Server** и **Mail File** в персональном документе.
3. Отключить почтовые маршрутизаторы и реплицировать каталог Domino на все серверы, чтобы не отказала почтовая служба пользователя, а после репликации перезапустить маршрутизаторы.
4. Удалить значок с Рабочего стола пользователя и поместить туда новый ярлык, указывающий на другой почтовый файл.
5. Скопировать персональный документ пользователя, если он переносная из одного домена в другой, и вставить его в новый домен. Затем обновить местоположение почты в новом документе.
6. Удалить исходный почтовый файл (предварительно убедившись, что его уже реплицировали).

Notes значительно упрощает проведение всех указанных действий, поскольку большую их часть совершает процесс AdminP. Все, что мы должны сделать, - это создать запрос и затем подтвердить удаление исходного почтового файла. Однако AdminP делает почти все... Почти!.. Чтобы AdminP правильно выполнил работу, следует удостовериться, что все серверы имеют право реплицировать информацию друг другу. Необходимо поместить группу **LocalDomainServers** в поле **Can Create Replicas** (Разрешено создание реплик) каждого серверного документа.

Как и при переименовании пользователей, процесс AdminP выполняет определенные шаги для переноса почтового файла пользователя:

1. Запрос **Move Mail File** (Перемещение почтового файла) создает в базе данных Administration Requests запрос **Check Mail Server's Access** (Проверка доступа к почтовому серверу), чтобы убедиться, что исходный сервер может сделать реплику на новом сервере. Такая проверка происходит во время формирования запроса, поэтому, если исходный сервер не в состоянии сделать реплику, мы сразу же получим уведомление и сумеем предпринять какие-либо действия для решения проблемы.
2. Если обработка запроса **Check Mail Server's Access** проходит удачно, следует запрос **Create new mail replica** (Создать новую почтовую реплику). Создаются реплика и запрос **Add new mail file fields** (Добавление новых полей в почтовый файл).
3. Запрос **Add new mail file fields** добавляет два поля в персональный документ пользователя - **New Mail Server** (Новый почтовый сервер) и **New Mail File** (Новый почтовый файл), а кроме того, формирует новый запрос - **Monitor new mail file fields** (Мониторинг полей нового почтового файла).
4. Запрос **Monitor new mail file fields** обрабатывается в следующем интервале выполнения процесса AdminP на новом сервере. При этом проверяется, реплицирован ли персональный документ пользователя на новый сервер и отправляется ли почта на новый почтовый файл. Затем следует запрос **Replace mail file fields** (Замена полей в почтовом файле).
5. Запрос **Replace mail file fields** обслуживается на административном сервере для каталога Domino. Он добавляет два новых поля, **Old mail server** (Старый почтовый сервер) и **Old mail file** (Старый почтовый файл), и вносит в них информацию об исходном местоположении почты, а также помещает в основные поля местоположения почты сведения о новых почтовых полях, появившихся на шаге 3. И наконец, запрос устанавливает в персональном документе флаг, указывающий, что необходимо обновить информацию клиента.
6. В процессе аутентификации пользователя его новым почтовым сервером происходят две операции. Первая - документ местоположения пользователя в его персональной адресной книге обновляется, и в него заносятся новое имя почтового сервера и новое местоположение почтового файла. Второе - создается запрос **Push changes to new mail server** (Выталкивание изменений в новый почтовый сервер), который заставляет локальный сервер пользователя перенести все последние изменения из старой базы данных в новую и формирует запрос **Get Information for Deletion** (Получить информацию для удаления). ;*
7. Запрос **Get Information for Deletion** обрабатывается на старом почтовом сервере. Он получает копию почтового файла и делает запрос **Approve file deletion** (Утвердить удаление файла).
8. Теперь и нам придется кое-что предпринять. Мы должны периодически проверять базу данных Administration Requests на наличие заявленных запросов. Проще всего открыть вид **Pending Administration Approval** (Приостановленные административные утверждения) в базе данных Administration Requests. Поступающий туда запрос на удаление почтового файла следует подтвердить. Выведите документ на экран в режиме редактирования и щелкните по кнопке **Approve File Deletion** (Утвердить удаление файла). Появится окно подтверждения, позволяющее при необходимости

отказаться от изменений. Для удаления файла нажмите **Yes**. Откроется контрольное окно. Щелкните по ОК.

9. При нажатии кнопки подтверждения документ удаляется из вида **Pending Administration Approval** и следует запрос **Request File Deletion**. Он обрабатывается в соответствии с параметрами настройки AdminP на исходном почтовом сервере и формирует новый запрос - **Delete Mail File** (Удаление почтового файла).
10. **Delete Mail File** обслуживается на исходном почтовом сервере в соответствии с параметрами процесса AdminP. Наконец, исходный почтовый файл удаляется.
11. Если исходный почтовый файл обращался к общей (совместно используемой) почте, то запрос **Delete Mail File** создает новый запрос - **Delete unlinked mail file** (Удаление несвязанного почтового файла). Это позволяет задаче Object Collect (Сбор объектов) убрать все сообщения из Single Copy Object Store (Хранилище единственных копий объектов) перед окончательным удалением почтового файла, что будет выполнено в соответствии со значением параметра **Interval between purging mail files and deleting when using object store** (Интервал между очисткой почтовых файлов и их удалением с помощью хранилища объектов) в разделе Administration Process серверного документа.

Просуммировав все действия, которые необходимо совершить, и время, требуемое для корректного их выполнения, вы поймете, что очень удобно автоматизировать этот процесс с помощью AdminP. Данную задачу можно инициировать в программе NT User Administration.

Удаление пользователей

При частых перемещениях пользователи засоряют систему различными именами в группах, списках ACL, полях **Reader/Author**, ролях, почтовых файлах (иногда в полнотекстовых индексах), а также в частных видах, папках и агентах для баз данных. Можно позволить AdminP удалить весь этот мусор, инициировав запрос **Delete Person** (Удаление сотрудника). Существует несколько способов создания такого запроса:

- О из каталога Domino, выделив пользователя и выбрав **Delete Person** в меню **Actions** или на панели **Actions**;
- О в программе Domino Administrator, отметив пользователя на вкладке **People & Groups** и выполнив **People Tools => Delete**;
- О в программе Web Administrator, открыв персональный документ и указав **Delete Person** на панели **Actions**;
- О с помощью NT User Manager.

Все эти действия инициируют запрос **Delete Person** (Удаление пользователя), но с множеством оговорок. Вам не удастся сразу удалить пользователя (как описано далее) в Web Administrator или NT User Manager.

Инициирование запроса Delete Person

Создайте запрос на удаление сотрудника, выполнив одно из описанных ранее действий. Если вы работаете с каталогом Domino или программой Domino Administrator, откроется

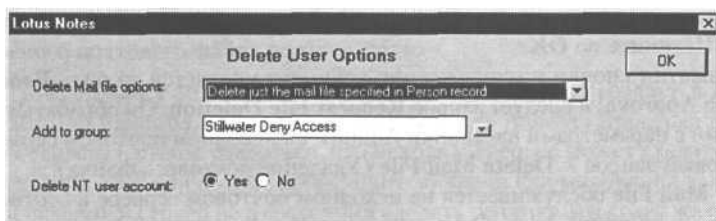


Рис. 12.6. Это диалоговое окно появляется при удалении пользователя средствами каталога Domino или программы Domino Administrator

диалоговое окно для подтверждения удаления пользователя или нескольких пользователей. Нажмите **Yes**. Появится окно, изображенное на рис. 12.6.

Вам надо установить следующие параметры:

- **Delete Mail file** (Удаление почтового файла):
 - **Don't delete mail file** (Не удалять почтовый файл) - выберите, чтобы оставить почтовый файл пользователя на сервере;
 - **Delete just the mail file specified in Person record** (Удалить только почтовый файл, указанный в персональной записи) - позволяет провести удаление только на почтовом сервере пользователя. Если вы не создавали реплики почтовых файлов пользователей на других серверах, отметьте этот вариант;
 - **Delete the mail file specified in Person record and all replicas** (Удалить почтовый файл, указанный в персональной записи, и все его реплики) - установите данный вариант, если формировались реплики почтовых файлов на других серверах, в целях перестраховки в случае отказа сервера. При задании этого параметра появляются дополнительные запросы в базе данных Administration (Администрирование), заставляющие *все* серверы искать реплики указанного файла. Не следует назначать серверы, на которых находятся реплики;
- **Add to group** (Добавить в группу). Введите или выберите имя группы (обычно группа **Deny Access**), в которую надо добавить пользователя;
- **Delete NT User Account** (Удалить учетную запись пользователя NT). Щелкните по **Yes**, чтобы удалить учетную запись NT данного пользователя.
- Щелкните по **OK**. Появится другое окно, изображенное на рис. 12.7.

Предупреждение

Ничто не мешает просто удалить персональный документ пользователя из каталога Domino. Однако таким образом не будет устранено имя пользователя из групп, списков ACL и т.д. Если на сервере разрешены анонимные соединения Notes, это может вызвать проблемы с обеспечением безопасности. Самое подходящее время удалять персональный документ - когда он используется только для Web-доступа и не связан с идентификационными данными Notes.

У вас есть на выбор три варианта:

- **Yes** - система Notes немедленно уберет персональный документ пользователя из каталога Domino. После этого агент просмотрит все персональные документы, чтобы

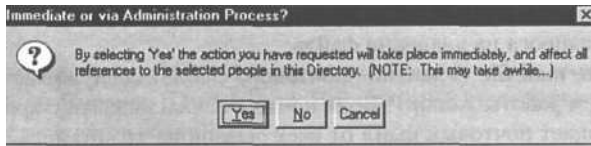


Рис. 12.7. Щелкните по **Yes** - и система выполнит задачи, которые в обычном режиме иницируются запросами **Delete Person** и **Remove from Person Documents**. Эти задачи не запускаются, если вы формируете запрос на удаление пользователя из **Web Administrator** или **NT User Manager**

удалить имя такого пользователя из полей **Owner** (Владелец) и **Administrator** (Администратор). По окончании работы агента в базе данных **Administration Requests** создается запрос **Delete in Access Control List** (Удаление из списка управления доступом);

- **No** - будет инициирован запрос на удаление в базе данных **Administration Requests**;
- **Cancel** - отмена удаления.

Процесс удаления достаточно сложен. Но есть два этапа, которые требуют особого внимания. Первый - подтверждение удаления почтового файла, второй - подтверждение удаления **Private Design Elements** (Частные проектные элементы), то есть частных папок или агентов в приложениях. **AdminP** предпринимает следующие действия:

- запрос **Delete Person in Address Book** (Удалить сотрудника в адресной книге) формируется в любое время в ответ на указание удалить пользователя, за исключением ситуации, когда выбирается немедленное удаление. В последнем случае документ убирается из каталога **Domino**. Запрос обрабатывается в соответствии с расписанием работы **AdminP**;
- по запросу **Delete in Person Documents** (Удаление в персональном документе) имя пользователя ищется в других персональных документах каталога **Domino** и вычищаются любые ссылки. Этот запрос выполняется автоматически, когда задается немедленное удаление пользователя. В противном случае он обрабатывается в соответствии с параметром **Execute once a day** (Исполнять один раз в день) из раздела **AdminP** серверного документа;
- по запросу **Delete in Access Control List** (Удаление из списка управления доступом) имя пользователя удаляется из **ACL** всех баз данных, к которым имеет доступ сервер, обрабатывающий запрос. Выполняется в соответствии с расписанием работы **AdminP**;
- запрос **Delete Reader/Author fields** (Удаление в полях **Reader** и **Author**) удаляет имя пользователя из полей **Reader** и **Author** всех баз данных, к которым имеет доступ сервер, обрабатывающий запрос. Выполняется в соответствии с параметром **Delayed Request** (Отложенные запросы) для **Administration Process** в серверном документе;
- запрос **Get information for deletion** (Получить информацию для удаления) обрабатывается немедленно и получает реплику идентификационных данных почтового файла пользователя для удаления;
- запрос **Approve file deletion** (Подтверждение удаления файла) является первым из тех, которые необходимо подтверждать. Откройте запрос и щелкните по кнопке **Approve File Deletion**. Периодически проверяйте базу данных **Administration Requests** на наличие запросов, ожидающих подтверждения, или ошибочных;

- О запрос **Request file deletion** (Запрос на удаление файла) создается сразу после подтверждения запроса на удаление файла;
- О запрос **Delete mail file** (Удаление почтового файла) обслуживается в соответствии с расписанием работы AdminP. Если почтовый файл связан с хранилищем объекта, AdminP очищает почтовый файл от всех ссылок на хранилище, отменяет репликацию и формирует запрос **Delete unlinked mail file**;
- О запрос **Delete unlinked mail file** (Удаление несвязанного почтового файла) обрабатывается согласно параметру **Interval between purging mail files and deleting when using object store**. Это позволяет задаче Object Collect удалить старые сообщения из хранилища объекта;
- О запрос **Approve deletion of Private Design Elements** (Подтверждение удаления частных элементов проектирования) – второй запрос, нуждающийся в подтверждении. Выведите запрос на экран и щелкните по кнопке **Approve Deletion of Private Design Elements**;
- О запрос **Request to delete Private Design Elements** (Запрос на удаление частных элементов проектирования) инициируется сразу после подтверждения предыдущего запроса;
- О по запросу **Delete Private Design Elements** (Удаление частных элементов проектирования) удаляются частные виды, папки и агенты, хранящиеся в базе данных.

Почему больше не работают агенты?

Если после удаления пользователя из каталога Domino начинают поступать сообщения, что не работают некоторые агенты, проверьте, не отсутствуют ли пользователи таких агентов. Это может сделать пользователь, имеющий право просматривать агенты. Выделите агент и откройте его свойства, выбрав **Properties SmartIcon**. Если в поле **Modified By** (Изменен кем) записан удаленный пользователь, заставьте разработчика с правом запуска агентов на сервере вызвать его и заново сохранить. Теперь агент будет подписан его именем. Можно специально создать отдельный ID-файл, чтобы впоследствии не возникало неприятных ситуаций при уходе одного из разработчиков.

Устранение неполадок

На самом деле не стоит сильно беспокоиться о проблемах пользователей. Их проблемы обычно связаны с испорченными ID-файлами или забытыми паролями, ^ предыдущих версиях Notes все, что вы могли предпринять, сводилось к поиску старой копии их ID-файлов и подходящего пароля.

Сейчас Notes позволяет вместе с ID-файлом хранить информацию для восстановления пароля. Однако, чтобы это сделать, необходимо заставить заверителя создавать ID-файлы с такой информацией и потом заново сертифицировать все ID-файлы. В главе 5 рассказывается, как разрешить восстановление паролей ID-файлов.

Восстановление утерянных паролей

Пользователю, который обращается к вам с заявлением, что он забыл свой пароль, предоставьте возможность восстановить ID-файл и ввести новый пароль. Нужно совершить следующие действия:

1. Переписать свой ID-файл из каталога данных, обычно /Lotus/Notes/Data/user.id, на дискету.
2. Перенести дискету на рабочую станцию коллеги, где есть клиент Notes, и выбрать **File => Tools => Recover ID** (Файл => Программные инструменты => Восстановление идентификационных данных).
3. Откроется диалоговое окно, где перечислены авторизованные пользователи и указано число паролей, необходимых для восстановления идентификационных данных. Пользователю следует обратиться к коллегам, названным в этом списке, и попросить их ввести пароль для восстановления ID-файла.
4. После указания требуемого количества паролей пользователю предлагается задать новый пароль и затем подтвердить его.
5. Теперь пользователю надо перенести восстановленный ID-файл на свою рабочую станцию и записать его вместо старого файла идентификационных данных.

Каждому администратору, к которому обратились за информацией для восстановления, надлежит:

1. Получить копию восстанавливаемого ID-файла. Копия может поступить от пользователя или из центральной почтовой базы данных, которая хранит резервные ID-файлы - вы сами определяете это при создании информации для восстановления у заверителя.
2. Открыть Domino Administrator, щелкнуть по вкладке **Configuration** и выбрать **Certification => Extract Recovery Password** (Сертификация => Извлечь пароль восстановления).
3. На экране в диалоговом окне файла нужно отметить восстанавливаемый файл и щелкнуть по **Open**.
4. Появится диалоговое окно, в котором указано, когда была создана информация для восстановления и когда она была принята, а также приводится пароль для восстановления.
5. Предоставить пользователю пароль для восстановления.

Если пользователь все же не может открыть файл идентификационных данных, скорее всего, файл испорчен. В этом случае необходимо сделать копию ID-файла, которую пользователь будет применять для восстановления, как описано выше.

ГЛАВА 13

ПОДДЕРЖКА КЛИЕНТОВ И УСТРАНЕНИЕ НЕПОЛАДОК

Клиент системы Notes версии 5 и 6 получил много новых средств вместе с изменением внешнего вида привычных средств. Администратор должен обеспечивать техническую поддержку конечного пользователя. Это зачастую означает, что ему приходится быть одновременно и учителем, и специалистом по устранению неисправностей.

В настоящей главе представлен обзор клиента Notes для администратора. Описываются многие новые средства. Однако обсуждение в основном сосредоточено на средствах, представляющих интерес для администратора. Когда речь идет о работе по поддержке пользователей, считается, что администратору следует знать понемногу обо всех аспектах системы Notes. Обзор начинается с ряда инструментов, которые доступны в Lotus и помогают поддерживать работоспособность пользователей.

Средства поддержки и диагностики клиента Notes R6 практически ничем не отличаются от аналогичных средств в версии 5, поэтому в данной главе обсуждаются возможности обеих версий клиента, при этом подразумевается, что все суждения в одинаковой степени относятся как к версии R5, так и к версии R6.

Клиентские средства устранения неполадок

Когда к администратору обращаются с проблемой, возникшей в клиенте Notes, часто приходится анализировать проблемы связи в сети. Чтобы клиент нормально соединился с сервером, нужно проверить состояние линии связи между клиентом и сервером.

Некоторые усовершенствования клиентов Notes требуют, чтобы администратор расширил свой набор средств по устранению неполадок. Например, пользователю может потребоваться отображать содержание какой-либо Web-страницы на своей начальной странице.

Если пользователь не в состоянии соединиться с Web-страницей с рабочей станции Notes, администратор должен проверить соединение клиента Notes с определенной службой или задачей на сервере. Это добавляет новые задачи к обычной работе администратора Notes.

Когда пользователь Notes не может установить связь с сервером, выводится сообщение типа «Server not responding» (Сервер не отвечает). После небольшой паузы звонит телефон у администратора. Быстро проверив ответ сервера со своей рабочей станции, администратор начинает проверять связь с рабочей станции пользователя. Он убеждается, что

рабочая станция не соединяется с сервером. Что же это - проблема Notes, стека протоколов или сети?

Полагая, что в прошлый раз клиент нормально соединялся с сервером, администратор начинает искать, что могло измениться. Существует два широко распространенных метода проверки правильности работы сетевых соединений на компьютере с операционными системами Windows 95/98/NT/2000. Третий способ - попытка акцентировать внимание на Web-связях. Это дополнение требует проверки доступности различных служб Internet. Предусмотрены следующие варианты:

- О общая проверка IP-соединения между рабочей станцией и соответствующим сервером с помощью утилиты PING;
- О отслеживание соединения между нужным сервером и рабочей станцией клиента Notes;
- О применение утилиты NotesCONNECT, которая предоставлена Lotus и контролирует доступность определенных служб на сервере через порты по умолчанию.

Под *службами* понимаются некоторые функциональные возможности, предлагаемые сервером, такие как протоколы HTTP, NNTP или FTP. Каждая служба обращается к нумерованному порту, назначенному руководящим органом. Более детально об этом рассказано в разделе о NotesCONNECT.

Сначала администратор должен узнать некоторую информацию о конфигурации, такую как IP-адрес, имя DNS рабочей станции и сервера. Если в сети не применяется служба DNS, проверьте наличие локального файла hosts или lmhosts. Эти файлы ASCII служат для разрешения (преобразования) числового адреса в имя.

Почему для проверки одного соединения используется три метода?

Каждый из рассматриваемых методов проверяет различные компоненты соединения рабочей станции с сервером. При устранении неполадок в сети обычно движутся от общего к частному. Методы, описанные ниже, удовлетворяют этому принципу.

Проверка IP-соединения состоит в определении того, подключена ли вообще рабочая станция к серверу.

При исследовании Notes-соединения с клиентской рабочей станции предоставляются сведения только о «родном» протоколе Notes (NRPC).

NotesCONNECT информирует о доступности служб на сервере. Это средство аналогично средству TCP probe, имеющемуся в базе данных Statistics & Events. NotesCONNECT функционирует на рабочей станции клиента для проверки доступности служб на сервере.

Проверка IP-соединения

Средство RJNG является традиционным способом проверки состояния связи клиентской рабочей станции со всеми остальными составляющими сети. Большинство администраторов знакомы с ним, поэтому здесь процесс описан вкратце. Существует множество книг, Web-сайтов и учебных курсов, которые более подробно рассказывают об утилите PING. Вам необходимо проверить:

1. Кольцевой адрес сетевого адаптера (PING 127.0.0.1). Если тест прошел успешно, то адаптер отвечает правильно. В противном случае посмотрите сетевой адаптер.
2. Сетевой адрес рабочей станции, чтобы убедиться, что стек TCP/IP настроен корректно и в сети нет другого компьютера с таким же адресом - это может быть причиной

временных проблем соединения, поскольку первая соединяющаяся машина имеет права, предоставленные для данного адреса.

3. Числовой IP-адрес сервера. Положительный отклик означает, что между клиентом и сервером есть связь на уровне протокола IP.
4. Полное различающееся имя домена для сервера Domino (например, PING orion.lotus.com). Клиент Notes обращается к серверу не по числовому адресу, а по имени. В случае успешного теста вы будете знать, что рабочая станция распознает имя сервера.
5. Псевдоним сервера Domino (например, PING OrionDomino), который применяется, когда полное доменное имя отличается от имени сервера Domino. Убедитесь, что в параметрах DNS или файле хостов псевдоним введен правильно.

Где найти IP-адрес сервера или рабочей станции?

Чтобы быстро найти числовой IP-адрес рабочей станции, откройте значок свойств сети на панели управления или введите в командной строке `ipconfig` (только для Windows 9x/NT/2000). Как подразумевает имя команды, `ipconfig` показывает информацию о настройке IP для хоста. Команда `ipconfig /all` отображает настройку не только TCP/IP, но и DNS, WINS, DHCP и NetBIOS.

Если администратор успешно выполнил все указанные действия, а рабочая станция все же не в состоянии соединиться с сервером, нужно посмотреть, правильно ли настроен клиент. Установив, что IP-соединение есть, отследите соединение с рабочей станции клиента Notes. Возможно, изменения были внесены в параметры настройки клиента или даже в параметры сетевого маршрутизатора после того, как пользователь в последний раз успешно связывался с сервером. Отслеживание соединения с рабочей станции клиента поможет выявить проблему.

Отслеживание соединения из клиента Notes

Убедившись в наличии IP-соединения, проконтролируйте соединение из клиента Notes - это позволит понять проблемы соединения, обусловленные параметрами настройками клиента. Например, неверная запись в документе местоположения (Location document) способна привести к сбою соединения, хотя физически оно существует.

Как отмечалось ранее, причина может заключаться даже в значениях Искрытых полей документа местоположения. В таких случаях пользователь получает сообщения типа **Unable to find path to server** (Невозможно найти путь к серверу). Не исключена ситуация, когда в результате изменений фильтра сетевой маршрутизатор пропускает все потоки, кроме трафика Notes. Эта ситуация явно наблюдается при попытке соединения из Internet через брандмауэр.

Отслеживая соединение из клиента Notes, можно увидеть точку, где происходит сбой связи NRPS. В случае изменения в фильтре маршрутизатора, соединение способно успешно пройти через несколько устройств и только после этого разорваться в маршрутизаторе. Проверять сеть из клиента Notes, вы устанавливаете, что клиент работает правильно, и определяете устройство, вызвавшее ошибку. Применение на первом этапе утилиты PING позволяет установить возможность физического соединения двух узлов сети. Тестирование

из клиента Notes отделяет конкретные типы сетевого трафика. В предыдущих версиях Notes с помощью этих двух средств решалось большинство проблем связи между пользователями.

Чтобы отследить соединение от рабочей станции до сервера Domino, откройте раздел **Ports** (Порты) в **User Preferences** (Предпочтения пользователя) и щелкните по кнопке **Trace** (Отследить). Notes попытается установить соединение с указанным сервером.

Если этот клиент в прошлый раз связывался с сервером, то Notes воспользуется IP-адресом, хранящимся в персональной адресной книге (Personal Address Book) клиента. Адрес находится в документе местоположения клиента в скрытом поле **\$SavedAddresses**. Notes всегда старается соединиться с сервером с помощью адреса, записанного в данном поле; это называется кэшированием. Кэширование предназначено для экономии времени при установке связи с сервером. Однако, если адрес сервера был изменен, возможны проблемы.

Предположим, что адрес сервера EagleMountain/Eagle изменили с 169.254.90.26 на 169.254.90.12. Соответствующее изменение было сделано и на вкладке **DNS**. Пользователь уже связывался с EagleMountain/Eagle в прошлом, а теперь при попытке установить соединение он получает сообщение **Unable to find path to server**. Выполняемые тесты - посредством PING сервера по имени или обращения к NotesCONNECT (см. в следующем разделе) - показывают, что сервер существует. А клиент Notes не в состоянии установить соединение. Отследив соединение из клиента Notes, пользователь узнает, что Notes все еще применяет при соединении адрес 169.254.90.26.

Если посмотреть свойства документа местоположения, который употреблялся для соединения с сервером, то значение поля **\$SavedAddresses** покажет старый IP-адрес.

Чтобы выявить подобную проблему, следует удалить текущий документ местоположения из Personal Address Book и создать новый. Это иницирует новый поиск адреса. Либо в файл notes.ini клиента поместить параметр dont_use_remembered_addresses=1. В рассмотренном выше примере представлен практический способ решения проблем пользователя. Применение нужных инструментов позволит сэкономить целый день!

NotesCONNECT

Компания Lotus создала новое средство для проверки соединений TCP/IP с помощью утилиты, которая использует собственный графический интерфейс GUI вместо командной строки или клиента Notes, описанных выше. Для проверки доступности служб через порт Notes по умолчанию (1352) NotesCONNECT применяет вызовы API, чтобы удостовериться в возможности установления соединения TCP/IP от одного компьютера к другому. В отличие от метода, которым отслеживаются соединения с сервером из клиента Notes, NotesCONNECT служит для проверки доступности нескольких других типов служб, кроме Notes.

Поскольку NotesCONNECT применяет функции API, а не интерфейс клиента Notes, это средство позволяет определять, что является причиной проблемы соединения - сеть или клиент Notes. NotesCONNECT не прибегает к информации из Personal Name & Address Book клиента, каталога Dornhino или логики разрешения адресов Notes.

NotesCONNECT подобна утилите PING, но у нее другая методология. PING генерирует IP-пакеты и поддерживает один из протоколов стека TCP/IP - ICMP (Internet Control Message Protocol - протокол управляющих сообщений Internet). NotesCONNECT

проверяет доступность определенной службы через конкретный или «хорошо известный» порт и устанавливает соединение, более похожее на соединение, присущее Domino.

Единственное ограничение этого средства в том, что оно позволяет тестировать указанные службы через порты, установленные по умолчанию. Номера портов по умолчанию присваиваются Internet Assigned Number Authority - центральным авторизатором по присвоению номеров протоколов Internet. Если для общих служб порт назначен по умолчанию, нежелательно, чтобы этот же порт использовало еще одно приложение, вызывая тем самым проблему.

Для просмотра скрытых полей в документе местоположения пользуйтесь NotesPeek

В предыдущем примере на самом деле имеется четыре поля. Для повышения производительности при последующих соединениях в этих полях кэшируется информация о серверах, с которыми в прошлом связывался клиент. Чтобы просмотреть эти поля, откройте страницу **Document Properties** (Свойства документа) для документа местоположения в персональной адресной книге. Поле **\$\$SavedAddresses** содержит только одну запись. В остальных полях может быть несколько значений. Однако в **Document Properties** отражено только одно значение. Просмотреть остальные значения позволяет средство NotesPeek, которое обсуждается далее.

\$\$SavedAddresses содержит имя DNS сервера, числовой IP-адрес или псевдоним.

\$\$SavedPorts определяет порт, через который было установлено соединение с каждым сервером, помещенным в поле **\$\$SavedServers**.

\$\$SavedDate хранит дату последнего соединения со всеми серверами, перечисленными в поле **\$\$SavedServers**.

\$\$SavedServers записывает имена серверов, с которыми соединялся клиент.

Например, серверы Domino соединяются с клиентом Notes через NRPC (Notes Remote Procedure Calls - удаленный вызов процедур Notes). По умолчанию данная служба настроена на порт 1352. Его номер разрешается менять, хотя делается это нечасто. При настройке разведенных серверов¹ желательно настроить конкретные порты для вызовов NRPC (см. руководство по администрированию Notes).

Более общий пример - служба HTTP. По умолчанию она доступна через порт 80. Но может возникнуть много проблем, если на одном компьютере будет установлено несколько Web-серверов. В таких случаях только один Web-сервер отвечает на запросы через порт 80, а другой будет применять, например, порт 8080. Но даже с этим Граничением NotesCONNECT является очень полезным средством, заслуживающим внимания. Более полная информация о нумерации портов по умолчанию содержится в RFC 1340.

Обойти проблему, описанную выше, удастся с помощью значения **Other** в поле **Service List** (Список служб) в окне NotesCONNECT (рис. 13.1). Если известен номер порта, назначенный для службы, которую нужно проверить, выберите в поле **Service List** значение **Other** и введите этот номер в поле **Target Port Number** (Номер требуемого порта). NotesCONNECT проверит доступность запрашиваемого порта, но не сумеет определить, какая служба отвечает через него.

В поле **Target Host Name or IP Address** (Имя требуемого сервера или IP-адрес) вводится либо имя сервера, либо его IP-адрес. В первом случае NotesCONNECT обращается

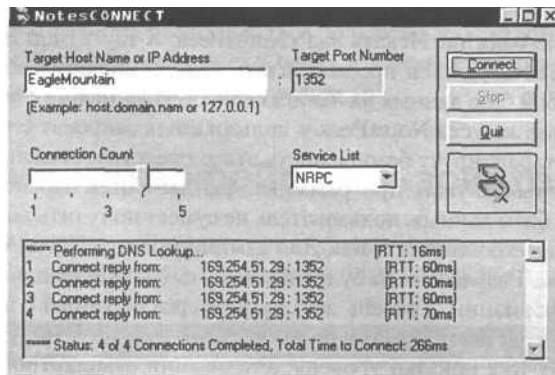


Рис. 13.1. NotesCONNECT успешно установила соединение с Domino-сервером EagleMountain с помощью протокола NRPC через порт 1352

к службе DNS для преобразования имени в IP-адрес. Если имя сервера не указано в таблице DNS или произошла ошибка DNS, допускается задавать непосредственно IP-адрес.

NotesCONNECT в состоянии проверять доступность следующих служб (поскольку Domino поддерживает все эти протоколы, администраторы убедятся, что NotesCONNECT - крайне удобное средство):

- О NRPC;
- О DIIOP;
- О FTP;
- О HTTP;
- О HTTPS;
- О ШАР;
- О LDAP;
- О NNTP;
- О POP;
- О SMTP;
- О SOCKS Proxy.

Компания Lotus официально не распространяет и не поддерживает NotesCONNECT. Однако эту утилиту можно найти в Notes.Net по адресу: <http://notes.net/sandbox.nsf>. Пояснительная статья есть в Notes.Net в разделе Webzine. Следует искать Testing TCP/IP Connections with NotesCONNECT.

NotesPeek

Еще одно «неофициальное» средство, которое можно получить у Lotus, позволяет пользователю заглядывать внутрь базы данных Notes. Как и NotesCONNECT, NotesPeek использует собственный интерфейс и предоставляет почти всю информацию, которую только может видеть клиент Notes в базе данных.

Представьте себе возможность увидеть число удалений, просмотреть элементы проектирования, репликацию идентификационных данных (ID) или базу данных DBIID, используемую журналом транзакций. Это замечательное средство совместимо с версиями R4,

R5 и R6. Утилита есть на сайте Notes.Net (<http://www.notes.net/sandbox.nsF>), а пояснительная статья - в разделе Webzine. Искать надо NotesPeek: X-ray Vision Into Notes Databases.

С помощью NotesPeek удастся просматривать любую информацию, доступную через интерфейс API в любой базе данных на любом сервере, соединение с которым обеспечивает клиент Notes. После запуска NotesPeek у пользователя запросят его пароль Notes. Разработчик NotesPeek гарантирует безопасность этого средства, так как для просмотра информации базы данных служат программные файлы Notes. Поскольку NotesPeek не обходит списки ACL базы данных, пользователь не сумеет получить доступ к информации, которая недоступна из его клиента Notes. Для администратора NotesPeek может оказаться бесценным средством. Разработчики будут применять NotesPeek для предоставления детализированной информации. Уровень детализации, реализуемый с помощью NotesPeek, гораздо выше, чем требуется обычному пользователю.

Например, на рис. 13.2 показан уровень детализации стандартного почтового файла. Объемы дополнительной информации, добываемой посредством NotesPeek, свидетельствуют, что обычный пользователь клиента Notes, который в состоянии только читать текст сообщения, не получает многих интересных данных.

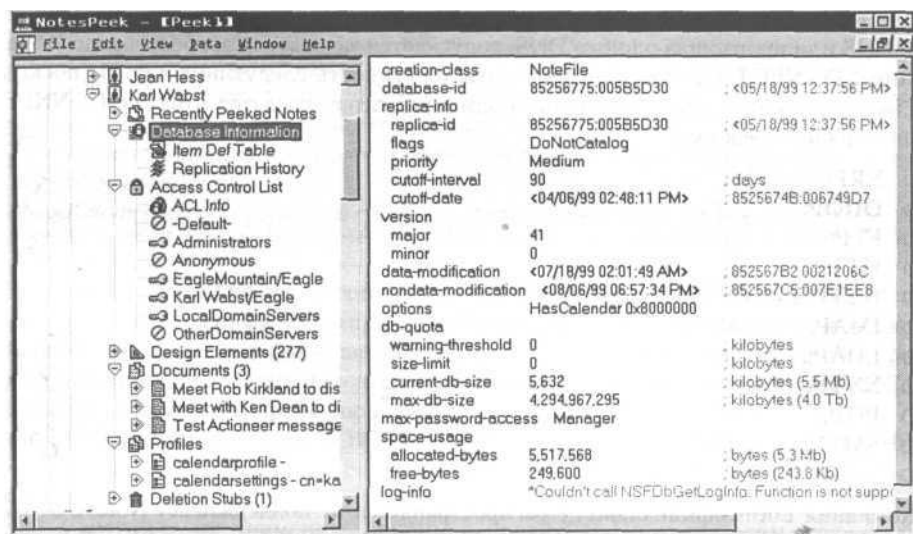


Рис. 13.2. NotesPeek позволяет просматривать все элементы базы данных - от списков ACL до элементов проектирования. Здесь изображена информация для почтового файла R5

NotesPeek дает возможность легко открывать несколько окон, осуществлять поиск и управлять способами показа информации. Если вам нужно поддерживать клиенты Notes, обратитесь к NotesPeek. Как было отмечено, средство NotesPeek полезно при просмотре скрытых значений в документе местоположения пользователя. Администраторы могут также применить NotesPeek, чтобы увидеть число операций удаления в базе данных или для проверки DBIID во время решения с помощью журнала транзакций проблемы возврата в базе данных. Дополнительные возможности выявятся в ходе работы.

Возможно, средство NotesPeek было создано для разработчиков баз данных, однако администраторы могут по-разному распоряжаться большей частью предоставляемой информации. Средства разработки обычно имеют очень высокую стоимость, поэтому зачастую Notes-администраторы не в состоянии их приобрести.

Графический интерфейс пользователя

Теперь, когда мы имеем несколько средств для устранения неисправностей и просмотра содержимого баз данных, настало время взглянуть на интерфейс клиента и его составляющие.

Начальная страница

Наиболее явное различие между Notes R4.x и R5/6 заключается в добавлении нового элемента интерфейса, который компания Lotus назвала **Welcome page** (Начальная страница). Многие пользователи, особенно работавшие с клиентами Notes более ранних версий, отнеслись к этому добавлению скептически.

Начальная страница ставит опытного пользователя в непривычную ситуацию. Многим не нравится, что нужно изучать абсолютно новый интерфейс продукта, который они использовали десятилетиями. В последующих разделах описаны некоторые достоинства и недостатки нового интерфейса. Разрешается поменять или вообще убрать начальную страницу. Потребности компании и отдельных пользователей могут диктовать способ разветвления версий R5/6 среди конечных пользователей. Этот раздел посвящен реализации таких возможностей.

Разработанный заново, интерфейс может быть настроен по желанию пользователя. Однако существует опасность, что если пользователи будут действовать по собственному разумению, то они полностью нарушат управление и сойдут с толку других пользователей. Следует рассматривать обе стороны медали. Некоторые пользователи захотят настроить начальную страницу так, чтобы она показывала план работы на день и была более продуктивной. Другие же пожелают, чтобы на Рабочем столе постоянно была видна их любимая развлекательная Web-страничка. Остальные загонят ее в преисподнюю, чтобы больше никогда не выводить. Вас, как администратора, будут постоянно спрашивать, что нужно сделать, чтобы управлять доступными свойствами или вообще убрать начальную страницу. Вот несколько ответов на эти вопросы.

Редактирование начальной страницы

При запуске клиента Notes появляется *базовая начальная страница*. В правом верхнем углу находится раскрывающееся меню. Изменить вид начальной страницы не составит особого труда даже для новичков.

Обратите внимание, что в R5 кнопка **Options** (Параметры), которая позволяет изменять характеристики экрана, на базовой начальной странице отсутствует. Чтобы увидеть эту кнопку, пользователь сначала должен переключиться на другой вариант оформления страницы. Нужно отметить, что в версии R6 пользовательская настройка начальной страницы предполагает создание нового ее варианта с помощью кнопки **Create new Welcome Page**,

в то время как базовые варианты страницы из раскрывающегося списка служат для получения «стандартных» представлений:

1. Откройте список и выберите один из доступных вариантов оформления экрана, например Basic Plus. Справа от раскрывающегося меню появится кнопка Options (рис. 13.3).

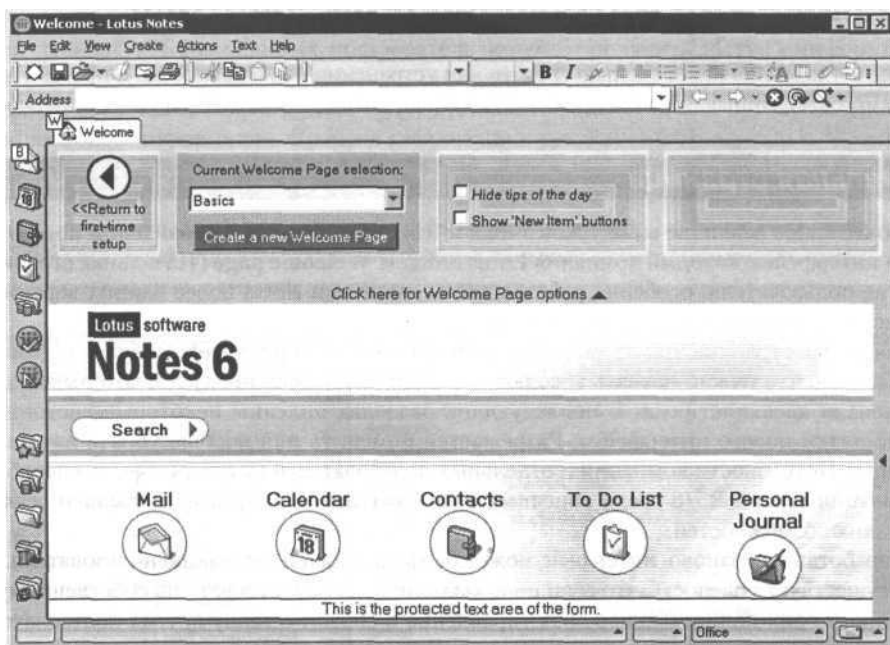


Рис. 13.3. Для настройки внешнего вида начальной страницы пользователя щелкните по кнопке Options

2. Нажатием на кнопку Options выведете на экран окно с несколькими вкладками, в котором допускается поменять макет экрана и число видимых панелей, а также их содержимое.
3. Измените параметры настройки страницы и затем сохраните их под другим именем, которое потом будет присутствовать в раскрывающемся меню. Можно вывести на экран от трех до пяти панелей. Каждый вариант имеет определенный состав по умолчанию.
4. Щелкните по вкладке Content (Содержание) - рис. 13.4, чтобы просмотреть параметры настройки по умолчанию. Пользователю разрешается менять содержимое любых отображаемых панелей.
5. Выберите новое содержимое панели из списка Frame content (Содержимое кадра). Если вы отметите Web Page, то сможете либо указать адрес URL из заранее установленного списка, либо ввести новый. Такие же параметры доступны при задании Quick Links (Быстрые ссылки). Здесь нужно назначить имя, выводимое на экране, и связать с ним URL, который открывается щелчком мышь по этому имени.

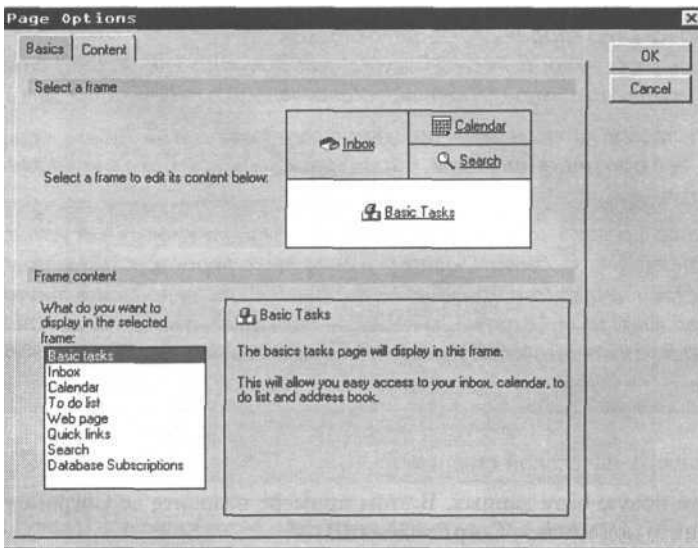


Рис. 13.4. Выберите панель, которую нужно изменить, щелкнув по ней в верхней половине окна Page Options

6. Настроив страницу так, как вам нужно, щелкните по ОК - и начальная страница изменится в соответствии с вашими параметрами настройками.

Например, пользователи могут комбинировать средства Notes и Web-страницы, вставляя на панели ярлыки для объектов, необходимых во время работы. Возможно, какой-то пользователь настроит страницу так, чтобы одна панель содержала ярлыки **Mail**, **Calendar**, **Address Book** и **To Do List**, другая показывала Web-сайт компании, а в остальных были представлены средства поиска для каталога баз данных Notes, LDAP-к-аталогов и средства поиска в Web. Другой захочет, скажем, изменить содержимое одной или нескольких панелей и отображать базы данных или Web-страницы, которые он сам создавал.

Управление начальной страницей

Все это может показаться достаточно разумным. Однако бывают случаи, когда управление начальной страницей со стороны пользователя нежелательно. Некоторые организации строго отслеживают или даже блокируют доступ в Internet. Описываемые методы управления касаются комбинации административных средств и модификации шаблона баз данных bookmark.ntf.

Для управления начальной страницей, появляющейся на рабочей станции Notes, измените файл bookmark.ntf и включите измененный шаблон в комплект дистрибутивного программного обеспечения своей компании. После начальной установки можно перенести изменения на рабочие станции пользователей через профили установки пользователя (**User Setup Profile**).

Эта тема более детально рассматривается в статьях и соответствующих книгах по программированию версий R5 и R6. В настоящей главе приводится краткий обзор информации о реализации таких функций с помощью определенной последовательности действий.

Замените начальную страницу любой закладкой

Пользователи могут выбрать любую базу данных, документ или Web-страницу и применить ее для замены начальной страницы, установленной по умолчанию. Для этого надо:

1. Щелкнуть правой кнопкой мыши по нужной закладке.
2. Выбрать *Set bookmark as Home Page* (Установить закладку в качестве домашней страницы).

Такой метод позволяет в качестве домашней страницы по умолчанию установить рабочее пространство R4. Чтобы пользователям было легко переключаться между стилем рабочего пространства R5/6 и начальной страницей R5/6, перенесите значки рабочего пространства и начальной страницы на панель Bookmark. В качестве домашней страницы допускается установить любой элемент. Пользователь может выбирать удобный ему интерфейс.

Чтобы управлять начальной страницей:

1. Создайте новую базу данных. В этом примере назовите ее Corporate Frameset dB и сохраните под именем CorpFramesetdB.nsf.
2. В новой базе данных создайте макет, отображающий информацию, которую должен видеть на своей начальной странице пользователь. Сохраните макет как NewCorpFrameset. Закройте базу данных.
3. Выведите на экран шаблон базы данных Bookmark (bookmark.ntf) с помощью клиента Design.
4. Сформируйте новый макет и установите, чтобы NewCorpFrameset загружался из базы данных CorpFramesetdB.nsf. Сохраните его с именем NewCorpWelcome.
5. У нового макета в файле bookmark.ntf укажите свойство **Prohibit design replace/refresh to modify** (Запретить изменение и обновление дизайна).
6. Запустите агент Toggle Advanced Configuration Editor (Редактор переключения дополнительной конфигурации) в базе данных bookmark.ntf. Обратите внимание: агент активизирует режим **Advanced Configuration Mode** (Режим¹ дополнительной настройки), позволяя изменять профили оформления и их свойства. При втором запуске режим отключается.
7. Вернитесь на вид набора панелей (кадров). Выделите **-Welcome-** и просмотрите его в Notes. Появится начальная страница по умолчанию.
8. В раскрывающемся меню на начальной странице отметьте **Create new page style** (Создать новый стиль страницы). Откроется окно, очень похожее на окно, позволяющее пользователю настраивать начальную страницу. Теперь в нем есть еще одна вкладка - **Advanced Properties** (Дополнительные свойства). Откройте ее (рис. 13.5).
- 9г Сбросьте флажок **Allow end users to edit this page** (Разрешить пользователям редактировать эту страницу).
10. Установите флажок **Ignore all layout settings and instead load this frameset** (Игнорировать все параметры настройки оформления и загрузить этот макет). В находящемся ниже поле введете имя настроенного набора панелей.
11. В поле **Unique sort key** (Уникальный ключ сортировки) введите значение 00000000. Для страницы **Basics** ключ по умолчанию равен 00000001, поэтому ключ сортировки, состоящий из всех нулей, в раскрывающемся меню будет отображать вашу новую страницу выше страницы **Basics**.

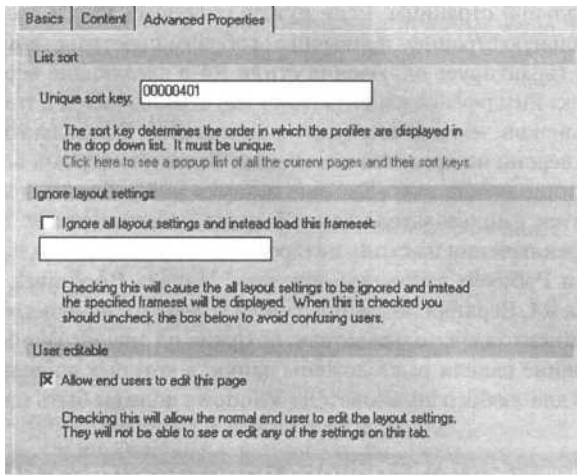


Рис. 13.5. Вкладка появляется после выполнения агента *ToggleAdvancedConfigurationEditor*

12. Щелкните по ОК - и вы увидите на экране новую начальную страницу.
13. Удалите из файла набор кадров, которые не следует выводить. Это могут быть все макеты, кроме вашего.
14. Определите соответствующие уровни в списке ACL, которые должны быть унаследованы при обновлении модели базы данных bookmark.nsf. Не забудьте включить уровень анонимного доступа [Anonymous].
15. Если теперь включить базу данных bookmark.ntf в дистрибутивное программное обеспечение установки клиента, то начальная страница на рабочих станциях пользователей будет настроена в соответствии с новым шаблоном.

Используя комбинацию Notes, HTML и Java, разработчик может создавать самые современные интерфейсы. Там, где располагалась кучка значков баз данных, в которых самым современным средством был показ трехмерных кнопок, сейчас разместится замысловатый интерфейс в Web-стиле.

Многие корпорации в своих сценариях установки клиентов Notes применяют заданные заранее параметры настройки. Изменяя файлы bookmark.ntf и desktop5.dsk (desktop6.ndk в версии R6), компания в состоянии назначать и контролировать внешний вид своих клиентов Notes.

Как для Domino, так и для Notes существует установка по умолчанию (Silent Install) Мастера InstallShield. В документации Notes содержится более подробное описание настройки процесса установки клиента. На сайте поддержки пользователей компании Lotus имеется по крайней мере одно пособие Technote #170629, рассматривающее этот процесс. Документацию по InstallShield можно получить на Web-сайте компании по адресу <http://www.installshield.com>.

Замена начальной страницы

Изменения не всегда приветствуются. Иногда сложно требовать, чтобы опытный пользователь исследовал тонкости нового интерфейса и тратил время на изучение принципов

использования начальной страницы. Если нужно облегчить таким пользователям жизнь, стоит заменить начальную страницу привычным рабочим пространством R4. Обратите внимание, что Lotus не гарантирует включения стиля R4 в следующие версии клиента Notes.

Интересный аспект интерфейса клиента Notes R5/6 заключается в том, что он был разработан скорее для новичков, чем для опытных пользователей. В результате многим пользователям предыдущих версий не нравятся изменения. Зачастую первый вопрос, который они задают администратору, звучит так: «Как мне вернуть мой рабочий стол обратно?» На самом деле он находится у пользователя, но надо знать, где его искать.

Средство для переключения на стиль интерфейса R4 размещается на панели **Bookmark** (Закладка) слева на Рабочем столе пользователя. Панель **Bookmark** остается там даже в случае интерфейса R4. Верхняя половина панели содержит значки для почты, календаря, адресной книги и списка задач пользователя, похожие на значки Windows.

На нижней половине панели расположены папки, в которых собраны дополнительные значки. Интерфейс для любого пользователя Windows должен быть наглядным.

Использование в R5/6 рабочего пространства стиля R4

Клиент Notes R5/6 имеет в левой стороне рабочего пространства панель **Bookmark** со значками (ярлыками), похожими на значки баз данных в рабочем пространстве R4. Для хранения соответствующих значков служат папки, подобные папкам Windows.

Значок **Workspace** (Рабочее пространство), вызывающий интерфейс R4, входит в папку **Databases** (Базы данных) на панели **Bookmark**. Пользователь может в любое время выбрать его и перетащить на панель закладок. После этого щелчком по данному значку включается привычный интерфейс рабочего пространства R4.

Применение знакомого интерфейса вместе с начальным экраном R5/6 и закладками связано со своим набором ограничений. Например, значки на классических страницах рабочего пространства и значки на закладках синхронизируются только при установке или обновлении для версии R5, то есть добавление или удаление закладок и значков баз данных не сказывается на других интерфейсах. Это стало возможным в клиенте Notes R6. Аналогичная ситуация возникает, когда пользователь переименовывает страницу в рабочем пространстве R4, ожидая, что его закладки отразят изменение. Но, к сожалению, они не синхронизированы. Компания Lotus разрабатывала клиент R5/6 в расчете, что пользователи будут обращаться либо к закладкам Web-стиля, либо к клиенту R4, но не к обоим средствам сразу. И она не гарантирует, что в последующих версиях останется классический рабочий стол Notes.

*

Функциональные возможности панели Bookmark

Как и у значков баз данных, у значков закладок есть связанный с ними набор действий. Тип действия зависит от выбранной закладки. Некоторые действия были доступны и в предыдущих версиях Notes, а некоторые - новые для R5/6. Например, при щелчке правой кнопкой мыши по закладке **Mail**, **Calendar**, **Address Book** или **To Do** вы увидите следующий набор параметров:

- **Open** (Открыть);
- **Open Replica** (Открыть реплику);
- **Open in New Window** (Открыть в новом окне);
- **Open in Designer** (Открыть в Domino Designer).

Другие варианты приводят к дополнительным пунктам меню. Они также могут показаться знакомыми по предыдущим версиям:

- **Database** (Базы данных);
- **Replication** (Репликация);
- **Create** (Создать).

Приведенные ниже значки доступны для всех закладок при щелчке правой кнопкой мыши по значку закладки либо базы данных на панели **Bookmark**:

- **Open Folder** (Открыть папку);
- **Create a new folder** или **Create Folder** (Создать папку);
- **Remove Folder** (Удалить папку);
- **Rename Folder** (Переименовать папку);
- **Change Folder Icon** (Изменить значок папки).

Эти варианты также хранятся в файле bookmark.nsf. Активный пользователь рискует случайно удалить папку Database icon или Workspace icon, где по умолчанию хранится значок **Workspace**. В текущей версии клиента Notes самым быстрым способом восстановления значка **Workspace** является удаление или переименование bookmark.nsf и перезапуск клиента.

Пользователи предыдущих версий будут предупреждены, что значки закладок не накладываются друг на друга, как значки баз данных в классическом рабочем пространстве Notes. Если пользователь делает закладки для нескольких реплик одной базы данных на разных серверах, то для каждой из этих реплик создается значок в определенной папке, что усложняет работу администратору, отслеживающему каталоги Domino на нескольких серверах. Кроме того, отсутствует явный способ установления принадлежности значков. Обратите внимание, что когда вы перемещаете курсор над значком базы данных, на панели состояния отображается полный путь к ней. Вы не заметите этого, если будете смотреть на значки вверх экрана.

Проблемы отображения начальной страницы на мониторах с маленьким разрешением

Минимальное разрешение экрана, поддерживаемое в версии R5/6, - 800x600. Клиенты на компьютерах с меньшим разрешением могут активизировать горизонтальную полосу прокрутки в обычном меню, но поскольку вертикальной полосы прокрутки там нет, нижняя часть экрана не будет видна. Lotus разрабатывает приложения для графики с высоким разрешением. Большинство корпоративных пользователей предпочитают технику высокого класса, поэтому для многих это свойство не является существенным недостатком. Однако в версии R5/6 разработчики должны изменить размеры программ просмотра в приложениях баз данных, чтобы они соответствовали размерам экрана.

Предпочтения пользователей

В этом разделе обсуждаются предпочтения пользователей в клиенте Notes R5/6. Предпочтения предоставляют конечному пользователю определенный контроль над способами отображения элементов и реализации некоторых средств. Существует ряд альтернатив, заслуживающих внимания администраторов, хотя о них часто умалчивается.

Одна из наиболее важных групп параметров в разделе **User Preferences - Security Settings** (Параметры безопасности). Большинство администраторов оставляют в ECL (Execution Control List - список управления исполнением) параметры по умолчанию, подвергая систему некоторому риску. Для получения более подробной информации о ECL читайте главу по защите информации.

Еще одна область, которую должны учитывать администраторы, - это Web-параметры, такие как элементы управления ActiveX в браузере Notes (см. главу 15).

Пользователи должны иметь в виду, что в R5/6 больше нет кнопки, выбирающей автоматически загружаемую базу данных. Теперь нужно, щелкнув правой кнопкой мыши по закладке, отметить **Set bookmark as Home Page** (Установить закладку в качестве домашней страницы). Указанная база данных загружается при запуске клиента Notes. Некоторые дополнительные параметры, доступные в предыдущих версиях Notes, в R5/6 отсутствуют:

- **Typewriter fonts only** (Использовать только шрифты печатной машинки) - при выборе этого параметра клиенту Notes доступны только моноширинные шрифты;
- **Large fonts** (Большие шрифты) - отображаются шрифты, которые немного больше по размеру и чуть темнее;
- **Keep workspace in back when maximized** (Помещать развернутое рабочее пространство Дюэда всех окон);
- **Monochrome display** (Монохромный монитор) - даже на цветных мониторах обеспечивается режим вывода в градациях серого;
- **Keep all windows within main Notes window (MD)** (Все окна внутри главного окна Notes) - любое окно Notes выводится независимо от главного окна. Каждое окно имеет собственное меню и панель **SmartIcon**.

Администраторы должны знать некоторые новые предпочтения, которые можно установить:

- **Icon color scheme** (Цветовая схема значков) - задает способ отображения значков закладок;
- **Bookmark size** (Размер закладок) - можно установить **Small** (Маленькие), **Medium** (Средние) и **Large** (Большие). Полезно для людей, имеющих проблемы со зрением;
- **Default fonts** (Шрифты по умолчанию) - пользователи должны обратить внимание, что ряд шрифтов, которые они ранее применяли, в R5/6 отсутствуют в списке доступных, например *Helv/Helvetica*. Были и виртуальные шрифты, то есть операционная система отображала их каким-то другим шрифтом без засечек. Теперь в **User Preferences** по умолчанию предлагаются следующие шрифты: **Sans Serif** (Без засечек), **Serif** (С засечками), **Monospace** (Моноширинный) и **Default** (По умолчанию);
- **New mail sound** (Звук нового сообщения). Звуковой файл, который проигрывает Notes при получении нового сообщения, можно задавать с помощью кнопки, а не редактирования файла *notes.ini*. К сожалению, нет средства для прослушивания звука перед его выбором.

Динамические профили установки пользователей

Клиент Notes предлагает администраторам способ управления элементами, отображаемыми в рабочих пространствах пользователей. В предыдущих версиях Notes для уже

установленного клиента не было централизованного способа внесения изменений и стандартизации Рабочего стола. В R5/6 администраторы могут добавлять базы данных и изменять определенные элементы на Рабочих столах пользователей даже после того, как клиент установлен. Это выполняется с помощью **User Setup Profile** в каталоге Domino. В R4 профиль **User Setup Profile** служил для заполнения определенных полей во время установки клиента. Начиная с версии R5 этот документ применяется для динамического изменения некоторых полей при аутентификации пользователя с домашним сервером, указанным в документе местоположения пользователя. Изменения вносятся посредством редактирования **Setup Profile** с помощью клиента администрирования, причем изменения распространяются процессом Administration Process.

Изменяя **User Setup Profile**, администратор может менять параметры настройки таких элементов клиента Notes, как:

- информация браузера;
- сквозной сервер;
- серверы поиска в домене;
- информация о вторичных серверах;
- прокси-сервер;
- безопасность апплетов Java;
- сервер поиска в каталоге домена;
- дополнительные поля, назначенные потребителям.

Для использования этих возможностей необходимо, чтобы и клиент, и сервер работали под управлением версии R5 или R6. Обратите внимание, что администратор в состоянии только добавлять или изменять параметры установки, но не может ничего удалять. Пользователь вправе отменить изменения своего профиля, открыв документ местоположения и выбрав **Actions=>Advanced=>Set Update Flag** (Операции=>Дополнительно=>Установить флаг обновления). Если пользователи не получают обновления профилей, проверьте это значение.

Использование ID-файла администратора на сервере

Когда администратор обращается к своему ID-файлу на сервере, необходимо отключить динамическую конфигурацию клиентов, добавив в файл *notes.ini* сервера строку

DesableDynConfigClient=1

Изменение почтовой службы

Общепризнано, что наиболее популярное компьютерное приложение на сегодняшний день" - это электронная почта. Клиент Notes всегда предоставлял удобные и защищенные почтовые услуги. В версии R5/6 внесен ряд изменений, о которых следует знать администратору.

Почтовые правила

Клиент Notes R5/6 имеет новое средство - Mail Rules (Почтовые правила). Пользователи могут задавать критерии, по которым Notes будет автоматически выполнять определенные действия, такие как помещение документов с заданным содержанием в указанную папку.

Создавая правила, пользователь в состоянии распределять входящие сообщения. Администратор должен знать почтовые правила. Пользователи могут обращаться за помощью при установке правил и при решении проблем, возникающих с созданными правилами. Диалоговое окно **Mail Rule** изображено на рис. 13.6. Оно открывается щелчком по папке Rules в почтовом файле пользователя.

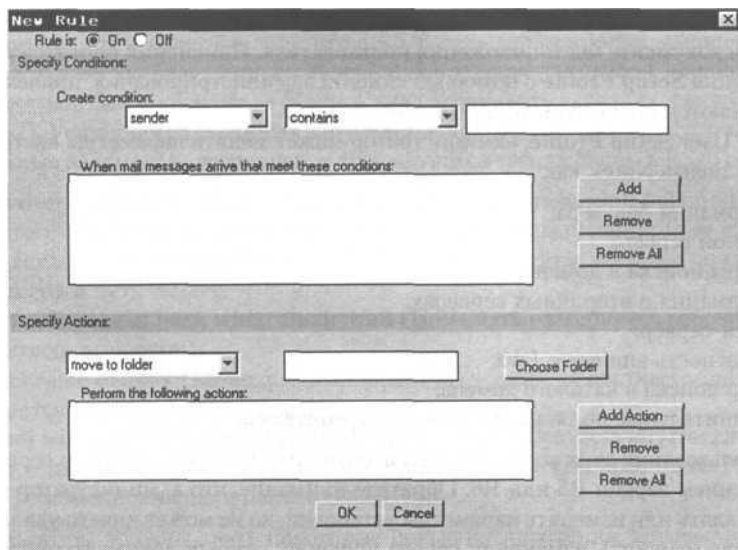


Рис. 13.6. В окне Mail Rule представлены знакомые поля почтовой формы Notes, с помощью которых можно задавать условия для выполнения определенных действий над входящими почтовыми документами

Для задания условий в окне **Mail Rule** предназначены следующие поля почты Notes:

- **Sender** (Отправитель);
- **Subject** (Тема);
- **Body** (Содержание);
- **Importance** (Важность);
- **Delivery priority** (Приоритет доставки);
- адресные поля: **To** (Кому), **CC** (Копия), **BCC** (Скрытая копия);
- размер в байтах.

Над сообщениями, удовлетворяющими указанным условиям, разрешается выполнять такие действия:

- переместить в другую папку;
- скопировать в папку;
- изменить важность; •
- удалить.

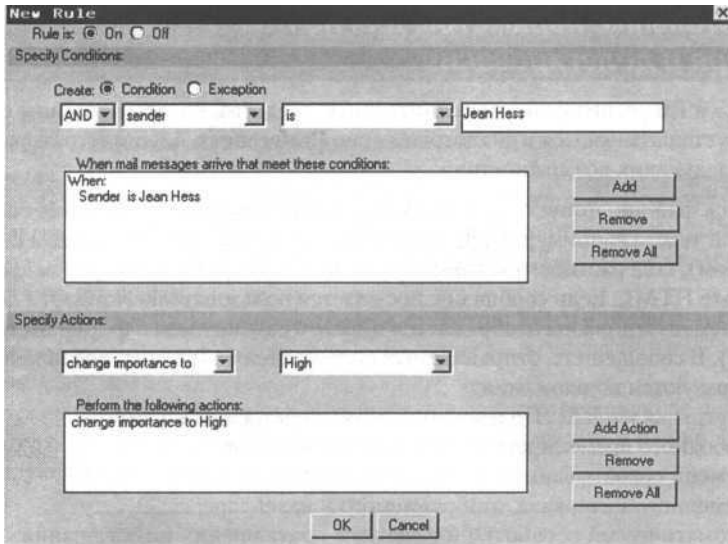


Рис. 13.7. Данное правило меняет в сообщении значение поля Importance на High

На рис. 13.7 показана заполненная форма **New Rule**. Когда приходит сообщение от Jean Hess, его важность меняется на **High**. С помощью другого правила, в котором включено напоминание (memo), а поле **Importance** содержит значение **High**, допускается перемещать такие сообщения в отдельную папку, просматриваемую пользователем прежде всего.

Правило можно включить и выключить при редактировании почтового файла пользователя. Интерфейс, которым обладают правила, похож на интерфейс окна **Agent Builder** (Построитель агентов), но располагает меньшими функциональными возможностями.

Правила действуют, даже если рабочая станция клиента выключена или на ней не выполняется сеанс клиента. Правила базируются на сервере, поэтому их функции реализуются во время работы почтового сервера.

Автоматическая проверка орфографии

Большинство людей имеют образное мышление. Способ общения зависит от осознания и понимания текущей ситуации. Орфографические ошибки не способствуют правильному восприятию сообщения. Начиная с версии R5 в Notes имеется средство, которое проверяет орфографию в сообщении перед тем, как его отправить. Проверку орфографии можно задать для отдельных сообщений, выбрав на вкладке **Basics** окна **Delivery Options** (Параметры доставки) опцию **Auto Spell Check** (Автоматическая проверка орфографии).

Чтобы включить проверку орфографии для всех сообщений, в почтовом файле пользователя выберите **Tools => Preferences** (Программные инструменты => Предпочтения) и установите флажок **Automatically check mail messages for misspellings before sending** (Автоматически проверять орфографию перед отправкой).

Дополнительные параметры для почты, календаря и делегирования

В версиях R5 и R6 реализованы дополнительные средства, которые связаны с почтовыми службами и устанавливаются в диалоговом окне **Preferences**. Администраторам необходимо знать о следующих возможностях:

- О подпись файлов. Допускается, чтобы пользователь добавлял в конце сообщения открытый текст (например, Eagle Mountain Computing вместе с адресом и контактным номером), содержимое текстовых файлов или рисунок в растровом формате либо формате HTML. Если сообщение посылается пользователю Notes, эти дополнительные элементы должны отображаться вместе с сообщением в форме **Memo** (Напоминание). В сообщениях, отправляемых пользователям Internet, добавленные рисунки преобразуются во вложения;
- О параметры календаря. Пользователь может настроить параметры:
 - свободного времени для встреч, совещаний и т.п.;
 - времени срабатывания сигнала и звука этого сигнала;
 - временного интервала, отображаемого в календаре;
 - автоматической обработки и рассылки приглашений на совещания;
 - вывода на экран списка дел на текущий день в календаре.
- О параметры делегирования. Настройки делегирования для календаря и почты позволяют владельцу почтового файла назначать для других пользователей возможность:
 - читать почту, календарь и список дел в этой базе данных;
 - читать элементы списка дел в календаре, а также читать и отправлять почту от имени владельца;
 - читать, отправлять и редактировать любые почтовые, календарные и плановые документы (документы расписаний);
 - удалять почтовые, календарные и плановые документы.

Дополнительные утилиты на Notes CD: Помощник Notes

Notes Minder (Помощник Notes) - новое средство в версии R5/6. Эта программа проверяет почту и отслеживает события календаря, даже когда не работает клиент Notes. При запуске программы на панели задач Windows отображается маленький значок. Когда Notes Minder обнаруживает новое входящее сообщение или наступает время определенного события календаря, граница значка становится красной и начинает мигать. Если удерживать курсор мыши над этим значком, Notes Minder выведет сведения о состоянии почты или времени ее последней проверки.

Поместите ярлык Notes Minder в меню **Автозагрузка** на рабочей станции пользователя, чтобы автоматически отслеживалось состояние почтового ящика и элементов календаря. Кроме того, пользователь может запустить Notes с панели задач. При щелчке мышью по значку Notes Minder активизируется клиент Notes. Notes Minder также загружают из папки Lotus Application.

Дополнительные утилиты на Notes CD: Actioneer

Actioneer - дополнительная программа, которая находится в каталоге APPS на компакт-диске Notes. Она позволяет вносить информацию в календарь клиента Notes, даже когда сам клиент не работает.

Поскольку Actioneer имеет доступ к календарю пользователя, программа запрашивает пароль у пользователя, даже если он уже вошел в операционную систему. После запуска программы на панели задач появляется маленький значок. Для открытия Actioneer необходимо щелкнуть по значку.

Щелкните по вкладке **To Do**, **Appointment** или **Journal Entry** и введите текст. Actioneer попытается на основании этого текста заполнить такие поля, как дата, время начала и время окончания.

После сохранения записи Actioneer помещает ее в соответствующую позицию календаря пользователя. На рис. 13.8 изображено окно ввода информации, а на рис. 13.9 показана запись, которую программа внесла в календарь.

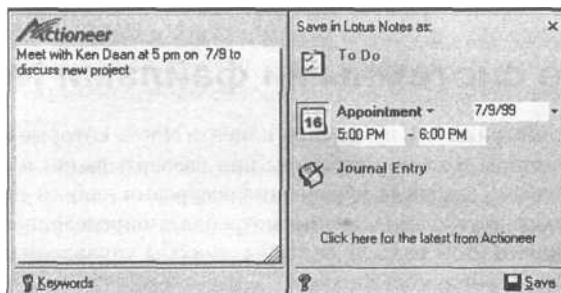


Рис. 13.8. Введите текст в Actioneer, и программа преобразует ключевые слова в запись календаря

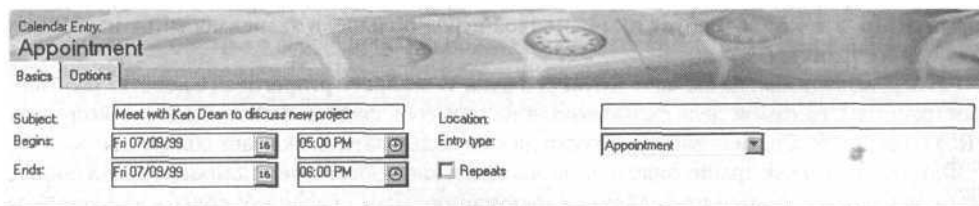


Рис. 13.9. Запись в календаре пользователя

Подписка на документы

Клиент R5/6 позволяет пользователю настроить подписку, которая будет извещать его обо всех изменениях базы данных. Пользователю предлагается указать извещение о новых

документах, измененных документах или документах, удовлетворяющих определенному критерию. Критерий может основываться на формуле или выборе по полям **Author (Автор)**, **Subject (Тема)** и/или **Size (Размер)**.

В базах данных с большим числом подписчиков не исключено возникновение проблем. Поскольку Notes будет автоматически проверять наличие новых сообщений, удовлетворяющих заданному критерию, каждая новая подписка добавит в систему дополнительные задачи. По умолчанию клиент Notes проверяет подписку каждый раз при запуске и при любой проверке почты. Это назначается в **User Preferences (Предпочтения пользователя)**. Из-за увеличения трафика и нагрузки сервера, вызванного проверкой и получением новых документов в каталоге Domino каждые 10 минут сотнями пользователей, возможно существенное снижение скорости работы системы, что, в свою очередь, замедлит доступ к базам данных.

Администраторы располагают средствами ограничения числа баз данных, на которые разрешено подписываться пользователям. Чтобы отменить подписку на определенные базы данных, отметьте на вкладке **Advanced** окна **Database Properties (Свойства базы данных)** параметр **Don't allow headline monitoring (Не разрешать наблюдение за базой данных)**. Изменить это значение позволяет администратору клиент администрирования. В Domino Administrator допускается вносить изменения сразу в несколько баз данных за одну операцию.

Управление системными файлами Notes

До этого момента рассматривались изменения клиента Notes, которые касаются конечного пользователя. Архитекторы и администраторы при развертывании в сети системы Notes сталкиваются с типичными задачами управления ресурсами любого сетевого сервера. Система Notes, как и любое другое приложение, потребляет определенные ресурсы, которые требуют регулирования. В этом разделе описаны способы управления воздействием клиента Notes на рабочую станцию пользователя.

Пользователи R4, вероятно, обратили внимание на существенное увеличение размера файла при просмотре свойств обычного рабочего пространства R5/6. Это произошло из-за добавления графических элементов начальной страницы. Например, Рабочий стол R4 занимал 4 Мб, а в R5 он требует памяти вдвое-втрое больше, в зависимости от настройки начальной страницы.

Размер, выводимый на вкладке **Advanced** окна **Workspace properties (Свойства рабочего пространства)**, на самом деле складывается из размеров файлов desktop5.dsk (desktop6.ndk в R6) и cache.dsk. Сжимая рабочее пространство, пользователь сжимает оба файла.

Файл desktop5.dsk хранит значки пользователя, эшированные реплики непрочитанных меток и некоторую дополнительную информацию. Файл cache.dsk содержит элементы оформления из недавно использованных баз данных на сервере, журнал непрочитанных меток, называемый Unread Journal, и дополнительную информацию. Такие файлы могут быть достаточно большими. Размеры файлов в каталогах на файловых серверах становятся настоящей проблемой во многих компаниях. Например, компании, выполняющие централизованное резервирование файлов пользователей, имеют для этого немного времени, если стараться не снижать производительность работы пользователей. Поэтому методы управления размерами файлов пользователей могут стать достаточно жесткими.

Кроме резервирования существует еще два вопроса, с которыми придется столкнуться администраторам при управлении файлами, - это *размер* и *размещение*. Из двух рассмотренных выше файлов cache.dsk заметно больше. Свойство **Workspace properties**

может показывать размер в 5 Мб, хотя файл desktop5.dsk занимает не более 1 Мб, а остальное приходится на долю cache.dsk.

Потребление дискового пространства – проблема многих сетей, рабочих станций и переносных компьютеров. Управление размером больших файлов позволяет сэкономить деньги и увеличить дисковое пространство, доступное пользователям. Рассмотрим сеть из 1000 компьютеров, на каждом из которых эти два файла занимают 5 Мб. А теперь предположим, что это минимум, а в среднем для них требуется от 5 до 50 Мб дискового пространства...

Существует несколько способов управления размером файла cache.dsk. Администратор может программно удалить его и позволить перестраивать при каждом сеансе или задать определенное значение для максимального размера файла на вкладке **Advanced** в окне **Workspace properties**. При удалении файла cache.dsk затрагивается отслеживание непрочитанных меток. Установить максимальный размер тоже достаточно сложно, поскольку пользователю легко изменить его.

Дублирующиеся записи в окне Установка и удаление программ системы Windows

После обновления клиента рабочей станции с версии R4 на версию R5 в окне **Установка и удаление программ** панели управления операционной системы можно обнаружить двойные записи для Lotus Notes. Не существует точного способа различить эти записи. Если пользователь попытается отменить установку для одного из клиентов, то он либо удалит новую версию, либо получит сообщение о невозможности удаления

`HKEY_LOCAL_MACHINE\software\Lotus\Notes\4.0`

(регистрационная информация продукта в системном реестре).

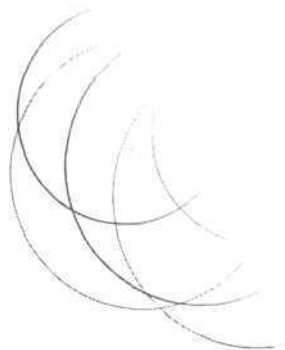
Дело в том, что программа установки R5 не очистила записи реестра, касающиеся R4. Компания Lotus исправила ошибку в версии R6, но для предыдущих версий обновление на рабочих станциях приводит к появлению дублированных записей. Можно использовать редактор реестра RegEdit32, чтобы все-таки удалить запись реестра, касающуюся R4, но нет оснований считать, что возникнут какие-либо проблемы, если эту запись не трогать. Интересно, что запись реестра, касающаяся R4, остается там даже после удаления R5.

Изменяя параметры в файле notes.ini, можно определять размещение файлов desktop5.dsk и cache.dsk. С помощью параметра **CACHE** в notes.ini администратор может задавать местоположение кэш-памяти. Это позволяет хранить файл cache.dsk на сетевом диске больших размеров либо на локальном диске пользователя. Сохранение desktop5.dsk и cache.dsk на локальном диске увеличивает производительность рабочей станции пользователя, поскольку ей не придется обращаться за часто используемой информацией в сеть. Размещение cache.dsk поможет объяснить пользователю, что необходимо иногда уменьшать размер этого файла, чтобы экономить дисковое пространство.

Системные параметры часового пояса

По умолчанию в клиенте Notes R5/6 часовой пояс и летнее время синхронизируются с параметрами операционной системы. Эти параметры хранятся в текущем документе местоположения пользователя. Если на компьютере часовой пояс, летнее время и время по Гринвичу не установлены либо указаны неправильно, Notes тоже будет отображать неточное время.

ГЛАВА 14



ПОДДЕРЖКА БАЗ ДАННЫХ И УСТРАНЕНИЕ НЕПОЛАДОК

В этой главе обсуждаются характерные проблемы баз данных Domino и действия, необходимые для поддержания их работоспособности: как хранить и обслуживать базы, чтобы в лучшем виде предоставлять пользователям. Одна из частей рассматриваемого процесса - поддержка и восстановление базы данных, устранение неполадок. Вторая часть - управление, а также развертывание и оптимизация базы с целью достичь наиболее полной реализации всех возможностей.

Здесь описана, кроме того, роль администратора и владельца базы данных, которые не обязательно являются одним и тем же лицом или группой. Разработчик или дизайнер базы данных тоже вносит определенный вклад в ее производительность. Кто бы ни выступал в этих ролях, ему следует знать область ответственности каждой из них.

Развертывание приложения

База данных или группа баз данных образует приложение, которое разрабатывается для выполнения определенной задачи или набора взаимосвязанных задач, функционирует как средство для обмена мнениями, хранения важных документов и данных, сбора и распространения информации или наблюдения за бизнес-процессами или проектами.

Построение и развертывание приложения включает в себя несколько шагов:

1. Планирование приложения. Участвуют заказчик (пользователи или их представители) и разработчик приложения, которые решают, для чего предназначено это приложение и в общих чертах определяют, как оно должно функционировать. Разработчик и дизайнер приложения на основании такой информации пишут план приложения и затем согласовывают его с заказчиком, внося последние поправки.
2. Создание файла базы данных и элементов проектирования, необходимых для выполнения цели приложения. Разработчик приложения собирает все элементы, которые требуются при построении базы данных: поля, формы, виды, агентов, действия, навигаторы, страницы, макеты и т.д.
3. Разработка и внедрение защиты приложения. На основании сведений от заказчика о том, какие пользователи могут что-то делать в приложении, разработчик на стадии построения элементов приложения внедряет некоторые средства защиты.

Администратору нужна информация о частях приложения, имеющих отношение к серверу, таких как агенты, чтобы обеспечить поддержку по общим вопросам защиты в процессе разработки. В конце концов, список ACL каждой базы данных - это область ответственности администратора, хотя изначально ACL может настраиваться разработчиком. Администратору должен быть предоставлен доступ на уровне Manager (см. главу 10).

4. Развертывание приложения для маленькой экспериментальной группы, которая тестирует приложение. Когда приложение готово к проверке небольшой группой пользователей, администратор контролирует добавление баз данных приложения на сервер.
5. Учет отзывов о приложении. Экспериментальная группа максимально полно использует приложение, стараясь выявить в нем возможные ошибки и предложить пути исправления и усовершенствования. Разработчик вставляет в приложение все согласованные доработки и устраняет недостатки. Администратор контролирует приложение, чтобы не возникало проблем на сервере и приложение не ухудшало производительность сервера.
6. Предоставление приложения всем пользователям (развертывание). Основная часть проекта завершена, хотя разработчик может вносить определенные корректировки даже после внедрения приложения. Либо разработчик, либо администратор создает для приложения исходный полнотекстовый индекс. На сервер переносится копия (не реплика) исходной тестовой базы данных, причем необходимо сформировать шаблон базы данных, чтобы была возможность вводить последующие изменения в макет базы (см. ниже раздел о добавлении базы данных на сервер). База данных и ее шаблон в целях безопасности подписываются (см. раздел о защитной подписи). Администратор настраивает окончательный список ACL, создает все необходимые группы и информирует пользователей, которые могут работать с приложением.

На этом этапе администратор должен настроить репликацию баз данных приложения (см. главу 9) и установить ограничение на ее размер. Теперь ему надлежит убедиться, что базы данных реплицируются, а также поддерживать и обновлять списки ACL и заниматься любыми проблемами, возникающими у пользователей.

Разрешение текущих проблем приложения - задача администратора базы данных, в роли которого может выступать администратор системы, однако выполнение этих функций по силам и опытному пользователю. Такому пользователю требуется доступ на уровне Manager, и он будет отвечать за поддержку списков ACL, а также информировать администратора о необходимости внесения изменений. Членов групп, указанных в ACL, надо обновлять по мере увольнения прежних сотрудников или при приеме на работу новых. Это еще одна область ответственности администратора базы данных (по крайней мере, пользователя с соответствующим доступом к каталогу Domino, позволяющим изменять состав группin). Администраторы баз данных обычно улаживают конфликты репликации и сохранения, проверяют правильность ввода данных и обеспечивают работу службы технической поддержки по вопросам работы приложения.

Теперь, когда вам ясно, какие пользователи вовлечены в процессы построения, развертывания и поддержания баз¹ данных приложения, рассмотрим, как администратор системы или администратор базы данных выполняет задачи по поддержанию базы данных и управлению ею.

Добавление новой базы данных на сервер

Прежде чем применять новую базу данных на сервере, необходимо подготовить сервер к работе с новым приложением. Например, следует убедиться, что все вовлеченные пользователи и серверы имеют соответствующий доступ к этому серверу. Для любой базы данных, которой будет адресована почта, нужно сформировать документ входящей почты (Mail-In document). Также могут понадобиться разрешения на запуск агентов на сервере, особенно в случае сценариев LotusScript и агентов Java.

Следует также продумать структуру каталогов на сервере. Размещение набора взаимосвязанных баз данных в одном подкаталоге упрощает управление ими при репликации, а настройка документа соединения для репликации по каталогам облегчает пользователям поиск «своих» приложений и делает приложения более управляемыми в плане безопасности.

Отслеживание жизненного цикла приложения

Приложения создаются и удаляются. Приложения, предназначенные для нужд определенных проектов, после завершения этих проектов больше не требуются. Другие тихо умирают по мере того, как пользователи находят иные способы достижения цели. Между тем число баз данных растет с увеличением количества обращений пользователей к Notes и Domino в поисках решения возникающих проблем. По прошествии определенного времени только немногие люди знают, какие функции выполняют базы данных, имеющиеся на сервере, кто их создавал и нужны ли они на данный момент. Хотя из каталога баз данных удастся почерпнуть некоторую информацию о каждой базе, расположенной на сервере, это нельзя считать слежением за полезностью базы данных. Авторы красной книги IBM «Secrets to Running Lotus Notes: The Decisions No One Tells You How to Make» Мэрион Хокер (Marion Hawker), Амиа Гринфилд (Amita Greenfield), Хелен Роузен (Helen Rowan) и Эндрю Уэйнрайт (Andrew Wainwright) предлагают создать баз данных Notes Application Registry (Реестр приложений Notes), содержащую информацию о создателе и назначении приложения, о том, какие базы данных входят в его состав, а также сведения, помогающие найти необходимые базы. Эту книгу, наряду с остальными красными книгами по Lotus Notes и Domino, можно найти на сайте IBM: <http://www.redbooks.ibm.com/solutions/lotus>.

И наконец, прежде чем поместить базу данных на сервер, убедитесь, что в ее списке ACL вам предоставлен доступ уровня **Manager**, а также что можно создавать новые базы данных на этом сервере. *

Чтобы скопировать базу данных на сервер:

1. Щелкните правой кнопкой мыши по значку базы данных и выберите **Database => New Copy** (База данных => Новая копия).
- 3- В диалоговом окне **Copy Database** (Копирование базы данных) укажите в поле **Server** сервер, на который нужно поместить копию.
3. Измените название, чтобы оно отображалось как ярлык для серверной копии этой базы данных.
4. В поле **File Name** (Имя файла) введите путь и имя файла базы данных. Хотя операционная система поддерживает длинные имена файлов, сервер Domino лучше работает с восьмисимвольными именами плюс расширение .nsf.

5. Для копирования элементов проектирования базы данных вместе со всеми документами задайте **Database design and documents** (Дизайн и документы базы данных). Если вы не хотите копировать документы, созданные во время разработки, укажите **Database design only** (Только дизайн базы данных).
6. Необязательный параметр. Если список ACL уже настроен в процессе разработки и нужно сохранить его характеристики, выберите **Access Control List** (только убедитесь, что имеете доступ **Manager**). Если вы будете заново настраивать список ACL, не устанавливайте этот флажок. В новой копии вам автоматически будет предоставлен доступ **Manager**, и вы сами определите уровни доступа остальных пользователей.
7. Необязательный параметр. Чтобы создать полнотекстовый индекс для новой копии базы данных, выберите **Create Full Text index** (Создать полнотекстовый индекс). Полнотекстовый индекс нужен для поиска в базе данных, но его можно сделать и позже.
8. Необязательный параметр. Для шифрования новой копии базы данных щелкните по кнопке **Encryption** (Зашифровать). Шифрование означает, что для получения доступа к базе данных пользователь должен иметь соответствующий ID-файл (файл идентификационных данных). Шифрование может быть нестойким (защищает от случайного доступа), средней стойкости (обеспечивает достаточно хороший уровень защиты и быстрый доступ) и стойким (максимальная защита, но документ открывается медленнее). Хотя зашифрованные базы данных чаще всего служат для защиты реплик и копий на рабочих станциях, особенно на переносных компьютерах, иногда их используют и на серверах.
9. Необязательный параметр. Щелкните по кнопке **Size Limit** (Ограничение размера) и установите максимальный размер базы данных - 1, 2, 3 или 4 Гб. Эта кнопка применяется только для баз данных версии R4 с расширением .ns4 или для баз данных, расположенных на серверах и не имеющих возможности обновления до версии R5/6. Для R5/6 максимальный размер базы данных равен 64 Гб в Windows или UNIX и 32 Гб - в OS/2.
10. Щелкните по ОК.

Начальная настройка свойств базы данных

Завершив копирование базы данных на сервер, откройте окно **Database Properties** (Свойства базы данных): щелкните правой кнопкой мыши по значку этой базы? и выберите **Database => Properties** (База данных => Свойства). На вкладке **Design** (Дизайн) установите флажок **Show in Open Database dialog** (Показывать в окне открытия базы данных), чтобы пользователи могли получить доступ к базе данных с помощью меню **File => Database => Open** (Файл => База данных => Открыть).

Если вы или разработчик базы данных создали для нее шаблон (рекомендуется), необходимо в ее свойствах указать имя файла шаблона. На вкладке **Design** установите флажок **Inherit design from template** (Наследовать макет из шаблона) в версии R5 или **Inherit design from master template** (Наследовать макет из главного шаблона) в R6, затем в поле **Template name** (Имя шаблона) введите имя файла шаблона. Скопируйте шаблон на сервер. Формирование шаблонов баз данных позволяет разработчикам проверять следующие

изменения, не затрагивая текущие документы. Если эти изменения полностью протестированы, вам останется просто обновить макет базы данных.

Чтобы пользователи могли восстанавливать удаленные из базы данных документы, установите флажок **Allow soft deletions** (Разрешить мягкое удаление) на вкладке **Advanced** (Дополнительно) диалогового окна **Database Properties** (Свойства базы данных). В поле **SUndelete Expire Time** (Время задержки удаления) в версии R5 или **Soft delete expire time in hours** (Время задержки мягкого удаления, в часах) в версии R6 определите промежуток времени (в часах), в течение которого пользователь сумеет восстановить удаленный документ. Чтобы пользователи могли применить мягкое удаление, в базе данных должен быть вид, отображающий удаленные документы. Его в состоянии создать разработчик приложения или администратор. Для этого вида назначается тип **Shared** (Общий). Пользователь открывает его, выделяет необходимые документы и восстанавливает их (см. раздел об улучшении производительности базы данных).

В окне **Database Properties** на вкладке **Basics** (Основные параметры) есть два свойства, которые влияют на производительность базы данных:

- **Allow use of stored forms in this database** (Разрешить использование форм, хранящихся в базе данных). Если вы не копируете и не отправляете по почте документы этой базы данных, вам, скорее всего, не потребуется такой режим. Отменив его, вы сократите размер базы и улучшите ее производительность;
- **Display images after loading** (Отображать изображения после загрузки). При установке этого флажка увеличивается производительность базы данных, поскольку отпадает необходимость переноса картинок во время загрузки. Однако размер базы не меняется. Можно согласовать с разработчиком, чтобы все картинки хранились как графические ресурсы, а не импортировались в страницы или формы. При работе с графическими ресурсами каждая картинка хранится в единственном экземпляре, что существенно экономит дисковое пространство.

Управление базой данных с помощью вкладки **Files** окна **Domino Administrator**

Программа Domino Administrator является основным средством для наблюдения, поддержки и управления базами данных. Укажите сервер на панели **Server** (Сервер) и щелкните по вкладке **Files** (Файлы) - рис. 14.1. Панель **View** (Вид) покажет файловую структуру Notes и Domino на этом сервере. Содержание панели **Files** зависит от выбранного каталога. Чтобы закрыть панель **View**, щелкните по кнопке **All** (Все), которая станет кнопкой **Tree** (Дерево каталога).

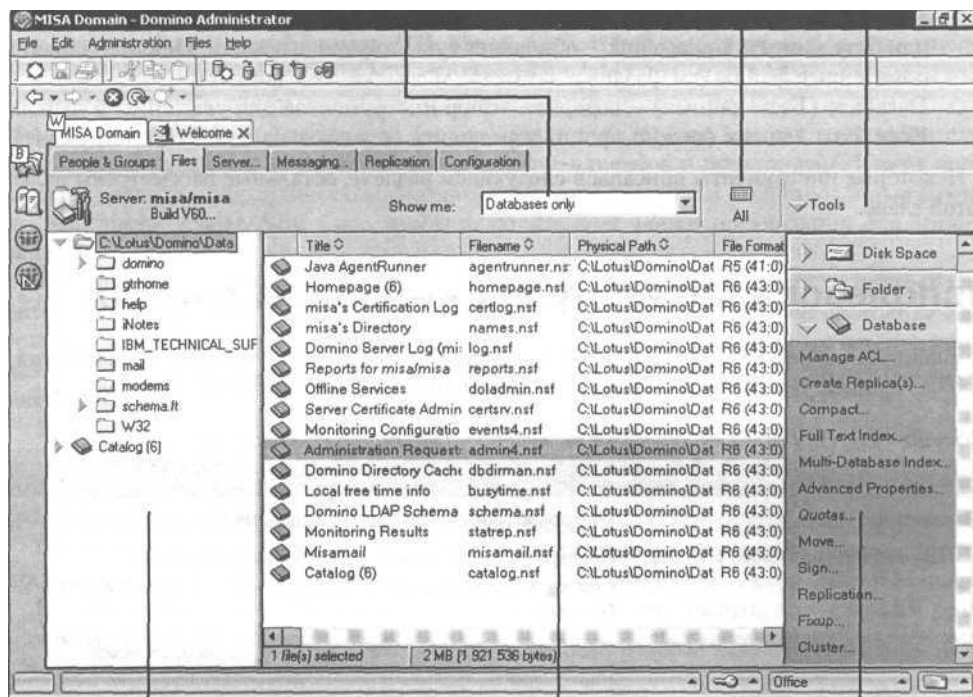
В списке **Show me** выберите тип файлов, которые должны отображаться в панели **Files**: **Databases only** (Только базы данных), **Templates only** (Только шаблоны), **Mail Boxes only** (Только почтовые ящики), **All database types** (Все типы баз данных), **All files** (Все файлы), **Database links only** (Только ссылки баз данных) или **Custom** (Пользовательский режим).

Панель **Files** показывает файлы, тип которых задан в поле **Show me**. По умолчанию выводятся столбцы **Title** (Название), **File Name** (Имя файла), **Physical Path** (Физический

Нажмите для
открытия/сокрытия
панели инструментов

Выберите
тип файлов
для просмотра

Нажмите для
открытия/сокрытия
панели View



Панель View (Вид)

Панель Files (Файлы)

Панель Tools
(Программные инструменты)

Рис. 14.1. Многие инструменты для наблюдения, поддержки и управления базами данных находятся на вкладке Files. В большинстве случаев можно выбрать базу данных и перетащить ее на нужный инструмент

3

путь), File Format (Формат файла), Size (Размер), Max Size (Максимальный размер), Quota (Квота), Warning (Предупреждение), Created (Создан), Last Fixup (Последняя привязка) и Is Logged (Зарегистрирован). Чтобы убрать или поменять местами столбцы, выберите File => Preferences => Administration Preferences (Файл => Предпочтения => Предпочтения администратора) и затем щелкните по значку Files. Если выделить столбец в окне Use these Columns (Использовать эти столбцы) и нажать на стрелку, направленную влево, этот столбец будет удален. Поменять столбцы местами позволят стрелки, направленные вверх и вниз, рядом с надписью Reorder. Затем щелкните по ОК.

Конкретная база данных (или шаблон) открывается двойным щелчком по ней на панели Files.

Панель **Tools** имеет три раздела:

- О **Disk Space** (Дисковое пространство) - отображает размер диска и свободное пространство на жестких дисках выбранного сервера. Выводится круговая диаграмма для каждого диска, которая показывает степень его заполнения;
- О **Folder** (Папка) - перечисляет параметры для управления папками и ссылками баз данных: **New** - формирует новую папку, **New link** - создает новую ссылку на папку или базу данных, **Update link** - обновляет существующие ссылки, **Delete** - удаляет помеченные файлы (см. раздел о каталогах и ссылках баз данных);
- О **Database** (Базы данных) - содержит набор инструментов для указанной в панели **Files** базы данных (можно просто перетащить ее значок на нужный инструмент).

Некоторые инструменты описаны в следующем разделе, остальные рассмотрены далее в этой главе.

Использование инструментов базы данных

Компания Lotus рекомендует регулярно выполнять определенные действия по поддержанию баз данных. В табл. 14.1 описаны эти действия и указана частота их выполнения.

Таблица 14.1. Регулярно выполняемые задачи по поддержанию баз данных

Частота	Задача
Ежедневно	Контролировать репликацию баз данных
Ежедневно (по умолчанию в 13.00)	Поддерживать синхронность баз данных, созданных с помощью шаблонов, и самих шаблонов посредством задачи Designer
Ежедневно (по умолчанию в 14.00)	Обновлять все виды и полнотекстовые индексы, запуская задачу Updall
Ежедневно для больших архивных баз данных, еженедельно для всех остальных базы данных	Проверять и устранять конфликты репликации и сохранения
Иногда	Контролировать кэширование баз данных
Еженедельно	Контролировать работу баз данных
Еженедельно	Контролировать размер баз данных φ
Еженедельно или ежемесячно для баз данных R5/6, еженедельно в нерабочее время для базы данных R4	Выполнять уплотнение
По необходимости	Все остальные

Многие инструменты, служащие для поддержки баз данных, находятся на вкладке **Files** • окна **Domino Administrator**. Отметьте нужный сервер и щелкните по вкладке **Files**. Затем на панели **Files** задайте требуемую базу, щелкните по значку **Database** на панели **Tools**. Щелкните по названию программного инструмента, который нужно применить к выбранной базе данных.

Управление списками ACL базы данных

Чтобы не открывать списки ACL каждой базы данных, можно воспользоваться этим инструментом для одновременного обновления ACL сразу нескольких баз. Перед его употреблением убедитесь, что имеете доступ уровня **Manager** к каждой редактируемой базе данных.

Определение уровней доступа к нескольким базам данных несильно отличается от установки его для одного списка ACL одной базы. Чтобы добавить выбранные группы или отдельных пользователей в ACL, щелкните по **Add** (Добавить). Можно занести имена пользователей, групп, серверов, идентификационные данные реплик баз данных, значение **Anonymous** (Анонимный доступ) для пользователей Internet и пользователей Notes, персональные и групповые имена Internet-клиентов и псевдонимы. Имена необходимо вводить в иерархическом формате, хотя допускаются и подстановочные символы, например */Sales/ABC Corp, чтобы включить всех членов организации или организационной единицы.

Если вы не предоставляете доступ анонимным пользователям Internet, то Internet-клиенты должны аутентифицироваться с помощью имени и пароля или по протоколу SSL. Internet-клиентов следует перечислить по именам, которые указаны в их персональных документах, причем поля **Default** (По умолчанию) и **Anonymous** надо установить в значение **No Access**.

Назначьте уровень доступа отдельным пользователям, серверам, группам пользователей и группам серверов. Если вы не хотите всем пользователям и серверам предоставлять какой-либо определенный доступ, задайте уровень доступа **Default** (По умолчанию). Информация об уровнях доступа приведена в главе 10.

Ответственными за базу данных должны быть по крайней мере два человека - в отсутствие одного все функции будет выполнять второй. Обоим нужен доступ уровня **Manager**.

Не устанавливайте для пользователя или группы уровень доступа выше, чем им на самом деле требуется. Избегайте конфликтов репликации и сохранения, присваивая вместо уровня **Editor** уровень **Author**.

При необходимости распределите роли на вкладке **Roles** (Роли). Если вы добавляете роли в ACL, то окно **Roles** показывает только изменения, а существующая информация не отображается. Поэтому при переименовании какой-либо роли необходимо щелкнуть по кнопке **Rename** (Переименовать) и указать в поле **From** (Из) первоначальное имя роли, как оно записано в ACL (учитывая скобки и регистр). Удаляется существующая роль щелчком по **Remove** и указанием имени удаляемой роли (скобки можно не учитывать).

На вкладке **Advanced** следует назначить административный сервер, чтобы можно было обновлять имена и управлять ими в ACL, а также в полях **Author** и **Reader** баз данных с помощью процесса Administration Process.

Создание реплик нескольких баз данных

Инструмент Create Replica(s) (Создать реплики) позволяет создавать реплики на серверах того же домена Notes, а также на серверах других доменов. Между сервером-источником и сервером-получателем необходимо обеспечить соединение (необязательно, чтобы они находились в одном кластере), а вы и сервер-источник должны иметь возможность формировать реплики на сервере-получателе. Требуется доступ как минимум **Reader** к базе данных, реплику которой вы делаете. На сервере-источнике следует запустить процесс Administration Process.

Когда сервер-получатель расположен в другом домене, убедитесь, что:

- О создан кросс-сертификат, если серверы не имеют общего заверителя;
- О на сервере-источнике в базе данных Administration Requests (Административные запросы) есть исходящий документ Cross Domain Configuration (Междоменная конфигурация). Это позволит процессу Administration Process передавать запрос **Create Replica** (Создать реплику) на сервер-получатель;
- О на сервере-получателе в базе данных Administration Requests существует входящий документ Cross Domain Configuration. Тогда Administration Process будет получать запрос **Create Replica** от домена сервера-источника;
- О документы соединения (Connection document), отвечающие за маршрутизацию почты, настроены таким образом, чтобы сервер-источник мог отправлять почту хотя бы одному серверу в домене сервера-получателя.

Откройте программу Domino Administrator на вкладке **Files** для сервера-источника (см. рис. 14.1). На панели **Files** выберите базу данных, для которой нужно сформировать реплику или реплики. Щелкните на панели **Tools** по разделу **Database** и выберите команду **Create Replica(s)** или перетащите указанную базу данных на этот инструмент.

Назначьте для реплики сервер-получатель; если в текущем домене есть кластеры, щелкните по кнопке **Show only cluster members** (Отображать только серверы кластера), чтобы отображались лишь серверы этого кластера. Для задания другого сервера щелкните по **Other** (Другой).

Чтобы определить путь к пользовательскому файлу на сервере-получателе, щелкните по **File Names**, укажите путь и щелкните по ОК. Повторите описанную операцию для каждого сервера-получателя. Если вы не назначите путь, реплика будет помещена на сервере-получателе в то же место, что и на исходном сервере. Чтобы внести реплику в каталог, расположенный в каталоге данных сервера Domino, введите имя каталога, обратный слэш и имя файла, например Projects\Tradeshaw. Если каталога нет, сервер Domino создаст его.

После щелчка по кнопке ОК появится диалоговое окно, отображающее число обработанных баз данных и обнаруженные ошибки.

Быстрый способ создания реплик с помощью вкладки **Files** заключается в перетаскивании мышью. При этом реплика формируется в той же папке на сервере-получателе, но папка уже должна существовать. На панели **Files** выберите базу данных, для которой делается реплика. Затем перетащите ее на нужный сервер на панели **Server**. В открывшемся диалоговом окне отметьте **Create Replica** и затем на сервере-получателе пометьте папку, в которую следует поместить реплику.

Уплотнение для освобождения пространства

По мере удаления документов и вложений файлов из базы данных в ней остается неиспользуемое место. Сервер Domino старается повторно целиком заполнить освободившееся пространство, но сделать это не всегда удастся из-за фрагментации. Чтобы удалить такие области, необходимо уплотнить базу данных.

Для просмотра занятого места проверьте вид **Database => Sizes** (База данных =Ф Размеры) файла журнала сервера, отчеты **File Statistic**, генерируемые задачей Statistics Collector, или вкладку **Info** (Информация) в диалоговом окне **Database Properties**. Но они не всегда точно отображают реальные размеры. Не принимайте решение об уплотнении на основании только этой информации.

Хотя уплотнение базы данных в основном служит для восстановления свободного места, необходимо применять его также и для включения и выключения определенных свойств базы данных, запуска инструментов архивирования и восстановления баз данных с ошибками.

Существует три типа уплотнения:

- О уплотнение на месте с восстановлением пространства (-B). Не сокращает размера файла базы данных, но восстанавливает неиспользуемое пространство. Взаимоотношения между уплотненной базой и журналом транзакций не затрагиваются. Во время уплотнения пользователи могут работать и редактировать базу данных. Применяется к базам, для которых ожидается такой же размер или его увеличение;
- О уплотнение на месте с восстановлением пространства и сокращением размера (-B). Тип уплотнения, заданный по умолчанию в том случае, когда запускается уплотнение без установки определенных параметров, которые недоступны для протоколирования транзакций. Этот режим одновременно сокращает размер базы данных и восстанавливает свободное пространство. Работает немного медленнее. Если вы определяете такой режим заблокированным базам данных и у вас есть сертифицированное для версии R5/6 средство создания резервных копий, то после уплотнения сделайте полное резервирование базы. Во время уплотнения пользователи также имеют доступ к базе данных. Запуская такое уплотнение по меньшей мере раз в неделю, удастся оптимизировать дисковое пространство;
- О уплотнение с копированием. Режим требует наличия дополнительного дискового пространства, поскольку сначала формируется копия базы данных, а потом, по окончании уплотнения, исходная база данных удаляется. Назначается по умолчанию при активизации свойств базы данных, которые требуют ее реструктуризации, то есть для **Document table bitmap optimization** (Оптимизация образов таблиц документов) или **Don't support specialized response hierarchy** (Не поддерживать специализированную иерархию откликов). Кроме того, устанавливается по умолчанию при уплотнении базы данных, для которой предполагается реструктуризация, отложенная из-за вызова команды **Compact** (Уплотнение) из диалогового окна **Database Properties** (Свойства базы данных). Применяется также в R4. Пользователи и серверы не могут редактировать документы базы данных во время уплотнения, а читать их они в состоянии только с ключом -L.

В Domino существует несколько способов запуска уплотнения:

- О для одиночной базы данных укажите **Compact without options** (Уплотнение без параметров) в диалоговом окне **Database Properties**;
- О на сервере задайте Compact с помощью инструмента **Task => Start** (Задача => Запуск) в Domino Administrator;
- О на консоли сервера введите команду Compact с необходимым набором параметров;
- О запустите Compact посредством документа программы, который позволяет планировать запуск уплотнения в определенное время;
- О в Domino Administrator на вкладке **Files** обратитесь к инструменту Compact, чтобы уплотнить одну или несколько баз данных. До окончания уплотнения вы не сможете работать с программой Domino Administrator.

Для уплотнения базы данных с помощью инструмента Compact сначала отметьте сервер на панели **Server** (когда сервер не назначен, Compact работает с локальными базами данных). Щелкните по вкладке **Files** и на панели **Files** укажите требуемую базу данных. Затем

на панели **Tools** задайте вкладку **Database** и щелкните по инструменту Compact или просто перетащите выбранную базу данных на имя этого инструмента. Установите параметры уплотнения и щелкните по ОК.

Для определения способа уплотнения используется несколько опций. Они представлены в табл. 14.2.

Таблица 14.2. Параметры уплотнения

Параметр	Эквивалент команды на консоли управления (с учетом регистра)	Описание
Compact only if unused space	-S процент	Уплотняет все базы данных, имеющие установленный процент (n%) неиспользуемого пространства. Рекомендуется уплотнять базы с 10% неиспользуемого пространства. Отбрасывает индексы видов, созданные при разработке. Уплотнение с копированием. Задается перед записью базы данных на магнитную ленту
Set maximum size of database to 4 GB (Установить максимальный размер базы данных равным 4 Гб)	-M	Применяется только для баз данных R4. Устанавливает максимальный размер равным 4 Гб и уплотняет базы данных. Уплотнение с копированием
Keep or revert database to R4 format (Сохранить или преобразовать базу данных в формат R4)	-R	Уплотняет базы данных, не преобразуя их в формат R5/6, или преобразует базы обратно в формат R4. Уплотнение с копированием
Archive database (Архивировать базу данных)	-A	Архивирует и удаляет документы из базы данных без уплотнения самой базы
In-place (На месте) - рекомендуется	-b	Восстанавливает неиспользуемое место без изменения размера файла базы данных
In-place with size reduction (На месте с уменьшением размера)	-B	Восстанавливает неиспользуемое место и уменьшает размер файла базы данных. Если вы работаете с журналом транзакций, то после окончания уплотнения сделайте полное резервирование баз данных
Copy Style: Allow access while compacting (С копированием: разрешить доступ во время уплотнения)	-L	Пользователи могут получить доступ к базе данных во время уплотнения, но если пользователь изменяет базы данных, уплотнение прерывается

Таблица 14.2. Параметры уплотнения (окончание)

Параметр	Эквивалент команды на консоли управления (с учетом регистра)	Описание
Copy Style: Ignore errors during compaction (С копированием: пропускать ошибки во время уплотнения) Недоступно из инструмента Compact, но уплотняет базы данных в комбинации с другими инструментами	-i	Уплотнение продолжается, даже если обнаруживается ошибка, например порча документа
	-f	Отключает свойство базы данных Document table bitmap optimization (Оптимизация изображений таблиц документа). Уплотнение с копированием
	-F	Активирует свойство базы данных Document table bitmap optimization. Уплотнение с копированием
	-h	Отключает свойство базы данных Don't support specialized response hierarchy (Не поддерживать иерархию специализированных откликов). Уплотнение с копированием
	-H	Активирует свойство базы данных Don't support specialized response hierarchy. Уплотнение с копированием
	-T	Активирует журнал транзакций
	-t	Отключает журнал транзакций
	-и	Отключает свойство базы данных Don't maintain unread marks (Не сохранять непрочитанные метки)
	-И	Активирует свойство базы данных Don't maintain unread marks Архивирует и удаляет документы из базы данных, а затем уплотняет ее

Улучшение производительности базы данных

На вкладке Advanced диалогового окна Database Properties (Свойства базы данных) имеется несколько параметров, позволяющих улучшить производительность базы данных (рис. 14.2). Когда пользователи начинают жаловаться на ухудшение производительности базы, можно активизировать некоторые параметры (табл. 14.3).

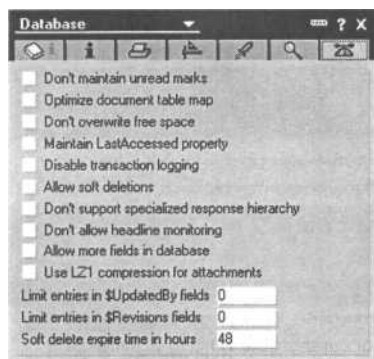


Рис. 14.2. Многие параметры на вкладке **Advanced** диалогового окна **Database Properties** улучшают производительность базы данных. Однако при активизации некоторых из них, таких как **Don't overwrite free space**, меняются функциональные возможности (указанный параметр ослабляет защиту базы данных)

Таблица 14.3. Дополнительные параметры базы данных, улучшающие ее производительность

Параметр	Описание
Don't maintain unread marks (Не сохранять непрочитанные метки)	Хранит информацию о прочитанных документах и о документах, не замедляющих работу базы данных. Если такая информация не нужна, поставьте этот флажок
Document table bitmap optimization (Оптимизация изображений таблиц документа) в R5 или Optimize document table map (Оптимизация изображений таблиц документа)	Notes хранит таблицы информации о документах, к которым система обращается при обновлении вида. При активизации данного параметра система связывает таблицы с формами, которые применяются документами. Затем Notes ищет вид, содержащий формы, используемые документами в обновляемом виде, только в этих таблицах. Поддержка таких связей немного ухудшает производительность, но заметно ускоряет обновления маленьких видов в больших базах данных. Для активизации указанного параметра необходимо уплотнить базы данных
Don't overwrite free space (Не перезаписывать на свободное место)	В качестве средства защиты Notes автоматически производит запись на место удаленных данных. Это может уменьшить производительность. Когда база данных защищена физически, свободное место в ней быстро перераспределяется, поэтому, если вопрос защиты не очень важен, лучше активизировать названный параметр
Maintain LastAccessed property (Поддерживать свойство LastAccessed)	Установка параметра может ухудшить производительность. По умолчанию база данных хранит сведения о последнем изменении документа. При активизации этого параметра также сохраняется информация о последнем чтении документа. Обращайтесь к данному параметру только в целях отслеживания активности документа за определенный промежуток времени при архивации и удалении
Disable transaction logging (Отключить журнал транзакций)	Параметр отключает журнал всех транзакций функций API сервера Domino. Вы теряете возможность поддержания целостности базы данных и быстрого отката транзакций вперед и назад, а также поддержки резервирования и восстановления функций API. Прежде чем активизировать этот параметр, необходимо сравнить выигрыш в производительности и потерю указанных возможностей

Таблица 14.3. Дополнительные параметры базы данных, улучшающие ее производительность (окончание)

Параметр	Описание
Allow soft deletions (Разрешить мягкое удаление)	Позволяет пользователям восстанавливать удаленные из базы данных документы. Для этого нужен специальный вид, отображающий удаленные документы (см. раздел о начальной настройке свойств базы данных)
Don't support specialized response hierarchy (Не поддерживать иерархию специализированных откликов)	Для баз данных, которые не работают с документами типа «отклик» и «отклик на отклик» или в видах отображают иерархию откликов, нет необходимости в функциях OAllChildren или @AllDescendents . В таких базах данных выбор этого параметра улучшает производительность
Don't allow headline monitoring (Не разрешать наблюдение за базой данных)	Пользователи могут подписываться на документы и получать извещения, которые отображают любые интересные их объекты. Просмотр базы данных многими пользователями сильно уменьшает ее производительность. Чтобы отменить такой просмотр, активизируйте данный параметр
Allow more fields in database (Разрешить большее количество полей в базе данных)	При выборе этого параметра допускается добавлять в базу данных до 64000 полей, однако при этом ухудшится ее производительность
Limit entries in \$UpdateBy fields (Ограничить записи в поле \$UpdateBy)	Любые изменения, внесенные в документ, сохраняются в поле \$UpdateBy. Поддержка названного свойства существенно увеличивает расход дискового пространства и сильно замедляет обновления и репликацию. Введите число в данное поле, чтобы ограничить количество отслеживаемых изменений. При достижении установленного предела самая старая запись удаляется и заменяется новой
Limit entries in \$Revision\$ fields (Ограничить записи в поле \$Revisions)	Все документы хранят информацию о времени и дате каждого изменения в поле \$Revisions. Такие сведения требуются для разрешения конфликтов сохранения и репликации. По умолчанию здесь может содержаться до 500 записей. Введите число в это поле, чтобы ограничить количество хранящихся записей (для разрешения конфликта необходимо минимум 10 записей) и улучшить производительность базы. По достижении установленного предела самая старая запись заменяется новой. Этот параметр рекомендуется для баз данных, которые содержат много документов, часто реплицируются или не имеют реплик либо включают в себя редко изменяемые документы
Undelete Expire time (Время задержки удаления) в R5 или Soft delete expire time in hours (Время задержки удаления в часах) в R6	Промежуток времени (в часах), в течение которого пользователь может восстановить удаленные документы (если включена функция Allow soft deletions)
Use LZ1 compression for attachments (Использовать для вложений алгоритм сжатия LZ1), только для R6	В версии R6 позволяет применять более совершенный алгоритм сжатия вложений

Чтобы не определять эти параметры отдельно для каждой базы данных в диалоговом окне **Database Properties**, удобно прибегнуть к инструменту **Advanced Properties** (Дополнительные свойства). Требуется иметь к обрабатываемым базам данных уровень доступа **Designer** или **Manager**.

Для установки **Advanced Properties** откройте **Domino Administrator**, на панели **Server** назначьте сервер, выведите на экран панель **Files** и отметьте базы данных, для которых нужно задать дополнительные параметры. На панели **Tools** укажите раздел **Database** и затем **Advanced Properties** (рис. 14.3). Для каждого параметра, который надо выбрать, отметьте флажок **Select** и затем поставьте флажок для параметра, чтобы активизировать его (или снимите, чтобы отключить). По окончании щелкните по **OK**.

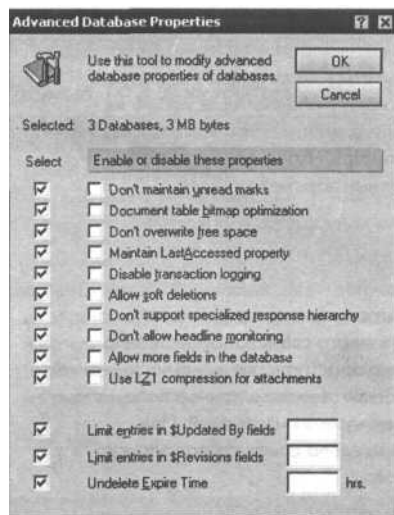


Рис. 14.3. Параметры, устанавливаемые индивидуально для каждой базы данных в диалоговом окне *Database Properties*, это окно позволяет применить к нескольким выбранным базам

Уплотнив предварительно базы данных, можно эффективно применить к ним следующие три параметра:

- **Don't maintain unread marks** (Не сохранять непрочитанные метки);
- **Document table bitmap optimization** (Оптимизация изображений таблиц документа);
- **Don't support specialized response hierarchy** (Не перезаписывать на свободное место).

С помощью командной строки эти параметры активизируются во время уплотнения (см. раздел об уплотнении для освобождения пространства).

Использование квот для поддержания размера базы данных

Базы данных в **Windows** и **UNIX** могут достигать 64 Гб, а в **OS/2** – 32 Гб (базы данных **R4** имеют максимальный размер 1, 2, 3 и 4 Гб). Если у вас есть жесткий диск, способный хранить базы таких размеров, то устанавливать квоты бессмысленно. Квота – это инструмент администратора, желающего контролировать размеры баз данных в целях поддержания высокой производительности и эффективного использования дискового пространства. Квота определяет максимальный размер базы данных.

Когда пользователь пытается открыть базу данных, которая достигла размера, определенного квотой, выводится сообщение **Cannot allocate object - database will exceed its disk quota** (Невозможно разместить объект - база данных превысит установленную квоту).

Такое же сообщение появляется на виде **Miscellaneous Events** (Разные события) в журнале регистрации. Если в базе данных есть место, оставшееся от удаленных документов, то пользователи могут добавлять в нее документы, даже если исчерпан лимит, установленный квотой.

Наиболее вероятный результат сообщения о превышении лимита (квоты) - это немедленный (и, скорее всего, раздраженный) телефонный звонок пользователя администратору, особенно если база данных является почтовой. Маршрутизатор будет доставлять почту, даже если достигнут предел, причем пользователь в состоянии читать почту и обновлять виды, но не может добавлять документы и виды в свой почтовый файл. Чтобы более строго следить за почтовыми базами данных, стоит установить свойство маршрутизатора **Obey database quotas during message delivery** (При доставке почты учитывать квоту базы данных). Назначая квоту, можно дополнительно задать порог базы данных. Порог (граничное значение) - это определенный размер, который меньше квоты. По достижении порога базы данных пользователь получает сообщение **Warning, database has exceeded its size warning threshold** (Предупреждение! Размер базы данных достиг порога предупреждения). Такое же сообщение появляется на виде **Miscellaneous Events** в журнале регистрации.

В ответ на звонок раздраженного пользователя по поводу сообщения о достижении порога проинформируйте, что почту он будет получать, но скоро размер базы данных станет максимальным. Это самое лучшее время поднять вопрос об архивировании или удалении некоторых почтовых сообщений.

Для непочтовых баз данных полезно установить порог, предупреждающий пользователя о необходимости что-то предпринимать для сокращения размера базы: архивировать старые и удалять неиспользуемые файлы, изменять параметры производительности базы, чтобы сделать ее меньше, ограничить размер реплик с помощью **Replication Settings** (Параметры репликации), сократить интервалы между очистками, чтобы чаще убирать остатки после удаления файлов или уплотнять базы данных. Можно также перенести базы данных на другой диск, на котором больше свободного места.

Для установки квоты и порога базы данных откройте Domino Administrator и выберите сервер на панели **Server**. Щелкните по вкладке **Files** и на одноименной панели выделите базы данных, для которых нужно задать квоту. На панели **Tools** отметьте раздел **Database** и щелкните по инструменту **Quotas** или перетащите указанные базы данных на имя этого инструмента.

Чтобы посмотреть абсолютный максимальный размер (в мегабайтах), текущий размер (в мегабайтах), текущую квоту и текущий порог предупреждения для каждой выбранной базы данных, нажмите **More Info** (Больше). Возвратитесь в диалоговое окно **Set Quotas** (Установка квот), щелкнув по ОК.

Выберите **Set database quota to** (Установить квоту базы данных для) и введите размер квоты в мегабайтах. Для определения порога предупреждения щелкните по полю **Set warning threshold to** (Установите порог предупреждения для) и укажите величину порога в мегабайтах. Щелкните по ОК. Заданные квота и порог предупреждения распространяются на каждую выделенную базу данных.

Архивирование документов базы данных

Архивирование документов созданных в R5/6 стало гораздо проще: теперь не нужно писать агенты. Для архивирования предназначено диалоговое окно **Database Properties** на вкладке **Basics**. Щелкните по кнопке **Archive Settings** (Параметры архивирования) и установите параметры архивирования, архивируемые документы и время их архивирования. Архив базы данных создается автоматически и по умолчанию имеет имя файла `archive\a_databasename.nsf`. Notes позволяет автоматически только архивировать базы данных, но можно устанавливать регистрацию архивирования. По умолчанию журнал архивов сохраняется под именем `archive\l_databasename.nsf`.

Перенос базы данных на новый сервер

Иногда возникает ситуация, в которой требуется перенести базы данных с одного сервера на другой. Это можно сделать вручную - с помощью инструмента Move (Перенести) в Domino Administrator или просто перетащив базу данных на другой сервер в том же окне. Но ни один из таких способов нельзя применить к почтовым файлам. Для перемещения почтовых файлов существует специальная процедура, выполняемая посредством процесса Administration Process. Также можно рассмотреть вопрос создания ссылки для базы данных или каталога, особенно если переносится база, находящаяся не в каталоге данных Domino (см. ниже).

Перенос базы данных вручную

Перенос базы данных на другой сервер реализуется либо с помощью операционной системы, либо за счет создания реплики этой базы в новом месте с последующим удалением исходной базы данных. Мы не рекомендуем действовать таким образом, за исключением случаев, когда база данных перемещается на сервер вне домена Notes или на сервер, не имеющий доступа к программе Domino Administrator.

В почтовой базе данных необходимо внести изменения в документ базы данных Mail-in (Входящая почта) в каталоге Domino, чтобы определить новое место. Также следует поменять в списке ACL переносимой базы данных имя сервера: удалить имя старого сервера и добавить имя нового. Убедитесь, что документ соединения правильно настроен для репликации на новом сервере (если только серверы не входят в один кластер).

Надо уведомить пользователей о переносе базы данных. Один из способов заключается в том, чтобы создать на месте старой базы новую с тем же названием (заголовком) и именем файла. Затем нужно сформировать в новой базе данных форму, в которой будет указано имя исходной базы, ее имя файла и путь, дата и причина перемещения, имя нового сервера, новое имя файла и путь. Для удобства можно даже сделать в этой форме кнопку, при нажатии на которую открывается нужная база данных. Попробуйте воспользоваться командой `@Command([FileOpenDBRepID]; "replicaIDnumber"; "newServerName")`.

Использование инструмента Move

Когда нет необходимости перемещать базу данных вручную, примените инструмент Move в Domino Administrator, который использует процесс Administration Process. Но прежде

удостоверьтесь, что на обоих серверах работает Administration Process. Вам потребуется право **Create Database** (Создание базы данных) в серверном документе на сервере-получателе и доступ уровня **Manager** с правом **Delete Documents** (Удаление документов) на сервере-источнике. Кроме того, сервер-источник или другой сервер (на котором есть реплика исходной базы данных) должны иметь право **Create Replica** (Создание реплики) на сервере-получателе. Сервер-получатель должен иметь для реплики в списке ACL на сервере-источнике доступ уровня не менее **Reader**.

Откройте Domino Administrator, на панели **Server** укажите сервер-источник, щелкните по вкладке **Files** и выделите на панели **Files** требуемую базу данных, затем на панели **Tools** раскройте раздел **Database** и отметьте инструмент Move (или просто перетащите выбранную базу данных на имя этого инструмента). Определите один или несколько серверов-получателей, если текущий домен содержит кластеры, задайте **Show me only cluster members** (Показать только членов кластера) и укажите нужный сервер. Если его в списке нет, нажмите **Other** (Другие) и введите иерархическое имя сервера-получателя.

Чтобы задать путь к перемещаемой базе данных на сервере-получателе, щелкните по кнопке **File Names** и укажите путь и имя файла, в котором должна быть сохранена база. В противном случае база хранится в том же месте, в котором она находилась на сервере-источнике. Для размещения базы в каталоге, расположенном в каталоге данных Domino, внесите имя каталога, обратный слэш и имя файла, например Planning\Tradeshow. Если каталог не существует, сервер Domino создаст его.

После щелчка по кнопке ОК появляется диалоговое окно, отображающее число обработанных баз данных и возникающие ошибки.

Если сервер-источник находится не в кластере, возможно, придется еще немного поработать - подтвердить удаление каждой исходной базы данных после того, как Administration Process завершит обработку запроса **Non Cluster Move Replica** (Некластерное перемещение реплики), который создает на сервере-получателе новую копию. Для этого требуется доступ к базе данных Administration Requests (Административные запросы) как минимум **Editor**. Откройте сначала базу данных Administration Requests, а затем вид **Pending Administrator Approval** (Подтверждение отложенного администрирования). Для каждой перемещаемой базы данных выведите на экран запрос **Approve Deletion of Moved Replica** (Подтверждение удаления перемещенной реплики) в режиме редактирования. Щелкните по кнопке **Approve File Deletion** (Подтвердить удаление файла), отметьте Yes, после чего сохраните и закройте документ.

Поставьте всех пользователей в известность о перемещении базы данных как и в случае переноса базы вручную. ^

Перетаскивание

Напоследок остался самый простой способ, при котором база данных сохраняется в определенной папке (формируемой дополнительно) на сервере-получателе. Здесь применяется Administration Process, так что этот метод не годится для переноса на сервер другого домена.

Откройте Domino Administrator, на панели **Server** выберите сервер-источник, щелкните по вкладке **Files** и выделите на панели **Files** требуемую базу данных. Перетащите выбранные базы на сервер-получатель на панели **Server**. В появившемся диалоговом окне задайте **Move database** (Перенести базу данных), укажите папку назначения и щелкните по ОК.

Защитная подпись

Подписывая базы данных или шаблон, вы добавляете подпись, которая может служить для защиты рабочей станции. После подписи базы данных или шаблона, разработанных в вашей организации, соответствующее имя добавляется в список ECL.

Если база данных создается на основе подписанного шаблона, она наследует подпись. В списке ECL (Список управления исполнением) рабочей станции пользователь может определить, какой доступ к его рабочей станции имеют базы, подписанные организацией или конкретным пользователем, но еще важнее указать уровень доступа для неподписанных баз данных.

Допускается подписывать отдельные документы проектирования или их элементы, но для этого нужен их файл идентификационных данных (Note ID), который находится на вкладке **Document IDs (ID документа)** окна **Document Properties (Свойства документа)** и начинается с NT... Когда вы записываете Note ID, пропустите нули между NT и номером.

Перед началом подписи убедитесь, что текущий ID-файл является тем файлом, который предназначен для подписи базы данных или шаблона. В Domino Administrator выберите сервер, содержащий подписываемые базы данных или шаблоны. Щелкните по вкладке **Files** и отметьте требуемые файлы. На панели **Tools** раскройте раздел **Database** и выберите Sign.

Укажите одну из перечисленных ниже операций:

- **All Design documents** (Все документы проектирования) - подписываются все проектные документы;
- **All documents of type** (Все документы выбранного типа) - подписываются заданные типы элементов проектирования: **Policy** (Политика), **Form (Форма)**, **View (Вид)**, **Icon** (Значок), **Design Note** (Заметки проектирования, только в R5), **ACL** (Список управления доступом), **Help Index** (Индекс справки, только в R5), **Help** (Справка), **Agent** (Агент), **Shared Field** (Общие поля), **Repl Formula** (Формула репликации). При выборе **Design Note** процесс подписи занимает достаточно продолжительное время, особенно если подписывается несколько баз данных или шаблонов;
- **This specific Note ID** (Определенный идентификационный элемент) - подписывается конкретный проектный элемент (см. ниже).

Если вы установили режим **Update existing signatures only** (Только обновить существующие подписи), который работает быстрее, то обновляются только существующие подписи. Этот режим применяется для изменения подписей элементов.

После щелчка по кнопке ОК появляется диалоговое окно, отображающее число обработанных баз данных и число возникших ошибок. Подробности сохраняются в журнале Notes.

Более детально о взаимодействии подписанных баз данных и ECL рассказывается в главе 10.

Временная отмена репликации

Если возникает проблема при репликации, то для ее разрешения требуется некоторое время. Нежелательно реплицировать базу данных в этот момент, поскольку проблемы с базой

могут отразиться и на другом сервере. Чтобы временно отменить репликацию, откройте окно **Replication Settings** (Параметры репликации), выбрав **File => Replication => Settings** (Файл => Репликация => Параметры). Затем на вкладке **Other** (Другое) установите флажок **Temporarily Disable Replication** (Временно отменить репликацию). После решения проблемы можно сбросить флажок и возобновить репликацию.

Для включения или отмены репликации сразу нескольких баз данных предназначен инструмент Replication на вкладке **Files** в Domino Administrator. На панели **Server** определите сервер, где хранятся базы данных, щелкните по вкладке **Files** и на одноименной панели отметьте базу данных. На панели **Tools** откройте раздел **Database** и укажите инструмент Replication или перетащите выбранную базу данных на имя этого инструмента. Задайте **Disable** (Отменить) и щелкните по ОК.

Чтобы возобновить репликацию, повторите все указанные действия, но в диалоговом окне **Replication** выберите **Enable** (Разрешить).

Восстановление поврежденных баз данных с помощью Fixup

Иногда в R5/6 встречаются поврежденные базы данных, хотя это случается нечасто благодаря журналу транзакций (см. раздел о регистрации транзакций). Повреждение баз данных скорее касается версии R4. Оно может быть результатом сбоя питания, сбоя системы, сбоя диска или неправильного обращения программы к базе данных через функции API.

Журнал Notes Log при обнаружении поврежденной базы данных регистрирует сообщение, например **Document NT000082NC in database Projects.nsf is damaged** (Документ NT000082NC в базе данных Projects.nsf поврежден), где номер, начинающийся с NT, - последние 10 разрядов идентификатора документа, отображаемого в окне **Document Properties** (Свойства документа). После сообщения следует строка, раскрывающая причину повреждения, например **Document is damaged or obsolete (unrecognized field)** - Документ поврежден или устарел (нераспознанное поле). Если проблема возникает с видом, который Domino пытается восстановить, или она появляется в процессе воссоздания, либо документ восстановить невозможно, то может быть выведено сообщение типа **Page format is incorrect** (Неверный формат страницы), **Invalid CNO vector - position == 0** (Недопустимый CNO-вектор - позиция == 0) или **Container integrity has been lost - rebuild** (Нарушена целостность контейнера - необходима перекомпоновка). ^

Существует несколько способов восстановления поврежденных баз данных:

- О запуск задачи Updall на сервере для восстановления поврежденных видов и полнотекстовых индексов (см. раздел о поддержке индексов баз данных);
- О запуск задачи Fixup на сервере для восстановления поврежденных видов и документов;
- О выполнение команды уплотнения Compact с ключом -C;
- О перекомпоновка видов с помощью комбинации клавиш **Shift+F9** - для одного вида или **Ctrl+Shift+F9** -> для всех видов в базе данных;
- О создание реплик базы данных.

Обычно, если повреждены виды, вы сначала запускаете Updall, а затем Fixup. Задачу Fixup можно запустить несколькими способами:

- О в окне Domino Administrator с помощью инструмента **Task => Start** (Задача => Запуск), расположенного в разделе **Server => Status** (Сервер => Состояние). Укажите параметры работы Fixup (совпадают с параметрами ввода командной строки). Этот метод служит для восстановления незарегистрированных баз данных;
- О посредством команды Load fixup параметры на консоли управления. Используется, когда при работе на сервере приходится вводить команды с консоли управления. Укажите имя файла базы данных или путь, чтобы восстановить конкретную базу либо все базы данных в указанной папке;
- О путем создания документа программы, чтобы запланировать запуск Fixup в определенное время. Программа должна иметь имя Fixup, а в поле **Command line** (Командная строка) следует указать необходимые параметры командной строки;
- О инструментом Fixup на вкладке **Files** в Domino Administrator. Лучше работает для одной или нескольких баз данных.

Чтобы применить инструмент Fixup, определите требуемый сервер на панели **Server** в Domino Administrator. Щелкните по вкладке **Files** и на одноименной панели выберите нужные базы данных. На панели **Tools** откройте раздел **Database** и отметьте инструмент Fixup. Установите параметры, необходимые для работы Fixup, и щелкните по ОК. Параметры для программы Fixup и их описание приведены в табл. 14.4. В столбце «Параметр Fixup» перечислены параметры, как они указаны в окне Fixup, а в столбце «Параметр командной строки» приводится эквивалент для командной строки или документа программы.

Таблица 14.4. Параметры программы Fixup

Параметр Fixup	Параметр командной строки	Описание
Report all processed databases to log file (Заносить отчет об обработанных базах данных в файл журнала)	-L	Регистрирует каждое выполняемое Fixup открытие и проверку базы данных на предмет повреждения. Если параметр не установлен, Fixup фиксирует в журнал только обнаруженные ошибки
Excludeview (Исключить вид) - работает быстрее	-V	Fixup не обрабатывает виды, уменьшая таким образом общее время функционирования. Задавайте только в том случае, когда не рассматривается повреждение видов
Perform quick fixup (Быстрое восстановление)	-Q	Проверяет документы быстрее, но не так тщательно. Отмените этот режим, чтобы обеспечить более тщательное восстановление
Scan only since last fixup (Проверять только с момента последней проверки)	-i	При обработке определенных баз данных Fixup просматривает только те документы, которые изменялись с момента последней проверки. Если отменить этот режим, Fixup будет контролировать все документы

Таблица 14.4. Параметры программы Fixup (окончание)

Параметр Fixup	Параметр командной строки	Описание
Scan all documents (Сканировать все документы - параметр команды Task, Start)	-F	При обработке всех баз данных Fixup проверяет все документы баз. Если отменить этот режим, Fixup будет контролировать только те документы, которые изменялись с момента последней проверки
Optimize user unread lists (Оптимизировать непрочитанные списки пользователей)	-U	Преобразует таблицы идентификаторов ID в формате предыдущей версии. Используйте по рекомендации службы технической поддержки пользователей
Don't purge corrupted documents (Не очищать поврежденные документы)	-N	Fixup не очищает поврежденные документы. В следующий раз, когда пользователь откроет базу данных или при запуске Fixup, база проверяется снова. Устанавливайте этот режим только в том случае, когда требуется сохранить данные в документах с незначительными повреждениями или когда нет реплики базы
Fixup transaction-logged databases (Исправлять базы данных с регистрацией транзакций)	-J	Fixup работает с базами данных R5/6, для которых включена регистрация транзакций. Если этот режим не выбран, базы данных с регистрацией транзакций не обслуживаются. Если применяется поддерживаемое R5/6 средство резервирования, следует в кратчайшие сроки после запуска Fixup выполнить полное резервирование базы данных

Г~

Быстрое восстановление

Если повреждены один или два документа, то лучшим решением может стать черновое восстановление. Этот способ работает, только когда имеется реплика базы данных на другом сервере (можно временно отменить репликацию, пока не будут восстановлены базы). Удалите поврежденные документы в базе данных на текущем сервере. Затем откройте реплику и скопируйте эти документы в буфер обмена. Закройте реплику и выведите на экран поврежденную базу. Вставьте документы в базуданных.

Если повреждено большое количество документов, то приходится восстанавливать базы данных с резервной копии. Но в этом случае существует риск потерять новые документы и изменения, внесенные с момента последнего архивирования.

Идентификация документов из журнала регистрации

Когда файл журнала (Log) сообщает о проблеме, возникшей с тем или иным документом, он обращается к документу по его идентификатору (Note ID), который можно найти на вкладке **Document IDs** окна **Document Properties**. Он начинается с NT...

Если вы хотите больше узнать о документах, перечисленных в журнале регистрации, отыщите их по Note ID или по UNID (Universal Note ID - универсальный идентификатор). Проще всего скопировать Note ID данного документа из журнала в буфер (или записать его вручную). Откройте Domino Administrator и выберите сервер, на котором расположена база данных. Выведите на экран вкладку **Files** и отметьте базу на панели **Files**. На панели **Tools** разверните раздел **Database** и укажите **Find Note** (Найти идентификатор).

Задайте поиск либо по Note ID, либо по Universal Note ID (UNID) и затем вставьте или введите соответствующий идентификатор в поле ID. Щелкните по **Find** (Найти). В полях **Fields** и **Properties** отобразятся свойства и характеристики документа. Щелкните по **Done** (Готово) и закройте диалоговое окно.

Наличие информации о документе и отчета журнала регистрации позволяет предпринять определенные действия для решения проблемы.

Note ID

Note ID - это 8-разрядная комбинация букв и цифр, которая однозначно идентифицирует позицию документа внутри определенной базы данных. Документы, являющиеся репликами других документов, в общем случае имеют разные идентификаторы Note ID.

Universal Note ID

Universal Note ID—это уникальная 32-разрядная комбинация букв и цифр. Она идентифицирует документ среди всех реплик базы данных. Документы с одинаковыми UNID являются репликами друг друга.

Ссылки на каталоги и базы данных

По умолчанию базы данных на сервере Domino хранятся в каталоге данных (catalog data). Для группировки взаимосвязанных баз в этом каталоге обычно создаются подкаталоги. Однако базы данных допустимо хранить в другой папке, которая связана с каталогом данных Domino. Назначая уровень доступа определенных пользователей, можно защитить базы данных, хранящиеся в папке каталога. Еще одна причина применения папки каталога - недостаток свободного пространства на данном сервере и его наличие на другом сервере.

Сначала сформируйте папку каталога для хранения баз данных. Загрузите Domino Administrator и выберите сервер, на котором нужно поместить папку. Откройте вкладку **Files**. На панели **Tools** щелкните по **Folder** (Папка), затем выберите **New** (Новая).

Введите имя новой папки в поле **Name** и щелкните по ОК. Если нужно убедиться, что папка создана, нажмите на **Refresh** (Обновить).

Затем переместите базы данных в новую папку (см. раздел о переносе базы данных на новый сервер). Далее сделайте ссылку либо на каталог, либо на базу данных. Ссылки - это текстовые файлы, хранящиеся в каталоге данных Domino. Они содержат ярлыки для баз данных и папок, но на самом деле представляют собой указатели на папки, в которых размещаются базы, или на место хранения отдельной базы.

Ссылка на каталог. Ссылка на каталог находится в каталоге данных и указывает на папку каталога. Когда пользователь просматривает содержимое каталога данных, например в диалоговом окне **Open Database** (Открыть базы данных), он видит имя ссылки на каталог (текстовый файл с расширением .Dir, который указывает на реальный каталог). Может ли пользователь обращаться к каталогу, зависит от уровня его доступа.

Ссылка на базу данных. Если вы работаете с отдельной базой данных, которая хранится вне каталога данных Domino, но не в папке каталога, создайте для этой базы ссылку в каталоге данных Domino. При формировании ссылки необходимо указать полный путь и имя файла базы. В конце ссылки Domino автоматически создает расширение .nsf.

Чтобы сделать ссылку, откройте Domino Administrator, на панели **Server** выберите сервер, на который вы поместите ссылку, и перейдите на вкладку **Files**. На панели **Tools** укажите **Folder** и щелкните по **New Link** (Новая ссылка). Введите имя ссылки в поле **Link name** (Имя ссылки). Это имя пользователи увидят в каталоге данных.

Определите тип ссылки. Назначьте **Folder** для ссылки на каталог или **Database** для ссылки на базы данных. Задайте полный путь к каталогу или базе (для ссылки на базу данных укажите также имя файла базы).

Если нужно переопределить права доступа к базе данных, введите или выберите пользователей, которые могут получить доступ (они должны быть записаны также в список ACL этой базы). Чтобы предоставить доступ Web-пользователям, создайте запись **anonymous** (Анонимный доступ), а чтобы запретить им применять ссылки на каталоги, добавьте в файл notes.ini запись DominoNoDirKinks=1.

Щелкните по ОК. Обновите виды, чтобы увидеть созданные ссылки.

Подумайте относительно целесообразности использования ссылок на серверах OS/2, поскольку это влияет на производительность.

При изменении содержимого папки каталога необходимо обновить ссылки. Выберите сначала ссылку на панели **Files**, а затем **Update Link** (Обновить ссылку) на панели **Tools**. Для удаления ссылки перейдите на вкладку **Files** программы Domino Administrator. Выделите ссылку на каталог или на базу данных, на панели **Tools** отметьте вкладку **Folder** и щелкните по **Delete**. Подтвердите удаление щелчком по **Yes**.

Мониторинг и анализ активности базы данных

У пользователей иногда возникают проблемы с производительностью баз данных. Что делать? Если активность базы велика, то можно изменить параметры, влияющие на производительность, создать реплику базы данных на другом сервере (особенно когда серверы связаны в кластер) или переместить базу на более мощный сервер или на сервер, у которого больше дискового пространства.

Использование Statlog для мониторинга активности

Как проследить за активностью базы данных? Задача Statlog ежедневно отслеживает активность базы данных¹. Она запускается по умолчанию раз в день в 5 часов утра и записывает отчеты об активности баз данных сервера в Database Activity Log (Журнал активности баз данных), который можно открыть с помощью видов **Database => Usage** (База данных => Использование) и **Database => Sizes** (База данных => Размеры) в журнале регистрации (Log.nsf). Кроме того, Statlog записывает отчеты в диалоговое окно **User Activity** (Активность пользователей) каждой базы данных. Проверив информацию, вы будете знать, что происходит в базе данных. При этом:

- О и в Database Activity Log, и в User Activity Statlog вносит общее число обращений, чтений и записей в базу данных со стороны пользователей и серверов за прошедшие 24 часа, неделю, месяц и за все время с момента ее создания. Кроме того, включены сведения об активности анонимных и аутентифицированных пользователей Internet;
- О Database Activity Log отображает неактивные виды (с нулевым размером);
- О User Activity показывает имена пользователей и серверов, которые обращались к базе данных. Все имена сортируются по дате обращения.

Чтобы воспользоваться файлом журнала (Log.nsf), откройте Domino Administrator, выберите сервер на вкладке **Server** и щелкните по вкладке **Analysis** (Анализ) - рис. 14.4. Отметьте **Notes Log => Database => Sizes** либо **Notes Log => Database => Usage** в зависимости от статистики, которую нужно просмотреть. Двойным щелчком по строке **Database Activity Log** разверните соответствующую базу данных.

Для работы в диалоговом окне **User Activity** откройте исследуемую базу данных и выполните **File => Database ^Ф Properties** (Файл => База данных => Свойства). В диалоговом окне **Database Properties** (Свойства базы данных) выберите вкладку **Info** (Информация) и затем щелкните по **User Detail** (Подробности). Отобразится только текущая информация. Если нужно получить сводку за определенный промежуток времени, скопируйте эту информацию в буфер (в версии R6 для этого служит кнопка **Copy to Clipboard**) и вставьте в файл, выделенный вами для накопления статистики об активности пользователей.

Если вы не зададите другой порядок, Statlog будет записывать информацию об активности базы данных в журнал User Activity всех баз данных. Пользователь может отменить запись отчета в User Activity определенной базы данных, но при следующем запуске Statlog возобновит эту операцию.

Для отмены автоматической записи отчетов Statlog добавьте в файл notes.ini строку **No_Force_Activity_Logging=1**. Так вы сэкономите дисковое пространство, поскольку каждый отчет занимает 64 Кб в каждой базе данных. При этом Statlog продолжит помещать отчеты в файл журнала.

Если автоматическая запись отчетов во все базы данных отменена, ее можно активизировать для определенных баз данных, которые необходимо контролировать, но только в том случае, когда в списке ACL вам предоставлен уровень доступа **Manager** или **Designer**. Выведите на экран базу данных, для которой нужно активизировать автоматическую запись отчетов, и выберите **File => Database => Properties**. Откройте в диалоговом окне **Database Properties** вкладку **Info** и щелкните по **User Detail**. Отметьте **Record Activity** (Запись активности) - если сбросить этот флажок, то автозапись отчета об активности

Если в документе сервера разрешена регистрация действий в базе данных. - *Прим. ред.*

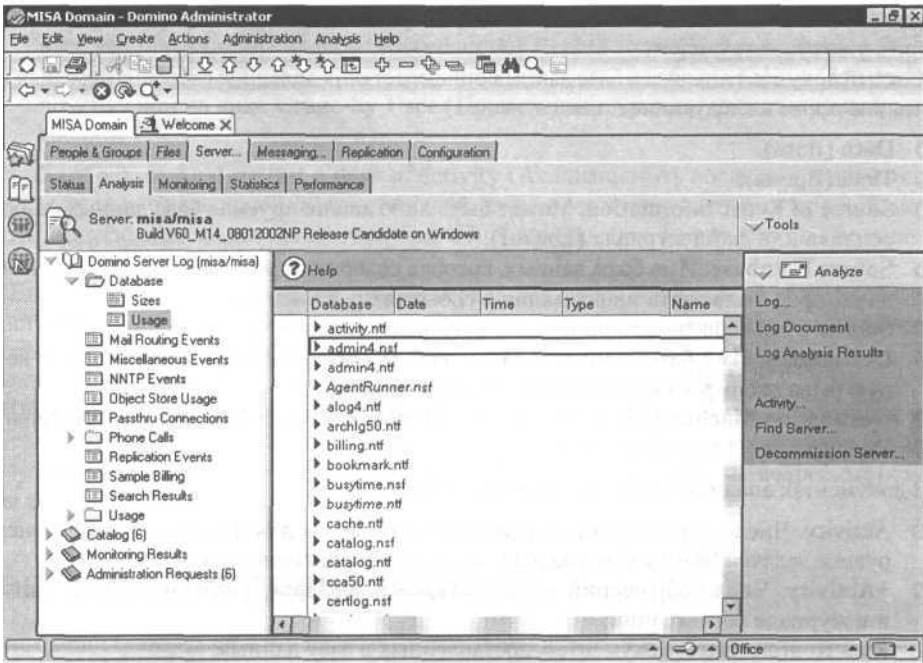


Рис. 14.4. Хотя можно открыть непосредственно файл Log.nsf, чтобы проверить записи журнала регистрации, вся информация доступна также в Domino Administrator. Запись открывается двойным щелчком по ней

будет отменена. Чтобы доступ к сведениям об активности имели лишь пользователи с уровнем доступа минимум **Designer**, установите флажок **Activity is Confidential** (Сведения об активности конфиденциальны).

Анализ базы данных

Для сбора информации об одной или нескольких базах данных запустите анализ базы данных. Собираемая информация включает в себя историю репликации, обращения пользователей для чтения и записи, создания документов, исправления и удаления, изменения оформления, добавления, обновления и удаления при репликации, а также почтовые сообщения, доставляемые почтовым маршрутизатором. Эти сведения добываются из многих источников, помимо самой базы данных, например из журнала репликации, диалогового окна **User Activity** и журнала Notes Log.

Данные, полученные в результате анализа, хранятся в специальной базе, которую следует сформировать перед запуском первого анализа. Она строится на основе шаблона Database Analysis (DBA4.ntf). Несмотря на оставшееся название версии R5 и R6 автоматически обновляют ее файл во время установки. Специалисты Lotus рекомендуют создавать такую базу на локальной рабочей станции, в противном случае необходимо убедиться, что пользователи, которые помещают базы данных на сервере, дают им разные имена. При

проведении анализа можно либо вносить в эту базу данных новую информацию, либо дополнять уже существующую.

Каждый документ анализа в базе данных описывает определенное событие, помещая информацию о нем в следующие поля:

- **Date** (Дата);
- **Time** (Время);
- **Source of Event Information.** Может быть либо анализируемая база данных, либо ее реплика или файл журнала (Log.nsf);
- **Source Database.** Имя базы данных, которая содержит прочитанные документы или из которой была взята информация о событиях репликации;
- **Source.** Имя сервера, хранящего исходную базу данных;
- **Destination.** Имя базы данных, в которой были обновлены документы или в которой была скопирована информация при репликации;
- **Destination Machine.** Имя сервера, на котором хранится база данных назначения;
- **Description** (Описание).

В документах анализа указаны следующие события:

- **Activity.** Число обращений пользователей и серверов для чтения и записи, генерируемое задачей Statlog (см. раздел о мониторинге активности);
- **+Activity.** Число обращений пользователей и серверов, указанное в базе данных и в журнале регистрации;
- **Mail Router.** Число документов, доставленных в базу данных;
- **Data Note.** Операции создания, редактирования и удаления документов;
- **Design Note.** Изменения в списке ACL и макете базы данных;
- **Replicator.** Журнал репликации;
- **+Replicator.** Число добавлений, обновлений и удалений при репликации, как указано в Log.nsf.

При выполнении анализа обратитесь к инструменту Analysis в Domino Administrator. На панели **Server** выберите сервер, на котором находится анализируемая база данных. Щелкните по вкладке **Files** и на одноименной панели отметьте необходимую базу данных. На панели **Tools** укажите раздел **Database**, а затем инструмент Analysis.

Выберите параметры:

- **Changes in: Data documents.** Отображает подробности о создании, редактировании и удалении документов; \$
- **Changes in: Design documents.** Собирает данные об изменениях в списках ACL и любых элементах проектирования баз данных;
- **User Activity: User reads.** Возвращает общее число обращений к документам со стороны пользователей и число обращений для чтения со стороны серверов;
- **User Activity: User writes.** Возвращает общее число обращений пользователей и серверов для создания, редактирования и удаления документов, а также общее число доставленных в базу данных почтовых сообщений;
- **Replication: Find replicas on other server.** Собирает информацию о репликах базы данных, расположенных на других серверах;
- **Replication: Replication history.** Информировать об успешных репликациях базы данных;

- О **In logfile: Miscellaneous Events view.** Перечисляет события, относящиеся к базе данных, как они указаны на виде **Miscellaneous Events** журнала регистрации;
- О **In logfile: Database usage view.** Предоставляет сведения об активности базы данных, помещенной на виде **Usage-by User** (Применение пользователями) журнала регистрации.

Введите в поле **Analyze last n days of activity** (Анализировать последние п дней активности) число п, означающее количество дней, за которое нужно получить отчет об активности. Допускается задать любое число до 99, однако имейте в виду, что чем больше это число, тем дольше продлится анализ.

Щелкните по **Results**. Укажите имя сервера и имя файла базы данных, в которой будут храниться результаты. Если база данных уже существует, щелкните по **Overwrite** (Перезаписать) - и старые данные будут уничтожены, или нажмите **Append** (Дописать) - и новые результаты анализа добавятся к уже имеющимся. Щелкните по **OK**.

Щелкните по **OK** и начните анализ. После окончания анализа откройте базу данных, просмотрите результаты и выберите один из доступных видов. Выведите документ Database Analysis Results (Результаты анализа базы данных), чтобы получить более подробные результаты анализа.

Регистрация транзакций

Регистрация транзакций - это новое средство, появившееся в R5. Когда регистрация включена, все изменения базы данных (такие, как открытие нового документа, добавление текста, сохранение документа) фиксируются и записываются в журнал транзакций. Впоследствии, в случае сбоя жесткого диска, журнал транзакций служит сторонним средством резервирования, с помощью которого можно восстановить базу данных.

Регистрация транзакций записывает обновления баз данных на диск во время высокой нагрузки сервера, что экономит время обработки. Вместо того чтобы помещать обновления в случайно выбранные части диска, транзакции сохраняются последовательно в файлах регистрации, что также уменьшает время обработки. Когда транзакции записаны, сервер Domino может безопасно обрабатывать их или отложить обновления баз данных до тех пор, пока не снизится нагрузка сервера.

Если вы разрешаете регистрацию транзакций, то не нужно обращаться к Fixup для восстановления поврежденных баз данных после сбоя системы. Это значит, что сервер будет быстрее запускаться. Утилита Fixup должна проверить все документы каждой базы данных, а журнал транзакций применяет или отменяет только те транзакции, которые не записаны на диск на момент сбоя.

Кроме того, при включенной регистрации транзакций проще выполнять ежедневное резервирование. Необходимо использовать сторонние утилиты архивирования, которые поддерживаются в версии R5/6, и регистрацию транзакций. Средство резервирования осуществляет ежедневную запись журналов транзакций вместо резервирования целых баз данных (такие средства выпускаются компаниями BEI, Cheyenne/CAI, CommVault, EMC Corporation, IBM, Legato Systems[^] Seagate Software и VERITAS Software).

Регистрация транзакций работает только с базами данных R5/6. Чтобы определить формат базы данных, откройте вкладку **Files** в Domino Administrator. Для баз данных R4 надо обратиться к Fixup.

Установка регистрации транзакций

Регистрируемые базы данных должны находиться в каталоге данных Domino или в одном из его подкаталогов.

Для установки регистрации транзакций откройте окно Domino Administrator. Перейдите на вкладку **Configuration** и выберите имя сервера из раскрывающегося списка **Use Directory on** (Использовать каталог на). Щелчком по **Current Server Document** (Текущий серверный документ) выведите на экран документ. Затем откройте вкладку **Transactional Logging** (Регистрация транзакций) в серверном документе (рис. 14.5). Если вы ее не видите, нажмите стрелку, повернутую вправо, в правом верхнем углу экрана, чтобы появились дополнительные вкладки.

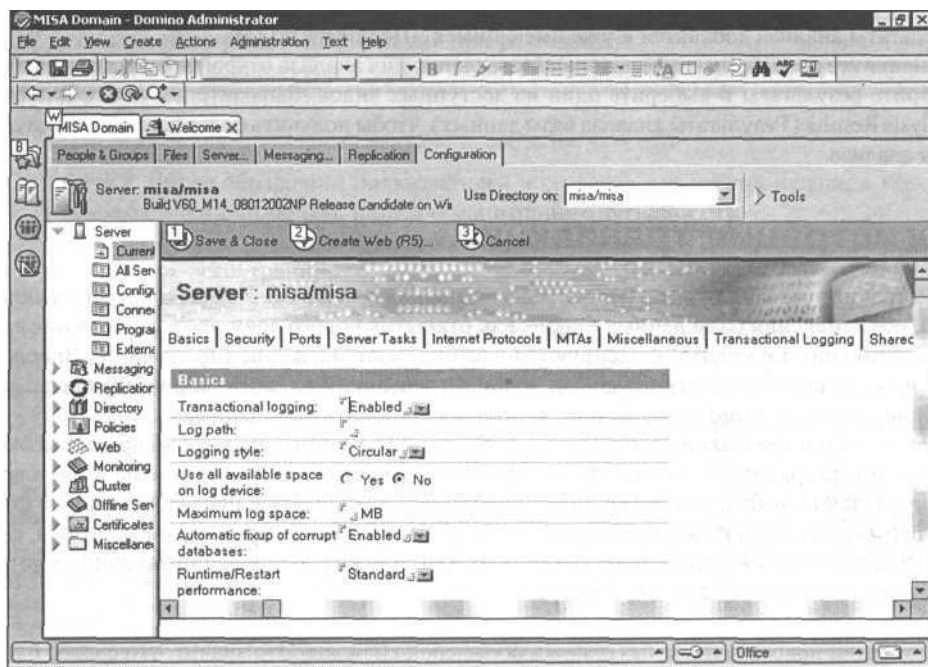


Рис. 14.5. Можно установить размер журнала транзакций минимум 192 Мб, но независимый накопитель, на котором хранится журнал, должно иметь минимум 1 Гб свободного пространства

Щелкните по **Edit Server** (Редактировать серверный документ), заполните необходимые поля (затем щелкните по **OK**, чтобы сохранить документ):

- О **Transactional Logging**. Чтобы включить регистрацию транзакций, задайте **Enabled** (Разрешить). По умолчанию отключено;
- О **Log Path** (Путь к файлу журнала транзакций). По умолчанию журнал хранится в подкаталоге \Logdir в каталоге данных Domino, но делать так не следует. Рекомендуется размещать его на отдельном зеркальном дисковом накопителе, а еще лучше - применить RAID (Redundant Array of Independent Disks - массив независимых

дисковых накопителей с избыточностью) нулевого или первого уровня со специализированным контроллером. Если назначением независимого устройства является только хранение файла журнала, установите для параметра **Use all available space on log device** значение **Yes**;

- О **Use all available space on log device** (Использовать все доступное пространство на устройстве регистрации). Чтобы задействовать все доступное место для хранения файла журнала, выберите **Yes** (log-файл должен размещаться на независимом устройстве). В этом случае можно не задавать значение параметра **Maximum log space**. Чтобы применить значение по умолчанию или определенное параметром **Maximum log space**, укажите **No**;
- О **Maximum log space** (Максимальный размер журнала регистрации). Максимальный размер (в мегабайтах) файла журнала регистрации транзакций. Значение по умолчанию - 192 Мб, максимальное значение - 4 Гб. В зависимости от выделенного размера файла для журнала регистрации Domino создает от 3 до 64 файлов;
- О **Automatic fixup of corrupt databases**. Выберите **Enabled** (Разрешено), чтобы автоматически запускать Fixup, если при обнаружении поврежденной базы данных сервер Domino не в состоянии обратиться к журналу регистрации транзакций для ее восстановления. Domino также назначает DBIID (уникальный идентификатор реплики базы данных) и уведомляет администратора о необходимости восстановления базы данных в максимально короткий срок. Автоматический запуск Fixup отменяется заданием **Disabled** (Отменено). В этом случае Domino просто сообщает администратору, что требуется запустить Fixup с параметром -J для поврежденных зарегистрированных баз данных;
- О **Runtime/Restart performance**. Domino оценивает все активные базы данных, чтобы определить число транзакций, необходимых для восстановления каждой из баз в случае сбоя системы. По окончании оценки Domino создает в журнале регистрации запись контрольной точки восстановления, в которой перечисляются все открытые базы данных и начальная транзакция, необходимая для восстановления. Кроме того, Domino заставляет сохранить изменения базы данных на диске, если это еще не сделано. Формирование контрольных точек восстановления влияет на производительность сервера. Выберите **Standard** (Стандартный режим) - и контрольные точки будут строиться регулярно (установлено по умолчанию, рекомендуется специалистами Lotus). Чтобы сервер Domino делал меньше контрольных точек и, следовательно, освобождал некоторые системные ресурсы сервера для повышения производительности, задайте **Favor runtime** (В предпочтительное время исполнения). Укажите **Favorrestartrecoverytime** (Предпочтительное время запуска восстановления), если надо иметь больше контрольных точек. При этом улучшается производительность при перезапуске, поскольку для восстановления требуется меньшее количество транзакций;
- О **Logging style**. Для повторного обращения к файлу журнала и перезаписи старых транзакций выберите **Circular** (Циклическая регистрация; установлено по умолчанию). Этот режим позволяет восстанавливать только транзакции, сохраненные в журнале транзакций. Назначьте **Archive** (Архивный режим), чтобы к файлам журнала не было доступа до тех пор, пока они архивированы (именно этот вариант советуют специалисты Lotus). Поскольку транзакции могут быть архивированы, когда журнал не работает, файл журнала не всегда содержит нужное число транзакций для

восстановления базы данных. Сторонняя утилита резервирования может скопировать и заархивировать существующий log-файл. Domino увеличивает число в имени файла журнала транзакций, начиная повторно работать с существующим файлом. Однако, когда все файлы журнала становятся недействующими и сархивированными, сервер Domino создает дополнительные log-файлы.

- О **Quota enforcement** в версии R6 позволяет применить квоты к файлу журнала регистрации транзакций.

При необходимости изменить параметры регистрации транзакций сначала создайте резервные реплики всех баз данных. Затем откройте серверный документ и измените требуемые параметры на вкладке **Transactional Logging**.

Отмена регистрации транзакций для одной базы данных

Не рекомендуется отменять регистрацию транзакций ни для одной базы данных, поскольку при последующих сбоях системы придется с помощью утилиты Fixup восстанавливать базу данных. Однако, если все же необходимо запретить регистрацию транзакций для одной базы данных, выполните следующие действия:

- О для создаваемой базы данных выберите **Disable Transaction Logging** (Отменить регистрацию транзакций) в диалоговом окне **Advanced Database Options** (Дополнительные свойства базы данных);
- О для существующей базы данных задайте **Disable Transaction Logging** в диалоговом окне **Advanced Database Options** на вкладке **Advanced** (Дополнительно);
- О укажите на вкладке **Files** в Domino Administrator базу данных, а на панели **Tools - Database => Advanced Properties**. Отметьте **Disable Transaction Logging**;
- О запустите Compact с параметром -t (параметр -T вновь разрешит регистрацию транзакций).

Убедитесь, что все пользователи закрыли базу данных. После этого посредством команды dbcache с параметром очистки (flush) кэш-памяти закройте все базы данных в кэш-памяти (см. раздел об управлении кэш-памятью баз данных). Откройте базу данных.

Если снять флажок **Disable Transaction Logging**, регистрация транзакций снова будет включена.

Восстановление после сбоя системы или сбоя носителя

При сбое системы сервер останавливается и его надо перезапустить. Во время перезапуска сервер Domino автоматически выполняет восстановление базы данных. Если базы были открыты во время сбоя, система использует журналы транзакций для применения и отмены транзакций баз данных, не сохраненных на диске. Fixup работает с базами данных более раннего формата, чем R5, с базами данных, у которых отменена регистрация транзакций или с поврежденными базами данных (при установленном параметре **Automatic fixup of corrupt databases** в серверном документе).

Сбой носителя (например, диска) может вызвать повреждение базы данных вплоть до ее потери. В этом случае для восстановления требуется стороннее средство резервного копирования.

Проблемы регистрации транзакций

Не волнуйтесь, если консоль управления сервером выводит сообщение об ошибке, в котором говорится, что путь к файлу журнала задан неверно или что базы данных требуют восстановления с помощью Fixup. Проверьте путь к log-файлу в серверном документе, и если окажется, что он указан правильно, посмотрите доступ сервера к каталогу. Если и этот путь задан верно и устройство нормально работает, перезапустите сервер и проблема должна быть устранена. Однако если путь описан верно, а устройство не работает, необходимо заменить его и перезапустить сервер. В таком случае сервер создает новые файлы журналов, файлы управления и назначает новые DBIID для каждой базы данных R5/6. Кроме того, при условии, что для параметра **Automatic fixup of corrupt databases** установлено значение **Yes**, запускается Fixup. В самые кратчайшие сроки после выполнения Fixup проведите полное резервирование (резервное копирование) базы данных.

Когда консоль управления сервером выводит сообщение об ошибке, в котором утверждается, что файл журнала поврежден и базы данных требуют восстановления с помощью Fixup, перезапустите сервер. Если сообщение больше не появляется, значит, log-файл не поврежден, а просто произошла ошибка чтения или записи файла журнала. Остановите сервер, чтобы правильно его выключить, произведите полное резервирование и перезагрузите сервер.

Если ошибки появляются снова, возможно, log-файл поврежден. В этом случае следует удалить поврежденный файл журнала и файл управления. В процессе перезагрузки сервера создаются новые log-файл и файл управления и для каждой базы данных R5/6 назначаются новые DBIID. Кроме того, если для параметра **Automatic fixup of corrupt databases** установлено значение **Yes**, запускается Fixup. Сразу же после выполнения Fixup проведите полное резервирование базы данных.

Часто возникающие проблемы восстановления носителя могут быть вызваны повреждением архивного файла журнала. Перезагрузите сервер, затем остановите и правильно выключите его. Перед запуском обратитесь к стороннему средству резервирования для восстановления файлов. Разрешите восстановление резервной базы данных, если архивный log-файл не может быть применен. Выполните полное резервирование базы и перезагрузите сервер.

Поддержка индексов баз данных

В базах данных существуют индексы видов и полнотекстовые индексы. Индексы видов – это объекты внутренней системы заполнения, которые предназначены для построения списков документов на виде или каталоге. Полнотекстовые индексы охватывают содержимое всех документов в базе данных для поиска текстовых строк.

Установка полнотекстовых индексов для поиска в базах данных

Если в базе данных не установлен полнотекстовый индекс, вы не сумеете найти в базе данных слова и фразы. Полнотекстовый индекс можно сделать при создании базы данных или

ее реплики с помощью панели **Search** (Поиск) в базе данных или вкладки **Full Text** (Полнотекстовый индекс) в окне **Database Properties** (Свойства базы данных). Каждый из указанных методов работает только с текущей базой данных. Инструмент Full Text Index (Полнотекстовый индекс) предоставляет возможность формирования и обновления индексов для нескольких баз данных одновременно.

Чтобы создать полнотекстовый индекс инструментом Full Text Index, необходимо иметь уровень доступа к обрабатываемым базам данных как минимум **Designer**.

Сначала в Domino Administrator на панели **Server** выберите сервер, на котором находятся обрабатываемые базы данных. Затем на панели **Files** вкладки **Files** отметьте базы, для которых создается индекс. После этого на панели **Tools** откройте раздел **Database** и задайте **Full Text Index**. Щелкните по **Create**. Установите необходимые параметры настройки индекса и щелкните по **OK**.

Параметры индекса определяют точность и скорость поиска в базе данных. Некоторые параметры влияют на размер базы данных, поскольку увеличивают размер индекса, который хранится в самой базе:

- **Index attached files with found text** (Включать в индекс вложенные файлы с поиском текста). Чтобы создать указатель для любого текстового файла ASCII, вложенного в базу данных, укажите этот режим, обеспечивающий более быстрый, но менее полный поиск, чем с помощью фильтров файлов. Добавление вложений в индекс увеличивает размер файла базы данных. Насколько значительным будет это увеличение, зависит от размера и количества вложений;
- **Index attached files with file filters** (Включать в индекс вложенные файлы с фильтрами файлов). Создает индекс для всего двоичного содержимого вложений. Хотя поиск работает медленнее, чем в варианте «с поиском текста», формируется более полный (и больший по размерам) индекс;
- **Index encrypted fields** (Включать в индексы зашифрованные поля). Увеличивает размер указателя в зависимости от объема текста в зашифрованных полях, что может вызвать проблемы информационной безопасности. Любой пользователь в состоянии найти слово или предложение, содержащиеся в зашифрованных полях, и увидеть список документов, в которые они включены, даже если само поле прочитать нельзя. Более того, если индекс не закодирован и может быть прочитан любым сотрудником, имеющим доступ к серверу, то пользователю не составит труда ознакомиться с текстом, который изначально был зашифрован. Ключ шифрования, являющийся частью ID-файла сервера, действует для всех баз данных этого сервера. Работая в описанном режиме, вы подвергаете риску все поля, зашифрованные с помощью такого ключа;
- **Index sentence and paragraph breaks** (Включать в индекс предложения и разрыв абзаца). Индекс кроме знаков конца слова включает в себя предложения и знаки разрыва абзаца, что увеличивает его размер;
- **Enable case sensitive searches** (Разрешить поиск с учетом регистра). При выборе этого режима очень сильно возрастает размер индекса, поскольку в него должны входить все варианты одного и того же слова с учетом регистра;
- **Index update frequency** (Частота обновления индекса). Индекс обновляется ежедневно во время работы задачи Updall на сервере в 2 часа утра (по умолчанию). Планирование обновлений основывается на документе программы для задачи Updall

(необходимо настроить документ программы для Updall в каталоге Domino). Ежечасные обновления, как следует из названия, совершаются каждый час. Немедленное обновление происходит сразу после закрытия базы данных. Выбранный вариант влияет на производительность сервера. При ежечасном или немедленном обновлении проследите за производительностью сервера и базы данных. Если она окажется низкой, уменьшите частоту обновлений.

С помощью инструмента Full Text Index обновляются или удаляются индексы сразу для нескольких выбранных баз данных. Укажите **Update** или **Delete** в зависимости от нужного вам действия и щелкните по ОК.

Использование задачи Update

Задача Update стартует при запуске сервера и затем работает постоянно. Ее цель - своевременное обновление видов. При изменении папки или вида все модификации и требующиеся обновления заносятся в очередь Update. По прошествии порядка 15 минут Update обновляет все индексы базы данных. После этого обновляются все базы данных с полнотекстовыми индексами, для которых установлено немедленное или ежечасное обновление.

Обнаружив поврежденный индекс вида или некорректный полнотекстовый индекс, Update удаляет его и затем строит заново.

Если позволяет производительность сервера, разрешается запускать несколько задач Update. В общем случае этого не следует делать на однопроцессорных компьютерах, а для многопроцессорной машины разрешается назначить по одной задаче Update на каждый процессор.

Чтобы активизировать несколько задач Update, создайте документ конфигурации. Щелкните по вкладке **Configuration** в окне Domino Administrator и из раскрывающегося списка **Use Directory on** выберите сервер. Отметьте **Server => Configurations** (Сервер => Конфигурации). Если такой документ уже существует, выделите его и щелкните по **Edit** (Редактировать). Для создания нового документа щелкните по **Add Configuration** (Добавить конфигурацию).

Откройте вкладку **NOTES.INI Settings** (Параметры настройки notes.ini) и щелкните по кнопке **Set/Modify Parameters** (Установить/изменить параметры). В поле **Item** (Элемент) задайте **Updaters** (Программы обновления). Введите число запускаемых задач Update в поле **Value** (Значение). Щелкните по ОК, затем по **Save and Close** (Сохранить и закрыть). Перезапустите сервер, чтобы вступили в силу новые параметры настройки.

Запуск Updall

Задача Updall заново строит все поврежденные индексы видов и полнотекстовые индексы, которые находит. Она не работает постоянно, а запускается ежедневно в 2 часа утра (по умолчанию). Кроме того, Updall вычищает остатки после удаления и избавляется от ненужных индексов видов (если индекс не используется в течение 45 дней). Для изменения временного интервала удаления таких индексов установите параметр **Default_Index_Lifetime_Days** в файле notes.ini.

Хотя Updall стартует ежедневно, ее можно запустить по требованию при необходимости очистить поврежденный индекс. Updall запускается одним из трех способов:

- О инструментом **Task => Start** (Задача => Запуск). В Domino Administrator выберите сервер, на котором должна работать задача Updall. Щелкните по вкладке **Server** и отметьте **Status**. На панели **Tools** укажите **Task** и затем **Start**. В списке задач выделите **Update all**. Задайте **Show advanced options** (Показать дополнительные параметры), чтобы настроить параметры работы Updall (необязательно). Щелкните по **Start Task** (Запустить задачу);
- О командой с консоли управления. Введите команду Load Updall path options непосредственно на консоли сервера или в Domino Administrator, укажите сервер, щелкните по вкладке **Server**, отметьте **Status**, затем щелкните по **Console**, задайте команду и нажмите клавишу **Enter**. Параметры командной строки для Updall описаны в табл. 14.5;
- О посредством документа программы (Program document). Щелкните по вкладке **Configuration** в Domino Administrator. В раскрывающемся списке **Use Directory on** отметьте сервер, на котором хранится редактируемая реплика каталога Domino. Щелкните по **Server**, чтобы открыть категорию, выберите **Program** (Программа) и укажите **Add Program** (Добавить программу). На вкладке **Basics** введите имя программы (Updall), командную строку (любые допустимые параметры) и сервер, на котором следует запустить эту задачу. Щелкните по вкладке **Schedule** (Расписание) и внесите информацию о планировании запуска. Щелкните по **Save and Close** (Сохранить и закрыть).

Таблица 14.5. Параметры командной строки для задачи Updall

Параметр	Описание
база^анных -С	Заново компонует неиспользуемые индексы видов и полнотекстовые индексы в базе данных. Необходимо указать базу данных
база_данных путь	Обновляет только определенную базу данных. Чтобы задать базы в какой-либо папке, определите путь к базе данных относительно каталога данных Domino
база^анных -Т название_вида	Обновляет конфетный вид в базе данных
-F	Обновляет полнотекстовые индексы, но не виды
-H	Обновляет полнотекстовые индексы, для которых установлена частота обновления «немедленно»
-L	Обновляет полнотекстовые индексы, для которых установлена частота обновления «немедленно», «ежедневно» или «ежечасно»
-M	Обновляет полнотекстовые индексы, для которых установлена частота обновления «немедленно» или «ежечасно»
-R	Заново компонует полнотекстовые индексы и все используемые виды. Этот режим требует значительных ресурсов, поэтому к нему следует обращаться только как к последнему средству решения проблем с повреждением индексов
-V	* Обновляет вид, но не полнотекстовые индексы
-X	Заново компонует полнотекстовые индексы и не трогает виды. Применяется для перекомпоновки вычисляемых полнотекстовых индексов

Запуск с клавиатуры

Задачи Update и Updall служат для обновления и восстановления баз данных, но что должен делать пользователь, если вид не открывается или выводит неверные документы? Существует три комбинации клавиш, которые может применить пользователь для очистки вида (кстати, они работают и на сервере):

- клавиша F9 обновляет текущий вид, позволяет просматривать изменения, произошедшие на виде с момента его открытия;
- клавиатурная комбинация **Shift+F9** заново компоует текущий вид, чтобы устранить любые проблемы;
- клавиатурная комбинация **Ctrl+Shift+F9** заново компоует все нескомпонованные виды в базе данных и обновляет все остальные виды. Применяется, когда невозможно запустить Updall.

Администрирование каталога баз данных

Каталог баз данных - это база данных, которая является централизованным списком всех баз организации, кроме почтовых. Виды в каталоге перечисляют все базы данных по категориям, владельцам, идентификаторам реплики, серверам и названиям. Каждая база имеет документ, содержащий имя сервера, имя файла, ID-файл реплики и имена любых серверов, групп или пользователей, обладающих доступом на уровне **Manager** к этой базе. Та же информация включена в документ About This Database (О базе данных) текущей базы. В любом документе есть набор кнопок, которые позволяют пользователю открывать и просматривать базу данных, а также добавлять ее в свои закладки.

Задача Catalog запускается ежедневно в 1 час утра по умолчанию на всех серверах и создает или обновляет каталог баз данных. Таким образом, когда какая-либо база переносится на другой сервер, соответствующая запись в каталоге обновляется в течение 24 часов.

Для заполнения каталога служит команда Load Catalog, вводимая с консоли сервера. Чтобы просмотреть документы в каталоге, следует открыть его с помощью ярлыков в Domino Administrator или инструментом Web Administrator.

Создание каталога баз данных

Формируя каталог баз данных, вы автоматически получаете доступ **Manager** к этой базе. После ее создания необходимо установить соответствующий доступ для администраторов, пользователей и групп. Присвойте базам данных категории, чтобы управлять их отображением в каталоге. Реплицируйте каталог на необходимое количество серверов. Вы также должны отслеживать размер каталога.

Для создания каталога баз данных выполните **File => Database => New** (Файл => База данных => Создать). Выберите имя сервера, на котором будет храниться каталог, введите его название (**Title**) и имя файла (**File Name**). Отметьте **Show Advanced Templates** (Показать дополнительные шаблоны). Щелкните по кнопке **Template Server** (Сервер с шаблонами), если после нее появляется надпись **Local** (Локально), и укажите сервер, содержащий шаблоны баз данных. Выделите шаблон каталога баз данных (CATALOG.NTF) в списке шаблонов и щелкните по ОК.

Настройка списка ACL

Щелкните правой кнопкой мыши по значку каталога баз данных и выберите **Database => Access Control** (База данных => Управление доступом). В списке ACL каталога баз данных отметьте доступ **Manager** для себя (должно быть уже установлено) и всех пользователей, которые имеют право изменять ACL, например для владельца базы данных. Установите уровень доступа **Manager** всем серверам, которые будут хранить каталог баз данных или его реплики. Доступ по умолчанию укажите равным **Reader**.

Назначение категорий

Каждой базе данных в каталоге можно присвоить одну или несколько категорий. Категории определяют порядок группировки на виде **Databases by Category** (Базы данных по категориям) - рис. 14.6. Если категории не установлены, данный вид будет пустым.

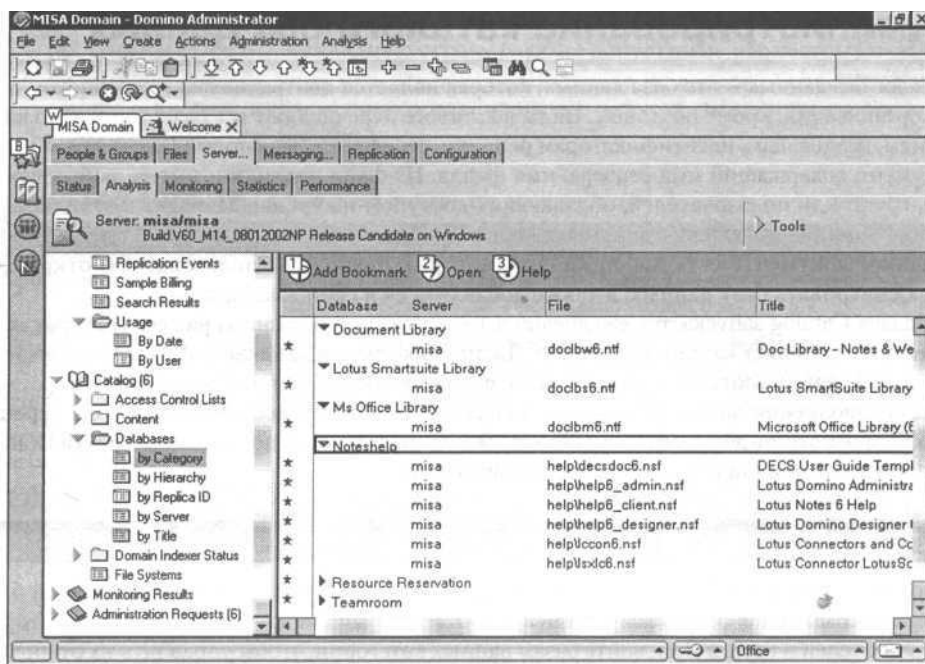


Рис. 14.6. Эти категории установлены для баз данных по умолчанию

Пользователь, назначающий категории, должен обладать минимальным уровнем доступа **Designer** к базе данных. Категории указываются по очереди для каждой из баз. Щелкните правой кнопкой мыши по значку базы данных и выберите **Database => Properties**. Откроется диалоговое окно **Database Properties** (Свойства базы данных). На вкладке **Design** (Дизайн) в этом окне выберите **List** (Список) в **Database Category** (Категория базы данных). В поле **Category** (Категория) перечислите все категории для текущей базы данных, разделяя их запятыми.

Повторите описанные действия для всех баз данных в каталоге. Необходимо отслеживать имена категорий баз данных, чтобы одинаковым базам присваивались равные категории. В этом случае вид **Databases by Category** будет правильно группировать одинаковые базы данных.

Сокращение размера каталога баз данных

Каталог баз данных может вырасти до огромных размеров, если не следить за ним. Это особенно важно, когда каталог реплицируется на другие серверы. Не исключено, что придется формировать отдельные каталоги баз данных для разных серверов, если наличие одного каталога приводит к проблеме со свободным дисковым пространством на каком-либо сервере.

Одним из способов сокращения размера каталога является удаление из него баз, в которых нет необходимости.

Кроме того допускается введение параметра -р для команды Catalog, исключающей из каталога список документов **Policy** (Политика). Поскольку программа Catalog запускается ежедневно, можно установить переменную ServerTaskAtl=Catalog -P в файле notes.ini.

К сожалению, это не действует для уже существующих документов политики (Policy document). Необходимо удалить текущий каталог, а затем вновь создать его с помощью команды Load Catalog -P.

Удаление базы данных из каталога

Хотя базы автоматически заносятся в каталог, можно удалить конкретную базу данных из него, сняв флажок **List in Database Catalog** (Показывать в каталоге баз данных) на вкладке **Design** окна **Database Properties**. Чтобы установить это свойство, требуется минимальный уровень доступа **Designer**.

Поиск в домене

Традиционно для организации поиска нужных документов пользователи должны иметь возможность просматривать базы данных с полнотекстовыми индексами. Поиск в домене расширяет эту функцию и позволяет исследовать все базы данных внутри одного домена.

Процесс поиска в домене делится на несколько частей, но начинается на сервере каталога домена, который обслуживает процесс централизованного администрирования поиска в домене. Каталог домена устанавливает, какие базы данных и файловые системы должны быть включены в индекс, а также управляет фильтрацией результатов для пользователей с различным доступом к базам данных и файловым системам. Средство Domain Indexer (Индексатор домена) строит центральный индекс, к которому обращаются все запросы.

Сервер каталога домена

Создание индексов и обработка запросов пользователей требует немного ресурсов, но сервер каталога домена должен быть способен выполнять эти задачи - быть быстрым и мощным, а также располагать достаточным свободным дисковым пространством.

В качестве сервера каталога домена в среде Windows NT компания Lotus рекомендует процессор минимум Intel Pentium Ц с тактовой частотой 266 МГц, 256 Мб ОЗУ и свободное

дисковое пространство, равное приблизительно 75% от общего размера индексируемого домена. Несколько процессоров, большие объемы ОЗУ и несколько дисков большого размера увеличивают эффективность и возможности поиска.

Если в домене шесть или более серверов Domino, стоит подумать о выделении сервера для индексирования и поиска в домене или об объединении серверов в кластеры для увеличения надежности, отказоустойчивости и распределения запросов пользователей.

Для настройки сервера каталога домена:

1. На панели **Server** в программе Domino Administrator выберите сервер, который выделяется в качестве сервера каталога домена.
2. Щелкните по вкладке **Configuration** (Конфигурация).
3. На панели **View** (Вид) раскройте значок **Server** (Сервер) и выберите **All Server Documents** (Все серверные документы).
4. Укажите серверный документ для сервера каталога домена. Задайте **Edit Server** (Редактировать сервер).
5. Щелкните по вкладке **Server Tasks** (Задачи сервера) и затем отметьте **Domain Indexer** (Индексатор домена).
6. В поле **Domain wide indexer** (Индексатор в рамках домена) установите значение **Enabled** (Разрешить).
7. Введите или выберите параметры расписания индексирования. Назначив частое индексирование, вы получите более точный индекс, но при этом индексирование потребует больше ресурсов. После проведения индексирования в течение определенного промежутка времени поэкспериментируйте с разной его частотой. Можно начать с 60 минут.
8. В поле **Limit domain wide searching to the following servers** (Ограничить поиск в домене следующими серверами) выберите серверы, которые будут включены в индекс. Если поле остается пустым, в индекс вносятся все серверы. При необходимости определите конкретные серверы посредством подстановочных символов (* /Servers/Stillwater).
9. Щелкните по кнопке **Save and Close** (Сохранить и закрыть).
10. На консоли сервера введите команду Load Catalog, чтобы запустить процесс каталога домена и в следующий запланированный момент времени выполнить задачу Domain Indexer.

Каталог домена

Каталог домена, основанный на шаблоне базы данных Catalog.ntf (как и каталог баз данных), хранит записи, которые отображают, какие базы данных и файловые системы сервер должен заносить в индекс и к каким формам необходимо обращаться для поиска в индексе. Сам индекс располагается на сервере каталога домена.

Каталог домена создается с помощью команды Load Catalog с консоли сервера при условии, что уже установлено средство Domain Indexer.

Настройка индексации файловой системы

Чтобы задать, какие файловые системы следует включить в поиск по домену, создайте для каждого сервера домена документ файловой системы. Любая файловая система может

войти в индекс при условии, что службы файловой системы в операционной системе, в которой работает сервер Domino, имеют доступ к этой файловой системе. Сервер каталога домена надо настроить как Web-сервер Domino, чтобы он был в состоянии возвращать ссылки на документы в файловых системах в качестве откликов на запросы клиента Notes и Web-клиентов.

Если вы планируете включить в индекс каталог, который не является частью каталога данных Domino, создайте ссылку на каталог или документ отображения/перенаправления (в документе конфигурации Web-сервера - Web Server Configurations).

Для установки списка файловых систем выполните следующие действия:

1. В Domino Administrator или на рабочей станции Notes выберите **File => Database => Open** (Файл => База данных => Открыть).
2. Укажите имя сервера каталога домена в поле **Server** и щелкните по **Open**.
3. Задайте **File => Create System** (Файл => Создать систему).
4. Отметьте имя сервера и щелкните по **Set/Modify File System List** (Установить/изменить список файловых систем).
5. В поле **File system** введите физическое место расположения файловой системы (укажите полный путь, кроме случаев, когда путь задан относительно каталога данных Domino, или путь URL).
6. Нажмите **Next** (Далее), чтобы добавить файловую систему в список.
7. Повторите шаги 3-5 для других файловых систем.
8. После заполнения списка щелкните по **OK**, затем по **Save and Close** (Сохранить и закрыть).
9. Перезагрузите сервер.

Настройка потоков

Каждый поток индексирования единоновременно вносит в индекс только один информационный репозиторий. При увеличении числа потоков индексирования сервер каталога домена может одновременно помещать в индекс большее число таких архивов, однако потребуются увеличение мощности процессора и, возможно, произойдет замедление откликов на запросы. При меньшем числе потоков поиск ускоряется, остается больше свободных ресурсов. Отрицательная сторона состоит в том, что изменения будут медленнее отражаться в индексе.

По умолчанию для одного процессора назначается два потока индексирования. Чтобы увеличить число потоков, задайте для переменной **FT_DOMAIN_IDXTHDS** в файле **notes.ini** большее значение, но не более восьми потоков на процессор, иначе очень сильно снизится производительность сервера, даже если у вас двухпроцессорный компьютер.

Включение базы данных в индекс домена

Использование инструмента Multi-Database Index (Индекс для нескольких баз данных) является важной составной частью построения индекса поиска в домене.

Необходимо иметь доступ **Manager** к каждой базе данных, которые нужно поместить в индекс. Чтобы задать индексирование для отдельной базы данных, установите флажок **Include in multi-database indexing** (Включить в индексирование несколько баз данных) на вкладке **Design** (Дизайн) диалогового окна **Database Properties** (Свойства базы данных).

Для назначения индексирования нескольких баз данных перейдите в программу Domino Administrator. На панели **Server** определите сервер, где находятся базы. Щелкните по вкладке **Files** и на одноименной панели укажите базы данных, которые должны войти в индекс. На панели **Tools** отметьте **Database** и затем **Multi-Database Index** (Индекс нескольких баз данных). Выберите свойство **Enabled** (Разрешено) и щелкните по ОК.

Индексатор домена Domain Indexer работает в соответствии с расписанием, установленным в серверном документе. Он просматривает каталог домена на предмет наличия новых баз данных, для которых включено свойство **Include in multi-database indexing**, а также ищет в существующих базах данных и файловых системах документы и файлы, добавленные или измененные с момента последнего запуска индексатора. Все найденное вносится в индекс домена.

Библиотеки баз данных

Библиотеки баз данных помогают группам пользователей находить необходимые базы или взаимодействовать с ними, не прибегая к поиску в диалоговом окне **Open Database** (Открыть базу данных). Интересующие базы данных заносятся в библиотеку, а главный вид библиотеки содержит алфавитный список всех этих баз и краткое резюме о каждой из них. Любой документ базы данных в библиотеке имеет имя, резюме, идентификатор реплики базы плюс имя владельца базы. Есть также кнопки, которые позволяют пользователю просматривать базу данных, открывать или создавать для нее ярлык на своей рабочей станции.

Библиотеки располагаются на сервере (хотя допускается создать локальную библиотеку для собственных нужд), и сервер может обладать одной или несколькими библиотеками. При обращении пользователя к базе данных в библиотеке сервер Domino находит ее по файлу идентификационных данных реплики и открывает. Domino сначала ищет ее на рабочей станции пользователя, затем на локальном сервере и, наконец, в каталоге баз данных локального сервера, чтобы указать путь к реплике.

Создавая библиотеку, вы становитесь библиотекарем, и в списке ACL для вас назначается уровень доступа **Manager**. По умолчанию установлен доступ **Author**. Пользователи с доступом **Author** могут заносить базы данных в библиотеку. Если пользователь с доступом **Reader** пытается внести библиотеку в базу данных, Domino отправляет запрос пользователя библиотекарю по электронной почте. После этого библиотекарь заполняет библиотеку.

Создание библиотеки

Для создания библиотеки на сервере требуется право **Create New Databases** (Создание новой базы данных). Необходимо выполнить такие действия:

1. На рабочей станции Notes выбрать **File => Database => New** (Файл => База данных => Создать).
2. В поле **Server** указать имя сервера, на котором нужно сформировать библиотеку.
3. Ввести имя файла библиотеки.
4. Щелкнуть по **Show Advanced Templates** (Показать дополнительные шаблоны).

5. Отметить шаблон **Database Library** (DBLIB4.NTF) в списке шаблонов. Если этот шаблон не виден, надо щелкнуть по кнопке **Template Server** (Сервер шаблона) и задать сервер, на котором есть дополнительные шаблоны.
6. Щелкнуть по ОК.

Назначение библиотекарей

Чтобы назначать библиотекарей, необходимо обладать уровнем доступа не менее **Editor** (Редактор) для списка ACL библиотеки. Библиотекари, которых вы назначаете, должны иметь уровень доступа не менее **Author**. Сделайте следующее:

1. Выберите библиотеку баз данных среди своих ярлыков.
2. Задайте **View => Go To => Librarians** (Вид => Перейти => Библиотекари).
3. Откройте документ библиотекарей (Librarians document) в режиме редактирования.
4. Введите имена пользователей, которые будут библиотекарями. Между именами автоматически добавляются точки с запятыми при сохранении документа.
5. Сохраните и закройте документ.

Публикация базы данных

При добавлении базы данных в библиотеку вы публикуете ее для доступа всем пользователям. Чтобы опубликовать базу данных, нужно иметь к ней доступ **Author** и совершить следующие действия:

1. Выбрать среди своих ярлыков значок необходимой базы.
2. Задать **File => Database => Publish** (Файл => База данных => Публиковать).
3. В списке **Available Libraries** (Доступные библиотеки) отметить библиотеку, с которой планируется работать. Щелкнуть по ОК.
4. Ввести краткое описание базы данных в поле **Abstract** (Цели). Это поле служит названием, которое отображается на виде.
5. В поле **Long Description** (Полное описание) поместить более подробное описание содержимого базы.
6. Сохранить и закрыть документ.

Управление кэш-памятью баз данных ->

Каждый сервер поддерживает кэш-память баз данных. Закрытая база данных помещается в кэш, когда ни пользователи, ни процессы ее не применяют. Это ускоряет закрытие. Она остается в кэш-памяти либо до момента ее открытия, либо на 15-20 минут.

Одновременно в кэш-памяти хранится более 25 баз данных или же их число равно значению переменной `NSF_Buffer_Pool_Size` в файле `notes.ini`, деленному на 300 Кб. Чтобы изменить указанное число, увеличьте значение переменной `NSF_DbCache_Maxentries` в файле `notes.ini`. Вместо этого можно добавить физическую память в компьютере.

Если нужно просмотреть базы данных, находящиеся в кэш-памяти, введите на консоли сервера команду `dbcache show`. Закройте базу в кэш-памяти с помощью консольной команды `dbcache flush`.

Для отключения кэш-памяти баз данных запишите в файле `notes.ini` строку `NSF_DbCache_Disable=1`.

Как узнать, когда требуется изменить параметры или вводить команды? Необходимо контролировать кэш-память базы данных, просматривая кэш-статистику. Можно набрать команду `show stat database.dbcache`. * на консоли сервера или просмотреть **Database Statistics** (Статистика базы данных) - рис. 14.7.

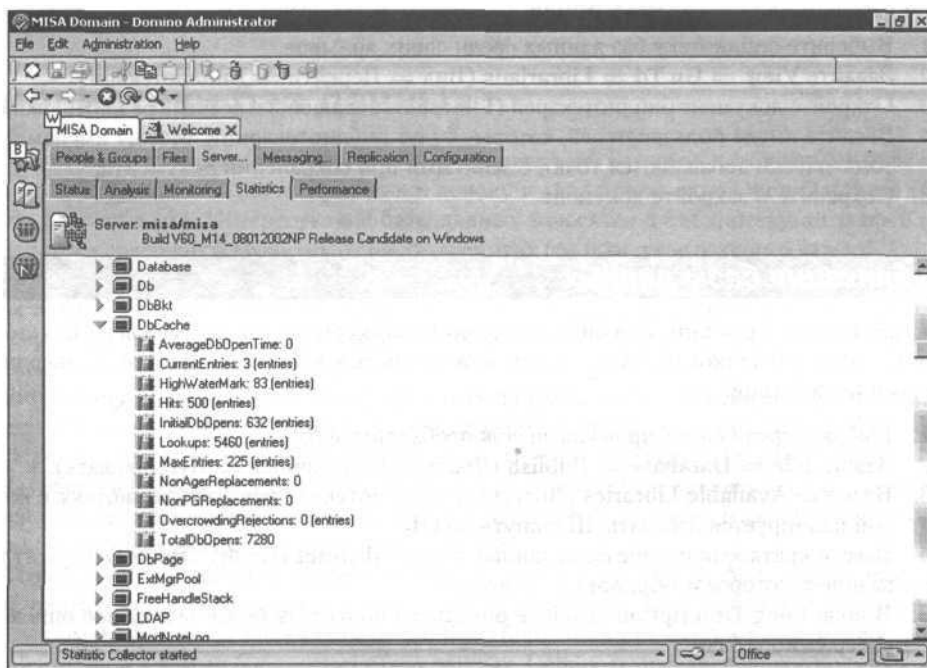


Рис. 14.7. Чтобы просмотреть статистику кэширования базы данных, выберите сервер, щелкните по вкладке **Server**, отметьте вкладку **Statistics** и раскройте категорию **Qrptbase**

Выведите на экран **DbCache**, если надо проверить статистику для кэш-памяти. Доступны следующие параметры:

- О **CurrentEntries**. Число баз данных, находящихся в кэш-памяти. Если это число часто приближается к значению **MaxEntries**, увеличьте количество баз, которые могут храниться в кэш-памяти;
- О **HighWaterMark**. Максимальное число баз данных в кэше в течение работы серверной программы. Это, не точный индикатор производительности кэш-памяти, поскольку число может быть искусственно завышенным из-за работы сервера при запуске;

- О **Hits**. Показывает, сколько раз InitialDbOpen обнаруживает базу данных в кэш-памяти. Кэш-память работает эффективно, когда число совпадений намного превышает число открытий базы данных. Если это не так, может понадобиться увеличить число баз, которые способна хранить кэш-память;
- О **InitialDbOpens**. Сообщает, сколько раз пользователи или серверы открывают базу данных, с которой на данный момент не работают другие пользователи или серверы;
- О **Lookups**. Число обращений к кэш-памяти баз данных. Высокое отношение числа совпадений к числу обращений означает эффективную работу кэш-памяти, а при низком отношении необходимо увеличить количество хранящихся в кэш-памяти баз;
- О **MaxEntries**. Число баз данных, которое в состоянии хранить сервер в кэш-памяти одновременно;
- О **OvercrowdingRejections**. Информировывает, сколько раз базу данных не удалось поместить в кэш-память, так как значение **CurrentEntries** равно или превосходит значение **MaxEntries** в 1,5 раза. Обычно это число мало. Если оно возрастает, увеличьте количество баз данных, которые могут храниться в кэш-памяти;
- О в версии R6 дополнительно выводятся значения параметров **AverageDbOpenTime** (Среднее время открытия базы данных), **NonAgerReplacements** (Неустаревшие замены), **NonPGReplacements** (Не-PG замены) и **TotalDbOpens** (Общее число открытий базы данных), которые, к сожалению, не описаны в документации.

Хотя многие проблемы устранения неполадок удастся решить с помощью инструментов, рассмотренных в этой главе, всегда возникают новые. Ответы на вопросы можно найти на сайте <http://www.support.lotus.com>. Полезная информация содержится также на сайтах <http://www.notes.net>, <http://www.lotus411.com> (на данный момент это сайт с советами по программированию, но будут добавлены рекомендации по системному администрированию) или <http://www.iris.com>.

•

ГЛАВА

15

УСТАНОВКА WEB-СЕРВЕРА, ПОДДЕРЖКА, НАСТРОЙКА И УСТРАНЕНИЕ НЕПОЛАДОК

Как известно, сервер Domino не имеет себе равных среди почтовых серверов, а также выделяется на общем фоне как серверная платформа для приложений. Менее известно, что он поддерживает устойчивый, гибкий, защищенный, масштабируемый и наращиваемый Web-сервер. Впервые HTTP-сервер для Domino был представлен только в версии R4.5, но, постепенно улучшаясь, он к настоящему времени стал одной из наиболее мощных и гибких платформ HTTP-серверов на рынке программных продуктов. В этой главе подробно рассматривается, как установить, настроить, оптимизировать, администрировать HTTP-сервер Domino и как устранять неисправности.

Новые функции HTTP-сервера Domino R5

Ниже описаны новые возможности этого сервера в версии R5:

- усовершенствованный HTTP-стек. Служба HTTP имеет много улучшений, включая большую производительность, защиту файловых систем и более надежную серверную поддержку;
- управление доступом для файловой системы Domino. Можно настраивать списки управления доступом (ACL) для файлов (HTML, WAW, GIF и т.д.), обслуживаемых файловой системой Domino;
- автоматическая оптимизация HTTP-сервера. Domino в состоянии автоматически настраивать различные параметры сервера на основании типов запускаемых Web-приложений;
- побайтная передача. В версии R5 допускается, чтобы Web-клиенты загружали файлы не огромными кусками, а небольшими частями, что ускоряет загрузку и делает ее более помехоустойчивой. Это означает, что, если соединение с сервером нарушено, пользователь может возобновить загрузку файла с того места, на котором она была прервана, вместо того, чтобы загружать файл заново;
- определение возможностей браузера. Посредством функции на языке формул ©BrouserInfo легко установить, какой Web-браузер работает на сервере, что упрощает адаптацию Web-приложений для данного программного сервера. До R5 это делалось с помощью CGI-переменных либо сценариев на клиентской стороне;

- О простые URL-адреса. Domino R5 позволяет присваивать уникальные имена страниц без применения уникальных идентификаторов. В результате появляются простые адреса URL, например www.definity.com/hatter.nsf/VoteGOP7OpenPage, где VoteGOP - имя страницы. В случае конкретного имени возможно еще большее упрощение URL, например www.acme.com/News.nsf/VoteGOP;
- О поддержка технологий CORBA/IIOP, а именно Common Object Request Broker Architecture (Архитектура брокера общих объектных запросов) и Internet InterORB Protocol (Протокол межброкерных объектных запросов);
- О Domino для Microsoft IIS. Microsoft Internet Information Server (IIS - информационный сервер Internet) теперь может использоваться как HTTP-сервер при работе с информационным содержимым сервера Domino. Благодаря этому потребители накапливают опыт и умение, продолжая применять удобные средства Domino;
- О менеджер кластеров Internet. Возможности кластеризации, выравнивания нагрузки и обработки сбоев применяются и для Web-браузеров, обращающихся к Web-серверу Domino;
- О аутентификация HTTP-сеанса. R5 предусматривает аутентификацию с помощью HTTP-сеансов и зашифрованных файлов cookie. Это облегчает подключение к сайту, обслуживаемому сервером Domino, и отключение от него;
- О поддержка виртуальных SSL серверов и ключей. Для каждого виртуального сервера может быть определен уникальный ключ, позволяющий виртуальному серверу обращаться к протоколу SSL. Кроме того, для любого виртуального сервера разрешается установить параметры защиты порта;
- О усовершенствованная поддержка сервлетов. Web-сервер Domino поддерживает серверные сценарии по спецификации JSDK 2.0;
- О улучшенное управление файлом журнала. В R5 можно установить период времени, в течение которого применяется log-файл: ежедневно, еженедельно или ежемесячно;
- О последний измененный заголовок HTTP. Domino R5 в состоянии отправлять вместе с ответами последний заголовок HTTP;
- О Domino Web Server API (DSAPI - прикладные интерфейсы API для Web-сервера Domino). Domino поддерживает API-функции сервера, что дает возможность пользователям, владеющим программированием, создавать собственные серверные расширения Web;
- О интеграция в масштабе предприятий. DECS (Domino Enterprise Connection Services - корпоративная служба соединения Domino) - это визуальный инструмент и высокопроизводительная среда сервера, которая позволяет пользователям создавать Web-приложения с реальным, естественным доступом к данным и приложениям в масштабе предприятия.

Новые функции HTTP-сервера Domino R6

В версии R6 появились следующие нововведения:

- О по умолчанию разрешен режим регистрации файлов cookie, что порождает новую серверную задачу в среде Windows NT и Windows 2000. Данные из этих файлов записываются в журнале регистрации перед текстовыми сообщениями;
- О заголовок ответов HTTP определяет новый тип правил для Web-сайта на виде **Domino Directory Server\Internet Sites** (Сервер каталога Domino/сайт сети Internet). Данное

правило позволяет добавить в ответ HTTP заголовок **Expires** (Истечение срока действия) или пользовательский заголовок, причем добавление осуществляется согласно установленным шаблонам на адрес URL или на код ответа;

- О реализована функция разового входа SSO (Single Sign-On) для Web-браузеров, обращающихся к Web-серверу Domino и Web-серверу WebSphere. Более того, обеспечен разовый вход на любой сервер домена Domino, поддерживающий функцию SSO. Допустимо создание нескольких документов Web-конфигурации для SSO (Web SSO Configuration) в каталоге Domino Directory или домене.

Обзор стека HTTP сервера Domino

Выше представлен краткий обзор нескольких новых средств, которые помогают сделать и без того достаточно популярный продукт еще лучше. В настоящем разделе описано, как работает HTTP-сервер Domino.

Почему Domino используется как HTTP-сервер

Система Domino уже давно известна как устойчивая, защищенная и масштабируемая система передачи сообщений коллективного использования. После добавления новых улучшенных средств в версии R5 и R6 Domino получила широкое распространение в качестве очень мощного и защищенного сервера Web-приложений.

Одна из основных причин, которые делают Domino такой превосходной платформой для Web-приложений, состоит в том, что система работает как стандартный HTTP-сервер, имеет возможность обслуживать статические HTML-файлы и, что более важно, в состоянии динамически преобразовывать содержимое баз данных Notes в Web-страницы.

Эта способность означает, что любые приложения, такие как приложения локальных сетей, корпоративных сетей и Internet-приложения, быстро перестраиваются для установки как на рабочих станциях Notes, так и в Web-браузере. Web-приложения располагают теперь такими мощными средствами среды Notes/Domino, как:

- О надежная система информационной безопасности, включающая в себя сертификаты X.509, SSL, базовую аутентификацию, списки ACL баз данных, уровень доступа **Maximum Internet Access** (Максимальный доступ из Internet), доступ анонимных пользователей и многое другое. Более подробно об этом читайте в главе 10 или в файле справки Domino Administration (help5_admin.nsf или help6_a^min.nsf);
- О поддержка большого количества протоколов, в том числе TCP/IP, SMTP, NNTP, CORBA/IIOP, LDAP, X.509, SSL и S/MIME. Дополнительная информация по данному вопросу имеется в файле справки Domino Administration (help5_admin.nsf или help6_admin.nsf);
- О RAD (Rapid Application Development - быстрая разработка приложений), такие как агенты LotusScript для динамической генерации страниц и выполнения задач CGI с помощью событий WebQueryOpen и WebQuerySave, интегрированная поддержка сценариев JavaScript, языка формул, Java-агентов, апплетов Java и серверных сценариев (сервлетов), поддержка стандартного языка CGI посредством каталога CGI-BIN и множество инструментов RAD, например формы, страницы и проектировщики моделей. Более детальные сведения об этом можно найти в файле справки Domino Administration (help5_admin.nsf или help6_admin.nsf);

- О превращение Domino в межплатформенную среду разработки, способствующую углублению знаний и опыта персонала компаний;
- О сквозной поток HTML, позволяющий внедрять HTML в «родные» элементы проектирования Domino, дополнительно увеличивая возможности и производительность пользовательских приложений;
- О отличная интеграция баз данных, среди которых хранилища объектов Native Notes (файлы .nsf), подключения ODBC, NotesPump, DECS и другие инструменты для связи с унаследованными системами (help5_designer.nsf или help6_designer.nsf);
- О интегрированная поддержка приложений автоматизации (рабочих потоков). Notes/Domino уже поддерживает маршрутизацию почтовых форм и документов. То же касается и Web-приложений;
- О объединение серверов в кластеры, разбиение серверов, наличие виртуальных серверов и других дополнительных средств, которые помогают убедиться, что ваши важные приложения доступны пользователям в тот момент, когда они в них нуждаются. Подробнее об этом говорится в файле справки Domino Administration (help5_admin.nsf или help6_designer.nsf);
- О возможность исчерпывающего поиска по полнотекстовому индексу. Domino поддерживает поиск для одной базы данных, для нескольких баз и в пределах домена.

Как работает Domino

При обращении Web-браузера к странице, расположенной на сервере Domino, система определяет объект запроса - файл в файловой системе или содержимое базы данных. Когда запрашивается статическая HTML-страница в файловой системе, Domino предоставляет эту страницу только пользователю, имеющему право доступа к ней. Если файл защищен, пользователь должен пройти аутентификацию перед получением доступа.

Приведем пример URL, который иллюстрирует запрос статического HTML-файла в файловой системе Domino:

<http://www.definiti.com/html/index.html>

Если браузер обращается к содержимому базы данных Domino и пользователю предоставлено право доступа к запрашиваемой информации (может потребоваться аутентификация), Domino преобразует исходный элемент Domino в Web-страницу или апплет Java (в зависимости от способа построения приложения разработчиком) и открывает его для пользователя. Для создания мощных, надежных интерактивных Web-приложений подходят любые из перечисленных ниже элементов Domino - отдельно либо совместно с другими элементами:

- О формы About;
- О агенты (Java, Formula или LotusScript);
- О апплеты;
- О страницы;
- О документы;
- О папки;
- О формы;
- О макеты (наборы кадров);
- О навигаторы;

«

- О модели;
- О использования;
- О виды.

Ниже представлен пример, иллюстрирующий запрос содержимого базы данных Domino:

<http://www.definiti.com/external/test.nsf/All+Docs?OpenView&StartKey=Hatter>

На рис. 15.1 изображен процесс получения страницы от сервера Domino.

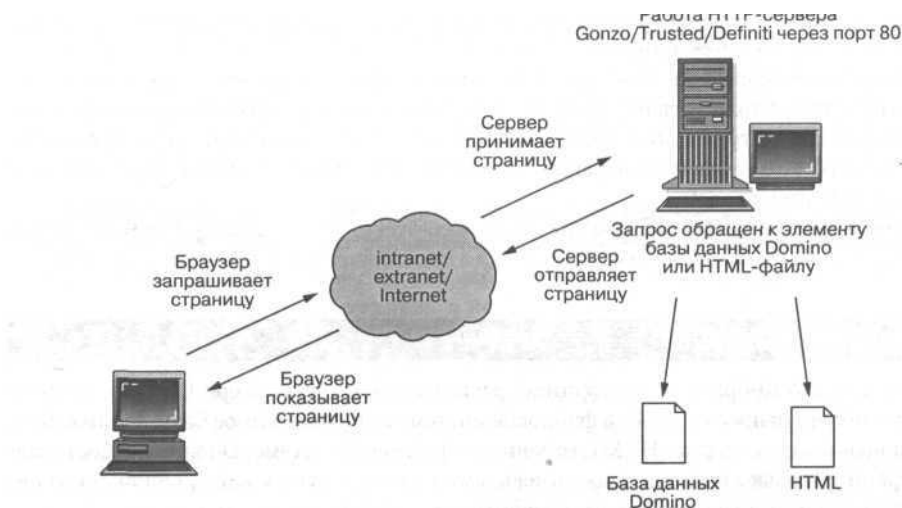


Рис. 15.1. Функции, выполняемые сервером Domino

Фактически любому приложению Domino легко стать Web-приложением. Однако не обязательно все возможности клиента Notes поддерживаются в браузере, поэтому необходимо ознакомиться со средствами Domino, которые позволяют преобразовывать элементы в формат HTML. Более подробно о построении приложений Domino рассказывается в базе данных справочной системы Notes Designer Help (help5_designer.nsf или help6_designer.nsf).

Установка HTTP

С момента создания среды Notes компания Lotus сделала большой шаг вперед в области установки и настройки сервера Notes/Domino, так что настройка сервера Domino еще никогда не была так проста, как сейчас. То же самое можно сказать и про HTTP-сервер Domino.

В следующем разделе показано, как настроить HTTP-сервер на работающем сервере Domino и как установить HTTP-сервер во время установки нового сервера Domino.

Установка HTTP на рабочем сервере Domino

Для установки и настройки HTTP-сервера на рабочем сервере Domino необходимо выполнить следующие действия:

1. На сервере Domino следует так настроить стек TCP/IP, чтобы он правильно работал и была возможность им управлять.
2. Запустите программу Domino Administrator, щелкните по вкладке **Configuration** (Конфигурация), выберите **Server** и выведите на экран серверный документ (Server document) того сервера, на котором планируется установка HTTP.
3. Откройте вкладку **Ports => Internet Ports** (Порты => Internet-порты). Если вы не хотите, чтобы все соединения с этим сервером работали с SSL, убедитесь, что в поле **TCP/IP port status** (Состояние порта TCP/IP) и в поле **SSL port status** (Состояние порта SSL) установлено значение **Enabled** (Разрешено) - рис. 15.2.

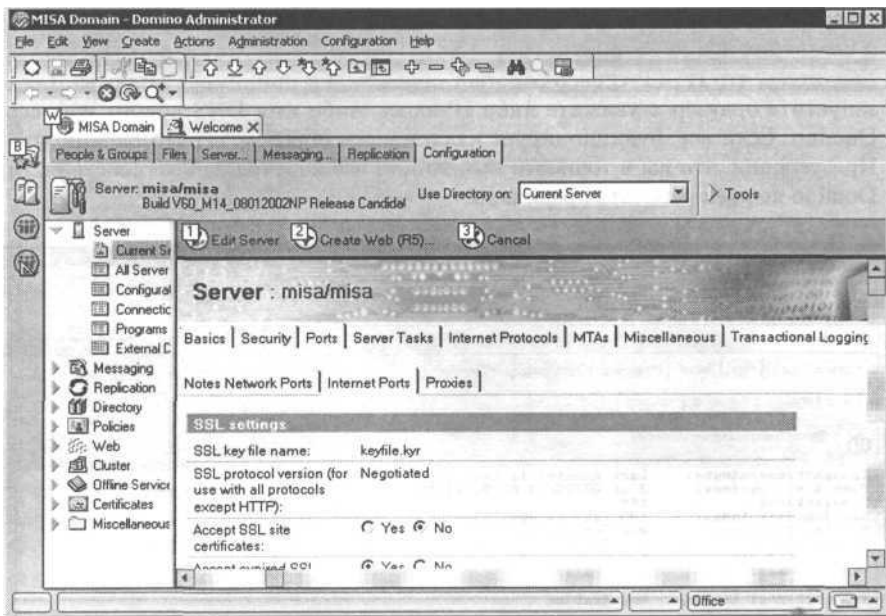


Рис. 15.2. Раздел **Ports** серверного документа

4. Сохраните измененный серверный документ.
5. Запустите сервер Domino и активизируйте задачу HTTP. Можно загрузить серверную задачу двумя способами. Первый способ: перейдите на вкладку **Server => Status** (Сервер => Состояние). Затем выберите **Task => Start** (Задача => Запуск) и в диалоговом окне **Start New Task** (Запуск новой задачи) отметьте **HTTP Web server** (рис. 15.3). Щелкните по кнопке **Start Task** (Запустить задачу). Второй способ: переключитесь

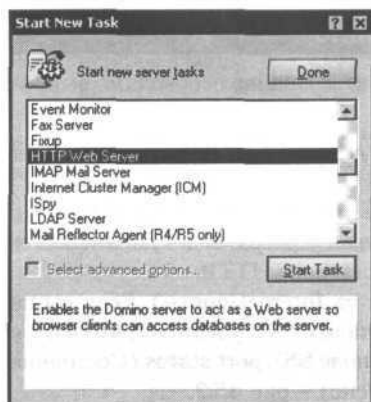


Рис. 15.3. Диалоговое окно Start New Task

в режим удаленной консоли управления (или на консоль управления сервером) и введите команду load http (рис. 15.4).

6. Убедитесь, что HTTP-сервер работает правильно и принимает запросы. Для этого запустите браузер и укажите либо IP-адрес, либо имя DNS нового Web-сервера Domino. Если все функционирует надлежащим образом, сервер Domino ответит. При условии, что вы в точности выполнили все перечисленные действия, сервер Domino должен работать правильно.

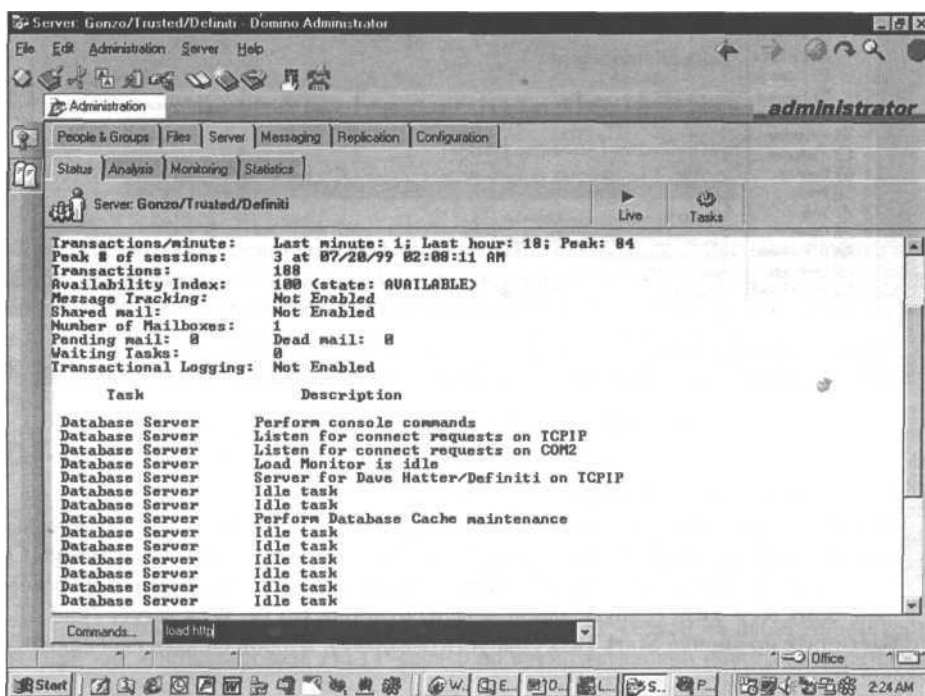


Рис. 15.4. Удаленная консоль управления сервером

Далее в этом разделе описывается, какие параметры можно настроить для HTTP-сервера на вкладках **Ports** => **Internet Ports** => **Web** (Порты => Internet-порты => Web), **Internet Protocols** =* **HTTP** (Internet-протоколы => HTTP) и **Internet Protocols** => **Domino Web Engine** (Internet-протоколы => Web-двигатель Domino) серверного документа Domino.

Настройка портов

Вкладка настройки портов (рис. 15.5) служит для управления состоянием портов и их настройки. Параметры настройки портов очень важны, поскольку от них непосредственно зависит возможность формирования соединений.

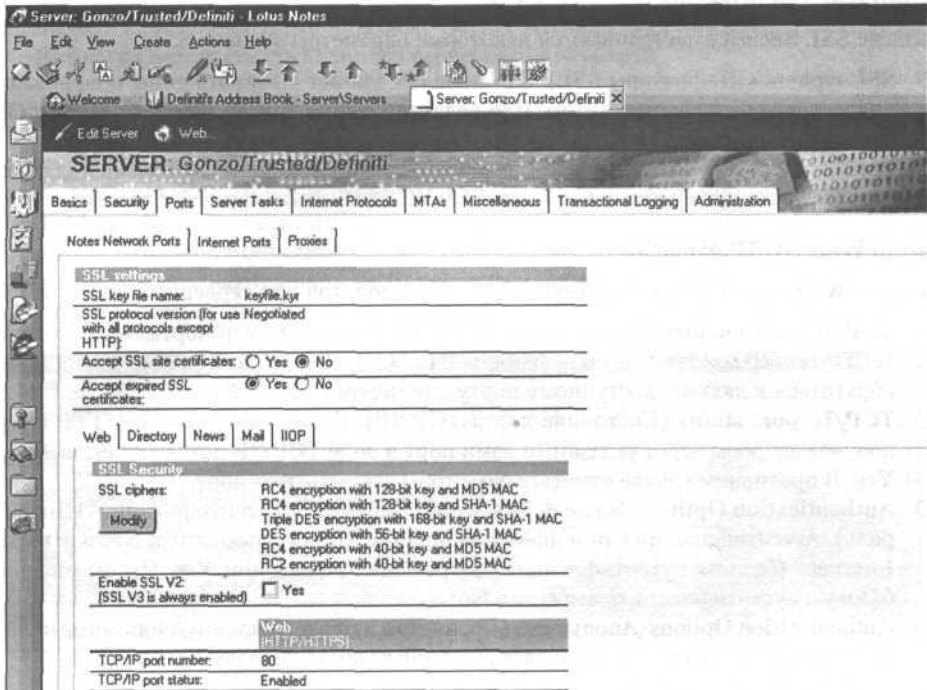


Рис. 15.5. Вкладка Internet Ports

Раздел SSL

Раздел SSL позволяет устанавливать некоторые важные параметры протокола SSL:

- О **SSL key filename** (Имя файла ключа SSL) - имя файла цепочки ключей SSL, содержащего ваш сертификат для сервера Domino. По умолчанию - keyfile.kyr. Убедитесь, что в данном поле записано только имя файла без пути. Кроме того, указанный файл должен иметь расширение .kyr;
- О **SSL protocol version...** (Версия протокола SSL). Выберите версию SSL, которую нужно установить. По умолчанию задано **Negotiated** (Согласование). Более подробно об SSL рассказывалось в главе 10;

- О Accept SSL site certificates (Принимать сертификаты сайтов SSL). Если нужно предоставить доступ пользователям, которые не работают с общими сертификатами SSL, но применяют протокол SSL, укажите Yes. В противном случае отметьте No, чтобы отменить соединения с помощью локальных сертификатов SSL. По умолчанию задано No;
- О Accept expired certificates (Принимать просроченные сертификаты). При необходимости проверять сроки действия сертификатов установите No. В противном случае задайте Yes и тем самым разрешите доступ пользователям с просроченными сертификатами. По умолчанию - Yes.

Раздел SSL Security

В разделе SSL Security настраиваются некоторые параметры защиты SSL:

- О SSL ciphers (Шифраторы SSL). Это поле предлагает выбирать типы шифрования, поддерживаемые вашим сайтом. Для редактирования списка нажмите Modify (Изменить);
- О Enable SSL V2... (Разрешить SSL версии V2). По умолчанию включена поддержка SSL V3. Если нужно активизировать SSL V2, установите данный флажок.

Раздел Web (HTTP/HTTPS)

В разделе Web определяются параметры настройки портов для серверной задачи HTTP:

- О TCP/IP port number (Номер порта TCP/IP). Введите номер порта, через который HTTP-сервер должен получать запросы. По умолчанию назначен порт 80, но можно обратиться к любому доступному порту с номером выше 1024;
- О TCP/IP port status (Состояние порта TCP/IP). Если нужно, чтобы HTTP-сервер получал запросы через указанный вами порт в поле TCP/IP port number, выберите Yes. В противном случае отметьте No, чтобы закрыть этот порт;
- О Authentication Options\Name & Password (Параметры аутентификации\Имя и пароль). Аутентификация с помощью комбинации «имя пользователя Notes + пароль Internet» (базовая аутентификация) разрешена при задании Yes. Чтобы отменить базовую аутентификацию, выберите No;
- О Authentication Options\Anonymous (Параметры аутентификации\Анонимные пользователи). Значение Yes предоставляет анонимным пользователям доступ для HTTP-запросов, а No закрывает его;
- О SSL port number (Номер порта SSL). Введите номер порта, который будет опрашивать HTTP-сервер во время соединений с помощью протокола SSL. По умолчанию - 443.
- О SSL port status (Состояние порта SSL). Если нужно, чтобы сервер обращался к порту, указанному в поле SSL port number, выберите Yes. В противном случае укажите No и тем самым закройте данный порт;

Порт 80

Помните, что если вы указываете не 80-й порт (по умолчанию), пользователям придется включать номер нового порта в адреса URL для запроса ресурсов сервера. Например, *http://www.definiti.com: 8080/welcome, nsf.*

- Authentication Options\Client Certificate (Параметры аутентификации\Сертификат клиента). Для разрешения аутентификации с помощью сертификатов X.509 отметьте Yes, а для отмены такой аутентификации - No;
- Authentication Options\Name & Password (Параметры аутентификации\Имя и пароль). Если нужно разрешить аутентификацию с помощью имени пользователя и пароля через SSL, задайте Yes, в противном случае - No;
- Authentication Options\Anonymous (Параметры аутентификации\Анонимные пользователи). Доступ для анонимных пользователей через SSL открывается установкой Yes, а отменяется выбором No.
- Enforce server access settings (Применить параметры доступа к серверу, только в R6). Значение Yes предписывает серверу HTTP использовать параметры безопасности, установленные в разделе Server Access (Доступ к серверу) на вкладке Security (Безопасность) данного серверного документа.

Настройка HTTP

Вкладка HTTP позволяет настраивать огромное количество параметров, определяющих порядок обслуживания запросов сервером Domino. Здесь рассмотрены все разделы вкладки HTTP (рис. 15.6). В версии R6 существенно изменился состав параметров в разделах, причем для сохранения обратной совместимости с версией R5 появились специальные вкладки. Ниже описываются параметры настройки протокола HTTP согласно версии R6, причем оговариваются отличия от версии R5.

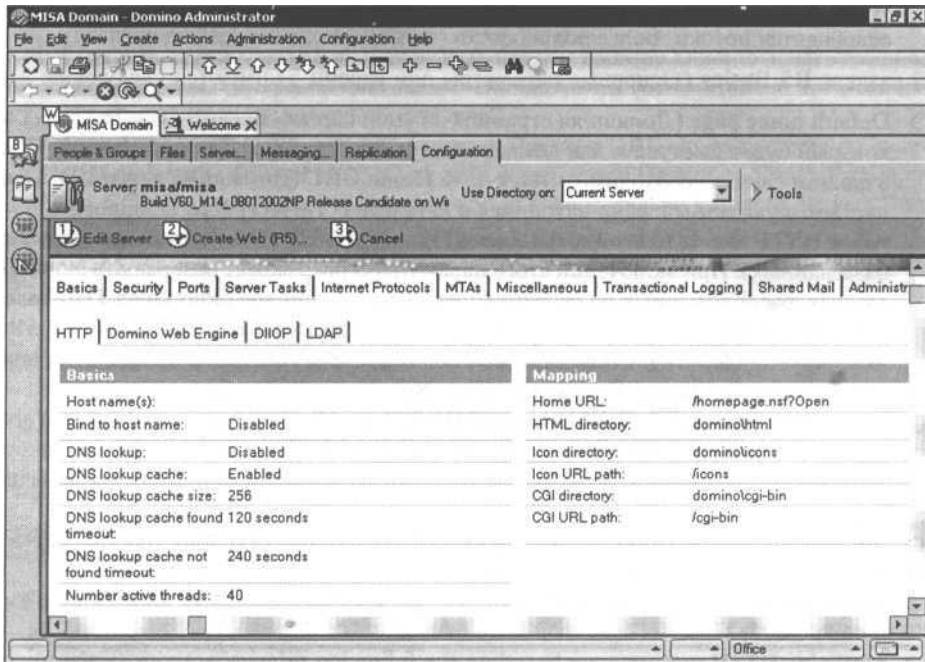


Рис. 15.6. Вкладка HTTP

Раздел Basics

В разделе **Basics** (Основные параметры) расположены следующие поля:

- **Host name** (Имя хоста). Это поле допускает задание до 32 имен хостов текущего сервера Domino. Когда оно пустое (по умолчанию), Domino определяет имя хоста на основании стека TCP/IP сервера;
- **Bind to host name** (Связывание с именем хоста). Если нужно указать псевдоним в поле **Host name**, активизируйте этот параметр. По умолчанию установлено **Disabled** (Запрещено);
- **DNS lookup** (Поиск по DNS). Если данный параметр включен, то Domino при попытке определения запрашиваемого пользователем имени хоста будет искать это имя в службе DNS;
- **DNS lookup cache** (Кэш просмотра DNS, только в R6). Разрешает кэширование запросов к службе DNS;
- **DNS lookup cache size** (Размер кэша просмотра DNS, только в R6). По умолчанию установлено 256 записей;
- **DNS lookup cache found timeout** (Тайм-аут для обнаружения в кэше просмотра DNS, только в R6). По умолчанию задано 120 секунд;
- **DNS lookup cache not found timeout** (Тайм-аут для необнаружения в кэше просмотра DNS, только в R6). По умолчанию назначено 240 секунд;
- **Number of active threads** (Число активных потоков). Определяет число потоков, которые можно одновременно запустить на сервере Domino. Когда сервер достигает установленного предела, новые запросы помещаются в очередь до тех пор, пока не освободятся потоки. Более подробно это описано далее в настоящей главе.

В разделе **R5 Basics** (Основные параметры для версии 5) имеются следующие поля:

- **Default home page** (Домашняя страница по умолчанию). Введите имя файла HTML, который будет выступать как домашняя страница сервера. Для правильной работы в данном случае необходимо, чтобы поле **Home URL** (Домашний адрес URL) было пустым, а указанный файл находился в каталоге HTML сервера Domino;
- **Allow HTTP clients to browse databases** (Разрешить HTTP-клиентам просматривать базы данных). При включении этого параметра сервер может возвращать список баз данных, расположенных на сервере (похоже на диалоговое окно **Open Database** на рабочей станции Notes). Когда пользователь открывает сайт, сервер явно или неявно формирует адрес URL с помощью команды ?OpenServer, которая проверяет значение данного параметра. По умолчанию - **No**;
- **Maximum requests over a single connection** (Максимальное число запросов во время одного соединения). В поле задается максимальное число запросов от одного браузера. По умолчанию - 5. Более подробно об этом рассказано в разделе, посвященном настройке;
- **Minimum active threads** (Минимальное число активных потоков). Данный параметр больше не применяется и служит только для обратной совместимости с R4;
- **Maximum cached commands** (Максимальное число кэшируемых команд). По умолчанию - 128;
- **Optimize HTTP performance based on the following primary activity** (Оптимизировать производительность HTTP на основе следующих основных действий). По умолчанию выбран вариант **Advanced** (Пользовательская настройка).

Поиск в DNS

Включение этого параметра означает, что вместо IP-адресов будут регистрироваться имена хостов клиентов, что, однако, отрицательно влияет на производительность сервера. Если вы не хотите регистрировать имена хостов или вообще не проводите регистрацию, сбросьте данный флажок.

Отмена просмотра баз данных

Из соображений безопасности этот режим нужно отключить для всех серверов с доступом в Internet, чтобы хакеры не могли получить несанкционированный доступ к информации о базах данных.

Раздел Mapping

В разделе **Mapping** (Отображение) помещены следующие поля:

- **Home URL** (Домашний адрес URL). Здесь задаются элементы проектирования, которые должны открываться, если пользователь вводит URL с явно указанным действием. Когда это поле остается пустым и не заполнено поле **Default home page** (Домашняя страница по умолчанию), серверу надлежит выполнить команду POpenServer, приводящую к ошибке при запрещенном просмотре баз данных. Если указана домашняя страница по умолчанию, не заполняйте данное поле;
- **HTML directory** (Каталог HTML). Назначьте серверу Domino путь поиска HTML-файлов в файловой системе. По умолчанию установлено Domino\HTML (относительно каталога данных Domino), если не определен другой путь;
- **Icon directory** (Каталог значков). Укажите, где серверу Domino искать графические изображения. По умолчанию задано Domino\icons (относительно каталога данных Domino), если не назначен другой путь;
- **Icon URL path** (URL-путь к значкам). Введите URL-адрес каталога со значками;
- **CGI directory** (Каталог CGI). Определите, где сервер Domino должен искать программы CGI. По умолчанию - Domino\cgi-bin (относительно каталога данных Domino), если не описан другой путь;
- **CGI URL path** (URL-путь CGI). Задайте URL-адрес каталога с CGI-программами.

Раздел DSAPI

Раздел **DSAPI** состоит из одного поля:

§

- **DSAPI filter filename** (Имя файла фильтра DSAPI). Если вы применяете фильтры DSAPI, то в поле указывается имя файла для этого фильтра.

Раздел Enable Logging To

В разделе **Enable Logging To** (Разрешить регистрацию в) помещены поля, управляющие форматом регистрации Domino:

- **Log files** (Файлы журнала). Если нужно, чтобы сервер Domino регистрировал Web-запросы к текстовым файлам файловой системы, установите в этом поле значение **Enabled**;
- **Domlog.nsf**. Если требуется, чтобы Domino регистрировал Web-запросы к базам данных Domino, укажите **Enabled**.

Раздел Log File Settings

Поля раздела **Log File Settings** (Параметры файла журнала) позволяют управлять порядком добавления регистрационных записей:

- **Access log file** (Файл регистрации доступа). В этом поле указывается формат для регистрации обращений к сайту - общий или расширенный общий;
- **Time format** (Формат времени). Здесь определяется формат времени для регистрации Web-сервера - либо формат местного времени (по умолчанию), либо формат времени по Гринвичу;
- **Log file duration** (Длительность хранения log-файла). В поле устанавливается период времени, по окончании которого регистрационная информация, хранящаяся в файле журнала, будет стерта и заменена новой - **Daily** (День), **Weekly** (Неделя), **Monthly** (Месяц) или **Never** (Никогда);
- **Maximum log entry length** (Максимальная длина регистрационной записи, только в R6). По умолчанию равна 10 Кб;
- **Maximum size of access log** (Максимальный размер файла регистрации' доступа, только в R6). По умолчанию - 0, то есть регистрация доступа не производится.

Раздел Log Filenames

В разделе **Log Filenames** (Имена файлов журналов) расположены поля, где назначаются файлы, в которые следует записывать регистрационную информацию:

- **Directory for log files** (Каталог для log-файлов). Если включена регистрация, задайте каталог, в котором должны храниться log-файлы;
- **Access log** (Регистрация доступа). Введите имя текстового файла, хранящего информацию о доступе из Internet. По умолчанию access-log;
- **Agent log** (Регистрация агентов). Укажите имя текстового файла, хранящего информацию о работе агентов. По умолчанию agent-log;
- **Referrer log** (Регистрация ссылок). Задайте имя текстового файла, хранящего информацию о ссылках URL. По умолчанию referrer-log;
- **Error log** (Регистрация ошибок, только для R4 и R5). Введите имя, которое будет использоваться для текстового файла, хранящего информацию об ошибках внутреннего Web-сервера. По умолчанию error-log;
- **CGI error log** (Регистрация ошибок CGI). Определите имя текстового файла, хранящего информацию об ошибках, выдаваемых CGI-программами. По умолчанию cgi-error-log;

Раздел Exclude from logging

В раздел **Exclude from logging** (Удалить из регистрации) входят поля, которые содержат информацию, не включенную в журналы регистрации Domino:

- **URLs** (Адреса URL) - задаются любые URL-адреса, для которых необходимо отменить регистрацию запросов. Так, если ввести `http://www.definiti.com?openServer`, запросы к этому адресу регистрироваться не будут;
- **Methods** (Методы) - указываются все методы HTTP, не подлежащие занесению в журналы регистрации. Например, POST;

- **MIME types** (Типы MIME) - назначаются типы MIME, обращения к которым не следует записывать в журналы регистрации. Например, `images\jpg`;
- **User agents** (Агенты пользователей) - перечисляются все агенты, запросы к которым не должны помещаться в журналы регистрации. Так, если задать `HelloWorld`, запросы к этому агенту регистрироваться не будут;
- **Return Codes** (Возвращаемые коды) - указываются любые коды, возвращаемые сервером и не вносимые в журналы регистрации. Например, всем известный код 404;
- **Hosts and Domains** (Хосты и домены) - выбирается, для каких хостов и доменов необходимо отменить регистрацию запросов. Например, если ввести `definiti.com`, запросы к этому домену регистрироваться не будут.

Раздел Timeouts

Раздел **R5 Timeouts** (Тайм-ауты, временные ограничения для версии R5) составляют поля, определяющие интервалы времени, в течение которых могут выполняться указанные функции перед тем, как сервер разрывает соединение:

- **Input timeout** (Тайм-аут ввода) - интервал времени между соединением с сервером и запросом пользователя. По умолчанию указано 2 минуты. По истечении этого времени соединение разрывается;
- **Output timeout** (Тайм-аут вывода) - интервал времени между запросом пользователя и ответом сервера. По умолчанию установлено 20 минут. По истечении этого времени соединение разрывается;
- **CGI timeout** (Тайм-аут CGI-программ) - продолжительность работы CGI-программы. По умолчанию задано 5 минут. По истечении этого времени сервер выдает предупреждение. По прошествии еще 5 минут выполнение программы принудительно прерывается;
- **Idle thread timeout** (Тайм-аут свободного потока) - интервал времени, в течение которого сервер держит открытым свободный поток. Если число рабочих и свободных потоков превышает значение, указанное в поле **Minimum Idle threads** (Минимальное число свободных потоков), то по истечении времени, заданного в этом поле, поток закрывается. По умолчанию установлено значение 0 - потоки не должны завершаться.

В разделе **Timeouts** (Тайм-ауты, временные ограничения) располагаются поля, задающие интервалы, в течение которых могут выполняться определенные функции, прежде чем сервер R6 разрывает соединение:

- **HTTP persistent connections** (Постоянные соединения по протоколу HTTP). Разрешает формирование непрерываемых (постоянных) соединений HTTP;
- **Maximum requests per persistent connection** (Максимальное число запросов для одного постоянного соединения). По умолчанию равно 5;
- **Persistent connections timeout** (Тайм-аут постоянного соединения). По умолчанию составляет 180 секунд;
- **Request timeout** (Тайм-аут запроса). По умолчанию указано значение 60 секунд;
- **Input timeout** (Тайм-аут ввода). По умолчанию - 15 секунд;
- **Output timeout** (Тайм-аут вывода). По умолчанию - 180 секунд;
- **CGI timeout** (Тайм-аут сценария CGI). По умолчанию - 180 секунд.

Раздел Web agents

В разделе **Web agents** (Web-агенты) расположены поля, управляющие некоторыми особенностями работы агентов при вызове в качестве Web-приложений. В версии R5 этот раздел находится на вкладке **Basics**, но в версии R6 перенесен на вкладку **Domino Web Engine**. Поля данного раздела:

- О **Run Web agents concurrently** (Запускать Web-агенты одновременно). В данном поле определяется возможность одновременного запуска агентов, загруженных Web-браузером. По умолчанию указано **Enabled**. Если компьютер мощный, оставьте значение по умолчанию;
- О **Web agent timeout** (Тайм-аут Web-агентов). Здесь задается интервал времени, в течение которого работает агент, прежде чем сервер прерывает его выполнение.

Разделы Network Settings и HTTP Protocol Limits

В разделах **Network Settings** (Сетевые параметры) и **HTTP Protocol Limits** (Ограничения для протокола HTTP) можно установить несколько параметров, действующих только в версии R6. От этих параметров зависят характеристики доступа к серверу по протоколу IP и подключений по протоколу HTTP.

Не забывайте о производительности

Все указанные параметры определенным образом влияют на производительность и рассматриваются в разделе о настройке Web-сервера.

Настройка Web-агентов

Эти параметры описаны в разделе о настройке Web-сервера.

Настройка Web-двигателя Domino

Параметры Domino Web Engine (Web-двигатель Domino) управляют различными аспектами работы HTTP-сервера. Они обсуждаются в последующих разделах (рис. 15.7).

Раздел HTTP Sessions

Ниже перечислены поля раздела **HTTP Sessions** (Сеансы HTTP):

- О **Session authentication** (Аутентификация сеанса) - служит для определения необходимости аутентификации Web-сеансов. По умолчанию отключено;
- О **Idle session timeout** (Тайм-аут свободного сеанса, в R5) - здесь задается время (в минутах), в течение которого сеанс может оставаться открытым, но свободным до его закрытия. По умолчанию - 30 минут;
- О **Maximum active sessions** (Максимальное число активных сеансов, в R5) - в этом поле указано максимальное число сеансов, которые могут быть открыты с HTTP-сервером одновременно. По умолчанию это число равно 1000. Если сервер обладает достаточными ресурсами, допускается задать большее число, увеличив тем самым количество одновременно обслуживаемых пользователей.

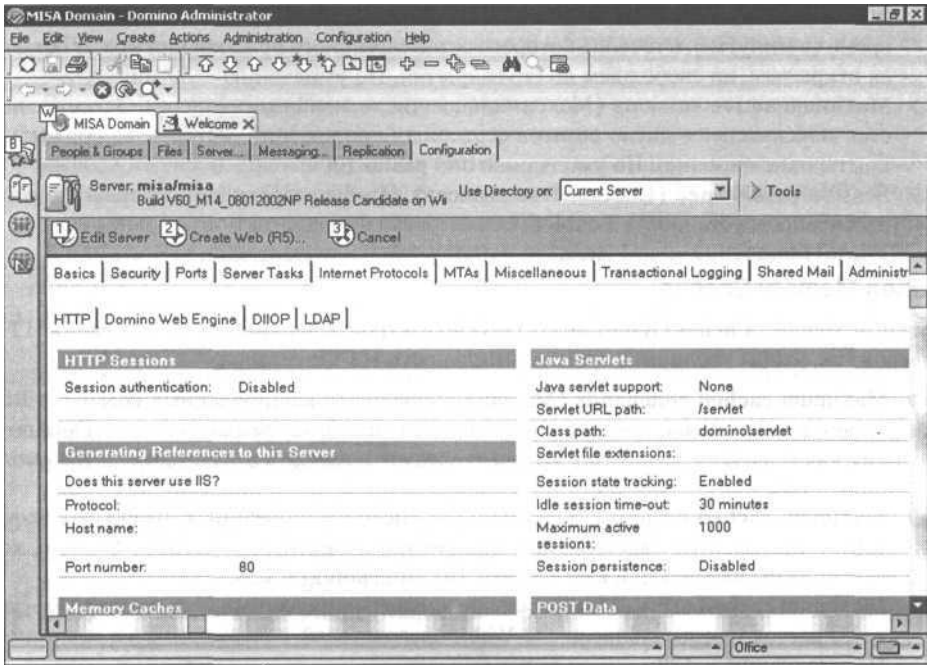


Рис. 15.7. Вкладка Domino Web Engine

Раздел Java Servlets

В разделе **Java Servlets** (Серверные сценарии (сервлеты) Java) можно установить характер взаимодействия серверных приложений Java с двигателем HTTP сервера Domino:

- **Java servlet support** (Поддержка сервлетов Java). В этом поле устанавливается факт и способ поддержки приложений Java. Если здесь выбрано значение **None**, то сервлеты Java не поддерживаются, а если значение **Domino servlet manager** - то Domino управляет этими серверными приложениями. Последний вариант, **Third-part servlet support**, требует наличия стороннего средства управления сервлетами. По умолчанию - **None**;
- **Servlet URL path** (URL-путь к сервлету). Вводится URL-путь к Java-приложениям. По умолчанию - **/servlet**;
- **Class path** (Путь к классам). Это поле служит для задания пути к файлам классов серверных приложений;
- **Servlet file extensions** (Расширения файлов сервлетов). Указываются расширения файлов серверных приложений;
- **Session state tracking** (Отслеживание состояния сеансов). Если нужно отслеживать состояние сеансов сервлетов, активизируйте этот флажок. Значение по умолчанию - **Disabled**;

- **Idle session timeout** (Тайм-аут свободного сеанса). Это поле позволяет определить время (в минутах), в течение которого сеанс серверного приложения может оставаться открытым, но свободным до его закрытия. По умолчанию - 30 минут;
- **Maximum active sessions** (Максимальное число активных сеансов). Здесь назначается максимальное число сеансов серверных приложений, которые могут быть открыты одновременно. По умолчанию оно равно 1000;
- **Session persistence** (Постоянство сеансов). Чтобы разрешить поддержку постоянных сеансов, установите **Enabled**.

Раздел Memory Caches

В разделе **Memory Caches** (Кэш-память) можно настроить параметры кэширования HTTP-серверов так, чтобы увеличить производительность HTTP-сервера:

- **Maximum cached commands** (Максимальное число кэшированных команд, в R5) - задается максимальное число URL-запросов, преобразуемых в команды Domino, таких как OpenView, openPage, которые следует помещать в кэш-память. По умолчанию - 128;
- **Maximum cached designs** (Максимальное число кэшированных проектных элементов) - указывается максимальное количество проектных элементов Domino, которые должны вводиться в кэш-память. По умолчанию - 128;
- **Maximum cached users** (Максимальное число кэшированных пользователей) - устанавливается максимальное число Web-пользователей, содержащихся в кэш-памяти. По умолчанию - 128;
- **Cached user expiration interval** (Срок хранения кэшированных пользователей) - определяется время (в минутах), по истечении которого удаляется кэш-память пользователя.

Раздел POST Data

Раздел **POST Data** (Передаваемые данные) служит для управления объемом данных, которые могут быть отправлены HTTP-серверу командой POST протокола HTTP:

- **Maximum POST data** (Максимальное количество передаваемых данных). Это поле позволяет ограничить размер блока данных, которые допускается передавать на сервер во время операции POST. По умолчанию задано значение 0, то есть предел не установлен. Если нужно ввести какое-либо ограничение, укажите максимальный размер блока передаваемых данных в килобайтах;
- **File compression on upload** (Сжатие файла при загрузке). Если необходимо передавать файлы из браузера с помощью сжатия Notes, выберите **Enabled**. После сжатия файлы нельзя загружать побайтно, но при этом экономится дисковое пространство.

Раздел Conversion/Display

В разделе **Conversion/Display** (Преобразование/отображение) устанавливается порядок преобразования определенных данных перед отправкой и формат, в котором они должны выводиться для Web-клиента:

- **Image conversion format** (Формат преобразования изображений). В этом поле назначается формат преобразованных изображений, вставленных в Notes. Есть два варианта - JPEG и GIF. Значение по умолчанию - GIF;

- **Interlaced rendering** (Чересстрочная развертка, только в R5). Если принят формат GIF, то для ускорения загрузки изображений в браузере можно воспользоваться чересстрочным выводом на экран. Чтобы включить эту функцию, выберите **Enabled**;
- **Progressive rendering** (Прогрессивная развертка). Когда применяется формат JPEG, ускорить загрузку изображений в браузере можно посредством последовательного вывода на экран. Данная функция активизируется при задании значения **Enabled**;
- **JPEG image quality** (Качество изображений в формате JPEG, только в R6). Определяет в процентном отношении качество изображений JPEG. По умолчанию установлено 75%. Это поле доступно после установки в поле **Image conversion format** значения **JPEG**;
- **Default lines per view page** (Число строк на страницу вида, установленное по умолчанию). Данное поле позволяет указать число строк для вида, отображаемое в браузере, когда нельзя определить этот параметр в учетной записи. По умолчанию - 30. Значение 0 говорит о том, что предел не задан;
- **Maximum lines per view page** (Максимальное число строк на страницу вида). - В поле назначается максимальное число строк вида, открываемого в браузере. По умолчанию 1000. Значение равно 0, когда предел не установлен;
- **Default search results limit** (Ограничение числа результатов поиска, установленное по умолчанию). Здесь указывается, какое число результатов поиска отображается в браузере. По умолчанию - 250;
- **Maximum search results limit** (Максимальное число результатов поиска). В данном поле устанавливается максимальное число выводимых результатов поиска, осуществляемого из браузера. По умолчанию - 1000. Значение 0 показывает, что предел не задан;
- **Make this site accessible to Web search site crawlers** (Сделать этот сайт доступным для «Web-червяков»). Поле позволяет сделать содержимое Domino доступным для внешних инструментов поиска. При активизации этого параметра синтаксическая структура Domino ? преобразуется в структуру !;
- **Redirect to resolve external links** (Переадресация для преобразования внешних ссылок).

Раздел Character Set Mapping

Поля в разделе **Character Set Mapping** (Отображение набора символов) в R5 или в разделах **Character Set** и **Language** (Язык) в R6 служат для управления наборами символов, используемых в сервере Domino (эти параметры особенно важны для многоязычных и/или глобальных сайтов):

- **Default character set group** (Набор символов по умолчанию) - выбирается набор символов для вывода в браузере. По умолчанию - western;
- **Convert resource strings to** (Преобразовывать строки ресурсов; только в R5) или **Default resource strings language** (Язык по умолчанию для строк ресурсов; только в R6) - задается язык, на который должны переводиться строки ресурсов. По умолчанию установлен английский. В версии R6 можно указать альтернативный язык для ресурсных записей в поле **Additional resource strings language** (Дополнительный язык для строк ресурсов);
- **Use UTF-8 for output** (Использовать для вывода UTF-8). UTF-8 - это расширенный набор символов ASCII, который разбивает значения Unicond на восьмиразрядные

последовательности. Если вы работаете с Unicod, допускается установить в этом поле **Yes**, чтобы разрешить преобразование. В версии R6 возможна кодировка UTF-8 для форм HTML, если задать **Yes** в поле **Use UTF-8 for HTML forms** (Использовать UTF-8 для HTML-форм);

- ☐ **Use auto-detection if database has no language information** (Использовать автоопределение, если в базе данных отсутствует языковая информация). Здесь разрешается автоопределение применяемого языка, если в базе данных информация о языке отсутствует;
- ☐ **Western** (Западный). Отображается западный набор символов. По умолчанию ISO-8859-1;
- ☐ **Central European** (Центрально-европейский). Отображается центрально-европейский набор символов. По умолчанию ISO-8859-2;
- ☐ **Japanese** (Японский). Отображается японский набор символов. По умолчанию SJIS;
- ☐ **Traditional Chinese** (Традиционный китайский). Отображается традиционный китайский набор символов. По умолчанию Big5;
- ☐ **Simplified Chinese** (Упрощенный китайский). Отображается упрощенный китайский набор символов. По умолчанию GB;
- ☐ **Korean** (Корейский). Отображается корейский набор символов. По умолчанию KSC5601 (EUC);
- ☐ **Cyrillic** (Кириллица). Отображается русский набор символов. По умолчанию KOI8-R;
- ☐ **Greek** (Греческий). Отображается греческий набор символов. По умолчанию ISO-8859-7;
- ☐ **Turkish** (Турецкий). Отображается турецкий набор символов. По умолчанию ISO-8859-9;
- ☐ **Thai** (Тайский). Отображается тайский набор символов. По умолчанию Windows-874;
- ☐ **Baltic** (Балтийский). Отображается балтийский набор символов. По умолчанию Windows-1257;
- ☐ **Arabic** (Арабский). Отображается арабский набор символов. По умолчанию Windows-1256;
- ☐ **Hebrew** (Иврит). Отображается набор символов иврита. По умолчанию ISO-8859-8;
- ☐ **Vietnamese** (Вьетнамский). Отображается вьетнамский набор символов. По умолчанию Windows-1258;
- ☐ **Character set in header** (Набор символов в заголовке). Если нужно, чтобы сервер передавал информацию об используемом наборе символов в HTTP-заголовке, установите этот флажок;
- ☐ **Meta character set** (Набор мета-символов). Данный параметр тесно связан с предыдущим. Если нужно, чтобы сервер передавал информацию о применяемом наборе символов в теге META заголовка HTTP, активизируйте этот флажок.

Раздел Disk Cache for Images and Files

В разделе **Disk Cache for Images and Files** (Кэш-память диска для изображений и файлов) содержатся параметры, которые в R5/6 не применяются (разработчики оставили их только для обратной совместимости):

- ☐ **Cache directory** (Каталог кэш-памяти). В поле задается имя каталога, в котором хранятся кэш-файлы. По умолчанию - domino\cache;

- О **Maximum cache size** (Максимальный размер кэш-памяти). Определяется максимальный размер кэша (в мегабайтах). По умолчанию - 50 Мб;
- О **Delete cache on shutdown** (Удалять кэш-память при выключении). Если нужно, чтобы при выключении сервера кэш-память очищалась, установите этот флажок. Значение по умолчанию - **Disabled**;
- О **Garbage collection** («Сборка мусора»). Здесь выбирается автоматическая очистка кэш-памяти посредством удаления редко используемых файлов. Отметьте в этом поле значение **Enabled**, чтобы включить «очистку» кэша;
- О **Garbage collection interval** (Интервал «сборки мусора»). Если включена «сборка мусора», можно назначить временные интервалы (в минутах), по прошествии которых из кэш-памяти удаляется «мусор». По умолчанию - 60 минут.

Важно помнить, что значения, установленные в документе виртуального сервера (Virtual Server document), имеют преимущество по отношению к параметрам в серверном документе.

Документы виртуального сервера

Domino R5 упрощает поддержку нескольких сайтов благодаря документам виртуального сервера. Для каждого поддерживаемого сайта создается отдельный документ виртуального сервера и с этим сайтом сопоставляется статический IP-адрес. Чтобы сформировать документ виртуального сервера, откройте Domino Administrator и выберите сервер, на котором нужно поместить виртуальный сервер (рис. 15.8). В версии R6 почти все, что связано с Web,

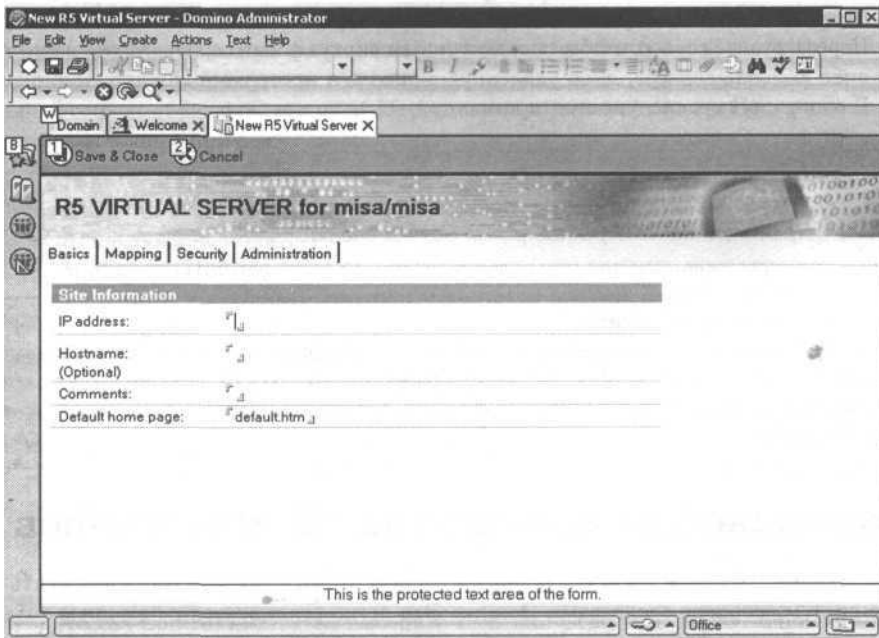


Рис. 15.8. Документ виртуального сервера

имеет специальную отметку о принадлежности к версии R5. Возможно, компания Lotus собирается модернизировать такие средства, но пока это еще не сделано.

Затем выполните следующие действия:

1. Щелкните по кнопке **Web** и выберите **Create Virtual Server** (Создать виртуальный сервер).
2. В приглашении **Virtual Document Type** (Тип виртуального документа) отметьте **Virtual Server** (Виртуальный сервер).
3. На вкладке **Basics** заполните следующие поля:
 - **IP-address** (IP-адрес). Введите IP-адрес виртуального сервера. Помните, что это должен быть статический адрес;
 - **Hostname** (Имя хоста). Укажите имя хоста виртуального сервера (необязательно);
 - **Default home page** (Домашняя страница по умолчанию). Задайте имя HTML-файла, выводимого при обращении к данному виртуальному серверу. Этот параметр не является обязательным и работает только в том случае, когда поле **Home URL** не заполнено.
4. Щелкните по вкладке **Mapping** и задайте адрес URL, который необходимо открыть при обращении пользователя к URL, установленному в поле **Home URL**. Помните, что значение **Home URL** преобладает над значением **Default home page**. Значения параметров в остальных полях в большинстве случаев лучше оставить без изменения, если только вам не нужно определить конкретные каталоги для каждого виртуального сервера. В последнем случае внесите в эти поля соответствующие сведения.
5. Щелкните по вкладке **Security** (Защита) и введите необходимую информацию. Обычно вполне достаточно значений по умолчанию.
6. Сохраните новый документ виртуального сервера.
7. Перезагрузите сервер, чтобы стал доступным виртуальный сервер. Можно применить либо консоль сервера, либо удаленную консоль в программе **Domino Administrator**. В обоих случаях следует ввести команду `tell http restart`.

Настройка виртуального сервера

Если виртуальный сервер пытается использовать файлы совместно с другими серверами, можно оставить эти параметры настройки без изменений.

Риск взлома системы защиты

Имейте в виду, что если активизирован просмотр каталогов, команда `/?Open&i URL` выведет все базы данных для всех виртуальных серверов, поскольку **Domino** работает с каталогами данных совместно со всеми виртуальными серверами. Неплохо было бы отключить этот параметр.

Использование документов защиты файлов

Еще одно замечательное средство появилось в версии R5 - возможность защитить файловую систему сервера средствами **Domino**. Это легко реализуется с помощью создания документов защиты файлов (File Protection document), которые позволяют управлять доступом Web-пользователей к файловой системе сервера. Например, допускается для анонимных Web-пользователей закрыть доступ к любым файлам JPEG.

Документы защиты файлов можно настроить для целого каталога или для отдельного файла; как вы, наверное, догадались, по умолчанию установлен путь к каталогу данных Domino, но ничто не мешает назначить защиту файлов и для других каталогов. Специалисты Lotus рекомендуют такую защиту для всех каталогов, доступных Web-пользователям.

Хотя это средство на самом деле достаточно полезное, при работе с документами защиты файлов необходимо иметь в виду несколько предупреждений. Первое: защита файловой системы применяется к любым файлам, которые обращаются к другим файлам (например, к HTML-файлам, вызывающим файлы изображений), но не к файлам, открываемым CGI-программами, серверными приложениями (сервлетами) и агентами, которые выводят на экран другие файлы.

Например, можно создать документ защиты файлов, который разрешает группе **Definitive Developers** запускать сценарий CGI с именем Test. Однако, если Test открывает другие файлы, служба File Protection не проверяет права доступа к этим файлам. Файлов, выводимых другими файлами, это не касается. Так, когда HTML-файл ссылается на изображение JPEG, файл изображения защищен, а пользователь не имеет права доступа к нему, то изображение будет недоступным.

При первом запуске сервера Domino R5/6 документ защиты файлов создается в каталоге Domino для папки domino\adm-bin. Этот документ предоставляет администраторам (список администраторов берется из поля **Administrators** серверного документа) права **Write/Read/Execute** (Чтение/запись/выполнение программ), а остальным пользователям присваивается уровень доступа **No Access**. Необходимо помнить, что список администраторов в документе защиты файлов после первого запуска не обновляется при добавлении имен в поле **Administrators**.

Создать документ защиты файлов достаточно просто. Откройте Domino Administrator и выберите сервер, файловую систему которого нужно защитить. Если вы защищаете виртуальный сервер, убедитесь, что указали именно виртуальный сервер. После этого выполните перечисленные ниже действия:

1. Щелкните по кнопке **Web** и отметьте **Create File Protection** (Создать защиту файлов).
2. На каждой вкладке введите необходимую информацию. На вкладке **Basics** расположены следующие поля:
 - **Applies to** (Применяется к) - имя сервера (или виртуального сервера) для которого создается данный документ. Это поле информационное, изменить значение в нем нельзя;
 - **Path** (Путь) - диск, каталог или файл, который нужно защитить, путь вводится относительно каталога данных Domino.
3. Щелкните по вкладке **Access Control** (Управление доступом), заполните единственное поле и сохраните документ:
 - **Current access control list** (Текущий список управления доступом). Внесите пользователей и группы, которые могут получить доступ к указанным вами файлам и каталогам, а также уровень доступа. Эти параметры похожи на списки ACL базы данных. Пользователи, не указанные в списке, получают доступ по умолчанию (**No Access**). Чтобы добавить пользователя в список, щелкните по кнопке **Set/Modify Access Control List**, затем выберите **User** или **Group** в Domino Administrator либо введите имя в поле **Name** и отметьте **Read/Execute access (GET method)**, **Write/Read/Execute access (POST and GET methods)** или **No Access**. Определив пользователей, щелкните по **Next**, чтобы добавить эту запись в список доступа. Чтобы

удалить запись, выделите ее и нажмите **Clear** (Очистить). Если анонимные пользователи должны иметь доступ к файлам, введите в поле **Name** значение **Anonymous** и установите соответствующий уровень доступа.

4. Сохраните новый документ защиты файлов.
5. Перезагрузите сервер, чтобы защита файлов вступила в силу. Можно сделать это с помощью либо консоли сервера, либо удаленной консоли в программе Domino Administrator. Введите команду `tell http restart`.

Документ защиты файлов изображен на рис. 15.9.

Рекомендуется Lotus

Специалисты Lotus рекомендуют определять документы защиты файлов для всех каталогов, доступных Web-пользователям и пользователям, которые допущены к остальным файлам и каталогам на сервере.

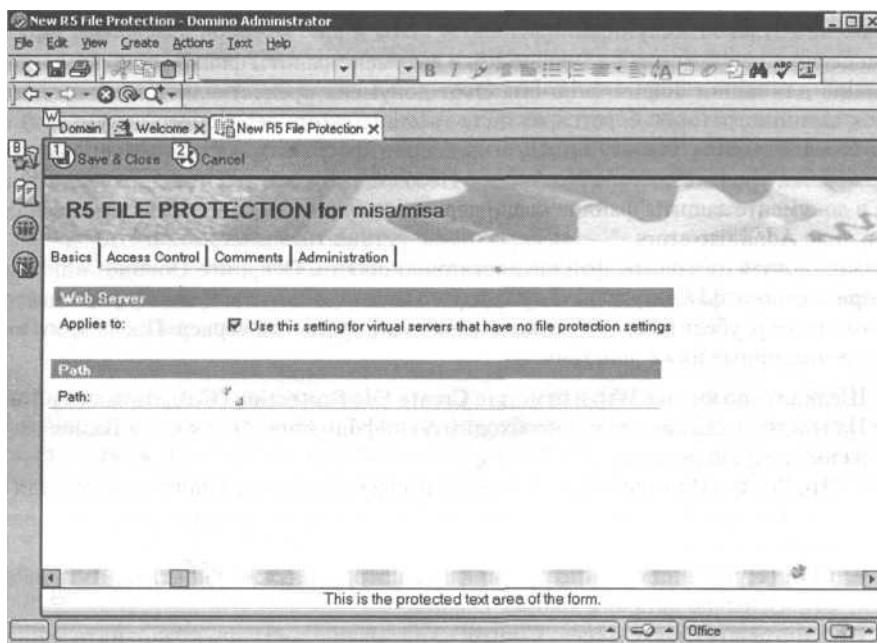


Рис. 15.9. Документ защиты файлов

Использование документов отображения/переадресации

В Domino R5/6 легко отображать расположение ресурсов и производить переадресацию (перенаправление) посредством документов отображения/переадресации (Mapping/Redirection document). Те же документы позволяют управлять файлами баз данных,

HTML-файлами, файлами изображений, сценариями CGI и другими файлами, находящимися в различных местах, а также перемещать их на новые места, не меняя ссылки URL и серверные документы. При переадресовке ресурс URL появляется в новом месте. Однако при отображении адреса URL он оказывается скрытым от пользователя.

Типы доступа

Команда *GET* позволяет пользователю открывать файлы и запускать программы в каталоге. Команда *POST* обычно служит для передачи данных в программу CG, следовательно, доступ по *POST* нужно предоставлять каталогам, содержащим сценарии *CG*. Значение **No Access** закрывает доступ указанным группам или пользователям.

Например, если нужно переместить базу данных *home.nsf* с сервера *gonzo.definiti.com* на сервер *borg.definiti.com*, формируется документ отображения/переадресации, который будет перенаправлять пользователя с *gonzo.definiti.com* на *borg.definiti.com*.

Чтобы создать такой документ:

1. В Domino Administrator укажите серверный документ сервера, на который нужно переадресовать или отобразить URL-каталог.
2. Щелкните по кнопке **Web** и выберите **Create URL Mapping/Redirection** (Создать отображение/переадресацию URL).
3. Щелкните по вкладке **Basics** и заполните поле **What do you want to setup** (Что нужно установить), выбрав один из трех вариантов:
 - **URL => Directory** (URL => Каталог). Чтобы отобразить URL на другой каталог, отметьте данный вариант. Это полезно, когда нужно переименовать каталоги или переместить файлы либо хранить файлы на разных дисках, не затрагивая пользователей. Переадресованный URL не отображается в поле **Location** на рабочей станции пользователя;
 - **URL => Redirection URL** (URL => Переадресация URL). Укажите такой вариант, если требуется переадресовать входящий URL на другой адрес URL. При этом адрес, на который перенаправляется пользователь, отображается в браузере;
 - **URL => URL**. При задании данного варианта входящий URL перенаправляется на другой адрес URL, который применяется при переносе групп файлов, создании псевдонимов для длинных имен файлов, переименовании каталогов и хранении файлов на разных дисках. Имейте в виду, что нельзя отобразить страницы, хранящиеся в базе данных Domino, на другой URL. При использовании этой методики переадресованный URL не выводится в браузере.
4. Если вы создаете отображение на виртуальный сервер, щелкните по вкладке **Site Information** (Информация о сайте) и укажите в поле **IP Address** значение IP-адреса виртуального сервера. Это требуется только в случае работы с виртуальным сервером.
- 5.- Щелкните по вкладке **Mapping** (Отображение) и введите необходимую информацию:
 - **First URL path** (Первый URL-путь) в R5 или **Incoming URL string** (Входная строка URL) в R6. Назначьте путь входящего URL, который должен быть переадресован на другой URL или каталог;
 - **Second URL path** (Второй URL-путь) в R5 или **Target server directory** (Каталог целевого сервера) в R6. Опишите полный путь каталога или URL, на который необходимо переадресовать пользователя. Помните, что, если вы обращаетесь к документу отображения/переадресации «URL => URL» или «URL => Directory»,

следует задать путь на том же сервере, на котором находится каталог, определенный путем URL.

6. Щелкните по вкладке **Access** (Доступ) и установите тип доступа пользователей в поле **Access** (Доступ). Вам будут предложены следующие варианты:
 - если вы выбрали «URL => Directory», укажите тип доступа к этому каталогу, который надо предоставить пользователям. **Read** позволяет читать файлы в каталоге с помощью браузера, а **Execute** - запускать оттуда программы;
 - для любых каталогов, содержимым которых являются HTML-файлы или файлы изображений, определите доступ **Read**, но не **Execute**;
 - доступ **Execute** разрешите только для каталогов, включающих в себя сценарии CGI и другие файлы, которые можно запустить из браузера. Не предоставляйте доступа **Read** - пользователям не нужно смотреть содержимое этих каталогов.
7. Сохраните документ.
8. Введите на консоли сервера или на удаленной консоли команду `tell http restart`, чтобы новые параметры вступили в силу.

Документ отображения/переадресации изображен на рис. 15.10.

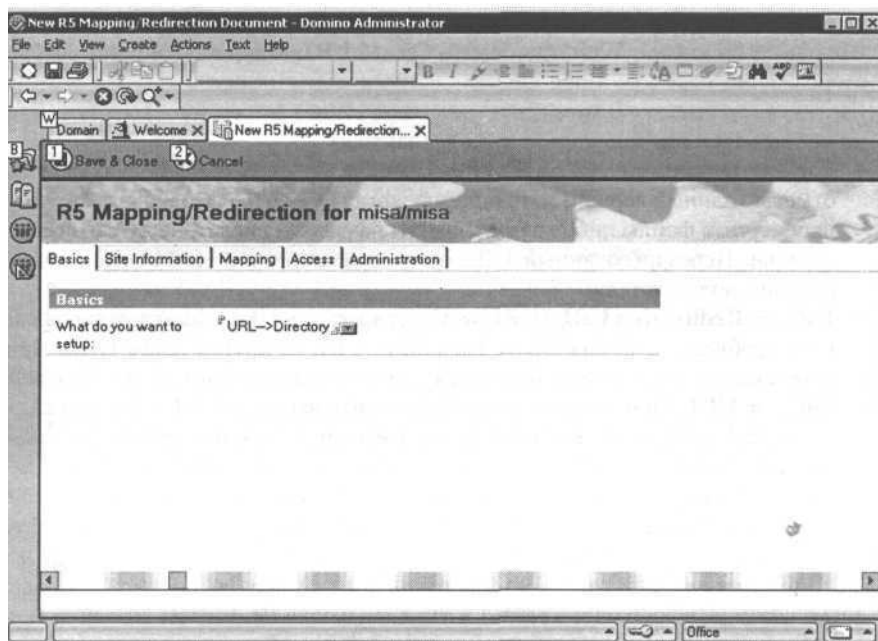


Рис. 15.10. Документ отображения/переадресации

Использование Web-областей

В Domino R5/6 можно создавать средства управления аутентификацией в домене Web для определенных дисков, каталогов и файлов на сервере Domino. Когда пользователь пытается получить доступ к одному из этих ресурсов, в диалоговом окне аутентификации

выводится текстовая строка, указанная в документе Web-области (Web realm document). После того как пользователь предоставляет свой сертификат, браузер с помощью этой области устанавливает, какие сертификаты следует отправлять вместе с URL в ответ на последующие запросы, а какие - занести в кэш-память, чтобы избежать повторной аутентификации при запросах к тем же ресурсам.

Кроме того, строка области применяется ко всем подкаталогам переадресованного пути, кроме случаев, когда этот подкаталог обращается к собственному документу Web-области. Важно, что в области, которая не определена для конкретного пути, сам путь будет служить Domino в качестве строки Web-области.

Сформировать документ Web-области достаточно просто:

1. В Domino Administrator выберите сервер или виртуальный сервер, на котором нужно создать область Web.
2. Откройте серверный документ или документ виртуального сервера и щелкните по кнопке **Web**.
3. Выберите **Create realm** (Создать область).
4. Заполните следующие поля документа Web-области (рис. 15.11):
 - **IP Address** (IP-адрес) - IP-адрес виртуального сервера (необходимо только при применении виртуального сервера);
 - **Path** (Путь) - путь, для которого определяется область. Это может быть диск, каталог или файл. Имейте в виду, что путь указывается относительно каталога данных Domino;

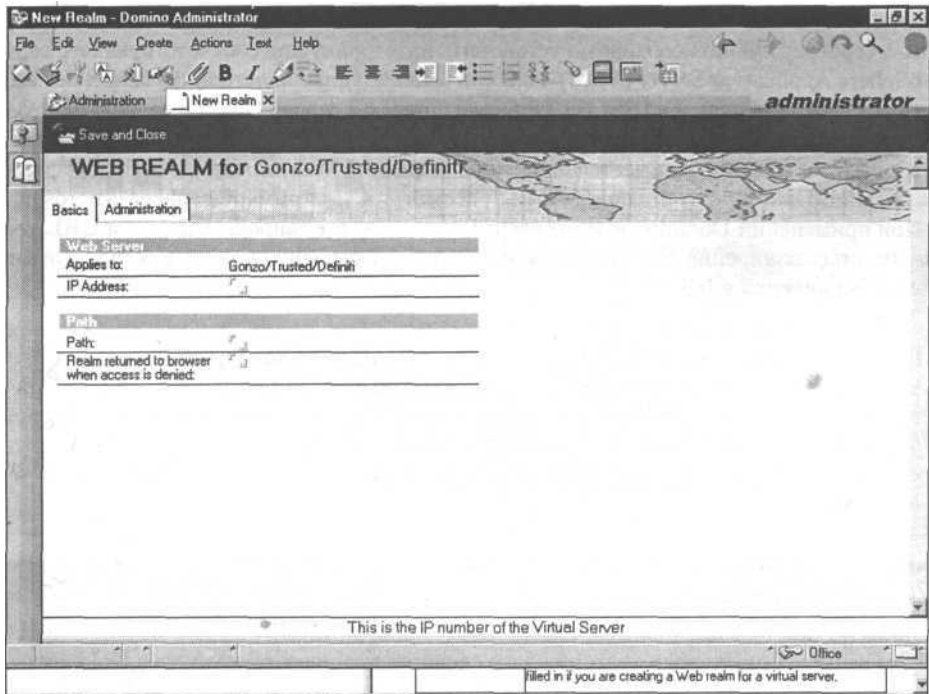


Рис. 15.11. Документ Web-области

- **Realm returned to browser when access is denied** (Область, отображаемая в браузере при отказе в доступе). Введите текстовую строку, указывающую место на сервере. Она будет появляться в окне аутентификации браузера при неверной аутентификации.

Сохраните новый документ Web-области

Сохранив новый документ Web-области, перезагрузите сервер, чтобы установленные параметры вступили в силу. Это можно сделать либо на консоли сервера, либо на удаленной консоли с помощью команды `tell http restart`.

Использование HTTP-стека Microsoft IIS

Одним из наиболее полезных (и замечательных) новых средств в R5/6 является возможность использования Web-сервера Microsoft IIS (Internet Information Server) для обработки запросов к содержимому Domino. Эта модель имеет два преимущества. Во-первых, она позволяет применять существующую инфраструктуру и навыки. Во-вторых, когда пользователь взаимодействует с приложениями Domino, системы безопасности IIS и Domino функционируют совместно, чтобы обеспечить высокую защищенность данных, хранящихся в базах Domino. В версии R6 сохранена поддержка программного Web-сервера Microsoft IIS, но основной моделью стало взаимодействие сервера Domino (как окончательного заднего сервера) с сервером IBM HTTP Server (IHS) в качестве окончательного переднего сервера. Для этого в сервере Domino необходимо установить надстройку для соответствующего сервера WebSphere Application Server (WAS) 4.0.3 или выше. Данная надстройка распознает запросы как к серверу IIS, так и к IBM HTTP Server, причем в сервер Domino передаются только касающиеся его запросы (например, для доступа к одной из баз данных), в то время как остальными запросами занимается окончательный передний Web-сервер. Совместное функционирование Domino с Web-сервером мы рассмотрим на примере сервера Microsoft IIS.

При применении Domino for IIS сервер IIS передает все запросы к адресам URL, содержащим .nsf (расширение файлов баз данных Domino), серверу Domino, а остальные запросы обрабатываются в IIS.

При использовании Domino for IIS отключите серверную задачу HTTP

Чтобы использовать Domino for IIS, сервер Domino должен работать, пока загружено расширение Domino ISAPI. В этой модели могут быть запущены все серверные задачи (кроме HTTP - она начнет конфликтовать с Domino ISAPI), которые будут обслуживать клиентов Notes и выполнять другие функции, такие как маршрутизация почты, NNTP и репликация.

Средства, поддерживаемые Domino for US

Domino for IIS обеспечивает много средств, поддерживаемых службой Domino HTTP. В этом разделе представлен краткий обзор средств Domino, совместимых с Domino for IIS:

- О средства Web-приложений - поддерживаются все, имеющиеся в Domino Designer;
- О защита баз данных - поддерживаются все средства защиты баз данных Domino;

- О соединения и регистрация - IIS обрабатывает сетевые соединения и регистрацию запросов к серверу, следовательно, эти средства на сервере Domino не поддерживаются;
- О фильтры функций API для Web-сервера Domino не поддерживаются;
- О документы конфигурации Web (Web Configuration document) - параметры, такие как защита файлов, виртуальный сервер, отображение/перееадресация URL, которые определяются в документах конфигурации Web, не поддерживаются;
- О Servlet Manager (Менеджер сервлетов) - Domino Servlet Manager в Domino for IIS не поддерживается. При необходимости такой тип деятельности реализуется с помощью других продуктов, в частности IBM WebSphere Application Server;
- О ICM (Internet Cluster Manager - менеджер кластеров Internet) сервера Domino не поддерживается. Вместо него можно воспользоваться менеджером кластеров компании Microsoft;
- О параметры серверного документа - Domino for IIS не поддерживает параметры, имеющиеся в серверном документе Domino для задачи HTTP. Поддерживаемые средства перечислены в табл. 15.1.

Таблица 15.1. Поддерживаемые параметры серверного документа

Расположение	Параметр
Вкладка Security (Безопасность)	Internet server Authentication (Аутентификация сервера Internet)
Ports\Internet Ports\Web	TCP/IP port status (Состояние порта TCP/IP) Authentication options (Параметры аутентификации) Name & Password (Имя и пароль) Anonymous (Анонимные пользователи)
Internet Protocols\HTTP	Allow HTTP clients to browse databases (Разрешить HTTP-клиентам просматривать базы данных)
Internet Protocols\Domino	<HTTP Sessions settings> (Параметры сеансов HTTP)
Web Engine	<POST Data settings> (Параметры передачи данных) <Memory Cache settings> (Параметры кэш-памяти) <Character Set Mapping settings> (Параметры отображения наборов символов) Default lines per view page (Число строк на страницу вида, установленное по умолчанию) Maximum lines per view page (Максимальное число строк на страницу вида) Default search results (Число возвращаемых результатов поиска, установленное по умолчанию) Maximum search results (Максимальное число возвращаемых результатов поиска) Make this site accessible to crawlers (Сделать этот сайт доступным для «червяков»)

Для использования Domino for IIS могут потребоваться некоторые изменения

Приложения, которые обращаются не к базам данных Domino, а к таким ресурсам, как, например, HTML, сценарии CG и серверные приложения (сервлеты) Java, возможно, требуют внесения определенных изменений при работе с Domino for IIS.

Допустимо применять защиту файловой системы NT

Можно защитить системные файлы средствами операционной системы NT.

Как видите, Domino for IIS достаточно мощное и перспективное средство. Если ваша организация постоянно применяет Microsoft IIS и вы захотите с его помощью обслуживать Domino, надо настроить Domino for Microsoft IIS. Последующий материал данного раздела посвящен рассмотрению необходимых процедур.

Минимальные требования к Domino for IIS

Перед началом настройки нужно убедиться, что выполняются минимальные требования, необходимые для запуска Domino for IIS:

- О Microsoft Windows NT 4.0 с Service Pack 4 (поддерживаются платформы Intel и DEC Alpha);
- О Microsoft Internet Information Server (IIS) 4.0;
- О хорошее знание MMC (Microsoft Management Console - консоль управления Microsoft). MMC - это инструмент, который позволяет настраивать IIS. Более подробно о MMC можно прочитать в документации по Windows NT или на сайте <http://www.microsoft.com/NTServer/management/Techdetails/ProdArchitect/mmc.asp>;
- О рабочий сервер Domino R5/6;
- О файл notes.ini, находящийся либо в каталоге программ Domino, либо в каталоге, заданном серверной переменной PATH. Вместо этого можно включить полный путь к ID-файлу сервера в параметр ServerKeyEilename файла notes.ini;
- О ID-файл сервера, не настроенный на использование паролей, поскольку не удастся ввести пароль, когда IIS запускает расширение ISAPI сервера Domino;
- О изменение доступа к файлам в NT для каталога Domino и всех подкаталогов учетных записей пользователей, которые будут обращаться к Domino for IIS.

Настройка IIS для поддержки Domino for IIS

Если требования, перечисленные выше, выполнены, значит, все готово для настройки Domino for IIS. Необходимо начать с настройки расширения Domino ISAPI для IIS, чтобы при запросах URL в стиле Domino (с расширением файлов .nsf) IIS-сервер знал, как их обрабатывать. Это обеспечивается с помощью консоли MMC. Необходимы следующие действия:

1. Запустите консоль MMC и откройте окно MMC для своего Web-сайта (рис. 15.12).
2. Щелкните правой кнопкой мыши по значку Web-сайта IIS и выберите **Properties** (Свойства) - рис. 15.13.
3. Выберите вкладку **Home Directory** (Домашний каталог) - рис. 15.14.
4. Щелкните по кнопке **Configuration** (Конфигурация). Откроется окно **Application Configuration** (Конфигурация приложения) - рис. 15.15.
5. Щелкните по кнопке **Add** (Добавить), чтобы вывести окно **Add/Edit Application Extension Mapping** (Добавить/редактировать отображение расширения приложения) - рис. 15.16.

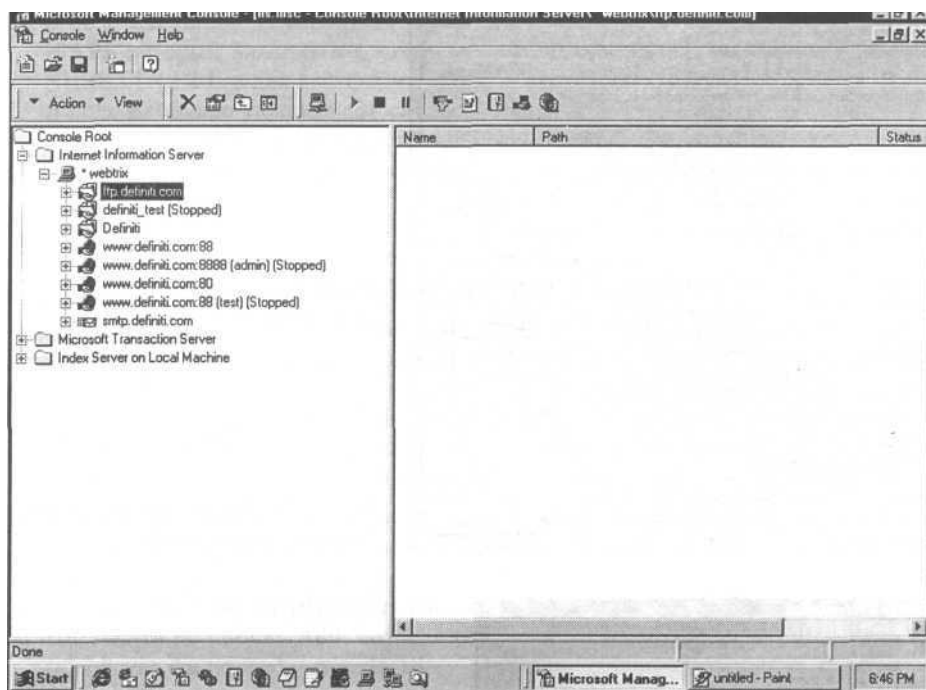


Рис. 15.12. Microsoft Management Console

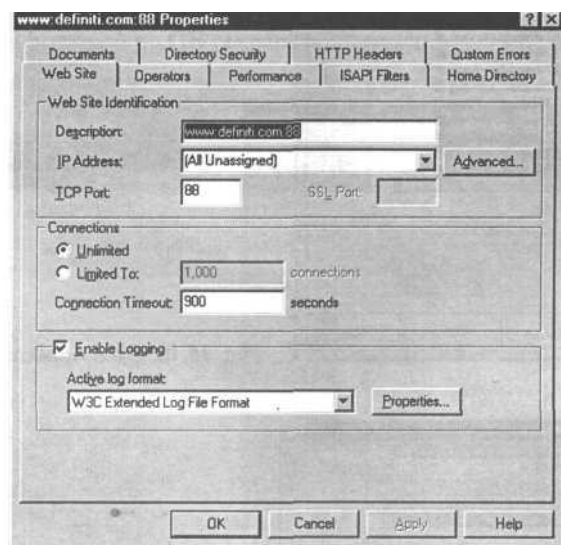


Рис. 15.13. Страница свойств Web-сайта IIS

6. В поле **Executable** (Выполняемое) введите полный путь и имя файла расширения ISAPI, который находится в каталоге Domino и называется для платформы Intel NIISEXTN.DLL, а для платформы Alpha - AIISEXTN.DLL.
7. В поле **Extension** укажите .nsf как расширение файлов баз данных Domino. Это покажет серверу IIS, что запрашиваются ресурсы Domino.
8. В поле **Method Exclusions** (Исключаемые методы) перечислите методы, не поддерживаемые Domino for IIS, - PUT и DELETE.
9. Установите флажок **Script Engine** (Двигатель сценариев) и сбросьте флажок **Check the File Exists** (Проверять существование файла).
10. По окончании щелчком по ОК сохраните изменения.

Кроме того, следует настроить фильтр расширений IIS, чтобы убедиться, что пользователи смогут правильно аутентифицироваться сервером Domino, и разрешить использование команды Domino /?OpenServer (поскольку для этой команды расширение .nsf не входит в адрес URL), если пользователи должны иметь возможность просматривать базы данных. Как упоминалось ранее, применение этого параметра не рекомендуется, поскольку в таком случае хакеры сумеют получить доступ к базам данных на вашем сайте.

11. Запустите консоль MMC и отройте файл MMC для Web-сайта (см. рис. 15.12).
12. Щелкните правой кнопкой мыши по значку Web-сайта IIS и выберите **Properties** (см. рис. 15.13).
13. Выберите вкладку **ISAPI Filters** (Фильтры ISAPI) - рис. 15.17.
14. Щелкните по кнопке **Add**, которая открывает диалоговое окно **Filter Properties** (Свойства фильтров) - рис. 15.18.
15. В поле **Filter Name** (Имя фильтра) введите любой текст, описывающий IIS-фильтр.
16. В поле **Executable** укажите полный путь и имя файла фильтра. Файл находится в каталоге Domino и называется NIISFILT.DLL (для платформы Intel) или AIISFILT.DLL (для платформы Alpha).
17. По окончании щелчком по ОК сохраните изменения.

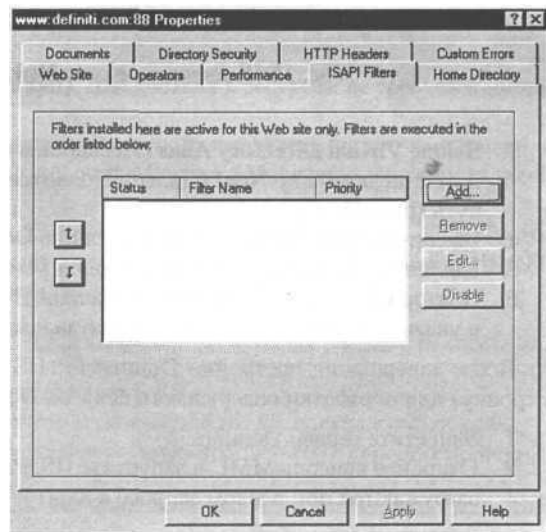
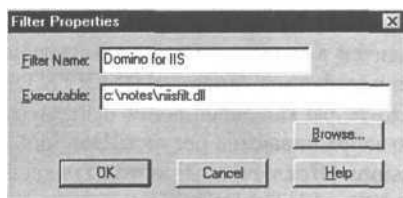
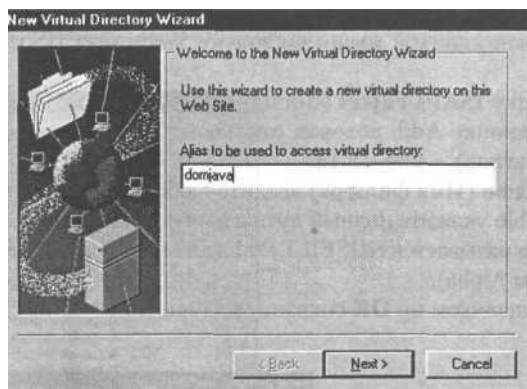


Рис. 15.17. Вкладка ISAPI Filters

Рис. 15.18. Диалоговое окно **Filter Properties**

Чтобы сервер Domino правильно загружал апплеты и значки Java, следует задать место их расположения:

1. Запустите консоль MMC и откройте окно MMC для Web-сайта (см. рис. 15.12).
2. Щелкните правой кнопкой мыши по значку Web-сайта IIS и выберите **New => Virtual Directory** (Новый => Виртуальный каталог). Откроется диалоговое окно **New Virtual Directory Wizard** (Мастер создания виртуальных каталогов) - рис. 15.19.

Рис. 15.19. Диалоговое окно **New Virtual Directory Wizard**

3. В поле **Virtual Directory Alias** (Псевдоним виртуального каталога) введите `domjava`. Затем щелкните по **Next** (Далее). Появится окно, в котором необходимо определить путь (рис. 15.20).
4. Введите полный путь к каталогу апплетов Domino (обычно `c:\notes\data\domino\java`).
5. Щелкните по **Finish** (Готово). Изменять установленные параметры доступа не нужно.
6. Повторите шаги 2-5 для файлов значков. В поле **Virtual Directory Alias** задайте `icons` и укажите полный путь к каталогу со значками (обычно `c:\notes\data\domino\icons`).

После завершения настройки Domino for IIS можно запускать это расширение (настройку) для обработки содержимого сервера Domino:

1. Запустите сервер Domino.
2. Откройте консоль MMC и запустите IIS. Расширения Domino for IIS автоматически загружаются при первом запросе к адресу URL сервера Domino.

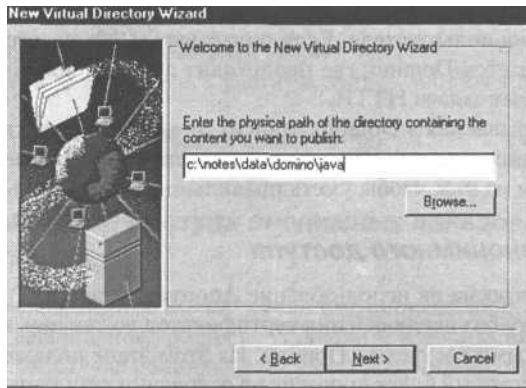


Рис. 15.20. Введите путь

Если вы захотите остановить службу Domino for IIS, выведите на экран MMC и остановите IIS.

Обзор защиты Domino for US

Последний элемент в мозаике Domino for IIS – настройка системы защиты, что позволяет удостовериться в надежной защите содержимого баз данных Domino. Domino for IIS имеет два уровня защиты: защита IIS и защита Domino (это достаточно удобно). Сначала IIS пытается проверить права пользователя в каталоге Windows NT. Если такая проверка проходит успешно, сертификат пользователя передается серверу Domino для последующего контроля с помощью алгоритмов Domino.

Поскольку система защиты Domino детально рассмотрена в главе 10, ниже мы остановимся только на средствах защиты и параметрах настройки системы IIS.

На момент написания данной книги Web-сервер IIS поддерживал четыре метода аутентификации пользователей:

- **Anonymous access** (Анонимный доступ). Для доступа к ресурсам не требуется имени пользователя и пароля;
- **Basic authentication** (Базовая аутентификация). Пользователь вводит имя и пароль и проверяется с помощью Security Account Manager (Менеджер учетных записей системы безопасности);
- **Windows NT Challenge/Response** (Запрос и подтверждение Windows NT). Протокол Microsoft поддерживается только между Microsoft Internet Explorer и IIS/NT. С другими браузерами этот протокол работать не будет;
- **Secure Sockets Layer (SSL)**.

Конфликт между задачей HTTP сервера Domino и IIS

Не загружайте задачу HTTP сервера Domino во время работы IIS, поскольку IIS обрабатывает запросы к Domino и это вызывает конфликт между задачей HTTP сервера Domino и US.

Для управления доступа к ресурсам, управляемым и обслуживаемым сервером IIS, требуется аутентификация пользователя. Если пользователь обращается к ресурсам Domino, его сертификат передается Domino, где происходит аутентификация по тем же алгоритмам, которые применяет задача HTTP.

Информация, передаваемая в Domino, зависит от методов аутентификации, используемых IIS. В последующих разделах описаны все методы, поддерживаемые IIS. Необходимо разобраться с каждым из них, чтобы уметь правильно их применять.

Использование анонимного доступа

Когда защита IIS настроена на использование **Anonymous access**, Web-пользователи могут обращаться к сайту без предъявления сертификатов до тех пор, пока они не пытаются работать с защищенными ресурсами Domino. На этом этапе пользователь должен предоставить сертификат, который будет проверен на основании стандартных процедур Domino.

Если вы настраиваете IIS на Anonymous access, обратите внимание на следующее:

- О Web-пользователю не нужна учетная запись в Windows NT;
- О Web-пользователь, обращающийся к закрытым ресурсам Domino, должен иметь учетную запись Domino (персональный документ в каталоге Domino) и пароль Internet;
- О переменные CGI AUTH_TYPE и REMOTEUSER будут недоступны для приложений, поскольку IIS рассматривает пользователя как анонимного.

Использование базовой аутентификации

Когда на сервере IIS включена базовая аутентификация, сертификат пользователя сначала сравнивается с учетными записями Windows NT. Если находится нужная учетная запись и она разрешает доступ к запрашиваемому ресурсу, доступ предоставляется. В противном случае в доступе отказывается. При условии, что в IIS установлена только базовая аутентификация, пользователь должен предъявить соответствующие реквизиты (в предположении, что для анонимных пользователей доступ закрыт). Имя пользователя, прошедшего аутентификацию, IIS передает в Domino, где пользователь аутентифицируется с помощью методов службы HTTP сервера Domino.

Средства каталогов

Все средства каталогов, доступные для задачи HTTP, такие как ШАР-каталог и множественные каталоги Domino, доступны и для IIS.

Для базовой аутентификации в Domino for IIS не требуется пароль Internet

Если в IIS установлена лишь базовая аутентификация, то пользователь аутентифицируется только на основании учетной записи Windows NT, а не по паролю Internet, хранящемуся в каталоге Domino.

Если вы настраиваете сервер IIS на базовую аутентификацию, обратите внимание, что:

- О доступ для анонимных пользователей закрыт;
- О Web-пользователь должен иметь учетную запись Windows NT и учетную запись Domino;
- О Domino игнорирует пароль Internet пользователя.

Совместное применение доступа анонимных пользователей и базовой аутентификации

Когда требуется, чтобы анонимные пользователи имели право доступа к общим ресурсам, но не могли открыть защищенные ресурсы, установите и анонимный доступ, и базовую аутентификацию. В этом случае пользователь сумеет получить доступ к открытым ресурсам без аутентификации. Однако если он попытается открыть защищенные ресурсы, то должен будет аутентифицироваться.

При настройке IIS на совместное применение доступа анонимных пользователей и базовую аутентификацию важно учитывать следующее:

- О доступ анонимных пользователей разрешен к открытым (незащищенным) ресурсам Domino и IIS;
- О если пользователь обращается к защищенным ресурсам, он должен предоставить реквизиты, которые проверяются в IIS и Domino согласно алгоритмам базовой аутентификации.

Использование Windows NT Challenge/Response

Windows NT Challenge/Response - разработанный компанией Microsoft протокол, который в настоящее время поддерживается только в браузере Internet Explorer (IE). Когда Web-пользователь обращается к сайту, IE автоматически передает текущее регистрационное имя (имя входа) пользователя в IIS. IIS сравнивает это имя с учетной записью NT на IIS-сервере. При обращении пользователя к ресурсам Domino IIS передает NT-имя пользователя на сервер Domino, который аутентифицирует его в соответствии с принятыми алгоритмами.

Если вы работаете только с Windows NT Challenge/Response, не забывайте:

- О к сайту можно обратиться лишь из браузера IE;
- О все Web-пользователи должны иметь учетную запись NT, чтобы получить доступ к любым ресурсам на сайте;
- О каждое имя в учетной записи NT необходимо добавить в персональный документ пользователя в каталоге Domino как псевдоним;
- О при любом запросе браузер IE автоматически передает имя учетной записи NT, делая невозможным доступ анонимных пользователей;
- О Domino игнорирует пароли Internet, рассматривая лишь имя учетной записи NT. Достоверность пользователя устанавливается только в IIS.

Совместное использование Windows NT Challenge/Response и базовой аутентификации

Если вы совместно используете Windows NT Challenge/Response и базовую аутентификацию, помните:

- О пользователи браузера IE аутентифицируются с помощью Windows NT Challenge/Response;
- О пользователи, работающие со всеми остальными типами браузеров, аутентифицируются посредством алгоритмов базовой аутентификации.

Совместное использование доступа анонимных пользователей, базовой аутентификации и Windows NT Challenge/Response

Если вы активизируете все три метода, для вас существенно, что:

- О при запросах к открытым ресурсам разрешен доступ анонимным пользователям;
- О пользователи браузера IE аутентифицируются с помощью Windows NT Challenge/Response;
- О пользователи, применяющие все остальные типы браузеров, аутентифицируются посредством алгоритмов базовой аутентификации.

Использование SSL

IIS-сервер, на котором включен протокол SSL, работает с реальным SSL-соединением. Когда Web-пользователь предоставляет клиентские реквизиты, IIS передает сертификат в Domino, а Domino уже аутентифицирует пользователя на основании этого сертификата (см. главу 10).

Настройка защиты Domino for IIS

Для настройки системы защиты сервера IIS выполните следующие действия:

1. Запустите консоль MMC и откройте Web-сайт (см. рис. 15.12).
2. Щелкните правой кнопкой мыши по значку Web-сайта IIS и выберите **Properties** (см. рис. 15.13).
3. Выведите на экран вкладку **Directory Security** (Защита каталога) - рис. 15.21.
4. Щелкните по кнопке **Edit** (Редактировать), чтобы открыть окно **Authentication Methods** (Методы аутентификации), в котором устанавливаются выбранные методы аутентификации - рис. 15.22.
5. Укажите необходимые методы аутентификации. Если нужно точно настроить порядок работы методов доступа анонимных пользователей и базовой аутентификации, щелкните по кнопке **Edit** и внесите необходимые изменения.
6. Щелкните по ОК.

Точная настройка

Установив и настроив свой сервер Domino, вы, возможно, захотите оценить его производительность. Domino R5/6 предоставляет множество новых средств наблюдения, позволяющих

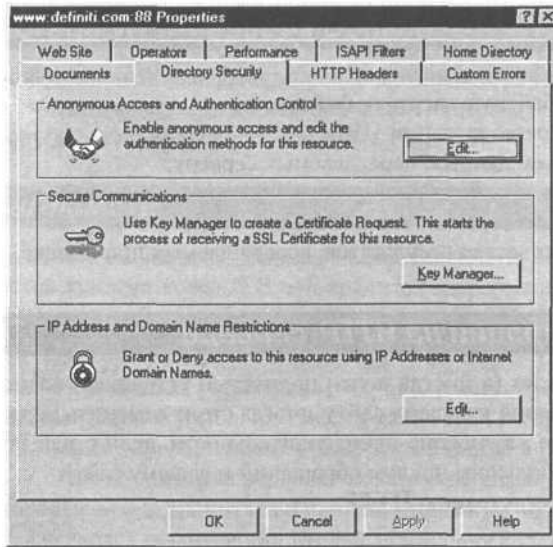


Рис. 15.21. Вкладка Directory Security

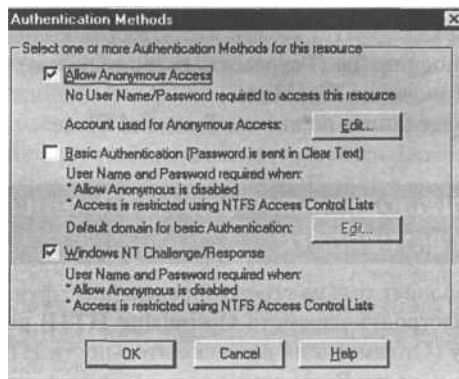


Рис. 15.22. Диалоговое окно Authentication Methods

контролировать и настраивать все параметры сервера Domino. В этом разделе внимание сконцентрировано на настройке задачи HTTP этого сервера. Более подробно об оптимизации, настройке и контроле производительности сервера Domino рассказывается в главах 18 и 19. Дополнительно можно посмотреть файл справки Domino Administration Help (help5_admin.nsf или help6_admin.nsf) или обратиться на сайт www.notes.net.

Для улучшения производительности и времени отклика сервера выполните несколько действий, связанных с точной настройкой HTTP:

- О отмените регистрацию на HTTP-сервере;
- О оптимизируйте производительность HTTP-сервера на основании его активности;
- О создайте кластер Web-сервера Domino;

- настройте кэш-память;
- определите сетевые тайм-ауты;
- укажите число потоков сервера;
- установите побайтную загрузку файлов;
- задайте метод переадресации URL;
- ограничьте объем данных, передаваемых серверу;
- воспользуйтесь прогрессивной разверткой при выводе файлов JPEG;
- ограничьте число строк, отображаемых на виде;
- ограничьте количество результатов, возвращаемых при поиске.

Отмена регистрации на HTTP-сервере

Хотя это сильно сужает (а иногда почти полностью устраняет) возможность отслеживания и анализа обращений к вашему сайту, иногда стоит отменить регистрацию HTTP, чтобы получить весомое улучшение производительности, если с ней возникают проблемы в связи со слишком большим числом обращений к вашему сайту.

Чтобы отменить регистрацию HTTP:

1. Откройте каталог Domino и выберите вид **Servers**.
2. Укажите настраиваемый сервер.
3. Вызовите серверный документ и щелкните по вкладке **Internet Protocols** (Протоколы Internet).
4. Выведите на экран вкладку HTTP, чтобы настроить конфигурацию задачи HTTP.
5. В разделе **Enable Logging To** (Разрешить регистрацию в) установите в полях **Log Files** и **Domlog.nsf** значение **Disabled**.
6. На панели **Actions** щелкните по кнопке **Save and Close**.

Оптимизация производительности HTTP-сервера

на основании его активности

Если сервер Domino выполняет только строго определенные функции, такие как маршрутизация почты, можно настроить параметр **Optimizing HTTP performance based on the following primary activity** (Оптимизация производительности HTTP-сервера с учетом основной деятельности) на вкладке **Basic** серверного документа, чтобы улучшить производительность сервера:

1. Откройте каталог Domino и выберите вид **Servers**.
2. Укажите сервер, который нужно настроить.
3. Откройте серверный документ и в нем вкладку **Basics** (появляется по умолчанию).
4. В поле **Optimizing HTTP performance based on the following primary activity** укажите необходимое значение: **Web Mail** (Почта Web), **Web Applications** (Web-приложения), **Both Mail and Web** (Почта и приложения) и **Advanced** (Дополнительно).
5. На панели **Actions** щелкните по **Save and Close**.

Создание кластера Web-сервера Domino

Удается получить значительный выигрыш в производительности, установив кластер серверов Domino, что приводит к выравниванию нагрузки и повышает надежность. Этот достаточно сложный вопрос детально рассматривается в главе 20.

Настройка кэш-памяти

Оптимальное время ответа на запросы Domino обеспечивается с помощью кэш-памяти, которая также известна как кэш команд. В ней хранится информация о командах HTTP, базах данных и пользователях, благодаря чему реализуется быстрый вызов этой информации. Domino R5 в настоящее время поддерживает следующие параметры кэш-памяти:

- О **Maximum cached commands** (Максимальное число кэшируемых команд, только в R5). Устанавливается максимальное число команд HTTP-сервера для анонимных пользователей. Процесс преобразования элементов Domino в HTML занимает определенное время. Этот параметр определяет количество команд (требующих преобразования), которые могут храниться в памяти, чтобы при повторном обращении к команде она вызывалась немедленно. По умолчанию - 128;
- О **Maximum cached designs** (Максимальное число кэшируемых проектных элементов). Задается максимальное количество кэшируемых элементов проектирования. Когда открывается база данных, Domino отображает каждый элемент на соответствующий идентификационный номер. Данный параметр указывает количество элементов, которые могут храниться в памяти, чтобы при повторном обращении к элементу он вызывался немедленно;
- О **Maximum cached users** (Максимальное число кэшируемых пользователей). После того как пользователь успешно аутентифицируется, Domino кэширует его имя, пароль и группу, членом которой он является. Параметр позволяет управлять числом пользователей, кэшируемых Domino. По умолчанию - 64;
- О **Cached user expiration interval** (Время хранения кэшированных пользователей). Назначается промежуток времени (в секундах), в течение которого Domino хранит информацию о пользователе в кэш-памяти. Необходимо периодически удалять такую информацию, чтобы пользователю приходилось снова аутентифицироваться. По умолчанию - 120 секунд.

Чтобы настроить параметры кэш-памяти:

1. Откройте каталог Domino и выберите вид **Servers**.
2. Укажите сервер, который нужно настроить.
3. Выведите на экран серверный документ и вкладку **Internet Protocols** (Internet-протоколы).
4. Откройте вкладку **Domino Web Engine** (рис. 15.23).
5. Перейдите в раздел **Memory Caches** и измените параметры по своему усмотрению.
6. На панели **Actions** щелкните по **Save and Close**.

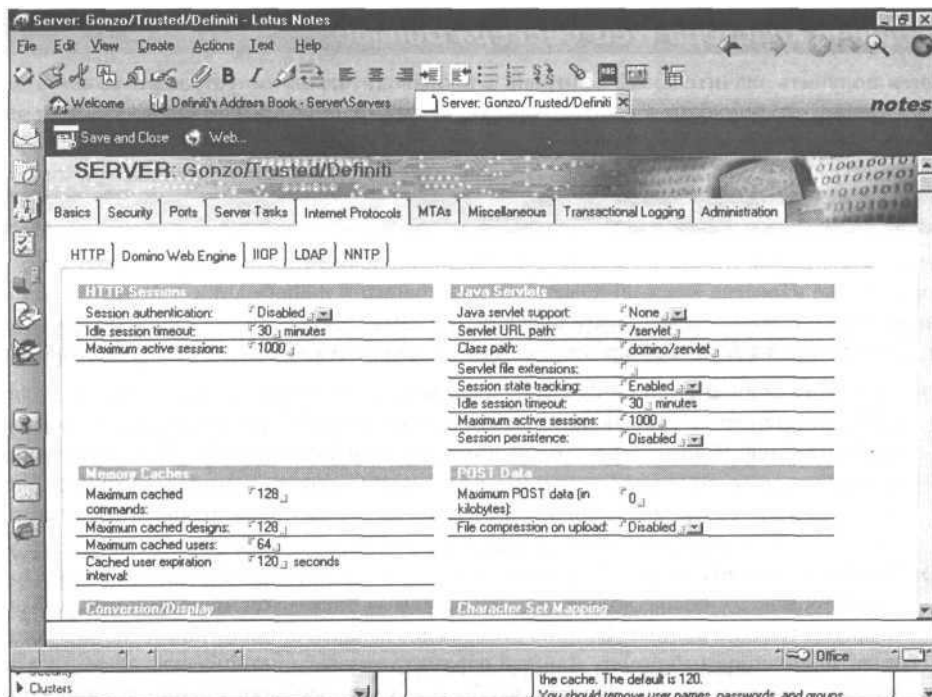


Рис. 15.23. Вкладка **Domino Web Engine** серверного документа

Наблюдение за параметрами кэш-памяти

Для наблюдения за влиянием параметров кэш-памяти на сервер Domino откройте **Domino => Cache statistics** (Domino => Статистика кэша) в клиенте Domino Administration.

Настройка сетевых тайм-аутов

Нерабочие сеансы сильно расходуют ресурсы сервера и могут стать причиной отказов при вызове служб. Domino предоставляет возможность задавать временные ограничения для большинства видов деятельности, что увеличивает производительность сервера и помогает сделать сервер доступным всегда. Domino R5/6 поддерживает установку значения нескольких тайм-аутов, которые были рассмотрены выше при описании вкладок **Timeouts**, **R5 Timeouts** и **Web Agents** для протокола HTTP.

Для настройки тайм-аутов HTTP-сервера выполните следующие действия:

1. Откройте каталог Domino и укажите вид **Servers**.
2. Выберите настраиваемый сервер.
3. Откройте серверный документ и щелкните по вкладке **Internet Protocols**.

4. Щелкните по вкладке **HTTP**.
5. В разделах **Timeouts**, **R5 Timeouts** и **Web Agents** измените параметры по своему усмотрению.
6. Щелкните по **Save and Close**.

Настройка числа потоков сервера

Установленное число потоков определяет, сколько пользователей может одновременно работать с сервером. При достижении максимального числа активных потоков новые запросы помещаются в очередь до освобождения потоков. Увеличение числа потоков может значительно повысить производительность.

Domino R5/6 поддерживает следующие параметры настройки управления потоками сервера:

- **Maximum requests over a single connection** (Максимальное число запросов во время одного соединения). Здесь задается максимальное число одновременных запросов, которые принимает сервер от одного браузера. Данный параметр касается браузеров, поддерживающих HTTP 1.1 или более поздние версии. По умолчанию - 1. Увеличение этого числа может значительно повысить производительность;
- **Number of active threads** (Число активных потоков). Поле определяет число потоков, которые можно одновременно запустить на сервере Domino. По умолчанию - 40. Если сервер достаточно мощный, то увеличение данного числа может значительно повысить производительность;
- **Minimum active threads** (Минимальное число активных потоков). Параметр остался только для обратной совместимости.

Чтобы настроить параметры потоков HTTP-сервера:

1. Откройте каталог Domino и укажите вид **Servers**.
2. Выберите сервер, который нужно настроить.
3. Откройте серверный документ и в нем вкладку **Internet Protocols**.
4. Щелкните по вкладке **HTTP**.
5. В разделе **Basics** установите соответствующие значения для описанных выше параметров.
6. Сохраните изменения и закройте документ.

Побайтная загрузка файлов

Domino R5/6 поддерживает побайтную загрузку файлов (загрузка файлов по частям) для Web-браузеров, обеспечивающих работу с протоколом HTTP 1.1 или более поздних версий. При побайтной загрузке браузер отслеживает процесс загрузки файла и после разрыва соединения загрузка продолжается с момента сбоя. Если этот режим отключен, пользователю приходится заново загружать файл целиком.

Для работы побайтной загрузки вложенные файлы не должны быть сжаты Notes (необходимо отключить параметр **Compress**).

Побайтная загрузка

Если Web-клиент поддерживает побайтную загрузку, Domino автоматически использует данное средство. К сожалению, на момент написания настоящей книги имеется только небольшое количество программных продуктов, поддерживающих это замечательное средство, в частности Adobe Acrobat Reader 3.01.

Задание метода переадресации URL

Чтобы управлять временем, необходимым для обработки ссылок на другие серверы, можно изменить параметр **Redirect to resolve external links** (Переадресация для обработки внешних ссылок). Необходимо включить этот режим на серверах, осуществляющих поиск в домене, и на серверах, для которых нужно обрабатывать ссылки на другие серверы. Имеются следующие варианты:

- **Disabled** (Отключено). Установлено по умолчанию. Сервер не принимает команды Redirect URL и при выполнении поиска в домене не генерирует их;
- **By Server** (Серверы по очереди). Чтобы искать имя сервера, указанного в URL, в репликах каталога Domino данного сервера, задайте такой режим. При этом сервер будет просматривать поля **Host names** и **Fully qualified Internet host name**.
- **By Database** (Базы данных по очереди). Самый медленный метод, поскольку поиск проводится на всех доступных серверах. Domino пытается найти базу данных в локальном каталоге сервера, а затем в каталоге домена.

Для настройки параметра **Redirect to resolve external links** выполните следующие действия:

1. Откройте каталог Domino и укажите вид **Servers**.
2. Выберите настраиваемый сервер.
3. Откройте серверный документ и щелкните по вкладке **Internet Protocols**.
4. Выведите на экран вкладку **Domino Web Engine**.
5. Перейдите в раздел **Conversion/Display** (Преобразование/показ) и измените параметры по своему усмотрению.
6. Сохраните и закройте документ.

Ограничение объема данных, передаваемых серверу

Многие Web-дизайнеры знают, что команда POST протокола HTTP позволяет браузеру отправлять данные на сервер. В Domino R5/6 есть возможность определить объем данных, который браузер способен передать серверу, а также установить сжатие файлов, загружаемых на сервер. Если настроить следующие параметры, то пользователи не сумеют посылать на сервер слишком большие объемы данных:

- **Maximum POST data** (Максимальное количество передаваемых данных). Назначается максимальный объем данных (в килобайтах), которые браузеру разрешается передать серверу. Если браузер превышает этот объем, появляется сообщение об ошибке. По умолчанию установлено значение 0 - предел не задан;
- **File compression on upload** (Сжатие файла при загрузке). Указывается, должны ли сжиматься файлы перед сохранением их в базе данных. По умолчанию отключено.

Побайтная загрузка

Помните, что, когда пользователь работает с браузером, поддерживающим побайтную загрузку, этот параметр должен быть отключен. Сжатые файлы нельзя загружать побайтно.

Чтобы настроить параметры передачи данных:

1. Откройте каталог Domino и укажите вид **Servers**.
2. Выберите настраиваемый сервер.
3. Вызовите серверный документ и перейдите на вкладку **Internet Protocols**.
4. Щелкните по вкладке **Domino Web Engine**.
5. В разделе **Post Data** (Передаваемые данные) измените параметры настройки по своему усмотрению.
6. Сохраните и закройте документ.

Использование чересстрочной/прогрессивной развертки изображений

Если в своих Web-приложениях вы используете изображения, можно обеспечить более быстрое их появление на экране, задав чересстрочный вывод для GIF-изображений и прогрессивный вывод для JPEG-изображений.

Чтобы включить эти параметры:

1. Откройте каталог Domino и выберите вид **Servers**.
2. Задайте настраиваемый сервер.
3. Выведите на экран серверный документ и перейдите на вкладку **Internet Protocols**.
4. Щелкните по вкладке **Domino Web Engine**.
5. В разделе **Display Conversion** укажите для параметров **Interlaced Rendering** (Чересстрочная развертка) и **Progressive Rendering** (Прогрессивная развертка) значение **Enabled**.
6. Сохраните и закройте документ.

Ограничение числа строк, отображаемых на виде

В Domino R5/6 можно установить, сколько строк будет отображаться Web-пользователю, открывающему вид. Имеется два параметра, управляющих числом строк:

- **Default lines per page** (Число строк на страницу, установленное по умолчанию) определяет число строк, выводимое в браузере, когда в URL не указан параметр счета.
 - Введите число от 1 до значения, указанного в поле **Maximum lines per page**. По умолчанию - 30;
- **Maximum lines per page** (Максимальное число строк на страницу) задает максимальное число строк вида, когда в URL не установлен параметр счета. Если вы не хотите ограничивать число строк, введите 0 (число строк в этом случае зависит от возможностей браузера). По умолчанию принято 1000. Вероятно, хорошим значением является 100.

Для настройки параметров числа строк выполните следующие действия:

1. Откройте каталог Domino и укажите вид **Servers**.
2. Выберите настраиваемый сервер.
3. Вызовите серверный документ и перейдите на вкладку **Internet Protocols**.
4. Щелкните по вкладке **Domino Web Engine**.
5. В разделе **Display Conversion** установите значения по своему усмотрению.
6. Сохраните и закройте документ.

Два описанных выше параметра работают совместно и могут внести значительный вклад в увеличение производительности сервера. Если установить слишком маленькие значения, пользователи будут чаще обращаться к серверу, чтобы найти необходимые данные. При чрезмерно больших значениях серверу придется долго обрабатывать информацию, поэтому между запросами пользователей и ответами сервера возникнут длительные задержки.

Ограничение числа результатов поиска

Как и в случае числа отображаемых строк, можно ограничить количество документов, возвращаемых в результате поиска. Для этого существует два параметра:

- О **Default search result limit** (Ограничение числа результатов поиска, установленное по умолчанию). Указывается количество документов, которое выводится, если в URL не определен параметр SearchMax. По умолчанию - 250, но можно ввести любое число от 1 до значения, установленного в поле **Maximum search result limit**. Значение 0 говорит о том, что предел не задан;
- О **Maximum search result limit** (Максимальное число результатов поиска). Задается максимальное количество выводимых документов, если в URL не внесен параметр SearchMax. По умолчанию - 1000. Значение 0 показывает, что предел не задан. Лучше не назначать 0, поскольку это «поставит сервер на колени».

Чтобы настроить пределы результатов поиска:

1. Откройте каталог Domino и укажите вид **Servers**.
2. Выберите настраиваемый сервер.
3. Откройте серверный документ и перейдите на вкладку **Internet Protocols**.
4. Щелкните по вкладке **Domino Web Engine**.
5. В разделе **Display Conversion** установите значения по своему усмотрению.
6. Сохраните и закройте документ.

Установка чисел результатов

Пользователь может самостоятельно задать количество документов, отображаемых в результате поиска, с помощью параметра SearchMax в командах SearchSite и SearchView.

Устранение неполадок

Domino является достаточно сложным программным продуктом, так что, когда случаются неполадки, виной тому обычно оказывается не один фактор. Данный раздел посвящен рассмотрению нескольких общих проблем, характерных для HTTP-серверов, некоторых

инструментов, позволяющих выявить эти проблемы, и ряда других ресурсов, помогающих справляться с трудностями.

Проблемы доступа по протоколу HTTP

В следующих разделах описываются некоторые общие проблемы доступа на сервере Domino.

Анонимные пользователи не могут получить доступ к ресурсам

Существует несколько причин, по которым анонимные пользователи не могут получить доступ к ресурсам:

- О в серверном документе в поле **Allow anonymous HTTP connections** (Разрешить анонимные HTTP-соединения) установлено значение No, что заставляет пользователей проходить аутентификацию;
- О список ACL базы данных, к которой обращается пользователь, настроен так, что доступ для анонимных пользователей закрыт. Если в полях **Default** и **Anonymous** выбрано значение **No Access**, то каждый пользователь должен пройти аутентификацию;
- О ресурсы, к которым обращается пользователь, защищены на уровне формы, вида или документа, вследствие чего доступ для анонимных пользователей к ним закрыт.

Аутентифицированные пользователи не могут получить доступ к ресурсам

Такое положение возможно, если:

- О в поле **Maximum Internet name & Password access** (Максимальный доступ по имени и паролю Internet) базы данных установлено значение **No Access**. При этом доступ к базе данных из браузера получить нельзя. Проверьте вкладку **Advanced** в списке ACL базы;
- О список ACL ресурса (базы данных, вида, формы, документа) настроен неправильно, либо в ACL неточно задано имя данного пользователя или группы;
- О пользователь неверно ввел имя или пароль. Пользователи, обращающиеся к ресурсам Domino из браузера, должны указывать пароль, записанный в поле **Internet Password** своего персонального документа.

О

Пользователям приходится аутентифицироваться несколько раз для доступа к одному сайту

HTTP-сервер Domino использует модель аутентификации промышленного стандарта HTTP. Обращаясь к закрытым ресурсам, пользователь должен сразу предъявить реквизиты, которые затем кэшируются на основании Web-области, сообщаемой браузеру Domino.

Пользователь, аутентифицированный для определенной области, может получить доступ к любым ее ресурсам, включая ресурсы нижележащих областей. Однако при попытке обратиться к одноуровневому или вышестоящим областям он должен аутентифицироваться и в этих областях.

Данный принцип иллюстрируется следующим примером. Когда вы получаете доступ к www.difiniti.com, www.difiniti.com является областью высшего уровня. Остальные части

сайта, такие как Services (www.difiniti.com/services), Products (www.difiniti.com/products) и Opportunities (www.difiniti.com/opportunities), - нижележащие области.

Если пользователь сначала аутентифицировался для области www.difiniti.com/products, а затем обратился к www.difiniti.com/jobs, он должен будет аутентифицироваться снова. Это происходит потому, что браузер просматривает список областей, для которых пользователь аутентифицировался, и обнаруживает, что пользователь не аутентифицирован для данной области или ее предка.

Чтобы пользователю не приходилось проходить подобную процедуру несколько раз, ему следует сразу аутентифицироваться для высшей Web-области.

Сервер Domino прекращает использовать Domino for IIS

Если вы применяете Domino for IIS, а сервер сразу после запуска IIS-сервера останавливается, проверьте наличие пароля в ID-файле сервера. При работе с Domino for IIS файл идентификационных данных сервера не должен быть защищен паролем.

Области

Область - это отправляемая сервером строка (обычно в адресе URL), указывающая место, для которого аутентифицировался пользователь.

Аутентификация

Если пользователь будет применять ссылки на другие сайты, ему может потребоваться новая аутентификация.

Пользователи не могут получить доступ к Web-серверу

Помешать пользователям соединиться с сервером Domino могут несколько обстоятельств. Приведем некоторые наиболее распространенные.

Проблемы TCP/IP

Для более глубокого анализа проблем TCP/IP их удобно разбить на две основные категории (как вы, возможно, знаете, вся книга посвящена TCP/IP): проблемы настройки пользователя и проблемы настройки сервера.

Проблемы настройки TCP/IP на рабочей станции пользователя

Протоколы TCP/IP на рабочей станции пользователя не всегда настроены правильно - и это вызывает ошибки при обращении к серверу. Хотя этот вопрос не входит в число рассматриваемых в данной книге, ниже описано несколько приемов, помогающих установить, что проблема действительно связана с рабочей станцией пользователя:

- О проверьте сетевой кабель и его подключение на обоих концах;
- О убедитесь, что сетевая карта реагирует на соединение (обычно светится зеленый светодиод);

- О проверьте параметры настройки сети в операционной системе рабочей станции пользователя;
- О на рабочей станции, функционирующей под управлением Windows, откройте сеанс DOS и введите команду `PING 127.0.0.1` (адрес локального ресурса, также известный как локальный хост). Если выдается сообщение **Request timed out** (Время ожидания ответа вышло), то стек TCP/IP настроен неправильно;
- О при правильном выполнении команды `PING 127.0.0.1` стоит проверить с помощью `PING` доступ к серверу Domino. Например, можно ввести `PING www.definity.com` (либо воспользоваться IP-адресом). Появление сообщения **Request timed out** показывает, что стек TCP/IP настроен неправильно.

Если вам не удастся «дозвониться» до сервера по имени (например, `www.definity.com`), попробуйте обратиться к его IP-адресу. Если вы получите нормальный отклик, проблема кроется в параметрах настройки DNS.

Когда сервер доступен, неполадка, вероятнее всего, связана с настройкой браузера или сервера Domino.

Проблемы настройки TCP/IP на сервере Domino

Ниже перечислены приемы обнаружения наиболее часто встречающихся ошибок при настройке TCP/IP на сервере:

- О проверьте сетевой кабель и его подключение на обоих концах;
- О убедитесь, что сетевая карта реагирует на соединение (обычно светится зеленый светодиод);
- О проверьте настройку сети в операционной системе сервера;
- О на сервере, работающем под управлением Windows, откройте сеанс DOS и введите команду `PING 127.0.0.1` (адрес локального ресурса, также известный как локальный хост). Если выдается сообщение **Request timed out** (Время ожидания ответа вышло), то TCP/IP настроен неправильно;
- О в случае правильного выполнения команды `PING 127.0.0.1` стоит просмотреть с помощью `PING` доступ к другим серверам Domino. Например, можно ввести `PING www.definity.com` (или воспользоваться IP-адресом). Появление сообщения **Request timed out** показывает, что стек TCP/IP настроен неправильно;
- О убедитесь, что сервер Domino функционирует;
- О удостоверьтесь, что работает HTTP-сервер. На консоли сервера или удаленной консоли в программе Domino Administrator введите команду `sh ta` и найдете задачу HTTP;
- О просмотрите серверный документ в каталоге Domino и убедитесь, что порт HTTP-сервера установлен правильно и открыт;
- О проверьте, не конфликтует ли установленный номер порта. Если вы не обращаетесь к порту 80, не исключено, что многие службы, такие как FTP (порт 20 или 21), будут конфликтовать с другими службами;
- О проверьте серверный документ в каталоге Domino и убедитесь: система защиты настроена так, что пользователь в состоянии получить доступ к серверу;
- О запустите браузер на сервере и попытайтесь обратиться к серверу.

При корректной работе всех систем проблема, скорее всего, заключается в сети (маршрутизаторы, брандмауэры, мосты и т.д.) или неправильной настройке браузера.

Проблемынастройкибраузера

Если пользователь не получает доступа к серверу Domino, это, возможно, происходит из-за неправильной настройки браузера. Выясните, куда обращается пользователь. Если он сначала обращается к прокси-серверу, определите адрес и протоколы этого прокси-сервера. Затем можно открыть свойства соединения браузера и правильно их настроить. Иногда верно и обратное: браузер настроен на применение прокси-сервера, а он не нужен.

Явные номера портов

Помните, что, если вы указываете номер порта, отличный от 80 (по умолчанию), пользователи должны вводить его в адресе URL. Например, <http://www.definiiti.com:8080>.

Программныеинструментыустранениянеполадок

В Domino имеется несколько инструментов, помогающих устранять различные неполадки. В данном разделе речь пойдет об инструментах, позволяющих справляться с проблемами, которые связаны с HTTP-сервером Domino. Большинство инструментов доступно из программы Domino Administrator.

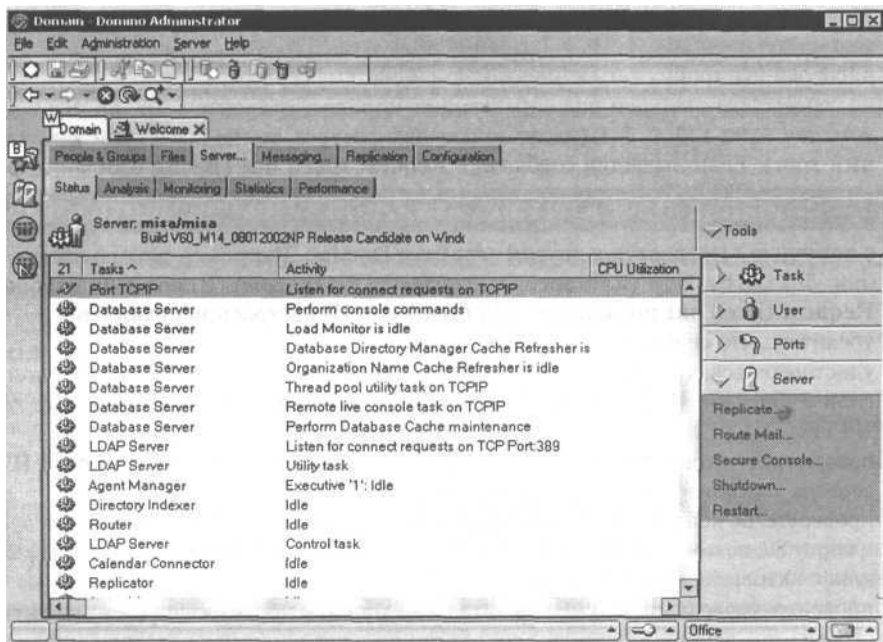


Рис. 15.24. Вкладка Server=>Status в Domino Administrator

Domino Administrator

Domino Administrator - это достаточно мощное средство, которое предоставляет возможность администрировать сервер Domino и решать большинство проблем внутри одной прикладной среды. Для преодоления проблем, связанных с HTTP-сервером, существует два наиболее полезных средства. Первое - вкладка **Server => Status**, которая отображает состояние задач, работающих на сервере (рис. 15.24). Второе - вкладка **Server => Statistic**, предоставляющая полезную статистику о сервере Domino, например число обработанных запросов к HTTP-серверу (рис. 15.25).

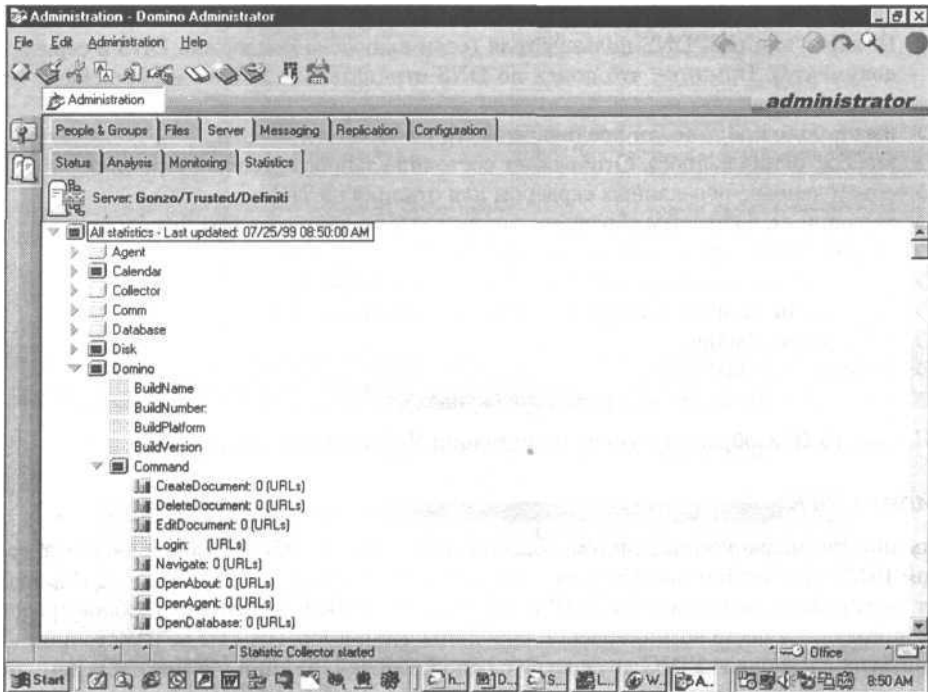


Рис. 75.25. Вкладка *Server=> Statistic* в Domino Administrator

Журнал регистрации сервера Domino

Каждый сервер Domino имеет свой журнал регистрации (Notes Log, файл log.nsf), который отслеживает деятельность сервера и выдает подробную информацию о пользователях и базах данных сервера. Но каждый сервер Domino можно заставить регистрировать информацию об HTTP-сервере либо в базе данных Notes, либо в текстовом файле. Имейте в виду, что на любом сильно загруженном сайте или на сайте, где вы собираетесь прибегнуть к стороннему инструменту анализа журнала регистрации, например Webtrends, необходимо задать регистрацию в текстовом файле.

Регистрация деятельности

Нельзя включить функцию регистрации деятельности HTTP-сервера. Это настраиваемый режим. Откройте каталог Domino и выберите необходимый сервер на виде **Servers**. Загрузите серверный документ и перейдите на вкладку **Internet Protocols**. Убедитесь, что на вкладке **HTTP** установлен один или оба метода регистрации (*log.nsf* и *Text files*).

В журнале регистрации имеется множество полезных сведений о том, что происходит на вашем сайте. Регистрируемая информация содержит:

- дату и время запроса;
- IP-адрес или имя DNS пользователя (если включена поддержка DNS в серверном документе). Помните, что поиск по DNS отрицательно влияет на производительность сервера;
- имя пользователя (если предъявлены его реквизиты);
- код состояния запроса. Отображает состояние запроса (успешно ли он обработан);
- объем данных, переданных сервером для отклика на запрос;
- тип данных, к которым обращается пользователь, например *text/html* или *image/jpg*;
- запрос HTTP, отправленный серверу;
- тип браузера, используемого для выполнения запроса;
- внутренние ошибки сервера или ошибки сценариев CGI;
- URL-адрес ссылки;
- IP-адрес или имя DNS;
- время обработки запроса (в миллисекундах).

На рис. 15.26 изображен журнал регистрации Web-сервера Domino.

Утилита PING

Большинство операционных систем, поддерживающих стек TCP/IP, поставляется со средством PING (Packet Internet Grouper - посыльный пакетов Internet). Эта утилита позволяет тестировать соединение TCP/IP и представляет собой достаточно удобное средство для определения места возникновения проблемы. Например, если вы не в состоянии «дозвониться» с помощью PING до сервера с одной рабочей станции, но можете к нему подключиться с другой, то проблема, скорее всего, не в сервере, а в рабочей станции или сегменте сети, с которым она соединена.

На рабочих станциях, функционирующих под управлением Windows 95/96/NT, можно открыть сеанс DOS и ввести команду PING <someaddress>, где <someaddress> - IP-адрес или имя хоста сервера, который требуется проверить (рис. 15.27). Если нужно вызвать справку по параметрам команды PING, запустите ее без параметров - и система выведет список доступных аргументов команды и их описание.

Если можно «дозвониться» до сервера, ясно, что дело не в сетевом соединении.

Telnet

Как и в случае с PING, большинство операционных систем, поддерживающих TCP/IP, поставляется с программой Telnet, которая позволяет соединяться с удаленным хостом при помощи TCP/IP. Можно посредством Telnet определить, отвечает ли сервер на запросы через порт 80 (или установленный вами порт) при сетевом обращении к указанному порту.

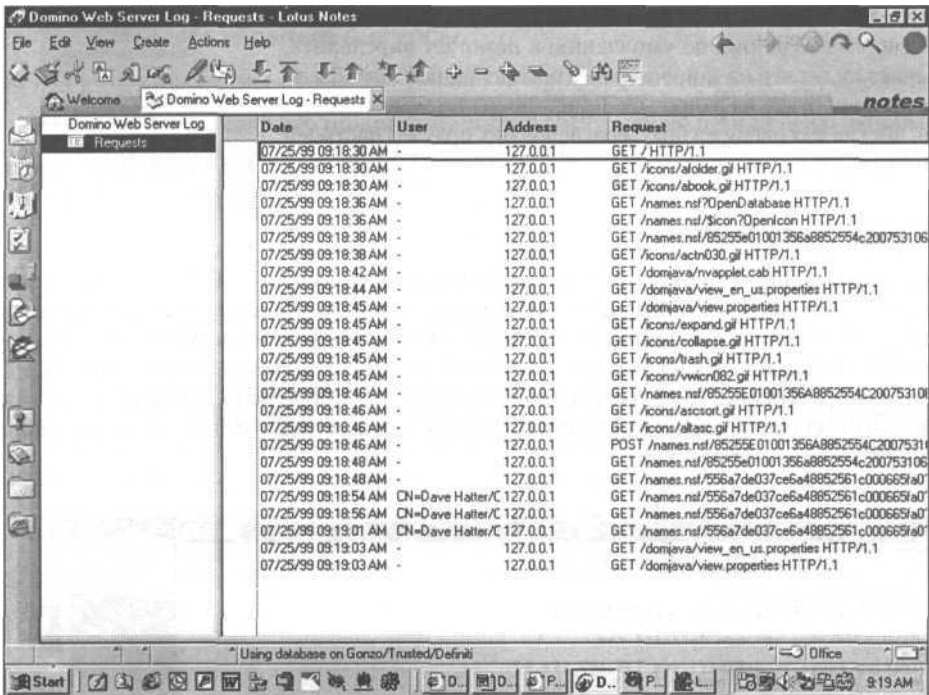


Рис. 15.26. Вид Requests журнала регистрации Web-сервера Domino

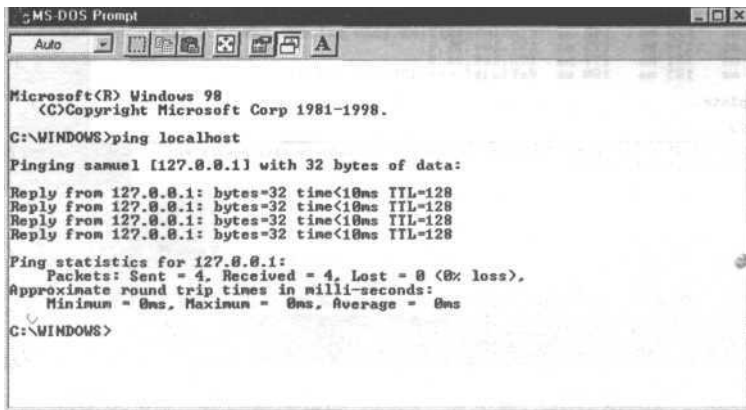


Рис. 15.27. Утилита PING

Для запуска программы Telnet в системе под управлением Windows откройте сеанс DOS и введите команду Telnet. Выберите **Connect** и по запросу укажите IP-адрес или имя удаленного сервера и порт. После этого можно задавать что угодно, но ответ всегда будет от HTTP-сервера, если он работает. На рис. 15.28 изображен ответ от HTTP-сервера Domino.

Telnet устанавливается вместе с любой версией операционной системы Windows по умолчанию и помогает определить, отвечает ли сервер на запросы через определенный порт. Если вам пришел ответ на запрос от Telnet, но вы не можете получить доступ к серверу из браузера, вероятно, браузер настроен неправильно.

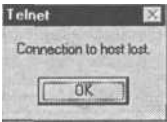


Рис. 15.28. Ответ сервера Domino программе Telnet

Утилита Trace Route

Как в PING и Telnet, в операционных системах с поддержкой TCP/IP имеется средство отслеживания пути - утилита Trace Route (tracert). Она позволяет точно определить, в какой части сети возникла проблема. Чтобы воспользоваться ею, в Windows откройте сеанс DOS и введите команду `tracert <someaddress>`, где `<someaddress>` - это TCP/IP-адрес сервера. На рис. 15.29 изображено отслеживание пути к `www.definitiv.com`. Если вам нужен файл справки, введите команду `tracert` без параметров - и система выведет список поддерживаемых аргументов.

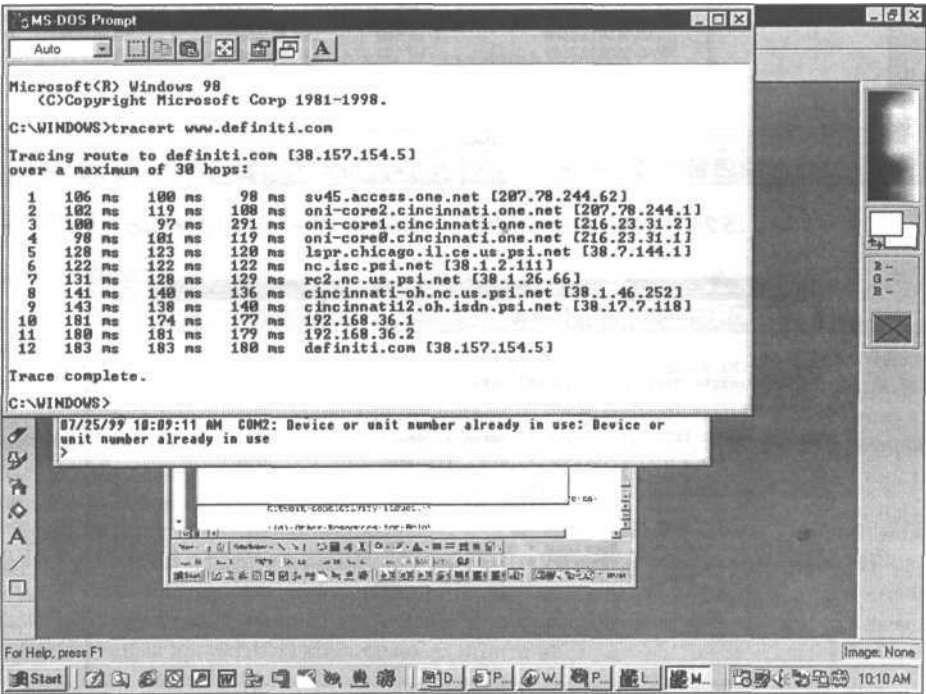


Рис. 15.29. Путь к Definitiv

Другие вспомогательные ресурсы

При появлении проблемы с сервером Domino можно обратиться к следующим ресурсам:

- О база данных Domino 5/6 Administration Help (help5_admin.nsf или help6_admin.nsf);
- О база знаний Notes Knowledge Base (kbnvl1.nsf);
- О база данных Business Partner Technical Forum (bptech98.nsf)> которая предоставляет только бизнес-партнерам компании Lotus.

Если, изучив настоящую главу и воспользовавшись указанными ресурсами, вы все же не смогли решить свою проблему, вам, вероятно, следует позвонить в службу технической поддержки компании Lotus, чтобы получить там квалифицированную помощь.

Дополнительные справочные ресурсы Notes/Domino

Большую часть информации, находящейся в базах данных Knowledge Base и Business Partner Technical Forum, можно найти на следующих сайтах: www.lotus.com, www.notes.net, www.dominoedge.com, www.dominohive.com, www.dominopower.com.



Сервер Domino кроме всего прочего является еще и почтовым сервером POP3 (Post Office Protocol 3 - почтовый протокол версии 3). Как сервер POP3 он может принимать и хранить почту пользователей и клиентских почтовых программ, а затем отправлять ее по запросу клиентам POP3. Используется порт TCP ПО. При обращении клиента POP3 к серверу для получения почты в процессе передачи сообщений происходит обмен командами и откликами.

Протокол POP3 не поддерживает методы передачи почтовых сообщений - он предназначен только для приема почты. Отправляют почту клиенты POP3 обычно с помощью SMTP (Simple Mail Transfer Protocol - простой протокол передачи почты), соединяясь для этого с почтовым сервером SMTP. Почтовым сервером SMTP может быть тот же компьютер, на котором работает POP3, или другой компьютер. Поскольку маршрутизатор Domino применяет SMTP, Domino следует поддерживать обслуживание исходящей почты для своих клиентов POP3»

POP3 является почтовым протоколом сети Internet, который предназначен для пользователей, работающих с почтой в автономном режиме. Создание почтового протокола началось в 1984 г. - когда стало ясно, что по мере увеличения числа персональных компьютеров все менее и менее желательно, чтобы они все время находились в Internet. Первоначально пользователи связывались с большими компьютерами, постоянно подсоединенным к сети, и могли получить доступ только к учетным записям почты, хранившимся на компьютере, к которому они подключены.

Почта POP3 и Domino

Пользователь с учетной записью почты POP3 имеет персональный документ в каталоге Domino и почтовую базу данных на сервере. В качестве такой базы выступает стандартная почтовая база Notes. Маршрутизатор помещает почтовые адреса пользователей в их почтовые базы данных так же, как переносит почту в любую базу пользователя. Поскольку пользователь применяет протокол POP3, маршрутизатор преобразует сообщение в формат MIME. Для получения почты пользователь аутентифицируется сервером Domino, чтобы сервер знал, что это за пользователь и какие почтовые файлы ему принадлежат.

POP-пользователь может аутентифицироваться либо с помощью имени и пароля, либо с помощью протокола SSL.

Получив почту, пользователь вправе оставить копии сообщений на сервере либо удалить их.

POP3 поддерживают практически все почтовые программы Internet, в том числе и те, которые чаще всего устанавливаются на компьютерах под управлением Windows:

- ☐ Microsoft Outlook Express;
- ☐ Netscape Messenger;
- ☐ Eudora Pro Mail;
- ☐ Lotus Notes Mail (версии 4.6 и выше).

POP3 или IMAP

Недостатком POP3 является то, что этот протокол позволяет пользователю забирать почту и обрабатывать ее только локально. Этот протокол не позволяет обращаться к почтовым сообщениям непосредственно на сервере. Из-за этого POP3 часто вытесняется протоколом IMAP (Internet Message Access Protocol - протокол доступа к сообщениям Internet), который также поддерживается сервером Domino (см. главу 17). Протокол ШАР позволяет пользователю работать с почтой на сервере или загружать ее на свой компьютер.

Пользователи POP в Domino в состоянии частично обойти эти ограничения. Они могут использовать Web-браузер, чтобы открыть свой почтовый ящик и работать с почтой непосредственно на сервере (указывается адрес URL, например <http://www.mailservername/mail/mailfilename.nsf>). Однако любое почтовое сообщение, удаленное на сервере во время доставки почты на рабочую станцию с помощью почтовой программы, теряется навсегда. Кроме того, между почтовой программой и почтовой базой данных на сервере нет никакой связи. Поэтому, когда пользователь создает папку в одном из мест (на своей рабочей станции с помощью почтовой программы либо на сервере с помощью Web-браузера), сделанные изменения не отражаются в другом месте.

Следовательно, если вы думаете над тем, какую службу установить для своих пользователей, POP3 или ШАР, то (при прочих равных условиях) предпочтительнее выбрать ШАР. В общем случае, когда у вас уже есть множество пользователей POP3 и нужно перевести их в среду Domino, самым безболезненным путем для них будет применение POP3. Если вам необходимо поддерживать пользователей, имеющих дело с почтовыми программами POP3, настройка POP3 тоже будет выходом из ситуации. В остальных «лучаях» старайтесь обходиться ШАР.

Вы, конечно, можете установить на сервере поддержку и POP3, и ШАР, чтобы удовлетворить всех пользователей. Но вряд ли стоит поступать таким образом.

Настройка протокола POP на сервере Domino

Для настройки POP на сервере Domino необходимо выполнить следующие действия:

1. Установите и настройте стек TCP/IP на сервере Domino и в операционной системе.
2. Настройте сервер POP3.
3. Запустите задачу POP3.

4. Для обслуживания исходящей почты задайте сервер SMTP. Это можно сделать либо на сервере POP3, либо на другом сервере Domino, либо на любом другом компьютере.
5. Зарегистрируйте пользователей службы POP в каталоге Domino.
6. Установите программное обеспечение работы с почтой на рабочих станциях пользователей.

Процедура установки сервера SMTP описана в главе 8, а остальные процедуры - в последующих разделах данной главы.

Настройка TCP/IP

Чтобы правильно настроить стек TCP/IP в Domino, надо сначала правильно настроить его в операционной системе. После этого можно открыть порт TCP/IP на сервере Domino с помощью методов, описанных в главе 3.

Следует также убедиться, что все пользователи способны обращаться к своим почтовым серверам. В большинстве случаев это означает, что имя сервера Domino должно быть правильно указано в списке имен серверов домена. Если имя сервера Domino отличается от имени хоста, на котором он работает, то в качестве имени сервера необходимо вводить оба имени. Другими словами, нужна запись A (Адрес), связанная с IP-адресом, и запись CNAME (Каноническое имя), в которой указано общее имя сервера Domino как псевдоним хоста компьютера.

Пусть, например, сервер POP3 называется MailOl/PlanetNotes. Компьютер, на котором он установлен, имеет имя хоста domsrv01.planetnotes.com. Для него задан IP-адрес 10.0.0.10. Необходимо, чтобы в службе DNS была запись A, отмечающая, что серверу domsrv01.planetnotes.com назначен IP-адрес 10.0.0.10. Если вашим пользователям требуется обращаться к серверу Domino по его общему имени, MailOl, вам нужна в DNS запись CNAME, которая означает, что domsrv01.planetnotes.com - это на самом деле mail01.planetnotes.com. Если пользователи связываются с сервером через Internet, необходимо обеспечить компьютеру MailOl постоянное соединение (например, через маршрутизатор к линии T-1) с вашим провайдером Internet, у него должен быть постоянный зарегистрированный IP-адрес (назначенный провайдером), а вышеописанные записи следует установить в базе данных DNS вашего провайдера. /

Настройка POP3

Допустимо настроить сервер POP в среде Domino через серверный документ в каталоге домена. В программе Domino Administrator откройте серверный документ на вкладке **Configuration**. Затем выберите **Ports => Internet Ports => Mail** (Порты => Internet-порты => Почта). Заполните поля в столбце **Mail (POP)**, как указано в табл. 16.1.

Таблица 16.1. Настройка полей в столбце Mail (POP)

Название поля	Описание
TCP/IP port number (Номер порта TCP/IP)	Обычно следует оставлять значение по умолчанию (110), то есть стандартный порт для почтовых серверов. Можно изменить этот параметр, если на компьютере установлено несколько серверов POP3, как в случае применения нескольких секционированных серверов Domino

Таблица 16.1. Настройка полей в столбце **Mail (POP)** (окончание)

Название поля	Описание
TCP/IP port status (Состояние порта TCP/IP)	Чтобы применять стандартный порт POP3, укажите значение Enabled . Если задано значение Disabled , пользователи почты должны обращаться к порту SSL
Authentication options: Name & Password (Параметры аутентификации: имя и пароль)	В этом поле автоматически устанавливается значение Yes , если вы открываете порт TCP/IP, или No - если закрываете его
Authentication options: Anonymous (Параметры аутентификации: анонимные пользователи)	Права выбора нет, поскольку сервер Domino всегда должен аутентифицировать почтового пользователя, иначе система не сможет определить, в какой базе данных находится его почта
SSL port number (Номер порта SSL)	Как правило, необходимо оставлять значение по умолчанию (995), то есть стандартный порт SSL для почты. Если установлено несколько почтовых серверов, можно изменить этот параметр
SSL port status (Состояние порта SSL)	По умолчанию порт закрыт. Чтобы сервер Domino применял SSL для аутентификации пользователей почты POP, откройте этот порт, а чтобы пользователи аутентифицировались только через порт SSL, закройте порт TCP/IP. Когда закрыты оба порта, почтовая служба отключается полностью
Authentication options: Client Certificate (Параметры аутентификации: клиентский сертификат)	По умолчанию - No . Чтобы пользователи предоставляли сертификаты X.509 для аутентификации с сервером, установите Yes
Authentication options: Name & Password (Параметры аутентификации: имя и пароль)	По умолчанию - Yes . Чтобы пользователи для аутентификации применяли сертификаты, установите No

Можно открыть почту POP тремя способами:

- ☐ с помощью только порта TCP/IP (110);
- ☐ посредством только порта SSL (995);
- ☐ при помощи обоих портов.

Если вы откроете оба порта, пользователи для доступа к своей почте смогут обратиться к одному из них на выбор, а если только порт SSL, то, чтобы активизировать аутентификацию SSL, клиенту придется воспользоваться одним из трех вариантов:

- ☐ представить сертификат (Client Certificate = Yes, Name & Password = No);
- ☐ ввести имя и пароль (Client Certificate = No, Name & Password = Yes);
- ☐ либо представить сертификат, либо ввести имя и пароль (Client Certificate = Yes, Name & Password = Yes). Domino сначала попытается применить базовую аутентификацию. Если она не будет выполнена (например, из-за того, что сервер не доверяет сертификату клиента), Domino потребует ввести имя и пароль, чтобы сравнить их с персональным документом в каталоге Domino.

При открытии порта SSL сервер Domino не позволит сохранить серверный документ, если оба параметра аутентификации SSL не будут равны No.

Дополнительная настройка, необходимая для секционированного сервера

Если почтовый сервер POP является секционированным сервером Domino, необходимо добавить в файл notes.ini, который находится в папке данных сервера, переменную POP3Address=IP Address или POP3Address=Fully Qualified Domain Name, где IP Address - IP-адрес сервера (например, 192.168.1.12), а Fully Qualified Domain Name (FQDN) - полное квалифицированное доменное имя компьютера (не путайте с именем Domino). Какой вариант предпочесть, зависит от того, что вы чаще меняете - IP-адрес или полное имя. Сервер MailOl может иметь следующие переменные:

POP3Address=10.0.0.10

или

POP3Address=domsrv01.planetnotes.com

Запуск задачи сервера POP3

Можно запустить (и остановить) задачу сервера POP3 вручную или активизировать ее автоматически при запуске сервера Domino. Удобнее, чтобы эта задача стартовала автоматически и работала постоянно, тогда не придется запускать ее каждый раз при перезагрузке сервера.

Для настройки автоматического старта POP3 добавьте POP3 в конец переменной ServerTasks в файле notes.ini сервера. Допустим, что переменная ServerTasks определена следующим образом:

^" • ~ServerTasks=Router, Replica, Update, Amgr, AdminP, HTTP

Измените ее так:

ServerTasks=Router, Replica, Update, Amgr, AdminP, HTTP, POP3

Файл notes.ini может находиться или в каталоге программ сервера Domino, или (на секционированных серверах) в каталоге данных сервера Domino, или (на серверах под управлением Windows, обновленных с версии R4.x) в папке Windows. Файл допускается редактировать либо непосредственно в текстовом редакторе, либо опосредованно с помощью команды, вводимой с консоли сервера, либо добавив переменную ServerTasks в документ конфигурации сервера. #

Чтобы добавить значение с консоли сервера, сначала требуется определить текущее значение этой переменной командой Show Config ServerTasks. Затем (если переменная задана как в предыдущем примере) вводится команда

Set ConfigServerTasks=Router, Replica, Update, Amgr, AdminP, HTTP, POP3

При использовании данного метода необходимо набирать команды очень аккуратно. Опечатка приведет к ошибке сервера при следующей перезагрузке. Проверьте правильность команды несколько раз.

Чтобы применить для установки этой переменной документ конфигурации сервера, перейдите на вкладку **Configuration** в Domino Administrator и откройте существующий файл конфигурации сервера либо создайте новый. В окне **NOTES.INI Settings** выберите

Set/Modify Parameters (Установить/изменить параметры). В поле **Item** (Элемент) укажите значение **ServerTasks**, а в поле **Value** (Значение) - полную строку серверных задач, разделенных запятыми. После этого щелкните по **Next** и по **OK**. Сохраните и закройте документ.

Еще раз напомним, что следует тщательно проверить команду перед ее внесением. Чтобы минимизировать вероятность опечатки, лучше скопировать в буфер значения из файла notes.ini и затем вставить их в нужные поля. При этом вручную придется вводить небольшую часть информации.

Вручную запустить задачу POP3 можно с помощью либо консоли сервера, либо программы Domino Administrator. Для запуска служит команда load POP3, а для остановки - команда tell pop3 quit или tell pop3 exit.

При работе с Domino Administrator откройте вкладку **Server => Status**. На панели **Task** выберите **Start**, затем в диалоговом окне укажите **POP3 Mail Server**. После запуска задача появляется на панели **Results**. Чтобы ее остановить, выделите любой экземпляр задачи POP3 на панели **Results** и выберите на панели **Task** команду **Stop**.

Регистрация пользователей POP3

Пользователь почты POP3 необязательно должен иметь ID-файл (файл идентификационных данных), если он не является пользователем Notes. Следовательно, достаточно вручную зарегистрировать пользователя POP3 (если надо), создав для него персональный документ и почтовую базу данных и добавив его имя в требуемую группу. С другой стороны, можно обратиться к диалоговому окну **Register Person** (Регистрация сотрудника) - и Domino Administrator сделает всю работу за вас. Следует только обратить особое внимание на значения в некоторых полях.

: зарегистрировать пользователя почты POP3:

1. Создайте персональный документ. В Domino Administrator откройте вкладку **People & Groups**, выберите POP3-сервер Domino (или другой сервер в том же домене), выведите на экран вид **People** (Сотрудники) и задайте **Add Person** (Добавить сотрудника). Заполните поля, описанные в табл. 16.2.

Таблица 16.2. Настройка параметров в диалоговом окне **Add Person**

Название поля	Описание
На вкладке Basics (Основные параметры)	
First name (Имя)	Заполните все три поля. User name (Имя пользователя)
Last name (Фамилия)	должно быть комбинацией имени (First name) и фамилии
User name (Имя пользователя)	(Last name)
Internet password (Internet-пароль)	Пароль, который будет применять пользователь для доступа к своей почте. Не оставляйте это поле пустым
На вкладке Mail (Почта)	
Mail system (Почтовая система)	Выберите POP или IMAP
Domain (Домен)	Имя домена почтового сервера
Mail server (Почтовый сервер)	Полное имя Notes почтового сервера POP3

Таблица 16.2. Настройка параметров в диалоговом окне **Add Person** (окончание)

Название поля	Описание
Mail file (Почтовый файл)	Частичный путь (начиная с каталога данных Domino) и имя файла почтовой базы данных пользователя (например, data\filename). Расширение .nsf в имени файла можно не указывать
Forwarding address (Почтовый адрес пересылки)	Не заполняйте
Internet address (Internet-адрес)	Введите допустимый адрес электронной почты пользователя. Этот же адрес должен быть указан в его почтовой программе
Format preference for incoming mail (Предпочтительный формат для входящих сообщений)	Выберите Prefers MIME (Предпочтение MIME)
Encrypt incoming mail (Шифрование входящих сообщений)	Задайте No

- 2. Добавьте пользователя в требуемую группу.
- 3. Создайте почтовый файл на сервере POP3. Он делается на основании шаблона Mail(R5.0) в версии R5 или Mail(6) в версии R6.
- 4. В списке ACL нового почтового файла установите доступ по умолчанию No Access, а для пользователя и почтового сервера задайте уровень доступа Manager с правом Delete documents (Удаление документов). Все остальные записи, включая собственную, удалите.

Если вы регистрируете почтового пользователя в окне Register Person, укажите Advanced в левом верхнем углу окна и заполните поля как обычно, учитывая исключения, показанные в табл. 16.3.

Таблица 16.3. Настройка в диалоговом окне **Register Person**

Название поля	Описание
	Вкладка Mail (Почта)
Mail system (Почтовая система)	Выберите POP
	Вкладка ID Info (Идентификационная информация)
Location for storing user ID (Место хранения файла идентификационных данных пользователя)	Сбросьте флажки In Domino Directory (В каталоге Domino) и In file (В файле). При этом не будет создаваться ID-файл, который не применяет пользователь

Настройка почтового программного обеспечения пользователей

Точная настройка клиентской программы, конечно, зависит от самой программы. Однако в любом случае необходимо ввести следующую информацию:

- О полное квалифицированное имя домена почтового сервера POP3 (например, osprey.planetnotes.com);
- О полное квалифицированное имя домена сервера SMTP;
- О имя учетной записи пользователя, в качестве которого выступает имя пользователя, указанное в созданном ранее персональном документе;
- О нужно ли удалять файлы с сервера после того, как пользователь загружает их на свой компьютер. Если пользователь будет работать с почтой на сервере (с помощью клиента Notes, IMAP или Web-браузера), а также локально посредством почтового клиента Notes, надо запретить удаление.

Остальные свойства пользователь устанавливает в зависимости от самой почтовой программы. Ряд почтовых программ Internet имеет множество свойств, которые может выбрать пользователь. Остальные программы достаточно малы, и у них немного параметров.

Настройка службы POP3

Для настройки порядка работы почтовой службы POP3 существует определенный набор переменных в файле notes.ini (табл. 16.4).

Таблица 16.4. Переменные файла notes.ini

Переменная	Описание
POP3DNSLookup=значение	Установите 1, чтобы разрешить обратный поиск имени компьютера пользователя в службе DNS. По умолчанию — 0. Это означает, что поиск в DNS отменен
POP3ExactSize=3На4eroie	Задайте 1, чтобы сервер POP3 возвращал точный размер сообщений. По умолчанию - 0, то есть возвращается примерный размер. При включенном параметре POP3ExactSize может закончиться время ожидания команды PASS, поскольку для команды STAT все сообщения должны преобразовываться, чтобы вычислялся точный размер. Такое преобразование продолжается долго, особенно если сообщений много и все они большие. Задавайте этот режим, только если пользователям нужен точный размер сообщений. В качестве альтернативного варианта можно включать или выключать параметр POP3 server returns exact size of messages (POP3-сервер возвращает точный размер сообщений) в документе конфигурации. Если эти параметры установлены и в документе конфигурации, и в файле notes.ini, то значение в документе конфигурации имеет преимуществ^
POP3NotesPort=номер_порта	Данную переменную можно применять вместо параметра TCP/IP port number в серверном документе для установки номера порта (отличного от 110), который будет использовать POP. В файле справки Administration Help для Domino Administrator говорится, что вы должны устанавливать указанную переменную для секционированного сервера, но на самом деле этого делать не следует
POP3_Conf ig_Update_Interval=MMHyTbj	Задает частоту обновления информации конфигурации службы POP3. По умолчанию - 2 минуты
POP3_Disable_Cache=значение	Укажите 1, чтобы разрешить кэширование сообщений пользователей. По умолчанию — 0, то есть кэширование запрещено

Таблица 16.4. Переменные файла notes.ini (окончание)

Переменная	Описание
	Задаёт адрес возврата по умолчанию для пользователей POP3 на уровне сервера. Сервер будет пользоваться адресом из персонального документа пользователя, если он там есть. Если адрес не указан, сервер применяет значение, определённое этой переменной. Если не назначено ни то, ни другое, сервер будет работать со значением, приведённым в поле Local primary Internet domain документа Global Domain, если таковое имеется. Если данное значение тоже отсутствует, сервер обратится к имени домена, установленному в собственном стеке TCP/IP. А если и этого параметра нет, служба POP3 будет выдавать ошибку инициализации
POP3_MarkRead=значение	Чтобы при загрузке сообщения помечались как прочитанные, установите 1. По умолчанию 0. Это значит, что сообщения не помечены как прочитанные
POP3_Messag_Stat_Cache_NshmPerUser=число	Определяется максимальное число сообщений одного пользователя, для которых кэшируется статистика, включающая в себя UNID и размеры сохранённых сообщений. Кэширование потребляет много ресурсов, поскольку сервер должен вычислить размер каждого сообщения. Кроме того, расходуются ресурсы памяти. По умолчанию установлено 50 сообщений. Если производительность сервера низкая, задайте меньшее значение

Контроль работы службы POP3

Чтобы убедиться, что служба POP3 настроена правильно, установите один или несколько зондов TCP Server. Рекомендуется протестировать службу POP3. Зонд можно создать на вкладке **Configuration** программы Domino Administrator. Выберите **Statistics & Events => Probes => TCP Server** (Статистика и события => Зонды => TCP-сервер) на панели **Tasks**. Затем на панели **Actions** выше панели **Results** укажите **New TCP Server Probe** (Создать зонд TCP-сервера). Если такого зонда ещё не существует, создайте его и в нём выберите **All Domino servers in the domain will probe their own configured ports** (Все серверы Domino в данном домене будут тестировать свои настроенные порты). Кроме того, создайте хотя бы один зонд, которым один сервер будет тестировать другой.

Статистику можно посмотреть на панели **Statistics** вкладки **Server** в Domino Administrator и дополнительно на панели **Monitor**. Если на сервере запущена служба Collector (Сбор статистики), которая накапливает статистику о данном сервере, то статистические отчеты также добавляются в базу данных Statistic Reports. Более подробно это обсуждается в главе 18.



Сервер Domino может служить почтовым сервером IMAP (Internet Message Access Protocol - протокол доступа к сообщениям Internet, версия 4). Как сервер IMAP он способен получать и хранить сообщения для клиентских почтовых программ, а затем работать с запросами клиентов IMAP через порт TCP 143.

IMAP не предоставляет возможности отправлять почту. Клиенты IMAP для этой цели обычно используют SMTP, соединяясь с почтовым сервером SMTP. Поскольку маршрутизатор Domino применяет SMTP, сервер Domino должен поддерживать обслуживание исходящей почты для своих клиентов ШАР.

Парадигма службы IMAP определяет три основные модели доступа к удаленному серверу сообщений:

- О *интерактивный режим*. Пользователь читает сообщения по очереди на почтовом сервере, управляет ими в памяти (перемещает, редактирует, удаляет) и затем сохраняет их опять же на сервере. Так работает с почтой пользователь Notes, когда в поле **Mail file location** (Размещение почтового файла) в текущем документе местоположения установлено значение **on Server** (На сервере);
- О *автономный режим*. Клиент считывает пакет сообщений с сервера, сохраняет их на рабочей станции, затем (по умолчанию) удаляет их с сервера, оставляя только копии в своей клиентской программе. После этого пользователь читает, редактирует, удаляет и перемещает сообщения автономно. Так работает почта POP3^
- О *без подключения*. Клиент считывает пакет сообщений с сервера и сохраняет их в кэш-памяти рабочей станции. Пользователь обрабатывает почту в памяти и тоже сохраняет изменения в кэш-памяти. В любой момент пользователь снова может соединиться с сервером и синхронизировать внесенные изменения с хранящимися на сервере оригиналами. Такова схема работы с почтой пользователя Notes, если в поле **Mail file location** в текущем документе местоположения установлено значение **Local** (Локально).

Поддержка службой ШАР всех этих моделей предоставляет пользователям разнообразные возможности, например позволяет получать доступ к почте с любой рабочей станции и работать с ней в интерактивном режиме, без подключения или в автономном режиме. Сообщения не «запираются» на конкретной рабочей станции, как это происходит в POP3. Более того, «главная» копия каждого сообщения сохраняется на сервере.

IMAP версии 4 поддерживает совместно используемые (общие) папки, что позволяет обеспечить дискуссии и сотрудничество как в среде Notes. Эта версия имеет иерархические каталоги. Она совместима с протоколом MIME и в состоянии удаленно определить структуру MIME-сообщения, после чего загрузить определенную часть сообщения, например аннотацию. Служба ШАР поддерживает эффективную передачу данных, что особенно важно при модемном соединении.

Поскольку ШАР является достаточно гибким протоколом, многие пользовательские программы очень быстро начинают его использовать. ШАР уже поддерживает большинство ранних версий многих клиентских программ, в том числе следующие программы, которые чаще всего устанавливаются на компьютерах под управлением Windows:

- О Microsoft Outlook Express, составная часть Internet Explorer, начиная с версии 4;
- О Netscape Messenger, составная часть Netscape Communicator, начиная с версии 4.0;
- О Eudora Pro Mail 3.1;
- О PC-Pine 3.0;
- О Simeon 4.1;
- О Lotus Notes, начиная с версии 4.6.

IMAP или POP

Почтовые службы ШАР и POP были разработаны для разных целей. POP предназначалась для автономной работы пользователей. Почтовые клиенты POP загружают сообщения с почтового сервера POP, затем обычно (хотя и необязательно) удаляют оригиналы оттуда. В результате остаются лишь копии на компьютере пользователя. По сути, почтовый сервер POP служит только местом временного хранения сообщений до тех пор, пока пользователь не заберет их.

ШАР предоставляет пользователю возможность работать с сообщениями не только со своего компьютера. Поскольку основные копии сообщений хранятся на сервере, пользователь способен работать со своей почтой из другой клиентской программы даже после загрузки копии сообщения в клиентскую программу. Все больше и больше пользователей понимают, что ШАР функционирует лучше, чем POP. У них есть один компьютер на работе, другой дома и, возможно, переносной компьютер для командировок. В результате ШАР быстро заменяет POP как более удобный тип почтовой службы Internet.

С другой стороны, многие люди имеют несколько учетных записей у разных провайдеров - скажем, одну на работе, одну в AOL и одну в Yahoo. Большинство порталов Internet предоставляет бесплатные почтовые услуги, поэтому можно просто зарегистрировать несколько почтовых ящиков. Некоторые пользователи обрабатывают почту именно таким образом. Например, один почтовый адрес предназначен у них для бизнес-контактов, другой - для своих знакомых, а третий - для коммерческих Web-сайтов, на которых они зарегистрированы. Так им удобно отделять дело от развлечений, а старую почту - от новой. Для подобных людей обрабатывать почту ШАР достаточно сложно. Они предпочитают использовать POP3, чтобы можно было читать почту из нескольких источников с помощью одной программы.

С точки зрения провайдера, служба POP3 требует меньше ресурсов сервера, чем служба ШАР. Применяя POP, пользователь соединяется с сервером и удаляет с него сообщения.

Если он не установил другие параметры и регулярно загружает почту, сервер не хранит старые сообщения.

С другой стороны, почтовые сообщения при работе с ШАР постоянно накапливаются на сервере, как и в Notes. Кроме того, сервер ШАР должен выполнять гораздо больше вычислений, так как пользователи IMAP создают и удаляют папки, перемещают и редактируют сообщения на сервере. И наконец, на сервере Domino установка IMAP требует множества дополнительных действий для настройки средств ШАР в почтовой базе данных пользователя. В случае службы POP ничего подобного делать не нужно.

Если вы решаете, что выбрать, то, наверное, лучшим вариантом будет ШАР. Данный протокол является расширенным протоколом POP, так что пользователи при желании могут применять его как POP. Но для сервера Domino существует немного причин для выбора между ними. При отсутствии почтовых пользователей Notes включите тот протокол, который удовлетворяет вашим нуждам и нуждам ваших пользователей, но не устанавливайте оба протокола.

Почта IMAP и Domino

Пользователь, имеющий учетную запись ШАР на сервере Domino, обладает персональным документом в каталоге Domino и почтовой базой данных на сервере, которая представляет собой немного измененную почтовую базу данных Notes. Маршрутизатор Domino заносит почтовый адрес пользователя в его почтовую базу данных и потом помещает почту в любую базу пользователя. Поскольку пользователь является пользователем ШАР, маршрутизатор преобразует сообщение в формат MIME.

Для работы с почтой пользователь аутентифицируется сервером Domino, чтобы сервер знал, что это за пользователь и какие почтовые файлы ему принадлежат. Пользователи ШАР могут аутентифицироваться либо с помощью имени и пароля, либо посредством аутентификации SSL. Протокол SSL - это стандартная схема аутентификации Internet, которая, как и аутентификация Notes, обращается к сертификатам и, следовательно, является более защищенной (см. главу 10).

Установка IMAP на сервере Domino

Для установки ШАР выполните следующие действия:

*

1. Установите и настройте стек TCP/IP на сервере Domino и в операционной системе.
2. Настройте сервер ШАР.
3. Запустите задачу ШАР.
4. Для обслуживания исходящей почты установите сервер SMTP. Можно установить его на сервере POP3, другом сервере Domino, либо на любом другом сервере.
5. Зарегистрируйте пользователей ШАР в каталоге Domino.
6. Откройте почтовые файлы пользователей для доступа ШАР.
7. По желанию создайте полнотекстовый индекс для почтовых файлов пользователей.
8. Установите программное обеспечение почты на рабочих станциях пользователей.

Процедура настройки SMTP на сервере Domino рассмотрена в главе 8. Остальные процедуры будут описаны в следующих разделах.

Настройка TCP/IP

Чтобы должным образом настроить стек TCP/IP в Domino, необходимо сначала правильно задать соответствующие параметры в операционной системе. После этого можно открыть порт TCP/IP на сервере Domino, используя методы, рассмотренные в главе 3.

Надо убедиться, что все пользователи IMAP способны обращаться к своим почтовым серверам. В большинстве случаев это означает, что имя сервера Domino должно быть правильно указано в списке имен серверов домена. Если имя сервера Domino отличается от имени хоста, на котором он работает, то в качестве имени сервера следует указать оба имени. Другими словами, нужны запись A (Адрес), связанная с IP-адресом, и запись CNAME (Каноническое имя), в которой указано общее имя сервера Domino как псевдоним имени хоста компьютера.

Настройка IMAP

Можно настроить сервер IMAP в среде Domino через серверный документ в каталоге домена. На вкладке **Configuration** (Конфигурация) в Domino Administrator откройте серверный документ. Выберите **Ports** => **Internet Ports** => **Mail**. Заполните поля в столбце **Mail (IMAP)**, как указано в табл. 17.1.

Таблица 17.1. Настройка полей в столбце **Mail (IMAP)**

Название поля	Описание
TCP/IP port number (Номер порта TCP/IP)	Обычно следует оставлять значение по умолчанию (143), которое определяет стандартный порт для почтовых серверов IMAP
TCP/IP port status (Состояние порта TCP/IP)	Чтобы применять стандартный порт IMAP, задайте значение Enabled . Если указано значение Disabled , пользователи почты должны обращаться к порту SSL
Authentication options: Name & Password (Параметры аутентификации: имя и пароль)	В этом поле автоматически устанавливается значение Yes, если открывается порт TCP/IP, или No, если порт закрыт
Authentication options: Anonymous (Параметры аутентификации: анонимные пользователи)	Выбора нет, поскольку сервер Domino всегда должен аутентифицировать почтового пользователя, иначе система не сможет определить, в какой базе данных находится его почта
SSL port number (Номер порта SSL)	Обычно оставляют значение по умолчанию (993), которое определяет стандартный порт SSL для почты IMAP
SSL port status (Состояние порта SSL)	По умолчанию порт закрыт. Чтобы сервер Domino использовал SSL для аутентификации пользователей почты POP, откройте его. Чтобы пользователи аутентифицировались только через порт SSL, закройте порт TCP/IP. При закрытии обоих портов почтовая служба отключается полностью

Таблица 17.1. Настройка полей в столбце Mail (IMAP) (окончание)

Название поля	Описание
Authentication options: Client Certificate (Параметры аутентификации: клиентский сертификат)	По умолчанию - No. Чтобы пользователи предоставляли сертификаты X.509 для аутентификации с сервером, установите Yes
Authentication options: Name & Password (Параметры аутентификации: имя и пароль)	По умолчанию - Yes . Чтобы пользователи для аутентификации должны были предъявлять сертификаты, задайте No

Можно настроить почту ШАР тремя способами:

- ☐ с помощью только порта TCP/IP (143);
- ☐ посредством только порта SSL (993);
- ☐ при помощи обоих портов.

Если открыты оба порта, пользователи смогут выбрать один из них для доступа к своей почте, а если только порт SSL, то для аутентификации SSL клиенту придется воспользоваться одним из следующих трех вариантов:

- ☐ представить сертификат (Client Certificate = Yes, Name & Password = No);
- ☐ ввести имя и пароль (Client Certificate = No, Name & Password = Yes);
- ☐ либо представить сертификат, либо ввести имя и пароль (Client Certificate = Yes, Name & Password = Yes). Domino сначала попытается применить базовую аутентификацию. Если ее не удастся выполнить (например, сервер не доверяет сертификату клиента), Domino потребует ввести имя и пароль, которые будут сравниваться с персональным документом в каталоге Domino.

При открытии порта SSL Domino не позволит сохранить серверный документ, если оба параметра аутентификации SSL не будут установлены в No.

Дополнительная настройка, необходимая для секционированного сервера

Если почтовый сервер IMAP является секционированным сервером Domino, надо добавлять в файл notes.ini, который находится в папке данных сервера, переменную IMAPAddress=IP Address или IMAPAddress=Fully Qualified Domain Name, где IP Address - IP-адрес сервера (например, 192.168.1.12), а Fully Qualified Domain Name (FQDN) - полное квалифицированное доменное имя компьютера, но не имя Domino (например, osprey.planetnotes.com, но не Osprey/Servers/Stillwater). Какой вариант предпочесть, зависит от того, что вы чаще меняете - IP-адрес или полное имя. Сервер MailOI может иметь следующие переменные: POP3Address=10.0.0.10 или POP3Address=domsrv01.planetnotes.com.

Запуск задачи сервера IMAP

Можно запустить (и остановить) задачу сервера IMAP вручную или активизировать ее автоматически при запуске сервера Domino. Удобнее, конечно, чтобы эта задача запускалась автоматически и работала постоянно.

Чтобы настроить автоматический запуск IMAP, добавьте IMAP в конец переменной ServerTasks в файле notes.ini сервера. Например, если переменная ServerTasks определена следующим образом:

```
ServerTasks=Router, Replica, Update, Amgr, AdminP, HTTP
```

измените ее так:

```
ServerTasks=Router, Replica, Update, Amgr, AdminP, HTTP, IMAP
```

Файл notes.ini может находиться либо в каталоге программ сервера Domino, либо (на секционированных серверах) в каталоге данных сервера Domino, либо (на серверах под управлением Windows, обновленных с версии R4.x) в папке Windows. Файл допускается редактировать или непосредственно в текстовом редакторе, или опосредованно - с помощью команды, вводимой с консоли сервера, или добавив переменную ServerTasks в документ конфигурации сервера.

Чтобы внести значение с консоли сервера, сначала необходимо определить текущее значение этой переменной командой Show Config ServerTasks. Затем (если переменная задана как в предыдущем примере) вводится команда

```
Set ConfigServerTasks=Router, Replica, Update, Amgr, AdminP, HTTP, IMAP
```

При использовании данного метода необходимо набирать команды очень аккуратно. Опечатка приведет к ошибке сервера при следующей перезагрузке. Проверьте правильность команд несколько раз.

Чтобы использовать для установки этой переменной документ конфигурации сервера, откройте вкладку Configuration (Конфигурация) в Domino Administrator, затем загрузите существующий файл конфигурации сервера либо создайте новый. В окне **NOTES.INI Settings** выберите **Set/Modify Parameters** (Установить/изменить параметры). В поле **Item** (Элемент) введите значение **ServerTasks**, а в поле **Value** (Значение) - полную строку серверных задач, разделенных запятыми. После этого щелкните по **Next** и по **OK**. Сохраните и закройте документ.

Еще раз напомним, что надо очень тщательно проверять каждое вносимое значение. Чтобы минимизировать вероятность опечатки, лучше скопировать в буфер значения из файла notes.ini и затем вставить их в нужные поля. При этом вручную придется вводить небольшую часть информации.

Вручную задачу ШАР можно запустить с помощью либо консоли сервера, либо программы Domino Administrator. Для запуска служит команда load IMAP, а для остановки - команда tell IMAP quit или tell IMAP exit.

При работе с Domino Administrator откройте вкладку **Server => Status**. На панели **Task** выберите **Start**, затем в диалоговом окне отметьте **IMAP Mail Server**. После запуска эта задача появляется на панели **Results**. Чтобы ее остановить, выделите любую копию ШАР на панели **Results**, затем укажите на панели **Task** команду **Stop**.

Регистрация пользователей IMAP

Пользователь почты ШАР необязательно будет иметь файл идентификационных данных, если он не является и пользователем Notes. Следовательно, достаточно вручную зарегистрировать пользователя ШАР (если требуется), создав для него персональный документ и почтовую базу данных и добавив его имя в требуемую группу. С другой стороны, можно

воспользоваться диалоговым окном **Register Person** (Регистрация сотрудника) - и Domino Administrator сделает всю работу за вас. Необходимо только обратить особое внимание на значения в некоторых полях.

Чтобы зарегистрировать пользователя почты ШАР:

1. Создайте персональный документ. В Domino Administrator откройте вкладку **People & Groups**, выберите ШАР-сервер Domino (или другой сервер в том же домене), откройте вид **People** (Сотрудники) и выберите **Add Person** (Добавить сотрудника). Заполните поля, описанные в табл. 17.2.

Таблица 17.2. Настройка диалогового окна **Add Person**

Название поля	Описание
На вкладке Basics (Основные параметры)	
First name (Имя)	Заполните все три поля. Имя пользователя (User name)
Last name (Фамилия)	должно быть комбинацией имени (First name) и фамилии.
User name (Имя пользователя)	(Last name)
Internet password (Internet-пароль)	Пароль, который будет служить пользователю для доступа к своей почте. Не оставляйте это поле пустым
На вкладке Mail (Почта)	
Mail system (Почтовая система)	Выберите POP или IMAP
Domain (Домен)	Имя домена почтового сервера
Mail server (Почтовый сервер)	Полное различающееся имя Notes для почтового сервера IMAP
Mail file (Почтовый файл)	Частичный путь (начиная с каталога данных Domino) и имя файла почтовой базы данных пользователя (например, data\filename). Расширение .nsf в имени файла можно не указывать
Forwarding address (Почтовый адрес пересылки)	Не заполняйте
Internet address (Internet-адрес)	Введите допустимый адрес электронной почты пользователя. Этот же адрес должен быть указан в его почтовой программе
Format preference for incoming mail (Предпочтительный формат для входящих сообщений)	Выберите Prefers MIME (Предпочтение MIME)
Encrypt incoming mail (Шифрование входящих сообщений)	Установите No

2. Добавьте пользователя в требуемую группу.
3. Создайте почтовый файл на сервере IMAP. Он формируется на основе шаблона **Mail(R5.0)** в версии R5 или **Mail(6)** в версии R6. Полезно дополнительно построить полнотекстовый индекс, чтобы IMAP-пользователь мог выполнять поиск.
4. В списке ACL нового почтового файла установите доступ по умолчанию No **Access**, а для пользователя и почтового сервера - уровень доступа **Manager** с правом **Delete Documents**. Остальные записи, включая собственную, удалите.

Если вы регистрируете почтового пользователя в окне Register Person, выберите опцию Advanced (Дополнительно) в левом верхнем углу и заполните поля как обычно, учитывая исключения, описанные в табл. 17.3.

Таблица 17.3. Настройка диалогового окна Register Person

Название поля	Описание
	Вкладка Mail (Почта)
Mail system (Почтовая система)	Выберите IMAP
Create full text index (Создать полнотекстовый индекс)	При включении этого параметра для клиентских программ IMAP появляются дополнительные возможности
	Вкладка ID INFO (Идентификационная информация)
Location for storing user ID (Место хранения ID-файла пользователя)	Сбросьте флажки In Domino Directory (В каталоге Domino) и In file (В файле). При этом ID-файл, который пользователь не будет применять вообще, не создается

Разрешение доступа IMAP к почтовым базам данных Notes

Хотя почта Notes и ШАР достаточно похожи, почтовые базы данных Notes не идентичны ШАР. Чтобы установить соответствие, необходимо запустить для них программу преобразования - ту же самую, к которой вы обращаетесь при преобразовании почтовых баз данных R4 в формат R5, но с параметром -t. При этом синтаксис команды, вводимой с консоли сервера, выглядит следующим образом:

```
load convert -m MailFilePathName
```

где MailFilePathName - частичный путь (относительно каталога данных Domino) и имя почтового файла или почтового каталога. Например, чтобы применить параметры настройки ШАР для базы данных Джо Доукса (Joe Doaks), расположенной в почтовой папке, введите следующую команду:

```
loadconvert -mmail\doaks.nsf
```

Установить параметры ШАР для каждой базы данных в почтовой папке позволяет команда

```
loadconvert -mmail\* .nsf
```

И наконец, если вы не сформировали полнотекстовый индекс почтовой базы данных при ее создании, сделайте его сейчас. В отличие от клиентов POP3, клиенты IMAP в состоянии выполнять поиск в почтовых базах. Чтобы включить полнотекстовый индекс существующей базы, выберите его на вкладке Files (Файлы) в Domino Administrator, а затем на панели Tools в разделе Database укажите Full Text Index.

Настройка почтового программного обеспечения пользователей

Точная настройка клиентской программы, конечно, зависит от самой программы. Однако в любом случае необходимо ввести следующую информацию:

- О полное квалифицированное имя домена почтового сервера ШАР (например, osprey.planetnotes.com);
- О полное квалифицированное имя домена сервера SMTP;
- О имя учетной записи пользователя, в качестве которого выступает имя пользователя, указанное в персональном документе, который вы создали;
- О префиксы каталогов, служащие корневыми каталогами.

Domino не использует префиксы каталогов, а ШАР использует. При настройке клиента ШАР можно не указывать префиксы. Например, в Outlook Express не заполняется поле **Root folder path** (Путь к корневому каталогу), в Netscape Messenger - поле **IMAP Server Directory** (Серверный каталог ШАР), а в Simeon 4.1 - поля **Folder Prefix** (Префикс каталога) и **Folder location** (Размещение каталога).

Некоторые клиенты ШАР не позволяют не указывать эти значения. В таких программах допускается просто задать полное имя домена сервера ШАР в среде Domino. Так, в PC-Pine необходимо что-нибудь поместить в полях **INBOX-PATH** и **Folder collections**. Если FQDN (полное квалифицированное доменное имя) вашего сервера - osprey.planetnotes.com, можно ввести INBOX-PATH {osprey.planetnotes.com} INBOX и Folder collections {osprey.planetnotes.com}.

Настройка службы IMAP

Для настройки порядка работы почтовой службы ШАР существует определенный набор переменных в файле notes.ini (табл. 17.4).

Таблица 17.4. Переменные файла notes.ini

Переменная	Описание
IMAPExactSize=3Ha4eHHe	Установите 1, чтобы сервер IMAP возвращал точный размер MIME-сообщений. По умолчанию — 0, то есть возвращается примерный размер. Domino проще оценивать, а не определять точный размер сообщения, поскольку вычисление точного размера сильно расходует ресурсы сервера. В качестве альтернативного варианта можно включать или выключать параметр IMAP server returns exact size of messages (IMAP-сервер возвращает точный размер сообщений) в документе конфигурации. Когда эти параметры установлены и в документе конфигурации, и в файле notes.ini, значение в документе конфигурации имеет преимущество
IMAPGreeting=npHBeTCTBHe	Указывается приветствие, которое сервер IMAP отправляет ¹ соединившимся клиентам. Когда это поле остается пустым, посылается следующее приветствие: OK Domino IMAP4 Server V. 5.0 ready Mon, 10 May, 1997 17:57:13 -0500
IMAPRedirectSSLGreeting сообщение	Указывается сообщение, которое сервер IMAP отправляет клиенту, переадресованному с TCP/IP-порта на SSL-порт
IMAPSSLGreeting= приветствие	Задается приветствие, которое сервер IMAP направляет соединившимся клиентам, подключившимся через порт SSL. Если поле пустое, отсылается следующее приветствие: OK Domino IMAP4 Server V. 5.0 ready Mon, 10 May, 1997 17:57:13 -0500
IMAP_Config_Update_ Interval=минуты	Назначается частота, с которой сервер IMAP проверяет изменения конфигурации. Если эта переменная не указана, наличие изменений проверяется каждые 2 минуты

Таблица 17.4. Переменные файла *notes.ini* (окончание)

Переменная	Описание
IMAP_Session_	Определяется период, после которого сервер IMAP разрывает неактивный сеанс клиента. Если данная переменная не установлена, сервер будет разрывать сеанс через 30 минут. Специалисты Lotus рекомендуют назначать не менее 10 минут, поскольку некоторые пользователи проверяют почту каждые 10 минут. Издержки при поддержке неактивных сеансов меньше, чем при разрыве сеанса и новом подключении

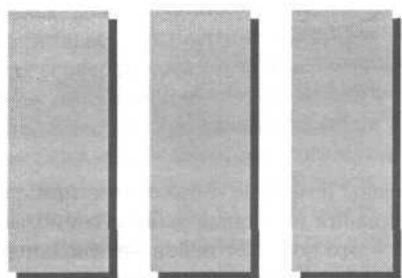
Контроль работы службы IMAP

Чтобы убедиться в правильной настройке службы ШАР, установите один или несколько зондов сервера TCP. Рекомендуется протестировать сервер IMAP. Зонд можно создать в программе Domino Administrator на вкладке **Configuration**. Выберите **Statistics & Events => Probes => TCP Server** (Статистика и события => Зонды => TCP-сервер) на панели **Tasks**. Затем на панели **Actions** (выше панели **Results**) выберите **New TCP Server Probe** (Создать зонд TCP-сервера). Если такого зонда еще нет, создайте его и в нем выберите **All Domino servers in the domain will probe their own configured ports** (Все серверы Domino в данном домене будут тестировать свои настроенные порты). Кроме того, создайте хотя бы один зонд, в котором один сервер будет тестировать другой.

Если на каждом тестируемом сервере работает задача Event, создание зонда заставит сервер сгенерировать статистику качества обслуживания для каждой службы Internet. Кроме того, в базе данных **Statistic Reports** появляются предупреждения, когда истекает лимит времени до момента отклика от тестируемой службы.

Статистику можно посмотреть на панели **Statistics** вкладки **Server** в Domino Administrator и дополнительно на панели **Monitor**. Если на сервере запущена служба Collector (Сбор статистики), которая накапливает статистику о данном сервере, то статистические отчеты также добавляются в базу данных **Statistic Reports**. Более подробно это обсуждается в главе 18.

ЧАСТЬ



ОПТИМИЗАЦИЯ
СЕРВЕРА

ГЛАВА

18



МОНИТОРИНГ СЕРВЕРА

В этой главе рассматриваются инструменты и методы сбора статистики о производительности в целях идентификации, отслеживания и анализа работы системы. Данную главу необходимо изучать вместе с главой 19 - это поможет найти оптимальный путь улучшения производительности для конечного пользователя. По мере увеличения инвестиций компании ожидается повышение уровня обслуживания и возврат этих инвестиций. Появление приложений электронной коммерции подразумевает, что сервер Domino должен иметь такую производительность, чтобы приносить прибыль, а не убытки.

Почему важен мониторинг системы

Мониторинг - это достаточно важное средство, снабжающее администратора значимой информацией об общей производительности системы и ее компонентов:

- получение сведений в результате мониторинга общих системных функций - первый шаг к обеспечению надежности служб, предоставляемых пользователям;
- данные мониторинга функций стратегических системных компонентов являются достоверными. При этом не нужно полагаться на видимые улучшения при модификации аппаратного устройства сервера, его программного обеспечения и сетевой системы;
- использование мониторинга экономит деньги, помогает избежать простоев и облегчает принятие решений в критическом режиме;
- XD в процессе мониторинга системных ресурсов выявляются возникающие проблемы и необходимость обновления оборудования, прежде чем приложения и пользователи исчерпают все ресурсы;
- повышение надежности ведет к увеличению эффективности.

Администраторы, связанные с электронной коммерцией, наверное, хорошо помнят некоторые события, в частности ситуацию, возникшую на сайте-аукционе eBay (www.ebay.com). Череда сбоев системы принесла огромные неприятности пользователям и инвесторам. Обычно сбои системы в компаниях не выставляются напоказ. Однако повышенное внимание к электронной коммерции в наши дни сделало eBay исключением из общих правил.

Официальные заявления, в которых говорилось о «проблемах инфраструктуры», были встречены с неодобрением. С момента первого сбоя на сайте возникало множество неполадок, что привело к необходимости отключить систему на несколько дней и вызвало огромные расходы вместе со снижением репутации компании. Накануне наверняка были какие-либо знаки, предупреждающие о неблагополучии. Серверы редко «умирают» внезапно. Они сначала вызывают о помощи. В основном мониторинг системы призван помочь «услышать» эти призывы.

Чтобы найти какую-либо информацию о сбоях в eBay, попробуйте задать слово «eBay» в любой поисковой системе. Вероятно, сведения, которые вы найдете, будут исчерпывающими для человека, планирующего создать коммерческий сайт.

Мы не ограничиваем обсуждение программным обеспечением Lotus. Сервер Domino работает поверх серверов, соединенных с помощью сетевых карт и различных протоколов с сетями во всем мире. Следовательно, мониторинг функций и взаимодействия этих систем должен представлять для администратора Domino особый интерес. В данной главе рассматривается система Domino, а не только сервер. Кроме того, поскольку большинство систем Domino работают на платформе Windows NT, особое внимание уделено именно этой операционной системе. Однако Domino может функционировать на других платформах, поэтому администраторам и консультантам нужно знать и о том, как программное обеспечение ведет себя в разных операционных средах.

Инструменты идентификации

В этом разделе описываются ресурсы для мониторинга. Презентации Lotus посвящены мониторингу системы для Windows NT, а средства для UNIX и AS/400 упоминаются лишь вкратце. Ниже представлен краткий обзор средств мониторинга и источников, из которых можно более подробно узнать о них:

- SAR (System activity reporter - репортёр деятельности системы) предлагает счетчики загрузки процессора, буфера, активности ввода/вывода дисков и магнитной ленты, активности телетайпа, активности переключений и системных вызовов, доступа к файлам, активности очередей, межпроцессного взаимодействия и страничной подкачки;
- VMSTAT предназначена для генерации статистических отчетов о виртуальной памяти. В системе UNIX, когда исчерпываются ресурсы оперативной памяти, ядро начинает работать с виртуальной памятью. Команда VMSTAT имеет следующий синтаксис:

```
vmstat [-{options}][disks] [interval] [count]
```

С помощью аргументов interval и count можно задавать интервал времени между отчетами (в секундах) и число интервалов, что позволяет наблюдать за работой памяти в интерактивном режиме;

- IOStat служит для генерации статистических отчетов об обращении к процессору, дискам и устройствам ввода/вывода. Помогает определить, где в системе возникают проблемы ввода/вывода. Команда iostat может использоваться для отображения объема данных, переданных между системой и диском или терминальным устройством;

- О NetStat отображает состояние сети. Генерирует отчеты о сети, например об использовании памяти ядра. Буферы памяти ядра обеспечивают быструю передачу входных данных в ядро. Недостаточные объемы буферов могут вызвать значительное снижение пропускной способности. Безопасно выделить большее число буферов удастся за счет увеличения объема памяти. Однако в некоторых операционных системах UNIX можно управлять объемом памяти, выделяемой для буферов;
- О Perfometer показывает производительность системы с помощью множества круговых диаграмм или гистограмм для системы SUN. Perfometer оценивает использование процессора, проблемы и трафик локальной сети, подкачку, прерывания устройств и загрузку.

Информация о мониторинге системы UNIX имеется на сайтах фирм-изготовителей, но существует также несколько других сайтов, на которых размещено много полезных сведений. Можно начать с UNIX Guru Universe по адресу www.ugu.com и UNIX System Administration Independent Learning (USAIL) по адресу www.uwsg.com.

IBM и Lotus расхвалили достоинства работы Domino на современной платформе AS/400. Встроенный монитор производительности AS/400 позволяет собирать сведения о памяти, диске, контроллере данных и сетевых данных. Поскольку среда достаточно специфическая, специалисты IBM предположили, что возникнет множество запросов информации о конфигурации и производительности Domino на базе AS/400. Обратитесь на следующие сайты:

- О www.as400.ibm.com/developer/domino/perform - данные о производительности и способах устранения известных проблем;
- О <http://www.as400.ibm.com/lotus-notes/notes.htm> - сведения о Domino на базе AS/400;
- О http://www.as400.ibm.com/lotus_notes/nnfaq_1b.htm - список часто задаваемых вопросов о Domino на базе AS/400.

Компания IBM выпустила по крайней мере четыре Красных книги по Domino 5 на базе AS/400. Аналогичные публикации ожидаются и для версии R6. Будут рассматриваться вопросы установки, администрирования, настройки производительности и секционирования серверов Domino. Красные книги по большинству платформ Domino можно найти по адресу www.redbooks.ibm.com.

Еще один инструмент (он не обсуждается в данной книге), предназначенный для более глубокого исследования, для мониторинга событий и откликов - это Tivoli Manager, поставляемый компанией IBM отдельно и в составе версии R6. Tivoli позволяет перезагружать сбойный сервер и проводить соответствующее администрирование по сети. Подробнее об этом рассказывается в «Managing Domino/Notes with Tivoli Manager, Enterprise Edition, Version 1.5, SG24-2104».

Ниже перечислены инструменты мониторинга системы Domino на базе NT:

- О Диагностика Windows NT;
- О Диспетчер задач;
- О Системный монитор;
- О консоль сервера Domino;
- О журнал транзакций Domino;
- О анализ журнала транзакций Domino;
- О задачи Collect, Event, MTC и ISpy;
- О база данных Statistics & Events;
- О база данных Reports;
- О монитор сервера Domino. • •

Все указанные элементы, кроме Диагностики Windows NT, Диспетчера задач и монитора производительности, присутствуют и на других платформах. В данной главе описано также несколько средств, увеличивающих возможности средств мониторинга.

Среда

Основные подсистемы (процессор, память, жесткий диск и сеть) в зависимости от роли системы используются по-разному, причем различия необходимо установить во время настройки и мониторинга. Этот принцип необходимо применить как на уровне операционной системы, так и на уровне сервера Domino. Система NT может работать как файловый сервер, сервер приложений или сервер домена любой организации.

В общем случае серверы Domino служат в качестве серверов приложений, поскольку пользователи обращаются к ним в рамках модели клиент/сервер через интерфейсные приложения. По сути, процессор и память используются в большей степени. Это не значит, что жесткий диск и сетевые подсистемы не применяются.

Далее рассматривается работа сервера в системе Domino. Сервер-концентратор, почтовый сервер и сервер приложений Domino выполняют разные функции, поэтому при мониторинге и конфигурировании надо найти наиболее вероятные «узкие места» домена, где возможна нехватка системных ресурсов определенного типа.

Отслеживание использования

Когда на сервере работает Domino, все процессы и выбранная серверная задача эксплуатируют одну или несколько подсистем сервера. Определение подсистемы, которая обслуживает каждую задачу, позволяет получить информацию о том, как надо контролировать систему и где искать возможные проблемы. Например, почтовому серверу и серверу-концентратору требуются разные ресурсы. Хотя работа обоих серверов сильно зависит от дисковой подсистемы, остальные выполняемые функции могут существенно различаться. К почтовому серверу непосредственно обращаются пользователи, и кроме стандартных почтовых служб Notes он в состоянии взаимодействовать с почтовыми службами Internet. Операционная система, сетевые интерфейсы, Domino и клиентское программное обеспечение функционируют как единая система. Ни одна из подсистем не может измениться, не повлияв на работу остальных подсистем.

Мониторинг и настройка - две части единого целого. Мониторинг предоставляет информацию о настройке производительности и использует эту информацию для регулирования одной или нескольких подсистем. Параметры настройки следует контролировать, чтобы получать дополнительные результаты и прогнозировать, какие изменения позволят улучшить производительность. В некоторый момент вы увидите, что система работает безупречно. Данные передаются, пользователи счастливы - можно сидеть и отдыхать. Только после того как опасность миновала, наступает время, когда можно спокойно пойти домой по окончании рабочего дня.

Определение базы

База (базовый уровень) представляет собой начальную точку для сравнения. Это очень важное понятие определяет эталон, с которым сопоставляется информация при мониторинге системы. Базу необходимо установить при вводе сервера в действие или перед

наращиванием его мощностей. Допустимо сравнивать с начальным уровнем эффект от изменения конфигурации и информации о пользователях, от установки программ, запуска процессов.

Включите в базу измерения памяти, процессора, диска и сетевых объектов, а также счетчики Notes. Когда начнут применяться ресурсы сервера, вы сумеете оценить отклик системы и действовать соответствующим образом. В таблицах, приведенных ниже, вы найдете информацию о конкретных объектах и счетчиках, которые необходимо включить. Лучше всего сгенерировать базу для рабочего и нерабочего времени, чтобы можно было исследовать отклонения от нормы.

Мониторинг, анализ и настройка системы требуют постоянной фиксации результатов. Далее в настоящей главе представлен обзор инструментов для мониторинга сервера Domino в среде Windows NT.

Правило цепной реакции при настройке производительности

Эмпирическое правило заключается в том, что метод устранения недостатка ресурсов в одной подсистеме, вызывает нехватку ресурсов в другой подсистеме. Мониторинг позволяет определить, кем или чем обусловлены изменения системных функций — пользователями, чрезмерной нагрузкой элементов системы или настройкой.

Средства мониторинга Windows NT

В последующих разделах рассматриваются средства мониторинга, имеющиеся в операционной системе Microsoft Windows NT. Многие средства присутствуют в самой операционной системе, а некоторые включены в набор NT Resource Kit и в его дополнения. Для получения более подробной информации стоит посмотреть документацию по Windows NT Server, Workstation и Resource Kit:

- Диагностика Windows NT (winmsd.exe);
- Диспетчер задач (taskman.exe);
- Системный монитор (perfmon.exe);
- служба регистрации данных (datalog.exe);
- средство мониторинга (monitor.exe);
- планировщик заданий WinAT (winat.exe);
- служба регистрации данных о производительности (perflog.exe).

Диагностика Windows NT

Эта утилита предоставляет данные о сети и компьютере. Администратор в состоянии просматривать, сохранять в файле или распечатывать отчеты, содержащие сведения о протоколах, устройствах отображения, службах, ОС и установленных в ней пакетах обновления, драйверах, прерываниях и портах. Сохранив копию отчета, можно получить некоторую базовую информацию. Допустимо распечатывать обновленные отчеты после изменений конфигурации системы, например после добавления жестких дисков. На рис. 18.1 изображено окно **Windows NT Diagnostics**.

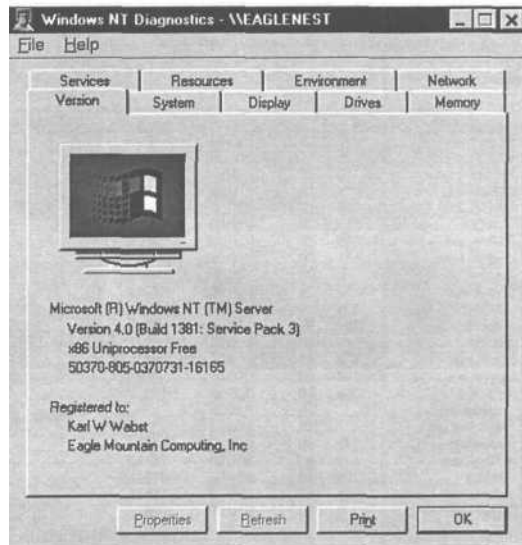


Рис. 18.1. Перейдите на соответствующую вкладку в окне Windows NT Diagnostics, чтобы просмотреть информацию или распечатать отчет

Диспетчер задач

Диспетчер задач обычно является первым остановочным пунктом администратора при возникновении проблемы с производительностью. Эта утилита предоставляет часть сведений, собранных Диспетчером производительности (Performance Manager).

На вкладке **Application** (Приложения) представлены данные о программах, работающих в системе на текущий момент. Беглый взгляд на эту вкладку позволяет определить, функционирует приложение или оно не отвечает на запросы системы. Чтобы быстро перейти к соответствующему процессу на вкладке **Processes** (Процессы), достаточно щелкнуть правой кнопкой мыши по нужному приложению, а не листать длинный список процессов.

На вкладке **Processes** (рис. 18.2) показаны все работающие в данный момент процессы. По умолчанию выводится три столбца. Чтобы на экране появилась дополнительная информация о процессах, выберите **View => Select Columns** (Вид => Выбрать столбцы). Щелкнув правой кнопкой мыши по процессу, установите для него приоритет. Предлагаются следующие варианты: **High** (Высокий), **Normal** (Обычный), **Low** (Низкий) и **Realtime** (Реального времени).

Последствия использования процессов реального времени

Выбирая приоритет реального времени для процесса, вы помещаете процесс над исполняемыми службами, которые отслеживают и отвечают на запросы клавиатуры. Используйте этот вариант только для программ, которые имеют заранее определенную точку выхода. Если вы, например, установите такой уровень приоритета для `nserver.exe`, то потребуются перезагрузить сервер, чтобы восстановить управление системой.

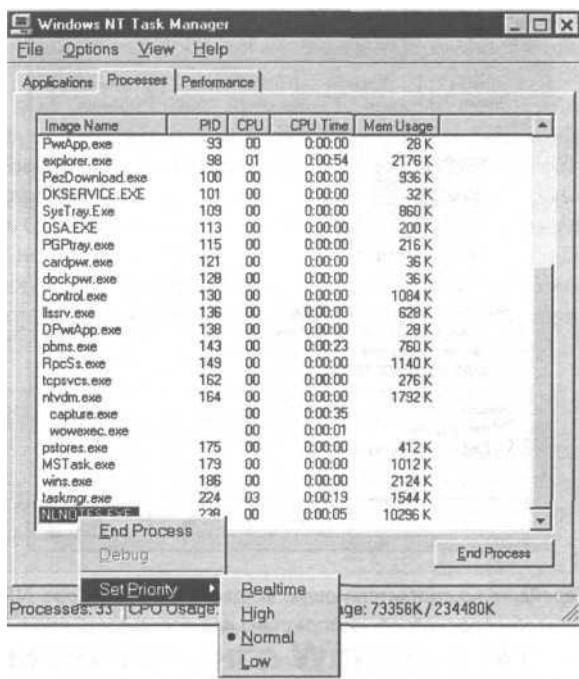


Рис. 18.2. Приоритет процесса обычно устанавливается в программном коде.
С помощью Диспетчера задач можно изменить приоритет работающего процесса

Система обрабатывает запросы от процессов в порядке их приоритета. Кроме того, процесс с низким приоритетом может быть прерван при запросе от процесса, имеющего высший приоритет. Изменения приоритетов рабочих процессов действительны только для текущего сеанса. При следующем запуске процесса он имеет приоритет, определенный программно.

На вкладке Performance (Производительность) представлена информация об использовании ресурсов (рис. 18.3). Проконтролировать производительность системы за определенный промежуток времени лучше Системным монитором.

ф

Системный монитор

Системный монитор позволяет отслеживать, анализировать и получать отчеты о работе различных подсистем NT, включая процессор, память, жесткие диски и сетевые ресурсы. Службы NT обеспечивают возможность автоматизировать процесс, чтобы администратор сумел зафиксировать информацию о производительности в определенные интервалы времени независимо от расписания. Запуск монитора производительности для новой или модернизированной системы позволяет определить базу для последующего сравнения производительности.

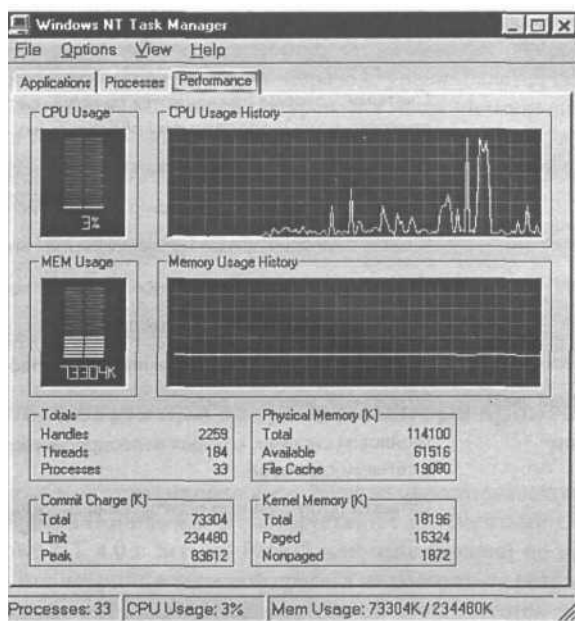


Рис. 18.3. На вкладке Performance выводится информация о текущем использовании процессора и памяти

Термины

Уделим внимание определению некоторых терминов, которые можно встретить в самой программе монитора производительности и в посвященной ему литературе. Многие администраторы Domino знакомы со средствами мониторинга, но не все читатели являются администраторами систем NT.

Объекты ядра

Объекты представляют системные ресурсы, такие как физические (смонтированные в компьютере) устройства, потоки, процессы и разделы общей памяти. Под *объектами ядра* понимается список объектов, которые по умолчанию включены в Системный монитор. Объекты появляются только для реально используемых компонентов, поэтому дополнительные объекты могут создаваться по мере добавления программ или служб. В табл. 18.1 приведен список объектов ядра NT. Некоторые объекты устанавливаются автоматически, а остальные нужно устанавливать отдельно. Например, некоторые счетчики TCP/IP недоступны, пока не запускается SMTP, а объекты Notes (и соответствующие экземпляры) недоступны до тех пор, пока не будут инициализированы из программы установки Domino.

Таблица 18.1. Объекты ядра монитора производительности NT

Объект	Описание
System (Система)	Счетчики, которые применяются ко всему системному программному и аппаратному обеспечению
Memory (Память)	Оперативное запоминающее устройство
Cache (Кэш)	Область памяти, которая хранит недавно используемые данные
Paging File (Файл подкачки)	Файлы, служащие для размещения виртуальной памяти
Processor (Процессор)	Физический процессор, установленный на компьютере
Thread (Поток)	Часть процесса, применяющая процессор
Physical Disk (Физический диск)	Установленные жесткие диски или устройства RAID
Logical Disk (Логический диск)	Разделы физического диска
Redirector (Редиректор)	Файловая система, которая переадресует запросы к сетевым серверам
Objects (Объекты)	Объекты программного обеспечения системы

Экземпляры

Экземпляр - это подмножество объекта. Так, если вы работаете на сервере с несколькими процессорами, объект процессора будет иметь три экземпляра - по одному для каждого процессора (0 или 1) и еще один экземпляр для Total (Общее значение). Выберите 1 или 0, чтобы установить счетчики для любого процессора, и Total - для обоих процессоров.

*

Счетчик

Счетчик определяет тип данных, доступный для выбранного типа объектов. Счетчики выдают отчеты о таких характеристиках, как деятельность, запросы и пространство, используемое объектом. Когда задается один из счетчиков, включаются все счетчики для указанного объекта, но выводятся только данные для выбранного счетчика. Щелкните по кнопке Explain (Объяснить) в окне Add to Chart (Добавить в диаграмму), чтобы увидеть определение этого счетчика.

Системный монитор содержит три типа счетчиков, отображающих:

- Averaging (Усредняющий) - среднее значение; #
- Instantaneous (Мгновенный) - последнее значение;
- Difference (Счетчик несовпадений) - разница между последним и предыдущим значениями. Отрицательные значения выводятся в виде 0. В основном наборе счетчиков в мониторе производительности нет счетчика несовпадений.

Накладные расходы

При запуске средств мониторинга нужно определенное количество системных ресурсов. Поскольку каждая задача потребляет ресурсы, запуск монитора производительности в тестируемой системе будет влиять на результаты. Накладные расходы состоят из аппаратных и сетевых ресурсов, необходимых для вычисления, хранения и отображения результатов.

..

Использование монитора производительности предоставляет возможность централизовать накопление статистики для нескольких серверов. Имейте в виду, что когда монитор производительности функционирует таким образом, увеличивается сетевой трафик. Может быть, лучше локально накапливать ресурсы и в часы наименьшей активности сети передавать данные в центральный пункт сбора информации. Прибегая к локальному накоплению статистики и общему сбору по сети, администратор должен рассмотреть соотношение «цены и качества».

Какой счетчик выбрать?

Наиболее важный счетчик тот, который автоматически выделяется при выборе объекта в мониторе производительности.

Проблемы, возникающие при запуске монитора производительности на сервере Domino

При удаленном запуске монитора производительности опасайтесь документированных экземпляров аварий сервера Domino 4.x. В соответствии с документами Lotus, на сервере под управлением Windows NT 4.0 с Service Pack 2 или выше аварий не происходит. Однако разумнее проводить мониторинг в тестовой среде, а не доверяться результатам мониторинга, выполненного в рабочей среде. Информация об этом имеется в Technote #142687 и #172380. Перед обновлением Domino до версии R5/6 убедитесь, что на сервере установлен нужный пакет обновления Service Pack. Возникают проблемы и при запуске монитора производительности на той же машине, на которой функционирует средство мониторинга Insight Manager Agent компании Compaq.

Журналы регистрации монитора производительности динамические. Размер журнала зависит от выбранных параметров и времени, в течение которого работает утилита. Эти журналы необходимо хранить на дисках, имеющих большие объемы свободного пространства. Файлы журналов также влияют на системную статистику. При сборе информации с помощью монитора производительности в течение длительного времени убедитесь, что на установленном диске достаточно свободного места. Измените интервал обновления (Update Time). При задании более длительных интервалов сокращаются размеры файлов и накладные расходы. По умолчанию во многих случаях интервал обновления равен одной минуте.

Критический элемент

Критический элемент («узкое место») - это место в системе с низкой производительностью. Целью мониторинга системы является обнаружение критических элементов и осуществление соответствующих действий для повышения производительности. Зачастую проблема в одном месте вызывает понижение производительности других компонентов системы. Следовательно, при мониторинге необходимо рассматривать систему в целом, а не фокусировать внимание на определенных ее компонентах.

Если, например, на сервере мало физической памяти, система начнет использовать файлы подкачки. По мере роста скорости подкачки увеличивается нагрузка на диск и процессор. При ухудшении ситуации возможно снижение производительности для конечного пользователя. Увеличение объема диска и мощности процессора облегчает положение, а добавление дополнительного объема оперативной памяти полностью решает проблему.

Добавление объекта Domino и счетчиков

Системный монитор в состоянии отображать данные из встроенных программ, таких как Domino. Администратору очень удобно собирать информацию обо всей системе, включая Domino, с помощью одной программы с общим интерфейсом. Дополнительное преимущество состоит в способности сопоставления статистики операционной системы со статистикой Domino. При этом отчеты содержат прекрасные результаты для управления системой.

Чтобы добавить объект и счетчики Lotus Notes для Domino, необходимо выбрать **Notes Performance Monitor** (Системный монитор Notes) во время установки Domino, либо перезапустить установку и указать только **Notes Performance Monitor** - в каталог программ Domino добавится файл notesreg.bat.

Пакетный файл запускается из командной строки. К нему дописывается параметр, включающий полный путь к каталогу программ сервера Domino. Программа обновляет регистр Notes и делает мониторы Domino доступными для монитора производительности ОС. После установки счетчиков Notes перезагрузите компьютер.

В данном примере каталог программ сервера расположен в D:\Lotus\Domino. Откройте командную строку и введите

```
notesreg.bat D: \Lotus\Domino
```

При следующем запуске монитора производительности будет доступен объект Lotus Notes. Экземпляры, отображаемые монитором производительности, знакомы администраторам, которые применяли команду show stat для сервера Domino.

Средство мониторинга Domino также следует настроить, поскольку оно предоставляет более подробную информацию о работе сервера Domino. Кроме того, Системный монитор не всегда функционирует в каждой ОС. Статистика Domino накапливается только тогда, когда запущен сервер Domino.

Запуск Системного монитора

Системный монитор можно запустить вручную или автоматически. Ручной запуск производится, когда требуется выборочная проверка производительности сервера, а автоматический запуск служит для плановой проверки сервера в назначенное время или в часы минимальной активности. Файлы настройки позволяют устанавливать контролируемые счетчики для данного сеанса. Файл настройки - это обобщенный набор объектов и счетчиков, предназначенных для определенных функций. Они особенно полезны при автоматических проверках для отслеживания состояния сервера.

*

Запуск вручную

Системный монитор запускается в Windows NT с помощью пунктов меню **Start => Administrative Tools** (Пуск => Администрирование) или из командной строки путем ввода команды PERFMON. При запуске из командной строки необходимо указать файл настройки. Расширения файлов определяют вид монитора производительности, для которого предназначен файл настройки (табл. 18.2).

Таблица 18.2. Расширения файлов, используемые при создании файлов настройки

Расширение файла настройки	Вид монитора производительности
.pta	Alarm (Предупреждение)
.pte	Chart (Диаграмма)
.pml	Log (Журнал регистрации)
.pmr	Report (Отчет)
.pmw	Workspace (Рабочая область)

Заставьте Domino заполнить счетчики монитора производительности

После установки счетчиков Domino в Системный монитор откройте консоль сервера Domino и введите команду `show statistic`. Счетчики не появятся в мониторе производительности до тех пор, пока соответствующая программа не обновит статистику. Команда `show statistic` заставляет это сделать.

Автоматический запуск

Сбор информации монитором производительности можно автоматизировать. Желательно установить автоматический мониторинг системы, чтобы информация поступала через назначенные промежутки времени, а не в зависимости от желаний и возможностей администратора. Автоматизация процесса позволяет накапливать статистику о нескольких серверах через одинаковые временные интервалы, а также в нерабочие часы.

Чтобы включить автоматический запуск монитора производительности, сначала убедитесь, что на каждом сервере запущена служба планирования (Scheduling Service). Для автоматического запуска и остановки мониторинга служит команда AT. Если вы еще не знакомы с ней, то ее легко освоить.

Например, автоматический мониторинг на сервере Eagle в рабочие дни с 10 до 11 часов утра включается следующими командами:

```
at \\Eagle 10:00 /date:M,T,W,Th,F "monitor Start"
at \\Eagle 11:00 /date:M,T,W,Th,F "monitor Stop"
```

Дополнительные сведения о команде AT имеются в документации Windo\^s NT.

Мониторинг работы дисков

Информация о работе дисков является очень важным компонентом мониторинга системы. Отслеживание поведения физических и логических дисков помогает при устранении неполадок и способствует повышению производительности сервера Domino. Счетчики дисков в мониторе производительности не включены по умолчанию. В табл. 18.3 описаны параметры активизации счетчиков производительности дисков.

Таблица 18.3. Дополнительные флаги для управления мониторингом использования диска

Команда	Описание
diskperf -Y	Включает счетчики производительности дисков на локальном компьютере
diskperf -YE	Дополнительный параметр E необходим для оценки дисков в чередующемся наборе
diskperf -Y[E] \\<имя_сервера>	Включает счетчики производительности дисков на удаленном компьютере
diskperf -N	Отменяет накопление статистики о дисках

После этого компьютер необходимо перезагрузить, чтобы новые параметры вступили в силу.

Можно включить счетчики производительности дисков с помощью панели управления:

1. Выведите на экран панель управления.
2. Откройте окно **Устройства**.
3. Выделите **Diskperf**, щелкните по кнопке **Запуск** и выберите параметр запуска (Startup) равным **Загрузка** (Boot).
4. Перезагрузите сервер.

Мониторинг сетевого интерфейса и протокола IP

Чтобы включить мониторинг сетевого интерфейса и IP-протокола, необходимо запустить службу SNMP на сервере Windows NT. При добавлении службы SNMP в Системный монитор добавляются соответствующие счетчики.

Виды монитора производительности

Системный монитор предоставляет возможность просматривать данные в реальном времени и историю событий, а также устанавливать пороги предупреждений. Имеется всего четыре вида:

- **Chart** (Диаграмма);
- **Report** (Отчет);
- **Log** (Журнал регистрации);
- **Alert** (Предупреждение).

Эти виды описаны в последующих разделах.

Диаграмма

Вид **Chart** (Диаграмма) позволяет просматривать в реальном времени данные об объектах, счетчиках и их экземплярах. Одновременно на диаграмме допускается вывод нескольких счетчиков. Диаграммы можно настроить так, чтобы они быстро запускались при мониторинге определенных приложений или подсистем.

Отчет

Вид Report (Отчет) генерирует отчеты на основании значений одного или нескольких счетчиков. Значения записываются через интервалы времени, установленные пользователем. Усредняющие счетчики показывают средние значения за истекший интервал времени. Мгновенные счетчики отображают значения на конец этого интервала.

Журнал регистрации

На этом виде счетчики записываются в файл для последующего анализа. Данные монитора производительности могут быть экспортированы в электронную таблицу для создания месячных отчетов или отслеживания тенденций (трендов) работы системы. Интересные моменты, обнаруженные во время регистрации, стоит пометить, чтобы впоследствии вновь обратиться к ним.

Предупреждение

Как и в сервере Domino, администратор в состоянии установить пороги для счетчиков. Системный монитор может отправлять пользователю предупреждения или запускать определенную программу один раз или при каждом достижении граничного значения. Это полезно при запуске, например, *psomrpt*, когда объем свободного пространства диска становится меньше требуемого уровня.

Итоговые таблицы объектов и соответствующих счетчиков

В табл. 18.4 (и во всех следующих) представлены обобщенные данные о системных компонентах NT, связанных с ними подсистемах и счетчиках, интересных для Domino.

Таблица 18.4. Компоненты монитора производительности, которые рекомендуется контролировать, если в системе работает сервер Domino

Компонент системы	Контролируемая подсистема	Счетчики, представляющие особый интерес
Аппаратное обеспечение	Процессор	% ProcessorTime % PrivilegedTime Interrupts/Sec System: Processor Queue Length # Server Work Queues: Queue Length
	Память	Pages/Sec Available Bytes Committed Bytes Pool Nonpaged Bytes Cache Faults per second
	Диск	Disk Queue Length % DiskTime

Таблица 18.4. Компоненты монитора производительности, которые рекомендуется контролировать, если в системе работает сервер Domino (окончание)

Компонент системы	Контролируемая подсистема	Счетчики, представляющие особый интерес
		Avg. Disk/Bytes Transfer Avg. Disk/sec Transfer Disk Bytes/sec % Disk Read Time % Disk Write Time
	Сеть	Network Interface: Bytes Total/sec Network Interface: Bytes Sent/sec Network Interface: Output Queue Length Server: Bytes Total/sec TCP Segments per Second TCP Segments Retranslates per Second UDP Diagrams per Second
	Lotus Notes	Mem.Allocated NET.TCPIP.Bytes.Received NET.TCPIP.Bytes.Sent NET.TCPIP.Sessions Established.Incoming NET.TCPIP.Sessions Established.Outgoing ServerAvailabilityIndex Server.Sessions.Dropped Server.Transactions.PerMinute Server.Transactions.PerMinute.Peak Server.Users

Далее в таблицах описаны функции каждого счетчика, указанного в табл. 18.4.

Подсистема процессора

В табл. 18.5 перечислены конкретные счетчики монитора производительности, предназначенные для контроля работы процессора на сервере NT, на котором установлен сервер Domino.

Таблица 18.5. Счетчики для мониторинга установленных процессоров &

% Processor Time	Время, в течение которого процессор не обслуживает неактивные потоки. Предпочтительное значение - менее 80% (на один процессор)
% Privileged Time	Время, в течение которого процессор работает со службами системы NT
% User Time	Время, в течение которого процессор взаимодействует с пользовательскими службами
Interrupts/Sec	Число обрабатываемых процессором прерываний от приложений или устройств. Чем меньше, тем лучше

Таблица 18.5. Счетчики для мониторинга установленных процессоров (окончание)

Счетчик	Описание
System: Processor Queue Length	Длина очереди запросов процессора. Все процессы используют эту очередь, в которой потоки ожидают рабочего цикла процессора. Чем меньше, тем лучше
Server Work Queues: Queue Length	Длина очереди запросов выбранного процессора

Подсистема памяти

В табл. 18.6 входят конкретные счетчики монитора производительности, применяемые для контроля памяти на сервере NT, где работает Domino.

Таблица 18.6. Счетчики для мониторинга памяти сервера

Счетчик	Описание
Pages/Sec	Число страниц, считанных или записанных на диск при обращении к страницам памяти, которые не загружены в память. Предпочтительное значение — менее 20
Available Bytes	Объем доступной реальной памяти - свободной памяти. Чем больше, тем лучше
Committed Bytes	Объем занятой памяти, включая файлы подкачки. Чем меньше, тем лучше. Не должно превышать 70% физической памяти
Pool Nonpaged Bytes	Реальная память в ядре системы
Cache Faults per second	Скорость, с которой система должна обращаться к диску из-за того, что данные находятся не в кэш-памяти

Дисковая подсистема

В табл. 18.7 приведены конкретные счетчики монитора производительности, осуществляющие контроль работы дисков на сервере NT, где функционирует Domino.

Таблица 18.7. Счетчики для мониторинга работы дисков

Счетчик	Описание
Disk Queue Length	Число запросов ввода/вывода, ожидающих обслуживания
% Disk Time	Время, в течение которого диск занят. Частые пики выше 70% свидетельствуют о нехватке ресурсов подсистемы
Avg. Disk/Bytes Transfer	Средний объем данных, передаваемых с диска на диск
Avg. Disk/sec Transfer	Среднее время обмена данными с диском. Чем меньше, тем лучше
Disk Bytes/sec	Скорость обмена данными с диском
% Disk Read Time	Время, в течение которого диск занят запросами
% Disk Write Time	Время, в течение которого диск занят запросами

Включение мониторинга IP-протоколов

Помните: при необходимости контролировать сетевой интерфейс и IP-протокол на сервере NT следует установить и запустить задачу SNMP. Не забудьте после этого вновь применить пакет обновления Service Pack NT.

Сетевая подсистема

Табл. 18.8 показывает конкретные счетчики монитора производительности, позволяющие контролировать сетевой интерфейс сервера NT, на котором размещен Domino.

Таблица 18.8. Счетчики для сетевого интерфейса сервера

Счетчик	Описание
Network Interface: Bytes Total/sec	Общее число байтов, переданных и принятых через сетевой адаптер. Постоянные высокие значения указывают на недостаток ресурсов. Сравните с базой
Network Interface: Bytes Sent/sec	Число байтов, переданных через сетевой адаптер
Network Interface: Output Queue Length	Глубина очереди сетевых запросов
Server: Bytes Total/sec	Общее число байтов, переданных и принятых сервером по сети
TCP Segments per Second	Число переданных и принятых сегментов TCP. Сравните с базой
TCP Segments Retranslates per Second	Число ретранслированных сегментов TCP
UDP Diagrams per Second	Общее число переданных и принятых датаграмм. Чем больше это значение, тем выше скорость трафика в режиме без установления соединения

Подсистема Lotus Notes

В табл. 18.9 приведены конкретные счетчики монитора производительности, рекомендуемые для контроля работы Notes и Domino на сервере NT (рис. 18.4).

Таблица 18.9. Счетчики для мониторинга системы Domino

Счетчик	Описание
Mem.Allocated	Число байтов, выделенных для сервера Domino
NET.TCPIP.Bytes.Received	Число байтов, принятых через определенный сетевой порт. Для каждого сетевого порта представлен один экземпляр
NET.TCPIP.Bytes.Sent	Число байтов, переданных через определенный сетевой порт. Для каждого сетевого порта представлен один экземпляр
NET.TCPIP.Sessions Established.Incoming	Число входящих сеансов, созданных для конкретного порта. Для каждого сетевого порта представлен один экземпляр

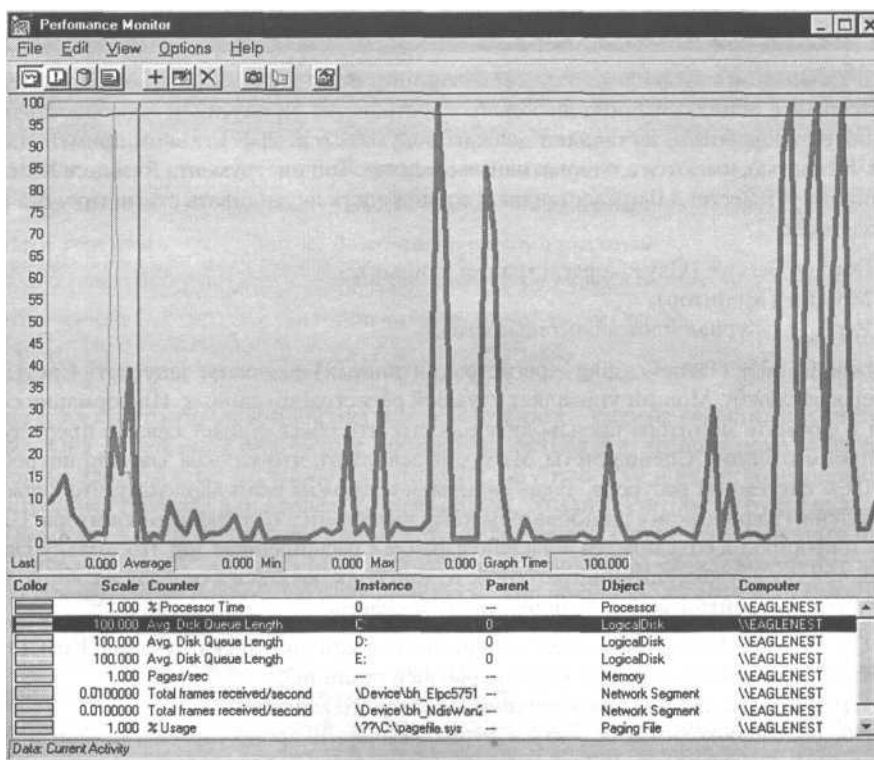


Рис. 18.4. Вид Chart (Диаграмма) монитора производительности NT позволяет контролировать различные системные счетчики

Таблица 18.9. Счетчики для мониторинга системы Domino (окончание)

Счетчик	Описание
NET.TCPIP.Sessions Established.Outgoing	Число исходящих сеансов, созданных для конкретного порта. Для каждого сетевого порта представлен один экземпляр
ServerAvailabilityIndex	Коэффициент, указывающий, насколько занят сервер в определенный момент. Чем больше, тем лучше
Server.Sessions.Dropped	Число прерванных сеансов, чаще всего из-за неактивности. Низкое значение Server_SessionTimeout вызывает рост данного показателя
Server.Transactions.PerMinute	Среднее число транзакций сервера Domino
Server.Transactions.PerMinute.Peak	Пиковое значение числа транзакций сервера Domino
Server.Users	Число пользователей, подключенных к серверу

Использование NT Resource Kit

Хотя Системный монитор предоставляет администратору важную информацию, недостатки, связанные с использованием дискового пространства, пропускной способностью сети и мощностью обработки, заставляют дважды подумать о неэффективном применении ресурсов. К счастью, имеются альтернативные средства. Три инструмента Resource Kit системы Windows NT Server 4.0 предоставляют возможность накапливать статистику без больших издержек:

- Datalog Service (Служба регистрации данных);
- Monitor (Монитор);
- PerfLog (Журнал производительности).

Служба Datalog (Data Logging - регистрация данных) позволяет запускать Системный монитор как службу. Monitor управляет службой регистрации данных. Информация сохраняется в формате монитора производительности, что обеспечивает связь с предыдущим механизмом отчетов. Специалисты Microsoft заявляют, что служба Datalog потребляет менее 0,6% системных ресурсов. Такая экономия возможна благодаря тому, что служба не обращается к графическому пользовательскому интерфейсу Системного монитора. Накопленная информация сохраняется локально в файле с расширением .log. Поскольку Datalog запускается как служба, администратору не нужно подключаться к серверу и собирать данные. Чтобы настроить Datalog на определенном сервере:

1. Скопируйте файлы datalog.exe и monitor.exe с компакт-диска Resource Kit CD в каталог \system32 на сервере (или на рабочей станции).
2. Откройте вид **Журнал регистрации** Системного монитора.
3. Добавьте необходимые объекты в журнал: выберите процессор, систему, физический диск, файл подкачки, логический диск, сетевой интерфейс и Lotus Notes.
4. Выполните **Options => Log** (Параметры => Журнал). Установите для **Update** (Обновление) флажок **Periodic** (Периодическое) и значение от 15 до 30 минут. Помните, что значения указываются в секундах.
5. Сохраните на компьютере файл рабочей области с понятным именем, например baseline.pmw.
6. Скопируйте файл рабочей области (baseline.pmw) в каталог \system32 на сервере.

Администратор управляет службой Datalog с помощью утилиты Monitor (Монитор), которая также поставляется с NT Resource Kit. Команды этого монитора используются для описания функций службы Datalog. #

Результаты просматриваются в Системном мониторе. Для автоматизации накопления статистики службой Datalog можно создать пакетный файл, содержащий необходимые команды, и запустить его либо описанной ранее командой AT, либо утилитой WinAT Scheduling. Допустимые команды монитора приведены в табл. 18.10.

Таблица 18.10. Команды утилиты Monitor, вводимые в командной строке для управления службой Datalog

Команда	Описание
monitor setup	описание Иницирует службу Datalog на указанном сервере
monitor filename.pmw	Задаёт файл рабочей области, который используется для накопления статистики

Таблица 18.10. Команды утилиты *Monitor*, вводимые в командной строке для управления службой *Datalog* (окончание)

Команда	Описание
monitor start	Запускает Datalog
monitor stop	Останавливает Datalog
monitor pause	Приостанавливает Datalog (пауза)
monitor continue	Возобновляет работу после паузы
monitor automatic	Запускает Datalog при загрузке системы
monitor manual	Устанавливает ручной запуск Datalog
monitor disable	Отключает службу Datalog

Еще одна программа, применяемая для мониторинга - служба регистрации системных данных. Она запускается при вызове программы *PerfLog.exe*, которая похожа на службу *Datalog*, но здесь данные сохраняются в формате CSV или TSV и их легко импортировать в электронные таблицы для последующего анализа. Утилита *PerfLog* не будет включаться в NT Resource Kit после третьего дополнения (Supplement Three). Очевидно, что при мониторинге некоторых объектов Microsoft Exchange с помощью служб возникнут некоторые проблемы. Более подробную информацию можно получить на сайте технической поддержки Microsoft (<http://www.microsoft.com/technet/support/default.htm>).

Использование WinAT для автоматизации задач NT

Планировщик задач, созданный на базе графического интерфейса пользователя, — *WinAT*, имеющийся в NT Resource Kit, — предоставляет возможность простого планирования программ, таких как *PerfLog* и Системный монитор. С помощью *WinAT* планируется запуск программ на локальных и сетевых компьютерах. Дополнительная информация имеется на компакт-диске NT Resource CD и на сайте технической поддержки Microsoft.

Средства мониторинга Domino

Domino обладает собственным набором средств мониторинга. В версии R5 и R6 включены дополнительные инструменты, в том числе зонды и графический интерфейс, называемый Domino Server Monitor (Монитор сервера Domino). Мастер Statistic and Event monitor облегчает настройку системы мониторинга по сравнению с предыдущими версиями сервера Domino.

Все показатели Lotus Notes в Системном мониторе заложены и в среде Domino. Для их вызова необходимо ввести команды на консоли сервера, в базе данных Statistic Reports и в клиенте Domino Administration. Дополнительная информация, такая как Domino server uptime (Доступное время сервера Domino), доступна только в сервере Domino. Хотя значения, предоставляемые операционной системой, имеют огромное значение для администратора, они не могут полностью заменить информацию, которой снабжает администратора сама система Domino. Основное преимущество получения статистики от Domino заключается в том, что сервер Domino постоянно обновляет свою информацию. В отличие от Системного монитора операционной системы, который необходимо запускать отдельно, сервер Domino обновляет статистику по умолчанию во время работы сервера.

Основной мониторинг сервера выполняется с помощью команд, вводимых либо с консоли сервера, либо посредством удаленного сеанса из клиента Notes. Команда `show statistics` выдает текущую статистику о системе, в том числе о счетчиках, установленных в Системном мониторе, и о нескольких дополнительных счетчиках.

Журнал сервера постоянно предоставляет администратору полный список событий Domino. Просмотр журналов сервера достаточно трудоемкое занятие, если только не прибегать к инструменту Log Analysis (Анализ журнала). Для быстрого поиска необходимой текущей и обобщенной информации гораздо удобнее инструмент Statistics and Events Reports (Статистические отчеты и отчеты о событиях).

Консоль сервера Domino

Не так просто выделить значимый текст на экране консоли сервера Domino. Во-первых, не всегда нужная информация находится на экране в момент поиска. Во-вторых, когда сервер занят обработкой запросов, информация может меняться очень быстро.

Команда `show statistic` позволяет просмотреть статистику на консоли сервера. Она отображает больше информации, чем Системный монитор, но в текстовом формате.

Если вас интересует конкретная статистическая информация, допускается в команде `show statistic` указать имя в качестве параметра. Например, чтобы просмотреть статистику о кэш-памяти баз данных, введите следующую команду:

```
sh statDatabase.DbCache.*
```

Некоторую информацию обеспечивают две другие команды. Для быстрой проверки сведений о пользователях, задачах и серверах можно воспользоваться командами `show tasks` и `show server`.

Команда `show server` в общем случае дает больше информации, не относящейся к пользователям. В табл. 18.11 обобщаются результаты, выдаваемые командой `show server`. Удобнее просматривать статистику в клиенте Domino Administration. Команды консоли сервера помогают, когда программа Domino Administration недоступна.

Таблица 18.11. Результаты работы команды `show server`

Результат	Описание
Version information (Информация о версии)	Версия программного обеспечения Domino, платформа, лицензия, текущее время и дата
Server name (Имя сервера)	Имя сервера, заданное при установке ф
Server directory (Каталог сервера)	Путь к каталогу данных Domino
Elapsed time (Истекшее время)	Количество дней, часов, минут и секунд, прошедших с последнего запуска сервера
Transactions (Транзакции)	Общее число транзакций, выполненных с момента последнего запуска сервера. Подсчитывается число открытий баз данных, их закрытий, считываний и записей в них, а также доставок почты в базы данных
Availability Index (Коэффициент доступности)	Вычисление рабочей нагрузки сервера в кластере
Message tracking (Отслеживание сообщений)	Показывает, включено или выключено это средство

Таблица 18.11. Результаты работы команды show server (окончание)

Результат	Описание
Shared Mail (Общая почта)	Показывает, включено или выключено это средство
Number of mailboxes (Число почтовых ящиков)	Число почтовых ящиков на сервере
Pending mail (Отложенная почта)	Число необработанных почтовых документов
Dead mail (Заблокированная почта)	Число почтовых документов, которые невозможно доставить и которые вернулись на сервер
Waiting Tasks (Ожидающие задачи)	Число необработанных задач сервера
Transactional Logging (Регистрация транзакций)	Показывает, включено или выключено это средство

Включение и настройка отчетности

В то время как в журнале статистика накапливается постоянно, отчетность Statistic and Events в R5/6 включается отдельно, посредством запуска одной или более серверных задач. Каждая задача отвечает за отчетность по разным типам информации. Чтобы активизировать задачу при каждом перезапуске сервера, можно загрузить ее с консоли или добавить в notes.ini. Эти задачи:

- Event Monitor (Event - Монитор событий);
- Statistics Collector (Collect - Сбор статистики);
- ISpy (Runjava ISpy);
- Mail Tracking Collector (MTC - Сбор почтовой статистики).

Большая часть собираемой информации сохраняется в базе данных Statistics Reporting (statrep5.nsf в R5 или statrep.nsf в R6), в которую опытные администраторы привыкли заглядывать. В R5/6 это достаточно удобный способ просмотра сведений с рабочей станции пользователя, когда недоступен клиент Domino Administration. Дополнительная база данных Report (report.nsf) служит для отслеживания почтовой статистики.

Как и в предыдущих версиях, настройки пороговых значений статистики и событий устанавливаются в базе данных Statistics and Events (event4.nsf) - Хотя документы можно настроить и вручную, компания Lotus создала новый Мастер конфигурирования, что упрощает мониторинг по сравнению с Системным монитором. Φ

Серверные задачи

Компания Lotus внесла значительные изменения в серверные задачи, предназначенные для мониторинга работы Notes и Domino. И новички, и опытные администраторы должны прочесть следующие разделы, чтобы уметь правильно настраивать мониторинг в системе R5/6.

Монитор событий

Задача Event Monitor (Монитор событий) контролирует возникновение событий на сервере Domino и должна работать на всех серверах, которые нуждаются в контроле. Поместите значение Event в строку ServerTask файла notes.ini. Задача автоматически создает базу

данных Statistics and Events. Для ручного запуска задачи введите команду Load Event на консоли сервера.

Системный монитор и средства мониторинга Domino дополняют друг друга

Для мониторинга системы в целом используйте Системный монитор, но когда необходимо получить более подробную информацию о работе Domino, используйте средства диагностики Notes.

Будьте внимательны

Во время установки Domino 5.0 задача Collect не добавляется в строку ServerTasks= файла notes.ini, даже если при этом были выбраны Events и Statistics. Следовательно, статистика не будет накапливаться в базе данных Statistic Reporting (statrep5.nsf). Задачу Event необходимо поместить в файл notes.ini, чтобы правильно генерировались отчеты. Lotus исправил эту ошибку в версии R6, но обязательно проверьте параметр ServerTasks после установки.

Если вы обновили версию Domino до R5/6, имейте в виду, что задача Report более не существует. Статистику обо всех серверах теперь собирает задача Collect. Удалите ссылку на Report из файла notes.ini, чтобы избежать ошибки при загрузке Domino R5.

Сбор статистики

Задача Collect несет ответственность за сбор статистической информации о контролируемом сервере. Ее достаточно запустить только на одном сервере домена, который будет контролировать все указанные серверы домена в соответствии с параметрами настройки документа Server Statistic Collection и базы данных Statistics & Events.

Как уже отмечалось при рассмотрении Системного монитора, для централизованного сбора информации требуются дополнительные ресурсы сети. Дополнительная нагрузка зависит от интервала отчетности задачи Collect, определенного в документе Server Statistic Collection. В географически разрозненных компаниях (например, международных корпорациях) администраторы стремятся уменьшить сетевой трафик, генерируемый во время отправки данных в центральную базу. Один из способов выполнения этой задачи состоит в создании реплики базы данных Statistic Reporting на втором сервере и отмене репликации между ними. Отчеты будут передаваться в ближайшую базу данных. Зато при желании можно объединить две реплики для обобщенного анализа.

ISpy

Эта задача применяется для отправки серверных и почтовых зондов. Результаты заносятся в базу данных Statistic Reporting как события. При ручном запуске ISpy введите на консоли сервера команду RunJava ISpy. Обратите внимание, что данная команда чувствительна к регистру. При первом запуске задачи в каталоге Domino создается запись в почтовой базе данных с помощью процесса Administration Process. Зонды – это новое средство, появившееся в R5. Почтовые зонды служат для проверки маршрутизации на определенный почтовый сервер. Зонды TCP-сервера позволяют контролировать доступность служб TCP через заданный порт.

Сбор почтовой статистики

Задача Mail Tracking Collector (МТС - сбор почтовой статистики) считывает файлы журналов регистрации и формирует обобщенные отчеты о трафике сообщений на сервере. Эти отчеты сохраняются в базе данных Reports (reports.nsf)- Для включения МТС необходимо ввести команду load mtc на консоли сервера. После загрузки эта задача создает базу данных Message Store. По умолчанию путь к ней указан как <NotesDataDirectory>\mtdata. Если путь не существует, то произойдет ошибка инициализации отслеживания сообщений.

База данных Statistic Reporting

Эта база данных (statrep5.nsf или statrep.nsf) собирает и упорядочивает статистику, а также сведения о предупреждениях и событиях, генерируемые каждой из трех серверных задач.

Статистические отчеты, которые отображают только наиболее часто просматриваемую информацию, сохраняются в этой базе данных. Отчеты генерируются по категориям, указанным в табл. 18.12.

Таблица 18.12. Категории статистической информации

Компонент отчета	Охватываемая статистика
Calendaring & Scheduling (Календарь и расписание)	Встречи и выделение помещений
Clusters (Кластеры)	Кластерный сервер и репликация
Communications (Связь)	Связь XPC и коммутируемые соединения
Mail & Database (Почта и база данных)	Шлюзы, репликация, почта
Network (Сеть)	Сеть
Single copy object store (Хранилище единичных копий объектов)	Общая почта
System (Система)	Агенты, диск, память, нагрузка
Web Server & Retriever (Web-сервер и система поиска)	Web-сервер и навигатор

В базе данных Statistics Reporting имеется четыре дополнительных вида, оставшиеся от предыдущих версий:

- **Alarms** (Предупреждения) выдает информацию о предупреждениях, формируемых при достижении определенных порогов. Предупреждения настраиваются в базе данных Statistics & Events (event4.nsf);
- **Events** (События) показывает результаты работы зондов и другие контролируемые события;
- **Spreadsheet Export** (Экспорт в электронную таблицу) отображает обобщенный системный отчет;
- **Graphs** (Диаграмма) представляет собой каскадный вид. В трех ниже лежащих видах содержится та же информация, что и на виде **Spreadsheet Export**. Каждый столбец вида выводится в форме диаграммы. Это виды **System Load** (Системная нагрузка), **Resources** (Ресурсы) и **Statistics** (Статистика). Формат предоставляемой информации не сравнится с данными от клиента Domino Administration, и администраторы редко обращаются к ней.

Статистика баз данных отображается неверно

В базе данных *Statistics Reporting* в версии R5 имеется одна проблема. В соответствии с Lotus Technote # 172443, раздел *Database Statistics* в *Statistics Reports* не заполняется из-за несоответствия между именем поля формы и именем поля, которое передается в базу данных. Например, поле **Buffer pool maximum** (Максимальный буферный пул) в форме **Statistics Report** определено как Database. BufferPool.Maximum. Для соответствия передаваемым данным поле должно быть определено как Database. Database. BufferPool.Maximum. Чтобы реализовать этот прием, вам сначала придется найти способ сохранить имя поля, в котором более 32 символов.

Компания Lotus решила проблему в версии 5.01. Число исправлений в квартальных версиях Lotus говорит о том, что гораздо проще исправить ошибку посредством обновления, вместо того чтобы пытаться написать код для корректировки.

База данных MessageStore

Названная база данных создается при первом запуске задачи МТС и не предназначена для прямого доступа пользователей. Содержит обобщенную информацию, такую как имя отправителя, имя получателя, время доставки и состояние. С помощью этих сведений база данных Reports генерирует отчеты о схемах маршрутизации, объемах сообщений и пользователях, которые чаще других обращаются к почте. Она также служит инструментом отслеживания сообщений, переданных и принятых сервером.

База данных Reports

Предназначена для создания отчетов о функционировании почты, схемах маршрутизации, объемах сообщений и самых активных пользователях почты на сервере. Отчеты могут генерироваться немедленно либо планироваться как ежедневные, еженедельные или ежемесячные. Существуют следующие отчеты:

- **Top 25 Users By Count or Size** (25 самых активных пользователей по числу или размеру сообщений);
- **Top 25 Senders By Count or Size** (25 самых активных отправителей по числу или размеру сообщений);
- **Top 25 Receivers By Count or Size** (25 самых активных получателей по числу или размеру сообщений);
- **Most Popular Next or Previous Hops** (Наиболее известные следующие или предыдущие транзитные участки);
- **Top 25 Largest Messages** (25 самых больших сообщений);
- **Message Volume Summary** (Сводка размеров сообщений);
- **Message Status Summary** (Сводка состояний сообщений).

База данных Statistics&Events

Сервер Domino постоянно генерирует статистическую информацию. Статистика отражает состояние операционной системы и определенных функций Domino и Notes. Администраторы обычно слишком заняты, чтобы просматривать статистику, предоставляемую сервером. Задача Events выполняет фильтрацию, выдавая предупреждения, когда достигаются

установленные пороги для некоторых счетчиков. В базе данных Statistics & Events задаются значения порогов и соответствующие предупреждения. Контролируемые события в любых реализациях отражают комбинацию общих системных операций и конкретных проблемных областей или устройств. Если формировать предупреждения для каждого события, создастся так много информации, что она очень скоро станет бесполезной и вызовет нехватку ресурсов. Потратьте время и просмотрите статистику, которая включена в базу данных Statistics & Events по умолчанию, чтобы выделить для себя ту информацию, которая имеет значение именно для вашей конфигурации. Пороговые значения и другие данные можно изменять в зависимости от конфигурации. Обычно вполне удовлетворяют значения, установленные по умолчанию, но такое упражнение знакомит администраторов с множеством возможных вариантов. Зачастую администраторы не применяют эту часть Notes, а потом покупают дополнительные продукты, которые выполняют те же самые функции.

События

События имеют две основные характеристики: тип и серьезность. Отчетность о событиях в Notes разбивает события на подсистемы, так же как Системный монитор NT отделяет подсистемы процессора, памяти, жесткого диска и сети. Типы событий различаются по области функционирования, к которой они принадлежат. Для Domino характерны следующие типы событий:

- **Add-in** (Надстроек);
- **AdminP** (Административного процесса);
- **Agent** (Агентов);
- **Client** (Клиентов);
- **Comm/Net** (Связи/сети);
- **Compiler** (Компилятора);
- **Database** (Базы данных);
- **Directory (LDAP)** (Каталога LDAP);
- **FTP** (Протокола передачи файлов);
- **Mail** (Почты);
- **Misc** (Различные);
- **Network** (Сетевые);
- **News (NNTP)** (Протокола передачи новостей);
- **Replica** (Репликации);
- **Resource** (Ресурсов);
- **Router** (Маршрутизатора);
- **Security** (Системы защиты);
- **Server** (Сервера);
- **Statistic** (Статистики);
- **Unknown** (Неизвестные);
- **Update** (Обновлений);
- **Web (HTTP/HTTPS)** (Событий Web).

Каждому событию присваивается определенный уровень серьезности. Серьезность определяет, насколько важно данное событие для функций, выполняемых системой Domino. Поскольку Domino - система, расположенная на сервере сети, то событие с высоким

уровнем серьезности может иметь меньшее значение на уровне системы. Например, если у контролируемого диска менее 10 Мб свободного места, этому событию в Notes присваивается значение **Warning (High)** (Предупреждение с высоким приоритетом). Уровни серьезности событий можно изменить в соответствии с конфигурацией системы.

Имеются следующие варианты:

- **Normal** (Обычный) - просто информационное сообщение;
- **Warning (Low)** (Предупреждение с низким приоритетом) - может произойти некоторое ухудшение производительности;
- **Warning (High)** (Предупреждение с высоким приоритетом) - возможно, требуется вмешательство;
- **Failure** (Авария) - серьезная авария в определенном компоненте системы;
- **Fatal** (Необратимый сбой) - есть опасность выхода системы из строя.

При возникновении определенного события среда Notes способна действовать от имени операционной системы, выполняя разные действия - от уведомления до запуска программ для устранения проблем. В целом Notes в состоянии осуществлять:

- широковещательную рассылку сообщений определенному пользователю или всем пользователям;
- отправку почтового уведомления в административную, пользовательскую, групповую или другую базу данных;
- регистрацию событий в локальной базе данных или в базе данных на удаленном сервере, обычно в базе Statistic Reporting;
- формирование отчета о событии в Event Viewer (Просмотр событий) системы Windows NT или в системном журнале UNIX;
- отправку пейджингового сообщения с измененным описанием события;
- генерацию прерывания SNMP;
- запуск программы при попытке решения проблемы на локальном либо удаленном сервере;
- передачу события на другой сервер домена, имеющий общий протокол с данным сервером.

Остальные варианты действий доступны, если в системе установлены программы управления сервером, например Notes View или HPOpenview.

Мониторы

Мониторы отличаются от событий тем, что с ними не связано никаких действий. Когда достигается какой-либо установленный порог, монитор вызывает соответствующее событие, которое в свою очередь выполняет связанное с ним действие.

Существует два типа мониторов: монитор баз данных и монитор статистики сервера. Мониторы баз данных служат для наблюдения за:

- недействующими базами данных;
- неиспользуемым файловым пространством;
- изменениями списков ACL;
- сбоями репликации.'

С помощью мониторов статистики обычно проводится наблюдение определенной статистики системы Domino. Мониторы статистики настраиваются в документе Statistic

Monitor (Монитор статистики). Когда контролируемый параметр достигает установленного порога, в базе данных Statistics (statrep.nsf) создается документ Alarm (Предупреждение). Просмотреть статистику можно в видах **Statistics Names** (Статистика по именам) или **Statistics by Description** (Статистика по описаниям) в базе данных Statistics & Events.

Чтобы настроить монитор статистики, сделайте следующее:

- О первое поле в документе Statistic Monitor позволяет администратору указывать, где проводится мониторинг – на одном сервере или на всех серверах домена;
- О после этого щелкните по кнопке **Change** (Изменить) и задайте контролируемую статистику. Откроется список доступных статистических параметров. При выборе определенных параметров могут появиться дополнительные аргументы, например единицы измерения каких-либо значений;
- О затем администратор задает необходимые пороговые значения, при достижении которых генерируется документ Alarm;
- О можно указать серьезность события. Варианты серьезности рассмотрены ранее.

Чтобы при создании документа Alarm получать уведомление, администратор может настроить документ Event Notification (Уведомление о событии), как описано ниже в этой главе.

Зонды

В то время как мониторы пассивны, зонды активно проверяют доступность указанного ресурса в назначенный промежуток времени. Если ресурс долго не отвечает на запрос, создается событие и выполняется связанное с ним действие. В Domino R5/6 существует три типа зондов (табл. 18.13).

Таблица 18.13. Зонды сервера Domino R5/6

Тип зонда	Функция
Domino server probe (Зонд сервера Domino)	Тестирует доступность сервера. Дополнительно проверяется возможность получения доступа к серверу и открытия определенной базы данных. Должен быть задан порт, используемый для соединения с сервером. Можно указать любую сеть, настроенную для данного сервера
TCP server probe (Зонд TCP-сервера)	Проверяет доступность сервера через конкретный порт. Зонд измеряет время ответа в миллисекундах. Можно проверить следующее службы: DNS, FTP, HTTP, IMAP, LDAP, NNTP, POP3, SMTP
Mail probe (Почтовый зонд)	Пользователю на тестируемый сервер отправляется проверочное сообщение. Это сообщение генерирует подтверждение от получателя. Выполнение указанных действий за установленное время свидетельствует об удачном тестировании. Можно настраивать интервалы и срок действия зонда

Открыв базу данных Statistics & Events (рис. 18.5), вы обнаружите в ней несколько кнопок, позволяющих настраивать уведомление о событиях, мониторы, зонды и средства устранения неполадок. Благодаря этому удастся упростить процесс настройки соответствующих процедур для новых администраторов. Можно создавать все указанные документы вручную.

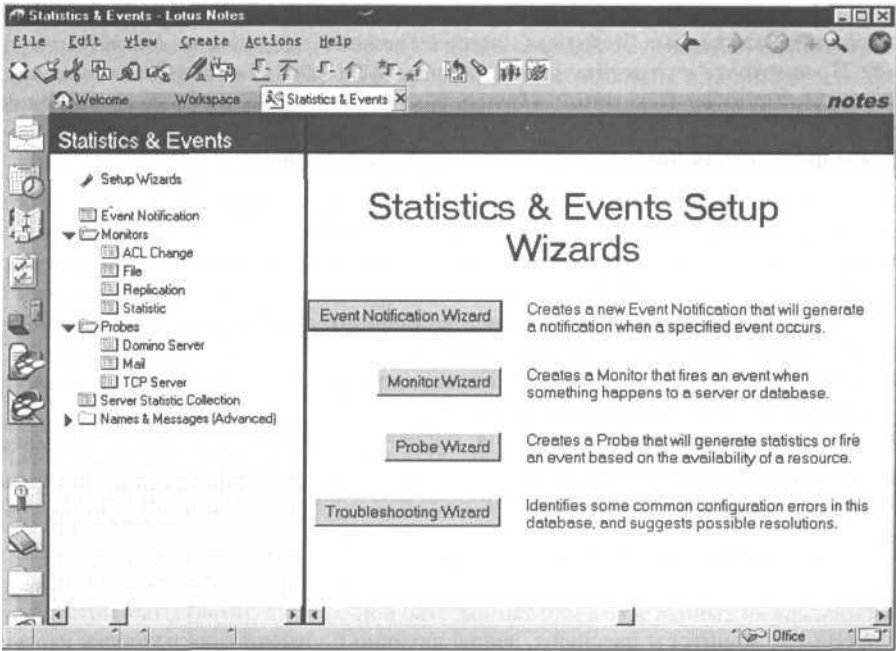


Рис. 18.5. Окно базы данных Statistics & Events

При использовании обоих методов присутствуют одинаковые варианты. Есть два исключения: нельзя документ Troubleshooting (Устранение неполадок) настроить вручную, а документ Statistic Collection создать с помощью Мастера.

Один документ Server Statistic Collection можно настроить на сбор статистики со всех серверов домена или с некоторого набора серверов. Если не настроены дополнительные документы Collection, то контролироваться будет только сервер, на котором работает задача Collect.

Настройка документа Server Statistic Collection достаточно проста. Параметры, необходимые для настройки, описаны в табл. 18.14.

Таблица 18.14. Поля документа Server Statistic Collection

Параметр	Описание
CollectingServer (Собирающий сервер)	Введите имя сервера, на котором запущена задача Collect
All servers in this domain (Все серверы домена)	Собирает статистику со всех серверов домена
All servers that are not explicitly listed to be collected (Все серверы, которые явно не* указаны для сбора статистики)	Собирает статистику с тех серверов домена, на которых в настоящий момент статистика непредусмотрена
From the following servers (Со следующих серверов)	Выберите конкретные серверы, с которых будет собираться информация

Таблица 18.14. Поля документа *Server Statistic Collection* (окончание)

Параметр	Описание
Database to receive reports (База данных, получающая отчеты)	Выберите этот параметр, чтобы включить запись статистики в определенную базу данных Обычно база данных <i>Statistic Reporting</i> (<i>statrep5.nsf</i> или <i>statrep.nsf</i>)
Collection report interval (Интервал отчетности)	Количество минут между генерацией статистических отчетов. Минимальное значение — 15 минут
Collection alarm interval (Интервал сигнала об аварии)	Количество минут между генерацией аварийных сигналов. Минимальное значение - 15 минут

Уведомление о событии

Параметры документа *Event Notification* представлены в табл. 18.15.

Таблица 18.15. Поля документа *Event Notification*

Параметр	Описание
Notification trigger (Переключатель уведомления)	Можно указать A built in or add-in task event (Встроенное или добавленное уведомление о событии). Выбор определяет, что будет отображаться на вкладках Event и Actions
Servers to monitor (Контролируемые серверы)	Отметьте Notify of the event on any server in the domain (Уведомлять о событиях любого сервера домена) или Notify of the event only on the following servers (Уведомлять о событиях определенных серверов), чтобы указать серверы, на которых запущена задача <i>Event</i> и которые вы хотите проконтролировать
Built in/Add-in Task event (Встроенные/надстроечные события задачи)	Эти параметры появляются, если выбран переключатель уведомления A built in or add-in task event
Щелкните по кнопке Event (Событие)	Открывает список доступных сообщений об ошибке и их типах
Выберите либо Events can have any message (Событие может иметь любое сообщение), либо Events must have this text in the event message (Событие должно иметь указанный текст в сообщении)	Генерируется событие, реагирующее на любую ошибку такого типа, или указывается база данных, имя сервера, пользователя и т.д., которые должны быть вставлены в сообщение
Actions taken in response to an event are selected (Действие в ответ на выбранное событие)	Дополнительно включите или отключите контроль этого действия. Контроль можно активизировать на определенный промежуток времени. Возможные действия рассмотрены ранее
Criteria to match (Критерий соответствия)	Эти параметры появляются, если выбран переключатель уведомления Any event that matches a criteria (Любое событие, соответствующее критерию)

Таблица 18.15. Поля документа *Event Notification* (окончание)

Параметр	Описание
Выберите либо Events can be any type (События любого типа), либо Events must be this type (События данного типа), чтобы установить тип событий	Для получения информации о типах событий обратитесь к документации Domino. Иные типы событий расположены в дополнительных надстройках (прикладных программах)
Выберите либо Events can be any severity (События могут быть любой серьезности) или Events must be one of these severities (События должны иметь один из этих уровней серьезности), чтобы установить уровень серьезности	Серьезность может быть Fatal, Failure, Warning (high и low) и Normal

Мастер устранения неполадок

Мастер устранения неполадок (Troubleshooting Wizard) анализирует документы в базе данных Statistics & Events и пытается определить общие ошибки конфигурации, а затем генерирует отчет, содержащий все найденные проблемы и возможные пути их решения. Документы можно искать и выбирать. С помощью Мастера система Notes проверяет пути и имена файлов, указанные в документе конфигурации Statistics & Events.

Например, если вы создали монитор репликации, который проверяет базу данных sales.nsf на сервере x по крайней мере каждые 24 часа, то Мастер устранения неполадок пытается установить, допустимы ли значения указаны в документе Monitor. Если нет, Мастер сообщит, что не может найти базу данных на сервере x, и предложит проверить параметры соединения и настройки сети.

Мониторинг Domino из Domino Administration

Итак, мы рассмотрели большинство традиционных средств мониторинга сервера Domino. Хотя новые средства гораздо более привлекательны, необходимо уделить должное внимание основам. Информация, получаемая с помощью нового клиента Domino Administration, требует правильной настройки баз данных, мониторов и зондов, описанных в предыдущих разделах.

Клиент Domino Administration оснащает средства поддержки удобными графическими видами важных отчетов и статистической информации. Прежде чем обсуждать данные, предоставляемые клиентам администрирования, посмотрим несколько вариантов конфигурации, с которыми необходимо быть знакомыми. В следующем разделе приведен обзор параметров, имеющихся в диалоговом окне **Administration Preferences** (Предпочтения администрирования).

Предпочтения администрирования

Предпочтения для мониторинга сервера можно установить в диалоговом окне **Administration Preferences**, открываемом в меню **File** (Файл). Щелкните по кнопке **Monitoring** (Мониторинг) в окне **Administration Preferences**, чтобы выполнить следующие действия:

- О выберите контролируемые домены Domino. Серверы добавленного домена не появляются в мониторе сервера. После добавления новых элементов в список контролируемых доменов надо задать **Administration => Refresh => Server List => All Domains** (Администрирование => Обновить => Список серверов => Все домены) в клиенте администрирования;
- О ограничьте объем виртуальной памяти, выделенной для мониторинга. Допустимы значения от 4 до 99 Мб;
- О автоматически контролируйте все новые серверы;
- О укажите, где накапливается статистика для каждого места пользователя. Допускается назначить локальный компьютер или удаленный сервер, на котором запущена задача Collect;
- О задайте интервал опроса контролируемых серверов;
- О укажите, следует ли тестировать серверы при запуске клиента Domino Administration.

Работа с окном Administration Preferences

Для открытия окна **Administration Preferences** существует клавиатурная комбинация. В клиенте Domino Administration щелкните правой кнопкой мыши по значку сервера, расположенному на панели значков, и выберите **Preferences** (Предпочтения).

Свойства сервера

Ранее в этой главе упоминалось, что мониторинг сервера подразумевает подробную фиксацию результатов. Сбор базовой информации так же важен, как при мониторинге операционной системы. В R5/6 можно получить сведения о конкретном сервере, открыв окно свойств сервера (как и для базы данных).

Свойства сервера можно просмотреть, щелкнув правой кнопкой мыши по значку нужного сервера в клиенте Domino Administration. Если отображаются **SmartIcon** (Интеллектуальные значки), можно выбрать сервер и щелкнуть по **SmartIcon Properties** (Свойства интеллектуального значка). Получаемая информация разделена на пять вкладок (табл. 18.16).

Таблица 18.16. Информация, указанная в окне **Server Properties**

Вкладка	Свойства
Basics (Основные параметры)	Отображает версию сервера Domino, платформу, лицензию, текущее время и дату. Информация аналогична отчету, выдаваемому командой <code>show tasks</code>
Disks (Диски)	Показывает информацию о жестких дисках, установленных на компьютере, о буквах, обозначающих диски, о проценте свободного пространства, об объеме свободного пространства (в мегабайтах) и размере дисков
Cluster (Кластер)	Выводит информацию о кластере, если сервер находится в кластере. Статистика содержит имя кластера, порог доступности, коэффициент доступности, сетевой порт кластера, тайм-аут зонда, значения счетчиков и членов кластера
Ports (Порты)	Предоставляет доступ к диалоговому окну настройки портов

Таблица 18.16. Информация, указанная в окне **Server Properties** (окончание)

Вкладка	Свойство
Advanced (Дополнительно)	Отображает статистику, включая общее и максимальное количество транзакций и число транзакций за истекшие час или минуту. В пользовательскую статистику входит текущее число пользователей, максимальное число пользователей и дата регистрации максимального количества пользователей, а в статистику о памяти - доступность, выделенная память и доступная память

Информация на вкладке Status

Вкладка **Status** (Состояние) предоставляет краткую справку о задачах, портах и пользователях, работающих в данный момент на сервере (рис. 18.6). Первый экран состоит из двух частей. Верхняя половина экрана отображает общее число задач, настроенных портов и текущей деятельности, а нижняя - информацию о текущей работе пользователей и сеансах. Выводимая информация аналогична результату работы команды `show tasks`.

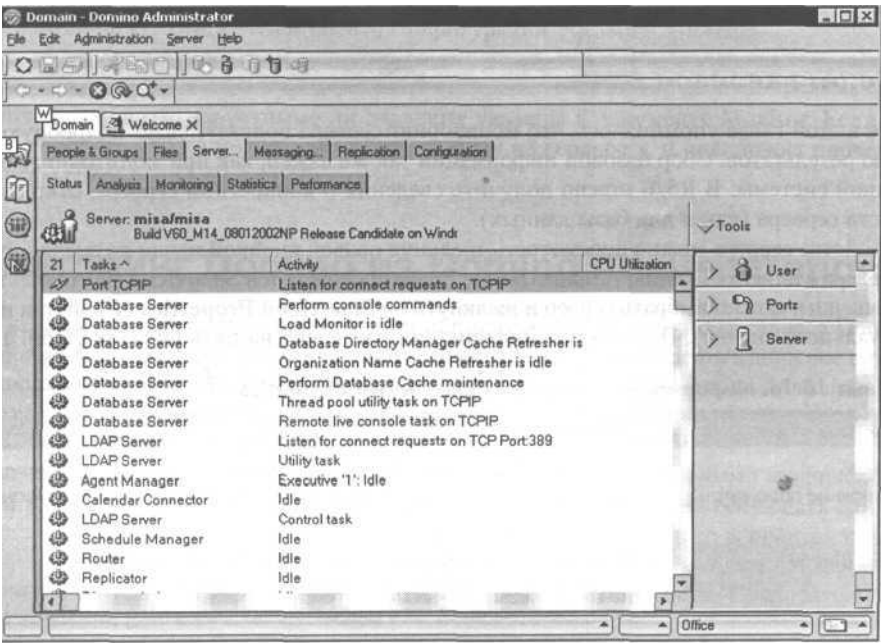


Рис. 18.6. Вкладка **Status** содержит информацию о системных задачах, портах и пользователях

Администраторы будут приятно удивлены, найдя на данной вкладке гораздо больше функциональных возможностей, чем представляется на первый взгляд. Это опять же задачи и информация, доступная из всех остальных частей системы Domino и Notes. Программа

Domino Administration объединяет многие административные функции, облегчая ежедневную работу администратора.

В меню имеются соответствующие команды, однако многие администраторы предпочитают клавиатурные комбинации.

Щелкните по задаче правой кнопкой мыши, чтобы получить возможность выполнить такие действия:

- воспользоваться командой **tell** для выбираемых параметров указанной задачи. Например, параметры команды **tell** для выделенной задачи **AdminP** позволяют администратору обработать все запросы или задать типы задач **AdminP**, указывая их в диалоговом окне. В этом окне также приводится описание каждого доступного параметра;
- остановить задачу;
- запустить новую задачу;
- щелчком правой кнопкой по настроенному порту закрыть его.

Просмотр откликов на команды удаленного сервера

В клиенте *Domino Administration* при использовании команды **tell**, которая выдает отклик на консоль сервера, не отображается сам отклик. Можно либо просмотреть его именно на консоли, либо перед использованием команды **tell** щелкнуть по кнопке **Console** (Консоль) и запустить сеанс консоли сервера, а затем переключиться на вид **Console**, чтобы увидеть отклик.

L

Если вы щелкнете правой кнопкой мыши по имени пользователя, вам будут предложены следующие варианты:

- передать сообщение в широковещательной рассылке всем пользователям или конкретному пользователю. К сожалению, чтобы передать сообщение конкретному сотруднику, его имя придется вводить вручную;
- прервать сеанс выбранного пользователя.

При щелчке по кнопке **Console** на вкладке **Status** открывается окно удаленного пульта сервера. Команды можно вводить, как и в предыдущих версиях *Notes*. Эта кнопка позволяет запускать сеанс **Live** (Живой) для консоли сервера и в реальном времени просматривать информацию на выбранном сервере. Для переключения на другой сервер укажите нужный сервер на панели значков. Кнопка **Tasks** (Задачи) возвращает обратно на вид **Tasks**.

Информация на вкладке Analysis

Вкладка **Analysis** (Анализ) дает возможность открывать серверные (рис. 18.7):

- журнал регистрации (**log.nsf**);
- каталог;
- ○ вид **Statistics Reports** в базе данных **Statistics & Events**;
- базу данных **Administration Requests** (Административные запросы).

Каждая база данных на вкладке **Analysis** аналогична по типу базам данных **Portfolio** в предыдущих версиях *Domino*. На этой вкладке размещены также инструменты **Log Analysis**

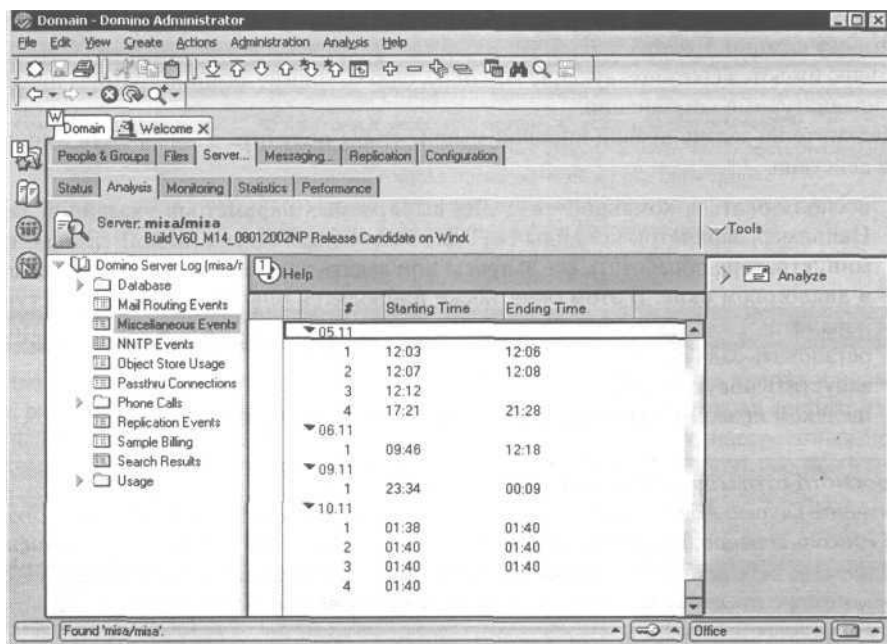


Рис. 18.7. Вкладка **Analysis** предоставляет удобный способ доступа к базам данных Log, Statistics Reports, Administration Requests и Catalog

(Анализ журнала) и Decommission Server (Списать сервер). Для мониторинга сервера применяется только Log Analysis.

Анализ журнала

Инструмент Log Analysis (Анализ журнала) находится на вкладке **Server => Analysis** (Сервер => Анализ) в клиенте Domino Administration. Он обеспечивает механизм поиска определенных символьных строк. Возможно, удобнее указать, чтобы система Notes создавала базу данных Results на рабочей станции, а не на сервере. Это уменьшит вероятность того, что другой администратор сохранит результаты поиска поверх ваших. Можно задать, чтобы результаты либо перезаписывались, либо добавлялись в базу данных. К сожалению, просмотр нескольких серверов в одной очереди не поддерживается. Чтобы имитировать это, определите одинаковые символьные строки для нужных серверов и назначьте добавление результатов поиска вместо перезаписи базы данных Results. Журнал можно также просмотреть с помощью Web Administrator.

Информация на вкладке Monitoring

Большая часть информации о мониторинге находится на вкладке Monitoring в клиенте Domino Administration.

Монитор сервера Domino

Быстрый взгляд на Domino Server Monitor (Монитор сервера Domino) позволяет сказать многое (рис. 18.8). В сведениях о задачах используется один из шести символов, отображающих состояние задачи на контролируемом сервере. Наблюдаемая статистика выводит числовое значение. В верхней части экрана на виде **By Timeline** (Шкала времени) находится регулируемая шкала времени, указывающая интервал обновления. Администратор на этой шкале устанавливает частоту обновления. Допустимые значения - от 1 до 60 минут. По мере сокращения частоты обновления увеличивается обобщение отчетных данных. Мониторинг запускается щелчком по кнопке **Start** или с помощью **Administration Preferences** (Предпочтения администрирования).

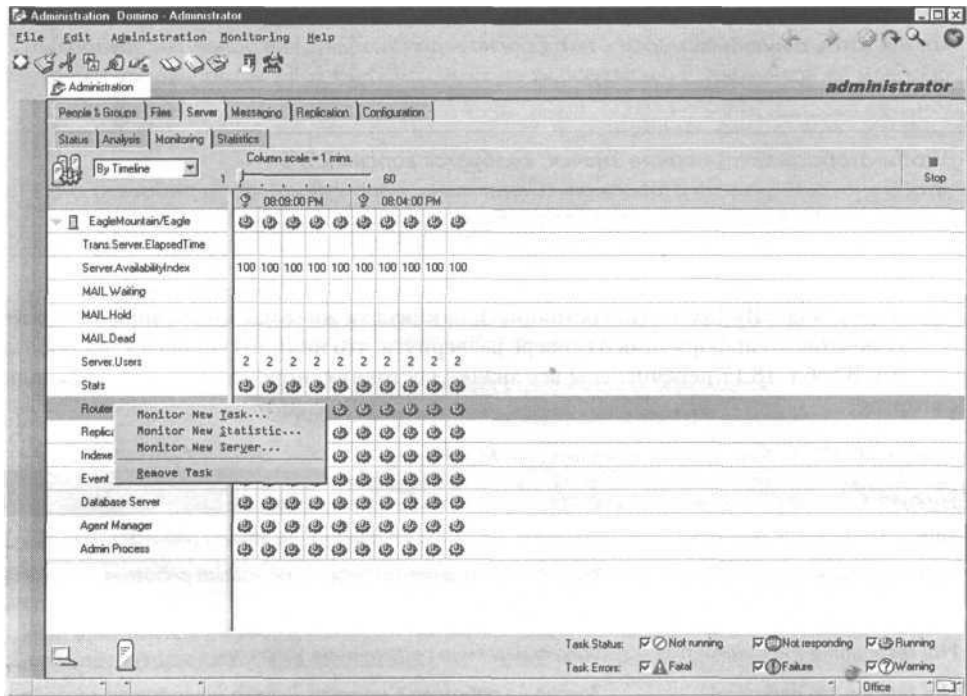


Рис. 18.8. Навкладке Monitoring графически отображается состояние операций сервера за определенные интервалы времени

Ограничения утилиты Log Analysis

Log Analysis способна просматривать только вид **Miscellaneous Events** журнала Domino - и никакие другие виды или журналы.

Щелкнув по имени сервера, администратор может увидеть состояние любой контролируемой задачи или статистики на сервере. Добавить дополнительные задачи, статистику или серверы или удалить задачу для отдельного сервера позволяет меню **Monitoring** или контекстное меню для имени сервера, а чтобы добавить или удалить дополнительные задачи или статистику для всех серверов, надо щелкнуть правой кнопкой мыши по вкладке **Server => Monitoring** и выбрать их в списке. Этот вид предоставляет хороший обзор, необходимый для большинства служб технической поддержки. Не хватает только возможности получать информацию о задачах с выводом ошибок.

Проблемы навигации

В R5 есть небольшая ошибка. При использовании клавиш **Page Up** и **Page Down** может нарушиться соответствие между именами серверов и статистикой. Задачи сервера прокручиваются, а имена серверов - нет. Если на экран выводится не более 10 серверов, то проблем не возникает. В последующих версиях компания Lotus устранила эту ошибку.

Чтобы отображались верные значки, требуется версия R5/6

Чтобы значки индикации отображались правильно, необходимо, чтобы работала система **Domino R5/6** и была включена задача **Event**.

На втором виде, **By State (По состоянию)**, принята та же самая символика отображения результатов, но информация о сервере развернута, что немного упрощает подробный просмотр. В табл. 18.17 перечислены все значки состояния, присутствующие на вкладке **Monitoring**.

Таблица 18.17. Значки состояния на вкладке **Monitoring**

Индикатор состояния задачи	Значение
Fatal (Необратимая ошибка)	Выдается необратимая ошибка, но задача работает
Failure (Авария)	Выдается сообщение об аварии, но задача работает
Warning (Предупреждение)	Выдается предупреждение, но задача работает
Not responding (Не отвечает)	Задача медленно реагирует на запросы
Not running (Не работает)	Задача не работала с момента запуска мониторинга сервера
Running (Работает)	Задача работает правильно

Информация на вкладке **Statistics**

Вкладка **Statistics (Статистика)** содержит те же результаты, которые получаются при вводе команды **show statistic** на консоли сервера (рис. 18.9). Преимущество просмотра статистики в клиенте **Dontino Administration** состоит в том, что вся статистическая информация форматируется и отображается графически. Статистика делится на категории в зависимости от типа. Щелчком правой кнопкой мыши можно раскрывать или закрывать категории либо копировать выделенную информацию.

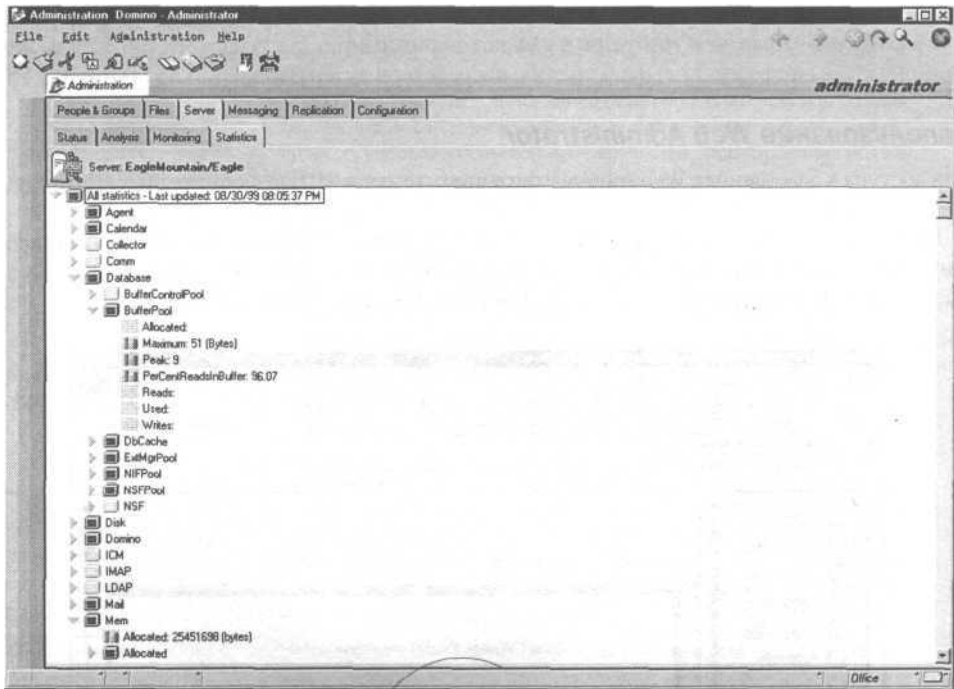


Рис. 18.9. На вкладке Statistics графически отображается текущая статистическая информация о сервере

Web Administrator

Программа Domino Web Administrator (Web-администратор Domino) выполняет многие функции Domino Administration вс* время сеанса HTTP с помощью браузера. При первом запуске задачи HTTP сервер Domino, создает базу данных Web Administrator (Webadmin.nsf).

Для доступа к этой базе данных пользователь должен быть указан в поле **Administrators** (Администраторы) каталога Domino

Установка Web Administrator

Установить Web Administrator достаточно просто. На нужном сервере должна работать задача HTTP, чтобы к нему можно было обратиться из браузера. После этого убедитесь, что имя пользователя указано в следующих полях серверного документа:

- **Administrators** (Администраторы);
- **Run Unrestricted LotusScript and Java agents on the server** (Запуск на сервере неограниченных сценариев LotusScript и агентов Java);
- **Administer the server from a browser** (Администрирование сервера из браузера).

База данных Web Administrator автоматически создается при первом запуске задачи HTTP на сервере. Защита базы данных, заданная по умолчанию, обычно допустима для

большинства сайтов. Проверьте назначенные роли, чтобы убедиться, что группам не предоставлено больше прав, чем требуется в вашей конфигурации. Доступ следует получать либо с помощью обычного имени и пароля, либо посредством аутентификации по протоколу SSL.

Использование Web Administrator

Для доступа к базе данных Web Administrator введите адрес URL в формате http://hostname/Webadmin.nsf.

Первое окно, появляющееся при открытии Web Administrator из браузера, - это информационная страничка, на которой показано имя сервера и имя хоста (рис. 18.10). Также выведены версия операционной системы, версия и номер сборки Domino.

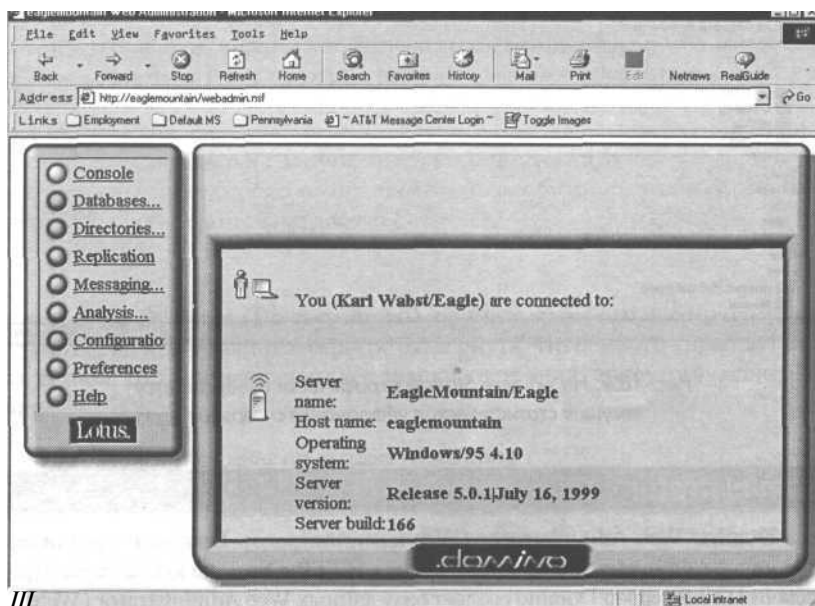


Рис. 18.10. Средство Web Administrator, имеющееся в Domino R5/6, позволяет администратору настраивать и контролировать серверы из браузера

С помощью меню Web Administrator можно выполнить действия, перечисленные в табл. 18.18.

Таблица 18.18. Действия, выполняемые с помощью Web Administrator

Console (Консоль)	Вводит команды для удаленной консоли сервера
Databases (Базы данных)	- o Create (Создать) - создание новой базы данных; - o Usage (Использование) — просмотр статистики использования базы данных из журнала сервера;

Таблица 18.18. Действия, выполняемые с помощью Web Administrator (продолжение)

Пункт меню Web Administrator	Функции
	○ Tools (Инструменты) - выполнение различных операций над базами данных, таких как запуск уплотнения, построение полнотекстового индекса, удаление базы данных, репликация, формирование новой реплики или просмотр и установка квот для размеров; ○ Catalog (Каталог) - просмотр каталога баз данных; ○ Access Control (Управление доступом) - настройка ACL базы данных. Необходимо иметь доступ на уровне Manager; ○ Sizes (Размеры) — просмотр баз данных в представлении By Size в журнале сервера. Помните, что размер базы данных не включает размер полнотекстового индекса. Индексы необходимо контролировать вручную
Directories (Каталоги)	○ People (Люди) - построение новой персональной записи и редактирование существующих; ○ Groups (Группы) - создание нового документа группы и редактирование существующих; ○ Deny Access Groups (Группы запрещенного доступа) - добавление и редактирование групп запрещенного доступа в каталоге Domino; ○ Alternative Language Information (Информация об альтернативных языках) - просмотр информации об альтернативных языках, если она настроено на сервере
Replication (Репликация)	Replication Events (События репликации) - просмотр вида Replication Events в журнале сервера
Messaging (Передача сообщений)	○ Routing Status (Состояние маршрутизации) - просмотр графического представления состояния маршрутизации сообщений. Две круговые шкалы отображают число необработанных, обслуживаемых и заблокированных сообщений. Большое число необработанных и заблокированных сообщений может занимать дополнительное пространство на диске и указывать на проблемы маршрутизации или сети; ○ Routing Events (События маршрутизации) - просмотр вида Mail Routing Events журнала сервера; ○ Mail Reports (Почтовые отчеты) - если включено отслеживание сообщений, можно запустить или просмотреть почтовые отчеты в базе данных Reports; ○ Mail Users (Почтовые пользователи) - просмотр вида Mail Users в каталоге Domino или добавление нового персонального документа; ○ Message Tracking (Отслеживание сообщений) - отслеживание получения и отправки сообщений за сегодняшний день, за вчерашний день, за последнюю неделю, за последние две недели или за все время, когда доступна эта информация; ○ Shared Mail (Общая почта) - просмотр информации об общей (совместно используемой) почте
Analysis (Анализ)	○ Logfile (Файл журнала) - просмотр журнала сервера; ○ Memory (Память) — просмотр круговой диаграммы об использовании памяти; ○ Statistics (Статистика) - просмотр статистических отчетов (Statistic Reports); ○ Diskspace (Дисковое пространство) - просмотр круговой диаграммы об использовании дискового пространства; ○ Administration Requests (Административные запросы) - просмотр административных запросов;

Таблица 18.18. Действия, выполняемые с помощью Web Administrator (окончание)

Пункт меню Web Administrator	Функции
Analysis	○ Statistics & Events (Статистика и события) - просмотр базы данных Statistics & Events; ○ Alerts (Аварийные сигналы) - просмотр системных сигналов в соответствии с серьезностью. Временной интервал можно выбирать. По умолчанию - 24 часа. Результаты объединяются по цвету. Зеленый означает Normal (Нормально), желтый - Warning (Предупреждение), а красный - Investigate (Необходимо вмешательство); ○ Web Statistics (Web-статистика) - просмотр Web-статистики в виде гистограммы, отображающей Web-запросы с момента последнего запуска сервера
Configuration (Настройка)	○ Servers (Серверы) - просмотр, редактирование и добавление записи сервера в каталог Domino; ○ Web Configuration (Конфигурация Web) - доступ к виду Web Configuration в каталоге Domino; ○ Clusters (Кластеры) - управление информацией о кластерах; ○ Connections (Соединения) — доступ к виду Connections в каталоге Domino; ○ Domains (Домены) - доступ к виду Domains в каталоге Domino; ○ Programs (Программы) - доступ к виду Programs в каталоге Domino; ○ Configurations (Конфигурация) - доступ к виду Server Configurations в каталоге Domino; ○ System Files (Системные файлы) - просмотр и редактирование текстовых файлов в каталоге данных Domino или в одном из подкаталогов
Preferences (Предпочтения)	Редактирование параметров, настройки интерфейса Web Administrator
Help (Справка)	Вывод базы данных Notes Administration Help

Web Administrator имеет доступ к информации, находящейся в файлах и базах данных сервера Domino. Если базы данных на сервере нет, эти сведения не выводятся. Для отображения информации применяются следующие базы:

- Administration Requests (Административные запросы);
- Database Catalog (Каталог баз данных);
- Domino Directory (Каталог Domino);
- Log (Журнал);
- Notes Administration Help (Справка по администрированию системы Notes);
- Statistics (Статистика);
- Statistics & Events (Статистика и события);
- Web Server Log (Журнал Web-сервера).

С помощью Web Administrator администратор может выполнять большинство функций, доступных в клиенте Domino Administration. Если вы включаете это средство, необходимо постоянно контролировать систему защиты. Преимущества очевидны, но из-за подверженности системы внешнему воздействию требуется осторожность. Проверьте свою работу. Это может стать тестом!

Утилита *Mean Time Between Failure of Iris*

Утилита MTBF (Mean Time Between Failure - средняя наработка на отказ) - инструмент, разработанный в исследовательской лаборатории Iris. И IBM, и Iris используют такую программу, но она не является официальным продуктом. Это еще один инструмент, который стал доступным в результате его широкого применения компанией-изготовителем. В главе 19 приводится обзор других средств.

MTBF ищет в журнале Notes сообщения о запуске и выключении. Когда обнаруживается сообщение о запуске сервера, перед которым нет сообщения о выключении, в базе данных создается документ Server Crash (Крах сервера). Затем MTBF еще раз просматривает журнал и выбирает последнее сообщение перед сбоем. Администратор может теперь внести свои примечания, чтобы отследить статистику сбоев.

MTBF не является средством, специально созданным для R5/6. Эта программа работает с R4 и более ранними англоязычными версиями Notes. С помощью MTBF можно собирать информацию о версии с одновременным выделением возможных аварийных ситуаций. Как отмечалось ранее, Notes генерирует большие объемы статистической информации и информации о событиях. Поместив ее в любое доступное место, легко создавать отчеты о сбоях посредством новых и тестовых программ. Для получения MTBF следует обратиться на сайт Sandbox.Notes.Net.

Контроль соединений между сервером *Domino* и клиентом *Notes*

Чтобы разобраться, почему в приложении увеличивается время ответа или ухудшается производительность, необходимо понять, как работают составляющие части соединения между клиентом и сервером. Вам известно, какие процессы идут после того, как пользователь вводит команду Notes или Domino? Рассмотрим, как раскрыть эти процессы и как с их помощью точно определить, какую часть системы необходимо проверить.

Узнав, что происходит между клиентом Notes и сервером Domino, вы лучше представите сами системы Notes и Domino. Существуют параметры настройки, которые позволяют выдавать отчеты о работе протокола NRPC. Обычно эти параметры находятся в файле notes.ini, чтобы предоставлять дополнительные результаты, которые помогают специалистам технической поддержки Lotus, когда вы к ним обращаетесь. Некоторые из названных параметров при неправильном использовании могут вызвать проблемы. Следующий параметр показывает переполнение жесткого диска, прежде чем это вызовет серьезную проблему.

Параметры *notes.ini*

Для вывода на экран:

```
Client_Clock=1
Debug_Console=1
```

Для вывода в файл:

```
Client_Clock=1 .
Debug_Outfile=<path\filename>
```

Любая функция пользователя, такая как открытие базы данных, состоит из нескольких запросов NRPC. Будет интересно и информативно объединить эти результаты с результатами, полученными при использовании дополнительных инструментов. Приведем пример того, как такие результаты можно объединить с эмпирическими данными и данными журнала, чтобы извлечь полезную информацию о системных функциях.

Предположим, что стоит задача собрать значимые данные о влиянии на пользователей внедрения клиента Notes R5/6 в сети. Проблема заключается в том, чтобы располагать сведениями, которые впоследствии удастся проверить самым объективным способом.

Во-первых, необходимо известными способами собрать информацию от клиентов. Можно, например, ходить по разным рабочим станциям с секундомером и измерять время функционирования различных систем. При этом придется выполнить множество вычислений, но вы не получите наглядной цепочки событий, приведших к измеренным результатам. Подобный метод позволяет оценить только время начала и окончания работы, то есть общее время работы.

Поместив параметры настройки в файл notes.ini, можно зафиксировать соединение между сервером и клиентом. Теперь результаты, полученные при повторении одинаковых видов деятельности на разных компьютерах, представляют собой эталонную базу для сети. Такой метод имеет дополнительное преимущество - он фиксирует интересные для разработчиков приложений данные о времени действия определенных процессов между рабочей станцией и сервером.

Начните с измерения времени открытия текущего клиента Notes. Затем установите клиент Notes R5/6 и повторите тест. Измените имена файлов, чтобы можно было сравнить результаты. Сопоставив данные, имеющиеся в эталонной базе, с новыми, вы сможете сформулировать гипотезу о влиянии внедрения нового клиента. После того как вы внесете соответствующие изменения в параметры настройки клиента, повторите тест и сравните его результаты с результатами предыдущего теста.

Хотя эта методика более эффективна, чем хождение по рабочим станциям с секундомером, она имеет определенные недостатки. Так, после неоднократного повторения одной и той же процедуры человек, выполняющий ее, становится более квалифицированным. Следовательно, время, необходимое для решения поставленной задачи, изменится, что внесет субъективный фактор.

С помощью дополнительных инструментов, таких как ProActive Load, можно последовательно тестировать работу Notes/Domino в зависимости от:

- О времени суток;
- О места в сети;
- О класса компьютера.

В файл notes.ini были добавлены следующие параметры:

```
Client_Clock=1
Debug_Outfile=c:\In50data\performance.txt
```

Строка Debug_Outfile служит для задания файла, в который записываются результаты (в данном примере performance.txt). В результате открытия клиента Notes R5/6 и его закрытия были получены следующие данные (функции баз данных не использовались):

```
(1-23 [1])OPEN_DB: (Connect toEagleMountain/SERVERS/Eagle: Oms) (Exchnames:
0ms) (Authenticate: 30 ms.)
(OPEN_SESSION: 10ms)
```

20ms. [126+290 = 416]
 (2-23 [2])GET_DBINFOFLAGS:10ms. [14+16=30]
 (3-23 [3])FINDDSIGN_NOTES:0ms. [38+16=54]
 (4-23 [4])OPEN_COLLECTION:10ms. [32+34=66]
 (5-23 [5])FOLDER_GETMODTIME_RQST:0ms. [78+60=138]
 (6-23 [6]) GET_NAMED_OBJECT_ID: 0 ms. [96+24 = 120] (Special database object cannot be located)
 (7-23 [7]) FIND_BY_KEY: 0ms. [48+26=74] (Entry not found in index)
 (8-23 [8]) CLOSE_COLLECTION: 0ms. [12 + 0 = 12]
 0ms. [12+0=12] (SessionClosed)

Как расшифровать результаты

Приведем пример результата:

(2-23 [2])GET_DBINFOFLAGS: 10ms. [14 + 16 = 30]

В табл. 18.19 описан каждый элемент. Пользуясь этой таблицей как руководством, постарайтесь проанализировать данные о влиянии параметров настройки. Разобравшись в одной строке результатов, вы начнете понимать, что происходит между клиентом Notes и сервером. Ясно представив себе весь процесс, вы сумеете извлечь для себя очень важную информацию.

Таблица 18.19. Описание результатов теста из файла *performance.txt*

Результат	Описание
(2-23 [2])	Порядковый номер
GET_DBINFOFLAGS:	Выполняемая задача
10 ras.	Время выполнения задачи
14	Передано данных
16	Принято данных
30	Общий объем данных (байтов)

Дополните сведения о клиенте информацией, накопившейся в журнале сервера за время тестирования. Объедините результаты работы инструментов, описанных в этой главе, с тестами соединений - и вы создадите полный отчет о поведении приложений R5/6. Например, результаты команды *show statistics* отображают подробную информацию о нагрузке сервера и сети в ходе описанного клиентского теста.

ГЛАВА 19



Когда речь идет о производительности сервера, на самом деле имеется в виду взаимодействие между аппаратным обеспечением сервера, сетью, локальной операционной системой, системой Notes и сторонними пакетами прикладных программ. Способ объединения этих элементов определяет, насколько хорошо заданная конфигурация выполняет порученную работу. Сервер Domino способен передавать тысячи сообщений за долю секунды, поддерживая переговоры, что может перестроить методы выполнения работы в компании, укрепляет электронную коммерцию или просто помогает служащим строить свои личные планы. Администраторы, пользователи и управляющие предпочитают наименее сложные способы увеличения скорости и надежности сервера. В данной главе рассмотрено, как добиться максимальной отдачи от сервера Domino. За справочной информации о компонентах Web обратитесь к главе 15, а для получения более подробных сведений о производительности сервера - на следующие сайты: www.redbooks.ibm.com/, www.lotus.com/performance, www.notes.net/today.nsf, www.compaq.com/activeanswers/about/lobbv.html, www.microsoft.com/support, www.mcp.com/personal, www.innervy.com/, www.rs6000.ibm.com.

Компоненты

В части I этой книги вы познакомились с установкой и запуском сервера. Теперь, когда вы просмотрели журнал сервера и послушали пользователей, можно решить, какая часть системы требует усовершенствования. Что именно вы будете делать, зависит от места возникновения проблемы.

При настройке производительности любой системы в первую очередь необходимо изучить конфигурацию компонентов, с которыми вам предстоит иметь дело, а также узнать, что вы имеете перед началом работы. Составьте опись конфигурации системы (звучит как тема для базы данных Notes). Система не ограничивается интерфейсом между сетью и аппаратным обеспечением сервера. Настройка производительности включает в себя все - начиная с данных, передаваемых через сервер, и заканчивая Рабочим столом пользователя.

Вторая задача при настройке производительности состоит в последовательном (если не постоянном) контроле компонентов системы. Это послужит прочным основанием для принятия правильных решений - и с этого необходимо начинать. Без мониторинга

производительности вы не сможете определить стартовую точку своей работы или то состояние, в которое перешла система. Как понять, где вы находитесь в данный момент? Прочтите главу 18, чтобы составить план мониторинга.

В настоящей главе сделано допущение, что сервер работает и известны основные операции Notes/Domino. Как уже указывалось, настройка не ограничивается аппаратным обеспечением сервера. Изготовители серверов понимают это и не сводят свои средства проверки только к программам тестирования оборудования. Компании-изготовители предполагают решение задачи от начала до конца. Администраторы Notes могут рассматривать производительность только той части системы, за которую они отвечают, но каждый уровень процесса либо повышает, либо уменьшает уровень производительности для конечных пользователей. Основные компоненты системы приведены ниже (но это только начальная точка):

- аппаратное обеспечение;
- операционная система;
- программное обеспечение Notes/Domino;
- сторонние программные продукты;
- сеть.

Аппаратное обеспечение

Одинаковой аппаратуры не существует. Я уверен, что вы не удивились. Большинство продавцов аппаратуры это знают еще более точно, чем мы с вами. Производители получают средства к существованию, внедряя доступные технологии в пользующийся спросом продукт. Производители серверов в своих рекламных объявлениях упоминают параметры производительности. Продавцы серверов заявляют, что сервер сможет обслуживать десятки тысяч пользователей. Нельзя сказать, что они заведомо искажают факты. Просто каждый продавец старается выставить свой продукт в лучшем виде.

Прежде чем скептически смотреть на эти параметры, попытайтесь понять, что они означают. Являются ли они результатами общепринятых, стандартных тестов? В каких условиях проводились проверка - в лабораторных или в реальных?

Нередко можно встретить рекламу серверов, где в отчетах NotesBench утверждается, что сервер в состоянии обслуживать десять тысяч и более одновременно работающих пользователей. Но вам неизвестно, какие действия выполняли пользователи во время теста, какой тип деятельности исследовался, какова конфигурация машины. Упоминается ли об объеме оперативной памяти, количестве процессоров и сетевых адаптеров? Всеми этими компонентами допустимо управлять, чтобы улучшить производительность. Если вы работаете в компании и занимаетесь крупными закупками, спросите продавца, есть ли у него потребитель, который использует такую же конфигурацию, что и вы. Полезно поинтересоваться, как функционирует такая конфигурация. Подобные разговоры могут дать гораздо больше, чем кажется на первый взгляд.

Ниже описаны режимы нагрузки для теста NotesBench. После обсуждения различий между несколькими режимами работы можно задать продавцу вопросы, которые помогут вам сэкономить деньги компании для более важных вещей, например таких, как ваша зарплата.

Основные правила из предыдущих версий Notes действуют во всех версиях. В представленном списке перечислены способы, с помощью которых продавцы «выжимают» из сервера максимальную производительность. Если вы использовали Notes в течение нескольких лет, то, наверное, уже встречались с некоторыми из них.

Из-за ограниченности бюджета и времени многие производители не вносят всех изменений. Расположите элементы в соответствии с приоритетом и по возможности внедрите их. Каждый из них является своеобразным методом увеличения производительности сервера. Также поможет анализ отчетов NotesBench, касающихся типов серверов, которые вы планируете установить. Важную информацию дают результаты тестов изготовителей оборудования. Несколько рекомендаций:

- применяйте максимально быстрые диски (10000 об/мин и более). Несколько дисков среднего размера лучше, чем один большой, разделенный (разбитый) на несколько разделов. Можно также поставить несколько контроллеров;
- распределите базы данных и программы по нескольким физическим дискам. Несколько считывающих/записывающих головок позволяют быстрее читать и записывать данные. Это удобно сделать с помощью массивов RAID или файловых указателей;
- регулярно проверяйте, не появилась ли новая версия BIOS;
- по возможности запишите файлы подкачки на отдельный физический диск. Если свободного диска нет, поместите их на диск с приложениями, а не с данными. Операционную систему и файлы подкачки лучше держать на разных физических или логических дисках;
- не помещайте файлы подкачки и другие подобные данные на одном диске с файлом журнала транзакций. Журнал транзакций постоянно обновляется на диске, при этом диск переходит в режим, отличный от режима произвольного доступа. Непрерывное переключение режимов увеличивает накладные расходы;
- экранные заставки могут потреблять много ресурсов процессора. Поскольку сервер должен находиться в защищенном месте за закрытой дверью, стоит отключить заставку. Если экранная заставка используется в целях безопасности, установите пустой экран. Генерация подробного графического изображения в некоторых заставках потребляет до 100% производительности процессора;
- запланируйте 200-300 Кб памяти сервера на одного активного пользователя (в предыдущих версиях Notes для этого выделялось 300-400 Кб памяти);
- с базами данных постоянно проводятся операции ввода/вывода. Увеличьте размер области чередования массива RAID до 8 или 16 бит. Кроме того, лучше применять аппаратные RAID, а не программные. Они работают быстрее и потребляют меньше ресурсов процессора;
- используйте адаптеры шины PCI (дисковые контроллеры и сетевые адаптеры) вместо EISA или EISA/PCI;
- ○ установите серверы с несколькими высокоскоростными процессорами. Версии R5 и R6 лучше работают с несколькими процессорами, чем предыдущие. Как ни странно, но несколько процессоров могут ухудшить производительность из-за управления распределением задач между процессорами. Для серверов NT 4.0 лучше всего использовать четыре процессора;
- подумайте о секционировании серверов Domino. Как правило, предусматривается один процессор на секцию. Платформа AS/400 является исключением из правил. AS/400 может логически отделить секции, что позволяет при сбое одной секции использовать остальные;
- при наличии нескольких сетевых адаптеров на секцию (вместо присвоения нескольких адресов на один адаптер) удастся достичь увеличения производительности;

- О избегайте регистрации в журнале сервера (log.nsf) и указания параметров отладки в файле notes.ini, пока это вам действительно не потребуется для решения конкретной проблемы. Если есть возможность выбора, фиксируйте результаты в текстовых файлах;
- О если сервер работает под управлением Windows NT 4.0, проверьте фрагментацию диска, когда сервер отключен для профилактики. NT 4 не имеет встроенного средства дефрагментации, поэтому необходимо найти сторонний продукт (в Windows 2000 есть встроенное средство дефрагментации);
- О не сжимайте системный диск NT, файл подкачки, журнал транзакций и диски, содержащие базы данных: многие клиенты отмечали при этом сбой системы, зависание сервера и потерю информации. Среда Lotus не поддерживает конфигурацию с сжатием;
- О установите в системном реестре NT для параметра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\Memory Management \LargeSystemCache значение 0 с помощью редактора реестра. Сервер станет работать как сервер приложений, а не как файловый сервер. Перезагрузите сервер, чтобы задать новые параметры;
- О устранили предполагаемые точки сбоя конфигурации. Если возможно, обратитесь к общедоступным средствам сокращения нагрузки для сильно загруженных серверов и обеспечения защиты от сбоев. Общедоступные средства включают в себя кластеры (и аппаратные, и программные средства Domino), HACMP или диски общего использования.

Операционные системы

Все современные операционные системы способны контролировать общее состояние серверных и сетевых операций. Фактически все сложные платформы Windows NT и UNIX, известные на сегодняшний день, располагают отличными средствами для отслеживания потенциальных проблем или «узких мест» в системе. В главе 18 описано, как установить счетчики в Системном мониторе NT, чтобы просматривать множество статистических отчетов о работе сервера.

Если вы планируете устанавливать новые версии Domino, ознакомьтесь с новыми инструментами, предлагаемыми поставщиками операционных систем, такими как средства Windows 2000. Существует официальное издание Microsoft - «Planning Windows NT Server 4.0 Deployment with Windows 2000 Server in Mind» (<http://www.microsoft.com/TechNet/deploy/nt4tont5/nt4tont5.htmV>)

Средства мониторинга производительности операционных систем могут работать либо по требованию, используя определенные экземпляры для сбора информации об определенных системах или подсистемах, либо постоянно в фоновом режиме. Большинство администраторов применяют эти средства, самостоятельно вызывая их, но для большой конфигурации вы, вероятно, захотите, чтобы некоторые средства функционировали постоянно. В то время как Notes обладает средствами тестирования производительности почтовых служб, такими как зонды, а агенты SNMP служат для проверки сетевых соединений, в операционных системах имеются собственные средства сбора системной статистики.

На сайте компании IBM содержится информация о настройке производительности AIX. На сайте http://www.rs6000.ibm.com/docJink/en_US/a_dor_lib/aixbman/prftungd/contperfinon.htm есть рекомендации о постоянном мониторинге в среде AIX. Все разработчики

основных ОС также предлагают свои продукты для оптимального мониторинга и настройки производительности системы. Администратору Notes должны быть знакомы все операционные системы, на которых работают его серверы. Сетевому администратору часто спрашивают, почему происходит то или иное событие. Поскольку в Domino присутствует компонент Web, администратору полезно знать основы системы защиты и сетевых технологий.

Специальный анализ системы UNIX

В этом разделе рассмотрены параметры, задаваемые для серверов Domino, функционирующих под управлением UNIX. Некоторые принципы, изложенные здесь, также относятся к AS/400. Параметры, установленные в файле notes.ini, подходят для UNIX и сервера Domino, работающего под управлением этой системы, что позволяет получить большую выгоду, если конфигурация изменяется на уровне ОС. Примером могут служить параметры, влияющие на использование памяти и распределение приоритетов процессов.

Notes_Shared_DPOOLSIZE

Notes_Shared_DPOOLSIZE - переменная окружения, которая определяет в операционных системах System V размер памяти или файлов, отображаемых в память (командой пнпар). Эта память предназначена для распределения данных между серверными задачами. Если сервер не может выделить дополнительную память, увеличьте значение указанной переменной, чтобы предоставить дополнительный ресурс. Прочтите документацию по ОС и уточните параметры, устанавливаемые по умолчанию, и действующие на них ограничения. Оба значения зависят от платформы.

AIX и HP-UX используют общую память System V. Для получения списка сегментов общей памяти, используемых Notes/Domino, запустите команду `ipcs -a`. Максимальный размер сегмента, с которым работает Domino, является значением по умолчанию для Notes_Shared_DPOOLSIZE на данной платформе.

Системы Solaris используют файлы, отображаемые в память по умолчанию, но поддерживают также и память System V. Выполните команду `ls -al/tmp` и зафиксируйте результаты, начинающиеся с .NOTESMEM. Максимальный размер полученного при этом файла и будет значением по умолчанию для переменной Notes_Shared_DPOOLSIZE.

Распределение приоритета задач

ОС UNIX способна работать лучше, если распределить приоритеты задач, выполняемых сервером Domino. Этот метод позволяет выделить для некоторых задач больше времени. Проще всего решить задачу, когда Domino является приложением, работающим на данном сервере. Однако можно получить снижение производительности, если низкоприоритетным задачам выделить ресурсы, необходимые для задач с более высоким приоритетом. Убедитесь, что сумеете восстановить предыдущие значения, если контрольные результаты покажут ухудшение производительности.

Чтобы уменьшить время отклика системы в Domino под управлением Solaris, надо изменить значения класса задач Time Sharing. Информация об этом содержится в отчетах NotesBench, выпускаемых компанией SUN.

Такие вопросы, как распределение приоритетов задач, лучше освещаются разработчиками ОС. Здесь же упоминанием о настройке системы только задается точка отсчета. Чтобы в полном объеме рассмотреть эти вопросы, свяжитесь с разработчиком и убедитесь, что правильно внедрили указанные принципы.

Установка Domino на серверах SUN

Дополнительная информация о настройке серверов SUN для Domino содержится в книге «Implementing Lotus Domino on SUN - Including Sizing Guidelines Architectural Examples», электронная версия которой представлена по адресу <http://www.sun.com/servers/workaroud/solutions/lotus.html>.

Для установки приоритетов задач в системах Domino под управлением AIX пользуйтесь командами `renice` и `/usr/samples/kernel/schedtune`. Настройка приоритетов определенных задач Notes поможет улучшить производительность. Познакомьтесь также с документацией по ОС.

Программное обеспечение Notes/Domino

В `notes.ini` есть несколько параметров, влияющих на производительность Notes и Domino после установки. Некоторые темы, рассматриваемые здесь, более подробно освещаются в других главах книги. Основной целью этой главы является выделение опорных точек для дальнейшего изучения. Некоторые изменения являются общими, остальные вносятся в зависимости от сложившейся ситуации. В последующих разделах описаны изменения существующих параметров и дополнительных параметров файла `notes.ini` сервера.

Настройка `notes.ini` сервера способна значительно повлиять на способ обработки запросов пользователей. Далее в нескольких разделах обсуждаются способы эффективной настройки параметров. Большинство из указанных изменений легко сделать с помощью клиента Notes вместо непосредственного редактирования `notes.ini`. Если вы модифицируете сам файл инициализации в текстовом редакторе, сначала создайте рабочую копию (сохраните файл под другим именем), чтобы в случае аварии можно было отменить изменения. Некоторые изменения вносятся в определенные поля соответствующих разделов серверного документа. Откройте клиент Domino Administration и выберите сервер, который нужно настроить. Затем выполните **Configurations => Add** (Конфигурация => Добавить) или **Edit => Configuration** (Редактировать => Конфигурация), если документ уже существует. Появится окно **Configuration Settings** (Параметры конфигурации). Перейдите на вкладку **NOTES.INI Settings** (Параметры настройки `notes.ini`), чтобы открыть окно, изображенное на рис. 19.1.

Интерактивная справка о командах AIX

Вопросы, касающиеся производительности и использования команд AIX, можно просмотреть по адресу <http://www.rs6000.ibm.com/doc-link/en-US/a-doc-lib/aixgen/wbinfnav/CmdRefToD.htm>.

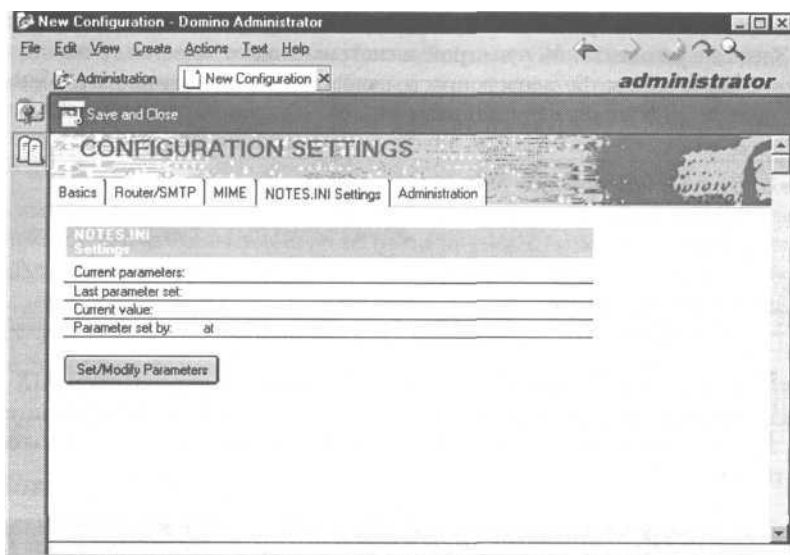


Рис. 19.1. Вместо непосредственного редактирования notes.ini можно использовать окно Configuration Settings в каталоге Domino

Щелкните по кнопке **Set/Modify Parameters** (Установить/изменить параметры). Откроется окно **Server Configuration Parameters** (Параметры конфигурации сервера). Затем нажмите на стрелку справа от поля **Item** (Элемент), чтобы вывести список доступных параметров, которые можно изменить в файле notes.ini (рис. 19.2).

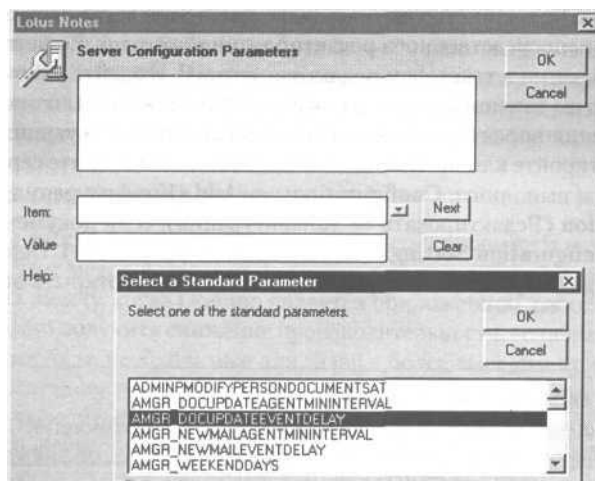


Рис. 19.2. Выберите параметр файла notes.ini, значение которого нужно установить

Откажитесь от соблазна одновременного изменения нескольких параметров: так вы не сможете точно оценить результаты. Важно контролировать журнал, Системный монитор и любые другие средства, позволяющие предвидеть влияние сделанных изменений на производительность системы. И еще раз напомним: необходимо сначала создать определенную базу, с которой будут сравниваться полученные результаты. Фиксация результатов может принять правильные решения и пригодится в качестве обоснования для обращения к руководству с требованием о приобретении дополнительной аппаратуры. И наконец, если вы выполняете какие-либо операции, подвергающие риску данные, сделайте полное резервное копирование.

Параметры *notes.ini*, влияющие на производительность

В данном разделе описываются параметры файла *notes.ini*, которые влияют на производительность сервера Domino. Можно устанавливать параметры либо непосредственно в файле инициализации, либо в окне **Configuration Settings**, рассмотренном в предыдущем разделе. Полезно после внесения изменений всегда просматривать журнал, чтобы найти ожидаемые (или неожиданные) изменения в работе сервера. Итак, на производительность сервера Domino влияют:

- О параметры, управляющие менеджером агентов, который запускает переключаемые событиями агенты. Когда создается событийный агент, Domino сразу его активизирует. Если агент в вашей системе запускается не тогда, когда планируется, проверьте эти параметры. Многие администраторы отменяют или задерживают исполнение агентов, установив для параметров *Amgr_DocUpdateAgentMininterval*, *Amgr_DocUpdateEventDelay*, *Amgr_NewMailAgentMininterval* и *Amgr_NewMailAgentEventDelay* значение 0. Только непроизводительные издержки системы могут вызвать задержку до двух минут. Обычно выделение больших ресурсов менеджеру агентов уменьшает доступные ресурсы для других операций. Можно установить частоту запуска агента с помощью следующих параметров:
 - *Amgr_DocUpdateAgentMininterval*. Задаёт время (в минутах), которое должно пройти между запусками агента, реагирующего на документы. По умолчанию - 30 минут;
 - *Amgr_DocUpdateEventDelay*. Определяет время (в минутах), которое должно пройти между событием обновления документа и запуском агента. Если в течение этого времени получено уведомление об обновлении еще одного документа, он тоже будет обработан. По умолчанию - 5 минут;
 - *Amgr_NewMailAgentMininterval*. Устанавливает время (в минутах), которое должно пройти между запусками агента, реагирующего на почту. По умолчанию - 0;
 - *Amgr_NewMailAgentEventDelay*. Назначает время (в минутах), которое должно пройти с момента получения новой почты и запуском агента. По умолчанию - 1 минута;
 - *DominoAsynchronizeAgents*. Указывает, как выполняются агенты, запущенные Web-клиентом, - одновременно или последовательно. По умолчанию установлено значение 0 (агенты должны исполняться последовательно). Чтобы разрешить одновременное выполнение Web-агентов, установите значение 1;

- О параметры, управляющие очередностью агентов. Указанные здесь параметры регулируют частоту проверки менеджером агентов наличия новых агентов в очереди:
 - Amgr_SchedulingInterval. Задаёт периодичность (в минутах) выполнения планировщика менеджера агентов. По умолчанию - 1 минута, но можно назначить любой период от 1 до 60 минут;
 - AmgrJJntriggeredMailInterval. Определяет периодичность проверки необработанной почты. Допустимы значения от 1 до 1440. По умолчанию - 60 минут;
 - О установки серверного документа для одновременно работающих агентов. Можно указать число агентов (максимум 10), которые система в состоянии запустить одновременно. На серверах, исполняющих много агентов, увеличение числа одновременно действующих агентов повысит скорость обработки сопутствующих данных. Задайте нужные параметры на вкладке **Server Tasks => Agent Manager** (Серверные задачи => Менеджер агентов) в серверном документе настраиваемого сервера (рис. 19.3).
- В зависимости от задач, выполняемых на сервере, можно обнаружить, что сервер помещает агентов в очередь. Просмотрите журнал и определите, образовывалась ли очередь до этого. По умолчанию максимальное число агентов равно одному днем и двум вечером. Увеличьте указанные значения и снова проверьте журнал;
- О параметры, влияющие на производительность секционированных серверов и серверов в кластере. Хотя программный код Domino достаточно хорошо распределяет ресурсы для одного сервера, обслуживание нескольких серверов может потребовать

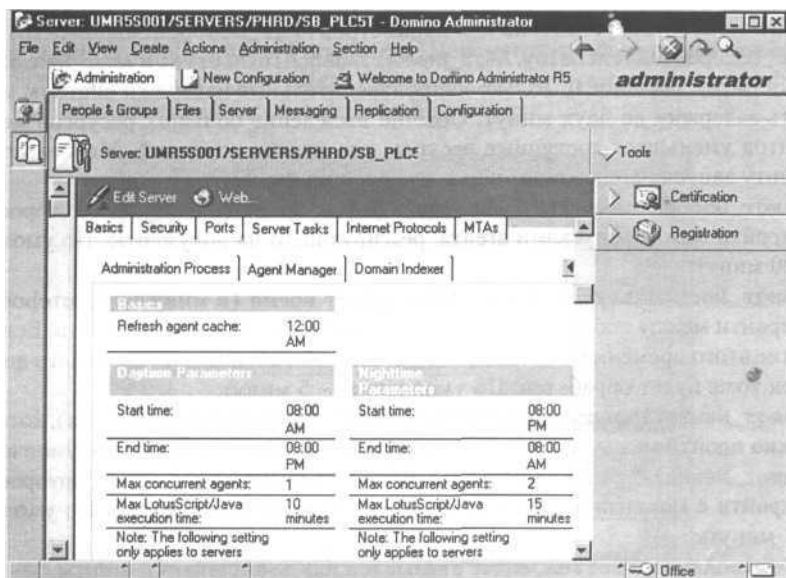


Рис. 19.3. Укажите максимальное число одновременно функционирующих агентов.

Для нерабочего времени число может быть больше, поскольку именно эти часы наиболее удобны для обработки многочисленных документов. Допустимо настраивать время начала и окончания работы для дневного и ночного времени суток

ручного вмешательства, поскольку средств распределения ресурсов между кластерами и секциями не существует (еще один элемент, который можно отнести к этой категории, - параметр **NSF_Buffer_Pool**, рассматриваемый позже):

- **Server_Availability_Threshold**. Влияет на распределение нагрузки в кластере. Установка слишком маленького значения (допустимы значения от 0 до 100) приведет к задержке обслуживания клиентов, которые могли нормально работать с другой, менее загруженной частью кластера. При задании чрезмерно большого значения появляются дополнительные издержки. По умолчанию - 0;
- **Server_Max_Concurrent_Trans**. Позволяет ограничить максимальное число одновременных транзакций сервера. Если вы указываете этот параметр для секционированных серверов, то рекомендуется, чтобы общее значение было не более 20. Например, если на одном компьютере работают две секции, установите значение меньше 10 для каждой секции. Для данного параметра нет значения по умолчанию.

В операционных системах **UNIX** и **AS/400** можно установить значение - 1, что позволит ядру ОС управлять планированием задач. Для таких платформ это может быть очень эффективным решением, значительно увеличивающим производительность;

О установка ограничений для числа пользователей и времени соединения (допускается ограничить число пользователей и время, в течение которого им разрешено оставаться подключенными к серверу):

- **Server_MaxUsers**. Позволяет устанавливать максимальное количество пользователей, которым предоставлен доступ к серверу. Когда достигается заданное число, сервер прекращает отвечать на запросы **Database Open** (Открыть базу данных). Ограничив число активных пользователей, можно увеличить производительность. Значение 0 означает, что число активных пользователей не лимитируется. Значения по умолчанию нет;
- **Server_Session_Timeout**. Указывает время (в минутах), по окончании которого сервер автоматически разрывает сетевое или мобильное соединение. Специалисты Lotus рекомендуют назначать не менее 15 минут. Очень маленькое значение приведет к тому, что сеансы будут открываться снова и снова, а это ухудшит производительность сервера. По умолчанию - 4 часа. Помните, что мобильное соединение характеризуется гораздо меньшим тайм-аутом, установленным в клиенте Notes. Меньший тайм-аут, установленный XPC, имеет преимущество над параметром сервера. XPC используется при модемном соединении или соединении с помощью **ISDN**.

Изменения параметров агентов в R5/6

В предыдущих версиях Notes был параметр (Max % busy before delay) серверного документа, который управлял помещением агентов в очередь в зависимости от загруженности сервера. Когда коэффициент использования сервера превышал значение, установленное в этом поле, сервер прекращал выполнение агентов до тех пор, пока не освобождались необходимые ресурсы. Начиная с версии R5 данный параметр не применяется.

*Начиная с версии R5 при помещении агента в очередь из-за нехватки ресурсов в журнал заносится запись **AMgr. Agent scheduling is paused** (Менеджер агентов: выполнение агента приостановлено). Если агенту для определенной работы требуется больше времени, чем положено, поищите такую запись в журнале.*

Задачи сервера

Со временем роль сервера в организации может изменяться. Например, сервер, который был когда-то почтовым, становится шлюзом, или вы усовершенствовали его и сделали концентратором. Даже на новом сервере следует удалить ненужные задачи. При обычной установке Domino в файл notes.ini по умолчанию помещается около 16 серверных задач.

Каждая работающая серверная задача потребляет определенные системные ресурсы. Освободите строку ServerTasks в файле notes.ini от лишних задач. Это сократит число работающих задач и высвободит ресурсы сервера. Если вам незнакомы функции задач сервера, обратитесь к приложению G книги «Administering the Domino System», входящей в комплект серверного ПО. Такой же список имеется в базе данных Administration Help и на сайте Notes.Net.

Откройте файл notes.ini и найдите строку ServerTasks. Сравните задачи, указанные в этой строке, с теми, которые требуются в данный момент. Если, например, вы не меняете пользователей служб Notes, то задачу компоновки можно удалить. В результате очистится также дисковое пространство, занимаемое базой данных компоновки. Будьте внимательны: не удалите по ошибке что-нибудь нужное.

Transaction Logging (Регистрация транзакций), новая серверная задача, появившаяся в версии R5, способна значительно повлиять на производительность сервера. Изменения баз данных перед сохранением на диске помещаются в журнал транзакций. Lotus рассматривает журнал транзакций как эффективный метод восстановления поврежденных баз данных посредством задачи Fixup, а также как новый способ резервирования. Специалисты Lotus заявляют, что включение регистрации транзакций может повысить производительность сервера более чем на 10%.

Однако у некоторых администраторов регистрация транзакций вызывает опасения, поскольку это требует изменения конфигурации контроллера и диска. Следует также упомянуть, что программ, позволяющих резервировать данные с помощью журнала транзакций, в версии R5 нет. Впоследствии компания IBM выпустила агент резервирования для R5 - ADSM, который подходит и для версии R6. Теоретически регистрация транзакций - хорошее средство, но прежде чем положиться на него, протестируйте его в своей конфигурации.

TranslogJStatus

Translog_Status включает и выключает регистрацию транзакций для всех баз данных R5/6, расположенных на сервере. (Регистрацию транзакций можно отключить на уровне базы данных, если она активизирована на уровне сервера.) По умолчанию установлено значение 0 (отключено). Этот и другие параметры, касающиеся регистрации транзакций, находятся на вкладке **Transaction Logging** в серверном документе. Вы не можете изменить значение переменной Translog_Status на вкладке **Server Configuration**. Оно определяется в файле notes.ini с помощью параметров, заданных на вкладке **Transaction Logging** в серверном документе. Регистрация транзакций - важное новое средство версий R5/6. Более подробно оно рассмотрено в главе об установке сервера и в документации.

Задачи Multiple Replicator и Mail Router

Можно улучшить производительность сильно загруженного сервера, настроив систему на использование задач Multiple Replicator (Множественный репликатор) и Mail Router (Почтовый маршрутизатор).

Почтовый маршрутизатор (mail.box) захватывается любым процессом чтения или записи в маршрутизатор, следовательно, несколько почтовых маршрутизаторов позволяют обрабатывать большее число сообщений. Проконтролируйте очереди сообщений и общую нагрузку системы на наличие сообщений об ошибках или на значительное снижение производительности до и после добавления дополнительных маршрутизаторов. В почтовые концентраторы репликации лучше ввести новые маршрутизаторы, а вот серверы приложений и концентраторы репликации могут значительно увеличить производительность, если дополнительно установить серверы репликации.

В большинстве систем при добавлении более одного маршрутизатора производительность возрастает незначительно. Основное правило Lotus гласит, что для систем с числом пользователей почты 200 достаточно одного маршрутизатора. Второй нужно добавлять, когда в системе 1000 пользователей, а при превышении этого числа необходимо установить 10 маршрутизаторов.

Обычно в системе работает один сервер репликации на один процессор сервера. Концентраторы репликации, к которым нет постоянного обращения пользователей, способны значительно увеличить производительность за счет настройки дополнительных задач репликации. Кроме того, если сервер выполняет множество перекрывающихся сеансов репликации, для улучшения производительности следует добавить дополнительные серверы репликации. Каждый экземпляр задачи репликации будет обрабатывать один сеанс.

Просмотрите события репликации в журнале сервера и документах соединения, чтобы найти самое удачное время репликации для радиальных серверов. Если сеанс через определенный порт идет дольше, чем все остальные сеансы, уменьшите частоту репликации или переведите сеанс на более скоростной порт. Множественные серверы репликации позволяют распределить расписание репликации и действительно сократить ее цикл.

Параметры, улучшающие производительность баз данных и каталогов

Речь идет о параметрах файла notes.ini, которые управляют способом распределения памяти сервера. Как правило, администраторы не применяют эти параметры, но из любого правила всегда есть исключение.

NSF_Buffer_Pool

NSF_Buffer_Pool - это раздел памяти, который управляет буферизацией ввода/вывода при передаче между функцией индексирования NSF и диском. Для одного экземпляра сервера Domino на одной машине нет необходимости устанавливать данный параметр, который может даже мешать нормальной работе. По умолчанию его значение определяется серверным программным обеспечением. Если сервер обновляется от предыдущих версий (R4), посмотрите указанный параметр в notes.ini. Lotus рекомендует удалить его перед обновлением серверов в единичном экземпляре.

При работе секционированных серверов этот параметр пригодится для повышения производительности, поскольку Domino не в состоянии динамически распределять память между секциями. Если на секционированном сервере часто происходит подкачка, задайте значение параметра ниже установленного по умолчанию (одна треть памяти системы) - это будет способствовать росту производительности. Параметр особенно полезен для платформ UNIX.

Для большинства платформ его максимальное значение равно 256 Мб. Исключением являются 16-разрядные платформы Macintosh и Windows, где максимальное значение составляет 16 Мб. Специалисты Lotus советуют пользоваться следующей формулой:

$$\text{NSF\_Buffer\_Pool} = \text{объем оперативной памяти} / \text{число секций} / 4.$$

NSF_DbCache_Maxentries

Параметр NSF_DbCache_Maxentries определяет число баз данных, которое сервер способен хранить в кэш-памяти. База, находящаяся в кэше, открывается гораздо быстрее, чем база, хранящаяся на диске. Минимальное число - 25, а максимальное - около 2000 (зависит от платформы). Повышение этого значения может привести к росту производительности за счет доступной памяти.

Дополнительная физическая память тоже увеличивает число баз данных, которые могут помещаться в кэш-памяти Domino. Значение по умолчанию, которое также указывается в notes.ini, больше 25 или значения NSF_Buffer_Pool (если оно установлено), деленного на 300.

Дополнительные свойства баз данных, влияющие на производительность

Если вы выберете значок базы данных, затем **File** => **Database** => **Properties** (Файл => База данных => Свойства) и в появившемся окне перейдете на вкладку с изображением шапочки с пропеллером (рис. 19.4), то получите доступ к следующим свойствам баз данных

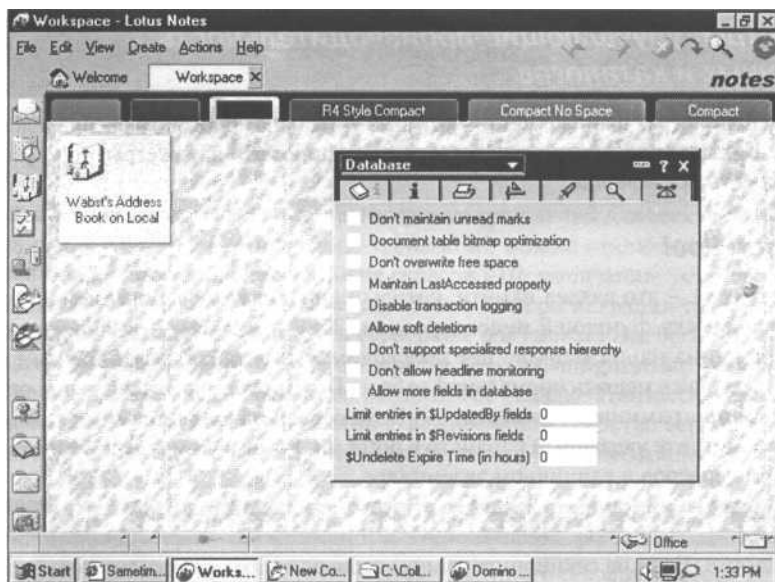


Рис. 19.4. Вкладка Advanced Properties для базы данных.
Некоторые свойства могут влиять на производительность базы и сервера

(важно иметь в виду, что выбор или отмена некоторых указанных свойств влияет на регистрацию транзакций; для обеспечения целостности информации может потребоваться полное резервное копирование базы данных):

- О **Don't maintain unread read marks.** Начиная с версии R5/6 можно было указать, нужно ли поддерживать непрочитанные метки для каждой базы данных. Поддержка меток снижает производительность. В конкретной базе данных, для которой нет необходимости в поддержке непрочитанных меток, как в случае системных баз (например, журнала каталога Domino), установите флажок против этого параметра;
- О **Document table bitmap optimization.** Когда Notes обновляет виды, система обращается к информационным вкладкам документа, чтобы определить, какие документы отображать на виде. Если выбрано свойство **Document table bitmap optimization**, Notes связывает вкладки с формами, используемыми каждым документом. Затем Domino просматривает только вкладки, связанные с теми формами, с которыми работают документы в обновляемом виде. После изменения этого свойства необходимо сжать базу данных, чтобы применить его, а если включена регистрация транзакций, то Lotus рекомендует в максимально короткий срок провести полное резервное копирование (архивирование) базы;
- О **Don't overwrite free space.** Для обеспечения защиты информации система Notes записывает новые данные на место старых. При этом предотвращается возможность доступа к старым данным, но появляются дополнительные операции ввода/вывода для диска, что отрицательно влияет на производительность. Если вы уверены, что сервер надежно защищен или по своей сути данные не слишком важны, можно установить этот параметр. Помните, что вы подвергаете информацию определенному риску в случае изменения состояния защищенности сервера;
- О **Maintain LastAccessed property.** По умолчанию каждая база данных хранит дату последней модификации любого документа. Если указать этот параметр, то Notes будет фиксировать все обращения к документу - для записи или чтения. Параметр обычно нужен, когда установлено удаление документов в зависимости от активности. Выбор данного параметра отрицательно сказывается на производительности;
- О **Disable transaction logging.** При назначении такого параметра регистрация транзакций для базы данных отключается. Регистрация транзакций ускоряет перезагрузку сервера, поскольку при загрузке нет необходимости запускать утилиту Fixup, а также активизирует функции API для резервирования и восстановления базы данных. Специалисты Lotus утверждают, что при введении регистрации транзакций производительность повышается на 10%;
- О **Allow soft deletions.** Этот параметр включает или отключает мягкое удаление в базе данных. В предыдущих версиях Notes удаленный документ терялся полностью и безвозвратно. Восстановить его можно было только с помощью стороннего средства резервного копирования либо из реплики базы данных, в которой он еще сохранился. Версия R5/6 позволяет помещать удаленные документы в Корзину, как в Windows 9x и NT;
- О **Don't support specialized response hierarchy.** Документы Notes отслеживают информацию о дочерних и «ответных» документах, которая требуется только в формулах выбора видов функций @AllChildren или @AllDescendents. Если вы не работаете с этими функциями, установите названный параметр. Когда включена регистрация транзакций, Lotus рекомендует выполнить полное резервное копирование базы данных в максимально короткие*сроки после изменения значения параметра;

- О **Don't allow headline monitoring.** Notes R5/6 позволяет пользователям настраивать заголовки на рабочих станциях, просматривая базы данных на предмет наличия интересующих элементов. Чем больше число пользователей, просматривающих базы, тем сильнее это влияет на производительность. Мониторинг заголовка можно включить или отключить на вкладке со значком шапки с пропеллером в окне **Database Properties** (Свойства базы данных). Чтобы изменить этот параметр сразу для нескольких баз данных, обратитесь к клиенту Domino Administration. Для самых больших баз указанный параметр лучше включить;
- О **Allow more fields in database.** Параметр позволяет базе данных формата R5/6 содержать до 64000 полей. Для баз данных R4 это число было ограничено значением 64 Кб, или 3000 полей. Однако параметр может вызвать проблемы в других областях. Трудности возникают с полнотекстовыми индексами, а вычисление форм с большим числом полей происходит гораздо дольше.

На вкладке со значком пропеллера можно изменить еще три поля, в которых устанавливаются числовые значения. Они предназначены для определения следующих параметров:

- О **Limit the size of SUpdateBy fields.** По умолчанию имя каждого пользователя или сервера, изменяющего документ, фиксируется в поле **SUpdateBy**, имеющемся в каждом документе Notes. Задайте числовое значение в данном поле, чтобы ограничить размер и, следовательно, количество фиксируемых изменений в документах базы. Когда размер поля **SUpdateBy** становится равным указанному, старые записи удаляются, чтобы освободить место для новых;
- О **Limit the size of SRevision fields.** По умолчанию каждый документ Notes содержит поле **SRevision**, используемое для фиксации изменений документа. Здесь хранится дата и время каждой модификации. Значения указанного поля применяются для разрешения конфликтов репликации и сохранения. По умолчанию Notes фиксирует 500 изменений для каждого документа. Один элемент расходует 8 байт. Сократив число фиксируемых изменений, особенно в больших базах данных, можно сэкономить дисковое пространство. С другой стороны, при этом увеличивается число возникающих конфликтов репликации и сохранения. Параметр удобен для баз данных, которые реплицируются и изменяются не очень часто;
- О **SUndelete Expire Time (in hours).** Если разрешено мягкое удаление, то в этом поле указывается, сколько часов удаленный документ еще хранится в Корзине. Если документ не восстанавливается в течение указанного времени, он окончательно удаляется из базы.

Инструменты производительности, поставляемые с Notes R5/6

Большая часть настоящей главы посвящена способам настройки производительности уже установленной системы. В данном разделе рассмотрены инструменты, посредством которых определяется наилучшая конфигурация нового сервера или настройки уже работающего.

Server.Load

Как и NotesBench, этот инструмент применяет определенные сценарии, имитирующие различную нагрузку, для измерения показателей производительности сервера. В отличие от NotesBench, администратор в данном случае может сам создавать сценарии для моделирования необходимой нагрузки.

Server.Load имеется на установочном диске Domino. Этот инструмент содержит сценарии, имитирующие режимы **Idle Usage** (Без нагрузки), **Simple Mail Transfer Protocol Routing** (Маршрутизация протокола SMTP), **Web** (Интерактивный режим), **IMAP** (Поддержка протокола IMAP) и **Shared Discussion Database** (База данных общих форумов). Для установки Server.Load выполните следующие действия:

1. Перейдите в каталог Apps\Sload на установочном компакт-диске. В главном окне установки нет ссылки на Server.Load.
2. Распакуйте единственный файл (sload.exe) в каталог программы Notes.
3. Для запуска Server.Load дважды щелкните по значку исполняемого файла. На рис. 19.5 изображен интерфейс программы Server.Load.

Общее описание всех рабочих нагрузок имеется в разделе NotesBench, а по адресу <http://www.notesbench.org> можно найти более подробную информацию.

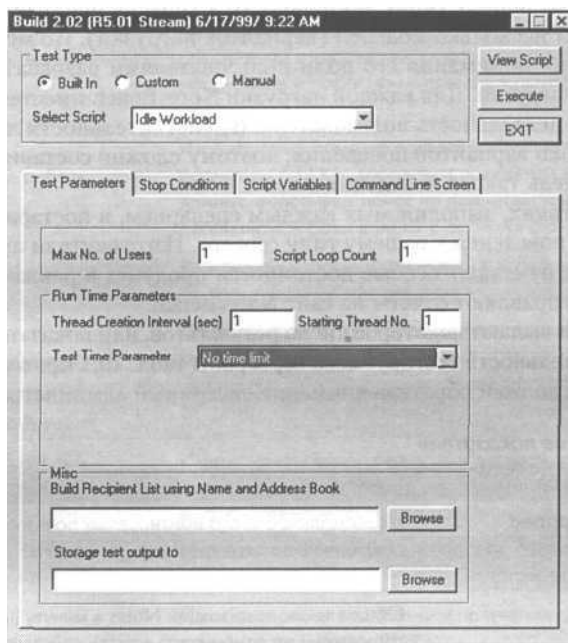


Рис. 19.5. Программа Server.Load позволяет имитировать нагрузку при разных условиях

Server. Planner

Server.Planner Domino - это инструмент, помогающий администратору собирать информацию о планировании производительности нового сервера. Он позволяет оценить сервер, используя контрольные данные изготовителей. Можно ввести сведения об ожидаемой нагрузке, чтобы приспособить информацию изготовителя к вашей конфигурации. Обращайтесь к Server.Planner для определения допустимых характеристик серверов, но не забывайте учитывать конкретные ситуации. Наборы данных для Server.Planner имеются на сайте NotesBench. К сожалению, ассортимент невелик.

ТестNotesBench

Хотя NotesBench разработан компанией Lotus, он не поставляется на компакт-диске Notes CD. Отчеты обычно генерируются изготовителями в собственных лабораториях. NotesBench дает стандартизированное средство оценки поведения Notes/Domino в зависимости от типа нагрузки. Информацию о производительности можно собирать с помощью определенных задач в зависимости от конфигурации.

Сценарии выполняются на отдельном компьютере, называемом *драйвером* (driver), который генерирует нагрузку для тестируемого сервера. Для обеспечения постоянства нагрузки сценарии нельзя изменять. Каждый имитируемый пользователь представляется в драйвере как поток. Следовательно, если вы, например, хотите запустить сценарий, имитирующий 500 пользователей, должно быть 500 потоков, выполняющих этот сценарий для сервера.

Поскольку при различных типах деятельности к серверу предъявляются разные требования, существует несколько моделей (вариантов нагрузки). По мере развития Notes/Domino и улучшения понимания его роли пользователями разрабатываются дополнительные варианты нагрузки. Для каждой нагрузки NotesBench имеется отдельный сценарий, имитирующий деятельность пользователя. В действительности любой пользователь объединяет несколько вариантов поведения, поэтому сложно составить сценарий, точно отображающий модель такого поведения.

Прочтите о действиях, выполняемых каждым сценарием, и постарайтесь максимально приблизить модель поведения к вашему типу сервера. Изготовители публикуют результаты на своих сайтах, отмечают особые достоинства продукта в рекламных объявлениях, а некоторые даже отправляют отчеты на сайт NotesBench.

Тесты NotesBench выдают некоторое число результатов, или показателей, позволяющих оценить производительность тестируемого сервера. В табл. 19.1 приводится список показателей, на которые должен обратить внимание системный администратор.

Таблица 19.1. Важные показатели

Показатель NotesBench	Описание
Maximum Users Supported (Максимальное число поддерживаемых пользователей)	Максимальное число имитируемых пользователей (потоков), соединенных с сервером во время теста
NotesMark (Уровень Notes)	Общее число транзакций Notes в минуту (tpm). Число транзакций по отношению к числу действий пользователя не равно 1:1. Например, открытие базы данных вызывает множество транзакций NotesMark
Average Response Time (Среднее время ответа)	Среднее время ответа сервера на запросы имитируемых пользователей за время теста; приблизительно равно времени ответа на запрос пользователя при такой же нагрузке сервера

Описание рабочих нагрузок

Консорциум NotesBench, который является независимой организацией, публикует описание доступных рабочих нагрузок для тестирования на сайте <http://www.notesbench.org>. Здесь можно найти дополнительную информацию о рабочих нагрузках и новых нагрузках

по мере их появления, а также узнать о том, как получить сертификат на проведение тестов NotesBench в вашей организации. В худшем случае вы будете просто потребителем готовой информации. В табл. 19.2 описаны некоторые рабочие нагрузки.

Таблица 19.2. Описание рабочих нагрузок

Рабочая нагрузка	Действие пользователя
Calendar and Scheduling (Календарь и расписание)	Нескольким получателям отправляются приглашения
Cluster Mail (Почта кластера)	Имитируемые пользователи на многоузловом кластере Domino читают, записывают, передают и получают почту
Cluster Mail and Shared Database (Почта кластера и общая база данных)	Имитируемые пользователи на трехузловом кластере одинаковых серверов. Каждый пользователь отправляет почту и добавляет документы в общую базу данных
Cluster Topology Impact (Влияние кластерной топологии)	Автономный сервер почтовых баз данных и обсуждений соединяется с кластером, а затем отказывает. Имитируемые пользователи работают в пределах почтовых и общих баз данных
Groupware B (Среда коллективной работы категории B)	Имитируемые опытные пользователи отправляют сообщения размером 532 Кб, добавляют документы в общие базы данных, выполняют поиск по полнотекстовому индексу и даже реплицируют базы данных с рабочих станций на сервер
Idle Usage (Без нагрузки)	Имитируемые пользователи просто создают сеанс с сервером, не производя никаких действий
Mail Only (Только почта)	Пользователи читают сообщения и отправляют почту, а также совершают различные действия
Mail and Shared Database (Почта и общая база данных)	Пользователи читают почту и обновляют общую базу данных
Mail Routing Hub (Почтовый концентратор-маршрутизатор)	Имитируется сервер без пользователей, который работает как почтовый маршрутизатор. Почта помещается в систему и затем передается серверу назначения
Online Users (Пользователи в интерактивном режиме)	Пользователи отправляют большие сообщения с вложениями
POP3 (Служба POP3)	Пользователи для отправки и получения сообщений применяют протокол POP3 sfr
Replication Hub (Концентратор репликации)	Имитируется концентратор репликации в топологии «концентратор—радиальные серверы». Здесь нет пользователей
Shared Discussion Database (Общая база данных обсуждений)	Пользователи дают нагрузку серверу, читая, создавая и обновляя документы в общей базе данных
SMTP POP3 (Службы POP3 и SMTP)	Пользователи для отправки и получения сообщений обращаются к протоколам POP3 и SMTP
Web Buyer (Web-покупатель)	Имитируемые Web-пользователи осуществляют покупки, просматривая информацию о продуктах, заполняя формы-заказы и обрабатывая заказы
Web Walker (Web-пользователь)	Web-пользователь просматривает домашнюю страницу и преследует все ссылки

Руководство пользователя NotesBench

Подробное описание всех рабочих нарузок NotesBench имеется в NotesBench User's Guide (Руководство пользователя NotesBench). Это руководство представляет собой базу данных Notes, которую можно найти на сайте NotesBench. Кроме того, рекомендуется получить копию книги «What Every Performance Minded Administrator Should Know About NotesBench Reports» (Что должен знать об отчетах NotesBench каждый администратор, обеспокоенный производительностью).

Чтобы побольше узнать по данному вопросу, рекомендуем как минимум прочесть маленькую статью «What to Look for In Performance Reports» (Что искать в отчетах о производительности). Она имеется в технической библиотеке в Зоне производительности (Performance Zone) компании Lotus на сайте <http://www.lotus.com/performance>.

Компоненты отчета NotesBench

NotesBench представляет собой стандартное средство, поэтому и отчеты, публикуемые тестирующей стороной, должны иметь стандартный формат. Если вы не знакомы с отчетами NotesBench, прочтите хотя бы отчет изготовителя одного из ваших серверов. Можно получить ценную информацию, даже если вы еще не искали новый сервер.

Элементы отчета NotesBench

Далее рассматриваются различные разделы, содержащиеся в отчете NotesBench. К сожалению, большинство администраторов Notes никогда не читали таких отчетов. Это просто потеря ценного источника информации. Аппаратные и программные средства, проверенные изготовителем, выделяются в отчете, как и допустимые пределы увеличения производительности. Предположим, что вы не получите той производительности, которая показана в лабораторных условиях. Маловероятно также, что вы будете обсуждать с продавцом конфигурацию сервера. Было бы хорошо, чтобы большинство администраторов и менеджеров оценили важность информации, имеющейся в отчетах NotesBench, и все же нашли время и прочли их. Итак, разделы NotesBench:

- **Executive Summary** (Резюме по работе). Здесь представлен общий обзор теста. Он должен содержать:
 - дату выполнения теста;
 - наименование организации, выполнившей тест; ϕ
 - модель сервера и производитель;
 - одно-два предложения о конфигурации сервера и методике тестирования.
 Кроме того, обычно приводится таблица, в которой обобщаются результаты теста, что позволяет быстро решить, нужен ли вам этот отчет;
- **Objectives** (Цели). Здесь производитель указывает, какие цели преследовались при проведении теста. Чаще всего целью является демонстрация новых средств и возможностей конфигурации;
- **Test Methodologies** (Методика тестирования). Здесь описывается, каким образом проводился тест. Следует внимательно прочесть данный раздел, понять, что было

сделано и как это можно применить в вашей конфигурации для повышения производительности. На основании приведенных сведений инженер должен настроить сеть и самостоятельно провести тест. Тестирующая организация обязана показать:

- конфигурацию компьютеров, применяемых во время теста. Она обычно включает в себя тестируемую систему, компьютер-драйвер и систему назначения;
 - тип сети и конфигурацию протокола;
 - изменения параметров Notes или системных параметров, отличающиеся от параметров по умолчанию;
 - используемые дополнительные устройства, программы и методы;
- О **Data (Данные)**. В этом разделе приводятся результаты теста. Показаны графические сводки по данным тестирования каждой рабочей нагрузки и информация о времени выполнения, скорости реакции системы и т.п. Обратите внимание на параметры, касающиеся максимального числа поддерживаемых пользователей, параметра **NotesMark (tpm)** и среднего времени ответа;
- О **Analysis (Анализ)**. Здесь описаны результаты, представлена информация о поведении компьютера на разных этапах теста;
- О **Conclusions (Выводы)**. Информация для потребителя. Производители часто помещают дополнительные сведения о способах работы с данной конфигурацией в организации;
- О **Statement by Auditor (Заключение проверяющего)**. Это заключение организации, проводившей тестирование, в котором отчеты и результаты теста приведены к стандарту консорциума NotesBench;
- О **Appendix A - Overall Test Setup and Software Versions (Общая настройка теста и версии ПО)**. В данном приложении показаны графическое изображение сетевых соединений, а также устройства и методы, участвующие в тесте. Хорошее место для поиска новых сетевых решений;
- О **Appendix B - System Configuration (Конфигурация системы)**. В этом разделе помещены таблицы, обобщающие информацию о конфигурации систем, которые используются в тесте, и описание их функций;
- О **Appendix C - Operating System Parameters (Параметры ОС)**. Здесь перечислены все системные «заплатки» и параметры конфигурации, отличающиеся от значений по умолчанию. Посмотрите, какие из этих параметров вы сможете применить;
- О **Appendix D - Notes Parameters (Параметры Notes)**. Здесь указаны установленные параметры Notes и Domino. Это должна быть полная копия файла notes.ini тестируемого сервера;
- О **Appendix E - Network Configuration File(s) (Файлы настройки сети)**. Перечислены применяемые протоколы и их разработчики. Следует фиксировать все параметры, отличающиеся от установленных по умолчанию;
- О **Appendix F - Guidelines for Information Usage (Путеводитель по использованию информации)**. Обычно представляет собой предложение, касающееся способов применения информации, которая содержится в отчетах, как правило **The information may be copied and distributed as long as the complete report remains intact** (Информация может копироваться и распространяться до тех пор, пока весь отчет не изменяется и не редактируется);

- О **Appendix G - Pricing** (Цены). В разделе показаны цены на тестируемое оборудование и ПО. Существуют строгие правила, касающиеся публикуемой информации о том, какие цены и соответствующие скидки получила тестирующая организация. Данный раздел дает общее представление о цене сервера с похожей конфигурацией;
- О **Appendix H - Additional Vendor Defined Information** (Дополнительная информация, определяемая производителем) - необязательно. Здесь производитель может указывать дополнительную информацию о предлагаемых товарах и услугах. Имейте в виду, что эти данные не проверяются и не сертифицируются тестирующей организацией.

Дополнительные средства сторонних разработчиков

Большое число компаний торгует продуктами, ориентированными на Notes/Domino. Продукты, о которых здесь идет речь, предназначены для настройки производительности на серверах Domino и приложениях Notes. Этот список не включает в себя все продукты, приведены только некоторые, облегчающие работу администратора. Программным продуктам, разработанным для анализа производительности, тоже требуются определенные ресурсы, поэтому необходимо проверять средства контроля на наличие отрицательного воздействия. Информацию об остальных продуктах, касающихся производительности Notes и Domino, можно найти в разделе Notes Performance Zone по адресу <http://www.lotus.com/Performance>.

ProActive Assistant от G2 Associates

Этот инструмент позволяет проводить сквозные тесты производительности, мониторинг и анализ системы Domino на рабочей станции. С помощью ProActive Assistant вы получите реальную информацию о сервере, сети и приложениях Notes. Данный инструмент имитирует нагрузку пользователя с помощью настраиваемых сценариев. Можно анализировать результаты в стандартных или настраиваемых отчетах. За дополнительной информацией обращайтесь по адресу <http://www.g2sys.com>.

GroupSizr Pro, WebSizr и MailSizr от Technovations

Инструменты служат для генерации информации о производительности и размерах конфигурации HTTP, Notes/Domino и почтовых приложений. GroupSizr Pro имитирует нагрузку пользователей как для серверов Domino, так и для других серверов. Программа генерирует отчеты о результатах для последующего анализа. WebSizr позволяет анализировать системы на основе Web и выдает данные, касающиеся размеров и характеристик транзакций HTTP. MailSizr предоставляет сведения о размерах и производительности почтовых серверов. За дополнительной информацией обращайтесь по адресу <http://www.technovations.com>.

IntelliWatch Pinnacle or Candle

Инструмент предназначен для автоматического мониторинга производительности Notes/Domino. Посредством параметров компонента Performance Manager (Менеджер производительности) IntelliWatch Monitor обнаруживает и исправляет некоторые маленькие проблемы, пока они не стали большими. Компонент Tracer проводит сквозную диагностику взаимодействия клиент/сервер в реальном времени. И наконец, компонент Analyzer фиксирует данные, полученные от Monitor, для их обобщения. За дополнительной информацией обращайтесь по адресу <http://www.candle.com>.

Производительность сети

Каждый администратор знает, что сетевой интерфейс сервера может оказаться основным «узким местом» системы. Полезно уделить внимание сетевому аспекту Notes и Domino. В главе 19 обсуждается методика оценки сетевой производительности сервера. Как правило, на производительность сервера влияют сетевые протоколы и сетевые карты.

Протокол

Если вы не используете TCP/IP, рассмотрите вариант применения этих протоколов как основного стека в сети. Все доступные средства Notes/Domino настроены на работу с TCP/IP.

Сетевая карта

Замените порты доступа к пользователям на сетевые карты (сетевые адаптеры) со скоростью 100 Мбит/с. Если ваша компания не хочет отказываться от 10-мегабитных карт, применяйте их в сети, предназначенной для репликации или кластеризации. Изоляция сетевого трафика может значительно повысить производительность в сильно нагруженных сетях. В секционированных серверах Notes выделите по 100 Мбит/с на одну секцию.

В сетях с особенно напряженным трафиком и на сайтах, которые должны иметь высокий коэффициент готовности, рассмотрите возможность установки многопортовых сетевых карт. Эти карты позволяют создавать несколько подключений к сети. Кроме того, некоторые из них поддерживают объединение портов (два порта группируются для получения большей полосы пропускания), защиту от сбоев в сети и разделение трафика.

ГЛАВА

20

ПОВЫШЕНИЕ ДОСТУПНОСТИ ДАННЫХ



Некоторые основные темы, рассматриваемые в этой главе:

- О кластеры серверов Domino;
- О секции серверов Domino;
- О службы счетов и аудита;
- О новые улучшенные службы.

Руководители предприятий, которые собираются построить и развернуть бизнес-приложения, предназначенные как для локальных, так и для глобальных пользователей, должны знать, что серверы Domino имеют высокий коэффициент готовности, масштабируемы и надежны. Большинство сложных технологических приложений бесполезны, если к ним нет доступа или они не могут обеспечить должную нагрузку. Сайт не имеет никакой ценности, если работает слишком медленно или в текущий момент недоступен.

В Domino 5 и 6 сделаны значительные шаги в направлении повышения производительности, масштабируемости, надежности и доступности. Более того, в Domino R5 появились средства распределения нагрузки и защиты от сбоев. Масштабируемость и надежность, ранее предлагаемые только для пользователей Domino, сейчас возможны также для Web-приложений и Web-клиентов с помощью ICM (Internet Cluster Manager - менеджер кластеров Internet). Аналогично средства передачи сообщений, такие как планирование, составление календарей и синхронные почтовые агенты, теперь тоже поддерживают защиту от сбоев и распределение нагрузки.

Все это позволяет пользователям продолжать планировать совещания с другими людьми и обрабатывать новую почту, даже если их почтовый сервер в данный момент отключен. Пометки о непрочитанных сообщениях синхронизируются между резервным и основным серверами заранее, а адресация поддерживается и тогда, когда основной сервер не работает. Кроме того, Domino R5/6 может интегрироваться с кластерами приложений на уровне ОС. Например, при работе под управлением Windows NT Domino интегрируется с Microsoft Cluster Server (MSCS) - см. ниже.

Существует несколько причин, по которым усовершенствование возможностей кластеризации и секционирования очень важно для системного администратора и организации в целом. В результате улучшения средств Domino и добавления новой службы

On Disk Structure (ODS) производительность Domino значительно повысилась. Время ответа сервера уменьшилось на 75%, операции ввода/вывода выполняются на 10-20% быстрее, а требования к объему памяти сократились примерно на 30%.

Кроме всего прочего, способность кластеризации увеличивает производительность и позволяет сохранить ее при расширении предприятия. Применение кластеризации и секционирования выгодно, поскольку минимизирует административные расходы и общую стоимость имущества, в дополнение к возрастанию производительности, масштабируемости и надежности. Постоянно возникает проблема - как поддерживать оптимальную производительность системы при минимизации расходов на информационные технологии. С помощью сервера Domino 5/6 гораздо проще получить максимум производительности при полном использовании всех имеющихся средств.

В крупных организациях, установивших серверы Domino, для которых всегда характерен большой сетевой трафик, секционированные серверы помогут лучше масштабировать каждый сервер. Разделение нагрузки и запросов пользователей на несколько серверов не только повысит производительность (и обеспечит прозрачную защиту), но и позволит полностью задействовать мощное современное оборудование. При введении дополнительных служб, таких как кластеризация секционированных серверов, важно понимать, какую роль один сервер играет по отношению к другому и как лучше установить Domino, чтобы получить максимальную производительность. В этой главе рассмотрены настройка файла notes.ini и конфигурирование серверных задач.

Кластеры серверов Domino

В последующих разделах речь пойдет о кластерах в конфигурации Domino и о том, как они работают. Обсуждаются защита от сбоев, распределение нагрузки, доступность, Cluster Manager, Cluster Administrator, Cluster Database Directory и другие серверные задачи. Раздел, посвященный планированию, установке и настройке, содержит подробное описание каждого шага - от рассмотрения требований до планирования, подготовки и установки. В разделе об администрировании детально анализируются все действия, необходимые для создания кластера, добавления и удаления серверов в кластере. Раздел о статистике позволяет изучить мониторинг и управление кластером, а также способы повышения производительности.

Кроме всего прочего, описана интеграция с Microsoft Cluster Server и показана процедура установки и настройки кластерных серверов Domino.

0

Описание

Кластеризацию можно определить как согласованный набор систем и приложений, увеличивающий доступность ресурсов, масштабируемость и эффективность, в сравнении с одной системой или приложением. Кластеризация Domino, более точно обозначаемая специалистами Lotus как *кластеризация приложений*, реализует высокую доступность и масштабируемость для корпоративных приложений в домене передачи сообщений, групповых приложений и Internet. Кроме того, функции защиты от сбоев и кластеризации Domino основаны на содержимом (запрашиваемом пользователем) и часто называются *маршрутизацией на основе информационного содержимого* (content-based routing).

Кластерная архитектура Domino может быть построена с помощью следующих компонентов:

- О Cluster Manager (Менеджер кластеров);
- О Cluster Database Directory (CLDBDIR.NSF - каталог баз данных кластера);
- О Cluster Database Directory Manager Task (CLDBDIR - задача менеджера каталога баз данных кластера);
- О Cluster Administrator (Администратор кластеров);
- О Cluster Replicator Task (CLRREPL - задача репликатора кластера);
- О Internet Cluster Manager (ICM - менеджер кластеров Internet).

При кластеризации все серверы в кластере постоянно обмениваются информацией относительно доступности сервера и синхронизируют реплики баз данных. Репликация между базами данных в кластере гарантирует постоянную синхронизацию между ними. На основании параметров распределения нагрузки Domino Cluster Manager сохраняет информацию на всех серверах и во всех репликах баз, направляя пользователя к оптимальному на данный момент серверу. Кластер Domino включает в себя от двух до шести серверов, обеспечивая постоянный и непрерывный доступ к информации предприятия.

Способность создания кластеров не нова для Domino. Кластеризация впервые была представлена в версии 4 как Notes for Public Networks (Notes для сетей общего пользования) и служила для компаний, предоставляющих услуги связи и Internet. Если сервер приложений был недоступен, пользователь отправлялся на другой сервер Domino, где хранилось такое же приложение. Однако в Domino R5 кластеризация поставляется в версии Enterprise Server. В составе кластера Lotus Domino 6 Enterprise Server могут работать серверы Lotus Domino 6 Utility, Domino Release 5 Enterprise, Domino Release 4.62 Enterprise, Domino Release 4.6 Advanced Services или Domino Release 4.5 Advanced Services.

С появлением Internet Cluster Manager (ICM), новой серверной задачи Domino R5, стала возможной организация кластеризации и распределения нагрузки для Internet-приложений и Web-клиентов. ICM функционирует как промежуточная среда между Web-клиентом и серверами в кластере, принимая запросы от клиента и выбирая наилучший сервер для обработки этих запросов. Репликация в кластере обеспечивает синхронизацию баз данных, а ICM - доступность серверов.

Кроме ICM в Domino R5/6 имеется еще несколько новых средств:

- О защита от сбоев и распределение для планирования и составления календаря (с помощью новой базы данных CLUBSY.NSF);
- О синхронные агенты New Mail Agents (Агенты новой почты), которые обрабатывают почту пользователя, даже когда его почтовый сервер не действует;
- О поддержка адресации и указания каталогов, если основной сервер вышел из строя;
- О синхронизация пометок о неп прочитанных сообщениях между резервным и основным серверами, когда последний не работает (помните, что эти пометки можно отключить).

Возможность кластеризации совместима с различными платформами, как и сама система Domino, и в состоянии функционировать при различных аппаратных конфигурациях. Кластеризацию поддерживают следующие платформы:

- О NT и Windows 2000/Intel;
- О NT/Alpha;
- О Win 95/98;

- OS/2;
- NLM;
- AIX;
- HP-UX;
- Solaris/Intel;
- Solaris/Sparc.

Репликация в реальном времени и другие новые средства Domino гарантируют синхронизацию корпоративных приложений. В настоящей книге подчеркивается, что одним из таких важных средств является новый клиент администрирования Domino Administration. Следовательно, возможность администрирования и контроля средств кластеризации и производительности, порогов пропускной способности и мощности системы в версии R5/6 значительно увеличилась.

Ниже перечислены преимущества использования кластеров Domino:

- высокая доступность баз данных благодаря защите от сбоев;
- распределение рабочей нагрузки;
- масштабируемость;
- синхронизация данных;
- анализ рабочих нагрузок;
- несложное техническое обслуживание аппаратуры и программного обеспечения без перерывов в работе;
- простое резервное копирование баз данных.

Защита от сбоев

В Domino R5/6 возможность кластеризации допустимо расширить, чтобы передача сообщений и приложения также поддерживали защиту от сбоев и распределение нагрузки. Если на сервере Domino есть аппаратные или программные проблемы, возникает сбой в сети, сервер не обслуживается, а если база данных помечена как **Out of service** (Не обслуживается) или **Pending delete** (Приостановленное удаление), кластер направит запрос на другой сервер, который продолжит обслуживание запроса почтового клиента, клиента Notes или Web-клиента.

Следующий список событий показывает, какие действия включают защиту от сбоев в кластере:

- открытие базы данных (SCommand ([FileOpenDatabase])), сценарий LotusScript, использующий OpenWithFailover, или код Java, применяющий метод OpenDatabase класса lotus.domino.DbDirectory);
- вывод на экран ссылки на документ, на вид или на базу данных;
- попытка репликации с недоступной базой данных в кластере;
- компоновка почты;
- поиск имени в каталоге Domino (и средство автозавершения ввода);
- маршрутизация почтовых сообщений внутри домена;
- агенты, обрабатывающие почту, действующие с новыми потоковыми документами;
- средства планирования, в частности приглашения на встречи и поиск свободного времени;
- поиск серверов;
- щелчки по значку **Open URL** (Открыть адрес URL) и по ссылкам URL в определенной части изображения или доступ к нужному адресу URL из Web-браузера.

Защита от сбоев происходит при возникновении проблемы доступа:

- О к серверу:
 - сервер отключен;
 - неполадки соединения в сети;
 - достигнуто максимальное число пользователей (параметр `Server_Maxusers` в файле `notes.ini`);
 - сервер ограничен (параметр `Server_Restricted` в файле `notes.ini`);
 - сервер находится в состоянии **BUSY** (Занят) из-за достижения максимальной разрешенной нагрузки;
- О к базам данных:
 - база данных помечена в Cluster Database Directory (CLDBDIR.NSF) как **Out-of service** (Не обслуживается);
 - база данных помечена в Cluster Database Directory (CLDBDIR.NSF) как **Pending delete** (Приостановленное удаление).

К сожалению, существуют условия, при которых защита от сбоев не срабатывает и пользователь не может получить доступ к запрашиваемому серверу, базе данных или URL. Вот несколько таких случаев:

- О сервер становится недоступным после того, как пользователь уже открыл базу данных;
- О пользователь загружает базу данных через раскрывающееся меню (**File => Database => Open**) или пытается просмотреть ее свойства (**File => Database => Properties**);
- О маршрутизатор старается доставить почту, но для параметра `MailClusterFailover` в файле `notes.ini` установлено значение 0;
- О создается новая база данных;
- О репликация проводится с доступным сервером, даже когда с ним работает максимальное число пользователей или у него максимальная нагрузка либо когда база данных помечена как **Out-of service**. Это не влияет на репликацию.

Можно умышленно вызвать защиту от сбоев, чтобы пользователь с недоступного сервера был направлен на другой сервер в кластере. Такое может произойти во время обновления аппаратного и программного обеспечения, операционной системы или при замене сервера.

Чтобы установить на сервере состояние **RESTRICTED** (Ограничен), необходимо добавить (или изменить) параметр `Server_Restricted=x` в файле `notes.ini`. Если $x=1$, то текущим состоянием сервера станет **RESTRICTED**, которое изменится при перезагрузке сервера. Когда $x=2$, состояние **RESTRICTED** не меняется даже после перезагрузки. Для отмены ограничения сервера установите значение 0. В отличие от состояния **BUSY**, в котором сервер способен принимать запросы при отсутствии других доступных серверов, в состоянии **RESTRICTED** он отклоняет запросы в любом случае.

Распределение нагрузки

С помощью распределения нагрузки администратор может устанавливать пороговые значения, при достижении которых запрос пользователя будет направлен на другой доступный сервер, чтобы ни один из серверов не перегружался. После того как сервер достигает порогового значения (Cluster Manager отмечает сервер как **BUSY**) или число обслуживаемых пользователей становится максимально допустимым, следующие запросы к базам

данных направляются на другие реплики баз в кластере. Для определения места расположения и доступности базы, к которой лучше всего переадресовать запрос, менеджер Cluster Manager использует Cluster Manager Database Directory (Каталог баз данных менеджера кластера). Если больше нет реплик указанной базы данных или все серверы находятся в состоянии **BUSY**, открывается исходная база. Порог доступности не влияет на репликацию, следовательно, репликация выполняется даже при условии, что база данных в настоящий момент занята.

Коэффициент готовности периодически (приблизительно раз в минуту) определяется сервером на основании среднего времени ответа на предыдущий запрос. Коэффициент готовности - это целое число от 0 (низкая нагрузка) до 100 (высокая нагрузка). Для вычисления коэффициента сначала рассчитывается отношение времени ответа на запрос при текущей нагрузке к оптимальному времени ответа на такой же запрос при меньшей нагрузке. Полученный результат вычитается из 100. Имейте в виду, что время ответа сервера обычно составляет небольшую часть от времени ответа, которое видит пользователь. Если коэффициент готовности меньше установленного порога, сервер отмечается как **BUSY**. Пока сервер занят, запросы направляются в другие реплики базы данных, расположенные на другом сервере в кластере.

Для установки порога коэффициента готовности необходимо добавить (или изменить) параметр `Server_Availability_threshold=x` в файле `notes.ini`, где `x` - число от 0 до 100.

Чем больше значение `x`, тем меньшую нагрузку способен выдержать сервер до перехода в состояние занятости. Если задать 100, сервер окажется занятым постоянно - до тех пор, пока не будет указано значение 0, отменяющее распределение нагрузки (значение 0 установлено по умолчанию).

Нагрузкой сервера можно управлять, определив максимальное число пользователей, которым разрешено одновременно работать с сервером. Когда достигается установленный порог, сервер переходит в состояние **MAXUSERS** (Максимальное число пользователей), отклоняя все следующие запросы и направляя их в другие реплики базы данных в кластере до момента, пока число пользователей не уменьшится.

Максимальное число пользователей задается путем добавления (или изменения) параметра `Server_MaxUsers=x` в файле `notes.ini`, где `x` - число пользователей, которые вправе одновременно работать с сервером. Этот параметр не влияет на репликацию. Следовательно, репликация будет выполняться, даже когда к серверу обращается максимальное число пользователей. Данный параметр имеет силу и для серверов, не объединенных в кластеры. Для них при достижении порога запросы не могут направляться на другие серверы и потому просто отклоняются.

Доступность баз данных

Имеется три параметра управления доступностью базы данных (рис. 20.1):

- **Out of service** (Не обслуживается);
- **In service** (Обслуживается);
- **Pending delete** (Приостановленное удаление).

Чтобы изменить доступность базы данных (используемую для управления состоянием доступности кластера):

1. Откройте Domino Administrator на существующем сервере Domino.
2. Щелкните по вкладке **Files** (Файлы).

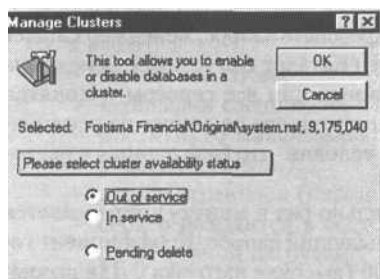


Рис. 20.1. Доступность базы данных

3. Выведите на экран каталог, найдите нужную базу данных и на панели **Results** (Результаты) выделите ее.
4. На панели **Tools** (Программные инструменты) отметьте **Cluster** (Кластер) или щелкните правой кнопкой мыши по значку базы данных и выберите **Cluster** из контекстного меню.
5. В диалоговом окне **Manage Clusters** (Управление кластерами) укажите необходимое состояние базы данных (см. рис. 20.1).

Помечая базу данных как **Out of service**, вы заставляете пользователей обращаться к ее реплике на другом сервере в кластере. Это можно делать, когда вы, например, выполняете текущее обслуживание базы. Пользователи, которые обратились к базе до того, как вы назначили ее необслуживаемой, продолжают работать с ней. Кроме того, база данных по-прежнему реплицируется.

Чтобы восстановить обслуживание базы, укажите **In service**.

Если вы определяете базу данных как **Pending delete**, она отмечается для удаления, но ожидает завершения последнего активного сеанса пользователя. База, предназначенная для удаления, прекращает принимать запросы, следовательно, они будут направляться на другие базы данных в кластере.

Менеджер кластеров

Cluster Manager (Менеджер кластеров) служит для контроля состояния, доступности и нагрузки остальных серверов в кластере. Когда Cluster Manager определяет, что запрос пользователя необходимо направить в другую реплику базы данных, он использует каталог Cluster Database Directory, чтобы определить, на каком сервере находится требуемая реплика исходной базы (с помощью идентификатора реплики) и затем направляет запрос в соответствующую реплику. Если существует несколько реплик базы данных, менеджер кластеров предполагает, что для их репликации применяется выборочная репликация. Cluster Manager пытается направить запрос в ту реплику базы данных, которая находится в том же каталоге, что и исходная база.

Domino Cluster Manager автоматически запускается на каждом сервере кластера. Фактически при добавлении в кластер сервера Cluster Manager автоматически стартует в момент запуска сервера. Затем он определяет в каталоге Domino, какие серверы принадлежат к данному кластеру, сохраняя эту информацию в памяти (Cluster Name Cache - кэш-память имени кластера). Полученной информацией сервер обменивается с другими менеджерами кластеров, связываясь с ними посредством обмена зондами. Сведения, принятые от других менеджеров Cluster Manager, также помещаются в Cluster Name Cache и служат


```

Lotus Domino Server: Superman/Definiti

Stats                Idle
Schedule Manager     Idle
Event Monitor         Idle
Calendar Connector    Idle
Admin Process         Idle
Agent Manager         Executive '1': Idle
Agent Manager         Idle
Indexer              Idle
Replicator            Idle
Router               Idle

> show cluster
Cluster Information
Cluster name: DefinitiCluster1, Server name: Superman/Definiti
Server cluster probe timeout: 1 minute(s)
Server cluster probe count: 279
Server availability threshold: 0
Server availability index: 100 (state: AVAILABLE)
Cluster members (4)...
  server: Superman/Definiti, availability index: 100
  server: Ferris/Definiti, availability: UNREACHABLE
  
```

Рис. 20.2. Информация Cluster Manager

для распределения нагрузки и защиты от сбоев. На рис. 20.2 приведен пример информации, контролируемой Cluster Manager. Ее можно просмотреть, введя на консоли сервера команду `show cluster`.

Cluster Manager выполняет следующие задачи:

- контроль каталога Domino для выяснения принадлежности серверов к данному кластеру, что определяется по содержимому поля **Cluster Name** (Имя кластера) в серверном документе и списке членов кластера;
- контроль текущей доступности серверов и контроль нагрузки;
- обмен информацией о доступности с другими менеджерами Cluster Manager;
- обеспечение защиты от сбоев за счет перенаправления запросов пользователей в другие реплики баз данных в кластере;
- реализация распределения нагрузки путем выравнивания нагрузки между серверами в кластере;
- регистрация событий защиты от сбоев и распределения нагрузки в журнале сервера.

Каталог баз данных кластера

Cluster Database Directory (CLDBDIR.NSF - каталог баз данных кластера) используется менеджером Cluster Manager для управления информацией о базах данных и их репликах в кластере (рис. 20.3).

Эта база имеется на каждом сервере в кластере (если ее еще нет, она автоматически создается задачей Cluster Database Directory Manager при запуске сервера) и применяется компонентами кластера, чтобы определить, куда направить запрос пользователя при защите от сбоев, как управлять доступом к базе данных, которая реплицируется, и где искать другие реплики базы. При добавлении базы данных на сервер задача Cluster Database Directory Manager создает для нее документ Notes, содержащий следующую информацию:

- имя базы данных;
- сервер;

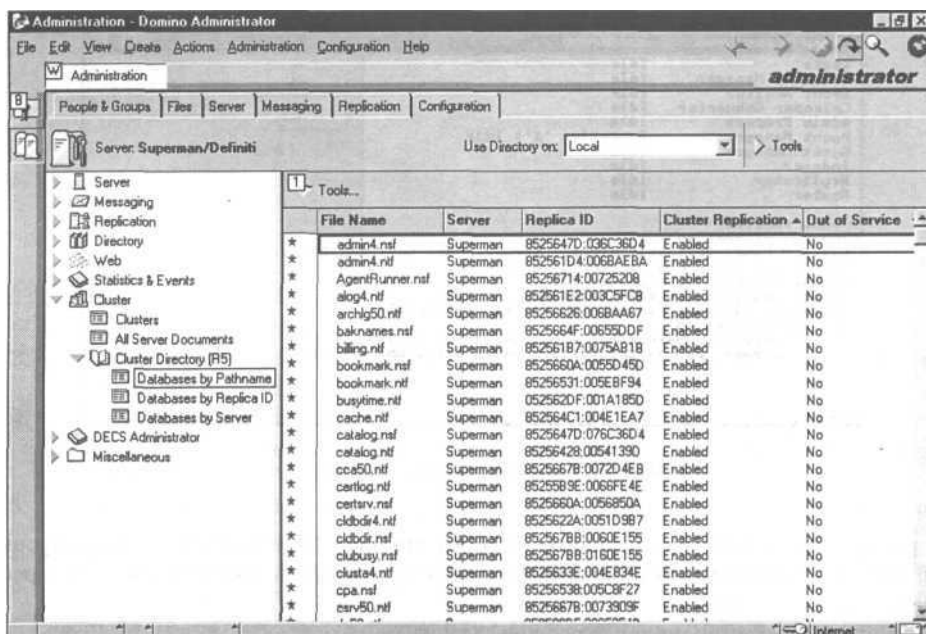


Рис. 20.3. База данных Cluster Directory

- О путь к файлу;
- О идентификатор реплики;
- О данные о репликации;
- О сведения о доступе.

Cluster Replicator (Репликатор кластера) обеспечивает немедленное распространение любых изменений в каталоге Cluster Database Directory между остальными каталогами Cluster Database Directory на других серверах кластера, гарантируя, что компоненты кластера всех серверов будут работать с одинаковыми данными.

Менеджер каталога баз данных кластера

III

Задача Cluster Database Directory Manager (CLDBDIR - менеджер каталога баз данных кластера) запускается на каждом сервере кластера. Она предназначена для поддержания корректного текущего состояния каталога баз данных кластера. Когда в кластер добавляется новый сервер, менеджер Cluster Database Directory Manager проверяет на нем наличие каталога Cluster Database Directory и, если не находит его, создает таковой. Когда на сервер добавляется база данных, Cluster Database Directory Manager формирует для нее документ в каталоге Cluster Database Directory, который содержит всю необходимую информацию, требуемую для компонентов кластера. Аналогично, если с сервера удаляется база данных, Cluster Database Directory Manager стирает соответствующий документ из каталога. И наконец, Cluster Database Directory Manager контролирует состояние баз данных сервера (смотрит, не помечена ли база как необслуживаемая или приготовленная для удаления).

«

Администратор кластеров

Cluster Administrator (Администратор кластеров) контролирует компоненты кластера и выполняет следующие функции:

- О при добавлении нового сервера в кластер запускает задачи Cluster Database Directory Manager и Cluster Replicator;
- О вносит задачи CLDBDIR и CLREPL в переменную ServerTasks файла notes.ini;
- О активизирует процесс Administration Process, если он еще не запущен;
- О когда из кластера удаляется сервер, задачи CLDBDIR и CLREPL останавливаются и вычищаются из переменной ServerTasks файла notes.ini, удаляется Cluster Database Directory (или обновляется на остальных серверах кластера).

Репликатор кластера

Задача Cluster Replicator (CLREPL - репликатор кластера) предназначена для синхронизации реплик баз данных в кластере, чтобы гарантировать просмотр пользователями одинаковой и согласованной информации. Когда изменяется одна из реплик базы данных в кластере, Cluster Replicator переносит эти изменения во все остальные реплики этой базы. Следовательно, репликатор Cluster Replicator скорее «запускается событием», чем «запускается по расписанию», как при стандартной репликации. Один экземпляр Cluster Replicator автоматически стартует для всех серверов кластера, однако с целью повышения производительности можно запустить несколько экземпляров.

Репликатор кластера использует каталог Cluster Database Directory, чтобы определить, какие базы данных имеют реплики на других серверах и какие из них необходимо реплицировать. Эта информация сохраняется в памяти и обновляется, когда меняется содержимое в каталоге Cluster Database Directory. Аналогично, если существуют невыполненные события репликации, они помещаются в очередь и хранятся там до момента, в который можно будет провести репликацию. Если в базе данных, ожидающей репликации, возникают дополнительные изменения, они добавляются к уже имеющимся и распространяются вместе со всеми остальными изменениями для повышения производительности. Если сервер назначения недоступен, событие репликации сохраняется в памяти до тех пор, пока сервер остается недоступным, а запись о повторе репликации вносится в журнал репликации.

Cluster Replicator выполняет репликацию баз данных только внутри кластера (методами «вытягивания» и «выталкивания») и игнорирует все формулы репликации и параметры, установленные на панели **Advanced** (Дополнительно) в диалоговом окне **Replication Settings** (Параметры репликации), поскольку реплицируются все документы. Кроме того, реплицируются все частные папки, но сохраняются параметры защиты. События репликации не регистрируются в журнале репликации, но записываются в память. Журнал репликации передается в базы данных приблизительно один раз в час.

Когда в кластер добавляется сервер, задача Cluster Replicator автоматически дописывается в переменную ServerTasks файла notes.ini. Несмотря на это, введите на консоли сервера следующую команду для запуска задачи Cluster Replicator:

```
>loadclrepl
```

Если репликатор кластера перегружен, можно запустить несколько задач на сервере. Они будут работать совместно, разделяя нагрузку репликации. Для включения нескольких Cluster Replicator добавьте необходимое количество записей clrepl в переменную ServerTasks файла notes.ini или несколько раз введите команду load clrepl на консоли сервера.

Стандартная репликация (с помощью задачи REPLICA) требуется для репликации баз данных вне кластера. Несмотря на то что в кластере работает Cluster Replicator, важно выполнять и стандартную репликацию на основе расписания, чтобы удостовериться, что базы данных постоянно обновляются. Следовательно, необходимо запланировать репликацию ежедневно или по крайней мере ежедневно.

Менеджер кластеров Internet

Более подробно Internet Cluster Manager (ICM) описывается в разделе о новых дополнительных службах версии R5/6.

Если сервер отказал...

Каждый раз после отказа сервера немедленно проведите репликацию внутри кластера!

Планирование, установка и настройка

Чтобы можно было работать с кластерами Domino, необходимо выполнить следующие условия:

- на всех серверах кластера должны функционировать Enterprise Server для версий 4.62-5.0 или Advanced Services для версий 4.5-4.6 (новые средства кластеризации, такие как ICM, в состоянии применять лишь серверы R5/6);
- каждый сервер может быть членом только одного кластера;
- все серверы обязаны соединяться по высокоскоростной локальной сети, поддерживать стек TCP/IP, использовать общий набор сетевых протоколов и быть членами одной сети Notes;
- все серверы нужно поместить в одном домене Domino, чтобы у них были одинаковые каталоги Domino;
- в домене, содержащем кластер, следует определить административный сервер. В противном случае процесс Administration Process (AdminP) не сможет менять управление кластером. Однако нельзя, чтобы административный сервер являлся членом кластера и был зарегистрирован как Enterprise Server;
- каждый сервер в кластере должен иметь иерархический идентификатор (следовательно, все прямые идентификаторы нужно преобразовать в иерархические);
- клиенты Notes должны быть клиентами Notes R4.5 или выше, чтобы они могли применять защиту от сбоев, а также поддерживать протоколы TCP/IP.

Кроме того, при настройке кластера проверьте следующее:

- серверы в кластере используют гораздо больше дискового пространства, чем отдельные серверы. В отличие от отдельных серверов, они обычно содержат больше реплик баз данных;
- серверы в кластере должны иметь больше оперативной памяти и более мощные процессоры.

При соблюдении этих условий для настройки кластера выполните такие действия:

- определите, нужна ли кластеризация и есть ли необходимые условия для создания кластера Domino;

- О задайте число серверов и то, какие именно серверы будут входить в кластер;
- О укажите, сколько реплик требуется создать для каждой конкретной базы данных и на каких серверах их расположить;
- О назначьте, каким образом распределить базы данных среди серверов кластера;
- О определите, нужно ли создавать для трафика кластера частную сеть;
- О сконфигурируйте кластер;
- О настройте плановую репликацию между серверами в кластере;
- О измените параметры и пороги кластера.

Ограничения кластера

Максимальное число серверов в кластере - шесть.

Если вы решили, что вашей организации необходимы кластеры, следующим шагом в планировании создания кластера является определение числа серверов. Кластер Domino может содержать от двух до шести серверов. Увеличение количества серверов в кластере повышает его способность распределять нагрузку, доступность и производительность. Однако дополнительные серверы следует устанавливать только в том случае, когда нужны производительность и избыточность. Дело в том, что увеличение числа серверов требует дискового пространства и может ухудшить производительность из-за большего числа обращений к процессору и более напряженного сетевого трафика.

При назначении числа серверов в кластере необходимо учитывать следующие факторы:

- О чем больше серверов и реплик баз данных, тем мощнее должны быть процессоры и тем больше понадобится дискового пространства;
- О каталог Cluster Database Directory (CLDBDIR.NSF) занимает примерно 2 Мб. Добавьте еще 1 Мб для каждых 2000 баз данных кластера;
- О с увеличением числа работающих на сервере задач возрастает необходимая для этого сервера мощность процессора;
- О чем больше на сервере запущено приложений, тем более мощный процессор ему требуется;
- О увеличение количества пользователей, обращающихся к серверу, повышает требования к мощности процессора и объему оперативной памяти. При задании объема ОЗУ исходите из значения 64 Мб плюс 1 Мб для каждых трех пользователей;
- О с ростом числа выполняемых на сервере задач репликатора кластера увеличивается объем нужной памяти. Для каждой задачи добавьте по 2 Мб оперативной памяти;
- О учитывая все вышеизложенное, необходимо оценивать не только текущие требования баз данных, но еще и те, которые будут предъявляться к серверу при направлении на него запроса пользователя с целью защиты от сбоев и для распределения нагрузки.

Следующим шагом после определения конфигурации серверов для кластера станет оценка числа реплик каждой базы данных в кластере. Вам не нужно создавать реплики всех баз на всех серверах кластера. Это будет неразумно и приведет к пустому расходованию ресурсов. Для некоторых баз вовсе не требуются реплики, следовательно, можно вообще удалить их из кластера. Для баз данных, которые должны иметь высокий коэффициент готовности или обрабатывают очень большую нагрузку, лучше сформировать реплики на каждом сервере (но не более трех).

Для баз, применяемых редко или содержащих данные, не нуждающиеся в столь высоком коэффициенте готовности, может оказаться всего одна реплика в кластере (если она вообще понадобится). Для определения числа реплик базы данных существует простой алгоритм - чем более высокие значения коэффициента готовности и нагрузки базы вам надо получить, тем больше реплик придется создать. Администраторы, как правило, знают, что базы данных Domino способны быстро заполнить дисковое пространство. Однако при низкой стоимости дисков доступность становится важнее затрат на их приобретение. Тем не менее при назначении числа реплик баз данных могут оказаться полезными следующие рекомендации:

- О размер базы данных - для больших баз лучше создавать меньшее число реплик;
- О количество и расположение потенциальных пользователей - при большом числе пользователей производительность, возможно, значительно повысится, если запросы будут распределяться среди нескольких реплик;
- О мощность сервера - сервер, установленный на самых современных компьютерах, в состоянии лучше обрабатывать дополнительные реплики баз данных;
- О пропускная способность - в случае возникновения проблем с пропускной способностью стоит ограничить репликацию;
- О использование баз данных - если с базами активно работают, то дополнительные реплики будут способствовать повышению производительности;
- О объемы данных - когда число документов и объем данных документа достаточно велики, создание многих реплик может ухудшить производительность. Необходимо оценить производительность сервера и конфигурацию сети, если есть сомнения по поводу пропускной способности.

При принятии решения о числе реплик баз данных следуйте здравому смыслу. Формирование более трех реплик приводит к огромной избыточности. Здесь применим закон «убывающего плодородия». Для большинства приложений вполне достаточно одной реплики. Однако для критически важной информации, которая должна быть доступна всегда, сделайте вторую или даже третью реплики. Дополнительные реплики иногда становятся лишними и чаще всего негативно влияют на ресурсы кластера.

Кроме того, лучше распределить самые загруженные базы данных между несколькими серверами. Если серверы имеют различную мощность, убедитесь, что поместили самые популярные базы данных на самые мощные серверы с максимальными объемами оперативной памяти. Располагайте загруженные базы данных на серверах с минимальным числом работающих задач, учитывая задачи Domino и задачи операционной системы. И снова здравый смысл подсказывает, что сервер, который использует ресурсы не на полную мощность, расходует их попусту, а перегруженный сервер отрицательно влияет на производительность.

Лучше всего начать с почтовых файлов Lotus Notes. Если вы вообще планируете вводить кластеры, для начала необходимо поместить в них почтовые файлы. Они очень быстро разрастаются и должны быть постоянно доступными для пользователей. Предприятие часто зависит именно от работы почты.

При настройке кластеризации для почтовых файлов необходимо распределить базы данных даже среди серверов в кластере. Имеет смысл специально назначить почтовый сервер. Поскольку это базы данных одного типа, гарантируется распределение нагрузки и в случае недоступности сервера. Однако для почтовых баз следует предусмотреть защиту

от сбоев, а не распределение нагрузки, поскольку только владелец почты получает доступ к соответствующей базе. Управлять всеми базами данных и их репликами позволяет каталог **Cluster Database Directory (CLDBDIR.NSF)**.

Настроив кластер для почтовых баз, добавьте в кластер базы данных приложений и сконцентрируйте внимание на защите от сбоев и распределении нагрузки. Для самых важных приложений сформируйте дополнительные реплики и поместите их на наиболее мощные серверы.

Создайте одну реплику для каждой базы данных в кластере. Затем проконтролируйте статистику кластера, чтобы определить потребность в дополнительных репликах. Не делайте реплики для баз данных, если для них защита от сбоев и распределение нагрузки не являются основными вопросами, - это только уменьшит эффективность кластера.

Производительность кластера может значительно увеличиться при построении внутри кластера частной сети. Установите сетевую карту в каждый сервер и соедините серверы с помощью отдельного концентратора или переключателя. Дополнительный трафик, возникающий за счет репликации в кластере и передачи данных между узлами сети, нередко приводит к заторам в основной сети. Создание частной сети внутри кластера снимает вопрос дополнительного трафика. Полезно также построить частную сеть внутри кластера вдобавок к соединению серверов посредством общей локальной сети - это гарантирует связь между серверами даже в случае разрыва сегмента сети. Более подробно процедура формирования частной сети для кластера описана в справочной базе данных Domino Administrative Help.

Чтобы мобильные пользователи могли почувствовать преимущества кластеров, им следует соединяться с кластером через сквозной сервер, который занимается направлением запроса на доступный сервер кластера. В противном случае пользователю придется по очереди обращаться к каждому из серверов кластера, а кластеризация при этом применяться не будет (если только для каждой реплики базы данных на каждом сервере в кластере на странице репликации пользователя не создано несколько элементов репликатора).

Если ваша организация использует службу Server Web Navigator, то каждая база данных Web на каждом сервере кластера должна быть репликой всех остальных. Следовательно, перед запуском Server Web Navigator на всех серверах кластера необходимо сформировать реплики основной базы данных Web (Web.nsf)- Иначе на каждом сервере будет создана новая база данных Web, а поскольку они не будут репликами друг друга, не удастся обеспечить защиту от сбоев.

Администрирование

В следующих разделах описано, как создать кластер, добавить в него сервер и удалить сервер из кластера. Подробно рассмотрены операции, необходимые для выполнения всех указанных действий. Кроме того, проанализировано влияние этих действий на серверы в кластере.

Создание кластеров

Чтобы добиться наилучших результатов, необходимо использовать при формировании кластера административный сервер. Требуется уровень доступа минимум **Author** с правом **Delete Documents** (Удаление документов) для каталога Domino и доступ **Author** к базе данных Administration Requests (Административные запросы) - рис. 20.4.

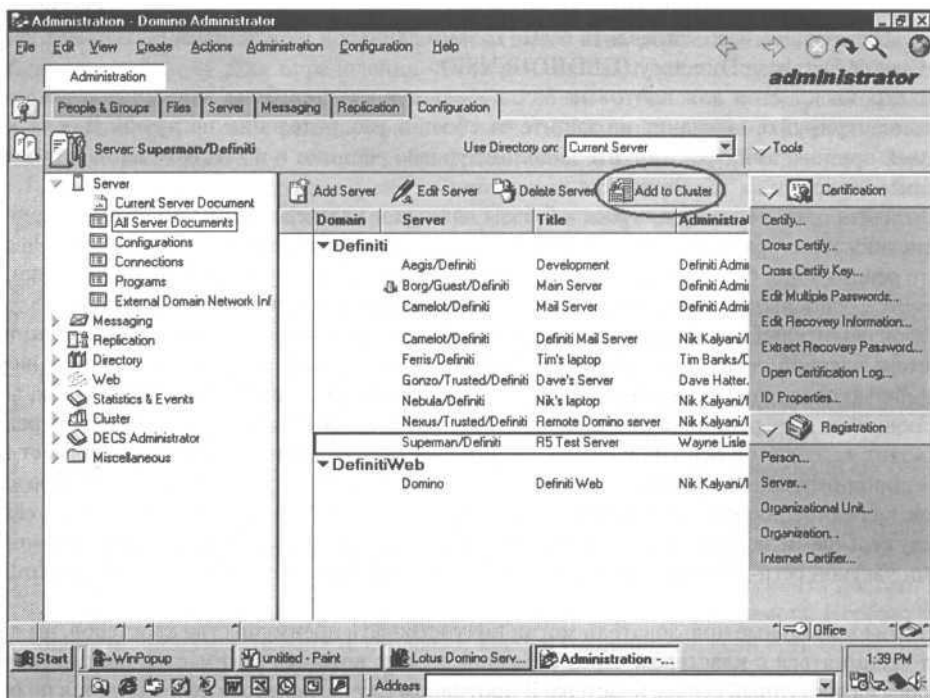


Рис. 20.4. Создание кластера

Чтобы создать кластер:

1. Откройте в программе Domino Administrator существующий сервер Domino.
2. Щелкните по вкладке **Configuration**.
3. Выведите на экран раздел **Server** и щелкните по **All Server Documents** (Все серверные документы).
4. На панели **Results** выберите серверы, которые надо включить в кластер.
5. Нажмите на **Add to Cluster** (Добавить в кластер).
6. В окне подтверждения щелкните по **Yes**.
7. Укажите операцию **Choose New Cluster** (Выбрать новый кластер), а не операцию добавления серверов в существующий кластер.
8. Введите имя нового кластера.
9. Укажите **Yes**, чтобы добавить серверы в кластер немедленно, или **No**, чтобы передать запрос в процесс Administration Process. При задании **Yes** процесс выполняется быстрее, но возможен конфликт репликации. Сервер, который является частью кластера, сразу начинает процесс репликации с другими серверами кластера. В противном случае приходится реплицировать изменения на один из серверов кластера. Когда указывается **No**, в процесс Administration Process отправляется запрос на добавление серверов в кластер. Этот процесс запускается немедленно и вносит имя кластера во все серверные документы. После этого изменение распространяется среди остальных серверов кластера. Если вы не применяете административный сервер,

запустите репликацию между текущим и административным серверами, а затем между административным сервером и остальными серверами кластера.

Результатом создания нового кластера является то, что на каждом его сервере выполняются следующие действия:

- О запускаются задачи Cluster Administrator и Cluster Manager;
- О Cluster Administrator добавляет в переменную ServerTasks файла notes.ini задачи Cluster Database Directory Manager (CLDBDIR) и Cluster Replicator (CLREPL);
- О Cluster Administrator запускает Cluster Database Directory Manager;
- О Cluster Administrator активизирует Cluster Replicator;
- О стартует процесс Administration Process;
- О Cluster Database Directory Manager изменяет базу данных Cluster Database Directory, чтобы включить в нее документы для каждой базы данных сервера;
- О репликатор распространяет изменения в каталоге Cluster Database Directory и каталоге Domino среди остальных серверов кластера;
- О серверы кластера начинают обмениваться зондами, содержащими информацию о состоянии сервера.

Добавление серверов в кластер

Для получения наилучших результатов при добавлении сервера в кластер следует воспользоваться административным сервером. Нужен уровень доступа минимум **Author** с правом **Delete Documents** к каталогу Domino и доступ **Author** к базе данных Administration Requests (Административные запросы).

Чтобы добавить сервер в кластер:

1. Откройте в Domino Administrator существующий сервер Domino.
2. Щелкните по вкладке **Configuration**.
3. Выведите на экран раздел **Server** и щелкните по **All Server Documents** (Все серверные документы).
4. На панели **Results** выберите сервер, который будет добавлен в кластер.
5. Щелкните по **Add to Cluster** (Добавить в кластер).
6. В окне подтверждения щелкните по Yes.
7. Укажите имя кластера, в который надо добавить новый сервер (рис. 20.5).
8. Выберите Yes, чтобы добавить сервер в кластер немедленно, или No, чтобы передать запрос в процесс Administration Process. #

Если задать Yes, то процесс выполняется быстрее, но возможен конфликт репликации. Сервер, являющийся частью кластера, сразу начинает процесс репликации с другими серверами кластера, иначе приходится реплицировать изменения на один из серверов кластера.

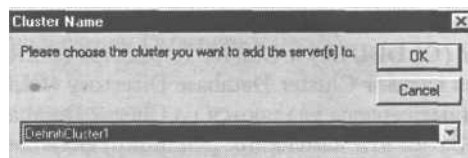


Рис. 20.5. Добавление серверов в кластер

При выборе No в процесс Administration Process отправляется запрос на добавление сервера в кластер. Запустите репликацию между административным сервером и остальными серверами кластера.

В результате добавления нового сервера на каждом сервере кластера выполняются следующие действия:

- О запускаются задачи Cluster Administrator и Cluster Manager;
- О Cluster Administrator помещает в переменную ServerTasks файла notes.ini задачи Cluster Database Directory Manager (CLDBDIR) и Cluster Replicator (CLREPL);
- О Cluster Administrator запускает Cluster Database Directory Manager;
- О Cluster Administrator активизирует Cluster Replicator;
- О стартует Administration Process;
- О Cluster Database Directory Manager создает базу данных Cluster Database Directory (CLDBDIR.NSF);
- О Cluster Database Directory Manager вносит в Cluster Database Directory документ для каждой базы данных нового сервера кластера;
- О репликатор распространяет изменения в каталоге Cluster Database Directory и каталоге Domino среди остальных серверов кластера;
- О добавленный сервер начинает обмениваться с другими серверами зондами, содержащими информацию о состоянии сервера.

Для перемещения сервера из одного кластера в другой добавьте его в новый кластер. Каталог Domino автоматически удалит его из предыдущего кластера.

Удаление серверов из кластера

Лучше всего удалять сервер из кластера с помощью административного сервера. Требуется уровень доступа минимум **Author** с правом **Delete Documents** к каталогу Domino и доступ **Author** к базе данных Administration Requests.

Чтобы удалить сервер из кластера:

1. Откройте в Domino Administrator существующий сервер Domino.
2. Щелкните по вкладке **Configuration**.
3. Выведите на экран раздел **Cluster** и щелкните по **Clusters**.
4. На панели **Results** выберите документ, представляющий удаляемый сервер.
5. Щелкните по **Remove from Cluster** (Удалить из кластера) - рис. 20.6.
6. Выберите **Yes**, чтобы удалить сервер немедленно, или No, чтобы передать запрос на удаление в процесс Administration Process.

После удаления сервера в каждом сервере кластера выполняются следующие действия:

- О запускается процесс Cluster Administration Process;
- О задача Cluster Replicator останавливается;
- О прекращает работу менеджер Cluster Database Directory Manager;
- О из переменной ServerTasks файла notes.ini удаляются задачи Cluster Database Directory Manager (CLDBDIR) и Cluster Replicator (CLREPL);
- О с сервера удаляется каталог Cluster Database Directory (CLDBDIR.NSF);
- О документы баз данных сервера удаляются из Cluster Database Directory доступного сервера кластера. Затем эти изменения реплицируются между всеми остальными серверами кластера.

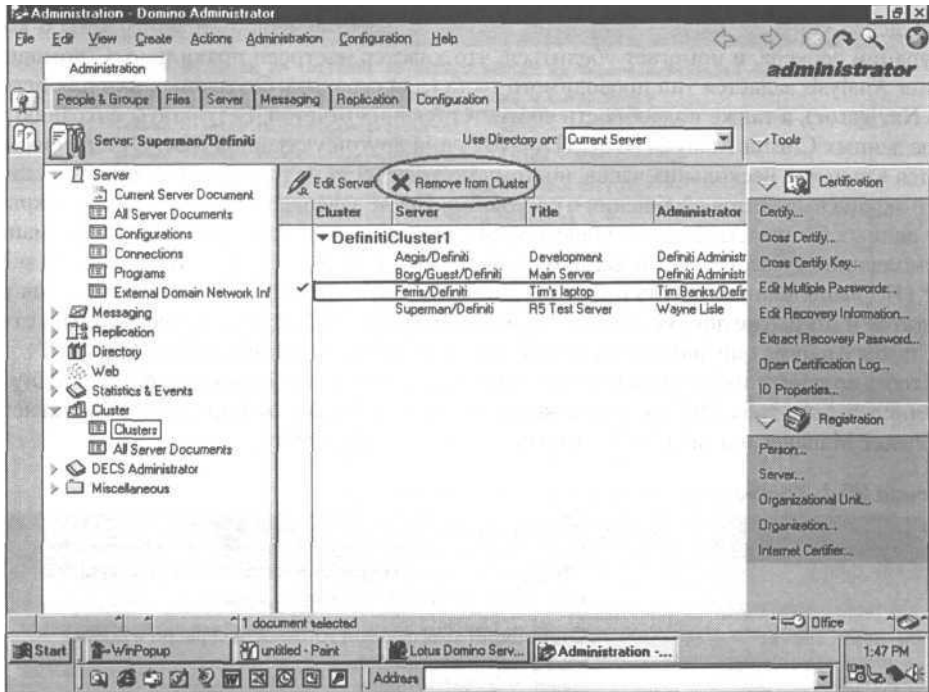


Рис. 20.6. Удаление серверов из кластера

Не выключайте сервер, пока процесс Cluster Administration Process не завершит свою работу. Если все же система отключается или блокируется, введите на консоли сервера команду CLADMIN, чтобы заново запустить Cluster Administrator.

Использование кластеров

После завершения установки и настройки кластера проконтролируйте эффективность защиты от сбоев и распределения нагрузки, репликацию и производительность сервера. Возможно, вам понадобится изменить некоторые параметры и пороги доступности, добавить или удалить реплики баз данных, переместить базы на другой сервер или добавить/удалить сервер кластера.

Статистика

Кластер анализируется по четырем категориям:

- отчет Cluster Analysis;*
- статистика Cluster Manager;
- статистика Cluster Replicator;
- статистика Internet Cluster Manager.

Средство Cluster Analysis генерирует отчеты, предоставляющие информацию о конфигурации сервера, и помогает убедиться, что кластер настроен правильно. С помощью Cluster Analysis задается тип проводимого теста (для серверов, баз данных или для Server Web Navigator), а также подробности соответствующих отчетов. Результаты сохраняются в базе данных Cluster Analysis (CLUSTA4.NSF) или другой указанной базе. Отчеты формируются в течение нескольких часов, поэтому по ходу теста на панели состояния в нижней части экрана выводятся сообщения о состоянии. После завершения отчета можно открыть базу данных Cluster Analysis и ознакомиться с результатами. Для просмотра информации по умолчанию существует три вида: **By Cluster** (По кластерам), **By Date** (По дате) и **By Test** (По выполненному тесту). Эти виды обеспечивают удобный поиск документов результатов и открытие документа для изучения подробностей отчета. Более детально отчеты Cluster Analysis описаны в справочной системе Domino Administration Help.

Чтобы получить информацию о кластере, его членах и их состоянии, введите одну из перечисленных в табл. 20.1 команд на консоли сервера. В табл. 20.2 представлена статистика Cluster Manager, а в табл. 20.3 - статистика Cluster Replicator.

Таблица 20.1. Команды просмотра информации о кластере

Команда	Информация
show cluster	Отображает имена серверов кластера, соответствующие коэффициенты готовности и число зондов
show stat server	Отображает коэффициент готовности сервера и порог коэффициента готовности
show stat server,cluster.*	Отображает остальную статистику, представленную на рис. 20.7

Таблица 20.2. Статистика Cluster Manager

Параметр	Описание
Server.Cluster.PortName	Порт по умолчанию для сетевого трафика кластера (если вместо порта по умолчанию нужно использовать любой доступный порт, введите звездочку)
Server.AvailabilityIndex	Целое число от 0 до 100, характеризующее доступность сервера (0 - нет доступных ресурсов, 100 - все ресурсы сервера доступны)
• Server.AvailabilityThershold	Текущий порог коэффициента готовности сервера
Server.Cluster.OpenRedirects.Failover.Successfull	Количество успешных перенаправлений сервером клиентов на другой сервер кластера после того, как Web-клиент не смог открыть базу данных по идентификатору реплики
Server.Cluster.OpenRedirects.Failover.Unsuccessfull	Количество неудачных перенаправлений сервером клиентов на другой сервер кластера после того, как Web-клиент не смог открыть базу данных по идентификатору реплики
Server.Cluster.OpenRedirects.FailoverByPath.Successfully	Количество успешных перенаправлений сервером клиентов на другой сервер кластера после того, как Web-клиент не смог открыть базу данных по пути к файлу
Server.Cluster.OpenRedirects.FailoverByPath.Unsuccessfull	Количество неудачных перенаправлений сервером клиентов на другой сервер кластера после того, как Web-клиент не ёмог открыть базу данных по пути к файлу

```

07/28/98 03:02:58 PM ATTEMPT TO ACCESS SERVER by Superman/Definiti was denied
> show stat server.cluster.*
Server.Cluster.Member.Aegis/Definiti.Index = UNREACHABLE
Server.Cluster.Member.Borg/Guest/Definiti.Index = INVALID
Server.Cluster.Member.Camelot/Definiti.Index = INVALID
Server.Cluster.Member.Ferris/Definiti.Index = UNREACHABLE
Server.Cluster.Member.Superman/Definiti.Index = UNREACHABLE
Server.Cluster.Name = DefinitiCluster1
Server.Cluster.OpenRedirects.FailoverByPath.Successful = 0
Server.Cluster.OpenRedirects.FailoverByPath.Unsuccessful = 0
Server.Cluster.OpenRedirects.Failover.Successful = 0
Server.Cluster.OpenRedirects.Failover.Unsuccessful = 0
Server.Cluster.OpenRedirects.LoadBalanceByPath.Successful = 0
Server.Cluster.OpenRedirects.LoadBalanceByPath.Unsuccessful = 0
Server.Cluster.OpenRedirects.LoadBalance.Successful = 0
Server.Cluster.OpenRedirects.LoadBalance.Unsuccessful = 0
Server.Cluster.OpenRequest.ClusterBusy = 0
Server.Cluster.OpenRequest.DatabaseOutOfService = 0
Server.Cluster.OpenRequest.LoadBalanced = 0
Server.Cluster.PortName = *
Server.Cluster.ProbeCount = 287
Server.Cluster.ProbeError = 0
Server.Cluster.ProbeTimeout(mins) = 1
>
  
```

Рис.20.7. Статистика ClusterManager

Таблица 20.2. Статистика Cluster Manager (окончание)

Параметр	Описание
Server.Cluster.OpenRedirects. LoadBalance.Successfull	Количество успешных перенаправлений сервером клиентов на другой сервер кластера после того, как Web-клиент не смог открыть базу данных по идентификатору реплики, когда сервер был занят
Server.Cluster.OpenRedirects. LoadBalance.Unsuccessfull	Количество неудачных перенаправлений сервером клиентов на другой сервер кластера после того, как Web-клиент не смог открыть базу данных по идентификатору реплики, когда сервер был занят
Server.Cluster.OpenRedirects. LoadBalanceByPath.Successfull	Количество успешных перенаправлений сервером клиентов на другой сервер кластера после того, как Web-клиент не смог открыть базу данных по пути к файлу, когда сервер был занят
Server.Cluster.OpenRedirects. LoadBalanceByPath. Unsuccessfull	Количество неудачных перенаправлений сервером клиентов на другой сервер кластера после того, как Web-клиент не смог открыть базу данных по пути к файлу, когда сервер был занят
Server.Cluster.OpenRequest. ClusterBusy	Общее число запросов клиентов, когда все серверы заняты
Server.Cluster. DatabaseOutOfService	Общее число попыток открытия базы данных, которая помечена как необслуживаемая
Server.Cluster.LoadBalanced	Общее число попыток открытия базы данных, когда сервер занят
Server.Cluster.ProbeCount	Общее число зондов, которыми сервер обменивался с другими серверами кластера
Server.Cluster.ProbeError	Общее число возникших ошибок при обмене зондами
Server.Cluster. ProbeTimeout (mins)	Интервал обмена межкластерными зондами. Его*можно просмотреть с помощью команды show stat

Таблица 20.3. Статистика Cluster Replicator

Параметр	Описание
Replica.Cluster.Servers	Общее число серверов, получающих реплики от текущего сервера
Replica.Cluster.Suiccessful	Общее число успешных операций репликации с момента запуска сервера
Replica.Cluster.Failed	Общее число неудачных операций репликации с момента запуска сервера
Replica.Cluster.Docs.Added	Общее число документов, добавленных репликатором кластера
Replica.Cluster.Docs.Updated	Общее число документов, обновленных репликатором кластера
Replica.Cluster.Docs.Deleted	Общее число документов, удаленных репликатором кластера
Replica.Cluster.Files.Local	Общее число баз данных на текущем сервере, для которых существуют реплики на других серверах кластера
Replica.Cluster.Remote	Общее число баз данных на других серверах, в которые репликатор распространяет изменения
Replica.Cluster.Retry.Skipped	Общее число пропущенных попыток репликатора распространить изменения в базе данных (если сервер назначения недоступен)
Replica.Cluster.Retry.Waiting	Общее число копий, которые ожидают повтора попытки репликации
Replica.Cluster.SecondsOnQueue	Общее время (в секундах), которое база данных провела в очереди в ожидании репликации
Replica.Cluster.SecondsOnQueue.Avg	Среднее время (в секундах), которое база данных проводит в очереди в ожидании репликации
Replica.Cluster.SecondsOnQueue.Max	Максимальное время (в секундах), которое база данных проводит в очереди в ожидании репликации
Replica.Cluster.SessionBytes.In	Общее число байтов, принятых при репликации
Replica.Cluster.SessionBytes.Out	Общее число байтов, отправленных при репликации
Replica.Cluster.WorkQueueDepth	Общее число баз данных, ожидающих распространения репликатором кластера
Replica.Cluster.WorkQueueDepth.Avg	Среднее число баз данных, ожидающих распространения репликатором кластера
Replica.Cluster.WorkQueueDepth.Max	Максимальное число баз данных, ожидающих распространения репликатором кластера

Для просмотра информации об отдельных членах кластера в программе Domino Administrator выполните следующие действия:

1. Откройте в Domino Administrator существующий сервер Domino.
2. На панели Server выберите необходимый сервер.

3. Щелкните по вкладке **Server**.
4. Перейдите на вкладку **Statistics**.
5. В списке **All Statistics** (Вся статистика) выберите **Server**, чтобы просмотреть коэффициент готовности и значения порогов. Для отображения остальной информации о кластере укажите **Server => Cluster** (Сервер => Кластер) - рис. 20.8.

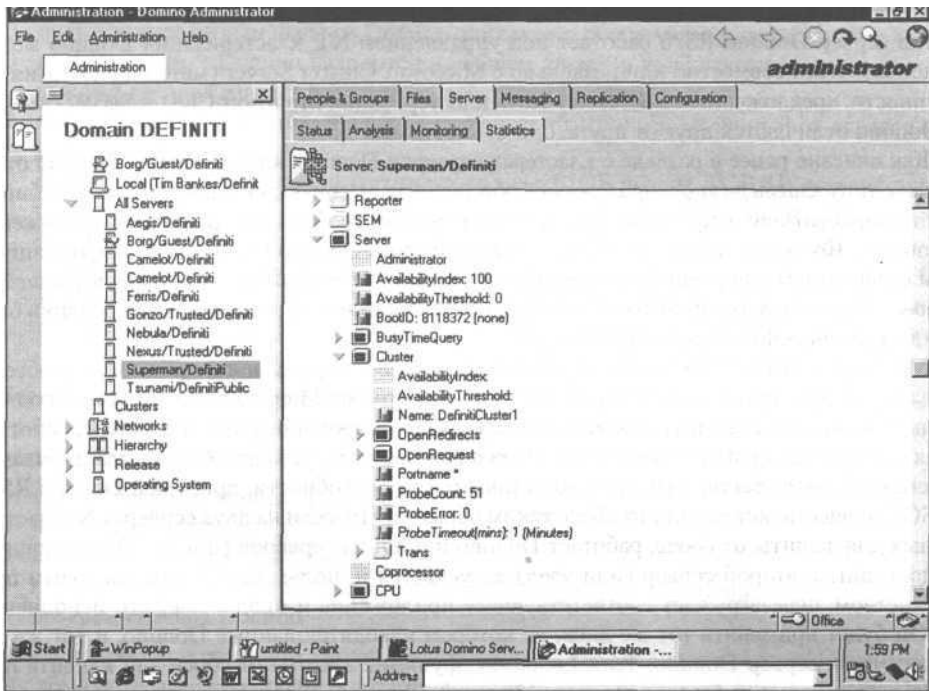


Рис. 20.8. Статистика о членах кластера

Другой способ:

1. Щелкните правой кнопкой мыши по нужному серверу на панели **Server** и выберите в контекстном меню пункт **Properties** (Свойства). Ф
2. Щелкните по вкладке **Cluster** в диалоговом окне **Server Properties**.

Если на сервере Domino работает задача Statistic Collector, то статистика Cluster Manager сохраняется в базе данных Statistics Reporting (STATREP.NSF). Откройте вид **Clusters** в этой базе данных, чтобы просмотреть статистическую информацию о кластере. Кроме того, можно просматривать события в журнале Notes на виде **Miscellaneous Events**.

Вместо того чтобы ждать, пока репликатор Cluster Replicator создаст отчетный документ, можно самостоятельно сформировать его с помощью команды

```
> telldrepl log
```

Чтобы включить регистрацию событий репликации в кластере, измените в файле notes.ini параметр `RTR_logging=1`. Для отмены регистрации событий репликации в кластере установите для этого параметра значение 0.

Сведения о статистике менеджера Internet Cluster Manager вы найдете в разделе о новых дополнительных службах R5/6. Более подробная информация о кластерах, потенциальных проблемах и сообщениях об ошибке имеется в справочной базе данных Domino Administration Help или по адресу <http://www.notes.net>.

Использование Microsoft Cluster Server

Когда сервер Domino R5/6 работает под управлением NT, кластеризация Domino может использоваться совместно или раздельно с Microsoft Cluster Server (метод повышения доступности, предложенный Microsoft). Хотя кластеризация Microsoft Cluster Server (MSCS) и Domino отличаются друг от друга, они совместимы.

Как описано ранее в разделе о кластерах серверов Domino, кластеризация Domino относится к типу *кластеризации приложений*, обеспечивая высокую доступность и масштабируемость корпоративных приложений в домене передачи сообщений, групповых приложений и Internet. Функции защиты от сбоев и кластеризации Domino основаны на информационном содержимом (запрашиваемом пользователем) и часто называются *маршрутизацией на основе содержимого* (content-based routing), причем применяются параметры и реплики базы данных, устанавливаемые пользователем.

Microsoft Cluster Server использует *кластеризацию операционной системы*, что обеспечивает высокую степень доступности. На данный момент Microsoft Cluster Server поддерживает аппаратную защиту от сбоев для двух NT-серверов или узлов в кластере, работающих с общим дисковым накопителем. Важно иметь в виду, что способность кластеризации Microsoft Cluster Server значительно отличается от способности, присущей Domino R5/6. MSCS осуществляет защиту от сбоев таким образом, что, если на двух серверах NT, настроенных для защиты от сбоев, работает Domino и один из серверов (или узлов) становится недоступным, второй сервер (или узел) запускается и, пользуясь общим дисковым пространством, перезагружает соответствующее приложение и продолжает его исполнение.

Он будет применять тот же диск, на котором находятся данные Domino, и тот же IP-адрес, что и сервер Domino. Таким образом, функция защиты от сбоев для клиента прозрачна. В отличие от Domino, кластер Microsoft Cluster Server гарантирует только защиту от сбоев и не поддерживает добавления узлов кластера с целью наращивания и распределения нагрузки.

Организация может внедрить Microsoft Cluster Server в конфигурации Active/Passive (Активный/Пассивный) или Active/Active (Активный/Активный).

В конфигурации Active/Passive в один момент времени запросы пользователя обрабатывает только один узел. Пассивный узел находится в резерве на случай отказа активного узла. Каталог Domino установлен на обоих узлах, чтобы пассивный узел смог обратиться к нему при отказе активного. Однако они все же работают с общими данными Domino, поэтому каталоги данных и файлы должны находиться на общем диске.

В режиме Active/Active запросы пользователя обрабатывают оба узла. Когда один узел отказывает, второй продолжает действовать, обслуживая пользователей обоих узлов. На них могут работать два сервера Domino - по одному на узел. Следовательно, необходимо установить по два секционированных сервера на каждый узел. Но они применяют общие данные Domino, поэтому каталоги данных и файлы следует размещать на общем диске.

Для запуска Domino на сервере Microsoft Cluster Server должны быть выполнены следующие условия:

- О поддерживается только Domino R4.6.2 или более поздние версии;
- О виртуальные серверы Domino (средство Web-сервера Domino) не поддерживаются MSCS;
- О при выборе конфигурации Active/Active серверы Domino настраиваются как секционированные серверы;
- О программные файлы Domino хранятся на локальном, не используемом совместно диске для каждого узла в кластере MSCS;
- О путь к программным файлам Domino одинаков в обоих узлах кластера;
- О каталог данных Domino находится на общем диске (в конфигурации Active/Active каждый каталог данных помещен на собственном диске);
- О каждому серверу Domino присвоен статический IP-адрес, отличный от адресов узлов кластера;
- О если сервер Domino использует протокол NetBIOS поверх TCP/IP, сетевой адрес сервера отличается от сетевого имени обоих узлов кластера (в качестве сетевого адреса обычно служит имя сервера Domino);
- О ID-файл сервера не имеет пароля, иначе перезагрузка сервера и защита от сбоев будут невозможны, поскольку сервер Domino станет ожидать ввода пароля перед началом работы. При создании идентификатора сервера установите длину пароля равную нулю.

Перед завершением настройки конфигурации MSCS необходимо создать следующие ресурсы/группы (записи не являются иерархическими и должны точно соответствовать тем типам ресурсов и приложений, которым они принадлежат):

- О группа ресурсов сервера Domino;
- О ресурсы IP-адресов;
- О имена ресурсов сетевых имен;
- О назначение ресурсов физического диска группе ресурсов Domino;
- О ресурсы сервера Domino.

Более подробно о создании группы ресурсов MSCS и установке сетевого имени как имени компьютера можно прочесть в справочной базе данных Domino Administrative Help.

Установка сервера Domino на Microsoft Cluster Server состоит из трех этапов:

1. Установка Domino на первом узле.
2. Установка Domino на втором узле.
3. Настройка серверов Domino.

Установка Domino на первом узле

При создании конфигурации Active/Passive требуется только один сервер Domino, а для конфигурации Active/Active необходимы два секционированных сервера Domino (каталог программ Domino формируется на отдельном диске каждого узла, а каталог данных располагается на общем диске).

Для установки Domino на первом узле:

1. С помощью MSCS Cluster Administrator переместите группы, содержащие общие диски, которые будут использоваться каталогами данных Domino в первом узле.
2. Запустите программу установки Domino Server, в окне приглашения щелкните по **Next**, примите условия лицензионного соглашения и введите регистрационную информацию.

3. Для конфигурации Active/Active выберите **Partitioned Server Installation** (Установка секционированного сервера) и задайте другой общий диск для каталога данных Domino второй секции.
4. Укажите папку для каталога программ как частную, не используемую совместно (рис. 20.9).

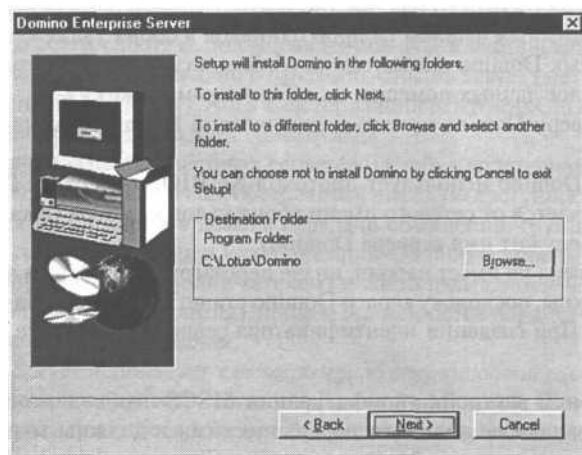


Рис. 20.9. Установка Domino на первом узле

5. Задайте **Customize** при назначении типа сервера Domino и разрешите работу сервера Domino как службы NT (этот режим можно изменить после установки).
6. Укажите папку для каталога данных Domino как одну из общих папок кластера.
7. Определите программную папку, в которую следует добавить новую конфигурацию.
8. Завершите работу с программой установки.
9. Если вы не настроили Domino как секционированный сервер, переместите notes.ini из каталога программ в каталог данных сервера. Вам, возможно, придется изменить ссылки на Domino Server и Domino Administrator, добавив пробел, знак равенства и путь в файл notes.ini (например, c:\notes\data = c:\notes\data\notes.ini).

Установка Domino на втором узле

Выполните те же действия, что и при установке Domino на первом узле. Укажите тот же каталог для программных файлов и каталог данных.

Настройка серверов Domino

Настройте серверы Domino:

1. Откройте в Domino Administrator существующий сервер Domino.
2. Щелкните по вкладке **Configuration**.
3. Если это не первый сервер в домене, зарегистрируйте его, выполнив **Registration => Server** (Регистрация => Сервер) на панели **Tools**. Имя сервера должно совпадать

с сетевым именем, указанным в MSCS. Установите длину пароля равную нулю, чтобы при запуске сервера пароль не требовался (рис. 20.10).

4. На втором узле кластера запустите сервер Domino, который загрузит программу конфигурации.
5. Настройте конфигурацию Domino (для сервера должны быть настроены протоколы TCP/IP или NetBIOS поверх TCP/IP).
6. Перезагрузите Domino. Это приведет к запуску сервера.
7. Для конфигурации Active/Active укажите, что сервер применяет IP-адреса, установленные для него.
8. Повторите шаги 1-7 для второго секционированного сервера.

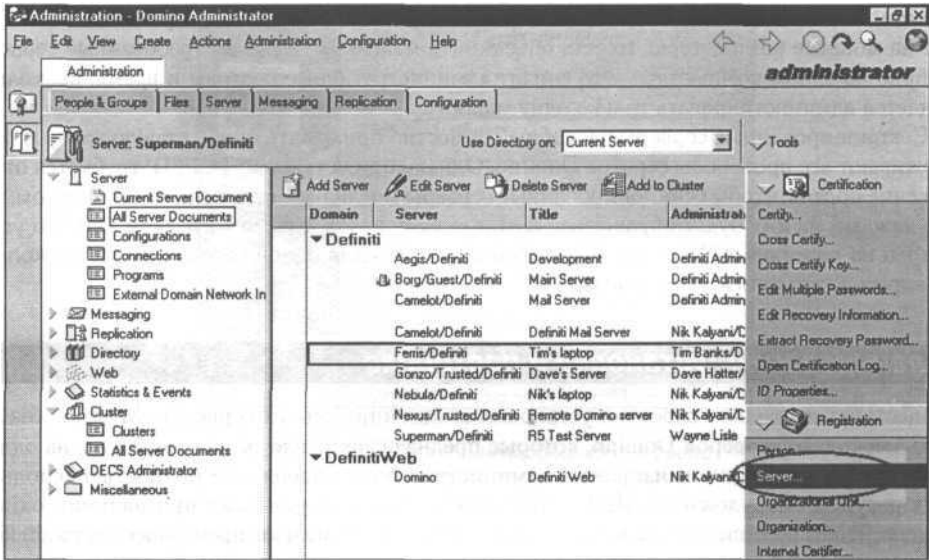


Рис. 20.10. Настройка сервера Domino

Теперь серверы Domino готовы к работе с MSCS. В Cluster Administrator щелкните правой кнопкой мыши по группе серверов Domino и выберите **Bring Online** (Включить). Можно остановить Domino с помощью Cluster Administrator. Для этого щелкните правой кнопкой мыши по группе серверов Domino и отметьте **Take Offline** (Выключить). Когда сервер Domino работает совместно с MSCS, клиенты Notes должны быть настроены для использования TCP/IP или NetBIOS поверх TCP/IP.

Сегменты сервера Domino

, Последующие разделы посвящены сегментам сервера Domino. В разделе о планировании, установке и настройке рассматривается подготовка и конфигурирование секционированных серверов. Описывается несколько конфигураций, таких как серверы с одним IP-адресом, серверы с уникальным IP-адресом, а также установка и удаление секционированных

серверов как служб Windows NT. Кроме того, в разделе об использовании секционированных серверов в кластере Domino обсуждается работа таких серверов и методы их обслуживания, контроля и удаления.

Описание

Сегменты сервера Domino позволяют нескольким серверам Domino работать на одном компьютере, а также максимизировать потребление ресурсов, минимизировать стоимость и в то же время обеспечивать надежный, высокопроизводительный доступ к службам Domino. Поскольку каждый секционированный сервер функционирует в своем сегменте памяти, при отказе одного из серверов все остальные продолжают работать, что повышает надежность. Можно максимально задействовать аппаратные средства, перенеся программное обеспечение на мощные компьютеры, то есть объединить маленькие мало востребованные серверы Domino на одном компьютере. Это снизит административные расходы и время, поскольку придется администрировать только одну машину.

Секционированные серверы способны совместно применять одну сетевую карту и поддерживают все протоколы сервера Domino. Однако при установке TCP/IP требуется отображение портов, чтобы секционированные серверы могли работать с одним IP-адресом, так что каждый из них будет обращаться к отдельному порту. Кроме того, если Domino установлен на платформе Windows NT, можно назначить для одной сетевой карты несколько IP-адресов (это описано чуть позже).

Планирование, установка и настройка

Существует несколько способов установки секционированных серверов. Можно объединить несколько серверов Domino, которые предназначены для разных доменов, на одном компьютере, чтобы минимизировать административные издержки и полностью использовать ресурсы оборудования. Или создать несколько серверов даже при наличии одного домена, чтобы повысить производительность. Ниже перечислены преимущества такой конфигурации:

- О лучшее распределение нагрузки, поскольку базы данных разнесены по нескольким серверам;
- О более удачное распределение процесса, работающего со всеми базами данных;
- О задачи Domino удастся разделить между несколькими серверами;
- О более эффективная обработка запросов к серверу Domino (особенно если сервер является симметричной многопроцессорной машиной);
- О возможность обслуживания большего числа параллельных задач/запросов;
- О меньшие размеры списков доставки почты и видов mailbox.

Установка секционированного сервера похожа на установку отдельного сервера. Фактически секционированные серверы применяют одни и те же программные файлы и каталоги. Однако каждый из них располагает собственным каталогом данных. Хотя такой вариант экономит дисковое пространство, появляются дополнительные требования к ресурсам системы. Несколько серверов обращаются к ресурсам одного компьютера, так что, когда на

одном сервере работает задача, сильно расходуя ресурсы, это отрицательно влияет на производительность остальных серверов. Очень важно при планировании задач для сервера и времени их выполнения учитывать задачи и время их работы на других секционированных серверах, а также их влияние на производительность остальных серверов.

Для установки сервера Domino:

1. Запустите программу установки Domino Server, в окне приглашения щелкните по **Next**, примите лицензионные соглашения и введите регистрационную информацию.
2. Поставьте флажок **Partitioned Server Installation** (Установка секционированного сервера) - рис. 20.11.

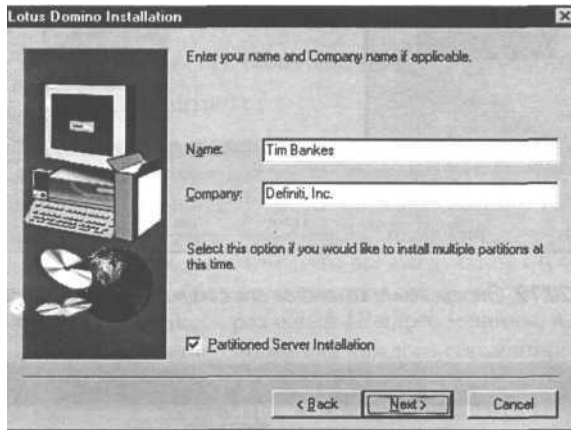


Рис. 20.11. Установка секционированного сервера

3. Укажите каталог, в котором будут храниться программные файлы, используемые всеми серверами.
4. Определите устанавливаемые компоненты при выборочной установке.
5. Задайте каталог данных для каждого секционированного сервера (рис. 20.12). Поскольку каждый сервер имеет собственный каталог данных, достаточно ввести описательное имя для каталогов (например, имя сервера), которое напоминает, какому серверу принадлежит каталог. Если вы не присваиваете конкретные имена, то по умолчанию первый каталог данных будет называться \notes\data, а к имени всех последующих добавится счетчик (\notes\data2 и т.д.). Каждый каталог данных для любого сегмента будет содержать все необходимые шаблоны, исполняемые файлы, файл notes.ini и т.д.
Имейте в виду, что переадресация виртуальных каталогов данных на другие каталоги или серверы осуществляется и с помощью файлов каталога Directory (.dir) в файловой системе, однако это может противоречить цели создания сегментов.
6. Выберите папки программ, в которые необходимо добавить новую конфигурацию.
7. Завершите процесс установки.

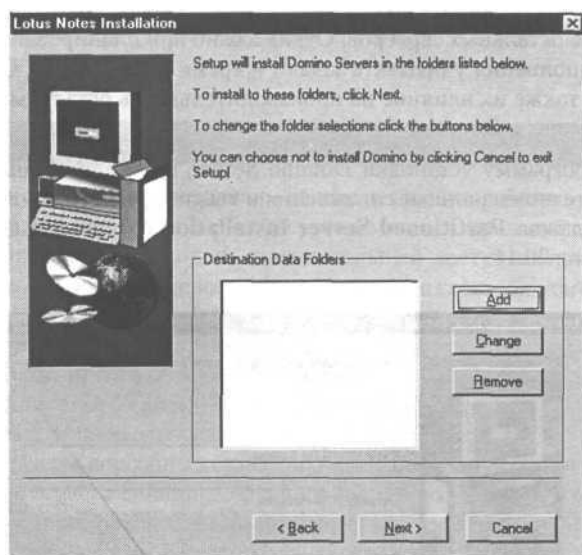


Рис. 20. 12. Определение каталогов для секционированных серверов

Настройка

Секционированные серверы, поддерживающие TCP/IP, можно настроить двумя способами:

- с одним IP-адресом;
- с уникальными IP-адресами.

Настройка серверов с одним IP-адресом

Один из способов настройки секционированных серверов заключается в том, что всем серверам присваивается один IP-адрес и затем настраивается отображение портов, чтобы каждый сервер обращался к своему порту. Все серверы в таком случае включены в одну сеть IP. При настройке отображения портов один сервер назначается в качестве сервера отображения портов, направляющего запросы HTTP и Notes на другие серверы, что будет происходить всякий раз при открытии клиентом нового сеанса с сервером. Хотя при ограниченном числе IP-адресов это удобно, недостаток заключается в том, что, когда сервер отображения портов становится недоступным, клиент не в состоянии установить соединение с другим сервером.

Можно назначить сегмент для обработки отображения портов и удалить все ненужные серверные задачи. Кроме того, все секционированные серверы должны находиться в одной сети IP. Даже на компьютере с достаточно мощным процессором и большим объемом оперативной памяти может возникнуть нехватка ресурсов из-за того, что все серверы пользуются одной сетевой картой, и, следовательно, производительность ухудшится.

Чтобы изменить отображение портов, отредактируйте файл notes.ini на сервере (если вы изменяете notes.ini, обязательно перезагрузите машину, тогда новые параметры вступят в силу). Файл notes.ini содержит имена серверов, IP-адреса и номера портов для каждого секционированного сервера. Сервер отображения портов по умолчанию использует порт

TCP 1352. Можно посмотреть зарегистрированные номера портов в файле SERVICES, который обычно находится в каталоге \WINNT\SYSTEM32\DRIVERS\ETC. В этом файле указаны номера портов, которые нельзя применять. Lotus рекомендует для дополнительных секционированных портов назначать порты от 13520 до 13524.

В файл notes.ini сервера отображения портов необходимо добавить следующие строки:

```
TCPIPTcpAddress=O, IPAddress:1352
TCPIP PortMapping00=CN=ServerName1/0=Org, IPAddress : 13520
TCPIP PortMapping01=CN=ServerName1/0=Org, IPAddress:13521
TCPIP PortMapping02=CN=ServerName1/0=Org, IPAddress: 13522
TCPIP PortMapping03=CN=ServerName1/0=Org, IPAddress:13523
TCPIP PortMapping04=CN=ServerName1/0=Org, IPAddress = 13524
```

В файл notes.ini всех остальных секционированных серверов нужно дописать строку

```
TCPIPTcpAddress=O, IPAddress:port
```

Префикс TCPIP - это имя порта, определенное в строке Port= файла notes.ini. Если имя порта изменено или настроено для нескольких портов TCP/IP, надо соответствующим образом изменить значение. Значения, указанные за переменной PortMapping, должны быть выстроены в восходящем порядке - от 00 и до 04. Любой пробел в последовательности или ошибка нумерации приведут к тому, что все следующие строки будут игнорироваться. Переменные ServerNameX и Org представляют собой действительное каноническое имя сервера, переменная IPAddress - реальный IP-адрес машины, а последнее значение в каждой строке - назначенный номер порта для каждого секционированного сервера.

При работе в среде Windows NT допускается указывать несколько IP-адресов для одной физической сетевой карты. Следовательно, можно распределить IP-адреса между всеми серверами и не прибегать к отображению портов при переадресации, а просто установить несколько сетевых карт и присвоить каждой один IP-адрес.

При работе со службами Internet (HTTP, POP3, NNTP, LDAP и ШАР) на секционированных серверах требуется выполнить некоторые дополнительные действия. Поскольку вы применяете отображение портов, в разделе HTTP Server серверного документа обязательно указывать значение имени хоста. Сервер будет работать с именем, заданным в сетевых параметрах операционной системы (Windows NT). Для каждой службы должен быть назначен уникальный порт TCP. Отредактируйте серверный документ, изменив разделы **Internet Port** и **Security Configuration** для всех секционированных серверов и установив уникальный номер порта для каждого сервера. Поскольку любой сервер Internet обращается к собственному порту, клиенту следует точно указывать номер порта в запросе (например, <http://fer'ris.definiti.com:8080/home.nsf>).

Настройка серверов с уникальными IP-адресами

Можно настроить серверы, присвоив уникальные IP-адреса каждому секционированному серверу и используя отдельные сетевые карты для каждого сервера. Можно обойтись одной сетевой картой, но при этом возникает риск снижения производительности. Если вы располагаете достаточным количеством IP-адресов, вариант с отдельными картами - наилучший. Поскольку у любого сервера имеется своя сетевая карта, пропускная способность увеличивается. Клиент получает доступ к серверу без транзита через сервер отображения портов, то есть вероятность доступа увеличивается (степень доступности выше). Еще одно достоинство отдельных IP-адресов состоит в том, что серверы могут находиться в разных сетях.

Для присвоения IP-адреса секционированным серверам добавьте в файл notes.ini следующую строку (чтобы изменения вступили в силу, после редактирования notes.ini обязательно перезагрузите компьютер):

ТСRIPТСrAddress=О,IpAddress:port

Префикс ТСРIP - имя порта, указанное в строке Port= в файле notes.ini. Если имя порта изменено или настроено для нескольких портов ТСР/IP, надо соответствующим образом изменить значение. Переменная ipAddress представляет собой реальный IP-адрес компьютера, а последнее значение в каждой строке - назначенный номер порта для каждого секционированного сервера. Оно должно быть установлено в 0, чтобы работать с портом Domino по умолчанию (1352). Если задать другое значение, пользователи не смогут соединиться с сервером.

При работе со службами Internet (HTTP, POP3, NNTP, LDAP и ШАР) на секционированных серверах требуется выполнить некоторые дополнительные действия. Поскольку вы присвоили уникальный IP-адрес каждому серверу, следует «привязать» имя хоста к серверу HTTP. Если этого не сделать, все серверы HTTP будут пытаться воспользоваться одним и тем же именем хоста, что вызовет конфликты. Отредактируйте файл notes.ini, изменив значение **Host Name** в разделе **HTTP Server** серверного документа.

Для настройки других служб Internet измените файл notes.ini каждого секционированного сервера. В табл. 20.4 представлены требуемые значения для всех служб.

Таблица 20.4. Изменения, необходимые для подключения дополнительных служб Internet

Служба	Параметр в файле notes.ini
Сервер POP3	POP3Address=имя_хосТа
Сервер IMAP	IMAPAddress=имя_хосТа
Сервер NNTP	NNTPAddress=имя_хосТа
СерверLDAP	LDAPAddress=имя_хосТа ; . . . , -

Запуск секционированных серверов как служб Windows NT

Установка серверов Domino как служб Windows NT имеет ряд преимуществ. С помощью инструментов Windows NT можно производить удаленное отключение и перезагрузку сервера Domino, а если перезагружается сервер NT (в результате сбоя питания или перезагрузки системы), то сервер Domino перезагрузится без подключения к NT. Нужен административный доступ к серверу Windows NT Server, на котором работает сервер Domino.

Одновременно с сервером Domino в апплете **Службы** (Services) панели управления устанавливается только служба Windows NT. При этом пользователь должен войти в систему и вручную запустить дополнительные секционированные серверы или выполнить командный файл. При отказе системы автоматически будет запускаться только один секционированный сервер! Для решения проблемы можно установить новые службы вручную с помощью NT Resource Kit:

1. Запустите из командной строки NT Resource Kit (файл ntreskit).
2. Чтобы добавить службу Windows NT для первого секционированного сервера Domino, введите следующую команду:

```
instsrv "DominoServer ServerName" c:\notes\nSERVICE.EXE
```


(Вместо ServerName укажите имя сервера, куда добавляется служба Windows NT, C: - это диск, на котором находятся программные файлы Domino, а notes\nSERVICE.EXE - путь в файл nSERVICE.) Добавьте службы Windows NT для всех остальных серверов, указывая соответствующее значение ServerName для каждого сервера.

3. Запустите редактор реестра Windows NT. Откройте папку для текущего сервера Domino:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DominoServer
ServerName

Добавьте полный путь в параметр ImagePath файла notes.ini и число экземпляров Domino в конец команды. Например:

C:\notes\nService.EXEc:\notes\MyServer\notes.ini2

Повторите эти действия для всех остальных служб.

4. Откройте панель управления и запустите апплет **Службы**.
5. Выберите службу установки для первого сервера Domino.
6. Щелкните по кнопке **Startup** (Запуск). В окне служб установите **Startup Type** (Тип запуска) в значение **Automatic** (Автоматический). Автоматический запуск Domino означает, что Domino будет стартовать при запуске Windows NT. Установите флажок для разрешения взаимодействия службы с Рабочим столом операционной системы, иначе консоль сервера Domino не сможет запускаться.

Удаление Domino как службы Windows NT

Можно удалить Domino как службу Windows NT, открыв командную строку, указав путь к каталогу Domino и выполнив команду ntsvinst -d.

Использование секционированных серверов в кластере Domino

Чтобы воспользоваться преимуществами кластеризации, включите секционированный сервер в кластер. Можно создать кластер секционированного сервера с отдельным сервером или с другими компьютерами, но не следует запускать секционированные серверы на том же компьютере в том же кластере (это одна из причин сбоев, противоречащая самой сути кластеризации). Аналогично при настройке отображения портов не включайте более одного сервера отображения портов кластера. Если вы вводите секционированный сервер в кластер, вы не должны помещать в него остальные секционированные серверы на том же компьютере. Не назначайте также более одного сервера отображения портов в кластере: возникает угроза, что все секционированные серверы окажутся недоступными, даже если они не входят в кластер сервера отображения портов.

Следовательно, если вы установили секционированные серверы и хотите использовать преимущества кластеризации (доступность, надежность и масштабируемость), необходимо включать в кластер все или некоторые из секционированных серверов с другим компьютером, на котором также работают секционированные серверы.

Техническое обслуживание и мониторинг

Техническое обслуживание и мониторинг секционированных серверов выполняются так же, как и для отдельного сервера. Поскольку создание нескольких секционированных

серверов на одном компьютере требует дополнительных системных ресурсов, важно с помощью Системного монитора соответствующим образом управлять ресурсами. Хотя каждый секционированный сервер имеет собственный каталог данных, он все же работает с системными ресурсами совместно с другими серверами (или мешает остальным).

В случае необходимости повысить производительность системы:

1. Измените значение переменной `Server_Max_Concurrent_trans` в файле `notes.ini` и установите максимальное число одновременных транзакций. Для NT оптимальное число одновременных транзакций равно примерно 20 (см. рис. 20.12). Если в системе работает два секционированных сервера, задайте для каждого значение 10. Укажите это значение в зависимости от числа секционированных серверов (чтобы параметры вступили в силу, после модификации `notes.ini` перезагрузите компьютер).
2. Измените значение переменной `Server_MaxUsers` в файле `notes.ini`, чтобы ограничить число пользователей, одновременно работающих с сервером. При достижении порогового значения все остальные запросы будут отклоняться (рис. 20.13). Параметры вступают в силу, если после изменения `notes.ini` перезагрузить компьютер.
3. В случае, когда один из секционированных серверов расходует значительную часть ресурсов, можно переместить сервер на другую платформу или обновить аппаратную конфигурацию текущей системы. При замедлении доступа к диску перенесите каталоги данных Domino на другой диск.

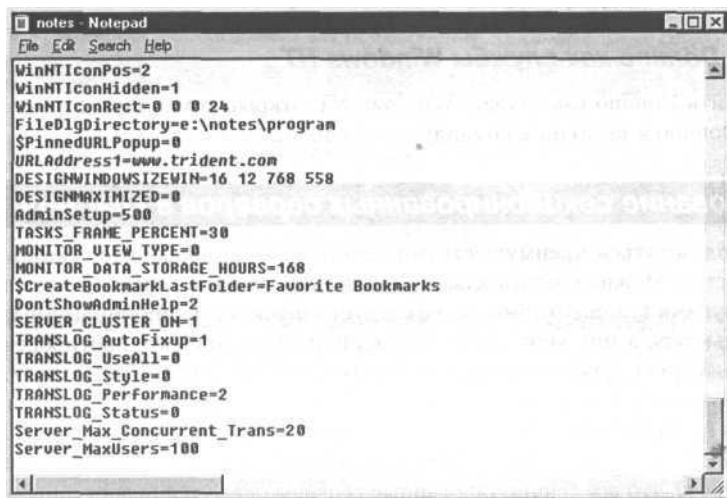


Рис. 20.13. Изменения в файле `notes.ini` для повышения производительности

4. Просмотрите журнал сервера Domino (`log.nsf`). Это поможет определить «узкие места» системы, требующие усовершенствования.
5. Проконтролируйте статистику каждого сервера и определите, какой из секционированных серверов потребляет больше всего ресурсов. Если один из серверов расходует ресурсы и влияет на производительность, это отражается и на других серверах, поэтому необходимо сравнить статистику по всем серверам.

Каждый секционированный сервер имеет собственный клиент Domino Administration. Однако при работе под управлением Windows NT одновременно может работать только один такой клиент. Под управлением UNIX допустимо запускать несколько клиентов администрирования. Если возникнут трудности с настройкой секционированных серверов и появятся ошибки, воспользуйтесь представленными в табл. 20.5 рекомендациями для устранения некоторых общих проблем.

Таблица 20.5. Проблемы, возникающие в серверах Domino

Ошибка	Потенциальная проблема
Server Not Responding (Сервер не отвечает)	- О Не работает сервер отображения портов; - О запрашиваемый сервер использует сетевую карту совместно с сервером отображения портов; - О неверно указаны параметры отображения портов в файле notes.ini: они либо ссылаются на другой секционированный сервер, либо перечислены не по порядку (чтобы изменения вступили в силу, после редактирования файла notes.ini необходимо перезагрузить компьютер) Проверьте файл notes.ini на сервере отображения портов. Убедитесь, что номера портов для IP-адреса каждого сервера соответствуют номерам портов, указанным в файле notes.ini секционированных серверов. Удостоверьтесь, что имена серверов и организаций заданы верно
Server's Name Changed (Имя сервера изменено)	Неверно указаны параметры отображения портов в файле notes.ini. Они могут ссылаться на другие секционированные серверы (чтобы изменения вступили в силу, после редактирования файла notes.ini необходимо перезагрузить компьютер)
NOTESPARTITION="x In Use (Используется NOTESPARTITION=x)	Вы пытаетесь запустить более одного сервера Domino в одном пространстве имен. Отредактируйте файл nserve.bat и убедитесь, что каждый командный файл использует уникальное значение переменной NOTESPARTITION

Удаление

Однажды вы можете решить, что необходимости в применении секционированных серверов больше нет. Следовательно, вы захотите удалить один или несколько серверов. На данный момент допустимо так поступить только с последним установленным секционированным сервером или со всеми вместе. Процесс удаления всех секционированных серверов аналогичен удалению программного обеспечения и похож на удаление несекционированного сервера.

Разрешается также удалить последний установленный секционированный сервер (вам не удастся выбрать, какой сегмент удалить):

1. Удалите каталог данных Domino для последнего сервера.
2. Если сервер имел уникальный IP-адрес, отключите этот адрес, а если секционированный сервер использовал в качестве имени сервера имя хоста, не отключайте IP-адрес. Это можно сделать только в том случае, если IP-адрес был добавлен при установке секционированного сервера.

3. Удаляя сервер отображения портов, назначьте другой сервер отображения портов. Если сервер применялся при отображении портов, измените файл notes.ini на сервере отображения портов, чтобы он более не ссылался на удаленный сервер.
4. При работе под управлением Windows NT внесите следующие изменения в реестр с помощью редактора реестра:
 - в ключе HKEY_LOCAL_MACHINE\SOFTWARE\Lotus\Notes\VSERVER выберите INSTANCE и уменьшите значение на единицу;
 - в ключе HKEY_LOCAL_MACHINE\SOFTWARE\Lotus\Notes\VSERVER\CLIENTn удалите запись для пути установки клиента (п) для удаленного секционированного сервера;
 - в ключе HKEY_LOCAL_MACHINE\SOFTWARE\Lotus\Notes\VSERVER\CLIENT убедитесь, что значения для клиентов (CLIENTn) перечислены последовательно.
5. Обновите файлы nclient.bat и nserve.bat в каталогах данных. Эти файлы определяют число экземпляров клиента и сервера. Ниже приведен пример:

```
SetNOTESPARTITION=1
start c:\notes\notes.exe=d:\notes\data1\notes.ini
```

У этих файлов не может быть разных значений для одного секционированного сервера, а у секционированных серверов на одном компьютере - общего значения NOTESPARTITION (см. рис. 20.4).

Счета и аудит

В следующих разделах рассматривается, как работают службы выписки счетов (Billing) и аудита (Auditing), как спланировать и установить эти службы и как функционирует база данных BILLING.NSF.

Описание

Информация о счетах может служить для обобщения сведений об активности в вашей организации при начислении пользователям платы за применение сервера Domino. Такая информация позволяет:

- О пользователям оплачивать создаваемую ими нагрузку;
- О контролировать тенденции использования;
- О проводить планирование ресурсов;
- О определить, поможет ли кластеризация повысить эффективность применения ресурсов и производительность системы.

Всего существует семь классов информации о счетах. Тип собираемых сведений указывается в файле notes.ini. Эти классы отслеживают такие данные:

- О **Agent** (Агент) - применяют ли пользователи и серверы агентов, а также время работы агентов;
- О **Database** (База данных) - факт и время работы серверов и пользователей с базами данных;

- О **Document** (Документ) - операции чтения/записи для указанных документов;
- О **HTTPRequest** (HTTP-запрос) - запросы Web-сервера;
- О **Mail** (Почта) - время, когда маршрутизатор передает сообщения другому серверу Domino;
- О **Replication** (Репликация) - момент, в который контрольный сервер начинает репликацию с другим сервером или клиентом;
- О **Session** (Сеанс) - начало и конец сеансов пользователей и серверов с контролируемым сервером, а также выполнение других функции создания и редактирования данных.

Планирование и установка

Чтобы включить начисление счетов:

1. Измените файл notes.ini и добавьте задачу Billing в переменную ServerTasks.
2. В файл notes.ini добавьте строку

```
BillingClass=listofclassestotrack
```

Вместо listofclassestotrack можно указывать Agent, Database, Document, HTTP-Request, Mail, Replication и Session.

3. Добавьте в файл notes.ini такую строку, чтобы указать место хранения информации о счетах:

```
BillingAddinOutput=n
```

Параметр п имеет следующие значения:

- 1 - сохранять записи в базы данных Domino;
- 2 - отображать значения на консоли сервера;
- 8 - сохранять записи в двоичном файле;
- 9 - сохранять записи и в базе данных Domino, и в двоичном файле.

Использование счетов

Сервер Domino собирает информацию о деятельности клиентов и серверов и помещает ее в очередь сообщений о счетах. Задача Billing периодически выбирает эту информацию из очереди, чтобы переместить ее в базу данных или в двоичный файл. Если выгопределите запись сведений в базу данных Domino, то система автоматически создаст базу Billing (BILLING.NSF). После этого задача Billing переместит документы из очереди сообщений о счетах в базу данных. Если вы зададите запись в двоичный файл, Domino автоматически сформирует файл BILLING.NBF. Задача Billing записывает информацию о счетах в файл BILLING.NBF в потоковом формате. Каждая запись начинается с описания длины и типа структуры, так что внешняя программа может проанализировать данные, хранящиеся в этом файле. Затем можно написать программу, которая будет с помощью имеющейся информации формировать финансовые отчеты (например, API-программу Domino или стороннюю программу обработки информации).

Новые улучшенные службы R5/6

Следующие разделы посвящены новым улучшенным средствам и службам версий R5 и R6.

Менеджер кластеров Internet

Одной из самых полезных задач, представленных в Domino R5/6, является ICM (Internet Cluster Manager - менеджер кластеров Internet). Мы подробно рассмотрим ICM - принцип работы, методы обслуживания и типы контролируемой информации.

Описание

Как отмечалось ранее в данной главе, в Domino R5/6 можно применять кластеры и распределять нагрузку для Web-клиентов с помощью задачи ICM (поддерживает протоколы HTTP и HTTPS). До версии R5 высокая доступность с помощью защиты от сбоев и распределение нагрузки не осуществлялись для Web-клиентов и Web-приложений. Задача ICM работает как промежуточная среда между Web-клиентом и Web-сервером и выполняет следующие функции:

- О контролирует доступность серверов Domino в кластере Domino;
- О хранит информацию о распределении баз данных на серверах внутри кластера;
- О управляет доступностью служб HTTP сервера Domino;
- О отменяет соединения с серверами, которые в данный момент не обслуживаются;
- О предоставляет соединение клиента с наиболее подходящим сервером, обеспечивая защиту от сбоев;
- О распределяет нагрузку среди серверов кластера (на основе установленных порогов);
- О поддерживает виртуальную IP-адресацию и отображение портов;
- О осуществляет маршрутизацию клиентов по информационному содержанию;
- О поддерживает шифрование и дешифрацию SSL;
- О поддерживает существующие модели защиты Domino.

ICM не требует дополнительного программного или аппаратного обеспечения, поскольку поставляется в версии Enterprise сервера Domino. Эта служба также поддерживается всеми ОС, с которыми работает сервер Domino. Соединение между клиентом и ICM должно использовать стек TCP/IP, а между ICM и сервером Domino в кластере может применяться любой протокол, совместимый с Domino. ICM управляет только запросами HTTP и HTTPS. Следовательно, если на сервере необходимо включить кластеризацию и распределение нагрузки для протоколов FTP, SMTP или UDP, приходится обращаться к сторонним программным продуктам. Издержки при работе ICM минимальны, а выгода может быть значительной.

Как работает ICM

Клиент HTTP посылает запрос Web-серверу Domino в кластере. Сервер читает серверный документ, определяет имя хоста для ICM и генерирует адрес URL, относящийся к ICM.

ICM поддерживает следующий список URL (команд HTTP):

- О вызов серверов, баз данных, видов, навигаторов, форм и агентов;
- О открытие, редактирование и удаление документов по идентификатору UNID, а также вывод на экран документов по имени из вида;

- О открытие файлов изображений, вложений и объектов OLE;
- О создание очередей поиска.

Получив запрос, служба ICM определяет, какие серверы находятся в кластере, пользуясь информацией из каталога Cluster Database Directory. Затем эта служба находит наиболее подходящий сервер, содержащий запрашиваемую базу данных, выясняет, для какого протокола (HTTP или HTTPS) настроен сервер и направляет запрос на соответствующий сервер.

При переадресации клиента служба ICM выполняет несколько действий:

1. Определяет, где располагаются реплики базы данных.
2. Устанавливает, не помечена ли база данных как необслуживаемая или подготовленная к удалению.
3. Проверяет коэффициент готовности всех серверов, содержащих реплики базы данных.
4. Контролирует доступность сервера, отправляя запрос PING на порт HTTP/HTTPS.
5. Исключает все серверы, которые недоступны, помечены как **RESTRICTED**, **BUSY** или **MAXUSERS**.
6. Если остается несколько серверов, то ICM выбирает сервер с минимальной текущей нагрузкой.
7. Если не осталось серверов, то ICM выбирает один из доступных серверов, помеченных как **RESTRICTED**, **BUSY** или **MAXUSERS**.

ICM не поддерживает защиту Domino и не участвует в процессе аутентификации, а просто переадресует запросы HTTP на уровне протоколов, отправляет обратно клиенту код ответа о переадресации и код сервера. Сеанс с ICM закрывается, после чего клиент HTTP направляет запрос нужному серверу. На этом этапе выполняются все операции, свойственные системе защиты Domino. С началом процесса аутентификации клиент должен аутентифицироваться (если только не разрешен доступ анонимным пользователям). После аутентификации идентификатор пользователя и пароль будут переданы вместе с заголовком для всех последующих запросов в пределах сеанса с тем же сервером. Информация о состоянии клиента сохраняется, поскольку все следующие запросы обращаются к тому же серверу. Если текущая Web-страница содержит ссылки на другие базы данных на том же сервере или на другом сервере в пределах кластера, Web-сервер Domino включит имя хоста службы ICM в адрес URL для базы данных. Таким образом, клиент все еще будет использовать ICM, чтобы получить доступ ко всем базам данных в пределах кластера.

Все названные этапы клиент может проследить по адресу URL. Имя хоста, путь и база данных будут меняться в зависимости от того, куда переадресовывается запрос клиента. ICM не защищает от неавторизованных пользователей, поэтому будет разумно обеспечить безопасность на самом верхнем уровне защиты Domino, например установить брандмауэр. Служба ICM поддерживает протокол SSL, который можно настроить так, чтобы формировались сеансы SSL.

ICM поддерживает информацию о доступности и состоянии серверов внутри кластера, отправляя зонды всем Web-серверам Domino в кластере.

Существует несколько ситуаций, когда ICM работает не так, как обычно:

- О когда адрес URL содержит путь к файлу, у службы ICM могут возникнуть сложности при разрешении URL для базы данных, если несколько серверов хранят нужные базы в одинаковых каталогах с таким же именем файла, но с различными идентификаторами реплик. В этом случае ICM выводит список баз данных и Web-клиент должен самостоятельно выбрать нужную;

- О когда адрес URL содержит идентификатор реплики, у службы ICM могут возникнуть сложности при разрешении URL для базы данных, если на сервере находится несколько реплик базы. Тогда ICM переадресует запрос клиента на сервер, содержащий хотя бы одну реплику базы данных, а Web-сервер Domino выберет предоставляемую реплику. Можно задать конкретную реплику базы данных, указав путь к ней в адресе URL;
- О когда адрес URL содержит значение элемента NotesID, ICM может не найти документ Notes и не сумеет обработать запрос. Это происходит из-за того, что каждая реплика базы данных имеет различные идентификаторы NotesID. Следовательно, при генерации URL следует удалить из него NotesID. Лучше обратиться к UNID, поскольку для всех реплик базы применяется одинаковый идентификатор UNID.

При работе службы ICM защита от сбоев и доступность не совсем надежна. Когда клиент HTTP переадресовывается на другой сервер, а сервер отказывает, клиент HTTP может превысить значение тайм-аута и Web-клиенту будет отправлено сообщение Server not Responding (Сервер не отвечает). Пользователь должен вернуться на предыдущую страницу, заново ввести URL или обновить страницу. На этом этапе ICM определит, что сервер не обслуживается, и направит запрос на другой доступный сервер. Однако клиенту, скорее всего, придется аутентифицироваться (в зависимости от параметров доступа для сервера и базы данных), если только он уже не аутентифицировался сервером во время предыдущего сеанса. Когда браузер и сервер поддерживают SSL3, аутентификация выполняется автоматически.

Настройка ЮМ

Каждому кластеру следует иметь выделенную службу ICM, работающую на сервере Domino. Поскольку ICM пользуется локальным каталогом Domino, эта служба должна находиться в том же домене, что и кластер Domino.

Процесс принятия решений при настройке ICM похож на процесс планирования исходного кластера. Необходимо учитывать несколько факторов, а именно:

- О число включаемых в кластер серверов;
- О мощность процессоров и объемы дисков серверов;
- О ожидаемый трафик и нагрузку серверов;
- О число реплик каждой базы данных и их размещение на серверах;
- О наличие выделенной частной сети для кластера;
- О место размещения и запуска службы ICM.

Решая, где расположить службу ICM, обратите внимание на следующее:

- О ICM может работать вне кластера на выделенном сервере, на котором должно функционировать минимальное число задач и который должен содержать минимально необходимое количество баз данных. Поскольку сервер выполняет только минимальное число задач и обслуживает ICM, надежность и производительность повышается. Когда ICM работает вне кластера, можно применять средства кластеризации операционной системы;
- О дальнейшее увеличение доступности достигается установкой нескольких служб ICM для обработки запросов HTTP вне кластера. Когда один ICM станет недоступным,

остальные будут обрабатывать запросы. Это можно сделать, запустив несколько служб ICM на машине с секционированными серверами или одну ICM на нескольких серверных компьютерах. При работе нескольких служб ICM они должны быть настроены на использование одного имени хоста, которое указано в качестве имени сервера домена (Domain Name Server). Следовательно, защита от сбоев будет прозрачна для пользователей. Это может повысить производительность в случае, когда одна служба ICM не в состоянии справиться с нагрузкой. Однако обычно несколько служб ICM не увеличивают производительности;

- О можно установить одну службу ICM для обработки запросов HTTP внутри кластера. ICM способна работать на любой машине в кластере. Однако, поскольку сервер обслуживает задачи ICM и все серверные задачи и, следовательно, выполняет больше задач, чем остальные серверы, убедитесь, что служба ICM помещена на самом мощном или, по крайней мере, на наименее загруженном сервере кластера. Когда служба ICM включена в кластер, она обращается к локальному каталогу Cluster Database Directory. Производительность увеличится, если установить несколько служб ICM в кластере;
- О и наконец, можно установить ICM внутри кластера и за его пределами. Основным сервером для обработки запросов HTTP - это служба ICM, работающая на сервере вне кластера. Когда сервер вне кластера становится недоступным, запросы обрабатываются службой ICM, функционирующей на сервере внутри кластера.

Если кластер настроен на обращение к ICM и выполняется задача ICM, HTTP-сервер Domino будет направлять к ICM запросы ко всем базам данных, перечисленным в каталоге Cluster Database Directory (clbdbir.nsf)- База данных Cluster Database Directory содержит информацию о месте хранения баз данных кластера и серверах, на которых они размещаются.

Служба ICM, установленная на сервере вне кластера, выбирает сервер в кластере, чтобы получить доступ к Cluster Database Directory. Если этот сервер становится недоступным, образуется соединение с другим сервером. ICM всегда применяет локальную реплику каталога Domino, поэтому служба ICM должна находиться в одном домене с кластером.

ICM настраивается после того, как установлены и настроены все серверы кластера Domino, в серверном документе, расположенном в каталоге Domino. Откройте в этом документе вкладку **Server Tasks**, затем вкладку **Internet Cluster Manager** (рис. 20.14).

Чтобы настроить ICM, нужно произвести следующие действия:

1. Откройте в программе Domino Administrator существующий сервер Domino.
2. Щелкните по вкладке **Configuration**.
3. Раскройте категорию **Server** и щелкните по **All Server Documents** (Все серверные документы).
4. Откройте серверный документ того сервера, на котором нужно включить службу ICM (выберите серверный документ и либо щелкните по **Edit Server** (Редактировать сервер) и нажмите **Enter**, либо выберите **File** => **Open** из раскрывающегося меню, либо просто дважды щелкните мышью по серверному документу).
5. Перейдите на вкладку **Server Tasks** (Задачи сервера).
6. Щелкните по вкладке **Internet Cluster Manager** (Менеджер кластера Internet).
7. Заполните необходимые поля, как указано в табл. 20.6 (рис. 20.15).
8. Сохраните и закройте документ.

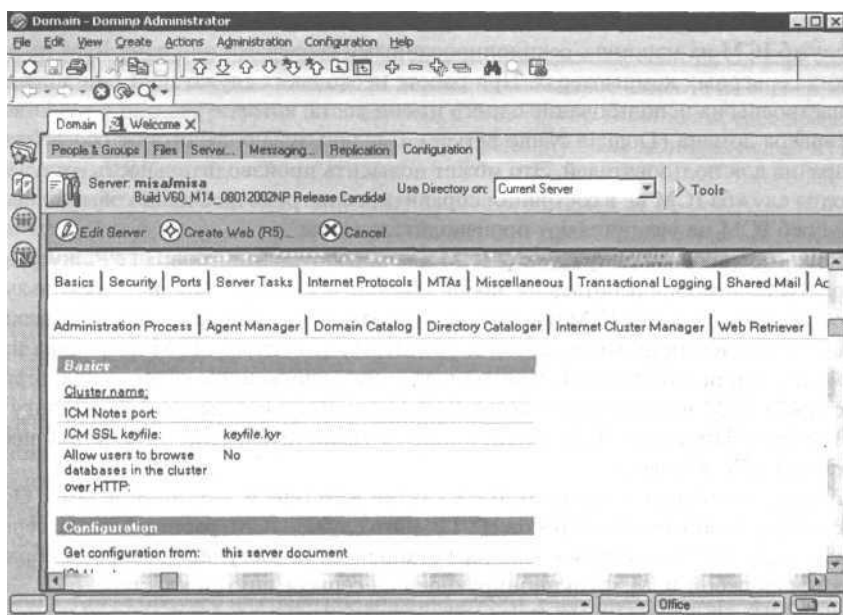


Рис. 20. 14. Менеджер кластера Internet

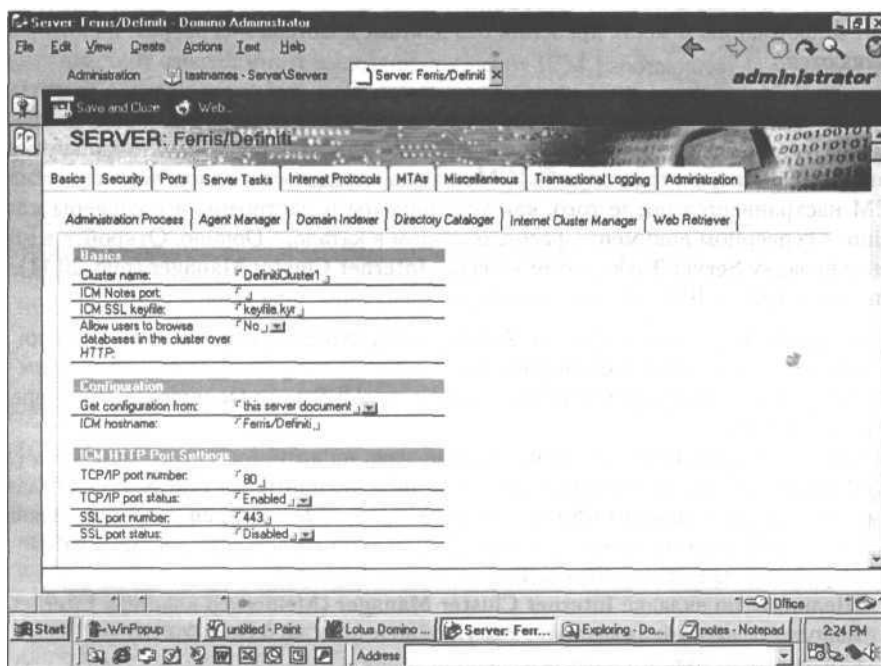


Рис. 20. 15. Установка значений полей для менеджера ICM

Таблица 20.6. Настройка менеджера кластера Internet

Поле	Описание
Вкладка Basics (Основные параметры)	
Cluster Name (Имя кластера)	Если ICM работает на сервере вне кластера, введите имя кластера Domino, которым будет управлять ICM. Если ICM функционирует на сервере внутри кластера, это поле не требуется заполнять
ICM Notes port (Порт Notes для ICM)	Порт Notes, через который ICM соединяется с клиентами HTTP. Если ввести конкретное значение, то ICM будет использовать только указанный порт. Можно оставить поле пустым (по умолчанию), что позволит ICM обращаться к любому порту
ICM SSL keyfile (Файл ключей SSL для ICM)	Имя файла ключей SSL, содержащего сертификаты ICM для аутентификации клиентов HTTP
Allow users to browse databases in the cluster over http (Разрешить пользователям просматривать базы данных кластера через HTTP)	Разрешает клиентам HTTP просматривать список баз данных, содержащихся в кластере (пользователь может применить команду ?OpenServer в URL)
Вкладка Configuration (Конфигурация)	
Get configuration from (Получить конфигурацию из)	При настройке нескольких ICM для использования одной конфигурации введите имя серверного документа, из которого будет взята конфигурация
Obtain ICM configuration from (Получить конфигурацию ICM из)	Когда в поле Get configuration from установлено значение Another server document (Другой серверный документ), в этом поле указывается имя сервера, на котором находится серверный документ, позволяющий получать информацию о конфигурации
ICM hostname (Имя хоста ICM)	Введите полностью квалифицированное имя хоста, к которому будут обращаться клиенты HTTP. Вероятнее всего это будет имя DNS, но можно указывать и IP-адрес. Данное поле необходимо, чтобы сервер HTTP мог генерировать адрес URL для ссылки на ICM. Когда задача ICM работает на том же сервере, что и задача HTTP, во избежание конфликтов лучше задавать IP-адрес самой службы ICM
Вкладка ICM HTTP Port Settings (Параметры порта HTTP для ICM)	
TCP/IP port number (Номер порта TCP/IP)	Номер порта для ICM. Если ICM работает на том же сервере, что и HTTP, но не имеет собственного IP-адреса, убедитесь, что номер порта, указанный в данном поле, отличается от остальных портов, к которым обращается этот сервер
TCP/IP port status (Состояние порта TCP/IP)	Включает/выключает соединение HTTP с ICM
SSL port number (Номер порта SSL)	Номер порта для SSL. Если ICM работает на том же сервере, что и SSL, но не имеет собственного IP-адреса, удостоверьтесь, что номер порта, указанный в данном поле, отличается от остальных портов, применяемых этим сервером
SSL port status (Состояние порта SSL)	Включает/выключает соединение SSL с ICM

Отмена просмотра баз данных клиентами Internet

В общем случае лучше запретить просмотр баз данных клиентами HTTP, особенно клиентами Internet и extranet, то есть для усиления защиты необходимо отменить эту возможность.

Измените документы конфигурации ICM для всех серверов кластера, на которых работает задача HTTP, независимо от того, действует ли на них собственно задача ICM. Это необходимо потому, что каждый сервер Domino обращается к параметрам ICM своего серверного документа, чтобы понять, каким образом направлять запросы Web-клиентов в службу ICM. Когда задача ICM стартует (при запуске сервера), ICM с помощью этой информации определяет имя кластера, сетевые адреса, имя хоста, параметры порта и т.д.

Как видно на вкладке **ICM HTTP Port Settings**, ICM поддерживает протокол SSL. Эта служба может применять те же сертификаты SSL, что и Domino, или другой набор сертификатов SSL. Допускается указать использование SSL, изменив параметры настройки Internet Cluster Manager в серверном документе.

Чтобы запустить задачу ICM вручную, надо ввести на консоли сервера команду load ICM. Но поскольку имеется множество других серверных задач, необходимо добавить ICM в переменную ServerTasks файла notes.ini:

```
ServerTasks=Router, replica, clbdbdir, clrepl, http, icm
```

Можно использовать ICM в кластерных конфигурациях, представленных в предыдущих версиях Domino. Фактически ICM направляет запрос на другой Web-сервер Domino независимо от его версии. Однако только Domino R5/6 в состоянии генерировать адреса URL, которые ссылаются на ICM. После того как запрос передается на сервер более ранней версии, возможности ICM теряются. Не исключено, что в смешанных кластерах будут ограничены некоторые средства защиты от сбоев и распределения нагрузки.

Чтобы избежать конфликтов, выделите для ICM собственный IP-адрес на каждом Web-сервере:

1. Сделайте IP-адрес доступным средствам операционной системы.
2. Запустите Domino Administrator.
3. Выберите в меню **Files => Preferences => User Preferences** (Файл => Предпочтения => Предпочтения пользователей).
4. Щелкните по значку **Ports** (Порты).
5. Щелкните по **New** (Создать).
6. Введите описательное имя для порта ICM, например iCMPort.
7. Выберите в качестве драйвера TCP (рис. 20.16).
8. По умолчанию порт находится в офисной сети, следовательно, это поле можно не изменять.
9. Щелкните по ОК.
10. Щелкните по ОК.
11. Если сервер содержит ICM, добавьте в файл notes.ini следующую строку для настройки порта:

```
PortName=TCP, adapter # or network #, #of sessions, datebuffer size
```

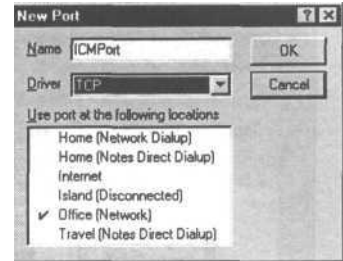


Рис. 20. 16. Настройка порта ICM

12. Добавьте в файл notes.ini такую строку (PortName - имя порта, указанное в Domino Administrator, см. шаг 6):
PortName_TcpipAddress=0 , IpAddress
13. Откройте вкладку **Configuration** в Domino Administrator.
14. Раскройте категорию **Server** и щелкните по **All Server Documents**.
15. Выведите на экран документ сервера, для которого нужно включить ICM (отметьте серверный документ, щелкните по **Edit Server** и нажмите **Enter**, либо выберите **File => Open** из раскрывающегося меню, либо просто дважды щелкните мышью по серверному документу).
16. Перейдите на вкладку **Server Tasks**.
17. Щелкните по вкладке **Internet Cluster Manager**.
18. Введите имя настраиваемого порта.
19. Если нужно обратиться к порту 80, то и для ICM, и для Web-сервера:
 - щелкните по вкладке **Internet Protocols**;
 - перейдите на вкладку **HTTP**;
 - в поле имени хоста введите IP-адрес для имени хоста Web-сервера Domino;
 - в поле **Bind to host name** (Связать с именем хоста) укажите **Enable** (Включить).

Управление и мониторинг ICM

Управлять и контролировать ICM можно из журнала сервера Domino (регистрационные данные) или из статистики (текущие данные).

Для просмотра журнала:

1. Откройте Domino Administrator.
2. Выберите сервер, содержащий нужный журнал.
3. Щелкните по вкладке **Server**.
4. Перейдите на вкладку **Analysis**.
5. Раскройте категорию **Notes Log**.
6. Выберите **Miscellaneous Events** (рис. 20.17).
7. Откройте на панели **Results** документ записей журнала (Log Entry document).

Или:

1. Выведите на экран файл журнала сервера Domino (log.nsf).
2. Откройте вид **Miscellaneous Events**.
3. Откройте документ Log Entry.

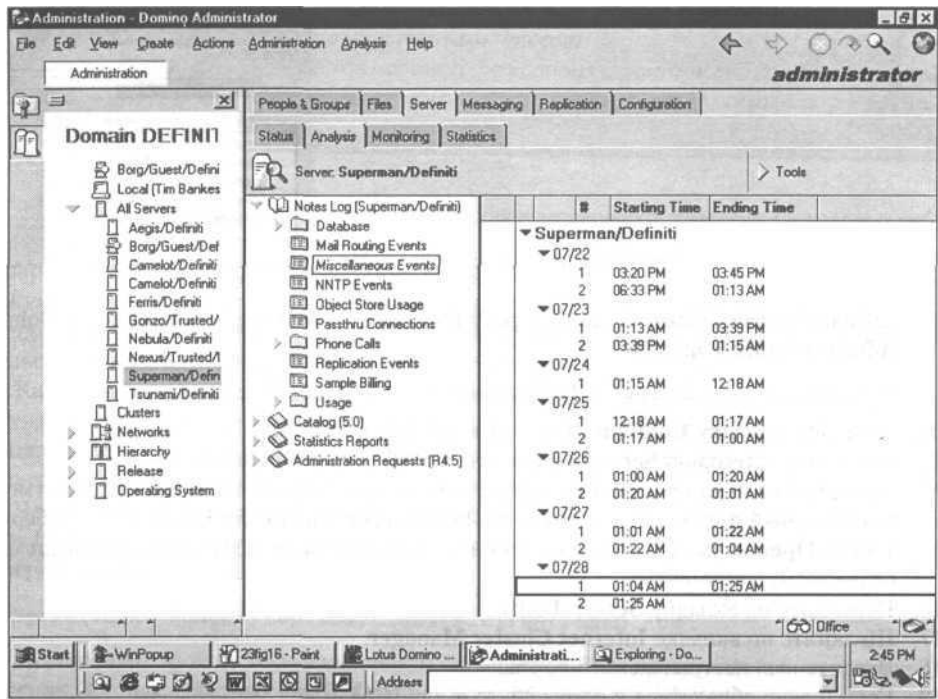


Рис. 20. 17. Просмотр событий журнала Notes

Чтобы просмотреть текущую статистику:

- 1. Загрузите Domino Administrator.
- 2. Выберите сервер, статистика которого вас интересует.
- 3. В списке **All Statistics** щелкните по **ICM** (рис. 20.18).

Можно также ввести команду `stat icm` на консоли сервера.
Список статистических параметров службы ICM приведен в табл. 20.7.

Таблица 20. 7. Статистика менеджера кластера Internet

ICM.AvailabilityIndex	Целое число от 0 до 100, указывающее на доступность сервера (0 означает отсутствие свободных ресурсов, 100 - полную доступность сервера)
ICM.Command.Total	Общее число команд URL, принятых ICM
ICM.Command.Unknown	Общее число команд URL, не распознанных ICM
ICM.Receive.Error	Общее число запросов клиента, не обработанных службой ICM из-за проблемы соединения между клиентом и ICM
ICM.Command.Redirects. Unsuccessful	Общее число успешно перенаправленных службой ICM запросов на сервер кластера

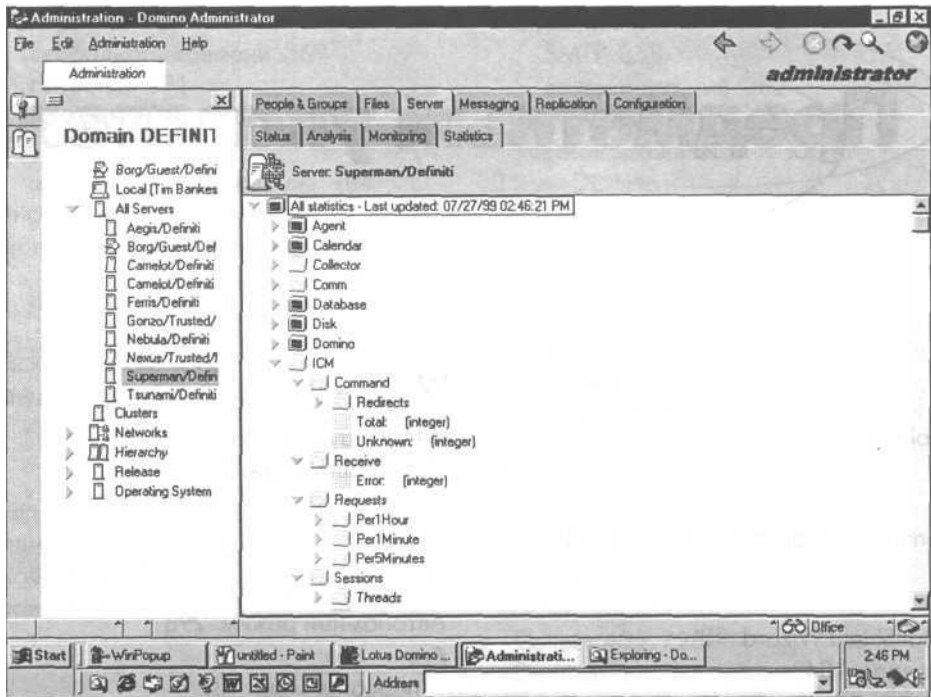


Рис. 20.18. Просмотр статистики в Domino Administrator

Таблица 20.7. Статистика менеджера кластера Internet (окончание)

ICM.Command.Redirects.Successful	Общее число неудачно перенаправленных службой ICM запросов на сервер кластера
ICM.Command.Redireds.ClusterBusy	Общее число перенаправленных службой ICM запросов, когда все серверы оказались заняты
ICM.RequestsPerl Hour.Total	Число запросов HTTP, принятых ICM за предыдущий час
ICM.RequestsPerl Minute.Total	Число запросов HTTP, принятых ICM за предыдущую минуту
ICM.RequestsPer5Minutes.Total	Число запросов HTTP, принятых ICM за предыдущие пять минут

Предметный указатель

B

Bookmark 578

C

Connection Configuration Wizard 282

I

InstallShield Wizard 92

IP-адрес 104

G

Guided Tour 121

L

Lotus Notes Client Configuration
Wizard 239

M

MTBF 747

N

NotesCONNECT 569

NotesPeek 571

S

Schedule Manager 364

T

TeamRoom 59

W

Web-браузер 34

Web-приложение 51

Автономный режим 298

Агент 156

 персональный 132

Административный запрос 127

Адрес сети Internet

 обратный 362

Алгоритм хеширования 460

Архитектура

 баз данных 36

 распределения данных 414

Аутентификация 456

Базы

 данных 709

 Reports 412

 Resource Reservations 365

 Web Navigator 189

 архивная 376

 восстановление 618

 входящих почтовых сообщений 331

 документно-ориентированная 34

 локальная копия 264

- перенос 604
- свободного времени 369
- свойства 591
- совместноиспользуемая 371
- уплотнение 596
- шаблон проектирования 104
- знаний 49
- Базовая начальная страница 573

В

- Версия рабочая 442
- Взаимодействие интерактивное 416

Г

- Группы
 - администрирования 121
 - новостей 300
 - поиска 283

Данные

- идентификационные
 - UNID 418
- функциональные 224
- справочные 49
- статистические 47
- сервера 404

Диаграмма 729

Документ

- выходного дня 368
- домена
 - глобального 362
 - соседнего 332
 - удаленного 332
- конфигурации 328
- конфигурирования сервера 162
- конфликтный 419
- личный 104
- маркируемый 145
- мониторинга репликации 450
- победитель 419

- соединения
 - SMTP 358
 - дополнительный 282
- уведомления о событиях 450
- учетной записи NNTP 300

Домен Domino

- соседний 331
- брандмауэр 80

Ж

Журнал

- персональный 234
- репликации 418

З

Заголовок

- сообщения 342
- почтового 298

Задачи

- Collect 405, 728
- Event 405
- InterNotes Web Retriever 290
- ISpy 406, 728
- Updall 621
- Update 621
- репликации 431

Запись 36

- A 341
- MX 341
- общих документов 485

Затор информационный 61

Защита

- операционной системы 47\$
- сетевая 473
- физическая 473

Зонд 733

И

Имя

- альтернативное 195
- хоста 109

Интерфейс многопортовый 289

8 2 0 DOMINO 5 & 6. АДМИНИСТРИРОВАНИЕ СЕРВЕРА

Информация

- конфиденциальная 41, 80
- общедоступная 80
- секретная 89

Информационный поток 55

- аппаратное управление 170
- программное управление 170
- сетевой 442

Календарь 38

Карта

- репликации
- топологическая 40
- системы 57

Каскадные адресные книги 514, 528

Каталог

Domino

- вторичный 513
- первичный 513

LDAP 192

- внешний 255
- мобильный перечень 514
- поддержка 514, 528
- перечень 514, 528
- перечня
 - мобильных пользователей 192
 - серверов 192
- системный 258

Квота 602

Кластер серверов 68

Кластеризация

- операционной системы 794
- приложений 794
- технология 427

Клиент 34

LDAP 192

- почтовой службы POP 294

Команда

- консоли 404
- управляющая 77

Контроль четности 67

Конфигурация 91

Конфигурирование

- динамичное 446
- сервера 91

Концентратор 178

- основной 427
- региональный 427
- почтовой службы 340

Конфликтная ситуация 415

Критический элемент 715

Кросс-сертификат 465

Л

Линия DSL 64

Лицензирование 34

М

Маршрут альтернативный 350

Маршрутизатор

- почтовый
- сервера Domino 326
- с фильтрацией пакетов 191

Массив RAID 67

Масштабирование 61

Меню раскрывающееся 121

Метод администрирования 34

Моделирование предварительное 307

Монитор процесса репликации 449

Мониторинг 706

Н

Набор

- данных 35 £
 - шрифтов TrueType 235
- ### Начальная страница 573

О

Обеспечение

- безопасности 89
- программное
- сервера 91

Объекты ядра 713

Отказ системный 66

П

- Пакет
 - SmartSuite 234
 - сетевой 191
- Папка
 - данных 93
 - домашняя 236
- Параметр
 - формата MIME 395
 - миграции 247
- Переименование 141
 - пользователя 552
- Переменная 94
- Перемещение пользователя 559
- План ротации 374
- Планирование 38
- Плата сетевого интерфейса 87
- Платформа 35
- Поле 36
 - синтаксис 392
- Полоса пропускания 61
- Пользователь 34
 - административный 196
 - анонимный 90
 - мобильный 34
- Порт
 - модема 166
 - обмена данными
 - последовательного 104
 - сетевой 104
- Почта электронная 35, 47
- Почтовое сообщение
 - заголовок 298
 - тело 298
- Правило
 - более позднего редактирования 440
 - наиболее частой повторяемости 440
 - почтовое 581
- Предпочтения
 - административные 121"
 - пользователей 579
- Предупреждение 729
- Программа
 - Calendar Connector 364
 - Domino Administrator 53
 - Domino Designer 53
 - Domino Server.Load 74
 - Domino Server.Planner 74
 - Event Dispatcher 450
 - SMTPMTA 316
 - антивирусная 92
 - клиентская 36
 - почтовой службы 391
- Протокол
 - DAP 81
 - IPX/SPX 71
 - LDAP 81
 - S/MIME 41
 - TCP/IP 70
 - почтовой службы
 - стандартный 255
 - сетевой 69
- Профиль установки пользователя 581
- Процедура
 - маршрутизации
 - почтовых сообщений 179
 - обновления 306
 - очистки базы данных 448
 - резервирования 67
 - установки 92
- Пул модемов 163
- Развертывание 54
 - приложения 588
- Регистрация
 - очередь 214
 - транзакций 615
- Редактирование конфликтное 438
- Режим
 - набора номера 167
 - фоновый 423
- Резервирование ресурсов 366

8.2.2. DOMINO 5 & 6. АДМИНИСТРИРОВАНИЕ СЕРВЕРА

- Репликация 40
 - или копирование документов 485
 - кластерная 417
 - плановая 414
 - по принципу Pull 415
 - по принципу Push 415
 - по требованию 417
 - частота 425
 - фоновая 423
- Репозиторий информационный 34
- Роль 485
- Ротация 374
- Сервер
 - Domain Search/Catalog Server 193
 - Domino 34
 - Domino Application Server 51
 - Domino Enterprise Server 51
 - Domino Go 52
 - Domino LDAP 192
 - Domino Mail Server 51
 - HTTP 44
 - Netscape Directory Server 81
 - Oracle 68
 - административный 181
 - базы данных 330
 - дополнительный 152
 - каталогов 514
 - LDAP 192
 - выделенный 192
 - консоль управления 122
 - концентратора 188
 - новостей 190
 - однопроцессорный 189
 - почтовый
 - IMAP 695
 - POP3 686
 - радиальный 427
 - резидентный 44
 - свойства 737
 - связи 164
 - сегментированный 68, 93
 - сквозной 132
 - тестовый 307
 - файловый 35
 - сетевой 250
 - форма конфигурирования 162
- Сервис каталогов LDAP 192
- Сертификатор 82, 459
- Сетевой переключатель 189
- Сеть
 - Domino 123
 - Internet 35
 - NetBEUI 70
 - иерархия 77
 - инфраструктура 77
 - локальная высокоскоростная 189
 - частная 191
- Система
 - Notes 34
 - Notes/Domino 34
 - SMTP 342
 - бухгалтерского учета 47
 - почтовой связи
 - внешняя 332
 - сбора статистических данных 450
- Системный монитор 712
- Скорость передачи данных 63
- Служба 567
 - Domain Index 193
 - Domain Search 193
 - LDAP 513
 - RAS 165
 - Replicator 417
 - Web Retriever 189
 - каталога дополнительная 192
 - почтовая
 - IMAP 686
 - локальная 288
 - совместно используемая 323

- просмотра каталогов 192
- синхронизации 248
- Событие 729, 731
 - серьезность 731
- Соединение
 - Pull Only 351
 - Pull Push 351
 - Push Wait 351
 - SMTP защищенное 389
 - беспроводное 44
 - конкурирующие 422
 - модема 164
 - с набором телефонного номера
 - сети 164
 - T-1 63
 - T-3 63
- Создание
 - агентов
 - LotusScript/Java 485
 - персональных 484
 - документов 484
 - папок
 - общих 485
 - персональных 485
- Сообщение
 - MIME многокомпонентное 394
 - почтовое 36
 - SMTP 326
 - некорректное 403
 - потерянное 402
- Список
 - доступа 124
 - управления исполнением 195,204
 - форм 228
- Справка контекстная 121
- Среда проектирования интегральная 44
- Ссылка
 - на базу данных 611
 - на каталог 611
- Стандарт X.500 81
- Станция рабочая 35
- Стек
 - Domino/HTTP 45
 - IP 80
- Строка текстовая 342
- Схема присвоения имен 81,91
- Сценарий 74
 - заимствования модемов 165
- Счетчик 714
- Таблица 36
- Тест NotesBench 73,751
- Топология
 - кольцевая 340
 - маршрутов 323
 - репликации 178
- Трафик сетевой 36
- Удаление документов 484
- Узел
 - контрольный 343
 - передачи данных 342
 - сети CompuServe 266
- Указатель 370
 - заголовка 371
- Уровень
 - громкости 167
 - доступа
 - Author 482
 - Depositor 482
 - Designer 482
 - Editor 482
 - Manager 482
 - No Access 482
 - Reader 482
 - сетевого 200
- Установка
 - автоматическая 258
 - совместно используемая 236

Учетная запись

NNTP 300

SMTP 296

POP 294

Ф

Файл

главного перечня 315

идентификационных данных 41

ключевой 472

команд модема 167

ответных сообщений 233, 258

почтовой службы

основной 314

почтовых сообщений

совместно используемый 375

программ 250

регистрации 259

Флаг 167

Формат

MIME 201

перемещаемых документов 234

канонический 82

сокращенный 82

текстовый расширенный 329

Функция

Collector 320

Domain Search 317

Event Notification 321

RAID 67

Site Search 317

базовая 35

восстановления идентификационных
данных/пароля 196

отслеживания

маршрутов 408

приложений 50

сообщений 408

поиска индексов 318

регистрации транзакций 186

управления версиями 440

хранения данных 36

Хост интеллектуальный 352

Ш

Шифрование

локальной базы данных 474

с двойным ключом 459

с одним ключом 459

Шлюз SMTP 339

Экземпляр 714

Экспорт в электронную таблицу 729

Язык альтернативный 195

Ярлык 93

Роб Кирклэнд

Domino 5 & 6

Администрирование сервера

Главный редактор *Захаров И. М.*
editor-in-chief@dmkpress.ru

Перевод *Хаванов А. В.*
Научный редактор *Кузьмин М. А.*
Выпускающий редактор *Левицкая Т. В.*
Верстка *Трубачев М. П.*
Графика *Салимонов Р. В.*
Дизайн обложки *Дудатий А. М.*

ИД № 01903 от 30.05.2000

Подписано в печать 11.06.2003. Формат 70х100'/i6.

Гарнитура «Петербург». Печать офсетная.

Усл. печ. л. 67,6. Тираж 1000 экз. Зак. № 1734.

Издательство «ДМК Пресс», 105023, Москва, пл. Журавлева, д. 2/8.

Web-сайт издательства: www.dmkpress.ru

Internet-магазин: www.abook.ru

Отпечатано на ордена Трудового Красного Знамени
ГУП Чеховский полиграфический комбинат
Министерства Российской Федерации по делам печати,
телерадиовещания и средств массовых коммуникаций
142300, г. Чехов Московской области
Тел. (272) 71-336, факс (272) 62-536