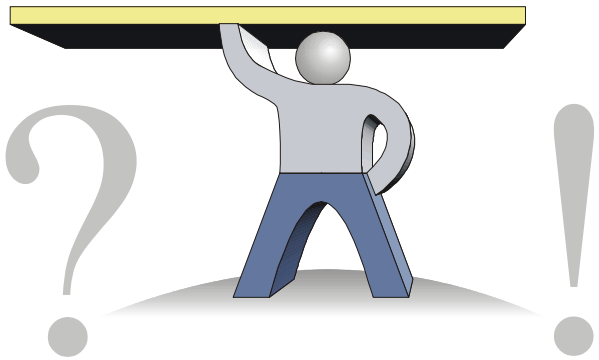
Компания
ИнтерТраст

тел./факс: (095) 956-7928
http://www.intertrust.ru
E-mail: postmaster@inttrust.ru

В. Некрасов

Lotus .domino™



Администрирование Lotus Domino R5 в вопросах и ответах

© *InterTrust Co.* Тел. 956-7928

В.В. Некрасов

"Справочное пособие для администраторов Lotus Domino R5"

Книга представляет собой адаптированный перевод базы данных «Domino 5 Administration help». В Работе основное внимание уделено вопросам администрирования (планирования, установка, настройки эксплуатации и защиты) Lotus Domino R5. Рассматриваются вопросы установки серверов Domino и клиентских станций Notes, команды консоли сервера и серверные задачи, используемые для настройки и контроля функционирования серверов, вопросы репликаций и передачи почты, сертификации и обеспечения безопасности, конфигурирования сервера Domino, использования кластеров из нескольких серверов Domino, мониторинга работы серверов и вопросы миграции с версии Lotus Domino R4.x на Lotus Domino R4.x.

Книга ориентирована на специалистов по компьютерным сетям, в функции которых входит планирование, настройка, управление и эксплуатация сетей Lotus Domino R5. Она может быть полезна разработчикам приложений в среде Notes и менеджерам, занимающимся вопросами проектирования и разработки информационных систем.

Lotus, Lotus Domino и Lotus Notes являются зарегистрированными торговыми знаками фирмы Lotus Development Corporation, an IBM Company. Все другие упомянутые в данном издании товарные знаки и зарегистрированные товарные знаки принадлежат их законным владельцам.

© InterTrust Co., 2000

© Некрасов В.В., 2000

© Оформление обложки Будылев С. В., 2000

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

Глубокоуважаемый читатель!

Предлагаемая Вашему вниманию книга представляет собой адаптированный перевод базы данных «Domino 5 Administration help». Мы приняли решение издать эту работу, так как считаем полезным и целесообразным предложить российским администраторам сетей Lotus Domino настольное справочное пособие, которое может облегчить их нелегкий и ответственный труд.

Мощь и сложность программного обеспечения Domino R5 такова, что уже не представляется возможным в реальные сроки, сопоставимые с временем жизни версии, подготовить и выпустить книгу, полностью раскрывающую весь спектр проблем и все тонкости администрирования Domino R5. Однако, наряду с предлагаемым Вам настоящим пособием, мы подготовили и уже начали издавать специализированные книги глубоко раскрывающие отдельные вопросы разработки приложений и администрирования в R5.

Мне доставляет особое удовольствие сказать несколько слов об авторе книги В. Некрасове. Мы познакомились с Вячеславом на нашем техническом Форуме «Вопросы и Ответы». Он живет и работает в г. Новороссийске и занимается вопросами поддержки и администрирования Lotus Domino. Я полагаю, что огромный труд, проделанный Вячеславом, будет востребован и по достоинству оценен российским нотусовым сообществом.

Книга ориентирована на специалистов по компьютерным сетям, в функции которых входит планирование, настройка, управление и эксплуатация сетей Lotus Domino R5. Она может быть полезна разработчикам приложений в среде Notes и менеджерам, чей род деятельности связан с проектированием и разработкой информационных систем.

Всех читателей, заинтересованных в более глубоком изучении практических вопросов администрирования и разработки приложений в Lotus Domino/Notes мы приглашаем в Авторизованный центр обучения (LAEC) Компании ИнтерТраст (тел. (095)-956-7928).

Я искренне надеюсь, что данная книга будет полезна широкому кругу читателей

С уважением,

Генеральный Директор Компании «ИнтерТраст»

А.А. Линев

1 Инсталляция, обновление программного обеспечения R5.

1.1 Какой тип инсталляции программного обеспечения сервера выбрать и чем они отличаются?

При выборе типа инсталляции Вашего сервера обычно руководствуются видом лицензии сервера, приобретенной Вашей организацией. От вида лицензии зависит и стоимость всего проекта, внедрения Domino в организации или ее филиалах.

Семейство серверов Domino R5 представляет собой программную серверную платформу, предоставляющую широчайший спектр функций передачи сообщений, мощную архитектуру Web-приложений для разработки деловых приложений, легко масштабируемых, надежных, которые удовлетворят даже самых крупных корпоративных заказчиков. Благодаря единой архитектуре, серверы Domino позволяют заказчикам воспользоваться гибкостью подхода “начать с малого и быстро расширяться”.

Семейство серверов Domino включает в себя три основных сервера:

*0 **Domino Mail Server** (почтовый сервер) – предоставляет ведущие в отрасли средства передачи сообщений и совместной работы, включая базы данных дискуссий, интегрированный доступ к Web, функции ведения календаря и группового планирования. Встроенные инструментальные средства обновления позволят Вашим пользователям быстро достигнуть высокой производительности работы. Кроме того, благодаря комплексным и интуитивно понятным инструментальным средствам администрирования сервером Domino очень просто управлять – независимо от того, развертываете Вы его во вновь созданной компании или на крупном предприятии с большим количеством удаленных серверов. Поддержка самых распространенных стандартов интернет и самого широкого спектра клиентов – HTTP, IMAP, POP3, ведущего в отрасли клиента Notes, а также устройств PDA и интеллектуальных телефонов – позволят Вам получить доступ к защищенным средствам передачи сообщений через интернет в любое время и из любого места.

*1 **Domino Application Server** (сервер приложений) – предоставляет полноценную платформу для Web-приложений, включающую в себя все выдающиеся возможности передачи сообщений почтового сервера Domino Mail Server. Встроенные средства Domino Enterprise Connection Services (DECS) – графический, не связанный с программированием интерфейс – это самый быстрый и самый простой способ интеграции в режиме реального времени традиционных и корпоративных систем с Web приложениями. Комплексная среда приложений предоставляет возможности для интеграции рабочих потоков, средств управления содержимым и функций передачи сообщений, в целях поддержки ориентированных на процессы приложений. Поддержка основных языков программирования, включая Java и Javascript, позволяет использовать при разработке нужных приложений для интранет и интернет любые популярные инструментальные средства. Кроме того, сервер Domino Application Server может быть интегрирован в существующую архитектуру приложений за счет поддержки CORBA/IIOP.

*2 **Domino Enterprise Server** (сервер предприятия) – предоставляет все функциональные возможности почтового сервера Domino Mail Server и сервера приложений Domino Application Server, усиленные за счет функций кластеризации Domino Clustering Services, благодаря которым обеспечиваются высочайшие показатели готовности и надежности, необходимые для самых критичных приложений. Благодаря уникальной технологии кластеризации в сервере Domino Enterprise Server обеспечиваются распределение нагрузки и отказоустойчивость клиентов Notes и браузеров Web.

1.2 Какие новые возможности появились в версии R5?

В версии R5 Lotus заложила ряд принципиально ряд новых возможностей, недоступных в более ранних версиях программных продуктов из серии Lotus Notes, Lotus Domino. Но это не мешает клиентам, использующим более ранние версии программного обеспечения, на своих рабочих станциях, обращаться к данным на серверах R5. Более того, сервера версий R3 и R4 могут работать с сервером R5 в одной сети или в домене Notes. Ниже приведен перечень новых функций появившихся в версии R5:

*3 Расширенные средства передачи сообщений через интернет – средства передачи сообщений Domino представляют собой оригинальные средства передачи сообщений интернет с поддержкой оригинальной схемы адресации интернет, оригинального расширения S/MIME и оригинального протокола маршрутизации SMTP.

*4 Защищенная инфраструктура передачи сообщений и приложений полностью интегрированные сертификаты X.509, способствует использованию более мощной схема шифрования для защиты данных. Используется архитектура Common Data Security Architecture (CDSA), благодаря которой мощные функции защиты данных Domino могут быть распространены на приложения независимых поставщиков с поддержкой S/MIME, SSL V3. Используется новая опция восстановление паролей для ID пользователей, интерфейсы прикладного программирования API для реализации специальных функций аутентификации и шифрования.

*5 Каталог Domino Directory – новый каталог Domino Directory в версии 5 отвечает потребностям даже самых крупных предприятий за счет полной поддержки LDAP v3 и наличия сильно сжатого индекса Directory Catalog.

*6 Управление системой передачи сообщений – детальные средства отслеживания сообщений, контроля и составления отчетов. Улучшенная система управления хранением сообщений Message Store Management, управление маршрутизацией, оригинальный протокол маршрутизации SMTP, легко устанавливаемые ограничения для сообщений и встроенные инструментальные средства обновления.

*7 Открытый, защищенный сервер Web-приложений, реализованная в Domino поддержка Web-сервера MS IIS позволяет расширить возможности существующей среды NT/IIS, в то время как управление доступом к HTML-файлам позволяет распространить основанную на ролях систему защиты данных Domino на среду интранет или интернет. Кроме того, средства обеспечения отказоустойчивости и распределения нагрузки посредством управления кластерами интернет, повышенная производительность ядра HTTP, доступ в реальном времени к полям реляционных баз данных, ведение контрольного журнала виртуального сервера, поддержка простых, легко отыскиваемых указателей URL и поддержка протоколов CORBA/IIOP позволяют легко интегрировать Domino в Вашу архитектуру приложений.

*8 Усовершенствованная база данных и архитектура, обеспечивают реальную масштабируемость при увеличении объема базы данных до 32 GB. Оптимизация памяти и системы ввода/вывода, а также ведение контрольного журнала транзакций, быстрый перезапуск после сбоя, поддержка в 2-4 раза большего количества пользователей и масштабируемый каталог Domino R5, в котором может находиться не менее миллиона зарегистрированных пользователей.

*9 Несравнимые показатели готовности и надежности – гарантируют Вашей серверной инфраструктуре соответствующие показатели готовности и надежности. В R5 поддерживаются средства обеспечения отказоустойчивости и распределения нагрузки для клиентов Notes и клиентов Web, тесная интеграция с кластерами операционной системы,

неограниченное количество разделов на сервере, ведение контрольного журнала транзакций, оперативная индексация, улучшенные функции автоматического перезапуска и восстановления, оперативное сжатие/сжатие на месте, а также поддержка полного и последовательного (с накоплением) резервного копирования в режиме он-лайн.

*10 Улучшенная программа установки/настройки – гибкие, управляемые "мастерами" программы установки, инструментальные средства обновления для cc:Mail, MS Mail и Exchange при регистрации, автоматическая настройка клиентов и расширенные шаблоны настройки серверов позволяют быстрее приступить к плодотворной работе.

*11 Средства администрирования Domino Administrator – упрощение администрирования за счет задачно-ориентированного интерфейса, функций "перетащи и отпусти" и логично организованных вкладок для упрощения доступа к наиболее часто выполняемым задачам. Кроме того, опубликованные интерфейсы прикладного программирования API для инструментальных средств сторонних поставщиков позволяют безупречно интегрировать Domino с другими решениями в области системного управления.

*12 Управление настольными системами, возможности управления настольными системами пользователей и сокращение расходов на поддержку за счет централизованных функций конфигурирования клиентов и обновления.

*13 Инструментальные средства управления знаниями – новое ядро поиска предоставляет пользователям возможность эффективно осуществлять поиск информации любого типа и находить искомое среди нескольких баз данных, в пределах домена и во всей файловой системе.

*14 Средства локализации в Domino, представляет собой превосходную платформу для международных организаций, для входящих и исходящих сообщений поддерживаются большое количество языков и наборов символов, упрощено конфигурирование системы для поддержки многоязыковых сообщений, поддерживается многоязыковый каталог.

*15 Начиная с версии 5.0.4, Lotus несколько изменил подход к видам лицензий. Если раннее имелось два вида лицензий North American и International English то, начиная с версии 5.0.4, Lotus переходит на единую Global лицензию. При использовании этого типа лицензии Вы можете использовать более сильное шифрование в 128 бит, доступные ранее только в North American типе лицензии. Эта функция поддерживается при установке ежеквартальных обновлений. Подробное описание Вы найдете по адресу:

http://www.notes.net/qmrdown.nsf/

*16 Начиная с версии 5.0.5, в поставку сервера входит поддержка сервиса DOLs (Domino Off-Line Service). Сервис позволяет работать с базами Domino сервера локально, при этом используется "тонкий" клиент iNotes. Данный сервис становится доступным при установке ежеквартального обновления версии 5.0.5. Подробное описание сервиса, с демонстрацией возможностей, Вы найдете по адресу:

http://www.lotus.com/home.nsf/welcome/inotes

1.3 Какие существуют общие принципы для обновления серверов до версии R5?

Перед тем как Вы приступите к модернизации системы до R5, убедитесь, что Вы ознакомились с документами файла README.NSF. База данных Notes Release содержит техническую информацию, которая не была включена в основную документацию.

Опыт показывает, что большинство организаций предпочитают переходить на R5 не сразу. Имеет место период, в котором существуют и старые версии системы, другие почтовые системы, которые сосуществуют с R5.

Lotus создавал R5 с расчетом совместимости всех версий. Возможно существования вместе - ключевых базы данных системы Domino Directory, Administration Requests. Они были разработаны для совместимости с более ранними версиями. Кроме того, новые функции, типа Simple Message Transfer Protocol (SMTP) и Multipurpose Internet Mail Extensions (MIME), в Domino не требует никаких изменений - просто, Вы модернизируете Router до R5. Ваши существующие пути маршрутизации и адресное пространство также будут работать в R5, поскольку они сделаны в R4. Короче говоря, модернизация и сосуществование нескольких версий должен быть безболезненным, позволяя Вашей организации перейти быстро на новую версию R5.

Чтобы модернизировать Вашу систему до R5, Domino система и Notes клиент должен иметь версию не ниже R4.1. Lotus рекомендует наращивать версии Вашей системы до самой последней, доступной Вам версии. Используйте для этого QMRs/QMUs, которые доступны по адресу:

`http://www.notes.net/`

Убедитесь, что все базы данных Вашей системы используют формат R4. Если Вы имеете некоторые шаблоны в формате R3, например адресные книги или почтовые файлы, Вы должны модернизировать их, по крайней мере, до R4.1, перед переходом на R5.

Если Вы модернизируете клиентов R3 в R5, программа установки проигнорирует файл рабочего пространства DESKTOP.DSK и создает незаполненный набор закладок.

1.3.1 Что нужно учесть при модернизации системы до R5?

Перед проведением модернизации, просмотрите список проблем, которые могут возникнуть в ходе модернизации.

Изменения или замена операционной системы.

Клиент Notes R5 больше не доступен для операционных систем: Windows3.1, IBM® OS/2® Warp и UNIX системы. Пользователи Notes этих системами могут продолжать работать с более ранней версией Notes, или заменить платформу, которая поддерживается R5 клиентом: Windows95, Windows98, WindowsNT, Windows2000 или Macintosh PowerPC.

Domino сервер R5 больше не выпускается для Novell NetWare. Организации, в которых сервер Domino установлен на NetWare, могут продолжать использовать более раннюю версию сервера Domino или заменить платформу сервера на: HP-UX, IBM AIX®, OS/2 WARP, WindowsNT, Windows2000 и Solaris.

Требования к аппаратным средствам.

Убедитесь что Ваше “железо” удовлетворяет требованиям аппаратных средств для Domino и Notes R5. Вам, возможно, понадобится модернизировать компьютер сервера и рабочие места пользователей.

См.. Release notes для более подробной информации.

Модернизация в международной организации.

Если Ваша организация международная, оповестите Ваших коллег о планируемой модернизации. Отделы региональных областей имеют как правило различные инфраструктуры - например, домены с высокими затратами по связи. Одни филиалы могут использовать удаленный доступ к сети, например MS RAS, а другие используют связь по сети LAN, и их требования к системе будут различны. Модернизация может затрагивать каждый филиал по-разному. Например, при переходе на R5, больше не надо иметь отдельный MTA сервер, для каждого набора символов или языка.

1.3.2 Какой должен быть порядок действий администраторов, при модернизации системы?

Модернизация Вашей Domino системы должна быть организованным процессом, чтобы минимизировать работу и избежать остановки пользовательских, деловых процессов. Сервер, например должен быть модернизирован во время, когда немногие пользователей связаны с ним (выходные или поздно вечером).

Lotus рекомендует модернизацию R5 в следующем порядке:

*17 Центральные, узловые Hub сервера

*18 Почтовые сервера

*19 Сервера приложений

*20 Клиенты Notes

*21 Приложения и базы данных

В первую очередь модернизируйте сервера, потом рабочие станции клиентов и только после этого приступайте к модернизации приложений. Вы минимизируете неудобства принесенные пользователям и деловым процессам. Пользователи не увидят всех новых возможностей R5, пока их клиенты не модернизированы; и наоборот, пользователи не смогут воспользоваться преимуществом, типа правил для почты, пока их сервера не будут модернизированы до R5. Кроме того, этот порядок позволяет администраторам привыкнуть к новому, более легкому управлению Domino серверами, с использованием клиента Domino Administrator

Hub сервера.

Hub сервера лучше работают с почтой и репликами и администрирование в Domino R5 выгодно улучшено. Hub серверами вообще управляют администраторами или опытные пользователи, которые могут быстро устранить любые проблемы происходящие в Вашей системе.

Во время, когда Вы модернизируете Hub сервера Вашей организации, новый клиент Domino Administrator R5 намного упростит задачи администрирования. Новый графический интерфейс, с расширенными функциями поиска неисправностей и контролем серверов, поможет вам в работе. Кроме того, Domino Administrator работает с новым шаблоном Domino Directory, который ускорит выполнение административных задач Вашими администраторами.

Почтовые сервера.

После модернизации Ваших Hub серверов, используйте знание и опыт, полученные в течение процесса модернизации, для устранения проблем с модернизацией почтовых серверов в Вашей организации. Domino R5 включает многочисленные новые возможности,

которые сделают Вашу почтовую инфраструктуру быстрее, мощнее и надежнее. Пользователи извлекут выгоду от увеличения производительности и новых функций встроенной поддержки MIME, SMTP и универсального почтового ящика. Модернизация почтовых серверов займет более длительный период времени и вовлечет большее количество людей, но опыт извлеченный из предыдущей стадии модернизации должен упростить этот процесс.

Не приступайте к модернизации почтовых файлов пользователей, с использованием нового шаблона R5, пока пользователи Notes не заменили свои рабочих станций на R5. Вы можете, модернизировать почтовые файлы пользователей в новый формат баз данных (ODS) для более быстрого обновления видов и более легкого восстановление испорченных ID файлов, а так же повышения производительности. Для Ваших пользователей, имеющих доступ к серверу только по POP3 или IMAP клиентов, Вы можете обновить почтовые файлы в R5 - немедленно.

Сервера приложений.

Ваши приложения и сервера, на которых они запущенны, является сердцем Вашего бизнеса, так что модернизируйте их с особой осторожностью. Тщательно проверите Ваши приложения на R5 перед модернизацией. Продумайте, стоит ли модернизировать ODS Ваших приложений в формат R5, для получения наилучшей производительности и использования резервного копирования, или лучше оставлять их в формате ODS R4.

Клиент Notes.

Только после модернизации серверов можно приступать к замене клиентов. Notes модернизирует клиентов R4 автоматически, при запуске программы инсталляции рабочей станции. Создает набор закладок в рабочем пространстве пользователя и обновляет персональную адресную книгу пользователя. В первое время пользователи могут нуждаться в помощи, так как новый интерфейс пользователя Notes, очень похож на Web-браузер.

Приложения и базы данных.

Как только Вы модернизируете Domino сервера и Notes клиентов, начинайте модернизацию Ваших приложений и баз данных. При модернизации, формат баз преобразуются в новый формат баз ODS R5, заменены будут стандартные базы данных и их шаблоны (почтовые файлы, базы данных обсуждения и библиотек документов). С этих пор, R4 и более ранние клиенты не смогут использовать возможности R5, удостоверитесь, что Ваши пользователи модернизировали свои рабочие места в R5, перед заменой шаблонов.

Модернизация баз в формат R5 ODS не сложна. Вы можете модернизировать реплики баз ODS R5 на серверах R5, позволить реплицировать эти копии на сервера R4, но запретить реплицировать дизайн. Таким образом, в Вашей инфраструктуре будут работать смешанные версии, Вы можете оставить некоторые базы данных в формате R4 ODS до тех пор, пока Ваша организация не закончит переход на R5. Тем не менее, модернизируйте любые R4 базы данных в формат ODS R5.

1.3.3 Нужно ли “проигрывать” проект модернизации?

Однозначно да.

Перед модернизацией Вашей системы, испытайте процедуры модернизации в тестовой среде, которая не влияет на Вашу основную рабочую среду. В тестовой среде Вы сможете проиграть Ваши действия, делать некоторые ошибки и получить ценный опыт.

Как правило, в маленьких компаниях организация тестовой среды вызывает проблемы, обусловленные нехваткой оборудования. По своему опыту могу сказать, что мне приходилось предоставлять собственную рабочую станцию для испытательных целей. Но некоторые неудобства, были компенсированы результатами и приобретенным опытом в установке и модернизации программного обеспечения. А если учесть тот факт, что на момент испытаний моя рабочая станция была - 486DX2-66 с 32Мв ОЗУ и 540HDD, то становится ясно, что такое “железо” можно найти в любой организации.

В тестовой среде желательно воспроизвести, в маленьком масштабе, Domino систему Вашей организации. Если Ваша организация использует Кластер серверов, испытайте Кластер R5 в смешанной среде R4/R5. Если Ваша организация имеет смешанную среду - например, некоторые клиенты использует R4.1, а некоторый R4.6 - проверьте процесс модернизации на обеих версиях.

Создайте список Notes и Domino баз данных, которые являются критическими для Вашей организации. Рассмотрите стандартное развертывание для Вашей инфраструктуры. Например, Ваша компания может разместить все почтовые файлы на одном сервере, чтобы гарантировать высокую надежность и сбалансировать нагрузку сервера. Внесите в список различные типы серверов, который Вы используете. Некоторые компании используют Domino только для передачи почты, другие используют их для приложений и Web-услуг.

В больших компаниях, можно рассмотреть развертывание системы R5, в масштабе одной рабочей группы, которая послужит моделью для остальной части организации. Используйте это развертывание R5, наряду с Вашим экспериментальным проектом, проверьте Ваши планы, и ожидаемые результаты.

1.3.4 Как можно протестировать приложения перед их модернизацией в новый формат?

Приложения R4 должны функционировать должным образом в R5. Однако вам необходимо проверить важные приложения, перед их модернизацией в тестовой среде R5.

Создайте список ключевых функций в Ваших приложениях и оцените их функциональные возможности под R5. Примените любые R5 шаблоны и R5 ODS приложения. Будьте осторожны, все документируйте и проверяйте

Делайте изменения в стандартных шаблонах. R5 шаблоны могут включать функциональные возможности, которые Вы добавляли или изменили в R4.

Обратите внимание, после модернизации дизайна в R5, Вы должны восстановить представления в базе данных. Вы можете сделать это, открыв базу данных в клиенте Notes и нажать клавиши CTRL+SHIFT+F9, или ввести команду на консоли Domino сервера.

```
load updall databaseName.nsf -r
```

Испытания приложений.

Ваша стратегия испытания может измениться в зависимости от числа используемых приложений. Вы должны определить, какие приложения вы должны проверять.

*22 Если Вы еще этого не сделали, установите Domino Designer на Вашем рабочем месте.

*23 Создает документы, с использованием каждой формы, включая скрытые формы. Удостоверитесь, что Вы можете вводить информацию в каждое поле в форме, что кнопки работают правильно, и что текст в форме показывается правильно.

*24 Открывайте в каждом Виде документы, которые Вы только создавали. Удостоверитесь, что они показываются, правильно и формулы вычисляют правильно. Удостоверитесь, что скрытые представления работают правильно.

*25 Просмотрите документы, которые Вы создали. Удостоверитесь, что они показываются, правильно и формулы вычисляют правильно.

*26 Если Notes использует, внешние базы данных, убедитесь, что модернизируется формулы правильно.

*27 Если прикладные формулы используются и посылают данные в скрытые виды в базах данных системы - например, Public Address Book – удостоверьтесь, эти формулы работают правильно.

*28 Если Notes использует, внешние OLE приложения, создает формы, которые используют OLE и запускают объекты.

*29 Проверяйте всех агентов, чтобы удостовериться, что они работают правильно.

*30 Проверьте безопасность Ваших баз данных. Например, проверьте список ACL доступа; ключи шифрования; роли читатели и доступ авторов.

*31 Если Notes использует формулы отбора репликации, испытайте эти формулы, чтобы удостовериться, они работают правильно. Например, проверьте базу данных реплики, чтобы удостовериться, какие документы выбираются и копируются должным образом.

*32 Вы должны проверить это для каждого приложения.

1.4 Как модернизировать почтовый интернет сервер R4 до версии R5?

Предыдущие версии Domino сервера использовали Агента Передачи Сообщения (MTA) для передачи почты в интернет. В R5, Router может маршрутизировать интернет почту с использованием протокола SMTP. Почтовые клиенты могут готовить интернет почту в формате MIME, или в формате Notes - Domino маршрутизирует оба этих формата и конвертирует почтовые сообщения автоматически, если это необходимо в любой из форматов.

При модернизации сервера то, что работало в R4, продолжает работать в R5. Вы почувствуете увеличение производительности, найдете много дополнительных функций и возможностей используя R5. При этом изменения в Вашей существующей конфигурации не потребуются. Domino использует все R4 установки без изменения.

1.4.1 Как модернизировать сервер, использующий SMTP/MIME Message Transfer Agent (MTA) до версии R5?

Далее приведен поэтапный план Ваших действий при модернизации Вашей системы до R5. Используйте его, чтобы быстро заменить программное обеспечение Вашего сервера и избежать потери данных пользователей.

1.4.1.1 Сохранение важных файлов Domino сервера.

Если Вы столкнетесь с ошибками в течение процесса модернизации. Вы всегда можете использовать резервные копии, чтобы восстановить Ваши данные.

*33 Сделайте копию каталога данных Вашего сервера (C:\NOTES\DATA). Этим вы сохраните DESKTOP.DSK, все ID файлы (включая ID сервера и сертификатора), LOG.NSF, NAMES.NSF, MAIL.BOX, и любые другие общие адресные книги, расположенные на сервере.

34 Сделайте копию содержания любых каталогов или файлов данных связей (.DIR)

*35 Сделайте копию NOTES.INI сервера. Этот файл расположен в системном каталоге (например, C:\WINNT40).

36 Сделайте копию любых других баз данных Notes (.NSF) и шаблонов Notes (*.NTF).

Обратите внимание, что Domino автоматически модернизирует MAIL.BOX в формат R5 и заменит ее дизайн. Любые сообщения находящиеся в MAIL.BOX будут сохранены.

1.4.1.2 Запрещение функции Housekeeping для SMTP/MIME MTA.

Перед модернизацией R4 MTA сервера, запретите функцию Housekeeping для Вашего MTA сервера. Эта функция временно приостанавливает работу MTA и запустит задачу сжатия баз данных Compact по захваченным задачей MTA базам, после чего вновь запускает задачу MTA. Функция позволяет уплотнить базы входящей и исходящей почты (SMTP.BOX, SMTPIBWQ.NSF, SMTPOBWQ.NSF), которые постоянно находятся в открытом состоянии, при работе MTA.

Удостоверитесь, что Вы сохранили все файлы MTA сервера. Из клиента Lotus Notes откройте адресную книгу для домена MTA серверов. Выбирайте документ сервера, на котором установлен Ваш MTA и переведите документ в режим редактирования. Откройте секцию Internet Message Transfer Agent (SMTP MTA). Перейдите в поле Enable daily housekeeping и установите значение - Disable. Сохраните изменение и закройте документ сервера.

1.4.1.3 Остановка задачи Router.

Остановка задачи Router нужна для того, чтобы запретить передачу почтовых сообщений с других серверов на сервер с MTA.

*37 Удостоверитесь, что Вы запретили выполнение функции MTA Housekeeping.

*38 Перейдите на консоль Domino сервера и введите следующую строку для остановки задачи Router:

```
tell router quit
```

В ответ сервер покажет остановку задачи Router.

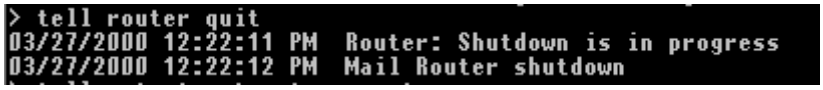


Рис. 1 Остановка задачи Router на консоли сервера Domino.

Остановка задачи Router запретит передачу сообщений в базу SMTP.BOX и позволит MTA освободить очередь на отправку сообщений. При этом будет продолжена обработка

сообщений, уже находящихся в этой базе данных. Поступающие сообщения в MAIL.BOX будут обработаны сервером после того, как Вы модернизируете его в R5.

1.4.1.4 Остановка подзадачи Inbound.

Остановка сессий входящих сообщений (Inbound), запрещает MTA получать сообщения по SMTP, адресованные Вашей организации, из интернета. Это позволит Вам очистить очереди подзадач Inbound и Outbound.

*39 Удостоверитесь, что Вы остановили Router.

*40 Введите на консоли сервера

```
tell smtpmta stop inbound transport
```

Сервер показывает открытые сессии Inbound и потом закрывает их:

Рис. 2 Остановка сессии Inbound на консоли сервера Domino.

1.4.1.5 Обработки сообщений в базе данных SMTP.BOX

После остановки задач Router и подзадачи Inbound, ждите, пока MTA обработает все сообщения в базе данных SMTP.BOX. Если имеются любые сообщения, ожидающие преобразования или ожидающие передачи, ждите, пока они не будут обработаны задачей доставки сообщений (DRT). Проверяйте обработку сообщения нажимая F9, или выбирайте из меню Вид – Обновить. Обработанные сообщения будут удаляться из вида. Как только вид будет пуст, или будет содержать только документы, отмеченные как не доставленные (мертвые), это значит что SMTP.BOX пуст.

Вам потребуется некоторое время, между обработкой сообщения и удалением сообщения из вида, из-за некоторой временной задержки DRT.

1.4.1.6 Очистка очереди сообщений на прием (Inbound Work Queue).

Очистка очереди Inbound Work Queue, подразумевает перемещение всех SMTP сообщений, адресованных получателям Вашей организации из базы Inbound Work Queue, в MAIL.BOX, после чего сообщения могут быть доставлены получателям. Сообщения, находящиеся в MAIL.BOX, будут доставлены после того, как Вы закончите модернизацию Вашего сервера и запустите его.

Иметься некоторая задержка между преобразованием сообщений и его удалением из вида, из-за некоторой временной задержки DRT.

1.4.1.7 Остановка SMTP/MIME MTA и сервера Domino.

После очистки всех сообщений MTA, можно закрыть и модернизировать сервер.

*41 Удостоверитесь, что Вы очистили очереди Inbound Work Queue.

*42 Переключитесь на консоль сервера Domino.

*43 Введите команду остановки сервера:

```
quit
```

*44 Закройте клиента Lotus Notes.

1.4.1.8 Проверка файла NOTES.INI для почтового интернет сервера.

После того, как Вы модернизируете Domino сервер до R5, Вы больше не нуждаетесь в команде load для SMTP/MIME MTA, так как R5 Router обеспечивает встроенную поддержку протокола SMTP с обработкой MIME. Удалите параметры Memory management, name lookup controls и debugging из NOTES.INI файла, так как задача Reporter больше не будет работать в R5. Удалите строки указанные ниже из файла конфигурации:

1. Удалите задачу Reporter и SMTPMTA из строки ServerTasks.

2. Если следующие строки существуют в файле, удалите их:

```
NSF_Buffer_PoolSize

NSF_DbCache_Maxentries

Server_Name_Lookup_Noupdate

Any debugging parameters
```

Обратите внимание. Функции задачи статистики, выполняемые задачей Reporter в R4, а так же статистический анализ, сейчас вместо задачи Reporter, использует задача Event. Она может контролировать базы данных, уведомляет администратора о достижениях установленных пороговых уровней. Кроме того, этот контроль может также регулироваться, чтобы автоматически уплотнять базы данных, которые достигают порогового значения.

1.4.1.9 Инсталляция программного обеспечение сервера Domino R5, на сервере MTA.

*45 Удостоверьтесь, что сохранили все важные Domino файлы.

*46 Удостоверится, что Вы проделали всем процедурам, для очистки сообщений из MTA.BOX.

*47 Установите программное обеспечение Domino R5 сервера. Если Вы устанавливаете Domino в тот же самый каталог, что и предыдущая версия, Вы не должны делать никаких изменений в конфигурации сервера. Если Вы устанавливаете Domino в новый каталог, программа установки попросит Вас сконфигурировать сервер.

*48 В течение установки программного обеспечения, выберите тип сервера, для которого Вы купили лицензию. Для многих организаций, это лицензия почтового Domino сервера.

*49 После инсталляции R5, запустите Domino сервер.

Обратите внимание. Программа инсталляции Domino сервера, не устанавливает клиента Domino Administrator. Вы должны выполнить вторую установку, используя программу

установки для этого клиента, чтобы установить Domino Administrator на компьютере сервера. Lotus рекомендует устанавливать этого клиента и администрировать сервер с отдельного компьютера.

1.4.1.10 Замена дизайна базы данных Public Address Book для почтового интернет сервера.

После модернизации - Domino сервер, Вам будет предложено модернизировать дизайн базы Public Address Book, на Domino Directory R5 (PUBNAMES.NTF). Новый шаблон Domino Directory работает с клиентом Domino Administrator, чтобы упростить администрирование сервера и его адресной книги. Domino Directory совместим, разработан и предназначен для использования в средах со смешанными версиями Domino серверов. Модернизируйте дизайн Вашей адресной книги в Domino Directory R5 с использованием нового шаблона после того, как Вы модернизируете программное обеспечение Вашего сервера. Когда Вы модернизируйте базу данных Domino Directory, уплотните базу данных и восстановите представления базы.

Перезапустите сервер. Проверьте консоль сервера, она не должна отображать никаких ошибок. Оставьте сервер командой с консоли сервера.

1.4.1.11 Уплотнение базы данных Domino Directory после замены дизайна.

Введите с командной строки, Вашей операционной системы, команду для уплотнения Вашей базы. В Microsoft Windows95/98/NT/2000 (Intel платформы), формат команды следующий:

```
Ncompact names.nsf
```

Обратите внимание. Уточните, как называется Ваш файл Domino Directory, если он имеет название не NAMES.NSF, в команде консоли укажите правильное имя файла для Domino Directory.

1.4.1.12 Восстановление представлений в Domino Directory.

Введите с командной строки, Вашей операционной системы команду восстановления видов ($ServerAccess) и ($Users) в Domino Directory.

В Microsoft Windows95/98/NT/2000 (Intel платформы), тип команды:

```
Nupdall names.nsf -t "($ServerAccess)" -r

Nupdall names.nsf -t "($Users)" -r
```

При восстановлении представлений ($ServerAccess) и ($Users), Domino Directory позволяют клиентам более быстрый доступ к серверу.

1.4.1.13 Восстановление представлений в базах данных на модернизированном Domino сервере.

Как только Domino сервер запущен, введите на консоли сервера:

```
Load updall
```

Эта команда восстановит представления баз данных, позволяя пользователям более быстрый доступу к Domino Directory и к другим базам данных на сервере.

1.4.1.14 Репликация нового дизайна Domino Directory на другие сервера.

Вы можете реплицировать дизайн Domino Directory на другие сервера Вашей организации, включая сервера версий R4 и R3. Domino Directory разработан и предназначен для использования смешанных версиях серверов.

Обратите внимание. Как только вы скопируете новый шаблон на другие сервера, Вы должны восстановить представления в Domino Directory на этих серверах. Представления восстанавливаются для шаблона R5 и на серверах R4/R3, при этом этот процесс занимает много времени. Lotus рекомендует Вам реплицировать шаблоны и восстанавливать представления для R5 серверов в выходные дни или в течение другого времени, когда сервера имеют минимальную загрузку.

1.4.1.15 Настройка конфигурации почтового интернет сервера.

Вы должны разрешить Вашей задаче Router передачу почты SMTP.

В документе Configuration Settings нужно разрешить функцию Server route mail с использованием SMTP. Документы Configuration Settings могут быть сконфигурированы для одного сервера, или для всех серверов в домене, или группы серверов. Отредактируйте документ Configuration Settings, который появится после модернизации сервера. Следует учитывать, что модификация воздействует на любые другие сервера, которые используют этот документ Configuration Settings. Если необходимо, создайте новый документ Configuration Settings для Вашего R5 почтового интернет сервера.

Например. Вы имеете почтовый сервер, Notes сервер, Firewall сервер. При этом только почтовому серверу будет разрешено передавать SMTP почту. Создайте два документа Configuration Settings. Один для почтового сервера, с разрешением маршрутизации почты SMTP. Второй для Notes и Firewall серверов без разрешения маршрутизации почты SMTP.

Обратите внимание, что Domino Directory для домена должен использовать шаблон R5, потому что назначения для встроенного SMTP появляются только в Domino Directory R5.

Если Вы не имеете документов Configuration Settings для Вашего Domino сервера, создайте их, используя процедуру ниже.

*50 Удостоверьтесь, что заменили дизайн Вашей базы Public Address Book на Domino Directory R5.

*51 Из клиента Domino Administrator, выбирайте закладку Настройки.

*52 Откройте секцию Сервер – Конфигурации.

*53 Выбирайте документ Конфигурации.

*54 Если Вы имеете документ Configuration Settings для своего сервера, выберите его и выбирайте кнопку Edit Configuration. Если его нет, выбирайте кнопку Add Configuration.

Если Вы создаете, новую конфигурацию, сделает следующее:

*55 Введите имя сервера в секции Basics.

*56 Выберите, Группу или конкретный сервер для кого эта конфигурация должна работать. Не выберите опцию - Use these settings as the default settings for all servers, если Вы

не хотите, чтобы любой из серверов использовал этот документ, для рассылки сообщений в интернет.

*57 Выбирайте закладку Router/SMTP.

*58 На закладке Basics, выбирайте кнопку выбора SMTP used when sending messages outside of the local Internet domain.

*59 Выбирайте - Enabled в окне и жмите кнопку OK.

*60 Если Ваша организация использует, промежуточный хост, введите в название или адрес IP в поле Relay host for messages leaving the local Internet domain.

*61 Сохраните созданный вами документ.

*62 Если Вы создали документ, он появляется в Вашем представлении.

1.4.1.16 Редактирование Server документ для почтового интернет сервера.

Редактируйте Server документ, для модернизированного сервера, чтобы разрешить задачу SMTP lister task, для разрешения inbound SMTP сессий. Это изменение разрешает серверу загружать SMTP Listener task, при запуске сервера.

Удостоверится, что Вы разрешили использование функции Server route outbound SMTP mail в документе Configuration Settings.

*63 Из клиента Domino Administrator, выбирайте закладку Настройки.

*64 Откройте секцию Сервер.

*65 Выбирайте представление - Все Документы Серверов.

*66 Дважды щелкните на документе сервера для почтового интернет сервера.

*67 Выбирайте кнопку Edit Server.

*68 На закладке Basics, выбирайте кнопку со стрелкой рядом с SMTP Listener task.

*69 Выбирайте значение – Enabled, затем – OK.

*70 Выбирайте кнопку сохранения документа.

*71 Закрывайте Domino Directory.

Примечание. Удаляйте SMTP routing из поля Routing Tasks, Server документа. Если вы оставите это поле не изменным , задача Router будет пытатся передать письмо в локальный домен R4 задаче SMTP MTA

1.4.2 Модернизация базы Administration Requests для MTA сервера.

Если вы модернизируете почтовый сервер - Domino, модернизируйте дизайн базы данных Administration Requests (ADMIN4.NSF), на шаблон R5 (ADMIN4.NTF). Если модернизация сервера произведена не на сервере администрирования, Вы не должны модернизировать шаблон, Вы просто реплицируете новый дизайн на все другие Domino сервера во время ближайший репликации.

1.4.3 Что нового в Domino Directory R5?

1.4.3.1 Использование профиля настройки для Domino Directory.

Когда Вы открываете Domino Directory после модернизации в первый раз, Вы увидите документ Domino Directory Profile. Профиль управляет характеристиками каталога сервера Domino.

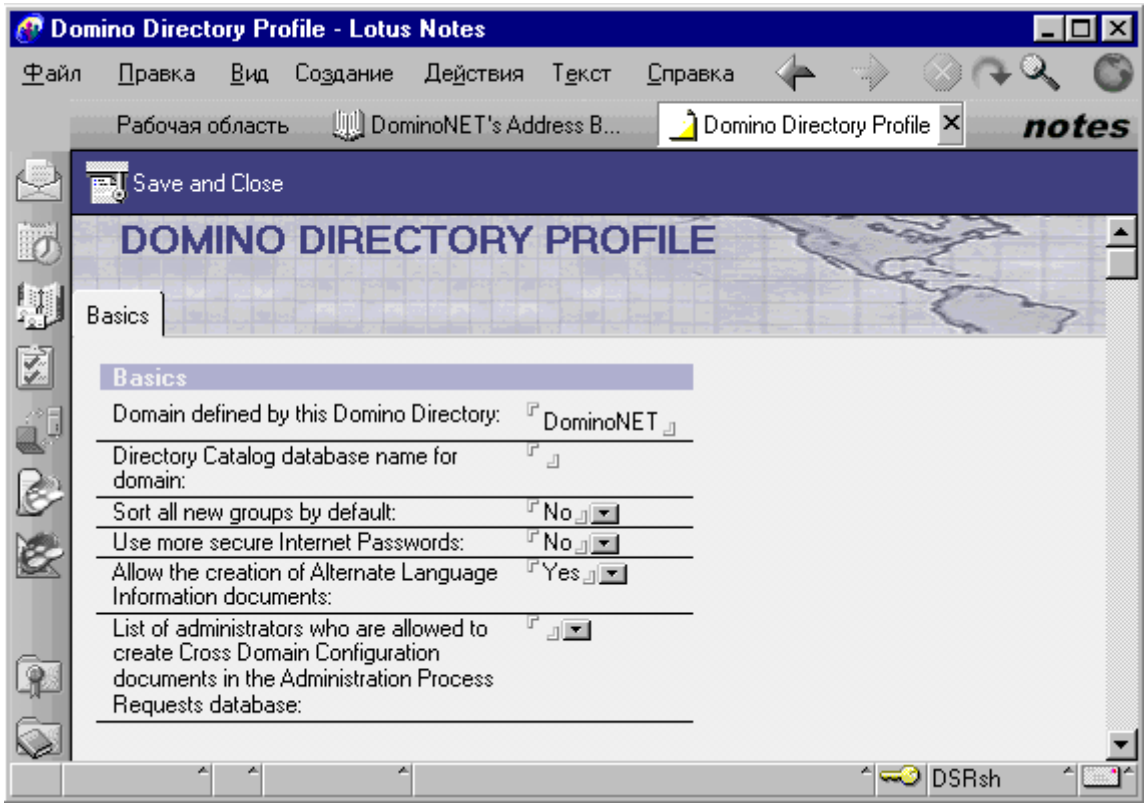


Рис. 3 Документ Domino Directory Profile - профиль Domino Directory.

1.4.3.2 Новые и удаленные представления в Domino Directory.

Domino Directory R5 содержит несколько новых представлений, но некоторые представления отсутствуют, которые имелись в Public Address Books R4.

Новые представления в Domino Directory R5.

*72 External Domain Network Information

*73 Holiday

*74 Web Configurations

Новые представления для пользователей в Domino Directory R5.

*75 Alternate Language Information

Новые скрытые представления в Domino Directory R5.

*76 $ExternalDomainNetworkAddress

*77 $ExternalDomainConfigurations

*78 $ExternalDomainServerConfigurations

*79 $Holidays

*80 $LDAPCN

*81 $LDAPG

*82 $LDAPHier

*83 $LDAPS

*84 $PeopleGroupsByLang

*85 $PeopleGroupsByCorpHier

*86 $PeopleGroupsByPhonetic

*87 $RegisterGroups

Представления R4, которые были удалены из Domino Directory R5.

*88 $ACLMONITOR

*89 $RepMonitors

*90 $Thresholds

*91 $NamesFieldLookup (when all clients are 4.5)

1.4.3.3 Новые формы в Domino Directory R5.

В Domino Directory R5 добавлено несколько форм.

*92 External Domain Network Information

*93 Configuration Settings (formerly Domain Configuration)

*94 Holiday

*95 (AlternateLanguageInformation)

*96 (ExternalDomainNetworkAddress)

*97 (FileProtection)

*98 (FileProtectionDialog)

*99 (Mapping)

*100 (VirtualServer)

*101 ($MessageSettings)

*102 (InternetMail)

1.4.4 Где находятся элементы конфигурирования серверов R4 и их аналоги в R5?

Документ Сервера R4 (Public Address Book).

Источник записей	**Где находится в R5**
Задача SMTP Mail Routing, поля Routing Tasks	Документ Configuration Settings: SMTP used when sending messages outside of the local Internet domain. Вы должны оставить значение SMTP Mail Routing в поле Routing Tasks, документа сервера, если сервер R4, а не-SMTP R5 сервер, маршрутизирует интернет почту в интернет.
General section – Fully qualified Internet host name	Документ сервера
General - Global domain name	Все R5 сервера используют все R5 документы типа Global domain документы, он не ищут ни какой определенный документ.
Control section – Poll for new messages every *X* minutes	Не используется в R5
Control - MTA work path	Не используется в R5
Control - Log level	Если сервер использует файл LOG.NSF – SMTP outbound, Router, SMTP inbound и SMTP задача оставляют записи в базе. Смотрите настройки переменных, для NOTES.INI, что бы настраивать детализацию этих записей.
Control - Enable daily housekeeping	Не используется в R5
Control - Perform daily housekeeping at	Не используется в R5
Conversion - header handling	Не используется в R5
Conversion - Attachment encoding method	Документ Configuration Settings – MIME - Conversion Options – Outbound
Conversion - Message content	Документ Configuration Settings – MIME – Conversion Options – Outbound
Conversion - Support return receipts	Документ Configuration Settings – MIME – Conversion Options – General – Return receipts
Conversion - Language parameters	Документ Configuration Settings – MIME – Basics и MIME – Settings by Character Set Groups
Conversion - Use character set detection routines	Документ Configuration Settings – MIME – Conversion Options – Inbound – Auto Detection, если сообщение не содержат информацию о character set information

Conversion - Message Typeface	Документ Configuration Settings – Conversion Options – MIME – Settings by Character Set groups
Conversion - Message Point Size	Документ Configuration Settings – Conversion Options – MIME – Settings by Character Set groups
Conversion - Outbound Macintosh message conversion	Документ Configuration Settings – Conversion Options – MIME – Advanced – Advanced Outbound Message Options – Macintosh attachment conversion
Inbound Configuration - Number of Processes	Не используется в R5
Outbound Configuration - Number of Processes	Не используется в R5
Outbound Configuration - Maximum outbound msg size	Документ Configuration Settings – Router/SMTP – Restrictions and Controls – Restrictions – Maximum message size
Transport Configuration - Host name mapping	Документ Configuration Settings - Router/SMTP – Basics – Host name lookup
Transport Configuration - Retry limit	Не используется в R5
Transport Configuration - Retry interval	Не используется в R5
Transport Configuration - Transfer mode	Не используется в R5

Документ Foreign SMTP Domain, из Public Address Book R4.

Источник записей	**Где находится в R5**
Allow mail only from domains	Документ Configuration Settings – Restrictions and Controls – Restrictions – Allow mail only from Notes domains
Deny mail from domains	Документ Configuration Settings – Restrictions and Controls – Restrictions – Deny mail from Notes domains

Messages addressed to [Internet domain] should be routed to [Domain name] or [Internet host]	Используется в R5 для маршрутизации почты интернет на Domino SMTP сервера, если все почтовые сервера могут маршрутизировать исходящую почту SMTP. Если Ваша организация использует только несколько SMTP серверов, при этом используется маршрутизация через R4 сервер, Вам придется продолжать использовать документы Foreign SMTP Domain и SMTP connection, для маршрутизации исходящей почты интернет для этих SMTP серверов.

Документ Global Domain из Public Address Book R4.

Источник записей	**Где находится в R5**
Global Domain документ	Все существующие документы могут выполнять маршрутизацию
Primary Internet domain (set in first Global Domain document in R4)	Документ Global Domain – Conversions – SMTP Address Conversion – Local primary Internet domain. R5 выбирает Primary Domain из первого документа, типа Global Domain.
Alternate Internet domain aliases (set in all other Global Domain documents in R4)	Документ Global Domain – Conversions – SMTP Address Conversion – Alternate Internet domain aliases (R5 выбирает aliases из всех документов Global Domain, за исключением первого)
Internet address lookup	Документ Configuration Settings – Router/SMTP – Basics – Address lookup. Если функция разрешена, R5 просматривает адреса в Domino Directory; если запрещено, Domino конвертирует Internet address.

Параметры из NOTES.INI файла сервера R4.

Источник записей	**Где находится в R5**
MailMaxThreads (максимальное число нитей передачи сообщений)	Документ Configuration Settings – Router/SMTP – Restrictions and Controls – Transfer Controls – Maximum transfer threads
MailDisablePriority (Установка равная 1, передача всей почты с приоритетом Normal, независимо от установленного приоритета)	Документ Configuration Settings – Router/SMTP – Advanced – Controls – Advanced Transfer Controls – Ignore message priority

MailLowPriorityTime (установка времени, для передачи почты с приоритетом Low)	Документ Configuration Settings – Router/SMTP – Restrictions and Controls – Transfer Controls – Low priority mail routing time range
Log_Mailrouting (контроль детализации маршрутизации почты)	Документ Configuration Settings – Router/SMTP – Advanced – Controls – Miscellaneous Controls section – Logging level
MailDynamicCostReset (число, как часто Router будет обнулять таблицу маршрутов, в случаи неудачного соединения)	Документ Configuration Settings – Router/SMTP – Advanced – Controls – Advanced Transfer Controls – Dynamic cost reset interval
MailEncryptIncoming (Вынуждает шифрование для всей доставляемой почты, независимо от установок в почтовых файлах)	Документ Configuration Settings – Router/SMTP – Restrictions and Controls – Delivery Controls – Encrypt all delivered mail
MailClusterFailover (разрешить доставлять почту на другой сервер член кластера, в случаи недоступности основного сервера)	Документ Configuration Settings – Router/SMTP – Advanced – Controls – Additional Controls – Cluster failover
SMTPMTA_IPPORT (порт SMTP)	Документ Server document – Ports – Internet Ports – Mail – Mail (SMTP Inbound) and Mail (SMTP Outbound) – TCP/IP port number
SMTPMTA_CONVERT_ORIGINATOR (просматривает адрес автора в Public Address Book)	Не используется в R5
SMTP_KEEP1MEANS1=X (заставить MTA обращаться к локальному домену, так же как и к остальным доменам)	Не используется в R5
SMTPMTA_DENIED_DOMAINS=*filename*, Имя файла в формате ASCII. Файл содержит имена доменов, с которых запрещено получать интернет почту.	Документ Configuration Settings – Restrictions and Controls – SMTP Inbound Controls и SMTP Outbound Controls sections
SMTPMTA_NO_INLINE_CONTENT_DISP =1 (Выключить поддержку RFC 1806. Убрать содержанья заголовка если заголовок в режиме inline)	Не используется в R5
SMTPMTA_TRACE_LEVEL=0x00000100 (enhanced tracing in log)	Не используется в R5

Документ SMTP Connection R4.

Источник записей	**Где находится в R5**

Relay host	Документ Configuration Settings – Router/SMTP – Basics - Relay host for messages leaving the local Internet domain. Вы должны также установить значение разрешено в поле SMTP used when sending messages outside of the local Internet domain, тогда все будет работать должным образом.

1.5 Как обновить программного обеспечения рабочей станции Notes R4 до версии R5?

Прежде всего, сохраните важные файлы клиента Notes. В случае если произойдет сбой в течение модернизации, или Вы столкнетесь с проблемами, Вы можете восстановить файлы из резервных копий.

Сохраните следующие файлы для каждого клиента Notes:

Файлы пользователя	**Место хранения файлов**
NOTES.INI (Файл конфигурации)	Системный каталог (для примера, C:\WIN95)
DESKTOP.DSK	Каталог данных Notes (для примера, C:\NOTES\DATA)
Персональная адресная книга (NAMES.NSF имя по умолчанию)	Каталог данных Notes (для примера, C:\NOTES\DATA)
ID файл пользователя (Для примера JSMITH.ID)	Каталог данных Notes (для примера, C:\NOTES\DATA)
Локальные базы данных (*.NSF)	Каталог данных Notes (для примера, C:\NOTES\DATA)
Локальные файлы, описывающие связи с внешними каталогами (directory links *.DIR)	Каталог данных Notes (для примера, C:\NOTES\DATA)
Шаблоны (*.NTF)	Каталог данных Notes (для примера, C:\NOTES\DATA)

Чтобы модернизировать Ваши рабочие станции клиентов до R5, Ваш Notes клиент должен иметь версию не ниже R4.1. Lotus рекомендует наращивать версии Вашей системы до самой последней, доступной Вам версии. Используйте для этого QMRs, которые доступны по адресу:

http://www.notes.net/qmrdown.nsf/

Пример. Если текущая версия клиента Notes у Вас R4.5, модернизируйте их до R4.5.7, установив соответствующие QMR и QMU.

1.5.1 Что нужно сделать перед модернизацией клиентов Notes R4?

Убедитесь, что все локальные базы данных Ваших клиентов используют формат R4. Если Вы имеете некоторые шаблоны в формате R3, например адресные книги или почтовые файлы, Вы должны модернизировать их, по крайней мере, до версии R4.1 перед переходом на R5.

Если Вы модернизируете клиентов R3 в R5, программа установки проигнорирует файл рабочего пространства DESKTOP.DSK и создает незаполненный набор закладок.

1.5.2 Как инсталлировать программного обеспечения Notes R5?

*103 Удостоверьтесь, что сохранили все важные файлы клиента Notes.

*104 Запустите программу установки SETUP.EXE, из дистрибутива клиента R5 и следуйте инструкциям на экране. Выбирайте тип клиента, для которого Вы купили лицензию. Укажите каталог для установки клиента, каталог в который была установлена рабочая станция Notes, предыдущей версии.

*105 Запустите рабочую станцию Notes. Notes модернизирует программное обеспечение автоматически, если Вы устанавливаете R5 в тот же самый каталог, что и предыдущая версия Notes. Если Вы устанавливаете R5 в другой каталог, Notes попросит Вас закончить процесс конфигурации. Если Вы устанавливаете Notes в различные каталоги, знайте, что программа установки размещает NOTES.INI файл в каталог данных Notes. В предыдущих версиях, программа установки помещала NOTES.INI в системный каталог операционной системы.

Обратите внимание, что Notes автоматически модернизирует Вашу персональную адресную книгу, с использованием дизайна R5. Если Вы имеете почтовые настройки, для интернет почты с использованием POP3, Notes преобразовывает Вашу запись в новый формат.

1.5.3 Что происходит с рабочим пространством R4, при обновлении рабочей станции до R5?

Notes R5 автоматически конвертирует Ваше рабочее пространство в закладки. Вы можете все еще получить доступ к рабочему пространство, если хотите - но новая навигационная модель делает этот ненужным.

Ваше рабочее пространство, конвертируется в кнопки-закладки, которые расположены на левой стороне экрана клиента.

Notes дает Вам следующие закладки первоначально:

Кнопки-закладки	**Описание**
Домашняя страница	Ваша домашняя страничка, с которой вы можете получить доступ почти ко всем наиболее важным функциям клиента, включая поиск в Web
Почта	Ваш почтовый ящик

Календарь	Календарь
Адресная книга	Персональная адресная книга
Задачи	Задачи
Репликатор	Закладка Репликатора.
Domino Administrator	Запуск клиента Domino Administrator.
Domino Designer	Запуск Domino Designer.
Избранные закладки	Ваши закладки и ссылки на различные документы и страницы
Базы данных	Базы данных организованные согласно Вашим старым закладкам, которые Вы использовали в рабочем пространстве
Дополнительные закладки	Закладки для поиска баз данных и Web страниц
Ссылки Internet Explorer	Закладки Избранного для Microsoft Internet Explorer
Ссылки Netscape Navigator	Закладки Избранного для Netscape Navigator

1.5.4 Какие изменения происходят в персональной адресной книге пользователя?

В персональной адресной книге R5 имеется множество новых форм, видов, подформ, агентов и библиотек программ, некоторые элементы дизайна удаленны.

Новые агенты в персональной адресной книге R5.

*106 Remove Profile

Новые формы в персональной адресной книге R5.

*107 Accounts

*108 International MIME Settings

*109 ($Internet/RAS Dial-Up Wizard)

*110 ($Notes Dial-Up Wizard)

Новые библиотеки скриптов в персональной адресной книге R5.

*111 RLAN Routines

*112 StackContainer

*113 Wizard

Новые подформы в персональной адресной книге R5.

*114 $CertifierExtensibleSchema

*115 $GroupExtensibleSchema

*116 $RLANotpp

Новые представления в персональной адресной книге R5.

*117 Advanced\Accounts

*118 Advanced\International MIME Settings

*119 ($Accounts)

*120 ($International MIME Settings)

*121 ($PeopleGroupsByLang)

*122 ($PeopleGroupsCorpHier)

Удалены представления из персональной адресной книги R5.

*123 ($NamesFieldLookup)

*124 ($ServersLookup)

1.5.5 Что происходит с базой данных Portfolio в Notes R5?

Базы данных Portfolio представлены в R5 как закладки интерфейса.

1.5.6 Можно ли модернизировать мой почтовый файл в формат R5, сразу после установки программного обеспечения Notes R5?

Не модернизируйте Ваш почтовый файл, с использованием шаблона R5, пока Ваш администратор Domino, не сообщит Вам, как сделать это, или модернизирует его сам, для Вас.

1.5.7 Что происходит с записями для интернет почты?

Notes R5, предоставляет Вам возможность создания записей, которые содержат информацию для доступа к почте POP3, IMAP и использования почты SMTP. Если Вы в R4 имели запись, на использование сервисов POP3, Notes, конвертирует эту информацию. Если Вы используете интернет почту, Notes создает SMTP запись для Вашего пользователя.

1.5.8 Меняются ли установки защиты рабочей станции, установленные по умолчанию?

Перед модернизацией Notes клиента, администратор домена может определить Administration Execution Control List (ECL) в Directory Domino. ECL устанавливает параметры безопасности по умолчанию для клиента Notes. Когда пользователь начинает работать с Notes, после модернизации его рабочего места, Notes определяет, к какой группе приложений относится пользователь, и что он может выполнять на клиенте Notes. Если группа не определена в ECL для клиента, Notes предупреждает пользователя об этом.

1.5.9 Как происходит синхронизация часового пояса и установка перехода на летнее время в Notes R5?

В клиенте Notes R5, операционная система синхронизирует временную зону и установки перехода на летнее время. Когда Вы запускаете Notes, клиент синхронизирует значения системы, чтобы соответствовать текущим настройкам Notes. В предыдущих версиях, Notes синхронизировал только время системы, которое могло быть не синхронизировано с установкой временной зоны системы.

Убедитесь, что временная зона и функция перехода на летнее время правильно установлены, в Вашей операционной системе.

Например. Если операционная система не имеет активизированной функции перехода на летнее время, и Вы вручную переводите часы, приведите в соответствие установки часового пояса и времени.

Изменение назначений на компьютерах Windows.

Установки часового пояса, даты перехода на летнее время, в документах Местоположения Notes равны установкам Windows системы. Если Вы переключаетесь на различные Местоположения, то эти установки модернизируют временную зону Windows и перехода на летнее время. Если Вы изменяете временную зону Windows или установки перехода на летнее время, в то время когда Notes запущен, Notes модернизирует назначения для текущего местоположения.

Когда Вы модернизируете R5 на компьютере Windows, Вы можете выбрать временную зону, если назначения временной зоны в одном из Ваших документов местоположения, не соответствуют назначениям системы Windows.

1.5.10 Возможно ли использование функций календаря и планирования для интернет почты в Notes R5?

В смешанной среде, с использованием маршрутизации Notes RPC и SMTP, Router сервера Domino автоматически перенаправляет, приглашения на встречи, напоминания, календарную информацию и информацию о планировании по протоколу Notes RPC, когда это возможно. Если Вы посылаете приглашение по SMTP, кому-либо в интернет – Notes преобразовывает его в текстовые строки.

Обратите внимание. Преобразование календаря и пунктов планирования в текст, когда сообщения передаются с использованием протокола SMTP, работает в R5 так же, как это делалось в версиях R4.5 и R4.6.

1.6 Могут ли существовать рабочие станции R4 и R5 на одном компьютере клиента?

Вопрос очень актуален, особенно в первый период внедрения R5 в организации. Здесь однозначного решения нет, каждый администратор решает эту задачу по-своему. Далее предлагается вариант решения, которым пользуюсь сам уже достаточно долго. Сразу скажу, что это не мое изобретение, нашел его описание в форуме “Вопрос ответ” и немного его подстроил для себя. В принципе его можно использовать и для серверов. Главный принцип построения логики заключается в том, что каталог запуска рабочей станции должен остаться неизменным, в нашем случае это C:\NOTES.

Далее излагается последовательность действий, которые необходимо сделать:

*125 Установите программное обеспечение, для первого клиента. В нашем случае это R4. Каталог для установки - по умолчанию C:\NOTES. Переносим файл NOTES.INI в каталог данных рабочей станции, обычно это C:\NOTES\DATA. В программном каталоге рабочей станции создаем текстовый файл с именем 1NOTES4.TXT, он нам понадобится немного позже. И последнее, что надо сделать, это средствами ОС переименовать каталог NOTES в NOTES4.

*126 Теперь беремся за вторую рабочую станцию – R5. Каталог для установки, по умолчанию C:\NOTES (Вот для чего мы временно переименовали каталог с рабочей станцией R4). Переносим файл NOTES.INI в каталог данных рабочей станции. В программном каталоге рабочей станции создаем текстовый файл с именем 1NOTES5.TXT. Иногда программа установки обнаруживает старый NOTES.INI и предлагает его переименовать в NOTES.000 – соглашайтесь, после завершения инсталляции верните файлу прежнее имя.

*127 Создаем два BAT-файла, для запуска наших рабочих станций. Определяем имена для них NOTES4.BAT и NOTES5.BAT. Файлы храним в корневом каталоге, например диска C:\. Далее привожу содержание команд файла NOTES4.BAT.

```
if exist c:\notes\1notes4.txt goto n4

if exist c:\notes\1notes5.txt goto n5

:n5

move c:\notes notes5
```

```
move c:\notes4 notes

:n4

c:\notes\notes.exe

echo Start Notes 4

:end
```

Логика всего вышеперечисленного очень проста. Для запуска рабочей станции версии R4 используется файл NOTES4.BAT. Если в каталоге C:\NOTES обнаружен файл 1NOTES4.TXT – значит, это каталог запуска действительно рабочей станции R4 – выполняется запуск рабочей станции. Если в каталоге C:\NOTES обнаружен файл 1NOTES5.TXT – значит это каталог запуска действительно рабочей станции R5. Программный каталог переименовывается в NOTES5, каталог NOTES4 переименовывается в NOTES и выполняется запуск рабочей станции.

Файл для запуска R5 содержит похожие строки и работает по такому же принципу, только для R5.

Вот такой принцип можно использовать для запуска рабочих станций, разных версий.

И ще одно замечание по этому поводу. Да, сосуществование двух клиентов на одной машине возможны, главная тонкость в том, что R4 клиент хранит Notes.ini в системной директории операционной системы, а R5 в текущей директории клиента.

Алгоритм поиска Notes.ini прост. При запуске рабочий станции проверяется текущая клиентская директория, если файл там не найден, проверяется системной директории операционной системы.

Итак, мы должны перенести notes.ini из системной директории OS в клиентскую директорию

Например :

Из \Winnt (если это NT либо WIN 2000) в \Notes

Далее можно преступать к инсталляции второго клиента R5 При проверке предыдущих версий Lotus Notes'а будет найдена старая версия Notes'а (R4) ответит отказам на предложения обновить версию ПО. И проинсталлировать новую версию в \Lotus\Notes.

Будет создан дополнительный Notes.ini для клиентского места версии R5.

1.7 Как в Notes R5, сделать так, чтобы при старте появлялось рабочая область, а не стартовая страница R5?

Выбирайте слева, на панели значков, пиктограмму Базы данных. Откройте окно свойств закладки Рабочая область. Выбирайте опцию - Сделать закладку домашней страницей.

1.8 Что такое QMRs/QMUs?

QMR и QMU – это так называемые ежеквартальные обновления и Update к ним (QMU), для серверов и рабочих станций Lotus. Выпускаются они довольно регулярно. В основном это обновления, в которых устраняются замеченные ошибки.

При установке очередного обновления, версия продукта повышается. Например, если Вы устанавливаете обновление 5.0 -> 5.0a на сервер, то при удачном завершении работы обновления и запуске сервера, на консоли сервера вместо версии 5.0, Вы увидите - 5.0a и т.д.

В настоящий момент доступны, и актуальны, обновления для версий R4 и R5. Более того, в настоящее время Lotus выпустил ряд дистрибутивов серверов, рабочих станций и обновлений к ним, с национальными интерфейсами. Доступен русский дистрибутив сервера R5, рабочей станции R5, а так же ежеквартальные обновления до версий 5.0.4a.

Программное обеспечение QMRs/QMUs, почти для всех языков, доступны по адресу:

http://www.notes.net/qmrdown.nsf/

1.8.1 После установки QMR или QMU в каталогах сервера и рабочей станции появились файлы с расширением *.IIB. Что это за файлы?

Действительно, после установки QMR или QMU в программных каталогах появляются файлы с расширением *.IIB. Причем некоторые из них имеют довольно внушительные размеры. Это резервные копии файлов, которые были заменены в процессе установки обновления.

Делается это для того, чтобы Вы могли восстановить предыдущую версию инсталляции, программного обеспечения. Для возвращения к предыдущей версии программного обеспечения, достаточно запустить программу обновления во второй раз. Инсталлятор определит, что он уже был запущен по Вашему каталогу программного обеспечения и, при наличии соответствующих резервных копий файлов, с расширением *.IIB - восстановит эти версии файлов.

Если вы не планируете возвращаться к предыдущим версиям серверов или рабочих станций, Вы можете удалить эти файлы, тем самым освободится немало места на жестком диске.

1.8.2 Что делать, если при установке QMR или QMU возникают ошибки, и процесс обновления останавливается?

Иногда, в процессе установки QMR или QMU возникают ошибки, и процесс выполнения обновления останавливается. Как правило пользователь получает окно предупреждения, аналогичное приведенному ниже.

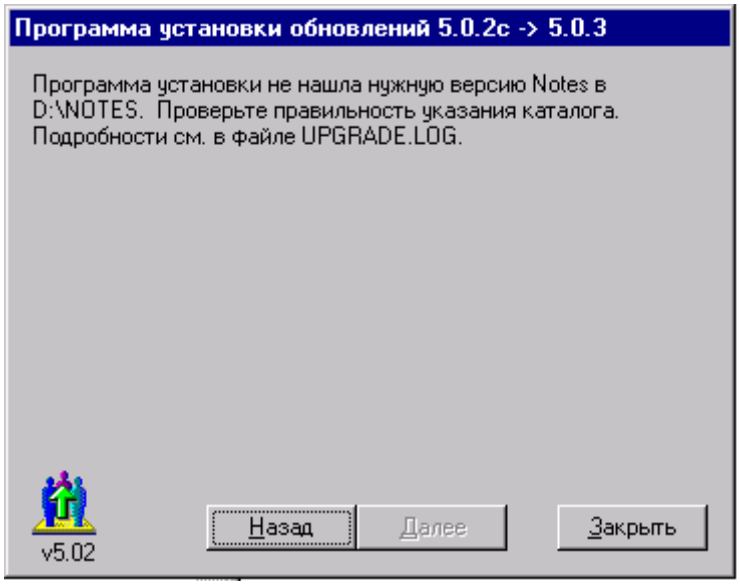


Рис. 4 Информационное окно с сообщением об ошибке, при запуске программного обеспечения обновления QMR или QMU.

Как правило, эти ошибки можно разделить на три категории:

*128 Проблемы с файлом программы обновления. Обычно возникает на первом этапе установки, когда программа пытается тестировать целостность дистрибутива. В таких случаях обычно проходится скачивать обновление заново. Ничего не поделаешь, файл программы обновления иногда скачивается с ошибками…

*129 Вторая проблема может быть связана с недостаточным количеством свободного места на диске сервера или рабочей станции. Как правило, об этой неприятности Вы можете прочитать в окне предупреждения, Вам будет указан минимальный размер необходимый для программы обновления. Очистите диск от ненужных файлов и запустите установку заново. Кстати, вы можете избавиться от файлов *.IIB, если не планируете их в дальнейшем использовать. Опыт показывает, что они занимают довольно приличное место на диске.

*130 Третья причина остановки обновления самая неприятная. Она связана с несоответствием контрольной суммы некоторых файлов, Вашего установленного дистрибутива. На первом этапе, программ обновления проверяет наличие и контрольные суммы файлов, которые (как я понимаю) будут обновлены в процессе модернизации программного обеспечения. Программа обновления всегда ведет протокол своей работы и записывает его в файл UPGRADE.LOG, который обычно находится в программном каталоге сервера или рабочей станции. Для выяснения причины остановки обновления просматриваем этот файл и выясняем причину по вине, которой произошла остановка.

Далее представлен фрагмент файла UPGRADE.LOG, с ошибкой в предпоследней строке, по вине которой и была прервана программа QMR:

```
Iris Incremental Installer v5.02 for W32Intel

Copyright (c) Iris Associates, Inc., 1994-1999.  All rights reserved.

Executable created 14:31:31 Sep 7 2000 for 5.0.2c Intl Server -> 5.0.3 Intl
Server.

Upgrade started at 17:46:44 Apr 03 2000 in D:\.
```

```
Using Notes program directory C:\NOTES

Using Notes data directory C:\NOTES\DATA

Identified Release 4.6.6c Intl Server.

File lsxbeerr.lss failed checksum. (Found 0xd2d65163, Expected 0x429b98fd)

Unable to verify release.
```

В большинстве случаев помогает замена файла, путем копирования его из дистрибутива. Если это, по каким то причинам невозможно, то действуем старыми “дедовскими” методами, по принципу “Нет файла – нет проблем”. Попробуйте перенести файл, с которым у вас возникли проблемы в другой, не-Notes каталог. Запустите программу обновления заново, проблема должна исчезнуть…

1.9 Как модернизировать базы данных и приложения в новый формат R5?

После модернизации Ваших Domino серверов и клиентов Notes, Вы можете приступать к модернизации Ваших баз данных.

Запустите Ваше приложение R4 без модификации на сервере R5. Попробуйте их перевести в новую структуру ODS R5. Некоторые известные проблемы несовместимости опубликованы далее. Проверите Ваши приложения на сервере R5, перед передачей баз данный в работу Вашим пользователям. Если Вы сталкиваетесь с проблемой, Вы можете посетить форум Lotus KnowledgeBase на Web-сервере

```
http://orionweb.lotus.com/basic.html.
```

Когда Вы планируете модернизировать шаблоны R5 и использовать новые возможности присущие R5, знайте, что R4 клиенты не смогут использовать эти возможности. Использование R5 шаблона и возможностей в смешанной среде серверов может причинить некоторые осложнения, если некоторые клиенты используют ранние версии Notes.

Lotus производил внутренние испытание, среди своих партнеров ISV и демонстрирует, что проблемы связанные с модернизацией приложений - несущественные. Однако Lotus настоятельно рекомендует проверить критические для предприятий приложения на сервере R5, перед передачей их в работу.

Имеются несколько способов для работы с базами данных и приложениями в среде R5:

*131 Модернизируйте сервера до версии R5, но оставьте базы данных в формате ODS R4 и используйте дизайн R4. Все клиенты смогут иметь доступ к этим базам данных без проблем, при этом не должно возникнуть никаких проблем с модернизацией.

*132 Модернизируйте сервера и базы данных до версии R5, но оставьте дизайн баз данных в формате R4. Все клиенты смогут получить доступ к базам данных без проблем. Вы не должны иметься никаких проблем с модернизацией. Вы сможете выполнять сжатие (Compact) баз данных в новом формате ODS.

*133 Модернизируйте сервера, формат баз данных, дизайн баз данных до версии R5

Клиенты R4 не смогут использовать все возможности R5. Вы будете должны заменить клиентов, чтобы использовать новые возможности новой версии. Уплотните базы данных в новом формате ODS, замените дизайн R4, на R5 и используйте новые R5 возможности.

1.9.1 Общие принципы модернизации баз данных в новый формат.

Перед модернизацией баз данных на сервере Domino R5, запустите задачу Fixup, для коррекции большинства ошибок, с которыми может столкнуться задача Compact в процессе преобразовании баз данных в новый формат

После модернизации, запустите задачу Updall –r, для восстановления представлений в базах данных. Эта операция существенно уменьшит время открытия представлений. Это особенно важно для баз данных, которые используются часто, или имеют большие представления.

1.9.2 Модернизация баз данных в формат R5.

Для выполнения преобразования баз данных в новый формат, используется задача Compact. Вы можете использовать ключ (-R) этой команды, чтобы сохранить базы в формате R4. Или изменить формат баз данных формата R5, обратно в формат ODS R4. Если вы не хотите преобразовывать некоторые базы данных в формат R5, и желаете оставить их в старом формате R4, переименуйте расширение этих файлов в *.NS4. Задача Compact будет игнорировать эти файлы при своей работе и оставит их в старом формате.

Ниже представлена процедура для преобразования Ваших данных в новый формат, при этом в свойствах баз данных вносится новая информация о ODS и ее версии:

*134 Модернизируйте сервер Domino до версии R5.

*135 Введите следующую команду на консоли сервер и нажмите клавишу ENTER.

```
load compact databaseName.nsf
```

где `databaseName.nsf` - имя файла базы данных, которую Вы желаете уплотнить в формат R5.

Выполнение преобразования формата баз данных с клиента Notes.

Если пользователь уплотняет базу данных с использованием клиента Notes R5 (например, из закладки Info, окна Свойств базы данных), сервер уплотняет базу данных для клиента. Таким образом, R5 Domino сервер уплотняет базы данных с использованием задачи Compact R5. Единственный способ предотвратить это состоит в том, чтобы переименовать расширения файлов баз данных R4 в *.NS4.

Обратите внимание. Формат файла с расширением *.NS4 является родным для Domino сервера R5 и не вызывает как правило никаких проблем при работе с данными.

1.9.3 Модернизация почтовых файлов пользователей.

Вы можете использовать специальную утилиту Convert, для преобразования почтовых файлов и автоматизировать процесс замены дизайна для группы файлов.

Убедитесь, что Вы заменили рабочие станции клиентов Notes R5, в противном случае пользователи не будет использовать возможности нового дизайна.

Процесс одновременной модернизации почтовых файлов должен проходить, когда пользователи не будут работать с ними - например, рано утром или в выходные. Уведомьте пользователей, что их почтовые файлы будут некоторое время недоступны, во время преобразования их в новый формат.

Если пользователи настроили свои почтовые файлы, проинструктируйте их, как сохранить эти настройки. Например, пользователь может сделать новую копию его почтового файла, в которую включается только дизайн базы данных. Это позволит пользователям обращаться и к измененному шаблону R4, и к новому почтовому шаблону R5. Во многих случаях, эти изменения не нужны, потому что новые возможности R5 используют те же самые функции. Пользователи, пробуют новый почтовый шаблон R5 без его изменения, чтобы определить то, какие изменения, они хотели бы сделать в нем.

*136 Запустите Domino сервер, на котором Вы хотите настроить почтовые файлы.

*137 Остановите Router командой с консоли сервера:

```
tell router quit
```

Остановка Router, останавливает движение почты Domino на время модернизации почтовых файлов пользователей. Почта, сохраненная в базе MAIL.BOX, остаются в ней до очередного запуска Router. Как только Вы модернизируете почтовые, файлы пользователей, загрузите задачу Router снова, она будет обрабатывать почту из MAIL.BOX.

*138 Загрузите утилиту преобразования Convert, для преобразования Ваших почтовых файлов. Ее синтаксис:

```
load convert [arguments]
```

*139 Как только Вы закончили преобразование почтовых файлов в формат R5, загрузите Router на Вашем сервере командой:

```
load router
```

*140 Информируйте пользователей о том, что Вы заменили дизайн их почтовых файлов. У них могут возникнуть вопросы о новых функциональных возможностях почтовых файлов R5. Если пользователи настроили свои почтовые файлы R4 до модернизации, проверьте их, используя дизайн R5, чтобы видеть, остается ли необходимые настройки в дизайне баз. Если это необходимо, пользователь или Ваш разработчик должен внести необходимые изменения непосредственно в R5 элементы дизайна.

Синтаксис и аргументы утилиты Convert, которые Вы можете использовать:

```
load convert [-r | -l | -f | -m] mailfilepath existingtemplatename
newtemplatefilename
```

Где:

-r конвертировать почтовые файлы из подкаталогов в указанном каталоге

-l создает текстовый список почтовых файлов (реплики файлов исключаются)

-f использовать текстовый файл со списком почтовых файлов, которые нужно модернизировать

-m конвертирует файл, или файлы для использования задачей IMAP

mailfilepath определяет полный путь к файлу или файлам, которые нужно модернизировать

existingtemplatename определяет имя шаблона дизайна, который нужно заменить

newtemplatefilename определяет новый шаблон для использования

Модернизация отдельного почтового файла.

Этот пример находит почтовую базу данных USER.NSF в подкаталоге \MAIL, каталога данных Notes. Утилита преобразования заменяет текущий почтовый шаблон - независимо от версии старого шаблона - на MAIL50.NTF, почтовый шаблон R5.

```
load convert mail\user.nsf * mail50.ntf
```

Модернизация всех почтовых файлов в каталоге.

Этот пример находит все базы данных расположенные в подкаталоге \MAIL, каталога данных Notes, которые используют шаблон StdR45Mail (R4.5x почтовый шаблон) и заменяет их шаблон дизайна на StdR50Mail (MAIL50.NTF).

```
load convert mail\*.nsf stdr45mail mail50.ntf
```

Модернизация всех почтовых баз данных в каталогах и подкаталогах.

Этот пример находит все базы данных расположенные в подкаталоге \MAIL, каталога данных Notes и во всех подкаталогах, каталога \MAIL (например, C:\NOTES\DATA\MAIL\GROUP1, C:\NOTES\DATA\MAIL\GROUP2, или C:\NOTES\DATA\MAIL\GROUP3) и модернизирует их с использованием почтового шаблона R5, MAIL50.NTF.

```
load convert -r mail\*.nsf * mail50.ntf
```

Создание текстового файла, который будет содержать список всех баз данных в каталоге \mail

Вы можете использовать утилиту преобразования почтовых файлов, чтобы создать текстовый файл, который будет содержать список всех первичных почтовых баз данных на Вашем сервере. В список не вносятся реплики почтовых баз данных, только первичные копии.

Пример создает текстовый файл, MAILLIST.TXT, в каталоге C:\TEMP. MAILLIST.TXT содержит список первичных почтовых баз данных на сервере, но исключает реплики. После того, как Вы создали текстовый файл, Вы можете использовать его, для модернизации почтовых баз данных, внесенных в этот список.

```
load convert -l c:\temp\maillist.txt
```

Модернизация всех почтовых файлов, имена которых перечислены в текстовом файле.

Из текстового файла MAILLIST.TXT берется список почтовых баз данных, которые Вы хотите модернизировать, который сохранен в каталоге C:\TEMP. Утилита определяет, используют ли базы данных имя шаблона дизайна, которое соответствует маске STD* (например StdR4Mail) и заменяет их шаблоном StdR50Mail (MAIL50.NTF).

```
load convert -f c:\temp\maillist.txt std* mail50.ntf
```

Преобразование почтовых файлов для использования задачей IMAP.

Когда Вы решаете использовать почтовый файл Notes с задачей IMAP, запустите утилиту преобразования почтовых файлов с ключом (-m). Этот пример находит почтовую базу данных USER.NSF в подкаталоге \MAIL и преобразовывает его для использования задачей IMAP.

```
load convert -m mail\user.nsf
```

Обратите внимание, когда Вы используете символ маски (*), для определения множества файлов, убедитесь, что все базы данных в выбранном каталоге являются почтовыми базами. Когда Вы используете символы (*), Domino заменяет дизайн всех баз данных попадающих в отбор по маске. Если Вы заменили по ошибке дизайн не почтовой базы, замените дизайн обратно. Для этого используйте соответствующий шаблон, чтобы восстановить дизайн. Вы можете делать это с помощью утилиты преобразования, определяя базу данных, которой Вы хотите восстановить первоначальный дизайн и определяя правильный шаблон.

1.9.4 Замена шаблонов на новые версии R5.

Domino R5 автоматически не модернизирует дизайн баз данных до R5. Например, когда задача Design запускается, она не модернизирует почтовые файлы R4 с использованием шаблона R5. Это позволяет Вам выбирать, когда модернизировать дизайн для Ваших почтовых баз.

Шаблоны для почтовых баз R5 на сервере R4.

Не размещайте почтовые базы R5 на серверах R4. Шаблоны R5 содержит новые функции, которые требуют наличие сервера R5, чтобы работать должным образом.

Запрещение репликации шаблонов между серверами R5 и R4.

Если Вы имеете почтовые файлы на сервере R5, с шаблонами R5, и Вы должны реплицировать эти файла на сервер R4, с шаблонами R4. Вы должны запретить репликацию дизайна для этих почтовых файлов. Для запрещения репликаций дизайна между серверами, сделайте следующее, для каждого почтового файла:

*141 Откройте реплику почтовой базы данных, для которой Вы хотите запретить репликацию дизайна.

*142 Выбирайте из меню Файл – Репликация – Настройка.

*143 Выбирайте закладку – Дополнительно.

Рис. 5 Закладка Дополнитено, в окне свойств базы данных.

*144 В секции Реплицировать входящие, уберите отметки - Формы, представления и т.д. и - Агенты.

*145 Выбирайте - OK.

*146 Удостоверитесь, что Вы сделали это для каждой реплики базы данных, которой Вы хотите запретить репликацию дизайна.

Обратите внимание, что эта процедура не работает для кластерной репликации!

1.9.5 Модернизация приложений для Web.

Элементы дизайна, с неподдерживаемыми формулами, в Domino версии 4.5 скрывались автоматически при отображении через Web. Теперь Вы можете показывать их, если Вы

выбираете опцию Web: использовать JavaScript при создании страниц, в свойствах базы данных. С выбранной опцией, Domino не проверяет ссылки или формулы кнопок перед использованием JavaScript, для воспроизведения страницы. Пользователи Web видят теперь все кнопки действий и ссылки, которые содержат команды и функции, которые не поддерживаются в приложениях Web.

Проверьте все формулы в ссылках. Удостоверитесь, что эти формулы настроены правильно и работают после того, как пользователь щелкает на ссылках. Замените в R4.5 функции Attachment Fields на Web Element - File Upload Controls, если Вы устанавливаете - Web: использовать JavaScript при создании страниц. Web: использовать JavaScript при создании страниц установка, не выполняет команду ([EditInsertFileAttachment]).

Web: использовать JavaScript при создании страниц установка, может вызвать неожиданные результаты, потому что работа функции URL в R5 отличается того, что было в R4.5.

1.9.6 Использование шаблонов для Web со старыми браузерами.

Web шаблоны по умолчанию, которые поставляются с R5, не поддерживают браузеры, которые не поддерживают стандарт JavaScript 1.1. Если браузер не поддерживающий JavaScript 1.1 пытается получить доступу к одному из шаблонов Web версии R5, он получит сообщение об ошибке. R5 включает специальные шаблоны Web, разработанные и предназначенные для работы со “старыми” браузерами.

Приложения, разработанные для использования в Web, ожидают обращения браузеров, которые не поддерживают JavaScript 1.1 стандарт и отображают сообщение, что возможности JavaScript не поддерживаются данными браузерами. Это - ограничение браузеров, а не проблема с шаблонами или приложениями. Domino и приложения Domino поддерживает все браузеры, но некоторых из инструментов, которые Вы можете использовать с Domino (например, JavaScript) не поддерживаются всеми браузерами.

R5 шаблоны Web, работает со следующими браузерами:

*147 Microsoft Internet Explorer 4.x

*148 Netscape Communicator 4.x

*149 Netscape Navigator 3.x

Если Вы разрабатываете приложения, к которым нужно иметь доступ через браузер, не поддерживающий стандарт JavaScript 1.1, но хотите использовать R5 шаблоны Web, убедитесь, что использовали специальные шаблоны Web разработанные для “старых” браузеров.

1.9.7 Замена дизайна базы данных Библиотека документов.

Когда Вы заменяете дизайн базы данных библиотеки документов R4.x или R4.6, на шаблон R5 (Doc Library Notes and Web), Запустите агента Upgrade Doclib R4 Documents to New Design в базе данных перед открытием любого из документа из преобразованной базы данных.

*150 Откройте базу данных, после замены шаблона.

*151 Выбирайте меню - Действия, а затем запустите агента Upgrade Doclib R4 Documents to New Design.

Если Вы не сделаете этого, Вы получите сообщение об ошибке, когда попытаетесь открыть документ или вид, они правильно не будут показывать статус документа.

1.9.8 Сохранение баз данных в формате R4.

Любой клиент Notes может получить доступ к базе данных на Domino сервере, независимо от версии клиентской части или версии сервера. Однако клиенты более старых версий Notes не могут использовать новые возможности баз данных более поздних версий. Например, клиент R4 Notes может получить доступ к базе данных R5 на Domino сервере, но не сможет использовать всех возможностей базы данных R5.

Если база данных сохранена на локальном диске клиента, только клиенты той же самой версии клиентской части Notes, могут получить доступ к ней. Например, к базе данных формата R4 можно обращаться локально клиентом R4 или R5, но не R3 клиентом.

Domino сервера могут хранить приложения в их родном формате и более ранних версиях. Например, сервер R4 может хранить базы в формате R4 и R3, но не в формате R5.

Чтобы создавать приложения формата R5, к которым могли бы получить доступ клиенты R4, и сохранялась бы возможность хранения этих приложений на серверах R4, нужно давать файлам баз расширение *.NS4. Используйте для этой цели, средства операционной системы, перед уплотнением баз данных в формате R5 ODS или сделайте новую реплику базы данных, с использованием расширения для файла *.NS4.

Обратите внимание, если R5 клиент уплотняет локальную реплику базы данных R4, переведя ее в формат R5 - к ней нельзя будет обращаться локально клиентом R4.

Вы можете всегда вернуть свои приложения к их более ранней версии ODS, используя ключ (-r) при выполнении утилиты Compact, или создавая новую реплику или копию базы данных в формате R4.

Возвращение баз данных из формата R5 в формат R4, с использованием утилиты Compact.

Перейдите на консоль Domino сервера и введите команду:

```
load compact databaseName.nsf -r
```

где `databaseName.nsf` - имя файла базы данных, которой хотите понизить версию до R4. Domino уплотнит базу данных в формат ODS R4.

1.9.9 Использование функции Transaction logging в Domino R5.

Когда Вы модернизируете сервер приложений и Ваши приложения и базы данных до R5, Вы можете использовать новую функцию Transaction logging. Убедитесь, что сделали следующее:

*152 Определили, диск сервера с достаточным количеством свободного места, для восстановления Видов, проверьте переменную View_Rebuild_Dir в NOTES.INI. По умолчанию, эта переменная установлена в системный каталог c:\temp. Дополнительный диск содержит, временные файлы для восстановления представления. Большой диск позволяет быстрее восстанавливать и оптимизировать представления. С использованием этой функции, восстановление происходит в целых пять раз быстрее, чем в R4. Размер диска, необходимого для восстановления представлений, зависит от размера представлений, которые Вы восстанавливаете.

*153 Используйте выделенный диск, чтобы хранить LOG файлы и Transaction logging. Местоположение по умолчанию для этих файлов - LOGDIR каталог в каталоге данных сервера. Выделенный диск позволяет, делать записи быстрее в LOG файл. LOG файл требует, по крайней мере, 200 МБ дискового пространства. Lotus рекомендует использовать диск не менее 1GB. Использование “зеркалированого” диска даже лучше чем единственный диск для восстановления данных.

Используйте утилиту резервного копирования, для сохранения файла Transaction logging, для максимального восстановления данных, в случае разрушения данных или ошибок. Выполняйте ежедневное сохранение и архивирование файла Transaction logging.

2 Администрирование серверов Lotus Domino.

2.1 Какие существуют особенности в администрировании смешанной среды серверов Lotus Domino?

2.1.1 Особенности маршрутизации интернет почты в смешанной среде серверов.

Router сервера Domino R5 может маршрутизировать интернет почту формата MIME и с использованием протокола Notes RPC. Router сервера R4 не поддерживают формат MIME или SMTP маршрутизацию, он используют для этого агента MTA, для выполнения этой задачи.

Вы можете управлять тем, как Router сервера R5 передает сообщения MIME на сервера R4, если он не имеет доступ на сервер, к документу Person пользователя. Router сервера R5 конвертирует сообщение MIME, в формат Notes, или конвертирует сообщение MIME в Notes формат и формирует также присоединенный файл, который содержит оригинальное сообщение MIME. Вы можете определять для Вашей системы метод преобразования MIME. Установка по умолчанию конвертирует сообщение MIME в формат Notes, без применения присоединенного файла.

Если Вы выбираете установку, при которой сообщение будет конвертироваться в формат Notes и будет формироваться присоединенный файл, то Domino будет сохранять полностью оригинальное сообщения в присоединенном файле. При этом если клиент попытается получить доступ, к сообщению используя почтового клиента интернет, Domino будет посылать ему сообщение формате MIME, из присоединенного файла. Сервер R4 хранит сообщения MIME в формате Notes, с использованием присоединенного MIME файла. При выборе такого способа хранения сообщений, в смешанной среде, требуется примерно вдвое больше места на диске сервера для хранения почты.

2.1.1.1 Конвертирование интернет почты в смешанных средах серверов.

При использовании смешанной среды серверов, сообщения формата MIME перед посылкой его в интернет, иногда требует преобразования. Преобразование выполняется при использовании следующих сценариев:

1. **Когда Вы используете сервер R4 с агентом SMTP/MIME MTA, для отправки и получения почты из интернет.**

Для отправки почты интернет, агент MTA конвертирует исходящие сообщения Notes в формат MIME и рассылает их с использованием протокола SMTP. Входящие сообщения интернет формата MIME конвертируются в формат Notes (с или без присоединенного файла MIME), а Router пересылает их с использованием Notes RPC. Агент R4 MTA конвертирует и пересылает сообщения, основываясь на данных документа Person получателя, в случае если MTA может получить доступ к этим документам. Проверьте установки поля Internet Message Storage в Person документах пользователей. В зависимости от выбранных Вами значений в этом поля, агент MTA сервера R4 будет выполнять или не выполнять преобразование:

*154 **Notes only** – Агент MTA конвертирует сообщение в формат Notes и пересылает его получателю.

*155 **Internet only** – Агент MTA сохранит MIME в присоединенном файле и пересылает его.

*156 **Notes and Internet** – Агент MTA конвертирует сообщение в формат Notes, сохраняет MIME в присоединенном файле, затем передает его.

2. Когда Router R5 доставляет сообщение в почтовый файл получателя.

Router проверяет поле Format preference for incoming mail, в Person документе получателя, из Domino Directory R5. Он определяет предпочтение интернет почты для получателя.

a) Если сообщение находится в формате Notes и

*157 значение поля - **Prefers Notes Rich Text** , Router доставляет сообщение.

*158 значение поля - **Prefers MIME** , Router конвертирует сообщение в MIME и доставляет MIME сообщение.

*159 значение поля - **No Preference** , Router доставляет сообщение.

Обратите внимание. Если значение поля - **No Preference**, Router доставляет сообщение в формате Notes, для того чтобы клиенты Notes клиенты R4 и R5 могли читать сообщение. IMAP и POP3 серверные задачи могут конвертировать сообщения в MIME, для клиентов интернет.

b) Если сообщение находится в формате MIME и

*160 значение поля - **Prefers Notes Rich Text**, Router конвертирует сообщение в формат Notes, форматирует и доставляет сообщение в формате Notes.

Обратите внимание. Если на сервере установлена переменная **MailDeliverCDorMime=1** в файле NOTES.INI, то Router не будет конвертировать сообщение, и доставит его в формате MIME.

*161 значение поля - **Prefer MIME**, Router доставляет сообщение.

*162 значение поля - **No Preference**, Router доставляет сообщение.

Если сообщение зашифровано (S/MIME формат), Router создает присоединенный файл содержащий S/MIME и создает сообщение Notes формата, объясняющее что сообщение зашифровано и не может быть преобразовано в формат Notes.

Обратите внимание. Если значение поля имеет значение - **No Preference**, Router доставляет сообщение в MIME, потому что R5 клиент и интернет клиент могут читать сообщение формата MIME. Router R5 конвертирует сообщение MIME для клиентов, которые не могут читать MIME.

3. Когда Router R5 сервера передает сообщение на сервер R4.

Если сообщение находится в формате Notes, Router R5 просто передает сообщение на сервер R4.

Если сообщение находится в формате MIME, Router пробует получить доступ к документу Person получателя. Если он имеет доступ к этому документу, он проверяет значение поля Internet Message Storage для R4, или Format preference for incoming mail для R5.

*163 Если в поле установлено значение - **Notes only** для R4, или **Prefers Rich Text Notes** для R5, Router конвертирует сообщение в формат Notes и передает сообщение в формате Notes.

*164 Если в поле установлено значение - **Internet only** для R4, или **Prefers MIME** для R5, Router сохраняет сообщение MIME в присоединенном файле и передает сообщение.

*165 Если в поле установлено значение - **Notes and Internet** для R4, или **No Preference** для R5, Router конвертирует сообщение в формат Notes, сохраняет оригинальное сообщения MIME в присоединенном файле и передает сообщение в формате Notes с присоединением MIME.

*166 Если сообщение зашифровано (S/MIME формат), Router создает присоединенный файл, содержащий сообщение S/MIME и создает сообщение Notes формата, объясняющее что сообщение зашифровано и не может быть преобразовано в формат Notes.

> **Обратите внимание.** Если на сервере установлена переменная **MailDeliverCDandMime=1** в NOTES.INI, Router конвертирует сообщение в Notes формат и добавляет в присоединенный файл, оригинальное MIME сообщение.

Если Router не может получить доступ к Person документу получателя, например если получатель находится в другом домене, или Router не может получить доступ к Domino Directory домена, то, по умолчанию Router конвертирует сообщения MIME в формат Notes и передает их. Вы можете управлять процессом конвертирования, настраивая поведение Вашего Router.

4. Когда Router R5 посылает почту по SMTP.

Если Router R5 должен послать сообщение в формате Notes с использованием протокола SMTP, он конвертирует это сообщение в MIME.

Обратите внимание. Что Агент SMTP/MIME MTA R4 поддерживает режим - Encapsulation. Режим, который помещает Notes-информацию в присоединенный файл, который мог бы быть преобразован назад в Notes другим агентом MTA R4. Router R5 этой функции не поддерживает, но сохраняет данные Notes другим методом так, чтобы любой Router R5 мог бы конвертировать информацию в формат Notes.

И еще одно замечание. Если к вам пришло письмо с прикрепленным файлом с мнением ENCAP2.OND это и есть инкапсулированное Router R4 письмо. Открепите его , переименуйте “*.nsf” и причтите письмо вложенное в эту базу.

5. Когда сервер R5 реплицирует данные с сервера R4.

Когда сервер R5 реплицирует, базы данных, которые содержат MIME на сервер R4. Например, если почтовый файл находится на сервере R5 и реплицируется на сервер R4, сообщения формата MIME в базе данных сервера R5, сервер Domino конвертируют MIME в формат Notes.

6. Когда клиент Notes R5 создает сообщение MIME и посылает его, через сервер Domino R4 на почтовый сервер пользователя R4.

Клиент R5 конвертирует сообщение из MIME в формат Notes и передает его на Domino сервер. Если в файле NOTES.INI на клиенте R5 установлена переменная **MailTransferCDandMIME=1** клиент Notes всегда конвертирует сообщение в формат Notes и добавляет присоединенный файл, содержащий оригинальное сообщение MIME.

Если сообщение зашифровано (S/MIME формат), Router создает присоединенный файл, содержащий оригинальное сообщение S/MIME и создает сообщение формата Notes, объясняющее что сообщение зашифровано и не может быть преобразовано в формат Notes.

IMAP и POP3 задачи сервера могут конвертировать сообщения формата Notes в MIME, чтобы посылать сообщения клиентам POP3 и IMAP.

2.1.2 Шифрованные сообщения в смешанных средах серверов.

Клиенты и сервера версий R4 не могут читать сообщения MIME, таким образом, сервер Domino R5 должен конвертировать сообщение MIME в документ Notes, с присоединенным оригинальным сообщением MIME и перенаправлять его на сервера версий R4. Domino сервер не может конвертировать зашифрованные MIME сообщения (S/MIME). Таким образом, когда S/MIME сообщение передается на сервер R4, Domino R5 конвертирует сообщение в присоединенный файл, содержащий S/MIME, генерирует сообщение формата Notes, предупреждающее, что сообщение является зашифрованным MIME и не может читаться этой версией программного обеспечения. Но это преобразование позволяет клиента IMAP, POP3 и R5 получать шифрованную почту MIME, которая передается с сервера R5 на сервер R4, или на другой сервер R5, без потерь и разрушения зашифрованной подписи.

2.1.3 Использование функции Message Tracking в смешанных средах серверов.

Используя функцию Message Tracking, администраторы могут отслеживать прохождение сообщений между серверами R5, на которых вы разрешили функцию Message Tracking. Если сообщение было передано на сервер ниже R5 или на Third-Party сервер, Вы больше не сможете следить за сообщениями с использованием Tracking Center.

Обратите внимание, что информация Message Tracking не доставляет сообщения, которые приходят в домен Domino из других источников, типа Third-Party почтового сервера.

Пользователи с почтовыми файлами формата R5 могут отслеживать прохождения сообщений, которые проходят через сервера, версии которых ниже R5 и Third-Party сервера, если эти сервера поддерживают запросы типа Message Tracking. Domino только возвращает информацию Message Tracking от серверов R5, на которых разрешена функция Message Tracking. Если Third-Party сервера не поддерживает эти поля, сообщения не может быть отслежены через эти сервера.

2.1.4 Использование шаблона Domino Directory R5 в смешанной среде серверов.

Шаблон Domino Directory R5 разработан и предназначен для использования в смешанных средах. После модернизации Вашего первого сервера до R5, Вы можете реплицировать новый дизайн на другие сервера Вашей организации. Новый шаблон разработан для совместимости с версиями серверов R4 и даже с серверами R3.

Вы должны модернизировать Domino сервера R4 в Вашей среде на самую последнюю версию R4, перед модернизацией их до R5. Например, в смешанной среде R4 и R5 серверов, Вы должны модернизировать R4 сервера от 4.6 до 4.6.2. Когда Вы переходите на R5, Domino спрашивает, хотите ли вы заменить дизайн базы данных Public Address Book. Если Ваш 4.6 сервер используют шаблон Domino Directory R5 (как рекомендуется) и Вы выбираете – Да. Domino перезаписывает шаблон Domino Directory R5 поверх старого шаблона R4.

2.1.5 Работа сервиса LDAP в смешанных средах серверов.

Как только Вы модернизируете Вашу адресную книгу Public Address Book в Domino Directory R5, Вы должны модернизировать Ваши Domino сервера, на которых запушен

сервис LDAP, по крайней мере, до версии R4.6.3. После этого, сервера должным работать должным образом с запросами LDAP и возвращать правильно запрашиваемую информацию. Directory Domino использует поле Address Internet, чтобы отвечать на запросы LDAP. Более ранние версии серверов не поддерживают эти функции.

2.1.6 Особенности использования кластера серверов в смешанных средах.

В смешанном кластере серверов R4/R5, пользователи не могут иметь почтовый файл формата R5. Почтовый шаблон R5 на серверах R4 не работает должным образом. Если Вы имеете смешанный кластер серверов с почтовыми файлами пользователей, Вам придется использовать дизайн R4 для почтовых файлов. Это необходимо, потому что кластерный репликатор игнорирует формулы выборочной репликации. Тем самым Вы не сможете предотвратить репликации дизайна почтовый файлов.

2.1.7 Идентификация пользователей Web сервером в смешанных средах серверов.

Сервер R5 дает Вам более мощный контроль для идентификации пользователей работающих через Web, с сервером. На закладке безопасности (Security), Server документа, доступны две опции для опции Web server authentication:

*167 More name variations with lower security.

*168 Fewer name variations with higher security.

Выбирайте значение More name variations with lower security, если хотите, чтобы пользователи опознавались, как это делалось в версиях серверов R4.6x - пользователи могут обращаться к серверу любым из следующих имен пользователя:

*169 **Last name only** - фамилия

*170 **First name only** - имя

*171 **Shortname** - короткое имя

*172 **Common name** - обычное имя

*173 **Full hierarchical name** - полное иерархическое имя

*174 **Any alias in the User name field** - любой алиас в поле пользователя

Эти установки идентификации, используют скрытый Вид ($Users) в Domino Directory и Public Address Book. Эта опция установлена по умолчанию.

Если Вы выбираете вторую опцию Fewer name variations with higher security, пользователи могут входить на сервер, вводя следующие данные:

*175 **Full hierarchical name** - полное иерархическое имя

*176 **Common name** - обычное Имя

*177 **Any alias in the User name field** - любой псевдоним в поле пользователя

Эти установки используют скрытый Вид ($LDAPCN) из Domino Directory.

Обратите внимание. Вы можете выбирать эту опцию только, если все Domino Directories используют для поиска HTTP дизайн R5.

2.2 Какие существуют конфигураций систем, построенные на основе Lotus Domino серверов?

Для наглядности описания существующих конфигураций систем, мы возьмем некую вымышленную корпорацию Acme, и будем описывать, как администраторы системы Acme настраивают Lotus® Domino™ в пределах своей организации. Эта корпорация не существует в реальности, примеры возможных конфигураций систем Вы не должны рассматривать как реальное руководство к действию, мы рассмотрим краткий обзор процесса конфигурации системы.

2.2.1 Что такое иерархическая схема имен организации и для чего она нужна?

Прежде, чем Вы установите первый сервер, Вы должны спланировать иерархическую схему имен пользователей и серверов. Иерархическая схема имен - краеугольный камень Domino безопасности, планирование схемы - критическая задача для всей системы.

Иерархическое имя состоит из одного имени организации или большего количества орг. единиц. Вы можете определить, могут ли пользователи и сервера в различных организациях и орг. единицах, связываться друг с другом.

Маленькая компания могла бы иметь организацию с только одним уровнем орг. единиц - например:

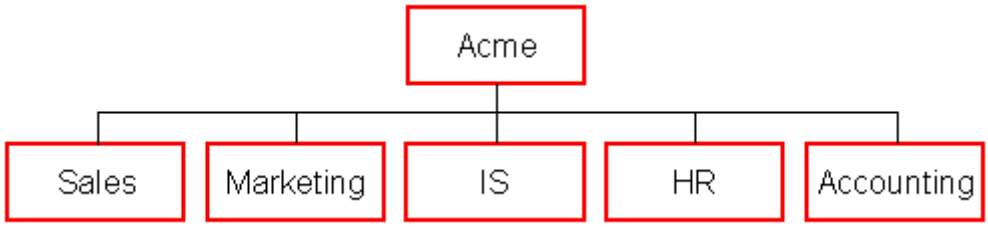


Рис. 6 Пример дерева сертификатов для маленькой организации.

Большая компания могла бы иметь несколько уровней орг. единиц - например:

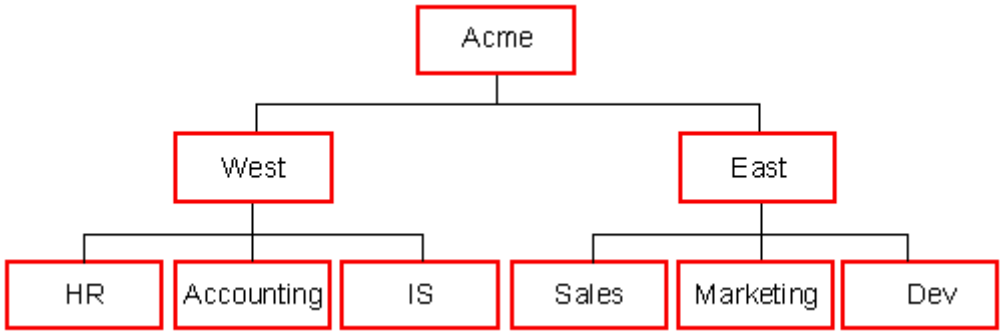


Рис. 7 Пример дерева сертификатов для крупной организации, с использованием географического принципа построения дерева сертификатов.

2.2.1.1 Примеры имен серверов и пользователей

После того, как Вы создаете иерархическую схему имен, Вы используете ID сертификатора, чтобы добавить нужные имена серверов и пользователей в схему Вашей организации. ID сертификатора - файл, который определяет, где в иерархии находятся и появятся, определенные Вами, имена.

Организации и орг. единицы отделяются друг от друга косой чертой (/) в именах пользователей или серверов.

Пример:

```
Mail-E/East/Acme или Alan Jones/Sales/East/Acme.
```

В нашем примере, сервера корпорации Acme организованы по месту их расположения. Например, все сервера восточного офиса, расположенного на восточном побережье, используют один и тот же сертификат орг. единицы. Организация серверов по местоположению эффективно, когда Вы хотите ограничить доступ к данным, основываясь на местоположении пользователей или серверов. При этом пользователи легко могут идентифицировать местоположение сервера, тем самым предупредить их от создания дорогостоящего способа связи, по WAN соединениям. В этом примере, Вы нуждаетесь в двух ID сертификатах для серверов - East/Acme и West/Acme.

Сервера.

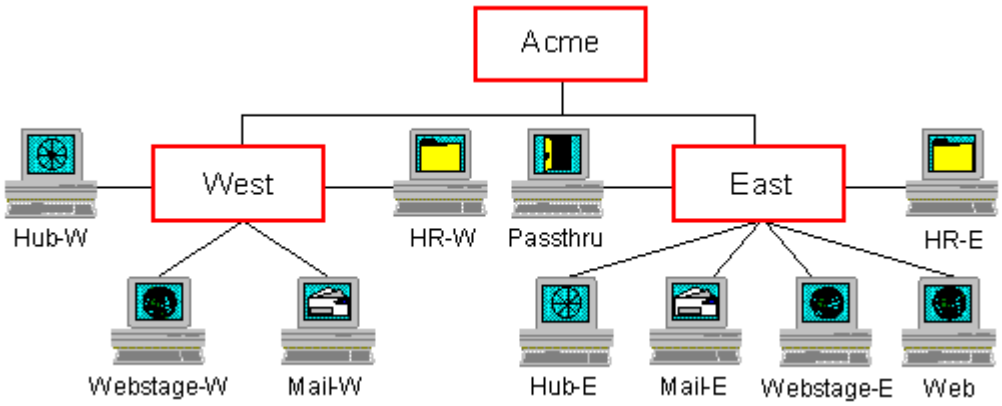


Рис. 8 Применение сертификатов для серверов в Acme.

В Acme корпорации, пользователи организованы по местоположению и отделам. Для организации пользователей по этому принципу, Вы можете позволить только отделу HR, на западном побережье доступ, на сервер приложений. Организация пользователей по местоположению и отделу также помогает контролировать одинаковые имена пользователей, если встречаются одинаковые имена и фамилии в корпорации Acme.

В этом примере, Вы нуждаетесь в шести дополнительном ID сертификатах для пользователей - Sales/East/Acme, Marketing/East/Acme, Dev/East/Acme, HR/West/Acme, Accounting/West/Acme и IS/West/Acme. Эти сертификаторы используют имена отделов, в которых работают Ваши пользователи.

Пользователи.

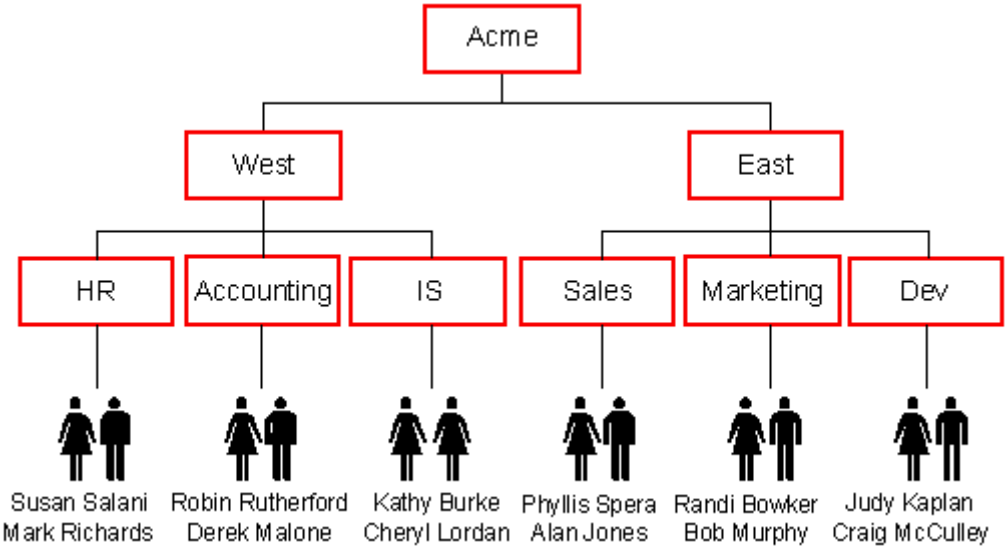


Рис. 9 Пример сертификации пользователей в Acme.

2.2.2 Типы Domino серверов, которые будут использоваться в построении системы.

2.2.2.1 Использование Hub серверов.

Рис. 10 Пример использования Hub серверов.

Hub сервера в Acme корпорации соединяются через сервера посредники, которые расположены на обоих побережьях - West и East. Сервера посредники географически удаленны и требуют, дорогостоящей линии связи - например, использование линии ISDN или МОДЕМОВ. Соединения через Hub сервера выгодно, потому что можете управлять этими связями, т.к. они, как правило, имеют высокую стоимость. При использовании Hub серверов, только два сервера должны связываться через WAN соединение, вместо того чтобы каждый сервер в организации связывался с другими серверами.

Firewall сервер - Domino сервер, защищает Hub-E/East/Acme и Hub-W/West/Acme снаружи от пользователей. Потому Firewall использует Domino сервер, вместо другого Firewall программного обеспечения, Hub сервера могут использовать их для передачи почты или репликаций.

2.2.2.2 Использование почтовых серверов и серверов каталогов.

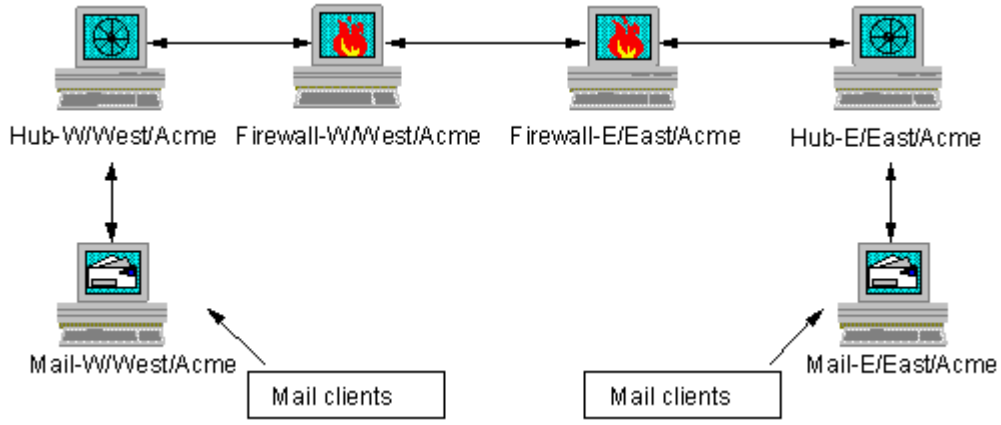


Рис. 11 Пример использования почтовых серверов и серверов каталогов.

Acme корпорации использует два почтовых сервера, для каждого географического местоположения по одному. Все пользователи посылают почту, используя почтовые базы данных, расположенные или на Mail-E/East/Acme или Mail-W/ West/Acme. Почтовые базы данных доступны для всех типов почтовых клиентов - Notes, IMAP, POP3 и браузеров.

Почтовые сообщения маршрутизируются подобно изменениям сделанным в базах данных. В этом примере, почта сервера маршрутизируется через Hub сервера на другой почтовый сервер. Например, когда Alan Jones/Sales/East/Acme посылает сообщение Susan Salani/HR/West/Acme, сообщение маршрутизируется с Mail-E/East/Acme до Hub-E/East/Acme, с Hub-E/East/Acme до Hub-W/West/Acme, затем с Hub-W/West/Acme до Mail-W/West/Acme. Susan Salani/HR/West/Acme читает сообщение, на ее почтовом сервере Mail-W/West/Acme.

Сервера каталогов позволяют пользователям и серверам посматривать информацию о пользователях и серверах, для поиска их адресов, или рассылки почты. Каталоги содержат информацию о том, как связаться с Notes пользователями, пользователями интернета и Domino серверами.

В нашем примере, копия базы Directory Catalog находится на каждом клиенте Notes, а копия базы Domain Directory находится на каждом сервере - Mail-E/East/Acme, Hub-E/East/Acme, Hub-W/West/Acme и Mail-W/West/Acme. Domino проверяет сначала Directory Catalog, для поиска имени и если имя не найдено, проверяет Domain Directory.

Domino использует репликации, отсылая изменения из одной базы в другую, расположенную на другом сервере. Например, если изменение сделаны на Mail-E/East/Acme сервере, изменения посылаются в копии на Hub-E/East/Acme, Hub-W/West/Acme и Mail-W/West/Acme сервера.

В Acme корпорации, репликации происходит автоматически в намеченное время. График репликаций определяется временем, требуемым для изменения данных на серверах.

2.2.2.3 Использование серверов приложений.

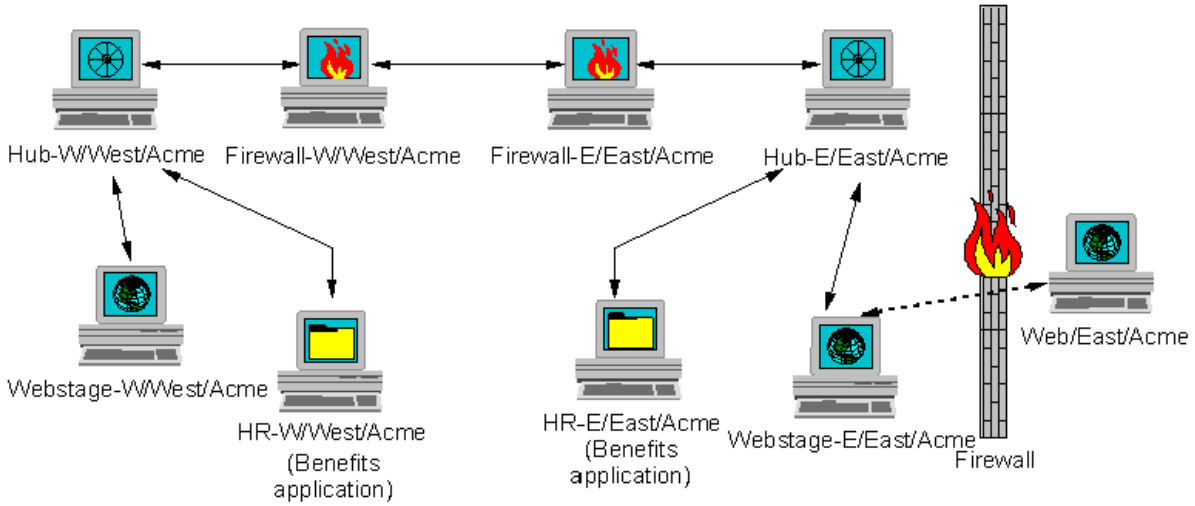


Рис. 12 Пример использования серверов приложений.

Приложения могут быть доступны для пользователя Notes, браузеров или Notes браузеров пользователей. Web приложения должны находится на серверах приложений, которые также установлены как Web сервера. Web сервер предоставляет данные пользователям использующим браузеры.

В этом примере, Web/East/Acme хранит Web приложения для Web организации. Приложения доступны для пользователей браузеров, которые находятся вне организации Acme корпорации. Webstage/East/Acme и Webstage-W/West/Acme имеют реплики Web приложений. Пользователи могут делать изменения в Web приложениях на Webstage-E/East/Acme и Webstage-W/West/Acme. Webstage-W/West/Acme использует график репликаций через Hub сервер Webstage-E/East/Acme.

Acme корпорация также имеет два сервера Web-HR-E/East/Acme и HR-W/West/Acme. Эти сервера содержат служебные приложения, только для внутренних служащих, кто используют рабочие станции Notes.

В этом примере используется – Firewalls, защищая связи между Hub серверами и защищая связь между Web/East/Acme и Webstage-E/East/Acme.

2.2.2.4 Использования Passthru сервера.

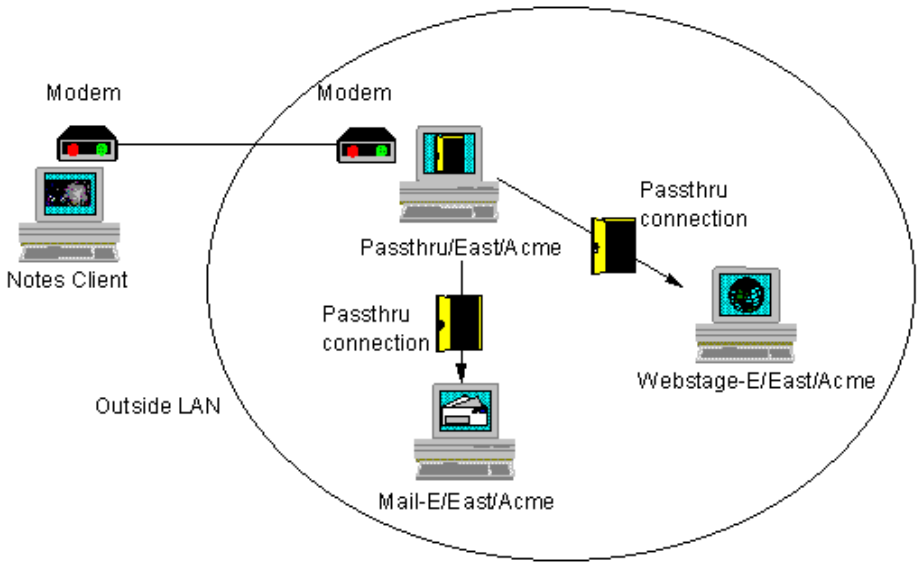


Рис. 13 Пример использования Passthru сервера.

Passthru сервера позволяют пользователям и серверам соединяются с отдельным сервером, для доступа их, ко всем другим серверам, к которому сервер Passthru имеет доступ.

Acme корпорация использует Passthru сервер, чтобы упростить связи пользователей к серверам с использованием модема.

Например, если Randi Bowker/Marketing/East/Acme берет Laptop домой и хочет прочитать почту на Mail-E/East/Acme, Randi набирает номер модема на Passthru/East/Acme и Passthru/East/Acme соединяет ее с Mail-E/East/Acme. После Randi вызывает Passthru/East/Acme, все сервера в организации East/Acme доступны ей. И Laptop Randi, и Passthru сервер должны быть снабжены модемами, однако, ни один из других серверов не нуждаются в модеме.

2.2.2.5 Законченная конфигурация серверов для организации.

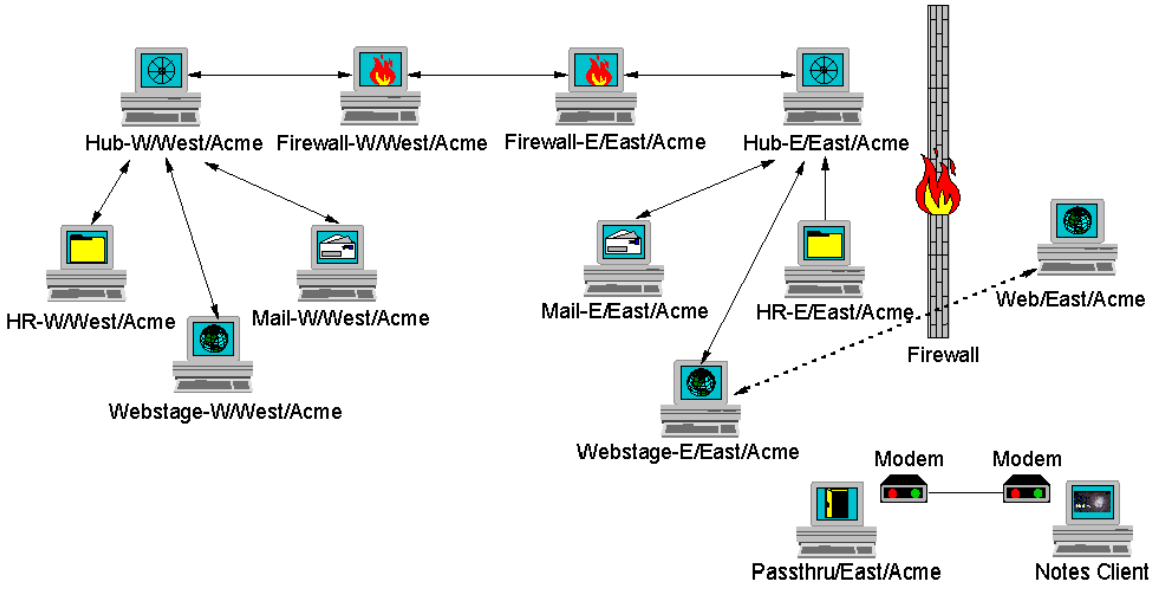


Рис. 14 Пример законченной конфигурации серверов для Acme.

Эта схема отображает все сервера в Acme корпорации – Hub, Directory, Mail, Application и Passthru.

Многие из функций, обсужденных в этом примере, управляются в соответствии с документами, находящимися в Domino Directory. Например, чтобы использовать Passthru сервер, Вы должны создать Passthru документ связи, и определить сервера, которые будут использоваться как Passthru сервера.

2.3 Как добавить дополнительный Domino сервер в домен?

После того, как Вы установили первый Domino сервер в домене, Вы можете свободно расширять Вашу систему и включать в систему дополнительные сервера.

2.3.1 Установка и конфигурирование дополнительного Domino сервера.

Прежде чем вы приступите к установке и конфигурированию дополнительных Domino серверов, Вы должны выполнить процедуры перечисленные ниже.

*178 Установить первый Domino сервер в домене.

*179 Создать иерархическую схему имен, основанную на структуре Вашей компании.

*180 Создать базу данных CertLog (CERTLOG.NSF), для регистрации дополнительных серверов и пользователей. Вы создаете базу один раз для всего домена. Если Вы создали его, при создании первого сервера или при установке предыдущего, Вы не должны создавать другой копии.

*181 Создать ID сертификатора, в зависимости от требований Вашей иерархической схемы имен.

*182 Разослать ID сертификаты администраторам других участков сети Notes.

*183 Добавить сервера, регистрируя их с соответствующими ID сертификаторами.

*184 Установить программное обеспечение для дополнительных серверов.

*185 Исполнить процедуры конфигурации, для новых серверов. Дополнительное конфигурирование зависит от задач и программ, которые Вы хотите запускать на серверах.

2.3.1.1 Создание схемы иерархических имен серверов и пользователей.

Сервер, организация, организационная единица, и имя пользователя может состоять из знаков верхнего регистра и нижнего, алфавитных знаков (A-Z), чисел (0-9), амперсанта (&), черточки (-), точки (.), пробела ( ), подчеркивания (_).

Иерархические имена используют следующие компоненты:

Компоненты	**Описание**	**Требуется знаков**
Common name (CN) Имя	Сервер или имя пользователя. Используется полное имя и фамилия для имени пользователя – для примера, Julia Herlihy.	Не более 80 знаков

Organizational unit name (OU) Орг. Единица	Департамент или местоположение – для примера, East/Acme. Применяется по желанию.	32 знака для орг. Единицы
Organization name (O) Имя организации	Имя компании – для примера, Acme.	3 – 64 Не включайте в название компании признак страны.
Country (C) Признак страны	Аббревиатура для страны – для примера, US. Применяется по желанию.	0 – 2

Пример иерархического имени, которое использует все компоненты:

```
Julia Herlihy/Sales/East/Acme/US
```

Типично, имена показываются в сокращенном формате, но они сохранятся внутри в каноническом формате, который является форматом, который содержит имя и связанные компоненты:

```
CN=Julia Herlihy/OU=Sales/OU=East/O=Acme/C=US.
```

Прежде, чем Вы назначаете серверам или пользователям иерархические имена, Вы должны спланировать схему обозначения организации.

Планирование схемы имен в организации.

Чтобы применять иерархические имена, Вы должны создать схему Вашей компании. Используйте эту диаграмму, в качестве примера, для планирования схемы имен. Иерархическая схема имен может использовать структуру дерева, которая отражает фактическую структуру Вашей компании. Наверху дерева - название организации. Ниже приведена схема имен в организации и орг. единиц, которые Вы создаете, чтобы отобразить структуру компании; Вы можете организовывать структуру по географическим признакам, по департаментам, или по обоим признакам.

В предыдущей главе мы уже говорили, что компания Acme создала эту диаграмму для серверов и пользователей:

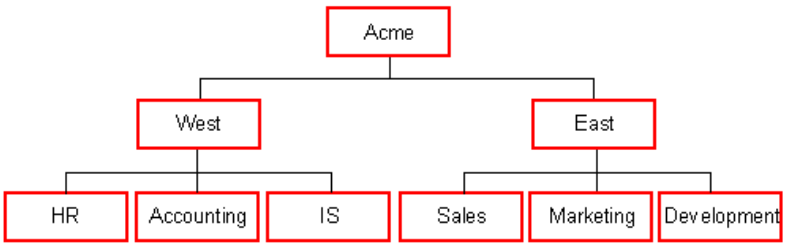


Рис. 15 Пример дерева сертификатов для организации Acme.

Просматривая рисунок, Вы можете видеть, где расположены сервера и пользователи в дереве имен. Acme решил базировать компанию по географическим признакам, на первом

уровне, и создать ID сертификаты для орг. единиц – East и West. На следующем уровне Acme сделал разделение сертификаторов, согласно отделов.

Ваша организация - часть одного Domino домена. В некоторых случаях, Вы можете распределить организацию на два или более доменов. Например, если Ваша компания большая, и Вы хотите распределить ответственность за безопасность системы, между несколькими администраторами.

Создание ID Сертификаторов.

Чтобы размещать сервера и пользователей в правильном порядке, в пределах иерархической структуры, Вы создаете ID сертификаторов для каждого узла в дереве Вашей организацией. Сертификат – это штамп в ID пользователей и серверов, свидетельство о том, где они расположены в организации. Сервер и пользователи, которые принадлежат тому же самому дереву, могут связываться друг с другом. Сервера и пользователи, которые принадлежат различным деревьям сертификатов, нуждаются во взаимной сертификации, для связи друг с другом.

Имеются два типа ID Сертификаторов, сертификат организации и сертификат орг. единицы. Сертификат организации расположен наверху Вашего дерева и обычно называется именем Вашей компании - например, Acme. Сертификат орг. единицы во всех ветках дерева расположен по иерархии ниже сертификата организации. В имени пользователя или сервера, он находится левее имени организации - например, East/Acme или Sales/East/Acme.

Чтобы управлять структурой, компания Acme создала ID Сертификаторов для каждого узла в ее организационной диаграмме:

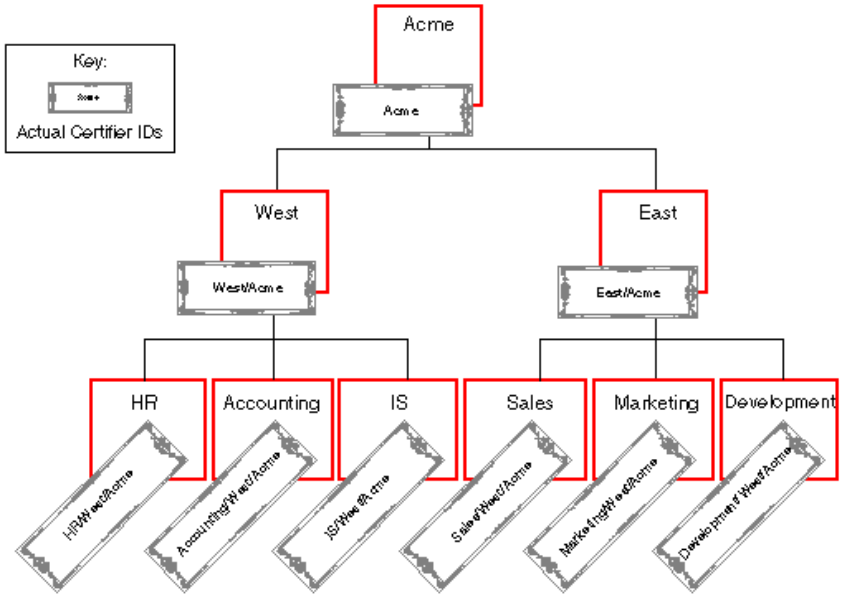


Рис. 16 Имена сертификаторов в организации Acme.

Чтобы регистрировать каждый сервер или пользователя, администратор Acme использует один из этих ID Сертификаторов, в зависимости от того, где этот сервер или пользователь находится в иерархии организации.

Например, чтобы регистрироваться Phyllis Spera, который работает в отделе маркетинга, расположенном на восточном побережье, администратор, использует сертификат

Sales/East/Acme. Полное иерархическое имя Phyllis Spera тогда будет Phyllis Spera /Sales/East/Acme.

Точно так же администратор создает HR-E сервер, расположенный на восточном побережье, с использованием сертификата East/Acme. Полное иерархическое имя этого сервера HR-E/East/Acme.

2.3.1.2 Создание базы данных Certification Log.

После того, как Вы установили первый Domino сервер в домене, создаете базу данных Certification Log, по шаблону (CERTLOG.NSF). Вы должны создать Certification Log только один раз для Вашей Domino системы. Вы можете даже использовать LOG от предыдущей версии, существующей системы. Если Вы удалите LOG, Вы можете освежать его, при этом Вы потеряете записи сделанные за предыдущий период работы системы.

Когда Вы добавляете сервера и пользователей к Domino, в Certification Log создается запись, как Вы регистрировали пользователей и сервера. Для каждого зарегистрированного сервера и пользователя, Certification Log хранит документ, содержащий следующую информацию:

*186 Имя и тип лицензии

*187 Дата сертификата и срок его действия

*188 Имя, тип лицензии, ID номер, ID сертификатора

Вы будете нуждаться в Certification Log, если Вы хотите использовать Процесс Администрирования для ресертификации и других задач.

Для создания базы данных Certification Log:

*189 Выбирайте из меню Файл – База данных – Новая.

*190 Выбирайте имя сервера, который будет хранить базу данных, в поле Сервер.

*191 Введите название базы данных Certification Log.

*192 Введите имя базы данных CERTLOG.NSF.

*193 Выбирайте сервер шаблонов.

*194 Выбирайте опцию - Показать дополнительные шаблоны, выбирайте шаблон Certification Log и жмите - OK.

*195 Выбирайте из меню Файл – База данных – Управление доступом и назначьте доступ Редактора всем администраторам Вашей системы, которые будут заниматься регистрацией серверов и пользователей, и ресертифицировать ID файлы.

2.3.2 ID Сертификатора

Создайте все ID сертификаторов, основываясь на иерархической схеме Вашей организации. В зависимости от нужд Вашей организации, Вы можете создать два типа ID, для организации и для орг. единиц. Вы будете использовать эти ID, чтобы регистрировать новых пользователей и сервера организации в Вашей системе.

Если Вы хотите добавить дополнительные имена к имени ID сертификата, Вы должны ресертифицировать ID сертификатора.

ID Сертификатора и сертификаты.

При использовании ID сертификатора, Вы создаете сертификаты, серверам и пользователям, когда регистрируете их. Каждый сертификат сохраняется в ID сервера или пользователя имеет силу, пока не истечет время определенное Вами течение регистрации. Для серверов и пользователей в различных деревьях, создайте взаимные сертификаты, чтобы разрешить связь между ними.

Каждый раз, когда Вы создаете ID сертификатора, Domino создает ID файл сертификатора и документ Сертификатов. ID файл содержит ID, который Вы используете, для регистрации серверов и пользователей.

Чтобы сохранить ID файл сертификатора, Вы определяете, где Вы будете хранить его, в процессе регистрации. Другой способ хранения, который Вы можете использовать, держать файл сертификатора в сейфе. Вы должны создать пароль для Вашего ID сертификатора. Вы должны использовать ID сертификатора только при регистрации нового сервера или пользователя.

ID сертификатор организации.

Когда Вы устанавливаете первый Domino сервер в домене, ID сертификатора автоматически создается. Программа установки хранит ID файл сертификата и сервера в каталоге Domino\Notes\Data и дает файлу сертификатора имя CERT.ID. Этим ID сертификатора автоматически сертифицирует первый ID Domino сервера и ID пользователя администратора. ID появляется наверху иерархического дерева имен и обычно называется именем Вашей компании - например, Acme.

Вы используете ID сертификатора, когда Вы создаете ID сертификатора для орг. единиц, следующего уровня иерархического дерева имен. Например, Ваша компания и ID сертификатора имеет имя - Acme. Вы хотите создать орг. единицы и ID Сертификаторов, для организации в компании дерева имен, по признаку местоположением. Вы используете ID сертификатора Acme, чтобы создать - например, West/Acme и East/Acme.

Если Ваша организация большая и децентрализована, Вы могли бы создать другой ID сертификатора, чтобы далее дифференцировать имена. Например, разделить структуру имен в компании, по принципу основанному на филиалах компании. Другая причина создавать дополнительного сертификатора - для более углубленной безопасности и для более легкого администрирования.

ID сертификатор для орг. единиц

Вы можете создавать до четырех уровней орг. единиц. Сертификат орг. единиц может отражать географическую или просто структуру компании.

Чтобы создавать первый уровень орг. единицы, ID сертификаторов, Вы используете ID сертификатора организации. Однако чтобы создать ID сертификатора орг. единицы следующего уровня, Вы используете ID орг. единицы первого уровня и так далее.

Например, если Вы хотите далее дифференцировать членов East/Acme, Вы используете этот ID сертификатора East/Acme, чтобы создать дополнительную орг. единицу, например, Sales/East/Acme, Marketing/East/Acme, и Development/East/Acme. Если Ваша схема имен не требует дополнительного уровня орг. единиц, используйте первый уровень ID Сертификаторов, чтобы сертифицировать пользователей и сервера.

Выгода от использования ID сертификатов - то, что Вы можете децентрализовать сертификаты, распределяя ID сертификаторов. Когда Вы децентрализуете, единственный

сертификат, один человек не должен регистрировать или сертифицировать каждого пользователя с использованием отдельного ID сертификатора.

Например, компания Acme имеет двух администраторов, которые управляет серверами и пользователями в West/Acme и серверами и пользователями в East/Acme.

Храните ID файлы Сертификаторов в физически безопасном месте. Храните резервную копию как страховку против пожара, наводнения, или воровства. Для дополнительной безопасности, Вы можете создавать больше чем один пароль (один пароль требуется как минимум) для каждого ID сертификатора.

2.3.2.1 Создание ID сертификатора для Организации.

Программа Domino Setup создает ID сертификатор для организации, когда первый сервер в домене установлен и сконфигурирован. Вы можете создать другой ID сертификатор, чтобы далее дифференцировать имена или более легко администрировать сервера и пользователей.

*196 Из клиента Domino Administrator, выбирайте закладку Настройка.

*197 Из панели инструментов Сервис – Регистрировать – Организация.

(Необязательно) Изменить регистрационный сервер (сервер, который будет хранить документ Сертификата в Domino Directory), выбирайте – Регистрационный Сервер, выбирайте нужный сервер и затем – ОК. Если Вы не определили регистрационный сервер, это будет сервер – по умолчанию:

*198 Локальный сервер, если он содержит Domino Directory

*199 Сервер, указанный в переменной NewUserRegServer в NOTES.INI

*200 Сервер Администрирования

*201 (Необязательно) Щелкайте на кнопке Файла учетной записи, если Вы хотите изменить местоположение ID файла. Убедитесь, что сохраняете ID в безопасном месте. по умолчанию ID сохраняется в каталоге c:\.

*202 Заполните эти поля:

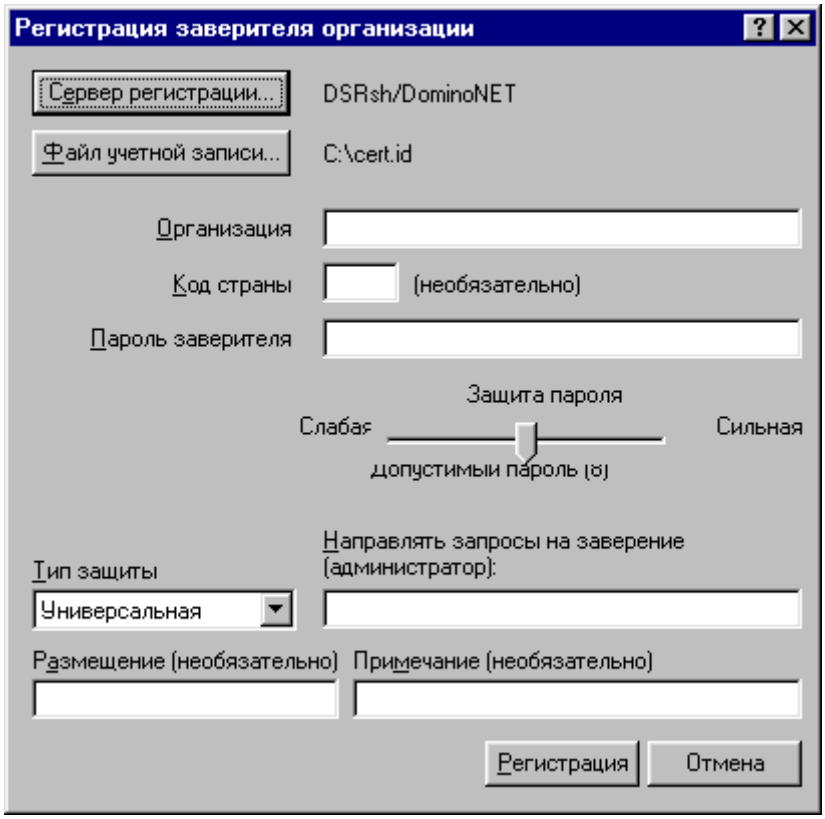


Рис. 17 Диалоговое окно регистрации сертификатора.

Поле	**Содержание**
Организация	Имя Организации. Введите Имя Организации из ID сертификатора созданного при создании первого сервера.
Код страны	Код страны.
Пароль	Пароль для ID.
Минимальное значение пароля в знаках	Минимальное количество знаков в пароле, по умолчанию 10 знаков.
Тип защиты	Выбирайте тип лицензии: *203 Универсальная (по умолчанию). *204 Для Северной Америки. **Обратите внимание**, начиная с версии 5.0.4, используется тип лицензии Global, которая приравнивается к Северо-Американскому типу лицензии.
Направлять запросы на заверение (Имя администратора)	Имя администратора, который обращается с запросом на сертификацию. Имя указанное здесь, появляется в документе Сертификатор в Domino Directory. Если Вы создаете ID сертификатора для администратора, введите имя этого администратора в это поле.
Комментарии	Комментарий.

Размещение	Необязательный текст, который появляется в поле Location документа Certifier.

*205 Щелкайте – Регистрация.

2.3.2.2 Создание ID сертификатора для Орг. единицы

Когда Вы создаете ID сертификатора для орг. единицы, Вы должны иметь под рукой иерархическую схему имен для Вашей компании. Схема имен помогает Вам определить какой ID сертификатора использовать, чтобы создать дополнительный ID сертификатора. Также, Вам понадобится ID сертификатора, который хотите использовать. В большинстве случаев Вы используете ID первого сервера, созданный при установке сервера.

*206 Из клиента Domino Administrator, выбирайте закладку – Настройка.

*207 Из панели инструментов – Сервис – Регистрировать – Подразделение.

*208 Вводят пароль для ID сертификатора и ОК. Пароль для ID сертификатора, который вы используете, чтобы создать ID сертификатора для орг. единицы.

*209 Для изменения ID сертификатора, из окна Регистрация заверителя подразделения, нажмите кнопку Заверитель. Выбирайте нужный ID сертификатора, вводите пароль и ОК

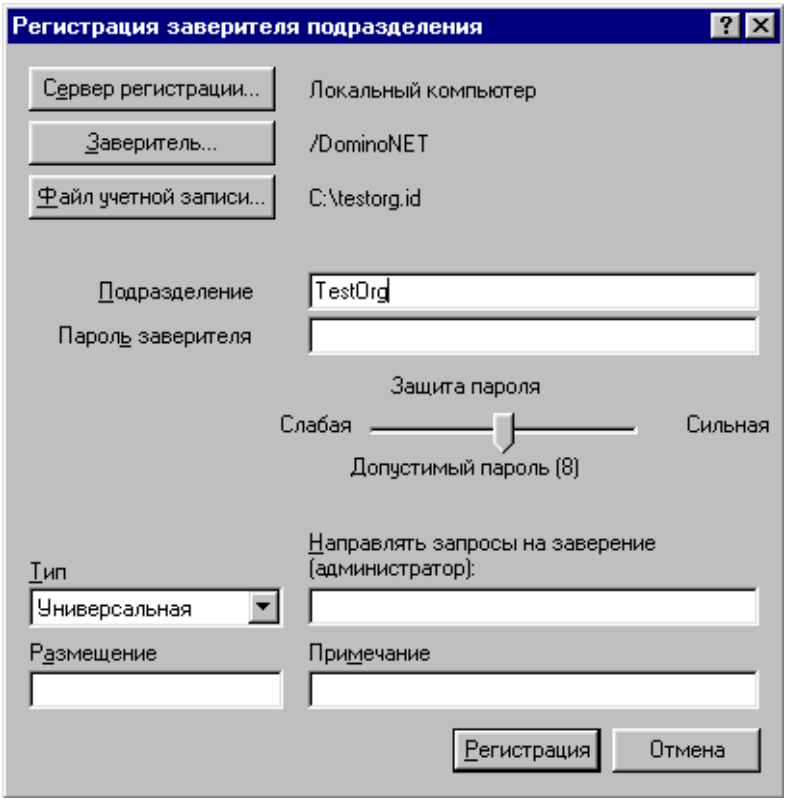


Рис. 18 Диалоговое окно регистрации орг. единицы сертификатора.

*210 Изменяют сервер регистрации (если необходимо).

*211 Заполните поля окна Регистрация заверителя подразделения, выбирайте – Регистрировать.

*212 В целом процедура очень похожа на процедуру регистрации ID для организации, но есть и отличие. При регистрации Вы можете изменить сертификат, которым будете сертифицировать создаваемый ID.

2.3.3 Общий подход к назначению паролей в Domino системе.

При создании паролей для пользователя, сервера, или ID сертификатора, Вы должны понять критерии, в соответствии, с которыми Domino гарантирует безопасность. Domino измеряет эти критерии согласно выбранному уровню безопасности. Можно назначать минимальный уровень безопасности для пароля ID файла. Критерий безопасности Domino, базируется на числе символов в поле пароля.

Значение пароля может изменять от слабого, до сильного, или от 0 (самого низкого значения, когда пароль не требуется) до 16 - самый высокий приоритет. Domino определяет по умолчанию значение пароля и устанавливает его равное 10, но Вы можете изменять эти значения.

Не все пароли равной длины имеют равную силу безопасности. Например, пароль - password состоит только из слов, но равен по длине паролю - 1168Acme, второй пароль имеет более предпочтительный формат т.к. содержит не только буквы, но и цифры и, буквы заглавного регистра.

Некоторые советы по выбору пароля.

*213 Не используйте в пароле слова, которые находятся в Domino словарях проверки орфографии. Пароли, содержащие слова, найденные в Domino словарях, для проверки орфографии является наиболее слабыми паролями с точки зрения безопасности.

*214 Смешанные пароли - Использование в пароле слов, которые содержат числа и знаки большого и малого регистра более сильная безопасность.

*215 Используйте вместо пароля предложение, особенно хорошо использовать слова с орфографической ошибкой. Это является наиболее сильным паролем.

*216 Пароли, которые имеют 12 символов или выше, имеют более качественный уровень доступа, чем 4 символа.

*217 Устанавливайте по умолчанию для всех полей Password Quality Scale (пароль) более высокие значения.

2.3.4 Регистрация и установка дополнительных серверов.

Прежде чем Вы сможете установить и настроить дополнительный Domino сервер, Вы должны зарегистрировать его. Чтобы зарегистрировать сервер Вы используете ID сертификатора, чтобы создать ID сервера, который содержит соответствующий сертификат.

Вы должны использовать следующую последовательность действий, для установки дополнительных серверов:

*218 Зарегистрировать каждый дополнительный сервер.

*219 Установить, с использованием зарегистрированного ID сервер, потом его настроить.

*220 Добавить или разрешить любые дополнительные порты для сети.

2.3.4.1 Регистрация дополнительного сервера.

Процесс регистрации создает Server документ для сервера, в базе данных Domino Directory и создает ID сервера. После регистрации и установки сервера, Вы можете настраивать сервер для выполнения им специфических задач (HTTP, LDAP и т.д.) если Ваша организация требует этих типов сервисов.

При регистрации серверов, Вы должны знать иерархическую схему имен Вашей компании. Схема имен помогает Вам разобраться, какой ID использовать, при регистрации каждого нового сервера. Вы должны также иметь доступ к этому ID сертификатора и знать его пароль.

Сервер Регистрации, на котором Вы регистрируете другие сервера, должен быть запущен и доступен Вам по сети. Чтобы зарегистрировать сервер на Вашей рабочей станции, Вы должны иметь доступ к Серверу Регистрации и иметь, по крайней мере, доступ Автора и роль ServerCreator в ACL Domino Directory. При регистрации сервера Domino делает следующее:

*221 Создает ID сервера для нового сервера и сертифицирует его

*222 Создает Server документ для нового сервера в Domino Directory

*223 Зашифрует и присоединит ID сервера к Server документу, или сохранит ID на диске сервера

*224 Добавляет имя сервера в группу LocalDomainServers в Domino Directory

*225 Создает запись для нового сервера в Certification Log (CERTLOG.NSF)

Для регистрации сервера сделайте следующее:

*226 Удостоверитесь, что Вы имеете доступ к ID сертификатора, который хотите использовать.

*227 Из клиента Domino Administrator, выбирайте закладку Настройка.

*228 Из панели инструментов, выбирайте – Регистрация – Сервер.

*229 Введите пароль ID сертификатора и выбирайте – OK.

Обратите внимание, Notes использует ID сертификатора, указанный в административных параметрах для рабочей станции, иначе использует ID, указанный в переменной CertifierIDFile NOTES.INI файла.

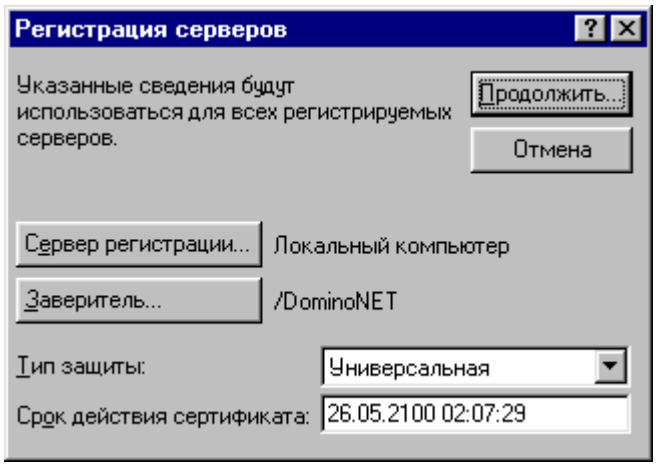


Рис. 19 Диалоговое окно регистрации сервера.

*230 (Необязательно) Измените регистрационный сервер

*231 (Необязательно) измените ID сертификатора

Выбирайте один из типов Лицензий:

Тип безопасности	**Значение**
Для Северной Америки	Сервер использует North American версию для Notes/Domino.
Универсальная (по умолчанию)	Сервер использует International версию для Notes/Domino.

Обратите внимание, начиная с версии 5.0.4, используется тип лицензии Global, которая приравнивается к Северо-Американскому типу лицензии.

*232 (Необязательно) измените дату истечения Server Сертификата, введите дату в формате mm-dd-yy в поле Срок действия сертификата. Дата по умолчанию - сто лет с момента текущей даты.

*233 Выбирайте – Продолжить и введите значения этих полей:

Поле	**Значение**
Имя сервера	Имя нового сервера.
Пароль	Пароль для сервера.
Длина пароля	Числовое значение длинны пароля.
Домен	Имя Notes домена.
Администратор	Имя Администратора Сервера.

*234 Нажмите иконку Уч. запись и введите значения в поля, потом жмите – Register:

Поле	**Значение**
Сервер Domino	Описание Сервера. Можно будет изменить с закладки Настройка в представлении Все документы сервера.
Сеть	Имя Notes сети
Локальный администратор	Локальный администратор - получает доступ Автора и роль ServerModifer к Domino Directory и Server документу.
Сохранить учетную запись	Где будет сохранен файл ID сервера. По умолчанию Domino сохраняет файл в Server документе, Domino Directory.

2.3.4.2 Установка дополнительных портов сервера

*235 После того, как Вы установили дополнительные Domino сервера, Вы можете добавлять дополнительные порты, например дополнительные сетевые протоколы.

*236 Из клиента Domino Administrator, выбирайте закладку Сервер.

*237 Из панели серверов, выбирайте сервер, на котором будете работать.

*238 Из панели инструментов, справа, выбирайте – Сервис – Сервер – Настройка портов.

*239 В окне портов, выбирайте создать, чтоб создать новые имена портов - например, LAN1 или TCP. Не используйте пробелы в именах. Если Вы создаете новые имена портов, определите для них драйвера и выбирайте – ОК.

*240 Установите “галочку” возле записи - Порт разрешен, выбирайте – ОК.

Выбирайте закладку Настройки – Сервер – Все документы на сервере.

Откройте нужный Server документ в режиме редактирования.

Выбирайте закладку Ports – Notes Network Ports, введите значения в поля, выбирайте - Сохранить:

Поля	**Значения**
Port	Имя Порта
Net Address	Например: HR-E.Acme.com, 192.168.222.1
Disabled/Enabled	Выбирайте значение - Enabled, для разрешения использования порта.

2.3.5 Настройка глобальных параметров администрирования. Установки по умолчанию.

Вы можете устанавливать глобальные параметры администрирования для Вашего домена. Эти предпочтение применяются при регистрации новых Сертификаторов, серверов и пользователей. Вы можете определять эти опции:

*241 Домен Регистрации

*242 Сервер Регистрации

*243 ID Сертификатора

*244 Параметры почты. Тип почтовой системы, почтовый сервер, шаблон для почтового файла

*245 Место сохранения ID пользователей, серверов и сертификаторов

*246 Длинна пароля для пользователей, серверов и сертификаторов

*247 Профиль настройки пользователя

*248 Интернет домен

В течение регистрации и сертификации, Вы можете изменить любую установку, которое Вы определяете.

Установка глобальных параметров администрирования.

Выбирайте из меню Файл – Параметры – Параметры администрирования – Регистрация.

Определите или измените любые из этих опций:

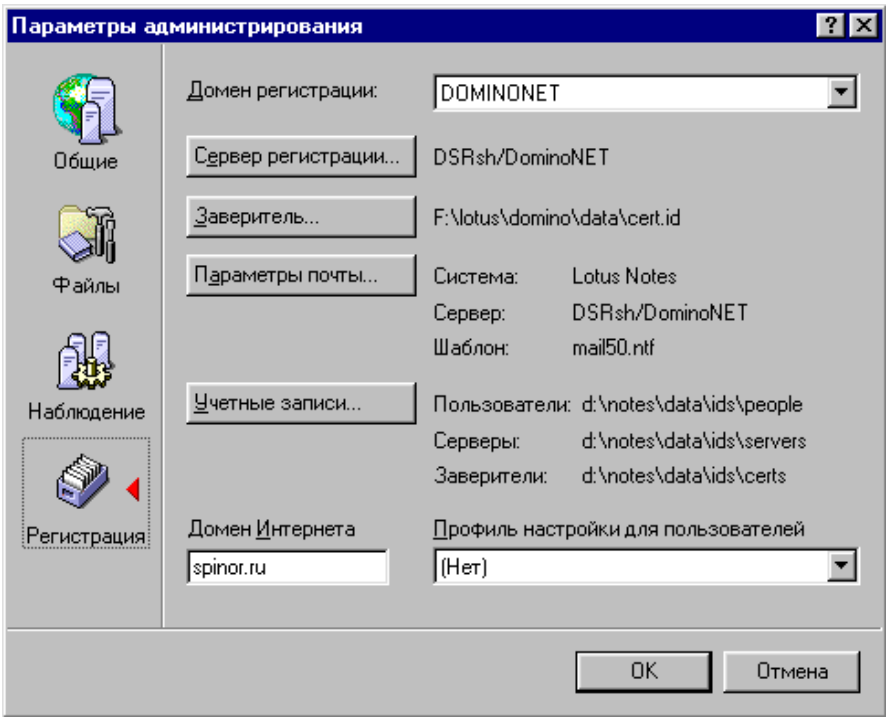


Рис. 20 Диалоговое окно параметров администрирования по умолчанию.

Поле	**Значение**
Домен регистрации	Выбирайте домен регистрации.
Сервер регистрации	Сервер регистрации.
ID Сертификатора	Имя сертификатора.
Параметры почты	*249 Выбирайте почтовую систему. *250 Выбирайте почтовый сервер. *251 Выбирайте шаблон для почтового файла пользователя.

Учетные записи	Выбор опций для файла ID: **ID пользователей** Хранятся ... \Data\IDs\People Минимальный пароль: 8 **ID серверов** Хранятся ... \Data\IDs\Servers Минимальный пароль: 0 **ID Сертификатора** Хранятся ... \Data\IDs\Certs Минимальный пароль: 10
интернет домен	интернет домен. По умолчанию: youhostTCPdomainname.com
Профиль настройки для пользователя	Выбирайте профиль пользователя из доступных, для использования. По умолчанию – Нет.

2.4 Как сконфигурировать Domino сервер, для использования удаленного доступа?

Domino сервер может работать не только в локальной сети, с использованием сетевого оборудования. Вы можете сконфигурировать сервер для работы с использованием удаленного доступа так, чтобы пользователи и сервера могли соединяться с ним.

2.4.1 Типы удаленных соединений

Чтобы удаленные соединения могли выполнять намеченные Вами задачи маршрутизации почты и репликации, Вы можете использовать модемы или другие устройства связи, типа ISDN устройства. Domino поддерживает следующие типы удаленных связей:

Тип соединения	**Описание**
Notes Direct Dial-Up	Этот способ использует Модем и X.PC протокол, чтобы позволять связываться серверам не использующим соединения по сети LAN, с другими Domino серверами. Вы можете использовать прямой набор модема, чтобы соединить сервера с использованием асинхронного сценария связи. Например, сервер использует файл сценария, чтобы соединиться с X.25 PAD и сервером по X.25 сети.

Network Dial-Up	Этот тип связи подобен Notes Direct Dial-Up, за исключением того, что сервер использует MS RAS, для использования сетевого протокола сети, вместо X.PC. После того, как связь установлена, сервер имеет доступ к Domino серверам и может использовать сеть, например для печати.
Passthru (with Notes Direct Dial-Up)	Этот тип связи позволяет определять сервер посредник, который действует как посредник, для получения доступа к определенному серверу. Для X.PC Dial-Up, сервер назначения не нуждается в модеме, если Passthru сервер имеет модем и может передавать информацию на него. Как администратор, Вы могли бы установить режим Passthru соединений, для удаленных пользователей, чтобы использовать одну телефонную линию для доступа пользователей к серверам. Чтобы использовать Passthru для удаленного соединения, Вы должны создать документы Notes Direct Dial-Up Connection для Passthru сервера, чтобы установить связь сначала с посредником.
Hunt group (with Notes Direct Dial-Up)	Эта связь позволяет рабочим станциям звонить на группу модемов Hunt, на больше чем один Passthru сервер. Группа Hunt – это телефонное устройство, которое может иметь один телефонный номер, но несколько линий на нем. Любой Passthru сервер в группе Hunt может получать запрос и передать его к серверу назначения. Чтобы использовать группу Hunt для этого типа конфигурации, Вы создаете документ Hunt group Connection, чтобы установить удаленное соединение.

В дополнение к удаленным типам связи, внесенным в список в предыдущую таблицу, Domino предлагает и другие типы связи. Некоторые из этих типов связи также требуют дополнительное программное обеспечение или дополнительные аппаратные средства, которые покупаются отдельно.

Тип соединения	**Описание**	**Дополнительная информация**
X.25	Установить прямое соединение по X.25 сети	Lotus Notes Connect for X.25 Install Guide and Administrator's Guide
X.400	Установить соединение с сервером X.400	Domino X.400 MTA Configuration Guide
cc:Mail™	Установить соединение с сервером cc:Mail	Planning and Installation for cc:Mail

News/NNTP Feed	Установить соединение с сервером NNTP	Setting up the NNTP Service

2.4.2 Соединение с использованием типа соединения Notes Direct Dial-Up.

Вы можете использовать Notes Direct Dial-Up, чтобы соединить сервер с удаленным Domino сервером. Удаленный Domino сервер может использовать модем или другое устройство связи, чтобы получать запросы от Вашего сервера. После того, как сервер соединяется с удаленным сервером, сервера могут исполнять задачи передачи почты или репликаций.

Чтобы связываться этим способом, сервер и удаленный сервер должен иметь один или большее количество модемов, подключенных к последовательными портами компьютера. Domino порты используют X.PC драйвер, который является протоколом, используемым для связи по модему. X.PC драйвер устанавливается автоматически, при установке Domino сервера.

2.4.2.1 Планирование топологии с удаленными серверами.

Чтобы спланировать топологию использования серверов, умеющих принимать вызовы для установки удаленных соединений, выполните эти процедуры:

*252 Определите, хотите ли Вы, чтобы рабочие станции и сервера использовали Passthru для доступа другим Domino серверам.

*253 Составьте список баз данных, к которым удаленные сервера и рабочие станции будут особенно часто обращаться.

*254 Если необходимо, настройте сервера для работы в качестве Passthru.

*255 Если Вы не хотите использовать Passthru сервера, создайте реплики баз данных на удаленных серверах. Например, используйте один удаленный сервер для всех почтовых баз данных, а другой для всех приложений баз данных, или разместите оба типа баз данных по одному на каждом из удаленных серверов.

*256 Определите число модемов, необходимых для каждого сервера.

2.4.2.2 Настройка топологии для использования удаленных серверов.

Пользователи и сервера могут соединяться с удаленным сервером, даже если они не находятся в той же самой физической сети. Например, географически удаленные офисы в пределах той же самой компании могут использовать удаленные сервера для передачи почты или реплицирования базы данных с центрального сервера.

Чтобы создать топологию удаленных серверов, сначала определяют базы данных, к которым рабочие станции и сервера будут иметь доступ наиболее часто. В частности подумайте относительно того, как Вы хотите маршрутизировать почту и реплицировать базы данных. Имеются ли удаленные пользователи или сервера, которые нуждаются в доступе к почте или другим базам данных. Если так, рассмотрите методы сделать эти базы данных доступными:

*257 Создайте реплики баз данных на удаленном сервере

*258 Установите модемы на серверах для доступа к ним пользователей и серверов

*259 Установите Passthru сервер для использования удаленными серверами или пользователями

Если Вы создаете реплики баз данных и размещаете их на удаленных серверах, удаленные пользователи могут иметь доступ к базам данных без необходимости делать связи с некоторыми серверами. Большинство пользователей имеет только один модем на их рабочих станциях, что означает, что они могут соединяться с только одним удаленным сервером одновременно.

Установка Passthru сервера позволяет удаленным, рабочим станциям или серверам соединяется с одним Domino сервером, чтобы получить доступ к другому Domino серверу. Использование Passthru сервера объединяет ресурсы модема на нескольких Domino серверов и централизует администрирование и поиск неисправностей.

После того, как Вы определяете базы данных, в которых пользователи нуждаются, Вы должны определить число модемов для Вашей системы.

2.4.2.3 Пример топологии Acme's для использования удаленных серверов.

Диаграмма топологии корпорации Acme's для удаленных серверов:

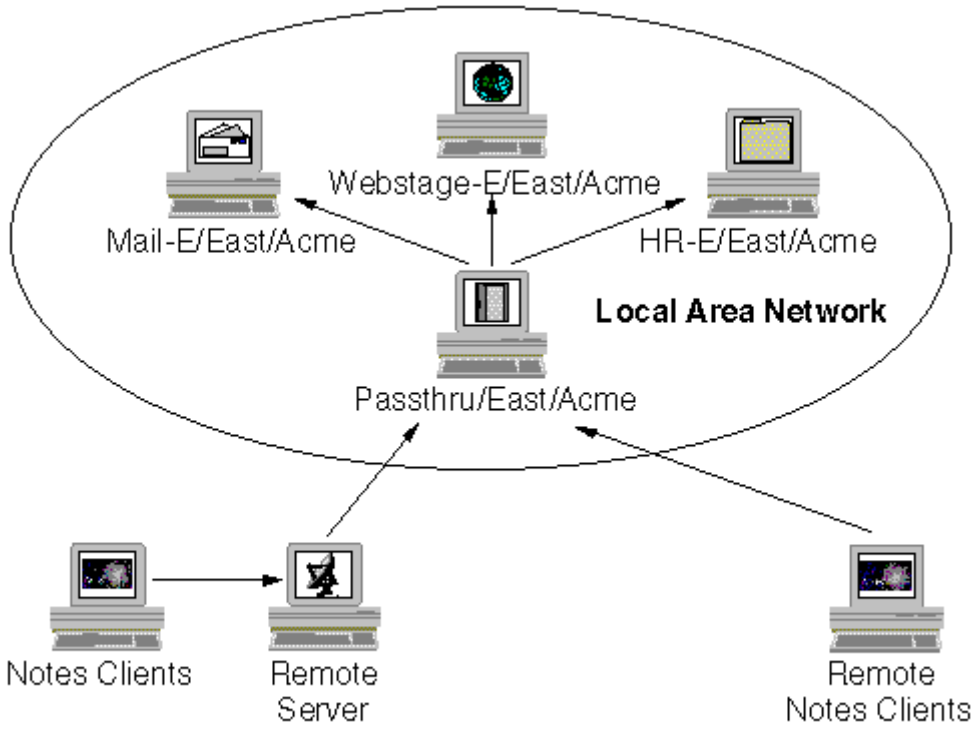


Рис. 21 Топология удаленных серверов Acme.

Компания Acme выбрала эту топология, чтобы удаленные пользователи и сервера имели доступ ко всей системе, соединяясь с одним сервером Passthru. Acme использует Passthru, только как мост между удаленным пользователем или сервером и остальной частью системы. Чтобы свести нагрузку на Passthru к минимуму, сервер не содержит никаких базы данных.

Пользователи, которые работают удаленно через Passthru, могут иметь доступ к любому серверу в системе. Поскольку большинство пользователей Acme, которые работает удаленно, имеют только один модем в их системе, используя Passthru, позволяет им иметь доступ ко всем серверам в одном сеансе связи. Чтобы уменьшать нагрузку на Passthru server, Acme рекомендует, удаленным пользователям делать реплики баз данных и работать с ними локально.

Удаленный сервер расположен в офисе Acme в Штате Огайо. Служащие, которые работают в этом офисе маркетинга, используют этот сервер для доступа к различным базам данных. Удаленный сервер содержит локальные реплики баз данных и реплицирует их один раз в день на центральный сервер. Используя удаленный сервер, пользователи в офисе Штата Огайо экономят время и ресурсы - поскольку они не должны обращаться к системе Acme слишком часто.

2.4.2.4 Определение количества модемов для удаленного сервера.

Для Domino сервера, чтобы связываться с другими серверами или рабочими станциями, Вы должны установить один или большее количество модемов. Число модемов, которые Вы можете использовать на сервере, зависит от операционной системы и ресурсов системы - например, число доступных последовательных портов. Каждый модем нуждается в собственном последовательном порте.

Если Вы ожидаете, тяжелый трафик при использовании удаленного доступа, установите дополнительные модемы или устанавливают много портовую плату для модемов.

Используйте эти вопросы, чтобы помочь Вам определить число модемов:

*260 Сколько пользователей и серверов будут использовать сервер одновременно?

Число модемов, которые Вы устанавливаете на удаленный сервер, определяет число пользователей и серверов, которые могут иметь доступ к серверу одновременно. Рассмотрите расходы по покупке большего количества модемов.

*261 Пользователи используют схему связи рабочая станция-сервер или репликация при вызове сервера?

Чтобы уменьшать загрузку сервера, заставьте пользователей использовать репликации, вместо работы в интерактивном режиме. При использовании репликаций, пользователи имеют локальные реплики баз данных на своих рабочих станциях. Пользователь работает с данными локально, затем, соединяясь с центральным сервером, обменивается новыми и обновленными документами с базой данных на центральном сервере.

*262 Какие типы пользователей соединяются с этим сервером?

Если Ваши пользователи коммерческие представители и всегда находятся в дороге, требование к серверу всегда выше, чем для пользователей, которые только иногда соединяются с удаленным сервером.

2.4.2.5 Пример топологии компании Acme's для удаленного сервера с использованием модемов.

Диаграмма показывает топологию Acme's с применением удаленных серверов использующих модемы:

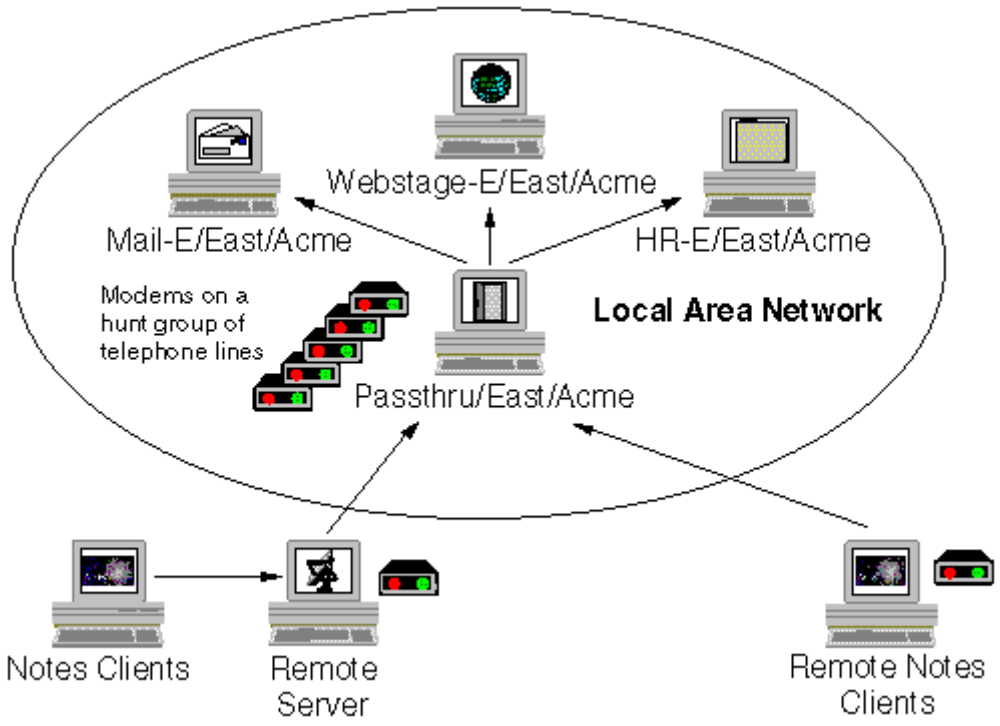


Рис. 22 Топология удаленных серверов Acme с использованием модемов.

Поскольку менеджеров нуждающихся в удаленном соединении и количество пользователей работающих из дома в любой данный день равно, в Acme установили пять модемов на Passthru сервер. Удаленный сервер также использует один из этих модемов для репликаций, но этот сервер связывается в ранние утренние часы и не мешает пользователям. Acme поощряет пользователей, которые работают удаленно, с использованием реплик баз данных, как правило, они работают с локальными копиями баз и лишь реплицируют иногда изменения на сервер.

Acme использует Hunt group для модемов так, чтобы пользователи имели в настройках только один телефонный номер, для соединения. Телефонная АТС Acme позволяет иметь

несколько модемов на одном телефонном номере. Для такого типа соединения, когда все модемы находятся на одном сервере, Acme не должен создавать Hunt group документ.

2.4.2.6 Настройка портов сервера.

После того, как Вы установили модемы на сервер, Вы должны настроить порт связи. Вы настраиваете порт, определяете тип модема, и номер порта, с которым модем связан. Каждый модем, который Вы устанавливаете, требует собственного порта.

При определении типа модема, Domino автоматически связывает модем с файлом конфигурации модема. Файл команд модема - текстовый файл, содержащий команды, которые Domino посылает в модем. Если ни один из типов модема не соответствует Вашему модему, Вы можете использовать файл Generic modem.

Если Вы определили порт в течение программы установки сервера, Вы не должны определить порт модема снова. Вы будете настраивать порт связи только тогда, когда добавляете дополнительный модем или другое устройство на сервер или когда Вы хотите перестроить используемый модем.

Этапы настройка порта сервера.

*263 Установите модем на сервере и проверьте, что операционная система видит порт и модем.

*264 Из клиента Domino Administrator, выбирайте закладку Сервер.

*265 Из панели Сервера, выбирайте сервер, на котором будете настраивать порт. Вы можете настраивать порт удаленно для серверов, которые не имеют клиентов, например UNIX или OS/2.

*266 Из панели инструментов, выбирайте на закладке Сервер – Состояние – Сервис – Настройка портов.

*267 Выбирайте имя порта, на который Вы установили модем.

*268 Если имя порта связи не существует, выбирайте кнопку Создать, выбирайте – XPC драйвер и затем щелкайте - OK.

*269 Выбирайте кнопку Параметры (Имя порта), где (Имя порта) - имя порта и затем – Тип модема, чтобы выбрать Тип модема.

*270 Если Вы не можете найти или не знаете, тип модема, выбирайте тип по умолчанию – Auto Configure.

*271 Измените, назначения порта по умолчанию, если хотите. Назначения порта по умолчанию работают в большинстве случаев. Однако если Вы выполняете поиск неисправностей, Вы можете захотеть подрегулировать некоторых из параметров.

*272 Выбирайте - Порт включен и затем щелкайте - OK.

2.4.2.7 Опции настроек порта.

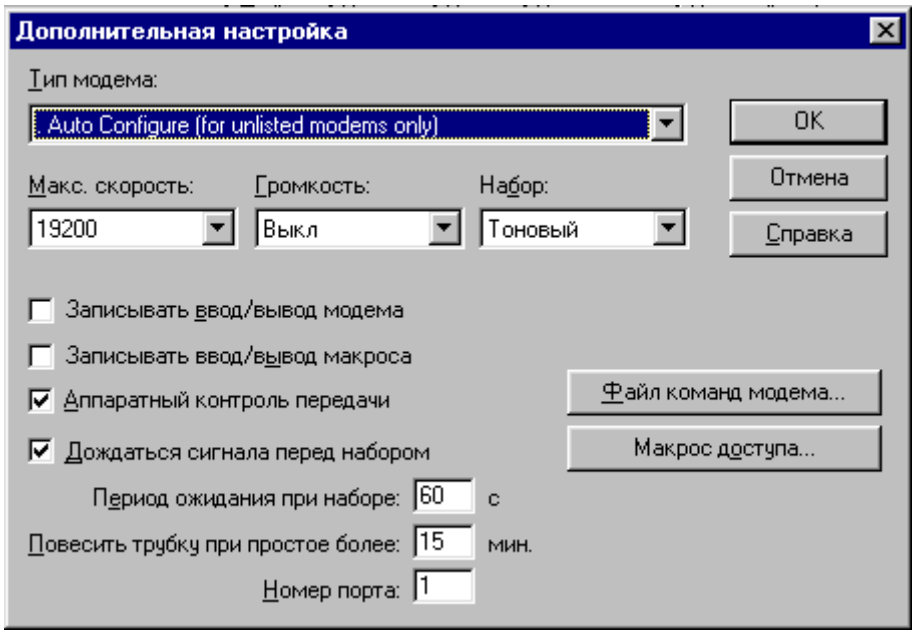


Рис. 23 Окно настройки порта и модема.

Эта таблица объясняет опции настроек порта.

Поле	**Назначение**	**По умолчанию**	**Совет**
Тип модема	Ассоциация модема, с командным файлом модема	.Auto Configure	Выбирайте используемый тип модема, или выбирайте .Auto Configure (AUTO.MDM), Domino автоматически выбирает соответствующий файл команд модема. Если .Auto Configure не работает, выбирайте Generic All-Speed Modem Файл (GEN_ALL.MDM). Если Generic All-Speed Modem файл не работает, вы можете редактировать файл модема для устранения проблемы
Максимальная скорость порта	Максимальная скорость работы порта. Порт связи на компьютере посылает данные в модем и получает данные от модема	19200	Выбирайте более низкую скорость порта, если Вы не можете соединиться с удаленным модемом. При использовании Нуль-модемного соединения, максимальная скорость порта на обоих компьютерах должна быть равная.

Громкость динамика	Позволяет Вам слышать вызов номера и установление соединение	Выключено	Нет
Способ набора номера	Выбор типа набора номера	Тон	Нет
Протокол модема I/O	Запись информации о соединениях модема в LOG файл	Не выбрано	Выбирайте Log I/O модем, если Вы имеете проблему с установлением связи.
Протокол скрипта I/O	Запись информации о выполнении скрипта и ответов в файл LOG.NSF	Не выбрано	Выбирайте Log I/O модем, если Вы имеете проблему с установлением связи.
Управление потоком данных	Управляет потоком данных, посланных между компьютером и модемом	Выбрано для всех операционных систем кроме UNIX	Если не выбрано, может появиться сообщения об ошибках в LOG файле.
Ожидать гудка в линии	Выключение обнаружение сигнала в линии	Выбрано	Используется для связи, где выход на АТС является проблемой
Задержка для повторного набора	Время, которое сервер ожидает соединения с сервером назначения.	60 секунд	Можно увеличить время ожидания модемом, ответа от удаленного модема.
Ожидание ответа	Время, которое модем ждет, перед тем как он положит трубку, если по каналу не передаются данные	15 минут	Используется для автоматического разрыва соединения, если на линии связи, нет движения данных в, течении указанного промежутка времени.

*© **InterTrust Co.** Тел. 956-7928*

Номер порта	Номер порта, к которому присоединен модем	По умолчанию, номер, введенный в поле Порта	Domino автоматически устанавливает номер порта для выбранного имени порта – для примера, если вы используете имя порта COM7, то номер порта - 7. Для UNIX систем, выбираете номер порта *N* (/ dev / cua*N*)
Файл модема	Позволяет Вам редактировать файл модема	AUTO.MDM	Для информации см. Modem Command Files.
Script приобретения	Позволяет Вам выбирать скрипт доступа	Нет	Для информации см. Acquire and Connect Script.

2.4.2.8 Командные файлы для модемов.

Командные файлы модема, которые имеют расширение MDM, сообщает модему как он должен работать. Они определенны в Domino и привязаны к типу модема, который Вы используете. Когда Вы выбираете тип модема, Domino выбирает файл модема, который соответствует этому типу. Domino поставляется с определенными файлами команд модема для широкого круга модемов. Кроме того, Domino обеспечивает Вас по умолчанию файлом AUTO.MDM, который Вы можете использовать, если командный файл модема не доступен для Вашего модема.

Domino копирует файлы модемов в Data\Modems. Команды, в модемных файлах устроены так, как требуется соответствие с XPC протоколом, Domino.

Domino обеспечивает Вас GEN_ALL.MDM файлом, который Вы можете изменять. Для информации относительно команд файлов модема, используйте текстовый редактор, чтобы читать файл TEMPLATE.MDM. Используйте этот файл и документацию, которая поставляется с модемом, чтобы изменить файл команд модема.

Изменяйте командные файлы для модемов только при следующих обстоятельствах:

*273 Если Вы нуждаетесь в дополнительных командах, которые Domino не обеспечивают

*274 Если в Domino нет модемного файла, который является совместимым с Вашим модемом

*275 Если установленный по умолчанию AUTO.MDM, не работает

Где можно получить обновление модемных файлов?

*276 Откройте страничку на http://www.notes.net и выбирайте изображение - Download.

*277 Выбирайте – Other Downloads, выбирайте – Download.

*278 Выбирайте - Notes Mobile Survival Kit и сделайте Ваш выбор для разгрузки.

Редактирование командного файла модема.

Когда Вы изменяете, командный файл модема, Вы можете только изменять файл на локальном сервере. Чтобы применять измененный файл модема на удаленный сервер, редактируйте файл, локально и копируйте эго в каталог Data/Modems на удаленный сервер. Вы должны перезапустить, сервер, чтобы изменения вступили в силу.

Используйте документацию, которая поставлялась с модемом, чтобы определить, какие дополнительные команды Вы можете добавлять к файлу команд модема.

*279 Из клиента Domino Administrator, выбирайте закладку - Сервер.

*280 Из панели инструментов, выбирайте - Сервер – Состояние – Сервис – Настройка портов.

*281 Выбирайте нужный порт.

*282 Выбирайте – Параметры порта.

*283 В Типе Модемов, выбирайте файл модема, который Вы хотите изменить

*284 Выбрать Файл команд модема.

*285 Редактируйте содержание файла.

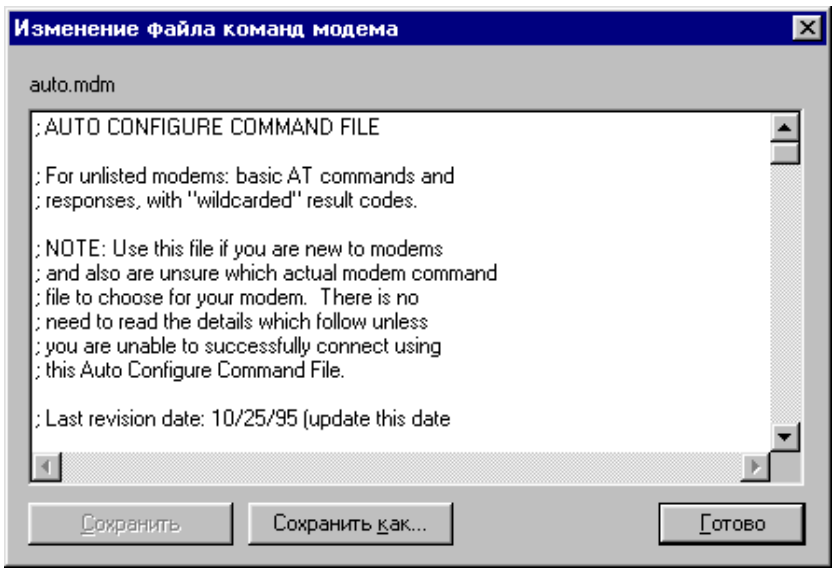


Рис. 24 Окно настройки командного файла модема.

*286 Выбирайте – Сохранить Как ... и введите новое имя для файла.

*287 Выбирайте – Готово, затем – OK, дважды.

2.4.3 Настройка сервера использующего удаленный доступ к сети.

Domino может использовать удаленный доступ к сети MS RAS. Установив соединение, сервер или пользователи соединяются с удаленным компьютером сети, они могут иметь полный доступ к сети Domino. Сервер может использовать Удаленные соединения, для выполнения задач передачи почты и репликаций, как, будто они непосредственно связаны с другими серверами по сети LAN.

Удаленный доступ, который поддерживается ISDN и MS RAS, позволяет компьютеру использовать линию ISDN, чтобы соединиться с сетью LAN. При использовании

удаленного доступа, Вы можете передавать сетевые пакеты от компьютера в удаленную сеть и на сервер. Типично используется PPP протокол, который является протоколом интернета.

*288 Установите и настройте удаленный доступ к Вашей сети для Domino (Dial-Up, MS RAS, Macintosh PPP).

Примечание Domino не поддерживает Макинтош сервер, но Вы можете соединять мак. Клиента с Domino сервером через удаленный доступ к серверу или сети.

*289 Установите протоколы сети, для использования удаленным доступом сервера. Протоколы должны быть совместимы со службой удаленного доступа.

*290 Установите для Domino сервер протокол сети, для использования его с удаленным доступом на сервер.

*291 Чтобы соединиться с серверами удаленным доступом, создайте документ подключения типа Удаленный доступ.

2.4.4 Passthru сервера и Hunt группы.

Функция Passthru позволяет рабочим станциям и серверам использовать сервер посредник, чтобы соединиться с другим сервером, который не имеет с нам общего протокола. Passthru сервер имеют несколько назначений использования в пределах топологии системы.

При использовании Passthru, Вы можете устанавливать связь по сети LAN между двумя серверами, которые не имеют общего протокола. Например, сервер А, который поддерживает только NetBIOS, должен соединиться с сервером С, который поддерживает только TCP/IP. Если сервер В поддерживает NetBIOS и TCP/IP, сервер В может действовать как Passthru сервер, чтобы осуществить связь между серверами А и С.

Подобное использование должно позволить пользователям рабочих станций иметь доступ к серверам, которые не поддерживают общий протокол с ней. Соединяясь с Passthru сервером, рабочая станция может получить доступ к серверу назначения, которые не поддерживают протокол рабочей станции.

Третье тип использования Passthru, позволять пользователям или удаленным серверам использовать одну телефонную сеть, для доступа к одному или нескольким серверам назначения, в той же самой сети LAN. Использование Passthru сервера этот путь к экономии затрат по связи с использованием модема, ко всем серверам организации.

Использование Hunt групп с Passthru серверами.

Если Ваша АТС поддерживает функцию Hunt группы (группы модемов с тем же самым телефонным номером), Вы можете разрешить пользователям, или удаленным серверам соединяется с Hunt группой на Passthru сервере. Hunt группа сможет посылать запросы на любой сервер, модем которого свободен. Ваша телефонная станция должна поддерживать этот тип конфигурации.

Hunt группа использует механизм телефонного переключение, чтобы переключить один телефонный номер на несколько модемов. Когда рабочая станция или сервер набирает номер телефона, он соединяется с любым доступным модемом. Вы можете использовать Hunt группы с одним или большим количеством Passthru серверов.

2.4.4.1 Настройки сервера для использования Passthru.

Для конфигурирования соединений серверов через посредник, Passthru, проделайте следующее:

*292 Создайте топологию серверов посредников.

*293 Настройте сервер посредник, используя Server документ

*294 Настройте, сервер назначения, используя Server документ, для доступа к нему через сервер посредник.

*295 Создайте документ подключения типа Passthru, в Domino Directory, для соединения серверов с использованием сервера посредника.

*296 Если любой из серверов не имеют прямого соединения по сети, создайте документ подключения для соединения с этим сервером или посредником. Этот документ может быть любого типа - Notes Direct Dial-Up, Network Dial-Up или Passthru.

2.4.4.2 Создание топологии Passthru серверов.

Чтобы создавать топологию Passthru серверов, Вам необходимо проделать следующее:

*297 Составьте список всех рабочих станций и серверов, которые нуждаются в доступе на Passthru сервер. Также внесите в список протоколы для рабочих станций и серверов.

*298 Составьте список серверов назначений, к которым вы хотите получить доступ. Также внесите в список протоколы для серверов назначения.

*299 Определите, где в топологии расположить Passthru сервер. Passthru сервер должен иметь все протоколы, которые используют рабочие станции и сервера. Кроме того, Passthru сервер должен иметь достаточное количество модемов.

*300 Если Вы ожидаете, интенсивное движение через Passthru сервер, создаете Dedicated Passthru сервер. Dedicated Passthru сервер, не содержит ни каких баз данных. Он функционирует исключительно как посредник. Определите, хотите ли Вы использовать больше чем один Passthru сервер в Hunt группе. В Hunt группе, один телефонный номер принадлежит всем Passthru серверам в группе, а нагрузка автоматически распределяется среди Passthru серверами. Все Passthru сервера в Hunt группе, должны уметь соединятся с серверами назначения.

*301 Определите пользователей и сервера, которым Вы хотите ограничить доступ на Passthru или серверам назначения. Внесите в список всех пользователей и сервера, которым Вы хотите ограничить доступ на Passthru сервера, затем создайте список ограничений для каждого сервера назначения.

*302 Внесите в список рабочие станции, которые должны использовать Passthru сервер и определите для них Passthru сервер по умолчанию. Если Вы имеете много рабочих станций, равномерно распределяете по станциям Passthru сервера, чтобы гарантировать оптимальную нагрузку на сервер.

*303 Если Вы планируете использовать Hunt группу, создайте список всех рабочих станций соединяющихся с каждой Hunt группой. Сделайте записи имен и телефонных номеров Hunt групп и имен всех серверов назначения.

2.4.4.3 Пример топологии Passthru серверов для компании Acme's.

Эта диаграмма показывает топологию Passthru серверов для компании Acme's:

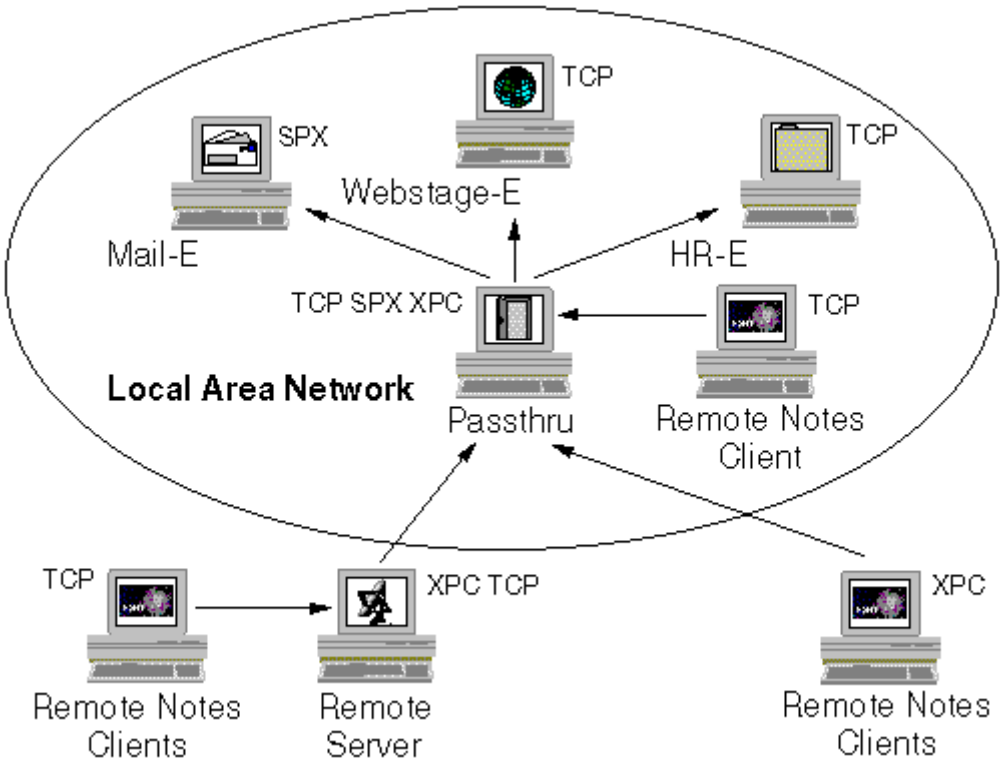


Рис. 25 Пример использования Passthru сервера в Acme.

Компания Acme имеет Dedicated Passthru север, который функционирует только как посредник, для доступа рабочих станций и серверов, на сервера назначения. Этот сервер не содержит никаких базы данных. Passthru поддерживает все протоколы, чтобы пользователи и сервера, соединялись с ним и имели доступ ко всей системе компании.

Обратите внимание, что Passthru может принести пользу пользователям и серверам в той же самой сети. Например, некоторые из клиентов Notes, в вышеупомянутой диаграмме, находятся в той же самой сети LAN, что и Webstage-E, и HR-E, но они не поддерживают общих протоколов. Они не могут иметь доступ на эти servers без использования сервера Passthru.

Вышеупомянутая топология требует следующей конфигурации:

*304 Notes Direct Dial-Up документ подключения, для связи удаленных серверов, с Passthru сервером

*305 Passthru документ подключения для удаленного сервера, чтобы определить Passthru

*306 Документа подключения на удаленном сервере, с каждым сервером назначения

*307 Модификации записи Место вызова, на клиентах Notes, чтобы определить имя Passthru сервера

*308 Notes Direct Dial-Up документ подключения для удаленных клиентов Notes для связи с Passthru

*309 Passthru документ подключения для удаленных клиентов Notes, чтобы определить Passthru связь

*310 Модификации Server документов (чтобы позволить соответствующие права доступа) на Passthru и сервера назначения.

2.4.4.4 Настройка Passthru сервера.

*311 Удостоверитесь, что Вы уже закончили конфигурировать Server документ для сервера.

*312 Из клиента Domino Administrator, выбирайте закладку Настойка.

*313 Выбирайте представление Сервер – Все сервер документы.

*314 Открыть Server документ для сервера, который Вы хотите определить как Passthru сервер и выбирайте – Редактировать Сервер.

*315 Выбирайте закладку Security, введите значения для полей секции Passthru Use и затем сохраните документ:

Поля	**Значение**
Route through	Любое значение из следующего. Любое значения, чтобы идентифицировать пользователей и серверов, тех, кому позволяется использовать этот сервер как посредник, для доступа к серверу назначения: Звездочка (*), чтобы определить всех пользователей и сервера, даже тех, кто не внесен в Domino Directory Звездочка (*) сопровождаемая именем имени сертификата - например, */Acme - чтобы определить всех пользователей и сервера сертифицированих выбранным сертификатом. Имена определенных серверов, пользователей и групп
Cause calling	Имена пользователей и серверов, которым позволено, вынуждать сервер делать телефонные звонки. Оставьте это поле пустым или добавьте звездочку (*), чтобы позволить всем пользователям и серверам эту привилегию. **Обратите внимание**, если вы позволяете всем пользователям и серверам использовать модем этого сервера, Passthru сервер в не отражает в LOG файле, пользователей и сервера, и не указывает их имен.
Destinations allowed	Оставьте это поле незаполненным, чтобы позволить перенаправление на все сервера. Иначе, введите имя определенного сервера, что бы пользователи и сервера могли иметь доступ, только к этому серверу, проходя через этот Passthru сервер

*316 Создайте документы Подключений, чтобы соединить Passthru сервер с серверами назначения, если Passthru и сервера назначения не имеют прямой связи по сети LAN.

*317 Определите Passthru сервера, изменяя их Server документы.

2.4.4.5 Настройка серверов назначений, к которым можно получить доступ с использованием Passthru серверов.

Вы должны перестроить сервера назначения, чтобы позволить определенным Passthru серверам иметь доступ к ним и назначить пользователям соответствующий доступ.

*318 Удостоверитесь, что Вы уже закончили конфигурировать Server документ, для Вашего сервера.

*319 Выбирайте представление Сервер – Все сервер документы.

*320 Открывайте Server документ, который Вы хотите перестроить как сервер назначения и щелкайте - Редактировать Сервер.

*321 Выбирайте закладку Security, введите в поле Passthru Use field значение и затем сохраните документ:

Поле	**Значение**
Access this server	Любое значение из следующего. Пользователи и сервера, которые могут получить доступ на этот сервер через Passthru: Звездочка (*), чтобы определить всех пользователей и сервера, даже тех, кто не внесен в Domino Directory Звездочка (*) сопровождаемая именем имени сертификата - например, */Acme – чтобы определить всех пользователей и сервера сертифицированих выбранным сертификатом. Имена определенных серверов, пользователей и групп

Обратите внимание на это поле Access, оно не затрагивает общий доступ к серверу. Определите общий доступ на Сервер в секции Access Server. Например, Вы могли бы не позволить некоторым пользователям, доступ на сервер через Passthru, они могут все еще получить доступ на сервер, если они имеют разрешение в секции Access Server.

2.4.5 Настройки сервера для доступа к нему через интернет

Вы можете расширять Вашу сеть, позволяя рабочим станциям Notes и Domino серверам связываться по интернет с Вашими локальными серверами. Перед использованием связей по интернет, Вы должны понять основы безопасности в интернете. Для доступности к Вашему Domino серверу через интернет сделайте следующее:

*322 Выбирайте поставщика интернет услуг ISP, чтобы получить доступ к интернет.

*323 Установите TCP/IP протокол.

*324 (Необязательно) Установите Proxy сервер, чтобы соединяться через Firewall с интернет.

*325 Проверяйте Вашу связь интернет, используя утилиту – PING.

2.4.5.1 Internet Service Providers и соединений по интернет.

Вы можете сделать Ваш сервер доступным через интернет. Чтобы делать сделать это, Вы должны установить соединение и заключать контракт с Поставщиком услуг интернета (ISP). Вы должны также регистрировать Ваше имя домена на DNS так, чтобы пользователи могли видеть адрес IP Вашего сервера, когда они хотят получить доступ к серверу из интернета.

Когда Вы делаете сервер доступным в интернете, Вы или используете прямую связь или прямую связь через Proxy сервер. Если Вы используете Proxy сервер, Domino сервер не должен соединиться с ISP на прямую, поскольку Proxy сервер уже устанавливает эту связь.

Соединение по выделенной линии (leased-line).

Связь Leased-line - прямая связь с интернетом. Если Вы используете тип связи Leased-line, Вы соединяете сервер с использованием сети LAN, через Router и выделенной линии.

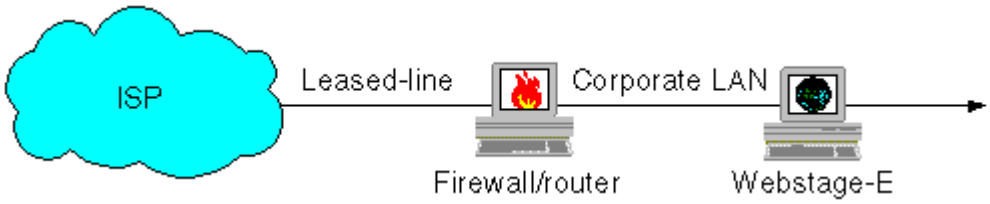


Рис. 26 Пример использования выделенной линии для соединения серверов с интернет.

Proxy соединение.

Proxy сервер обычно запускается вместе с Firewall программным обеспечением, чтобы передать запросы между серверами с обеих сторон Firewall. Если Ваша организация использует Proxy сервер для связи с интернет, Вы соединяете сервер с сетью LAN, которая проходит через Proxy и Firewall сервер ISP. Вы можете использовать Domino или не - Domino Proxy сервер для связи с интернет.

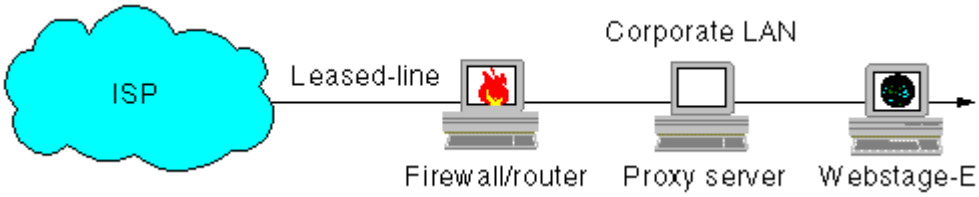


Рис. 27 Пример использования выделенной линии и Proxy сервера для соединения серверов с интернет.

2.4.5.2 Установка программного обеспечения для связи с интернет.

Прежде, чем Вы можете соединить сервер с интернетом, Вы должны установить программное обеспечение сети, которое является совместимым с интернетом.

*326 Если TCP/IP еще не установлен на Domino сервере, установите протокол, используя инструкции установки для операционной системы.

*327 Если Вы не имеете соответствующего порта, добавьте его и разрешите его использование сервером.

2.4.5.3 Установка Proxy сервера для соединения с интернет.

Proxy сервер общается со всеми Domino серверами и рабочими станциями в интернете. Когда Вы используете Proxy сервер, Domino сервер не должен соединиться на прямую с Поставщиком услуг интернета (ISP), так как Proxy сервер устанавливает связь вместо Вашего сервера.

Вы можете определить Domino Passthru сервер как Proxy. для интернета - таким же самым путем, каким Вы определяете Passthru сервер, для внутренней Domino сети. Вы не нуждаетесь в конфигурировании сервера по-другому для связи по интернет.

2.4.5.4 Тестирование подключение сети с использованием утилиты PING.

После того, как Вы устанавливаете соединение с интернетом, Вы должны проверить связь и убедится, что все работает должным образом.

Если Вы имеете прямую связь в интернет, самый легкий способ проверить связь состоит в том, чтобы использовать утилиту PING. Утилита позволяет Вам запросить другой компьютер, если ответ есть, это подтверждает, что программное обеспечение протокола работает правильно.

Если Вы не можете “пинговать” удаленный Domino сервер, то Ваше соединение не может работать должным образом, проверяйте Ваш Router.

Если Вы соединяетесь с интернетом через Proxy сервер, пробуете пинговать Ваш Proxy, чтобы проверить связь по сети.

Используйте следующий формат:

```
ping  xyz.com
```

Если пинг успешен, утилита возвращает сообщение в формате, подобном следующему:

```
64 bytes from 130.000.00.00: 1cmp_seq=4, time=0, ms
```

2.5 Как настроить соединения Domino серверов?

При репликациях баз данных и передаче почты, сервера должны соединиться друг с другом. Вы можете использовать для связи локальную сеть LAN, или удаленный доступ, типа MS RAS или Notes X.PC. Вы можете также использовать связь с использованием Passthru сервер. При желании, Вы можете соединить сервера через интернет.

Чтобы устанавливать связь, Вы можете создавать документы Подключений в Directory Domino. Документ подключения отвечает за связь и определяет, как и когда сервера должны соединяются для репликации и обмена почтой.

Большинство документов подключений имеет две части, сетевая часть и часть с расписанием. Сетевая часть определяет: какому серверу и как соединяться и как это сделать. Часть с расписанием решает, когда исполнить это действие и какое - тип репликации или маршрутизации на выбранный сервер.

Число документов подключений, которые Вы создаете для сервера, зависит от того, какими задачами управляет сервер. Когда Вы устанавливаете сервер, Server документ по

умолчанию позволяет передачу почты. Вы можете создать документ подключения для репликаций. В зависимости от того, как Вы используете Ваш сервер - Вы должны создать минимум один или два документа подключения на сервер, на который Вы планируете передавать почту или реплицировать данные.

Репликация между парой серверов требует одного документа подключения, на любом из серверов. Требуется только один документ, потому что работа репликатора - то есть запрос сервера, нужен только для соединения с сервером назначения, обмен информацией происходит в обоих направлениях.

Для передачи почты между парой серверов требует один подключения на каждом сервере, потому что маршрутизация почты между серверами работает в только одном направлении.

Например, Для передачи почты с сервера A на сервер B потребуется документ подключения для передачи почты на сервер B. И если сервер B будет передавать почту на сервер A, он нуждается в документе подключения на сервер A.

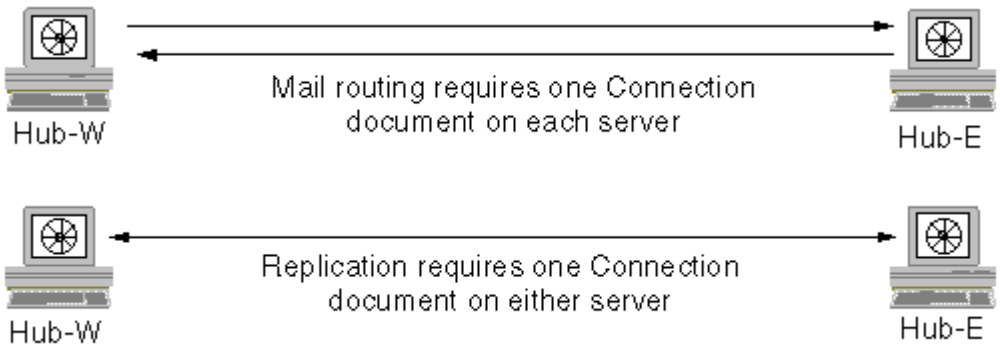


Рис. 28 Пример использования документов подключений для репликаций и передачи почты.

Если Вы хотите передавать посту между Domino и не Domino системой почты, Вы должны создать документ типа Foreign Domain в Directory Domain.

Сервер может также использовать информацию, из документа External Domain Network Information, для установки связи. Как администратор, Вы должны сконфигурировать этот документ, чтобы искать имена и адреса серверов в другом домене. При этом пользователи или сервера не должны будут создать документы подключения, для соединения с сервером в этих доменах.

Прежде, чем Вы создаете документы подключений, планируете топологию серверов связи для Вашей системы.

2.5.1 Как спланировать топологию для серверных подключений?

Вы должны планировать топологию сервера, чтобы потом сконфигурировать документы подключений. Топология - план того, как сервера будут соединяются друг с другом. При планировании топологии сервера, имейте в виду, что число документов подключений нужно свести к минимуму.

Эти факторы влияют на server топологию:

*328 Число серверов в компании.

*329 Находятся ли все сервера в тот же самой или различных Notes поименованных сетях

*330 Расположение Серверов - то есть, находятся ли они в том же самом домене Notes или в разных доменах

*331 Запущены ли задачи на сервере, такие как - репликации или передача почты

*332 Функционируют ли на Сервере задачи Passthru, Dial-In или Служба Удаленного Доступа

Имеются несколько подходов к серверной топологии. В зависимости от вышеупомянутых факторов. Ваша компания может использовать один или большее количество этих подходов в различных частях системы. Некоторые часто используемая топология включают **Hub–and-Spoke** и **Peer–to-Peer**.

2.5.1.1 Использование топологии Hub-and-Spoke.

Топология Hub-and-Spoke требует наличия одного центрального Hub сервера и других серверов, называемых - Spokes. Spokes сервера передают изменения баз данных и почту на Hub сервер, а Hub в свою очередь передает все на все другие сервера. В организациях с боле, чем одним Hub сервером, Hub сервера копирует изменения друг с другом, или с мастером Hub сервером.

Топология Hub-and-Spoke работает лучше всего в больших организациях; это минимизирует движение по сети и наиболее эффективная топология для репликаций. Если Вы используете Hub-and-Spoke, имеете в виду, что Ваша топология уязвима. Она зависит от единственного сервера, а в случае ее отказа, вся топология не работает.

Acme использует Hub-and-Spoke как часть сервер топологии:

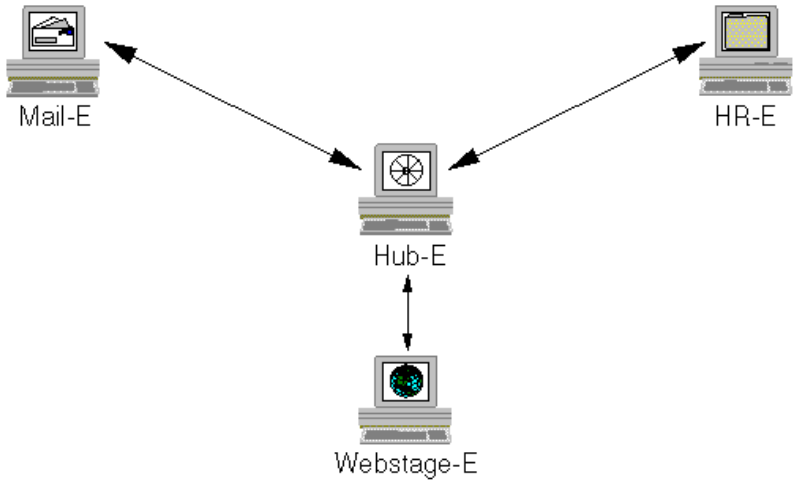


Рис. 29 Пример использования топологии Hub-and-Spoke.

2.5.1.2 Использование топологии Peer-to-Peer.

Топология Peer-to-Peer соединяет каждый сервер в Вашей организации с каждым другим сервером. Эта топология работает лучше всего в компаниях, которые имеют только несколько серверов.

Если бы Acme организовала свои сервера с использованием топологии Peer-to-Peer, топология могла быть построена следующим образом:

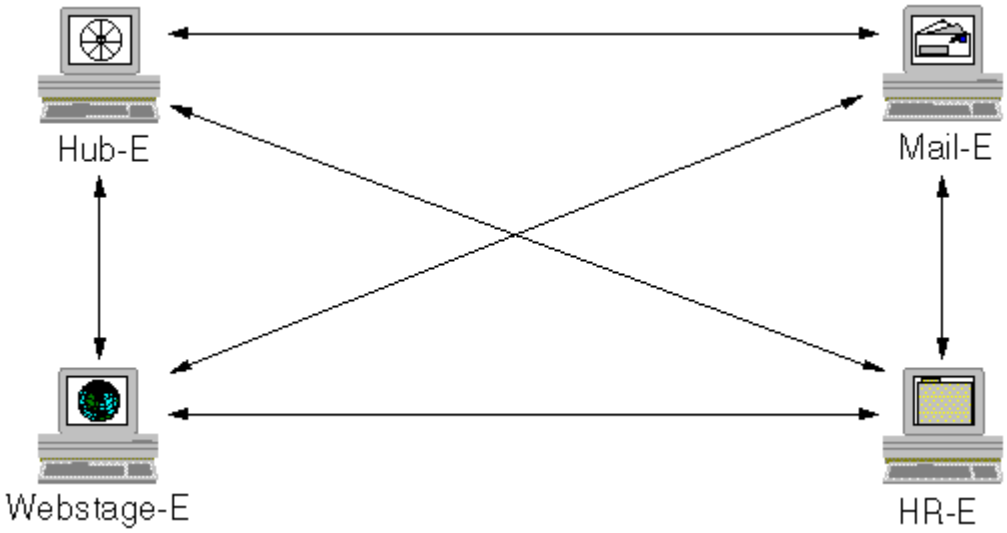


Рис. 30 Пример использования топологии Peer-to-Peer.

2.5.2 Процесс соединения сервера с сервером партнером.

Вы можете описывать связи на сервера, с рабочей станции на другие сервера. Метод для определения пути везде подобен, использует ли Вы документ подключения на рабочей станции или на сервере.

Сервер использует эту логику, чтобы определить, как соединиться с другим сервером:

*333 Сервер пробует соединиться с использованием того же самого метода, который использовался в последний раз.

Обратите внимание на эти два исключения:

*334 Если сервер никогда не связывался с сервером назначения, сервер ищет путь, состоящий из порта сети и любого Passthru сервера на сервер назначения.

*335 Если сервер соединялся с сервером, но связь все время терпела неудачу, сервер ищет новый путь, если это - первая попытка в течение дня.

*336 Для поиска пути на сервер назначения, сервер исполняет эти действия:

- Сервер проверяет, является ли это соединение связью порта WAN на сервер назначения.
- Сервер исследует документы подключения с нормальным приоритетом в Directory. Документы подключения с нормальным приоритетом, которые имеют в поле приоритет значение Normal.

*337 Если имеется несколько документов подключений, нормального приоритета для одного и того же сервера назначения, сервер использует документ в таком порядке:

- Локальная Сеть
- Сеть Dial-Up
- Notes Derect Dial-Up

- Passthru сервер
- Hunt group, Passthru сервера

Если сервер использует Passthru документ, то Notes должен быть способен найти путь к Passthru серверу. Вы можете использовать любой тип документа подключений, чтобы определить этот путь.

*338 Сервер проверяет информацию, сохраненную в памяти, относительно соединений на другие сервера, в Notes поименованной сети. Использует эту информацию, для определения пути к серверу назначения. Сервер читает эту информацию из Server документа, локального Directory Domino.

*339 При соединении локальных серверов, Domino Directory не содержит информации о сервере назначения, он пробует соединяться непосредственно с сервером назначением по сети LAN, используя имя сервера или адрес.

*340 Соединяющийся сервер проверяет низкоприоритетные документы подключений. Низкоприоритетный документ подключения - документ, в котором поле приоритета имеет значение - Low.

*341 Если сервер все еще не может найти путь к серверу назначения, он отображает сообщение, что связь не возможна.

Обратите внимание. Для рабочих станций, соединяющихся с серверами, логика поиска - такая же самая, за исключением того, что рабочая станция пробует использовать Passthru сервер, из документа Место вызова, чтобы организовать связь.

Чтобы проверять, можете ли Вы соединяться с сервером через определенный порт, используйте синтаксис команды на консоли сервера:

```
Trace port!!!servername
```

Вы можете просматривать информацию относительно того, как сервер делает связь, рассматривая информацию различных видов файла LOG.NSF. Вы можете изменять объем информации о связи, регистрируемой в файле LOG, изменяя уровень LOG.

2.5.3 Как создать подключения для сервера?

2.5.3.1 Подключение для двух серверов с использованием сети LAN.

Вы должны создать документ подключения для маршрутизации почты и репликации между серверами в сети LAN. Вы можете также создавать документ подключений, чтобы соединиться два сервера по сети LAN, чтобы гарантировать, что связь использует строго определенный протокол.

*342 Из клиента Domino Administrator, выбирайте закладку Настройка.

*343 Выбирайте Ваш сервер в поле Справочник из, для открытия нужного Domino Directory.

*344 Выбирайте – Сервер и затем выбирайте – Подключения.

*345 Выбирайте – Add Connection.

*346 Выбирайте поле Connection type – Local Area Network.

*347 Заполните поля:

Поля	**Значения**
Source server	Имя Сервера инициатора соединения.
Source domain	Имя Домена сервера инициатора. Это поле используется только для передачи почты.
Use the port(s)	Используемый для соединения порт, сервера инициатора.
Usage priority	Выбирайте следующие опции: *348 Normal - (по умолчанию) *349 Low
Destination server	Имя Сервера назначения.
Destination domain	Имя Домена сервера назначения. Это поле используется только для передачи почты.
Optional network address	Адрес сервера назначения, в зависимости от выбранного Вами протокола. Для TCP/IP, используйте полное имя интернет хоста и домена, или IP адрес. **Пример**, HR-E.Acme.com или 192.22.256.36. Это поле рекомендовано для TCP/IP и других протоколов для указания сетевого адреса.

*350 Нажмите Routing/Replication и затем закладку Schedule, назначьте расписание для Ваших задач, когда по времени, должно происходить соединение с сервером назначения.

*351 Сохраните Документ.

2.5.3.2 Подключение для сервера с использованием Direct Dial-Up (Dial-Up Modem).

*352 Убедитесь, что Вы уже установили модем.

*353 Из клиента Domino Administrator, выбирайте закладку Настройка.

*354 Выбирайте Ваш сервер в поле Справочник из, для открытия нужного Domino Directory.

*355 Выбирайте – Сервер и затем выбирайте – Подключения.

*356 Выбирайте – Add Connection.

*357 Выбирайте поле Connection type – Notes Direct Dial-Up.

*358 Заполните поля:

Поля	**Значения**

Source server	Имя сервера инициатора.
Source domain	Имя домена, сервера инициатора.
Use the port(s)	Имя коммуникационного порта, который будет использовать сервер инициатор.
Always use area code	Yes или No. Это поле определяет, использует ли сервер источник поле Код города, когда делает звонок. По умолчанию - No.
Usage priority	Normal или Low приоритет соединения. По умолчанию – Normal.
Destination server	Имя удаленного сервера.
Destination domain	Имя удаленного домена.
Destination country code	Код страны удаленного сервера.
Destination area code	Код города удаленного сервера.
Destination phone number	Телефонный номер удаленного сервера. Можно вводить несколько номеров, разделяя их точкой с запятой. Сервер будет использовать номера в последовательность, как они введены в этом поле, если предыдущий номер будет занят.

*359 Нажмите Routing/Replication и затем закладку Schedule, назначьте расписание для Ваших задач, когда по времени, должно происходить соединение с сервером назначения.

*360 (Optional) Заполните, если требуется следующие поля:

Поля	**Значения**
Login script file name	Имя скрипт файла, если удаленный компьютер, для соединения, использует скрипт.
Login script arguments	Любые аргументы сценария соединения, необходимые при вызове удаленного сервера, например login или пароль

2.5.3.3 Подключение для сервера с использованием Network Dial-Up.

Вы можете соединять сервера с использованием удаленного доступа к сети, типа MS RAS. Удостоверитесь, что Вы уже установили и сконфигурировали свой сервер для использования службы удаленного доступа.

*361 Из Клиента Domino Administrator, выбирайте закладку Настройка.

*362 Выбирайте Ваш сервер в поле Справочник из, для открытия нужного Domino Directory.

*363 Выбирайте – Сервер и затем выбирайте – Подключения.

*364 Выбирайте – Add Connection.

*365 Выбирайте поле Connection type – Network Dial-Up.

*366 Заполните поля:

Поля	**Значения**
Source server	Имя сервера инициатора.
Source domain	Имя домена, сервера инициатора.
Use LAN port(s)	Порт, который будет использоваться для службы удаленного доступа.
Usage priority	Normal или Low. По умолчанию – Normal.
Destination server	Имя сервера назначения. Можно использовать маски для доступа к нескольким серверам организации -- */Acme.
Destination domain	Имя домена назначения
Optional network address	Адрес сервера назначения. HR-E.Acme.com или 192.22.256.36

*367 Выбирайте закладку Network Dial-Up.

*368 Выбирайте - Microsoft Dial-Up Networking из окна выбора сервисов.

*369 Выбирайте – Edit Configuration и введите в имя удаленного соединения RAS, которое Вы хотите использовать для соединения с сервером назначения.

*370 (Необязательно) Заполните любые из полей, для использования этим соединением RAS и затем щелкайте - OK:

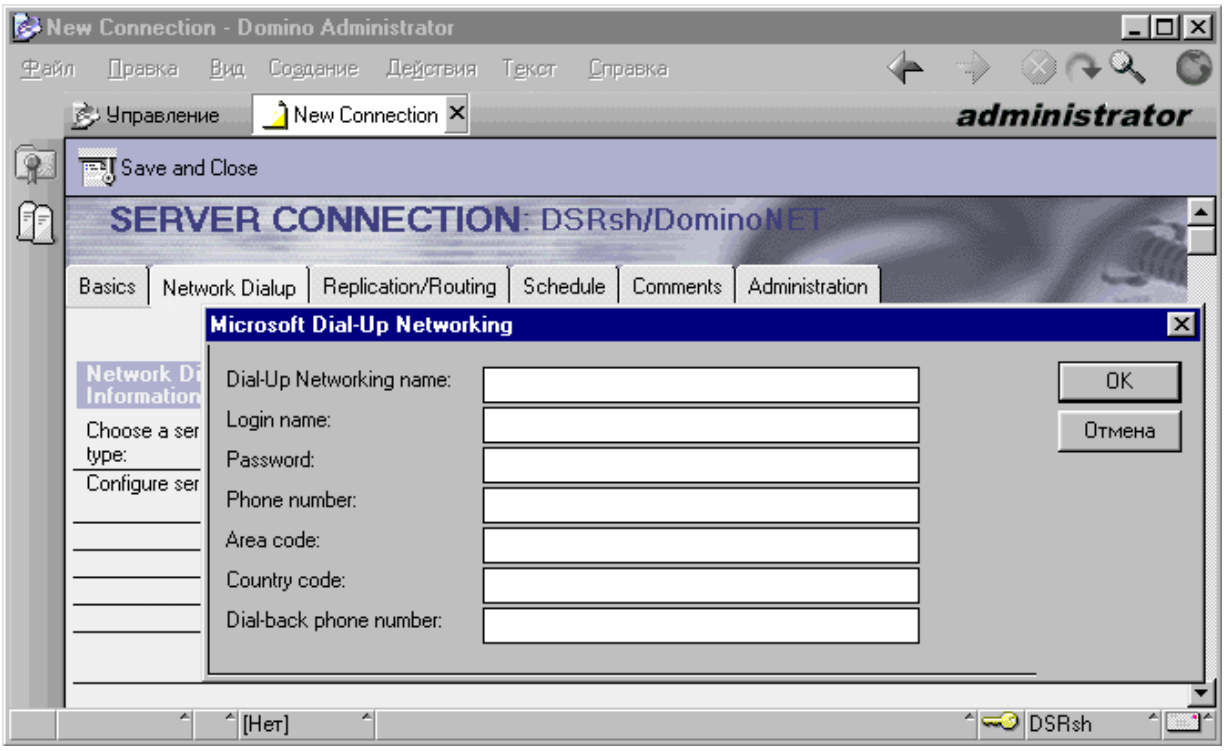


Рис. 31 Диалоговое окно ввода информации о MS RAS, для типа соединения Dial-Up.

Поля	**Значения**
Login name	Имя пользователя, для регистрации в удаленной сети.
Password	Пароль пользователя для регистрации в удаленной сети.
Phone number	Номер телефона сервера назначения.
Area code	Код города удаленной сети
Country code	Код страны удаленного сервера
Dial-back phone number	Полный телефонный номер, Вашего сервера, для использования удаленным сервером, при назначении функции - Calls Back.

*371 Нажмите - Routing/Replication, затем закладку Schedule, назначьте расписание для Ваших задач, когда по времени, должно происходить соединение с сервером назначения.

*372 Сохраните Документ.

2.5.3.4 Шифрование документа подключения Network Dial-Up.

Domino скрывает и шифрует часть параметров документа Network Dial-Up Connection, используя общие ключи определенных пользователей или ID серверов. Когда закончено редактирование, только пользователи и сервера с этими ID могут делать эти виды связи, с использованием этих документов, и могут просматривать параметры в документе.

Обратите внимание. Для документов подключения, созданных до Версии 5.0, Вы можете использовать следующие шаги, чтобы шифровать эти документы. Чтобы только

пользователи и сервера, которые Вы определяете, могли делать связи, с использованием документов и моги просматривать установленные параметры.

*373 Из клиента Domino Administrator, выбирайте закладку Настройка.

*374 Выбирайте Ваш сервер в поле Справочник из, для открытия нужного Domino Directory.

*375 Выбирайте - Сервер и затем выбирайте - Подключения.

*376 Откройте документ Network Dial-Up Connection.

*377 Выбирайте из меню Файл – Свойства Документа.

*378 Выбирайте закладку Безопасность, и отменить опцию - Who can read this document (кто может читать документ).

*379 В поле Public Encryption keys, введите имена пользователей и серверов, кто может иметь доступ к документу, и затем спасают документ.

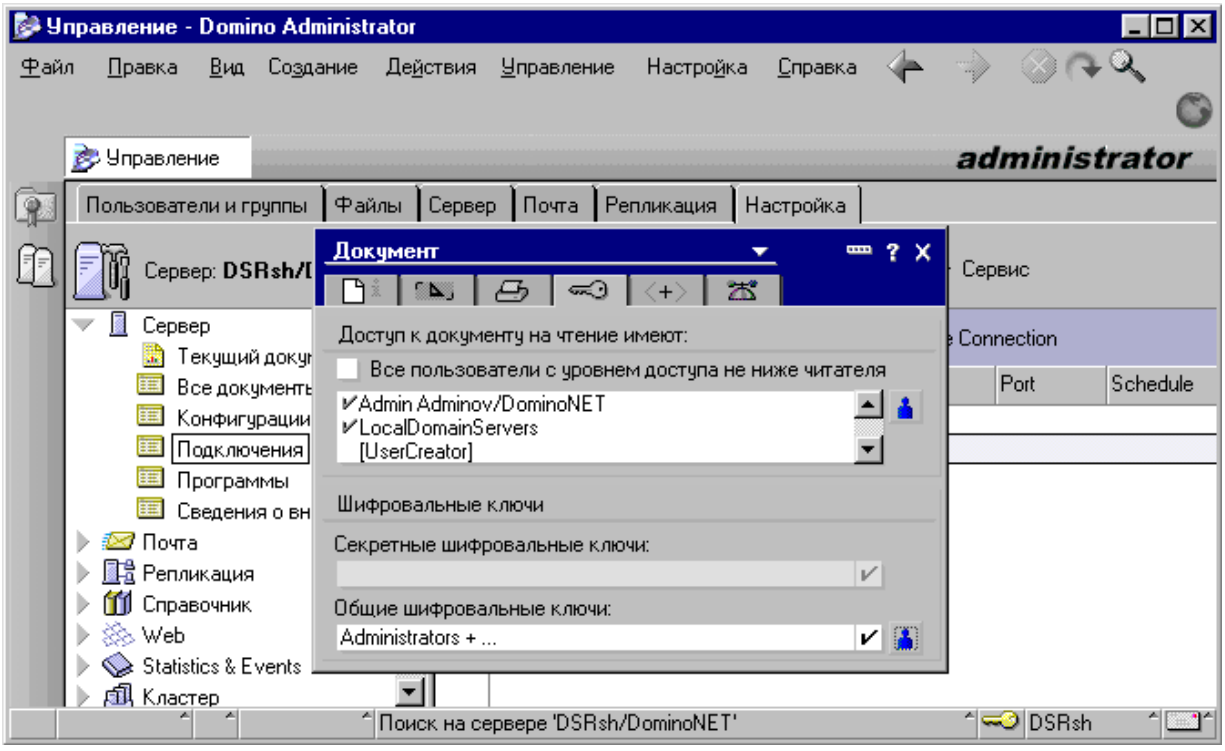


Рис. 32 Диалоговое окно свойств документа подключения, с использованием которого Вы можете ограничивать доступ к нему.

2.5.3.5 Подключение для сервера с использованием Passthru.

После того, как Вы установили Passthru на сервере назначения, Вы можете настраивать сервера, для использования соединения с использованием Passthru сервера.

*380 Из клиента Domino Administrator, выбирайте закладку Настройка.

*381 Выбирайте Ваш сервер в поле Справочник из, для открытия нужного Domino Directory.

*382 Выбирайте – Сервер, затем выбирайте – Подключения.

*383 Выбирайте – Add Connection.

*384 Выбирайте поле Connection type – Passthru server.

*385 Заполните поля:

Поля	**Значения**
Source server	Имя сервера источника.
Source domain	Имя домена сервера источника.
Use passthru server or hunt group	Имя сервера посредника или Hunt Group, для соединения с сервером назначения.
Usage priority	Приоритет для соединения: *386 Normal - (по умолчанию) *387 Low
Destination server	Имя сервера назначения.
Destination domain	Имя домена сервера назначения.

*388 Нажмите Routing/Replication, затем закладку Schedule, назначьте расписание для Ваших задач, когда по времени, должно происходить соединение с сервером назначения.

Если необходимо, создайте документ подключения, если сервер не имеет прямого соединения с Passthru сервером по сети LAN.

Примечание. Удостоверьтесь, что сервер источник не имеет по умолчанию Passthru сервера с этим именем. Проверьте, что в поле Passthru server (секция Server Location – Basics) в Server документе пусто. Это поле заставляет сервер отправлять все запросы связи, которые он не может установить, на сервер внесенный в это поле.

2.5.4 Какой приоритет использует Domino, при выборе использования документов подключений?

Если несколько портов функционирует на одном сервере, Вы можете заставить Domino использовать порт, который Вы определили в документе подключения, выбирая в поле приоритета документа, значение - Нормальный. Вы можете использовать этот выбор, чтобы выбрать определенный порт сети, чтобы использовать его между двумя серверами.

Например. На сервере разрешены SPX и TCP/IP порты. Имеется документ подключения, определяющий TCP/IP с приоритетом - Нормальный. Domino сначала смотрит документы подключение, находит TCP/IP порт определенный как нормальный и выбирает этот порт. Приоритет использования работает так же для модема, X.25, Dial-Up, Passthru Connection документов.

*389 Из клиента Domino Administrator, выбирайте закладку Настройка.

*390 Выбирайте Ваш сервер в поле Справочник из, для открытия нужного Domino Directory.

*391 Выбирайте – Сервер, затем выбирайте – Подключения.

*392 Откройте документ подключения, которой Вы хотите использовать и выбирайте – Edit Connection.

*393 Заполните поля:

Поля	**Значения**
Usage priority	Приоритет для соединения: *394 Normal - (по умолчанию) *395 Low

2.5.4.1 Соединение Сервер – Сервер, с использованием интернета.

Создайте документ подключения, чтобы соединить Domino сервер с другим Domino сервером через интернет, чтобы наметить задачи для серверов, типа репликаций или передачи почты.

Для Установки связи сделайте следующее:

*396 Выясните адрес IP или имя хоста сервера назначения.

*397 Создайте Server документ подключения в Domino Directory, для сервера.

*398 Редактируйте Server документ из Domino Directory, для соединяющегося сервера, при соединении через Proxy сервер.

2.5.4.2 Создание документа подключения для соединения серверов через интернет.

Вы создаете Server документ подключения, чтобы наметить репликации и маршрутизации почты для серверов по интернету.

*399 Из клиента Domino Administrator, выбирайте закладку – Настройка.

*400 Выбирайте Ваш сервер в поле Справочник из, для открытия нужного Domino Directory.

*401 Выбирайте – Сервер и затем выбирайте – Подключения.

*402 Выбирайте – Add Connection.

*403 Выбрать Local Area Network, в поле Connection type. Вы можете также использовать Dial-Up тип связи.

*404 Заполните поля:

Поля	**Значения**
Source server	Имя сервера источника

Source domain	Имя домена сервера источника
Use the Port(s)	TCPIP - порт и протокол, который будет использоваться при соединении через интернет
Usage priority	Normal или Low. По умолчанию – Normal.
Destination server	Имя сервера назначения
Destination domain	Имя домена сервера назначения
Optional network address	HR-E.Acme.com или 192.22.256.36.

*405 Выбирайте - Routing/Replication - Schedule, для назначения расписания для Вашего документа связи.

*406 Сохраните документ.

*407 Если соединение использует Proxy сервер, измените Server документ для использования Proxy сервера.

2.5.4.3 Создание документа подключения для двух серверов, через интернет, с использованием Proxy сервера.

*408 Из клиента Domino Administrator, выбирайте закладку Настройка.

*409 Выбирайте Ваш сервер в поле Справочник из, для открытия нужного Domino Directory.

*410 Выбирайте Сервер и затем выбирайте – Все документы сервера.

*411 Открывайте Server документ сервера, которым Вы хотите соединиться через интернет через Proxy и щелкайте – Редактировать Сервер.

*412 Выбирайте – Ports – Proxies и затем сделайте одно из следующего:

- Если Вы соединяетесь через HTTP Proxy, введите полное имя хоста, домена или IP адрес HTTP Proxy и номер порта. Например, ведите в это поле proxy.company.com:8080 или 192.168.77.34:8080.

- Если Вы соединяетесь через SOCKS Proxy, введите полное имя хоста, домена или IP адрес SOCKS Proxy и номер порта. Например, ведите в поле proxy.company.com:1080 или 192.168.77.34:1080.

Обратите внимание, если Вы ввели данные для обоих полей, Domino использует HTTP Tunnel proxy.

*413 Сохраните документ.

*414 Если Вы соединяетесь через Domino Passthru сервер, создаете Passthru документ подключения для Passthru сервера.

Обратите внимание, если Вы имеете конфигурацию Proxy, сервер использует Proxy для всех соединений. Для связей, которые не требуют, Proxy сервера, введите в имени сервера в No Proxy для этих хостов, или в секции domains на вкладке Ports – Proxies в Server документе сервера.

2.5.5 Как выполнить трассировку сетевого соединения между серверами?

Чтобы проверить, можете ли Вы соединяться с сервером, используйте Trace Connection. Результаты Trace Connection выдают Вам детальную информацию о соединении с сервером и проблемах связи по сети.

Когда Вы пытаетесь соединяться с сервером, информация автоматически появляется в строке статуса рабочей станции Notes или на консоли сервера, в зависимости от того, где Вы ввели трассировку связи. Вы можете использовать переменную NOTES.INI файла Console_LogLevel, чтобы управлять уровнем детализации, отображения сообщений.

Чтобы выполнить трассировку, введите команду на консоли сервера:

```
Trace servername
```

2.5.6 Для чего используется документ EDNI?

Документ External Domain Network Information (EDNI) позволяет пользователям соединяться более легко с серверами, которые не принадлежат Вашему домену. Без этого документа, Domino пользователи будут нуждаться в документах подключения, сделанных для серверов, во внешних доменах. EDNI документ из Domino Directory и содержит имена и адреса серверов из внешних доменов, которые используют специфический протокол. Когда пользователи пробуют соединиться с серверами из внешних доменов.

При создании EDNI документа, Вы определяете домен, в котором находятся сервера, и определяете протокол. Во многих случаях, TCP/IP - единственный протокол. Вы также определяете сервер в Вашем локальном домене, который запрашивает информацию, Requesting Server и сервер во внешнем домене, который снабжает информацией Information Server.

Перед созданием EDNI документа, определите, является ли информация о связи, полезна для Вашего домена. Например, если Вы используете NetBIOS протокол, который не может быть маршрутизирован, то прямая связь к внешнему домену не может быть установлена, даже если Вы имеете адрес сети сервера в EDNI документе. Также, если внешний сервер домена имеет несколько TCP/IP портов, адрес возвращенный EDNI документу не может быть адресом соответствующего порта, чтобы его можно было использовать. Потому что каждый протокол имеет собственные ограничения, Вы должны полностью исследовать и проверять способность поиска домена, используя информацию о сети в Вашей организации перед использованием этой особенности.

Вы можете создавать EDNI документ с любого сервера в локальном домене. В намеченное время, которое Вы определяете, Requesting Server соединяется с внешним сервером домена и обновляет информацию об адресах серверов. Эта информацию размещается в запросе на обработку для процесса администрирования серверов. Когда сервер администрирования обрабатывает запрос, он помещает информацию в ответ на EDNI документ, в Domino Directory.

Т.к. Requesting Server собирает информацию из Server документов, внешнего домена, эти документы должны быть сконфигурированы должным образом, чтобы позволять поиск имен серверов. Например, документ с полным именем хоста или адресом IP, позволит

произвести поиск, но документ только с общим именем не может возвратить результаты поиска, т.к. он не содержит IP адреса хоста.

EDNI документ работает с серверной задачей Getadrs. Удостоверьтесь что задача Getadrs, запущена.

Настройка документа External Domain Network Information.

*415 Из клиента Domino Administrator, выбирайте закладку Настройка.

*416 Выбирайте Ваш сервер в поле Справочник из, для открытия нужного Domino Directory.

*417 Выбирайте – Сервер и затем выбирайте – External Domain Network Information.

*418 Выбирайте – Add External Domain Network Information.

*419 Заполните эти поля и выбирайте – Сохранить и Закрыть:

Поля	**Значения**
Requesting server	Имя сервера запрашивающего информацию из внешнего домена
Information server	Имя сервера из внешнего домена, отвечающего на запросы
Domain to query	Имя внешнего домена
Protocols to query	Имя одного протокола, из внешнего домена, который будет обслуживать запрос

2.6 Как планировать репликации баз данных?

Чтобы сделать базу данных доступной пользователям в различных отделах, офисах, в различных сетях, или в различных часовых поясах, Вы создаете реплики баз данных. Все реплики имеют одинаковые ID реплик, которые создаются при создании база данных. Имена файлов баз могут быть различные, каждая копия может содержать различные документы, или иметь различный дизайн базы. Однако если их ID реплик идентичны, между этими базами данных могут происходить репликации.

Поскольку пользователи добавляют, редактируют, удаляют документы в базах данных, со временем, содержание баз данных становится не идентичным. Чтобы синхронизировать содержание данных во всех копиях, Вы используете документ подключения, для определения репликаций между серверами, которые хранят реплики этих баз данных. Тогда пользовательские изменения, замены в одной базе данных, будут распространяться в другие реплики базы, для других пользователей, кто имеет доступ к этим данным. Кроме того, использование реплик и планирования репликаций уменьшает движение данных по сети. Пользователи не должны соединиться с центральным единственным сервером, который хранит единственную реплику базы данных. Вместо этого, они могут иметь доступ к репликам базы данных на разных серверах.

Эти реплики баз данных могут также быть доступными через Web. При этом пользователи не зависят ни от одного сервера, когда они делают попытку доступа к критическим данным деловых процессов, по интернету. Если один сервер недоступен, пользователи могут иметь

доступ к другой реплике этой базы данных на другом сервере. Вы можете также использовать реплики, чтобы помочь управлять продолжающимся проектом, на участке Web. На выбранном сервере Вы можете устанавливать Web, где проектируете и проверяете новые страницы баз данных. Когда изменения (замены) проекта проверены и готовы к публикации, Вы можете реплицировать этот сервер на Web участок, который является доступным всем пользователям. Используя реплики, Вы ограничиваете Web пользователей от наблюдения Вашего делового процесса разработки приложений.

Создание новой реплики базы данных отличается от копирования базы данных, когда Вы выбираете из меню опция из меню Файл - База данных – Копия... Хотя копия базы данных может выглядеть точно так же, как и база, данных оригинала, копия и оригинал имеет разные ID реплики и, значит, не будет участвовать в репликациях.

2.6.1 Когда именно нужно создавать реплики баз данных?

Планируйте Вашу стратегию репликаций тщательно и создайте реплики на серверах, только когда это необходимо. Чем большее количество реплик, тем больше требование к серверу и сетевым ресурсам. Чтобы ограничить ненужное увеличение реплик, назначите права создания реплик на сервере только некоторым администраторам.

Создание реплики базы данных:

*420 Улучшите выполнение работ, тяжело используемой базы данных

*421 Распределяет нагрузку на сеть

*422 Держать базы данных, которые вы проектируете, отдельно от рабочих версий.

*423 Держит базу данных доступной, даже если один из серверов закрывается

*424 Делает базу данных доступной, для удаленных пользователей

*425 Разместив реплику шаблона на каждом сервере, Вы наследуете дизайн, для всех реплик баз данных расположенных на этом сервере.

*426 Если Вы создайте резервную копию (реплику) базы данных, Вы можете восстановить информацию, если основная база данный будет повреждена

Имейте в виду, что две реплики, всегда будут содержать слегка различное содержание, в промежутке между репликациями. Если пользователи нуждаются в доступе к наиболее современной информации в базе данных, Вы можете создавать реплики на кластере серверов и затем назначить репликации, для групп серверов. В кластере серверов, все реплики всегда идентичны, потому что каждое изменение (замена) немедленно копируется на другой сервер кластера.

2.6.2 Как происходит процесс репликаций между двумя серверами?

Для типа репликации сервер - сервер, задача Replicator на одном, вызывающем сервере, требует присутствия документ подключения в адресной книге сервера. Использование этого документа должно быть разрешено и для него должно быть намечено расписание соединения. По умолчанию задача Replicator загружается при запуске сервера.

Чтобы наметить репликацию между серверами, Вы создаете документы подключений, которые описывают, когда сервера должны соединяться для репликаций. Поскольку пользователи добавляет, редактирует и удаляет документы в базах данных, реплики баз, содержит слегка различную информацию в период между репликациями серверов. В

процессе репликации передаются только изменения базы данных, поэтому передача по сети и затраты на связь сводятся к минимуму.

В течение намеченной репликации, по умолчанию, сервер сначала забирает измененные документы с сервера назначения, а затем выталкивает изменения на сервер.

Вы можете также использовать серверную командует - Pull, Push и Replicate, чтобы начать репликацию между серверами немедленно.

2.6.2.1 Что происходит при репликации между двумя серверами?

*427 Replicator остается не задействован, пока сервер A не начинает репликацию на сервером B.

*428 Поскольку акции безопасности вступают в силу до репликации, два сервера подтверждают свою подлинность сравнением своих публичных и личных ключей. Сначала, два сервера находят общие сертификаты. Затем, они проверяют сертификаты друг друга, для гарантирования, их подлинности.

*429 Два сервера сравнивают списки баз данных, чтобы найти базы данных с идентичными копиями ID.

*430 Сервера проверяют время последнего изменения каждой из баз данных, чтобы видеть является ли это время более позднее, чем дата успешной прошлой репликации, зарегистрированной в истории репликации. Этот шаг позволяет серверам решить, что в базе данных должно копироваться.

*431 Для каждой измененной базы данных, сервера строят список из документов, элементов дизайна и изменений в ACL, которые произошли, начиная с последней репликации с другим сервером.

*432 Для каждого изменяемой базы данных, сервер A проверяет ACL базы, чтобы определить, какие изменения сервер B может сделать в реплике, а сервер B проверяет ACL, чтобы определить то, какие изменения сервер A может сделать.

*433 Если передача документов, дизайна и изменения в ACL разрешено для документов, сервер реплицирует только поля, которые изменились, при этом не копирует документы полностью. Для документов, которые были удалены, остаются “окурки”. Чтобы экономить место на диске, Domino удаляет эти “окурки” согласно интервалу чистки, который установлен в назначениях репликаций баз данных.

В зависимости от выше перечисленных действий, происходит одно из следующего:

*434 Если репликация заканчивает успешно, сервер A вписывает время в истории репликации сервера B, когда репликация была закончена. Сервер B использует такую же печать времени для сервера A, чтобы делать тот же самое.

*435 Если репликация не заканчивается успешно, отметки времени не регистрируются в истории репликации - так, чтобы будущее репликации будут использовать более раннюю метку времени. Неудавшиеся репликации регистрируются в виде Replication базы данных LOG.NSF.

Рассмотрите следующие аспекты при планировании графика репликаций:

*436 Топология Репликаций

*437 Число документов подключения, которое Вам понадобится для реплик

*438 Тип репликаций

*439 Время репликаций

*440 Базы данных, которые будут участвовать в репликациях

*441 Приоритет баз данных, которые будут реплицироваться

*442 Время ограничения для репликаций

*443 Запуск нескольких копий репликатора

2.6.3 Топология системы репликаций.

В Domino системе с больше чем одним сервером, Вы должны планировать топологию, которая решает, как соединять сервера при репликах.

Вы определяете топологию, создавая документы подключения в Domino Directory. Поскольку Вы планируете топологию, Вы должны рассмотреть и топологию движения почты и репликаций. Репликации между серверами требует одного документа подключения. Однако маршрутизация почты требует двух документов подключений, так как все это работает только в одном направлении. Часто более эффективно создавать сначала документы подключений для передачи почты, а затем добавлять репликации к этим же самым документам.

Топология репликаций обычно дублирует топологию Вашей Domino системы, и она обычно изменяется с размером Вашей организации. Маленькие фирмы используют топологию Peer-to-Peer, которая быстро распространяет изменения на все сервера, но неэффективна, когда появляется несколько серверов. Фирмы среднего размера могут использовать комбинацию репликаций Peer-to-Peer или могут осуществлять Hub-and-Spoke репликации. Большие организации, вероятно, будет использовать Hub-and-Spoke репликации, для максимальной эффективности или могут использовать кольцевую топологию репликаций между Hub серверами. Как Вы наметите свои репликации, зависит от Вашей серверной топологии и стратегии репликаций, которую Вы выбираете. Например, Acme корпорация использует Hub-and-Spoke топологию.

2.6.3.1 Использование топологии репликаций Hub-and-Spoke.

Hub-and-Spoke - наиболее эффективная топология для репликаций, потому что она минимизирует движение данных в сети, особенно в больших организациях. Hub-and-Spoke устанавливает один центральный сервер Hub, который намечает и начинает все репликации со всеми другим серверами типа Spokes. Spokes сервера передают на Hub сервер все свои изменения и почту, а Hub в свою очередь передает все изменения на каждый другой сервер. Hub сервера реплицируют изменения между собой или на мастер Hub серверов, в организациях которые используют больше чем один Hub. Короче говоря, Hub сервер действует как менеджер репликаций и почты в системе.

Чтобы наметить репликации в системе по типу Hub-and-Spoke, Вы создаете один документ подключения для каждой связи Hub-and-Spoke. В каждом документе подключения, Hub сервер - всегда сервер источник, а сервер назначения, всегда один из серверов Spoke.

Топология Hub-and-Spoke может быть особенно полезна, в целом для нескольких серверов, в централизованном офисе, который должен соединиться через телефонные или выделенные линии с региональными офисами. Если Вы имеете большой участок сети, Вы

можете использовать комбинацию топологий Hub-and-Spoke и Peer-to-Peer между двумя Hub серверами.

Применение топологии репликаций Hub-and-Spoke:

*444 Установите несколько протоколов на Hub сервера, чтобы позволить связь в Domino системе, которая будет использовать больше чем один протокол. Hub сервер может соединять с несколькими Notes поименованными сетями, где имеются отдельные Hub сервера.

*445 Используйте несколько частей сети - например, LAN и WAN.

*446 Централизуйте администрирование Domino Directory, ACL стандартизируйте базы данных. Ограничьте доступ на Hub сервера. Вы можете определить в ACL, Hub серверам - с доступом Менеджера, а Spokes - доступ Читателя, чтобы делать изменения в одной точной копии на Hub сервере.

*447 Разместите программы серверов, например агентов, на Hub серверах, чтобы делать их легко доступными.

*448 Соедините удаленные участки сети с Hub серверами.

*449 Минимизируйте движение сети, и максимизировать эффективность сети.

*450 Централизуйте данные, создайте резервные Hub сервера.

*451 Улучшите балансировку нагрузки на серверов. Однако движение по сети увеличивает нагрузку на сегменты сети с установленными серверами Hub. Если Вы имеете больше чем 25 серверов, установите несколько Hub серверов. Если Hub сервер выключается, репликации для этих Hub и Spokes будут недоступны, пока Hub сервер не будет восстановлен или заменен.

Примечание. Не использует Hub-and-Spoke репликации для баз данных, размер которых большей чем 100МБ. Реплицируйте базу данных непосредственно между серверами, намечая репликации для этой базы данных в документе подключения.

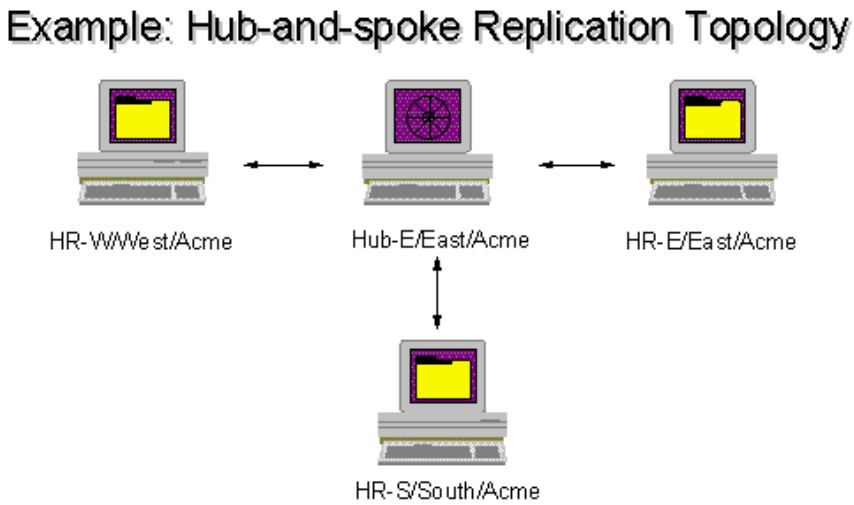


Рис. 33 Пример использования топологии Hub-and-Spoke для репликаций.

В этом примере, Acme корпорация имеет один Hub сервер, Hub-E/East/Acme и три Spoke сервера. Spoke сервера - HR-E/East/Acme, HR-S/South/Acme, HR-W/West/Acme - содержат служебные приложения. Любые изменения, замены в приложениях реплицируются через

Hub-E/East/Acme на HR сервера. HR сервера посылают изменения, замены Hub, которые в свою очередь посылает изменения на все HR сервера, используя для этого Hub.

С тремя документами подключения, которые Acme создал, Hub сервер исполняет репликации, сокращая нагрузку на Spokes сервера. При создании приложений, доступных на East, West, пользователи South запрещают их распространение через дорогостоящие связи WAN.

2.6.3.2 Использование топологии репликаций Peer-to-Peer.

Топология Peer-to-Peer соединяет каждый сервер в Вашей организации с каждым другим сервером. Эта топология неуправляема в организациях с большим числом серверов. Однако в маленьких организациях, эта топология гарантирует быстрое обновление данных. При использовании топологии Peer-to-Peer, потенциал для проблем репликаций уменьшается, потому что только два сервера связываются для каждой репликации и не требуют Hub, или посредника сервера. Однако Peer-to-Peer репликации требует многих документов подключений, увеличения администрирования, так как Вы должны избежать накладок в графиках репликаций

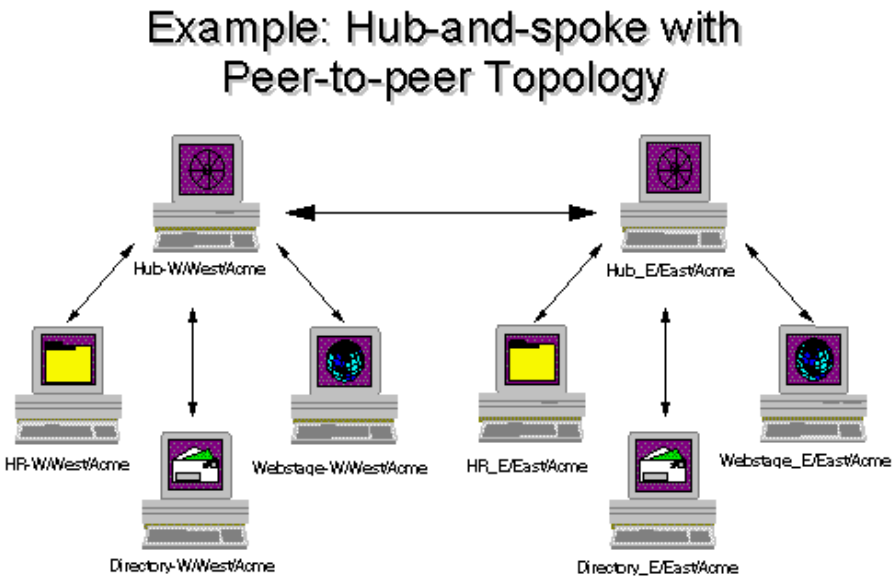


Рис. 34 Пример использования топологии Peer-to-Peer для репликаций.

В этом примере, Acme корпорация имеет два Hub сервера - Hub-W/West/Acme и Hub-E/East/Acme – связывающихся для репликаций по топологии Peer-to-Peer. Каждый Hub сервер реплицирует изменения с несколькими Spoke серверами. Любые изменения, замены через Hub доставляются на Spoke сервера. Spoke сервера посылают изменения, замены на Hub, а затем Hub реплицирует их друг с другом, и посылают изменения назад на Spoke сервера.

Иные топологии репликаций.

Другие менее эффективные стратегии топологии репликаций следующие:

Кольцо, которое соединяет сервера в круг, является подобно непрерывной топологии, но со связанными концами так, чтобы репликации происходят в закрытой петле.

От начала до конца, также известна как топология цепи, где два или больше серверов реплицируют данные последовательно с одного на другой на цепочке.

Двоичное дерево, которое соединяет сервера в пирамиду: вершина сервер соединяется с двумя серверами ниже, каждый из которых соединяется с двумя серверами ниже, и так далее.

2.6.4 Документы подключений для репликаций.

Для репликаций между двумя серверами, Вы создаете документ подключения, который определяет, как и когда происходит обмен изменениями. Используйте только один документ подключения одновременно, чтобы обратиться ко всем репликам между каждой парой серверов. Создание ненужного документа подключения увеличивает сетевой трафик.

Передача почты и репликации разрешаются по умолчанию, но Вы можете изменять эти установки и использовать отдельные документы подключений, чтобы наметить график для каждой из задач. Этим путем, Вы можете управлять диапазоном времени, или интервалом повторения для реплик и передачи почты раздельно.

Как Вы соединяетесь с серверами для репликаций, зависит от местоположения серверов. Вы можете соединять сервера для реплик по локальной сети или по телефонной линии, с использованием модема или службы удаленного доступа. Кроме того, Вы можете использовать Passthru сервера для репликаций.

Репликации по интернету выполняются, так же как и по сети LAN с использованием TCP/IP. Domino сервер должен быть в том же самом Notes домене, что и Domino сервер, с которым Вы хотите реплицироваться. Если они находятся в разных доменах, сервера нуждаются во взаимных сертификатах.

Настройка документов подключений для репликаций.

Назначайте только один сервер, для соединения в одно и тоже время.

*452 Удостоверитесь что:

- Вы создали документ подключения, чтобы соединить каждую пару серверов.
- Domino Directory копируется должным образом.

*453 Заполните эти поля:

Поля	**Значения**
Usage priority	Приоритет – Normal (используется по умолчанию)
Source server	Имя вызывающего сервера
Source domain	Имя вызывающего домена
Use the Port(s)	Используемый порт и протокол для установления соединения.
Destination server	Имя сервера назначения
Destination domain	Имя домена назначения

*454 Выбирайте закладку Routing/Replication и заполните эти поля:

Поля	**Значения**
Replication task	Выбирайте – Enabled
Replicate databases of Priority	Выбирайте приоритет: *455 High *456 Medium & High *457 Low & Medium & High (по умолчанию)
Replication type	Выбирайте тип репликации: *458 Pull Pull *459 Pull Push (по умолчанию) *460 Pull Only *461 Push Only
Files/Directories to Replicate	Вы можете выбрать конкретно, что именно реплицировать. Внесите в список несколько баз или каталогов, разделяя их точкой с запятой.
Replication Time Limit	Можете указать лимит времени для реплик

*462 Выбирайте закладку Schedule и заполните эти поля:

Поля	**Значения**
Schedule	Выбирайте – Enabled, для разрешения расписания
Call at times	Укажите Время вызова сервера назначения По умолчанию 8 AM - 10 PM
Repeat interval of	Интервал повторения вызовов По умолчанию 360 минут
Days of week	Укажите дни недели для соединений По умолчанию Sun, Mon, Tue, Wed, Thu, Fri, Sat

2.6.4.1 Выбор типа направления репликаций.

Когда Вы выбираете направление репликаций, Вы определяете для сервера, будет ли он посылать, или получать изменения. Направление, которое Вы выбираете, не затрагивает функциональные возможности процесса репликаций.

По умолчанию, Domino использует тип репликации - Pull-Push. Однако Вы можете определить различное направление для типа реплик.

Pull-Push - по умолчанию направление репликаций, является двухсторонним процессом, в котором опрашивающий сервер сначала забирает изменения, а затем выталкивает собственные на сервер назначения. При использовании типа репликаций Pull-Push, задача репликатор выполняется на сервере инициаторе.

Pull-Pull - двухсторонний процесс, в котором два сервера обмениваются изменениями. В схеме Pull-Pull используются, два репликатора - один на сервере инициаторе и один на отвечающем сервере.

Push-only - односторонний процесс, в котором запрашивающий сервер выталкивает изменения на сервер назначения.

Pull-only - односторонний процесс, в котором запрашивающий сервер притягивает изменения.

Чтобы изменять направление репликаций, откройте документ подключения и затем, в поле - Replication Type, укажите тип реплики для вызывающего сервера.

Вы можете также определить направление реплик, когда Вы вынуждаете реплику вручную. Например, Вы могли бы использовать метод Push-only, или Pull-only указывая выбранный метод на консоли сервера

2.6.4.2 Расписание репликаций.

Всегда планируйте репликации на время, когда деятельности в Вашей сети минимальна.

Вы можете наметить репликации Сервер - Сервер, на определенное время, или Вы можете определить диапазон времени с интервалом повторения. Намечая репликацию в диапазоне времени, Вы гарантируете, что сервера обмениваются информацией несколько раз в день. После того, как сервер сделает успешную попытку реплики, он ждет интервал времени, указанный в поле Repeat interval of, в документе подключения, перед следующим запросом сервера.

Пример. Предположим, что документ подключения намечает репликацию с Hub-E/East/Acme на сервер HR-E/EAST/ACME, с 8 AM до 5 PM с интервалом повторения 120 минут. Если Hub-E/East/Acme вызывает партнера по репликации и, реплицируется успешно в 8:30 AM, Hub-E/East/Acme сделает следующий запрос на репликацию в 10:30 AM.

Убедитесь, что учитываете часовые пояса, когда намечаете репликации между серверами в различных странах.

Если Вы хотите копировать документы, созданные в течение пиковых часов работы сервера, то намечайте репликации на не пиковое время, учитывайте в расчетах часовой пояс.

Например. Чтобы наметить репликацию между сервером в Нью-Йорке и сервером в Германии, наметьте репликацию между 3 AM и 1 PM по EST, чтобы будет соответствовать рабочим часам в Германии, которые на шесть часов позже, чем EST.

По умолчанию установки репликаций – с 8 AM до 10 PM, с интервалом повторения 360 минут.

Планирование репликаций в заданное время.

Используйте определенное время для репликаций низкоприоритетных баз данных, когда ежедневная модернизация баз данных достаточна, или когда Вы уверенны, что сервера

соединяться успешно после нескольких попыток. Вы можете реплицировать низкоприоритетные базы данных ночью, когда меньше всего загружена Ваша система.

В документе подключения, введите в поле Call at times - например, 8 AM. Введите 0 (ноль) для интервала повторения, так как связь не будет основана на диапазоне времени. Сервер позвонит, и соединиться в 8 AM. Если попытка будет неудачна, сервер попробует соединиться в течение часа. Если в течение часа связь не будет установлена, следующий запрос будет сделан в 8 AM следующего дня.

Планирование разовых репликаций, в определенные часы времени.

Используйте список, из определенных часов, чтобы наметить репликации для средне и низкоприоритетных баз данных, для которых несколько ежедневных репликаций баз будет достаточно, или когда вы уверенны, что попытки связи будут успешны после нескольких повторений. Например, можно использовать этот метод, для связи в различных сегментах сети, на том же самом участке сети.

В документе подключения, введите в поле Call at times значения - 8 AM, 1 PM, 4 PM. Введите 0 (ноль) для интервала повторения, так как связь не будет основана на интервале времени. Сервер сделает первую попытку в 8 AM. Если попытка будет неудачна, сервер будет повторять попытки в течение часа, до 9 AM. Следующий запрос произойдет в следующее намеченное время - 1 PM. Если попытки будут неудачны, сервер будет, повторяет попытки в течение часа, до 2 PM. Этот процесс продолжается в течение каждого определенного времени, которое Вы определяете.

Планирование репликаций в определенный интервал времени с интервалом повторения.

Определите диапазон времени, когда Вы намечаете репликации для баз данных высокого приоритета. В документе подключения, введите диапазон времени в поле Call at times, введите минуты в поле Repeat interval. Например, введите в поле Call at times интервал 8 AM - 5 PM, а в поле Repeat interval - 120 минут.

Если первый запрос неудачен в 8 AM, сервер будет периодически повторять попытки, пока не произойдет успешная репликация. Если сервер не может соединиться, он будет продолжать пробовать соединится до конца диапазона времени - 5 PM. Если сервер успешно соединится, повторное соединение будет через 120 минут после предыдущего законченного запроса.

Планирование репликаций в определенный интервал времени, но без интервала повторения.

Используйте диапазон времени без интервала повторения, для средних и низкоприоритетных баз данных. Также используйте диапазон времени без интервала повторения, когда ежедневной модернизации базы данных достаточно. Или, если Вы имеете занятые телефонные линии и знаете, что может потребоваться несколько попыток, для установки связи.

В документе подключения, введите в диапазон времени в поле Call at times - например, 8 AM - 5 PM. Введите 0 (ноль) для интервала повторения. Сервер делает первую попытку в 8 AM. Если попытка неудачна, сервер пробует снова и снова.

Время между запросом все время увеличивается, с каждой неудачной попыткой. Сервер повторяет призыв в течение всего диапазона, или пока связь не будет установлена. После неудавшегося запроса, сервер повторяет периодически запросы. Однако он перестает звонить, после успешного обмена информацией.

Планирование репликаций в определенный день недели.

Вы можете создавать различный график репликаций в течение различных дней недели. В документе подключения, введите дни, на которые Вы хотите запланировать репликацию.

Пример. Создайте два документа подключения. Сервер намечает репликации с понедельника по пятницу, второй в субботу и воскресенье.

Стратегия расписаний репликаций.

Вы можете использовать топологию Hub-and-Spoke. Например, Вы могли бы наметить репликацию первого сервера с 8 AM до 10 AM, следующего сервера с 8:05 AM до 10:05 AM и так далее. Вы можете создавать простой график коллективных реплик для Hub сервера, повторяя их так часто как нужно. Этот процесс распространяет все данные в пределах сферы влияния Hub сервера очень быстро.

2.6.4.3 Репликация только выбранных баз данных.

По умолчанию, Domino реплицирует все базы данных, которые имеют одинаковые ID реплик. Для реплик только определенных баз данных, редактируйте поле File/Directories to Replicate в документе подключения. В это поле, введите имена баз данных или имена каталогов, которые Вы хотите реплицировать. Отделите их друг от друга, точкой с запятой.

Чтобы определить выбранную базу данных для репликации, введите ее имя файла, включая .NSF расширение. Если база данных находится в подкаталоге, включите путь относительно каталога данных Notes - например, EAST\SALES.NSF.

Чтобы определить все файлы расположенные в каталоге, введите EAST\. Вы не можете использовать для этой цели звездочку (*).

2.6.4.4 Репликации баз данных согласно их приоритетов.

Менеджеры Базы данных назначают приоритет репликаций базам данных так, чтобы Domino администраторы могли наметить репликации для баз данных, основанных на приоритете. Например, Вы можете наметить первоочередной приоритет для баз данных, которые являются критическими для делового процесса - например, Domino Directory реплицируется часто. Вы можете наметить так же низкоприоритетные базы данных.

Установки репликаций с использованием приоритета, редактируются в поле Replicate databases of документа подключения. Установка по умолчанию Low & Medium & High priority.

Если двум репликам назначены, различные приоритеты, Domino используют приоритет, назначенный для реплик на сервере, который является инициатором репликации.

2.6.4.5 Ограничение времени репликаций.

Ограничение времени репликаций, предотвращает обширные сессии репликаций и позволяет Вам управлять стоимостью репликаций на удаленных участках Вашей системы. Например, если репликации зависят от удаленного соединения по телефону, и база данных требует времени на репликацию, Вы можете ограничивать период продолжительности реплик.

Чтобы ограничивать время реплик, Вы вводите значение в поле Replication Time Limit из документа подключения.

Предостережение: Если Вы определяете очень маленькое время, базы данных не смогут реплицироваться полностью. Файл LOG.NSF делает запись, указывающую, что произошло завершение связи, но репликация не была успешна. История репликации не обновляется.

Чтобы ограничивать репликации по времени для всего сервера, редактируйте NOTES.INI файл, чтобы включить переменную ReplicationTimeLimit.

2.6.4.6 Использование нескольких репликаторов одновременно

Если Вы создаете документы подключений, которые используют несколько репликаций сервера одновременно, или накладываются на репликации с различными серверами назначения, запускайте несколько репликаторов, чтобы обрабатывать каждую сессию. Многократный запуск репликатора эффективно используют ресурсы серверов, сокращают циклы репликаций, особенно на Hub серверах, при этом экономят время репликаций.

Когда Вы используете несколько репликаций, каждый репликатор обращается только с одной сессией репликаций. Например, если на сервере Hub-E/East/Acme намечена репликация с сервером HR-E/East/Acme и с Hub-W/West/Acme одновременно, один репликатор обрабатывает репликацию Hub-E/East/Acme и HR-E/East/Acme, другой репликатор обрабатывает реплику между Hub-E/East/Acme и Hub-W/West/Acme.

Несколько репликаторов обращаются с несколькими репликами, между одним сервером источником и несколькими серверами назначения одновременно.

Пример. Если База данных 1 и База данных 2 на Hub-E/East/Acme нуждаются в репликации с Hub-W/West/Acme, то только один репликатор общается с каждой сессией репликации, по очереди.

Исследуйте документы подключений, которые намечают Ваши репликации на каждом сервере. Регулируя графики реплик и запуская несколько репликаторов, Вы можете сокращать время полного цикла репликаций. С этим сокращением циклов, Вы можете наметить одни или более дополнительный циклов в день, что означает уменьшение интервалов времени для обновления данных баз данных, более быстрый цикл репликаций. После того, как Вы запускаете несколько репликаторов, Вы можете использовать команду - Tell, чтобы остановить все репликаторы; однако, Вы не можете использовать команду - Tell, чтобы остановить определенный репликатор.

Если Вы не используете несколько репликаторов, не намечайте реплики с сервера с использованием различных портов в одно и тоже время.

Пример. Если Вы используете один репликатор, не намечайте реплику с Hub-E/East/Acme на Hr-E/East/Acme по COM1, на тоже самое время, что и с Hub-E/East/Acme, на Hub-W/west/Acme по COM2 одновременно.

Разрешение использования нескольких репликаторов.

Метод	**Действия**
Из файла NOTES.INI	Редактируйте строки Replicators или ServerTasks для изменения значений запуска задач Репликатор, в NOTES.INI файле

С консоли сервера	Введите команду Load Replica на консоли сервера. Используйте этот метод, если Вы нуждаетесь в большем количестве репликаторов, если Вы не хотите закрывать сервер, чтобы изменить переменные в NOTES.INI файле. Каждый раз, когда Вы вводите в эту команду, сервер загружает новый репликатор.

2.6.4.7 Отклонение запросов на репликации с сервера.

Чтобы оградить сервер от принятия просьб о репликациях, редактируйте NOTES.INI файл, чтобы включить переменную ServerNoReplRequests. Если эта установка установлена в 1, сервер отказывается от всех запросов на репликацию.

Вы можете использовать эту особенность, чтобы уменьшить рабочую нагрузку репликаций на выбранном сервере.

2.6.4.8 Запрещение репликаций.

Чтобы запретить репликации - например, когда Вы проверяете репликации на нескольких серверах, или Вы не хотите, чтобы некоторые базы данных были реплицированы - Вы можете запретить репликации.

Чтобы запретить репликации, отредактируйте документ подключения в Domino Directory. В секции Replication, запретите использование репликации, установите значение поля Replication в Tasks – Disabled.

2.6.4.9 Форсирование намеченных репликаций.

Вы можете реплицировать изменения критических баз данных, типа Domino Directory, без ожидания намеченной репликации. После того, как Вы создаете документы подключений, Вы можете использовать команду консоли сервера, чтобы вынудить немедленную репликацию.

Имеются много ситуаций, когда принудительные репликации необходимы. Например, Вы можете захотеть модернизировать базу данных немедленно, без того, чтобы ожидать намеченной репликации, или Вы могли бы реплицировать данные с различных серверов, потому что обычно эти сервера недоступны.

Когда Вы вынуждаете немедленную репликацию Сервер - Сервер, Вы можете вести репликацию в одном или в обоих направлениях.

Команды для репликатора:

Replica - Реплицируются изменения в базах данных в обоих направлениях. Domino сначала забирает изменения, потом выталкивает измененные документы.

Pull - Реплицируются изменения в базах данных в одном направлении, где сервер только забирает изменения с другого сервера

Push - Реплицируются изменения в базах данных в одном направлении, где сервер только выталкивает изменения баз данных на другой сервер.

2.6.5 Просмотр расписания репликаций и карты топологии репликаций

Вы можете просмотреть графическое представление графика репликаций для каждого из серверов сразу из клиента Domino Administrator. График репликаций каждого сервера появляется отдельно, даже если сервер - член кластера, внесенной в список в поле Destination server в документе подключения.

Вы можете также видеть графическое представление Вашей топологии репликаций. Карты топологии репликаций наиболее полезны для быстро представления топологии.

Каждый сервер, сеть, группа и ПО cc:Mail, имеет собственное изображение. Линиями представлена каждая репликационная связь. Репликационная связь между двумя серверами, отображается как красная пунктирная линия. Многократные связи между серверами появляются как линии, соединяющие сервера друг с другом.

Просмотр расписания репликаций.

*463 Из клиента Domino Administrator, выбирайте закладку Репликация.

*464 Выбирайте – События реплицирования.

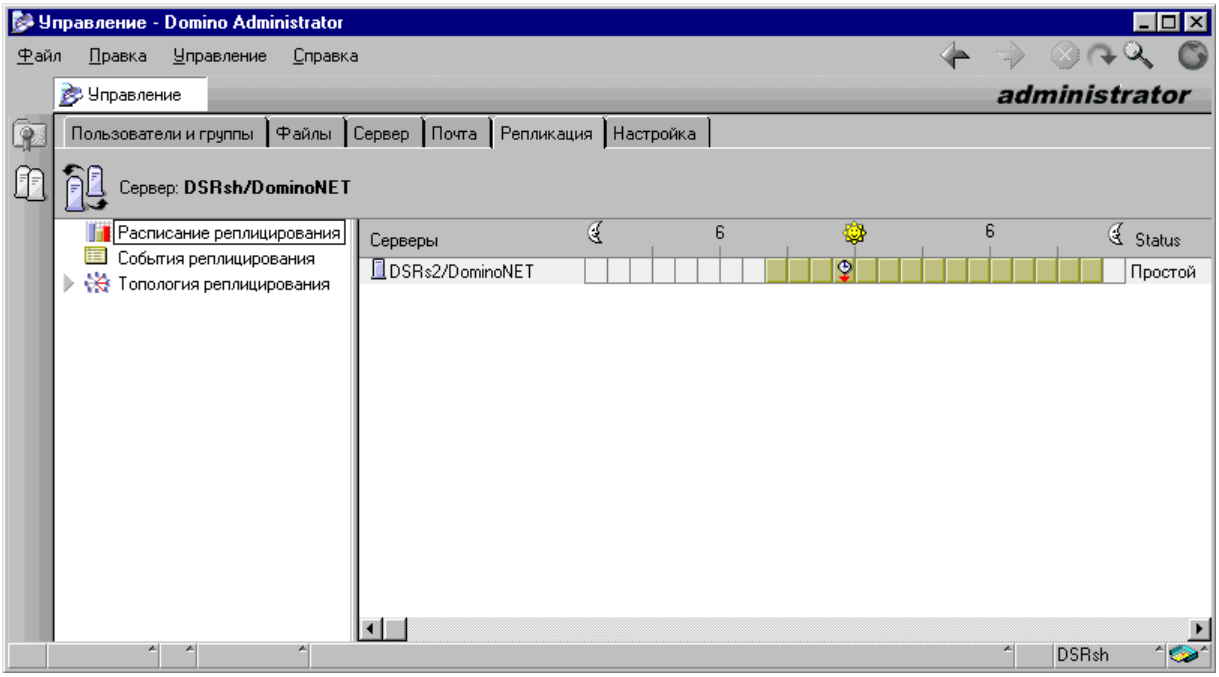


Рис. 35 Просмотр запланированных репликаций из клиента Domino Administrator.

*465 Видим статус для репликаций для каждого сервера:

- Расписание выполняется
- Расписание завершено
- Расписание не завершено

Старт задачи Topology maps на сервере.

Задача Maps должна быть запущена на сервере, которым вы управляете, чтобы рассматривать топологию репликации из клиента Domino Administrator. Пока задача Maps запущена, она регенерирует информацию топологии, каждую ночь - в полночь.

*466 Из клиента Domino Administrator, выбирайте закладку Сервер – Состояние.

*467 Если необходимо, выбирайте – Сервис – Задача – Start.

*468 Из окна Запуск задач - выбирайте задачу Maps Extractor.

*469 Выбирайте – ОК.

Просмотр топологии репликаций.

*470 Из клиента Domino Administrator, выберите сервер, для которого Вы хотите создать карту топологии.

*471 Выбирайте закладку – Репликация.

*472 Сделайте одно из следующего:

- Выбирайте Топология реплицирования – По подключения, чтобы просмотреть связи между серверами, связанные в соответствии с документами подключений или кластерам.
- Выбирайте Топология реплицирования – По кластерам, чтобы рассмотреть все кластера и сервера, связанный с ними.

*473 (Необязательно) Двойной щелочек на любом сервере, в карте топологии позволит вам сделать этот сервер центром карты.

*474 (Необязательно) Двойной щелчок на связи, откроет соответствующий документ подключения из Domino Directory.

Вы можете перемещаться по карте топологии, используя курсор клавиатуры. Вы можете изменить масштаб изображения, нажимая на клавиши - плюс (+) или минус (-).

2.6.6 Тестирование репликаций.

После того, как Вы создаете документы подключения и разрешите репликации, Вы можете проверять репликации. Прежде, чем Вы начинаете проверять, удостоверитесь, что Ваша сеть запущена и работает должным образом, все модемы доступны.

Чтобы проверять репликации, создайте новую реплику базы данных, сделайте изменение в ней, затем дождитесь реплики в другие базам данных. Вы можете или вынуждать репликацию, используя функцию - Репликация, из меню, или подталкивать ее с консоли сервера. Вы можете ждать, чтобы видеть, результат выполнения реплик автоматически на консоли сервера.

Проверьте консоль сервера, чтобы просмотрите сообщения, когда задача Replicator начинает работать. Replicator отображает список баз данных на консоли сервера, которые реплицируются в процессе репликации. Используйте команду просмотра задач Sh Ta, на консоли сервера, чтобы видеть, какая серверная задача запущена в настоящее время.

Для информации о репликах, проверьте историю репликаций в свойствах баз данных, а так же проверьте LOG.NSF для резюме по репликациям. Проверить фай LOG.NSF, можно из клиента Domino Administrator, щелкнув на закладке Репликация, представление - События репликаций.

Чтобы проверять, что репликационные связи не запрещены, Вы можете просмотреть представление - Топология реплицирования.

2.7 Настойка функции поиска Domain Search.

Глава описывает, как установить и настроить Domain Search, который позволяет пользователям искать в Notes домене документы, файлы и приложения с использованием выделенного для этой цели специального сервера.

2.7.1 Поиск в домене Domino серверов.

Domain Search, позволяет пользователям искать документы во всем Notes домене, файлы, приложения, которые соответствуют запросу поиска. Domain Search централизован и строится на Domain Catalog сервере, который использует Domain Catalog. В Domain Search также имеются фильтры, для конечных пользователей, основанные на их доступе индексированным базам данных и системам файлам.

Domain Indexer строит центральный индекс домена на сервере Domain Catalog, в него включается весь домен. Domain Catalog может реплицироваться на другие сервера. Domain Indexer производит индексацию файлов непосредственно на Domain Catalog сервере, эти файлы не реплицируются на другие сервера. Если Ваша организация имеет больше чем шесть, восемь Domino серверов, Lotus настоятельно рекомендует, чтобы Вы выделили один сервер под Domain Catalog. Этот компьютер не должен иметь никакой другой цели, кроме как индексировать файлы и осуществлять поиск в домене.

Domain Catalog сервер.

Когда Вы настраиваете Domain Search, убедитесь, что Domain Catalog сервер способен создавать индексы и обрабатывать запросы пользователей. Domain Catalog сервер должен быть быстр, мощен, и иметь большое количество места на диске, несколько посессоров, большое количество памяти и жесткие диски большого объема увеличат эффективность Вашего поиска.

Рассмотрите возможность кластера для Ваших Domain Catalog серверов, чтобы обеспечить системе большую надежность и сбалансировать нагрузку. Если Вы используете Domain Search кластер серверов, создаете реплику Domain Catalog на каждом сервере кластера.

Для Domain Search сервера под WindowsNT, Lotus рекомендует следующую минимальную конфигурацию:

*475 Intel Pentium II 266 MHz процессор

*476 RAM 256МБ

*477 Свободное место диска равняется приблизительно 75 процентам от размера индексируемого домена

Domain Catalog.

Domain Catalog – база данных, которая использует дизайн шаблона CATALOG.NTF. Записи, сохраненные в каталоге, указывают, какие базы данных и файлы, сервер должен индексировать. Проектировщики баз данных и менеджеры устанавливают, должны ли базы данных быть индексированы или нет, выбирая или запрещая опцию Include in multi database indexing, на закладке свойств базы данных. Администраторы могут конфигурировать эти назначения, используя Клиента Domino Administrator. При использовании Domain Catalog, администраторы определяют, какие файлы могут индексироваться.

Поиск из Web.

Клиенты Web имеет доступ к большинству функциональных возможностей Domain Search, включая запросы на поиск и вывод результата.

Настройка Domain Search.

Domain Search включает несколько форм по умолчанию для поиска системных файлов, определения размещение и вывода результатов поиска. Вы можете настраивать поиск и конечные формы.

Domain Search и R4 Catalog Баз данных

Задача Catalog собирает информацию о базах данных на всех Domino серверах в домене и создает документ для каждой базы данных в Domain Catalog. При сборе информации от других R5 серверов, используется задача Catalog, она репликациями собирает документы, которые уже существуют в каталоге серверов. Если сервер является или R4.x, или R5 сервер, который не имеет каталога, задача Catalog собирает необходимую информацию непосредственно о каждой базе данных на этом сервере и создает соответствующие документы для каждой базы данных в Domain Catalog.

Domain Search и полнотекстовый индекс отдельных баз данных.

Полнотекстовый индекс поиска может сосуществовать с Domain Индексом. Вы можете использовать полнотекстовый индекс для совместимости с предыдущими версиями Domino или Notes, или для серверов с ограниченным доступом пользователей.

2.7.2 Разрешение использования функций поиска Domain Search.

Вы можете использовать Domain Search после того, как Вы устанавливаете сервер версии R5. Чтобы разрешить Domain Search на сервере, проверьте поле Domain wide indexer, на закладке Server Tasks - Domain Indexer. Назначьте график индексации в Server документе, для этого сервера. Эти установки определяют, что Ваш сервер будет функционировать, как Domain Catalog сервер и заставит запускаться задачу Catalog ночью. Добавьте задачу Catalog в переменную ServerTasksAt1, в NOTES.INI файле на сервере. Если Вы установили Enterprise сервер, задача Catalog запускается по умолчанию.

Процесс администрирования создает группу LocalDomainCatalogServers, в Domino Directory и добавляет Domain Catalog сервер к этой группе. Когда Catalog запускается впервые, Domino создает базу данных Domain Catalog по шаблону CATALOG.NTF. При создании базы данных делает изменения в ACL, так что база данных копировалась должным образом в пределах домена. Сервер начинает индексировать домен в следующее, намеченное для этого время. Domain Indexer запускается и придерживается графика, определенного в Server документе, с закладки Server Tasks – Directory Cataloger. По умолчанию задача стартует в час ночи.

Установка и настройка Domain Search сервера.

*478 Из клиента Domino Administrator, выбирайте сервер, который Вы хотите сделать Domain Catalog сервером.

*479 Выбирайте закладку Настройка.

*480 Расширьте Сервер секцию в виде панели слева.

*481 Выбирайте - Все документы на сервере.

*482 Выбирайте Server документ, для Domain Catalog сервера и выбирайте опцию редактирования.

*483 Выбирайте закладку Server Tasks – Domain Indexer.

*484 Выбирайте кнопку со стрелкой рядом с полем Domain wide indexer

*485 Выбирайте значение – Enabled, а затем - OK.

*486 Составьте график индексации, удовлетворяющий потребностям Вашей системы.

*487 Выбирайте сервера, которые Вы хотите включить в индекс, в поле Limit domain wide searching to the following servers. Используйте знаки замещения символов, для индексации всех серверов - например */Sales/East/Acme. Если поле пусто, все сервера будут индексированы.

*488 Выбирайте – Сохранить и закрыть.

На консоли сервера введите, чтобы начать процесс индексации. Domain Indexer запустится в намеченное время.

```
load catalog
```

Настройка производительности Domain Search.

Определите потребности Вашей организации в поиске и приспособьте частоту, с которой Domain Indexer будет запускаться. Большая частота запуска задачи - более современные индексы, но потребляет большие ресурсы CPU. По умолчанию, Domain Indexer запускается, каждые 60 минут. Поэкспериментируйте с различными частотами индексации, чтобы достичь лучших результатов для Вашей организации.

Вы можете также настраивать число нитей индексации, используемых Domain Search, чтобы увеличить производительность поиска.

По умолчанию, Domain Catalog сервер использует две нити индексации на каждый процессор компьютера, так что сервер с двумя процессорами, использует 4 нити индексации по умолчанию. Добавляя переменную FT_DOMAIN_IDXTHDS=n в NOTES.INI Domain Catalog сервера, Вы можете управлять общим количеством нитей, используемых для индексации на этом сервере. Например, добавляя FT_DOMAIN_IDXTHDS=8 в NOTES.INI Domain Catalog сервера, с двумя процессорами будет использоваться 8 нитей.

Примечание. Не превышайте 8 нитей на сервер, это может отразится на производительности сервера, даже если на сервере больше чем 4 процессора.

2.7.3 Поиск в системных файлах.

Для каждого сервера домена, Вы можете создавать документ File System в Domain Catalog, чтобы определить, какие системные файлы включить в индекс домена. В документе File System, Вы определяете, какие системные файлы будут индексироваться и какие подкаталоги. Вы можете индексировать любые файлы системы, на которой Domino сервер запущен, Domino может иметь доступ к системным файлам. Domain Catalog требует, по крайней мере, доступ читателя к операционной системе.

Если Вы хотите индексировать системные файлы, на Domain Catalog сервере должен быть также запущен Domino Web сервер. Это позволяет серверу отображать связи с документам системных файлов и возвращать документы в ответ на запросы клиентам Web и Notes.

Настройка поиска в системных файлах сервера.

Закончите шаги ниже для каждого сервера, системные файлы которого, Вы хотите включить в Domain Catalog.

*489 Запустите клиента Notes или клиента Domino Administrator.

*490 Если Вы хотите индексировать системные файлы в каталоге, который - не являются подкаталогами Domino Data, создайте Directory link или Mapping/Redirection документ.

*491 Выбирайте из меню Файл – База данных – Открыть.

*492 В поле сервера, введите имя Domain Catalog сервера и щелкайте – Открыть.

*493 Выбирайте - Domain Catalog, затем – Открыть.

*494 Выбирайте – Add File System.

*495 Выбирайте имя сервера.

*496 Нажмите Add..., Edit Selected или Delete Selected System List.

*497 В поле File system, определите физическое местоположение системных файлов, чтобы включить их в поиск. Пример: c:\lotus\domino\data\files.

*498 Используйте каталог или URL поля, чтобы определить логическое местоположение файлов, типа /files. Введите в подкаталог, этого каталога - если она находится в каталоге Domino Data. Если Вы основали связь с каталогом, с использованием Mapping/Redirection, введите логическое местоположение directory или URL.

*499 Выбирайте – Продолжить и добавьте системные файлы каталога или список URL к списку.

*500 Повторить эти шаги, чтобы добавить большее количество системных файлов к списку.

*501 Выбирайте - OK, когда Вы закончили ввод файлов в список.

*502 Выбирайте - Сохранить и Закрыть.

*503 Определите Mapping/Redirection документ, для URL системных файлов каталога.

Например, если Вы хотите иметь доступ файлов индекса в c:\files каталог, создаете Mapping/Redirection документ, чтобы определить URL/files к каталогу c:\files.

Перезапустите сервер.

Обратите внимание, что безопасность в R5 работает только для баз данных. Следовательно, поиск в файловой системе, зависит от безопасности операционной системы - пользователи получают результат поиска, даже если они не уполномочены просматривать этот документ. Таким образом, пользователи не получат доступ ко всем результатам поиска. Убедитесь, что установили безопасность файловой системы должным образом и индексируете только системы файла, для которых безопасность - не является критичной.

2.7.3.1 Настройка поиска в системных файлах.

В следующем примере, Domino включает все файлы из каталога c:\lotus\domino\data в индекс, на сервере Mail-W/West/Acme. C:\lotus\domino\data – это каталог данных Domino сервера.

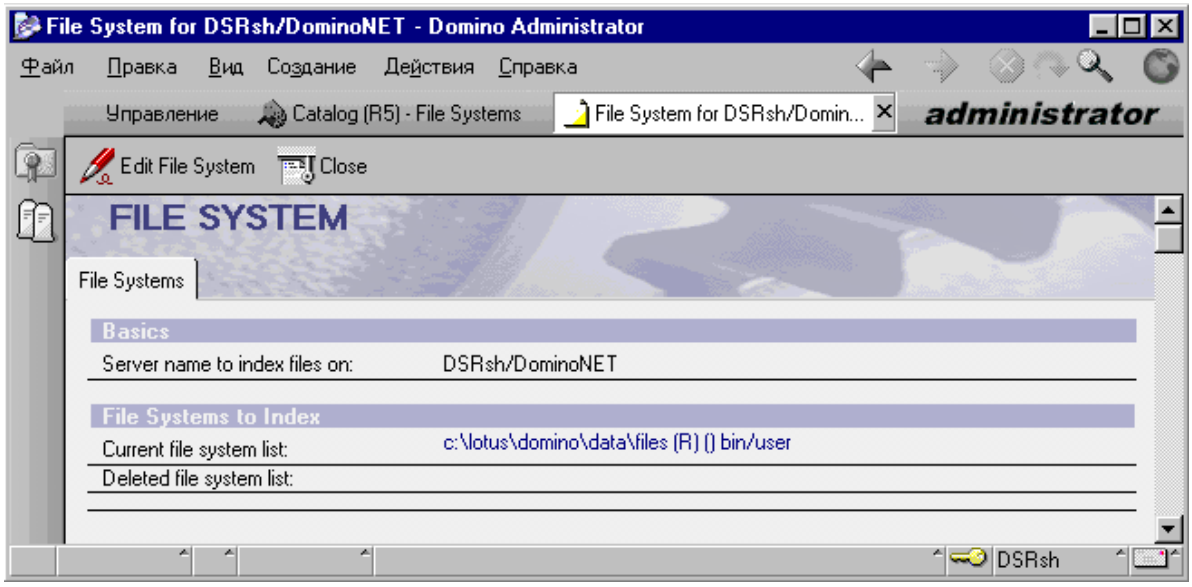


Рис. 36 Пример настройки поиска в системных файлах.

2.7.4 Включение баз данных в Domain Index.

Чтобы включать базу данных в Domain Index, разрешите опцию - Включить в индекс, охватывающий несколько баз данных, в свойствах базы данных. Процесс Domain Index действует следующим образом:

*504 Просматривается информация о каталогах в Domain Catalog относительно всех баз данных.

*505 Когда задача Domain Index запускается, она проверяет Domain Catalog и индексы всех базы данных, которые имеют разрешенную опцию - Включить в индекс, охватывающий несколько баз данных.

Включение баз данных в индекс домена.

Вы можете использовать Клиента Domino Administrator, чтобы добавить группу баз данных в Domain Index немедленно.

Из клиента Domino Administrator, выберите сервер, который содержит базу данных, которую Вы хотите включить.

Выбирайте закладку Файлы и затем выбирайте базы данных, которые Вы хотите добавить в Domain Catalog.

Выбирайте из меню справа опцию - Индекс по нескольким БД, затем выбирайте - OK.

Просмотр информации о Domain Catalog.

Используйте эти представления Domain Catalog для исследования этой информации о базах данных, серверов и пользователей в домене.

2.7.5 Конфигурирование Domain Index.

Центральный Domain Index решает проблемы связанные с поддержкой маленьких частных индексов, рассеянных по серверам в сети и позволяет пользователям создавать единственный запрос, который ищет разнообразные файла и баз данных.

Domain Indexer запускается согласно графику, который Вы определяете в Server документе и представлениях Domain Catalog для новых баз данных, которые имеют включенную опцию - Включить в индекс, охватывающий несколько баз данных. Он ищет документы и файлы в существующих базах данных и в системах файла, которые являются новыми или изменились с момента последнего обновления их в Domain Index.

2.7.6 Настройка клиентов Notes для использования Domain Search.

Когда Notes R5 клиент использует Domain Search, Notes, проверяет поле Catalog/Domain Search server, в документе Место вызова, чтобы решить к какому серверу Domain Catalog присоединиться для поиска данных. Как Вы устанавливаете Domain Catalog сервер для Вашего Notes домена, Domino делает запись этой информации в профиле установки пользователя по умолчанию в Domino Directory для домена, автоматизируя процесс Domain Search для клиентов Notes домена. Когда R5 пользователи Notes регистрируются на их домашних серверах Notes, проверяет их профиль и заменяет в документе Места вызова, имя сервера Domain Catalog. Используйте следующие шаги прежде, чем клиенты Notes зарегистрируются на домашнем сервере.

*506 Запустите R5 клиента Notes.

*507 Выбрать из меню Файл – База данных – Открыть.

*508 Выбирайте Персональную АК пользователя – Открыть.

*509 В левой панели выбирайте - Параметры – Места вызова.

*510 Сделайте следующее для каждого Места вызова, чтобы использовать Domain Search

*511 Выбирайте - Место вызова – Редактировать.

*512 Выбирайте закладку Серверы.

*513 Введите имя Domain Catalog в поле Сервер поиска в домене/каталоге.

*514 Выбирайте – Сохранить и Закрыть.

*515 Закройте Персональную АК.

Обратите внимание, что Domino администраторы могут устанавливать эту информацию для новых пользователей в течении регистрации пользователя, используя профили установки. Если пользователи вводят в название поискового сервера неправильное Имя - Notes возвращает ошибку.

2.7.7 Использование документа - Content Categories.

Content Maps - позволяет пользователям просматривать информацию скорее, чем поиск, с использованием полнотекстового поиска. Content Maps организовывает документы по темам в картах просмотра, во многих категорий на участках сети поиска, таких как AltaVista и Yahoo!

Вы можете создавать категории содержания документа для документов в Domain Catalog, чтобы организовать информацию в виде Content Maps.

Назначение документам категорий.

Вы можете назначать категории, на документы Notes и Web URLs. Вы назначаете категории из Notes R5 клиента, и Вы должны иметь доступ автора к базе данных Domain Catalog.

*516 Запустить R5 клиента Notes.

*517 Определите документ, или Web URL, который Вы хотите категоризировать.

Обратите внимание, если вы категоризируете документ Notes, Вы должны иметь, по крайней мере, доступ редактора к исходному документу.

*518 Выбрать из меня Файл – Свойства документа.

*519 Выбирайте закладку Мета.

Рис. 37 Закладка Мета, окна свойств документа.

*520 Делать одно из следующего:

- Чтобы назначать документу существующую категорию, выбирайте, категоризировать, выбирают один или большее количество категорий, и щелкают - OK.
- Чтобы назначать документу новую категорию, введите категорию в поле Категория.

*521 Щелкайте – Добавить в каталог.

Обратите внимание. Если вы не укажите для рабочей станции сервер поиска в документе Место вызова, кнопки Категория и Добавить в каталог - будут Вам недоступны.

Добавленный, документ Notes добавляет информацию категории в скрытое Meta поля заголовка документа и добавляет описание категории документа в представление категорий Domain Catalog. Добавленные Web URL добавляет категорий для URL к представлению категории в Domain Catalog сервер.

Просмотр представления по категории поиска.

Domain Catalog показывает содержащие категории в представлении категорий.

*522 Запустить R5 клиента Notes.

*523 Выбирайте кнопку со стрелкой, справа от изображения поиска.

Рис. 38 Кнопка поиска в клиенте R5.

*524 Выбирайте – Поиск в домене.

*525 Выбирайте – Browse Catalog.

*526 В панели навигатора, выберите Content/by Category view

*527 Расширить категории, чтобы просмотреть документы и URL.

*528 Двойной - щелчок на документе, или URL открывает связь с документами или URL.

Вы можете настраивать содержание вида и категорий, чтобы результаты удовлетворяли потребности Вашей организации.

Изменение категорий просмотра документов.

Вы изменяете категории, редактируйте документы связи Document Content в Domain Catalog. Вы должны иметь доступ Редактора к Domain Catalog.

*529 Запустить R5 клиента Notes.

*530 Выбирайте кнопку со стрелкой справа от изображения поиска.

*531 Выбирайте – Поиск в домене.

*532 Выбирайте – Browse Catalog.

*533 В панели навигатора, выберите Content/by Category view

*534 Расширить категории, чтобы просмотреть документы и URL.

*535 Выбирайте документ, которому Вы хотите изменить категорию, из меню выбирайте – Действие – Edit Document.

*536 Это действие откроет документ связи – Document Catalog.

*537 Определите новую категорию в поле Categories.

*538 Закройте и сохраните документ.

Обратите внимание на то, что эти изменения категории касаются только Domain Catalog, но не изменяют информацию категории, сохраненную в Meta полях документа непосредственно.

2.7.8 Безопасность в Domain Search.

Когда пользователь выполняет поиск Domain Search в данных, Domain Search проверяет каждый результат, сравнивая его с ACL базы данных, в которой результат был найден, чтобы проверить доступ пользователя, на чтение документа. Чтобы выполнять эту проверку, Domain Catalog содержит список для всех баз данных, который включают ACL базы данных. Проверка безопасности работает следующим образом:

*539 Domino проверяет доступ – Default - к базе данных ACL.

- Если – Default - имеет доступ читателя или больший, пользователь может читать документ и Domino возвращает результат в наборе результатов.

- Если – Default - имеет доступ менее читателя, Domino проверяет, имеет ли пользователь доступ читателя, или больший в ACL. Если нет, Domino не включает базу в результат.

*540 Если пользователь имеет доступ читателя или больше, Domino проверяет, имеет ли документ поле Readers.

- Если документ результата не имеет поля Readers, пользователь может читать документ и Domino возвращает результат в наборе результатов.

- Если документ результата имеет поле Readers, Domino проверяет, включен ли пользователь в поле. Если нет, Domino не включает результат в результат поиска.

- Если пользователь включен в поле Readers, пользователь может читать документ, и Domino возвращает результат в наборе результатов.

Для Domino, чтобы включить связь с документом в результат, пользователь должен быть способен, читать документ.

Безопасность поиска и список доступа пользователей к серверу.

Если Вы используете списки доступа к серверу, в пределах домена для ограничения доступа к информации, знаете, что Вы должны проверить ACL баз данных по этим серверам, чтобы гарантировать правильное фильтрование результатов поиска. Иначе, поиск может возвращать результат пользователю, для тех, кто не должен иметь доступ к документам. В некоторых случаях, пользователи могут получить конфиденциальную информацию, из результата поиска.

Например, корпорация Acme имеет два сервера приложений, App-E/East/Acme и App-W/West/Acme. Пользователи Acme - сертифицированы одним из двух сертификатов орг. единицы: /East/Acme или /West/Acme. App-E/East/Acme не позволяет доступ любому пользователю с сертификатом /West/Acme. Но базы данных на сервере, не должны быть доступны для /West/Acme пользователей и имеют доступ – Default - в их ACL - читатель, так как список доступа гарантирует, что /West/Acme пользователи не могут иметь доступ к базам данных.

Когда Acme осуществляет поиск с использованием Domain Search, пользователи /West/Acme, могут получить результаты поиска, которые включают связи с документами в базах данных сервера App-E/East/Acme, так как в списках управления баз данных, /West/Acme пользователям не запрещен доступ чтения результатов. Серверные списки доступа продолжают обслуживать пользователей, так как /West/Acme пользователи не могут иметь доступа к документам из связей, но простое существование связей, потенциально может показывать конфиденциальную информацию /West/Acme пользователям.

Чтобы избежать этой проблемы, проверьте Списки управления доступом для баз данных, которые защищены серверными списками доступа. Чтобы сделать это, предположите, что серверный список доступа не существует. Измените ACL так, чтобы, в отсутствии серверного списка доступа, база данных была бы гарантировано защищена. Это гарантирует, что Domain Search проверяет базу данных ACL и отфильтровывает результаты и пользователей, которые не могут иметь доступ к данным.

Обратите внимание, что этот пример предполагает, что Domain Catalog сервер имеет сертификат, которое позволяет доступ и на App-E/East/Acme и на App-W/West/Acme.

2.8 Настройка календаря и планирования.

Пользователи Ваших серверов могут использовать Domino Calendar и Domino Scheduling, чтобы намечать встречи и резервировать ресурсы Вашей организации.

2.8.1 Событие календаря и расписание.

Календарь Domino и опции расписания позволяет пользователям проверять свободное время других пользователей, список встреч с ними, заказывать ресурсы и оборудования. Вы можете также определить информацию об отпусках в Вашей организации. Пользователи импортируют эту информацию непосредственно в их персональные календари. Domino оперирует набором документов праздников отпусков, которые Вы можете изменять.

Календарь и функции планирования использует Schedule Manager - задача Sched, Calendar Connector - задача Calconn и Free Time system, комбинация задач Sched, Calconn и Nnotes. Когда Вы устанавливаете любой Domino сервер, кроме Directory сервер, задачи Sched и Calconn автоматически добавляются в NOTES.INI файл. Когда Вы запускаете сервер впервые, Schedule Manager создает базу Свободного Времени BUSYTIME.NSF, или CLUBUSY.NSF для кластера почтовых серверов. Процесс создает записи в базе данных для каждого пользователя, который заполнил профиль календарный и, чей почтовый файл находится на этом сервере или в одном кластере серверов.

Каждый пользователь может использовать персональный календарь и создавать профиль календаря, который определяет, кто может иметь доступ к информации о свободном времени этого пользователя и когда пользователь доступен для встреч. Когда пользователь приглашает другого пользователя на встречу, система Free Time выполняет поиск свободного времени. Free Time также ищет и возвращает информацию относительно доступных ресурсов. Если поиск охватывает поиск свободные времени по различным серверам, Calendar Connector генерирует эти запросы. Когда пользователи намечают событие в их календарях или заказывает ресурсы, задача Schedule Manager собирает и обновляет информацию о свободном времени в базе данных Free Time.

По умолчанию, Schedule Manager имеет доступ к базе данных свободного времени, так что Вы не должны переопределить что-либо в ACL для этой базе данных.

Использование базы данных Clustered Free Time.

Для кластеров почтовых серверов Schedule Manager создает кластерную базу данных Свободного Времени (CLUBUSY.NSF), когда сервер запускается впервые. Версия кластерной базы данных свободного времени работает так же как BUSYTIME.NSF. Каждый сервер кластера имеет реплику этой базы данных, с информацией о пользователях, сохраняется в ней, чьи почтовые файлы находятся на серверах в кластере.

Если Вы добавляете сервер в кластер, Schedule Manger удаляет базу BUSYTIME.NSF на этом сервере и создает CLUBUSY.NSF, которая реплицируется на сервера кластера. Если Вы удаляете сервер из кластера, происходит противоположное. Schedule Manager удаляет CLUBUSY.NSF и создает BUSYTIME.NSF. Schedule Manager не проверяет базы данных на наличие почтовых файлов или их изменений, удаления в кластере. База данных свободного времени содержит информацию о пользователях, чей почтовый сервер Вы удалили из кластера. Эти значения будут храниться до следующего обновления данных, которое происходит каждый день в 2 часа, чтобы обновить информацию о свободном времени пользователей, чьи почтовые файлы были добавлены, или удалены с почтового сервера. Вы можете обновить информацию в любое время, командой с консоли сервера:

```
Tell Sched Validate
```

Использование Scheduling Clustered выгоден тем, что информация всегда доступна пользователям, даже когда домашний пользовательский сервер выключен.

Другие преимущества использования Scheduling Clustered – увеличение производительности и уменьшение трафика передачи данных в сети. Потому, что база данных свободного времени доступна на всех членах кластера серверов, запрос пользователя не должен искать базу данных на домашнем сервере пользователя, т.к. почтовые сервера пользователей находятся в кластере.

2.8.2 Настройки календаря

Планирование расписания зависит от места расположения пользователей. Находятся ли они в том же самом Domino домене или в различных. Используют ли пользователи альтернативную программу расписания, типа Lotus Органайзер ® или IBM ® OfficeVision ®.

Для пользователей Вашего Domino домена, планирование автоматически установлено и может сразу применяться с использованием базы данных Free Time. Вы должны создать базу данных Resource Reservations, чтобы пользователи могли искать и резервировать общие ресурсы в Вашей организации.

Для пользователей соседнего домена (Adjacent), удостоверитесь, что Вы уже создали документы Adjacent Domain в Domino Directory, чтобы установить связь между доменами.

*541 Из клиента Domino Administrator, выбирайте закладку Настройка.

*542 Выбирайте нужный Domino Directory.

*543 Выбирайте из левой панели – Почта – Домены, затем откройте соответствующий документ Adjacent Domain.

*544 Выбирайте закладку Calendar Information, заполните поле и сохраните документ:

Поле	**Значение**
Calendar server name	Имя сервера в смежном домене, который будет принимать, обрабатывать все запросы планирования для этого домена

*545 Создайте базу данных Resource Reservations, если Вы хотите позволить пользователям поиск и резервирование ресурсов.

Для пользователей не соседнего домена (Non-Adjacent), для двух несмежных доменов, Вы должны определить сервер календаря в промежуточном домене, который является смежным, для сервера назначения домена.

Обратите внимание, что поиск свободного времени требуют разумного времени ответа по сети, при этом требуют соединения по сети LAN, от промежуточного домена, до Вашего несмежного домена.

Удостоверитесь, что Вы уже создали документы Non-Adjacent Domain, в Domino Directory, чтобы установить связь между доменами.

*546 Из клиента Domino Administrator, выбирайте закладку Настройка.

*547 Выбирайте нужный Domino Directory.

*548 Выбирайте из левой панели – Почта – Домены, затем откройте соответствующий документ Non-Adjacent Domain.

*549 Выбирайте закладку Calendar Information, заполните поле и сохраните документ:

Поле	**Значение**
Route requests through calendar server	Имя сервера календаря, который находится в смежном домене. Этот сервер будет принимать, и передавать запросы о свободном времени от источника, до целевого несмежного домена.

*550 Создайте базу данных Resource Reservations, если Вы хотите позволить пользователям поиск и резервирование ресурсов.

Для пользователей Lotus Organizer или IBM OfficeVision планирование работает с Lotus Organizer или IBM OfficeVision. Если пользователи хотят использовать расписание планирования в другой, удобной для него программе, Вы должны создать документ Foreign Domain, для каждой альтернативой системы расписания.

*551 Удостоверитесь, что Вы уже создали Foreign Domain документ, в Domino Directory для каждой альтернативой системы планирования.

*552 Из клиента Domino Administrator, выбирайте закладку Настройка.

*553 Выбирайте нужный Domino Directory.

*554 Выбирайте из левой панели – Почта – Домены, затем откройте соответствующий документ Foreign Domain.

*555 Выбирайте закладку Calendar Information, заполните поле и сохраните документ:

Поле	**Значение**
Calendar server name	Имя сервера, который управляет альтернативной программой расписаний.
Calendar system	Выбирайте или Lotus Organizer, или IBM OfficeVision из списка

*556 Для Notes пользователей, которые используют различные альтернативные программы планирования, введите имя альтернативных доменов в поле Calendar Domain, Person документа каждого пользователя.

*557 Создайте базу данных Resource Reservations, если Вы хотите позволить пользователям поиск и резервирование ресурсов.

2.8.3 Создание базы данных ресурсов - Resource Reservations.

База данных Resource Reservations - это место, где пользователи планируют и управляют ресурсами для Ваших встреч. Ресурсы могут включать в себя залы заседаний, оборудование, машины, механизмы, видео технику. Пользователи могут выбирать нужный ресурс и резервировать время для его использования.

База данных Resource Reservations содержит три типа документов: Site Profile, Resource, Reservation.

Документ Site Profile - определяет местоположение, где ресурс расположен.

Документ Resource - определяет имя ресурса. Например, название или номер зала заседаний.

После того, как Вы создаете профиль местоположения и документы ресурсов, менеджеры расписаний устанавливают свободное время ресурса, тем самым, определяя свободное время для пользователей.

Чтобы зарезервировать ресурс, пользователь может или создавать документ Reservation (резервирование ресурса) или добавлять ресурс в приглашение встречи. Чтобы создать базу данных резервирования ресурсов используйте шаблон RESRC50.NTF.

*558 Выбирайте из меню Файл – База данных – Контроль Управление Доступа.

*559 Занесите в список управления, имена пользователей, которые будут создавать документы Resource и документы Site Profile. Назначьте им роль CreateResource.

*560 Создайте Site Profile подразделения и документы Resource.

2.8.4 Создание документов Site Profile и Resource документы в базе планирования ресурсов.

Документ Site Profile определяет местоположение, где ресурс располагается. Вы должны создать, по крайней мере, один документ Site Profile прежде, чем Вы сможете создавать документы Resource.

Когда Вы создаете документы Resource, Вы определяете название ресурса, тип и готовность его. Вы определяете, кто может резервировать ресурс. После того, как Вы указали все ресурсы, пользователи могут вести поиск свободного времени для ресурса и резервировать ресурс для встреч при поиске свободного времени и приглашения пользователей на встречу.

Для каждого документа Resource, которого Вы создали, процесс администрирования создает документ Resource в Domino Directory.

Когда Вы создаете Site Profile или документ Resource, новый ресурс не доступен для пользователей, пока процесс администрирования не добавляет ресурс в Domino Directory, а задача Replicator не реплицирует изменения на все доступные реплики Domino Directory.

Создание документа Site Profile.

*561 Убедитесь, что Вам назначена роль CreateResource в ACL базы данных Resource Reservations.

*562 Из клиента Domino Administrator, выбирайте закладку Файлы.

*563 Из панели серверов, выбирайте сервер, с которым Вы хотите работать.

*564 Откройте базу данных Resource Reservations и выбирайте любое представление, кроме Calendar, My Reservations или Reservations Waiting for Approval.

*565 Выбирайте кнопку New Site.

*566 Заполните все поля и затем выбирайте – Сохранить и закрыть:

Поле	**Значение**
Site name	Имя местоположения, где расположен ресурс
Domain name	Имя домена, в котором расположена база данных Resource Reservations

Создание Resource документа.

*567 Убедитесь, что Вам назначена роль CreateResource в ACL базы данных Resource Reservations.

*568 Из клиента Domino Administrator, выбирайте закладку Файлы.

*569 Из панели серверов, выбирайте сервер, с которым Вы хотите работать.

*570 Откройте базу данных Resource Reservations

*571 Выбирайте кнопку New Resource

*572 На закладке Type, выберите тип ресурса - Room или Other

*573 Выбирайте закладку Resource Information и заполните поля:

Поле	**Значение**
Name	Уникальное название ресурса, например номер комнаты
Site	Позволяет просматривать список доступных участков хранения ресурсов и выбирать один из них
Category (появится, когда вы выбираете Other из Resource Type)	Название категорий для ресурса, например электроника или видео. Это поле также показывает имена всех предварительно введенных категорий, из которых Вы можете выбирать нужные.
Capacity (появится, когда вы выбираете Room из Resource Type)	Вместимость ресурса, способность вместить определенное количество человек
Description	Описание ресурса, например большой зал заседаний с видео

Other comments	Дополнительное описание, определенное этому ресурсу - например, зал заседаний хорош для планирования небольших по количеству участников встреч

*574 Выбирайте закладку Owner Options, заполните поля владельца ресурсов:

Поле опций	**Значение**
None	Никто не был назначен владельцем ресурса и любой может резервировать ресурс
Only owner can book resource	Владелец Resource. Только владелец может обрабатывать запросы Resource. Введите имя владельца ресурса в поле.
Only select list of people can book resource	Позволить только некоторым пользователям иметь доступ к ресурсу. Введите имена пользователей, чтобы разрешить резервировать этот ресурс, из списка имен. Любые пользователи, не указанные здесь не могут резервировать этот ресурс.
Only select list of people can book resource via autoprocessing - all others require owner approval	Позволить только некоторым пользователям доступ к ресурсу и назначить владельца ресурса. Введите имя владельца ресурса в поле имени Владельца. Владелец – человек, которому адресуются запросы от других пользователей. Введите имена пользователей, которым позволяется резервировать этот ресурс в списке имен.
Temporarily disable reservations	Щелкайте, чтобы временно запретить резервирование ресурса с использованием почтовых файлов. Если это поле отмечено, пользователи могут все еще резервировать ресурс вручную в базе данных Resource Reservations.

*575 Выбирайте закладку Availablity Settings, введите время, когда ресурс может быть доступен.

*576 Сохраните и закройте документ.

2.8.4.1 Редактирование и удаление документов ресурсов

После того как Вы создаете документы ресурсов, Вы можете изменять любую информацию из полей Availability Settings, Description, Other Comments, Ownership Options. Чтобы изменять любую другую информацию ресурса, Вы должны удалить документ ресурса и затем создать новый ресурс, содержащий новую информацию.

Новая информация о ресурсе будет Вам не доступна, до обработки ее процессом администрирования. Новые документы ресурсов репликатор должен копировать во все реплики на серверах, используемых для планирования ресурсов в Domino Directory.

Если Вы удаляете ресурс из базы данных резервирования ресурса, создается запрос на стирание ресурса, в базе данных Administration Request. Чтобы удалить ресурс и удалить его из Domino Directory, Вы должны открыть базу данных Administration Request и одобрить запрос на стирание ресурса. Обратите внимание, чтобы одобрять запросы на стирание ресурсов, Вы нуждаетесь в соответствующем доступе к базе данных Administration Request.

2.8.5 Создание документа Holiday.

Документы Holiday праздников, заполняются для Вашей организации, чтобы определить намеченные отпуска, праздники и нерабочие дней. Пользователи выбирают тип документов Holiday, чтобы импортировать и добавить эту информацию к их персональным календарям. Domino позволяет иметь набор документов Holiday, которые Вы можете изменять или удалять. Вы можете также добавлять документы Holiday, в Вашей организации. Документы Holiday расположены в Domino Directory.

Вы категоризируете документы Holiday согласно имени группы.

Например, Вы можете иметь группу с именем Полная рабочая неделя, которая содержит информацию об отпуске для служащих с полной рабочей неделей Вашей компании. По умолчанию Domino имеет набор документов Holiday, и имеют названия групп, связанные со странами. Например, Соединенные Штаты или Италия, и имеет группы содержащие документы, определяющие праздничные дни в каждой стране.

Как администратор, Вы можете изменять или удалять эти документы, чтобы приспособить список нерабочих дней, для Вашей организации. После чего Вы можете уведомить пользователей о группах нерабочих дней, что они имели современную информацию.

Вы можете добавлять документы в существующие группы, выбирая эту группу при создании нового документа. Вы можете также создавать новые группы, вводя новое название группы в документах Holiday. Помните, что Ваши пользователи импортируют документы праздников согласно имени группы, а не названия документа, так что Вы можете планировать, как организовать документы в группах.

Создание документов Holiday.

*577 Из клиента Domino Administrator, выбирайте закладку Настройка.

*578 Выбирайте нужный Domino Directory сервер.

*579 Выбирайте представление Miscellaneous/Holidays

*580 Выбирайте – Add Holiday.

*581 Выбирайте значение поля Group. Выберите существующую группу, чтобы связывать ее с праздником (отпуском), или создайте новую группу, введя новое название для группы.

*582 Введите данные в поля и затем выбирайте – Save And Close.

Обратите внимание, что некоторые поля в этой таблице зависит от предыдущего выбора поля.

Поле	**Значение**
Title	Имя праздника (отпуска), например Рождество
Detailed description (Optional)	Описание праздника, кому он посвящен и так далее
Repeat	Выбирайте, как часто праздник должен повторяется: *583 Ежегодно *584 Ежемесячно по дате *585 Ежемесячно по дню *586 Выборочно
Start Date	Дата начала праздника. Эта дата может быть фактическая дата праздника (Новый год), или это может быть дата, начала отпуска. Например, если Ваша организация дает служащим каждую пятницу, с июня по август, Вы ввели бы 1 июня, как дату начала и выбрали бы конечную дату - 31 августа. Это поле доступно для всех опций повторения кроме опции – Выборочно.
Repeat Dates	Дата или даты периодических праздников, например, 01/01/99, 01/02/2003. Это поле доступно только, если Вы выбрали - Выборочно, для поля повторения.
Continuing	Как долго Вы хотите, чтобы праздник повторился: *587 For - Праздник повторяется числом месяцев или лет *588 Until – повторения Праздника до определенной даты, это поле доступно для всех наборов повторения кроме – Выборочно.
Repeat for/until	Если Вы вводите For в поле Continuing, выберите число лет, или месяцев (в зависимости от Вашего выбора в поле Repeat). Если Вы вводите Until в поле, выберите дату, до которой Вы не хотите повторять праздник. Это поле доступно для всех наборов поля Repeat кроме – Выборочно
Repeat Interval	Выбирайте, как часто повторяется праздник, месяц, день. Это поле доступно только, если Вы выбрали - Ежемесячно днем или Ежемесячно по времени в поле Repeat.

Start from the end of month	Проверьте это поле, если Вы хотите создать отношения между датой начала и полями интервала повторения. Это поле полезно в течение отпуска или случаев, когда праздники, попадают на последние дни месяца.
If the date falls on a weekend	Выбирают, куда праздник должен передвинуться, праздник, если он выпадает на выходные. Это поле доступно для всех выбора повторения, кроме Ежемесячно, Днем и Выборочно.
Mark time as	Выбирает Занятый или Свободный. Определяет, делает ли календарь пользователя запись этого праздника как занятое или свободное время.

2.9 Конфигурирование Partitioned серверов.

Глава описывает установку и настройку Partitioned серверов.

2.9.1 Partitioned сервера.

Domino Partitioning сервер позволяет Вам иметь несколько Domino серверов, запущенных на одном, единственном компьютере. Использование таких типов серверов уменьшает расходы для приобретения аппаратных средств и минимизирует число компьютеров, которые Вы должны администрировать. Каждый сервер будет иметь собственный каталог данных Domino и NOTES.INI, но все сервера имеют тот же самый программный каталог Domino. Сервера могут помочь Вам эффективно использовать Ваши аппаратные средства. Например, вместо покупки нескольких маленьких компьютеров для Domino серверов, Вы можете купить единственный, более мощный компьютер и запустить Domino в мульти-серверном режиме на единственном компьютере.

Установка мульти-серверов, особенно эффективно, когда сервера находятся в различных доменах. Например, на одном компьютере Вы можете иметь домен для мульти-клиентов и домен для Web-клиентов. В большинстве случаев, Partitioning сервера предоставляется большее количество ресурсов компьютера и места на диске, чем сервера Домино на отдельных компьютерах. Это потому что программные файлы Domino, загружены для каждого сервера и каждый Domino сервер, должен иметь собственную копию Directory Domino и другие административные базы данных. Их также более легкое администрировать. В некоторых случаях, при управлении мульти-серверов одного домена на компьютере с мультипроцессорами может улучшать производительность, потому что компьютер одновременно управляет некоторыми процессами.

Поскольку Ваша система будет расти, Вы сможете мигрировать пользователей с мульти-серверов, на индивидуальные сервера. Partitioning сервер может также быть членом кластера, если Вам требуете высокая сохранность баз данных. Безопасность для Partitioning сервера та же самая, как и у серверов на собственных компьютерах.

Если один Partitioning сервер останавливается, другие продолжают работать. Поэтому приложения, которые Вы запускаете на Partitioning серверах, являются более надежными, потому что они продолжают работать. Если Partitioning сервер сталкивается с фатальной ошибкой, Вы можете его перезапустить, без перезапуска компьютера. Вы можете сделать это, потому что Domino добавляет переменную KillProcess в NOTES.INI, когда Вы

устанавливаете Partitioning сервера. Лучше использовать различные экаунты пользователей, для каждого Partitioning сервера, так Вы можете использовать соответствующую команду типа, nsd – kill или nproc – k, чтобы очистить остаточные процессы после крушения сервера (на UNIX системах).

Количество инсталлированных серверов на одном компьютере.

Domino поддерживает 6 Partitioning серверов на единственном компьютере. Число серверов, которое Вы можете устанавливать, зависит от потребностей Вашего предприятия и доступных аппаратных средств ЭВМ. Мощь компьютера и операционной системы, определяют число серверов. Вы может создавать их без заметного уменьшения производительности. Это хорошая идея запускать Partitioning сервера на компьютерах с мультипроцессорами и иметь, по крайней мере, один или два процессора для каждого Partitioning сервера, который Вы устанавливаете на компьютере.

Системные требования.

Domino поддерживает Partitioning сервера под управлением UNIX и WindowsNT.

Требования для запуска Partitioning серверов - те же самые что и для стандартных Domino серверов, с дополнительными требованиями:

*589 Добавьте 100МБ дискового пространства на каждый дополнительный сервер.

*590 128МБ RAM для каждого сервера.

*591 Выполните конфигурацию каждого Partitioning сервера, для использования TCP/IP.

2.9.2 Установка и настройка Partitioned серверов.

Установка программного обеспечения Partitioned серверов, подобна установке обычного сервера.

Обратите внимание, что все Partitioned сервера на компьютере, имеют общий программный каталог Domino, но каждый сервер имеет собственный каталог данных Domino.

*592 Запустите программу установки и следуйте инструкциям на экранах. Убедитесь, что выбрали опцию – Partitioned Server Installation.

*593 В программе установки, Вы вводите название каталога для программных файлов Domino, который является общим для всех Partitioned серверов. Вы также вводите в имя каталога для данных Domino для каждого Partitioned сервера.

Примечание. Присвойте каталогам данных Domino имена Partitioned серверов.

*594 Сконфигурируйте каждый Partitioned сервер для TCP/IP протокола.

*595 Сконфигурируйте и настройте каждый Partitioned сервер для использования нужных Вам сервисов - например, LDAP, NNTP, POP3, IMAP, или запустите его как Web сервер Domino.

2.9.3 Конфигурирование Partitioned серверов.

Имеются два пути в конфигурировании Partitioned серверов на Вашем компьютере.

*596 Вы можете назначать единственный IP, всем Partitioned серверам и затем использовать Mapping Ports,

*597 Вы можете назначать выделенный IP, каждому Partitioned серверу.

Использование одного IP адреса для всех Partitioned серверов.

Если Вы имеете ограниченное число IP, Вы можете использовать единственный адрес IP для всех Partitioned серверов. Настройте Port Mapping и назначите каждому Partitioned серверу собственный порт. Когда Вы устанавливаете Port Mapping, Вы определяете один из Partitioned сервер как Mapping сервер. Mapping сервер переадресовывает Notes и запросы Domino другим Partitioned серверам на компьютере.

Следующий рисунок показывает, как клиенту Notes и HTTP клиенту Web браузера передается доступ к Port Mapping сервера.

Порт Mapping сервера переадресовывает запросы клиентов на Partitioned сервера, которые они затребовали.

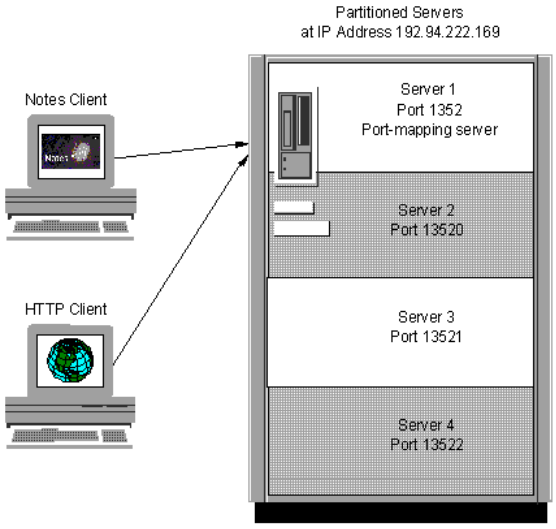


Рис. 39 Пример использования одного IP адреса для всех Partitioned серверов.

Использование единственного адреса IP имеет некоторые неудобства.

*598 Во первых, если порт Mapping сервера не запущен, клиенты обычно не могут устанавливать связь с любым Partitioned серверов.

*599 Во вторых, все Partitioned сервера на компьютере должны быть в той же самой IP сети.

*600 В третьих, (I/O) компьютера может иметь задержки, потому, что все Partitioned сервера разделяет единственную карту сети NIC.

Использование нескольких IP адресов для Partitioned серверов.

Если Вы имеете достаточное количество IP адресов, назначаете отдельный IP, каждому Partitioned серверу и используют отдельный NIC для каждого сервера. Такой подход позволяет доступ клиентов на каждый Partitioned сервер непосредственно, без использования Port Mapping сервера. Хотя Вы можете использовать один IP адрес, с единственным NIC, лучше не делать так из-за отрицательного воздействия на производительность компьютера.

Следующий рисунок показывает, как клиент Notes и HTTP, имеет доступ на любой из Partitioned сервера.

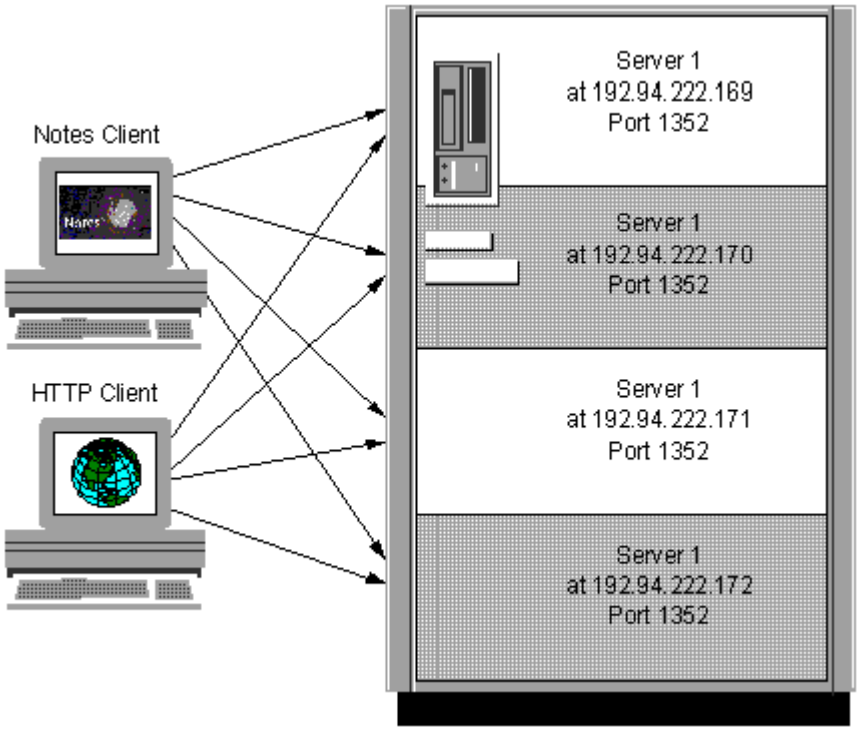


Рис. 40 Пример использования одного IP адреса для каждого Partitioned сервера.

Использование отдельных IP адресов имеет несколько преимуществ.

*601 Во первых, Partitioned сервера не зависят от Port Mapping сервера. Поэтому доступ ко всем Partitioned серверов более уверен и быстр.

*602 Во вторых, Partitioned сервера могут быть в различных IP сетях.

*603 В третьих, Вы можете использовать выделенный NIC, для каждого Partitioned сервера.

2.9.3.1 Назначение отдельных IP адресов Partitioned серверам.

*604 Из IP адресов, Вы выбираете по одному на каждый Partitioned сервер.

*605 Для каждого Partitioned сервера, определите адрес IP и задачу, которую Вы хотите.

Обратите внимание, если вы используете единственный NIC для компьютера, Вы можете использовать только первую запись в таблице.

Если Вы хотите использовать это	**Исполните эту задачу**
Partitioned сервер для связи между Notes и Domino	В NOTES.INI файле, введите *TCPIP*_TcpIpAddress=0,*IPaddress*:1352 Пример: TCPIP_TcpIpAddress=0,192.94.222.169:1352

Web сервер	На закладке Internet Protocols – HTTP из Server документа, введите имя хоста или IP адрес, для Вашего сервера в поле Host Name. Выбирайте – Enabled, в поле Bind to host name.
POP3 сервис	В NOTES.INI файле, введите POP3Address=*hostname* где *hostname* IP, адрес или полное имя Вашего хоста.
IMAP сервис	В NOTES.INI файле, введите IMAPAddress=*hostname* где *hostname* IP, адрес или полное имя Вашего хоста.
NNTP сервис	В NOTES.INI файле, введите NNTPAddress=*hostname* где *hostname* IP, адрес или полное имя Вашего хоста.
LDAP сервис	В NOTES.INI файле, введите LDAPAddress=*hostname* где *hostname* IP, адрес или полное имя Вашего хоста.

Обратите внимание, чтобы установить Partitioned сервер для Server Web Navigstor, Вы должны только установить Partitioned сервера для Notes и Domino. В поле Net Address из Server документа, введите в адрес IP, имя хоста, или общее имя Partitioned сервера. Введите в имя Partitioned сервера, как он определен на DNS сервере, или в локальном HOSTS файле.

2.9.3.2 Назначение нескольких IP адресов на один сетевой интерфейс NIC.

Если Вы используете единственный NIC, с несколькими IP адресами, Вы должны выполнить дополнительные инструкции по конфигурированию в Вашей операционной системе:

*606 HP-UX

*607 IBM AIX

*608 Sun Solaris

*609 WindowsNT

WindowsNT.

В панели управления WindowsNT, сконфигурируйте настройки сети, чтобы присвоить одному NIC, нескольких IP адресов. Для большего количества информации, см. документацию WindowsNT.

2.9.3.3 Использование одного IP адреса и Port Mapping на Partitioned сервере.

Конфигурируйте Partitioned сервера, чтобы использовать один IP адрес на одну сетевую карту, Вы используете Port Mapping. С Port Mapping, Вы назначаете уникальный номер порта на каждый Partitioned сервер и определяете один Partitioned сервер как Port Mapping. По умолчанию, Port Mapping сервер прослушивает запросы по порту 1352 и переадресовывает Notes и Domino запросы связи другим Partitioned серверам.

Если Port Mapping сервер терпит крах, существующие сессии на других Partitioned серверах остаются открытыми. В большинстве случаев, клиенты Notes не будут способны открыть новые сессии на любом Partitioned сервере. Однако потому что каждый клиент Notes сохраняет информацию о связях в памяти, включая переадресование Port Mapping сервера, клиент может соединиться с Partitioned сервером даже, когда Port Mapping сервер не запущен.

Port Mapping сервер требует дополнительных ресурсов системы, рассмотрите возможность определения одного Partitioned сервера только этой задаче. Чтобы сделать это, удалите все другие задачи сервера.

Port Mapping работает только для связи между Notes и Domino. Однако Вы можете использовать Server документ в Domino Directory и сконфигурировать IMAP, LDAP, NNTP, POP3 и Domino Web сервера, чтобы использовать уникальные порты для соединений. Когда Вы делаете это, Вы должны явно указывать номер порта клиентом, когда они пробуют соединиться с сервером. Например, если Вы назначаете номер порта 12080, для Domino Web сервера. Клиенты должны использовать следующую строку, для доступа к Web серверу:

```
http://actome.com:12080
```

Не запускайте все протоколы интернета на компьютере, который имеет единственный NIC. Даже один из протоколов может иметь узкие места ввода - вывода, когда компьютер имеет только один NIC.

2.9.3.4 Конфигурирование Port Mapping для использования с одним IP адресом.

Когда Вы устанавливаете Port Mapping, Port Mapping сервер автоматически маршрутизирует Notes и Domino запросы на другие Partitioned сервера.

*610 Решите, какой Partitioned сервер будет выполнять функции Port Mapping.

*611 Выбирайте уникальный TCP/IP номер порта для каждого Partitioned сервера на компьютере. Port Mapping сервер использует, по умолчанию порт 1352. Мы предлагаем использовать номера от 13520 до 13524 для дополнительных Partitioned серверов.

*612 В NOTES.INI файле для Mapping сервера, включите одну строку для Port Mapping сервера и по одной строке для каждого Partitioned сервера:

```
TCPIP_TcpIpAddress=0,IPAddress:1352
```

Где TCPIP - имя порта, а IPADDRESS - IP адрес Port Mapping сервера.

*613 Для каждого Partitioned сервера, введите:

```
TCPIP_PortMappingNN=CN=server_name/O=org,IPaddress:TCP/IP port number
```

Где TCPIP - имя порта, NN - число между 00 и 04 назначенный в последовательности возрастания, server_name - имя сервера, org - имя organization, IPADDRESS - адрес IP, и TCP/IP номер порта - уникальный номер порта, который Вы выбрали для Partitioned сервера.

Примечание Вы должны назначить номера для NN в порядке возрастания, начиная с 00 по 04. Если имеется перерыв в последовательности, Domino игнорирует последующие записи.

*614 В NOTES.INI файле каждого Partitioned сервера, включите строку:

```
TCPIP_TcpIpAddress=0, IPAddress:IPport_number
```

Где TCPIP - имя порта, IPADDRESS - адрес IP, и IPPORT_NUMBER - уникальный номер порта, который Вы выбрали для Partitioned сервера.

*615 В поле Net Address, закладки Ports - Notes Network Ports, Server документа, для каждого Partitioned сервера введите полное имя хоста и домена - например, Sales.Acme.Com - или введите общее имя сервера - например, Sales.

*616 Включите имя каждого Partitioned сервера как отдельную запись в DNS, или local HOSTS файл.

*617 Если Вы также планируете использовать Partitioned сервера для задач IMAP, LDAP, NNTP, POP3 или Web сервер, назначите каждой задаче уникальный номер порта, в поле TCP/IP port number, на соответствующих закладках (Web, Directory, News, Mail), в документе серверов.

Вы должны сообщить этот номер порта своим клиентам, когда они будут пробовать соединиться с этими серверами. Например, если Вы назначаете порт 12080 для Web сервера Acme.Com, клиенты должны использовать следующий URL, чтобы соединиться с сервером:

```
http://Actome.com:12080
```

2.9.3.5 Пример конфигурации с одним IP адресом и Port Mapping.

Этот пример показывает строки, которые Вы добавляете к NOTES.INI Partitioned серверов, чтобы установить Port Mapping для шести серверов.

Сервер 1 (является Mapping сервером).

```
TCPIP_TcpIpAddress=0,192.94.222.169:1352

TCPIP_PortMapping00=CN=Server2/O=Org2,192.94.222.169:13520

TCPIP_PortMapping01=CN=Server3/O=Org3,192.94.222.169:13521

TCPIP_PortMapping02=CN=Server4/O=Org4,192.94.222.169:13522

TCPIP_PortMapping03=CN=Server5/O=Org5,192.94.222.169:13523

TCPIP_PortMapping04=CN=Server6/O=Org6,192.94.222.169:13524
```

Сервер 2.

```
TCPIP_TcpIpAddress=0,192.94.222.169:13520
```

Сервер 3.

```
TCPIP_TcpIpAddress=0,192.94.222.169:13521
```

Сервер 4.

```
TCPIP_TcpIpAddress=0,192.94.222.169:13522
```

Сервер 5.

```
TCPIP_TcpIpAddress=0,192.94.222.169:13523
```

Сервер 6.

```
TCPIP_TcpIpAddress=0,192.94.222.169:13524
```

2.9.4 Использование Partitioned серверов в кластере серверов Domino.

Вы можете включать Partitioned сервера в кластер серверов Domino. Вы можете использовать в кластере Partitioned сервера с одиночными серверами и с Partitioned серверами, которые находящиеся на различных компьютерах.

Не включите Partitioned сервера, находящиеся на том же самом компьютере, в один кластер серверов. Если Вы используете Port Mapping, не включите больше чем один Port Mapping сервер в тот же самый кластер.

Когда Port Mapping сервер находится в кластере и возникает проблема в кластере, все Partitioned сервера на компьютере могут стать недоступным

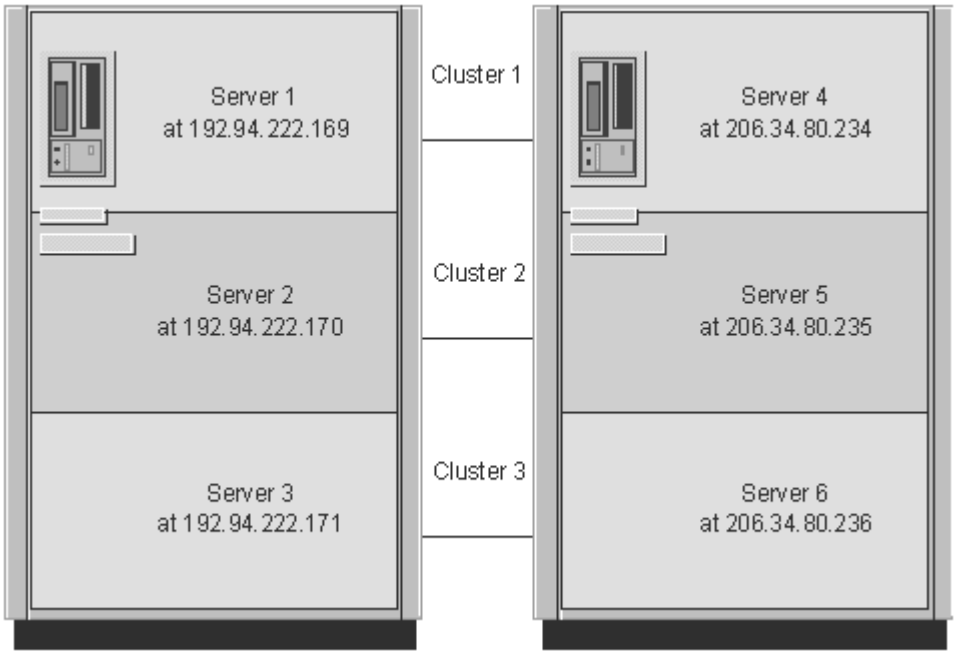


Рис. 41 Пример использования трех кластеров, на двух компьютерах, с тремя Partitioned серверами на каждом.

Когда Вы включаете Partitioned сервер в кластер, Вы не должны включать все Partitioned сервера машины в кластер. Следующий рисунок показывает два компьютера, каждый имеет три Partitioned сервера. Четыре из Partitioned серверов - сконфигурированы в два кластера, а два из Partitioned серверов находятся вне кластера.

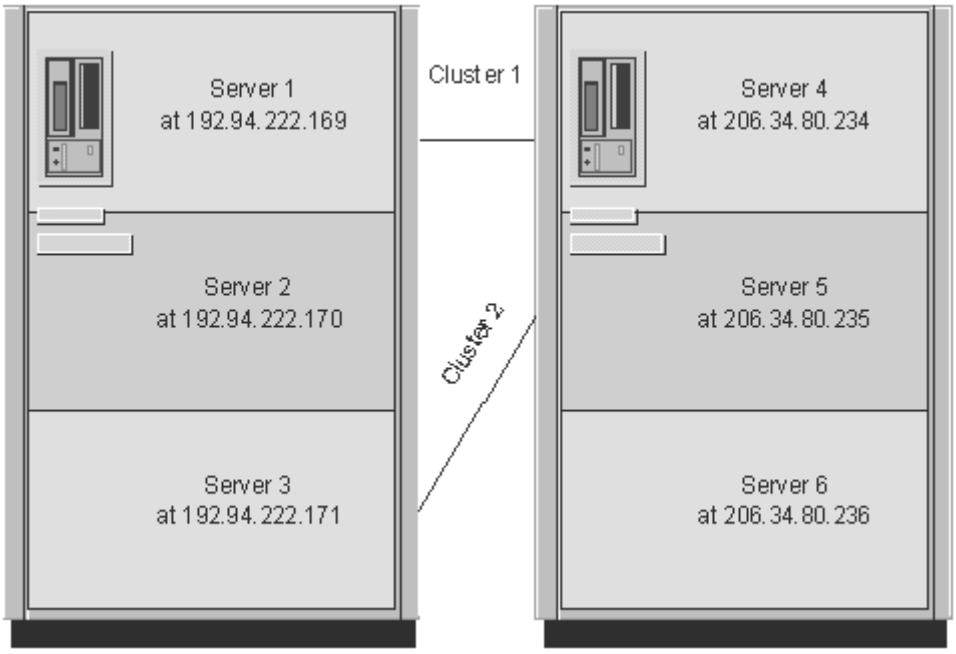


Рис. 42 Пример использования двух кластеров, на двух компьютерах, с тремя Partitioned серверами на каждом.

2.9.5 Удаление Partition сервера с компьютера.

Вы можете удалить все Partitioned сервера с компьютера или удалить последний установленный Partitioned сервер, который Вы установили

Удаление всех Partitioned серверов с компьютера.

Чтобы удалить все Partitioned сервера с компьютера, используйте программу Uninstall, которая поставляется с Вашей операционной системой.

Удаление последнего инсталлированного Вами Partitionedсервера.

Программа Uninstall не позволяет Вам определять, какой Partitioned сервер Вы хочет удалить. Uninstall удаляет только самый последний Partitioned сервер, который Вы добавляли на компьютер.

Обратите внимание, если Вы удаляете единственный Partitioned сервер с компьютера, Вы не можете потом использовать программу Uninstall в следующий раз, чтобы удалить другой Partitioned сервер с этого компьютера.

Чтобы удалить последний Partitioned сервер, который Вы установили, используйте эту процедуру:

*618 Сохраните все файлы, которые понадобятся Вам в дальнейшем, затем удалите каталог данных Domino для Partitioned сервера, который Вы будете деинсталлировать.

*619 Если Partitioned сервер использовал, уникальный адрес IP, уберите поддержку для этого IP. Если Partitioned сервер использовал имя хоста компьютера, как имя сервера Domino, не убирайте адрес IP.

*620 Если Partitioned сервер использовал Port Mapping, отредактируйте NOTES.INI Port Mapping сервера так, чтобы он больше не обращался к этому Partitioned серверу.

*621 Если Вы используете, WindowsNT, редактирует NT регистр, следующими способами:

*622 В папке HKEY_LOCAL_MACHINE\MACHINE\SOFTWARE\Lotus\Notes\VSERVER, выбирайте INSTANCE и уменьшите индекс на одну единицу.

*623 В папке HKEY_LOCAL_MACHINE\MACHINE\SOFTWARE\Lotus\Notes\VSERVER\CLIENT, удалите соответствующую запись для клиента и путь для инсталляции этого Partitioned сервера.

*624 В папке HKEY_LOCAL_MACHINE\MACHINE\SOFTWARE\Lotus\Notes\VSERVER\CLIENT, убедитесь, что внесенные в список клиенты последовательно расположены. Если Вы предварительно имели четыре Partitioned сервера и деинсталлировали сервер 2, измените список оставшихся Partitioned сервера как CLIENT1, CLIENT2, CLIENT3. Подтвердите, что эти строки соответствующими строками в NOTES.INI файле.

2.10 Настройка процесса администрирования - Administration Process.

Глава описывает как установить Administration Process, который упрощает задачи администрирования системы. Вы можете использовать процесс для удаления пользователей, создание реплик или редактирования ACLs.

2.10.1 Задача Administration Process

Administration Process - программа, которая автоматизирует многие обычные задачи администрирования. Например. Если Вы удаляете пользователя, Administration Process ищет имя пользователя в Domino Directory, удаляет его, удаляет имя пользователя из ACL и делает любые другие необходимые удаления касающиеся этого пользователя.

Administration Process автоматизирует эти задачи:

*625 Задачи переименования пользователей, групп, удаление пользователей, групп, удаление имен серверов, ресертификикация пользователей

*626 Задачи управления почтовыми файлами, удаление почтовых файлов, перемещение почтовых файлов.

*627 Задачи обслуживания документов сервера. Обновление типа CPU компьютера, платформы сервера, информация протокола сети в Server документе

Сервер администрирования.

Сервер администрирования обслуживает Administration Process. Вы определяете сервер администрирования для Domino Directory и для каждой базы данных. По умолчанию, первый Domino сервер, который Вы устанавливаете в домене, является сервером администрирования для Domino Directory. Сервер администрирования для Domino Directory обслуживает ACL Domino Directory, исполняет удаление, изменения имен, реплицирует эти изменения в другие Domino Directory домена.

Все базы данных нуждаются в сервере администрирования, чтобы управлять изменениями имен, удалением, которые будут происходить в базе данных - например, изменяется в ACL поля автора и читателя. Если база данных имеет реплики, и Вы назначаете сервер администрирования только для одной реплики. Тогда Administration Process делает все

изменения в этой реплике, а репликатор для этой базы данных распространит изменения во все другие реплики.

База данных Administration Requests.

Administration Process, прежде всего, взаимодействует с базой данных Administration Requests, запрашивает ее на сервере администрирования для Domino Directory, когда он запускается впервые на сервере. Чтобы завершить задачи, Administration Process отправляет по почте и отвечает на запросы в базе Administration Requests. Domino сервер используют реплики этой базы данных, чтобы распределить запросы, сделанные на одном сервере, на все другие сервера в домене.

Когда другой сервер устанавливается в домене, проверяется наличие базы данных Administration Requests, если она не существует, сервер создает “окурок” реплики, запрашивает базу данных с другого сервера в домене. Каждый сервер в домене хранит реплику Administration Requests, генерирует в ней запросы, используя Domino Directory.

База данных Certification Log.

Administration Process используется, чтобы выполнить изменения имен или ресертифицировать кого-либо, Вы должны создать базу данных Certification Log из шаблона (CERTLOG.NSF) на сервере, на котором хранится база данных Domino Directory. В базе будут регистрироваться все изменение имен или ресертификации пользователей и серверов. Если Certification Log существует на другом сервере, переместите Certification Log на сервер, содержащий Domino Directory, на котором Вы начинаете изменение имен или ресертификации пользователей. Это база содержит отчеты того, как Вы регистрируете сервера и пользователей, включая информацию относительно ID. Certification Log содержит сообщения, которые описывают результаты ресертификации, которые запрашивает Administration Process для своей работы.

2.10.2 Выбор сервера администрирования для Domino Directory

Выбор сервера администрирования для Domino Directory зависит от установки Вашей сети и доступного оборудования.

Всегда используйте самую последнюю версию Domino, на сервере администрирования Domino Directory, чтобы Вы могли использовать все самые новые опции Administration Process. При выборе сервера администрирования, для баз данных в домене, рассмотрите следующее:

*628 Использование Hub сервера, как сервер администрирования для Domino Directory и для других баз данных.

*629 Использование Dedicated сервера, как сервер администрирования для Domino Directory, при использовании одного или большего количества отдельных Hub серверов, как сервера администрирования для других баз данных.

*630 Использование многофункционального сервера, как сервер администрирования для Domino Directory, при распределении обязанностей администрирования для других баз данных на других серверах.

Если домен имеет только несколько серверов, Вы можете использовать первый выбор использования одного сервера администрирования для Domino Directory и других баз данных. Большинство ресурсов сервера администрирования используется для обновления Domino Directory, чтобы содержать Domino Directory в синхронизированном состоянии в

домене. Этот выбор централизует администрирование, но это может затрагивать выполнение работ на сервере. Поскольку обслуживание домена будет все время наращиваться, использование Administration Process и увеличивает нагрузку на сервер.

Второй выбор - использование регистрационного сервера, Dedicated сервера как сервера администрирования для Domino Directory. Вы можете использовать другой сервер типа Hub, для обработки ACL изменений других баз данных. Чтобы сделать это, определите для баз данных Hub сервера, сервер администрирования этих баз данных как - имя Hub сервера. Вы можете разделить ответственность за изменения в ACL баз данных, среди нескольких серверов администрирования. Но Вы должны удостовериться, что назначили сервер администрирования только одной реплике базы данных.

Использование сервера, который содержит почтовые файлы пользователей и другие базы данных, на сервере администрирования для Domino Directory возможно, но не рекомендуется по причинам загруженности таких серверов.

2.10.3 Настройка Administration Process

Чтобы настроить Administration Process, Вы должны выполнить эти задачи:

*631 Определить сервер администрирования для Domino Directory в домене. Это выполняется в течение установки сервера.

*632 Определить сервер администрирования для баз данных в домене.

*633 (Необязательно) Выполнить взаимную сертификацию доменов, чтобы позволить серверу администрирования в одном домене, экспортировать запросы или импортировать от сервера администрирования в других доменах.

*634 Проверить правильность настройки Administration Process.

*635 Установить ACL для Administration Process.

2.10.4 Выбор сервера администрирования для баз данных

Administration Process использует сервера администрирования, чтобы управлять изменениями, которые происходят в базах данных. Администратор или менеджер базы данных может определить сервер администрирования для базы данных. Исполните эту процедуру для назначения сервера администрирования:

*636 Из клиента Domino Administrator, откройте домен, содержащий сервер с базой данных, для которой Вы хотите назначить сервер администрирования.

*637 Из панели серверов выбирайте сервер, содержащий базы данных, которой Вы хотите определить сервером администрирования.

*638 Выбирайте закладку Файлы и затем выбирайте базу данных.

*639 Из панели инструментов выбирайте – Сервис – База данных – Управление доступом.

*640 Выбирайте – Advanced.

*641 Заполните эти поля, затем выбирайте - OK:

Поля	Значения
Сервер администрирования	Выбирайте одно из двух: *642 Выбирайте эту установку, чтобы назначить сервер администрирования. ACL базы данных автоматически будет обновлен, когда Administration Process будет запущен на сервере. *643 Не выбирайте эту установку и затем установите None, если Вы не хотите назначать сервер администрирования для базы данных. Список Контроля базы данных автоматически не будет обновлен, когда Administration Process запустится.
Изменять поля типа Readers And Authors	Поле, будет активировано только, когда выбрана предыдущая опция. Выбирайте одно из двух: *644 Обновлять поля Readers and Authors этой базы. *645 Не обновлять поля.

После ввода данных, выбирайте - OK.

2.10.4.1 Процесс Administration Requests в различных доменах.

Вы должны создать документы Cross-Domain, чтобы позволить серверу одного домена, посылать запросы администрирования по почте на сервера в другие домены. Конфигурируйте документы Cross-Domain после того, как Вы определяете сервера администрирования для Domino Directory в каждом домене. Administration Process для Domino Directory должен быть установлен на серверах в каждом домене. Cross-Domain работает, когда сервер администрирования для Directory - Domino сервер R5. Эти задачи могут быть выполнены в домене:

*646 Удаление пользователя

*647 Удаление сервера

*648 Переименование сервера

*649 Переименование пользователя

*650 Создание реплики

*651 Задачи управления создают другие запросы - например, Удаление в ACL, Переименование в полях Readers And Authors. Аналогично, в обработке с использованием Cross-Domain, эти запросы также создаются в другом домене, где они были созданы. Запросы, импортированные из другого домена, из последующих запросов, созданных обработкой.

Выгоды от использования Cross-Domain процесса администрирования.

В Cross-Domain обрабатываются:

*652 Запросы администрирования доменов могут защищать целостность данных в базах данных. Например, если человек удален из Domino Directory в одном домене, удаление пользователя происходит и в другом домене.

*653 Информации о контроле доступа распространяется между доменами, изменение имен размножаются по другим доменам. Например, люди и сервера зарегистрированные в одном домене могут также быть внесены в список документов Domino Directory и в базе данных ACL, в другом домене. Обработка Cross-Domain позволяет пользователям и серверам иметь доступ к базам данных и серверам в обоих доменах.

*654 Приложения легко можно распределять, потому что базы данных легко будут, копируются с серверов одного домена, на сервера в другом домене. Администраторы не должны установить индивидуальные обновления на всех серверах.

2.10.4.2 Создание конфигурации Cross-Domain и необходимых для этого документов.

Чтобы использовать Cross-Domain запросы администрирования, Вы должны создать эти документы в дополнение к Server документу:

*655 Документы Cross-Certificate для доменов.

*656 Документ подключения, позволяющий серверу соединяться с другим указанным сервером, в этом случае, другим сервером домена.

*657 Один или большее количество Cross-Domain документов конфигурации для каждого домена, из которого Вы импортируете запросы администрирования и в который Вы экспортируете запросы администрирования.

*658 Вы также должны добавить имя Anyone, чтобы создать документ конфигурации Cross-Domain, в поле List of administrators who are allowed to create Cross Domain configuration documents in the Administration Process Requests database, в документе профиля для Domino Directory. Если администратор пытается обрабатывать запрос между доменами, и имя администратора не будет внесено в список документа профиля, для Domino Directory, запрос администрирования будет терпеть неудачу.

База данных Administration Requests содержит документы конфигурации Cross-Domain, которые определяют, как обмениваются домены информацией, и обрабатывает запросы администрирования. Когда Вы конфигурируете документ конфигурации Cross-Domain, Вы определяете доверенные объекты. Доверенное лицо может быть человек, сервер или сертификатор. Все запросы, полученные из домена, должны быть подписаны одним из доверенных объектов. Запросы переименования - исключение; они подписаны сертификатором, так что их законность определена в соответствии с сертификатом и документами Cross-Domain при получении Domino Directory домена. Для запросов переименования, на сервере получателе в другом домене, должны иметься соответствующие взаимные сертификаты между иерархией доменов. Дополнительно Domino Directory назначения домена должен иметь документы Certifier, с публичным ключом сертификатора, для орг. структуры, представленной в запросе изменения имени.

*659 Выбирайте из меню Действие – Edit Directory Profile.

*660 В поле List of administrators who are allowed to create Cross Domain Configuration documents in the Administration Process Requests database введите имена любых людей, которым позволяется создавать документы конфигурации Cross-Domain.

*661 Сохраните и закройте документ.

Создание Cross-Domain документа конфигурации.

*662 Удостоверитесь, что Вы уже создали необходимый документ подключения, чтобы позволить связь между серверами.

*663 Из клиента Domino Administrator, выберите Файл – База данных – Открыть.

*664 Выбрать сервер, затем выберите Administration Requests (ADMIN4.NSF) и щелкайте - OK.

*665 Выбирайте – Add Configuration.

*666 На закладке Configuration выберите одно из двух:

- Outbound, чтобы создать outbound конфигурацию.
- Inbound, чтобы создать inbound конфигурацию.

Если Вы выбрали - Outbound, заполните эти поля и затем сохраните документ:

Поля	**Значение**
Domain to submit AdminP requests to	Имя домена или нескольких доменов, которым этот сервер пошлет запросы
List of AdminP requests to submit	Выберите тип запросов, которые этот server пошлет
List of approved signers	Имена подписывающих лиц - то есть доверенное лицо для типа запроса из домена создающего запрос. Подписывающее лицо должно быть менеджером Domino Directory и должно быть внесено в список в документ профиля, на наличие разрешения создавать взаимные документы конфигурации домена. Запрос на Create Replica требует, чтобы автор запроса на сервере источнике имел право на создание реплики на сервере назначения. Запрос Delete Requests, должен быть подписан, администратором домена источника. Запросы на Create Replica, должны быть подписаны сервером источником.
Only submit Create Replica requests to the domains listed above if the destination server is one of the following	Имя сервера, которому Вы пошлете запросы на создание реплики. Имя сервера должно быть в этом поле, и поле Domain to submit AdminP requests to. Эти поля показывают, что выбран запрос на Создание реплики.

Если Вы выбрали – Inbound, заполните следующие поля и сохраните документ:

Поля	**Значения**
Receive AdminP requests from domains	Введите имя одного или нескольких доменов, от которых этот сервер будет получать запросы
List of AdminP requests allowed from other domains	Выберите типы запросов, которые этот сервер примет от других доменов
List of approved signers	Имена подписывающих лиц - то есть доверенное подписывающее лицо для типов запроса домена назначения. Подписывающее лицо должно быть менеджером в Domino Directory и должно быть внесено в поле документа профиля, для разрешения создать взаимные документы конфигурации домена. Запросы на Create Replica требуют, чтобы автор запроса имел на сервере источнике, доступ создания реплик на сервере назначения. Запросы Delete Requests, должен быть подписан администратором домена источника. Запросы на Create Replica, должен быть подписан, сервером источником.
Only allow Create Replica requests if intended for one of the following servers	Имя сервера в Вашем текущем домене, который примет, запросы на реплики от других доменов. Эти поля показывают, что выбран запрос Create Replica.

2.10.4.3 Проверка работы Administration Process.

После того, как Вы настроили сервер администрирования и Administration Process, проверяйте, что процесс протекает правильно.

*667 Откройте базу данных Administration Requests (ADMIN4.NSF) на сервере администрирования для Domino Directory.

*668 Проверьте, что запрос, Server's build number, в Server документе, существует.

*669 По прошествию 60 минут, после того как Administration Process начинают работу, открывайте базу данных Administration Requests снова и проверьте документ ответа, указывающий, что Administration Process добавлял, номер сборки сервера в Server документе.

*670 Откройте Server документ и сделайте следующее:

*671 Из клиента Domino Administrator, выбирайте – Настройка – Сервер – Все документы на сервере

*672 Выбирайте сервер, чей документ Вы хотите открыть.

*673 На закладке Basics, проверите, что поле Server build number, содержит значение.

Закончить процедуру, Setting up ACLs for the Administration Process по мере необходимости.

2.10.4.4 Настройка ACL для Administration Process.

Каждый администратор, который использует Administration Process, должен иметь соответствующие права доступа и роли к Domino Directory, базе данных Administration Requests (ADMIN4.NSF) и базе данных Certification Log (CERTLOG.NSF).

Самый быстрый способ обеспечивать администраторов доступом, в котором они нуждаются, состоит в том, чтобы дать им минимальные уровни доступа:

*674 Для Domino Directory, создайте группу администраторов с доступом редактора и внесите в список группы администраторов

*675 Для базы данных Administration Requests, дайте доступ автора большинству администраторов. Если администратор будет одобрять запросы, дайте доступ редактора.

*676 Для базы данных Certification Log, дайте доступ автора с созданием документов

*677 Для удаления WindowsNT пользователя, запрос на удаления, должен быть сделан с машины WindowsNT, а инициатор должен быть WindowsNT администратором домена с правами удалять пользователей.

2.10.5 База данных Administration Requests.

Чтобы просматривать документы в базе данных Administration Requests, Вы можете использовать клиента Domino Administrator или Web Administrator.

Действия, которые требуют одобрения администратора.

Когда процесс администрирования запрашивает администратора одобрения и если оно получено, оно сохраняется в базе данных Administration Requests и процесс продолжается.

Действия, требующие одобрение администратора	**Объяснение**
Complete Moving a mail file	Перемещение почтового файла. Файл почты должен быть удален со старого сервера, после его перемещения на новый почтовый сервер.
Move a database replica from a non-clustered server	Перемещение баз данных репликацией на другой сервер. Удаляется реплики на старом сервере.
Accept administration requests from other domains	Принятие запроса администрирования из других доменов. Если имя сервера запроса принадлежит другому домену, а запрос должен удалять или переименовать пользователя или сервера.
Delete resources	Удаление ресурса. Удаляет ресурса, типа имени зала заседаний из Domino Directory. Ресурсы также связаны с календарями и планированием пользователей.
Delete mail files	Удаление почтового файла. Одобрение администратора требуется для удаления почтового файла для удаляемого пользователя
Move users to a different organization hierarchy	Перевод пользователя в различные иерархии организаций, требует одобрения администратора организации назначения.
Delete Private Design Elements	Одобрение администратора требуется, для удаления личных агентов, видов, папок

2.10.6 Обслуживание запросов администрирования.

Управление процессом администрирования влечет в себя одобрение запросов. На выполнение запросов требуется определенное время. Проверяйте базу данных Administration Requests на наличие ошибок при выполнении запросов.

Одобрение запросов.

Проверяйте базу данных Administration Requests ежедневно на наличие запросов, которые требуют одобрения.

*678 Из клиента Domino Administrator, выберите меню Файл – База данных – Открыть.

*679 Выбирайте нужный сервер и затем открывайте базу данных Administration Requests (ADMIN4.NSF).

*680 Отрывайте представление Pending Administrator Approval (ожидаемые одобрения запросы).

*681 Открывайте запрос в режиме редактирования, для чтения информации.

*682 Выбирайте – Одобрить.

Ускорение выполнения запросов.

Следуйте этой процедурой, чтобы инициализировать запрос на немедленное выполнение вместо ожидания времени Administration Process.

*683 Из клиента Domino Administrator, выберите сервер.

*684 Выбирайте закладку Сервер.

*685 Выбирайте Консоль сервера.

*686 Введите команду

```
Tell adminp all
```

Просмотр ошибок при выполнении запросов.

*687 Откройте базу данных Administration Requests (ADMIN4.NSF).

*688 Выбирайте представление All Errors by Date or View - All Errors by Server.

*689 Откройте документ ответа и читайте ошибки.

*690 После того, как Вы исправите проблему, щелкаете – Yes, в поле Perform request again (исполнит запрос снова) в документе ответа. В зависимости от задачи, Вы можете повторно запустить запросы из Domino Directory. Это происходит, если задача, например переименования пользователя, определила неправильное новое имя пользователя.

Вы может использовать Web Administrator, чтобы просматривать запросы Administration Process и ошибки, однако, Вы не можете одобрять или исправлять ошибки из Web Administrator.

2.10.6.1 Расписание выполнение запросов Administration Request.

Каждая значение в секции Administration Process Server документа, определяет время для определенных типов запросов. Назначения интервала и графика для репликаций для каждого сервера определяют, как быстро распространяются реплики по всему домену. Скорость с которой распространяются запросы в домене, зависит от графика репликаций для серверов. Если необходимо, Вы можете наметить дополнительные реплики, для ускорения обновления данных.

Чтобы установить время по умолчанию, когда запросы администрирования будут выполняться, редактируйте Server документ. Вы можете захотеть выполнить запрос немедленно, если запрос администрирования является для Вас критическим.

Расписание для запросов Administration Process.

*691 Из клиента Domino Administrator, выбирайте закладку Настройка.

*692 Выбирайте из левой панели - Сервер – Все документы на сервере.

*693 Выбрать сервер, чей документ сервера Вы будете редактировать.

*694 Выбирайте закладку - Administration Process.

*695 Заполните эти поля и затем сохраните документ.

Поля	**Значение**
Interval	Число минут, между обработкой запросов связанных с именами (переименование, удаление ресертификация). По умолчанию - 60 минут.
Execute once a day requests at	Время, обновления документов Person, при переименовании пользователей. По умолчанию - 12 AM.
Interval between purging mail file and deleting when using object store	Количество дней, для удаление почтовых файлов и удаления всех объектов в Shared Mail. По умолчанию - 14 дней.
Start executing on	День, в который модернизируются поля Authors And Readers, в базах данных и удаление распределенных элементов дизайна для удаляемого пользователя. По умолчанию - в воскресенье.
Start executing at	Время, в которое модернизируются поля Authors And Readers, в базах данных и удаление распределенных элементов дизайна для удаляемого пользователя По умолчанию - в 12AM.
Move mail file expiration days	Число дней, в течение которых Domino переносит почтовые файлы клиентов. По умолчанию - 21 день. Может иметь значение - от 7 до 60, включительно.
Store Admin Process log entries when status of no change is recorded	Статус протоколирования в базе данных Administration Process Когда база данных просматривается на предмет запросов, она делает запись протокола, в этой базе данных, или не делает... По умолчанию – Да. Выбор - Нет, может существенно уменьшать размер Вашей базы данных запросов администрирования.
Suspend Admin Process at	(Выборочно) Время, когда Administration Process прекращает обрабатывать запросы. Чтобы сохранить ресурсы сервера, приостанавливайте Administration Process в пиковые часы работы сервера.

Restart Admin Process at	(Выборочно) Время, когда Administration Process опять начинает обрабатывать запросы. Чтобы сохранить ресурсы сервера, Administration Process обычно останавливается и повторно запускается в не пиковые часы работы.

2.10.6.2 Изменение значения нитей для Administration Process.

По умолчанию, Administration Process использует три нити, чтобы обрабатывать запросы. Чтобы улучшать выполнение работ Administration Process, увеличьте число нитей.

*696 Из клиента Domino Administrator, выбирайте закладку Настройка.

*697 Выбирайте из левой панели - Сервер – Все документы на сервере.

*698 Выбрать сервер, чей документ сервера Вы будете редактировать.

*699 Выбирайте закладку Administration Process.

*700 Введите в поле Maximum number of threads, нужное Вам значение и затем сохраните документ.

*701 Перезапустите Administration Process, для вступления изменений в силу.

2.10.6.3 Создание представления $AdminP.

По умолчанию, Administration Process просматривает все документы в базе данных, ищет значения полей Readers And Authors, когда Administration Request обрабатывает запрос, значения этих полей будут получены. Администраторы и менеджеры базы данных могут создавать представление в базе данных, с ограниченным доступом и отображением полей Readers And Authors. Представлению должно быть назначено имя – $AdminP.

2.11 Установка и настройка Web Administrator.

Глава содержит информацию о конфигурировании Web Administrator, который позволяет Вам использовать браузер, чтобы управлять Вашими серверами.

2.11.1 Web Administrator

Если Вы имеете браузер и хотите управлять и просматривать установки Domino сервера, Вы можете использовать Web Administrator. Web Administrator имеет много возможностей, которые могут быть доступны из Domino Web Administrator. Вы можете, просматривать информацию о Вашем сервере и пользователях, изменять ACL баз данных и использовать удаленную консоль сервера. Web Administrator обеспечивает Вам свободный проход к Domino серверу для администраторов.

Web Administrator использует базу данных Web Administrator (WEBADMIN.NSF). При первом запуске HTTP задачи на Web сервере, Domino автоматически создает эту базу данных, в каталоге данных Domino. Domino назначает уникальный ID реплики, поэтому база данных Web Administrator не реплицируется между серверами.

Базы данных используемые Web Administrator.

Web Administrator использует несколько системных баз данных, в дополнение к базе данных Web Administrator (WEBADMIN.NSF). Если один из этих файлов не существует на сервере, Web Administrator не показывает команду, связанную с файлом. Например, если в Domino, не существует базы Help_5_Administration.nsf, в каталоге Help, Web Administrator не показывает команду Help.

2.11.2 Настройка Web Administrator.

Чтобы использовать Web Administrator, Вы должны выполнить следующие процедуры:

*702 Удостоверьтесь, что сервер, которым Вы хотите управлять, установлен как Domino Web сервер. Хотя Вы можете использовать сервер для других серверных задач - например, для передачи почту и др. услуги - Вы должны запустить HTTP задачу и использовать браузер для доступа к серверу.

*703 В целях безопасности, Вы можете управлять только сервером, на которых Вы устанавливаете эти задачи.

*704 Установите доступ к Web Administrator, к базе данных WEBADMIN.NSF - Администратор.

*705 Подготовьте браузер клиента, чтобы использовать базу данных Web Administrator. Если Domino Web сервер использует SSL, установите SSL для браузера клиента. Разрешите выполнение Java applets и JavaScript в Netscape Navigator, или Scripting Active в Internet Explorer Microsoft.

Domino создает базу (WEBADMIN.NSF) автоматически, при запуске HTTP задачи, в первый раз.

2.11.3 Установка доступа к базе данных Web Administrator

Domino автоматически создает базу данных на сервере, когда задача HTTP запускается в первый раз. По умолчанию, позволяется доступ к базе всем пользователям, внесенным в поле администраторов сервера Server документа. Администратор должен или ввести пароль интернета или получить SSL сертификат клиента. Web Administrator использует имя и пароль, или SSL, чтобы проверить идентичность администратора. Метод Web, который администратор использует, зависит от того, какие вы устанавливаете опции безопасности для сервера.

Чтобы позволять другим администраторам использовать Web Administrator, Вы должны сделать изменения в назначениях доступа для них.

Установки опций безопасности по умолчанию.

Следующее установки для Web в базе данных ACL. Вы не должны изменить эти назначения, если имя администратора занесено в поле администраторов Server документа.

Максимальный доступ к базе данных, через интернет.

Установки по умолчанию	Описание

Manager	Web Administrator использует эту установку, при доступе администраторов на сервер, использую имя и пароль для изменений ACL, Web базы данных. Web Administrator не использует эту установку, когда доступ администраторов на сервер использует SSL.

ACL.

Имя по умолчания	**Уровень доступа**
Имена, внесенные в поле Administrators из Server документа	Менеджер и роли ServerAdmin, ServerMonitor, DatabaseAdmin, FileRead и FileModify
Имя	Менеджер без ролей
- Default -	Нет доступа
Anonymous	Нет доступа
LocalDomainServers	Менеджер и роли ServerAdmin, ServerMonitor, DatabaseAdmin, FileRead и FileModify
OtherDomainServers	Нет доступа
Lotus Notes Template Development/Lotus Notes	Менеджер и роли ServerAdmin, ServerMonitor, DatabaseAdmin, FileRead и FileModify

Следующее установки, должны быть установлены на закладке Security, Server документа. Вы не должны изменить эти установки, если имя администратора находится в поле администраторов, Server документа.

Установки безопасности	**Имя по умолчанию**
Administer the server from a browser	Имена, внесенные в поле администраторов, Server документа для Domino Web сервера

Все агенты в базе данных Web Administrator, подписаны Lotus Notes Template Development/Lotus Notes, это предоставляют неограниченные привилегии выполнения агентов по умолчанию.

Чтобы использовать имя и пароль, администраторы должны иметь пароль интернета в их Person документах. Чтобы использовать SSL идентификацию клиента, администраторы должны получить сертификат клиента, SSL должен быть установлен на сервере. Кроме того, сервер должен требовать SSL связей, для доступа к базе данных.

2.11.3.1 Дополнительные настройки для доступа к Web Administrator.

Domino автоматически дает доступ всем пользователям из поля администраторов, Server документа, когда Domino создает базу данных Web Administrator. Чтобы позволять дополнительным администраторам использовать Web Administrator, Вы должны дать им соответствующий доступ.

Вы используете браузер и Web Administrator, чтобы выполнить процедуру ниже:

*706 Добавить администратора или имя группы к ACL базы данных Web Administrator (WEBADMIN.NSF), дать пользователю доступ Менеджера.

*707 Далее назначьте соответствующие роли базы данных Web Administrator.

*708 Делать одно из следующего:

- Если сервер требует имя и пароль, редактируйте Person документ каждого администратора и введите пароль интернета.
- Если сервер требует SSL идентификации клиента, настройте браузер для SSL.
- Редактируйте Server документ для Domino Web сервера и добавьте администратора, или имя группы в поле Administer the server from a browser, на закладке Security.

Роли для администраторов.

Если администратор не имеет соответствующей роли, Web Administrator не показывает связанные с ними команды. Администраторы не нуждаются в ролях, чтобы иметь доступ к командам Установок и Помощи.

*709 **ServerAdmin.** Получает доступ к Console, Analysis, Messaging, Directories commands, Configuration commands, Servers, Clusters, Domains, Configurations, Web Configurations, Connections, Programs.

*710 **ServerMonitor.** Получает доступ к Messaging, Replication, Analysis, Logfile, Statistics, Events, Memory, Diskspace, Alerts, Web Statistics, Billing.

*711 **DatabaseAdmin.** Получает доступ к Databases commands, Directories commands, People, Groups.

*712 **FileRead.** Получает доступ к Configuration, System Files (read only).

*713 **FileModify.** Получает доступ к Configuration, System Files (read/write).

2.11.4 Запуск и настройка Web Administrator

Когда Вы запускаете Web Administrator, он показывает информацию о сервере и администраторе, который связан с сервером - например, имя сервера и операционную систему сервера.

Для запуска Web Administrator

*714 Из браузера, введите в URL:

```
http://hostname/webadmin.nsf
```

Где `hostname` - имя Вашего хоста, или IP адрес Domino сервера которым Вы хотите управлять.

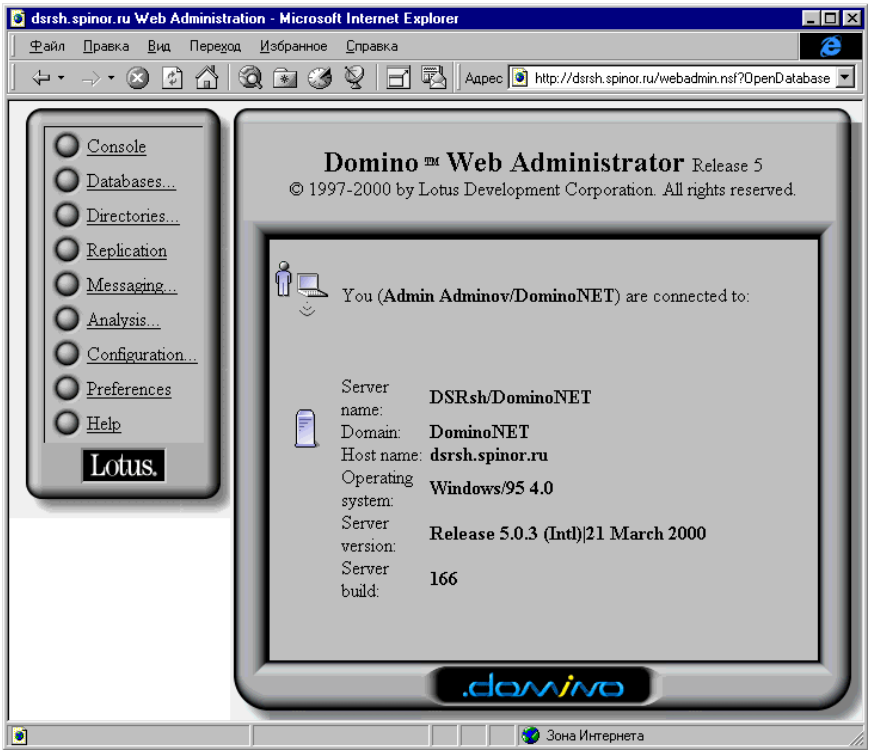


Рис. 43 Главное окно Domino Web Administrator.

*715 Введите Ваше иерархическое имя или обычное имя и Ваш пароль для интернета.

Примечание. Чтобы просматривать несколько версий Web Administrator в одно и то же время - например, чтобы контролировать почту и контролировать память сервера одновременно - запустите другую копию браузера с Web Administrator и установите оба окна рядом на экране. При запуске нескольких копий Web Administrator, используйте интерфейс Dropdown, чтобы показать большее количество информации в окне браузера.

Изменение установок Domino Directory, установленных по умолчанию.

По умолчанию, Web Administrator показывает пользователей и группы, из первичного Domino Directory, с именем NAMES.NSF. Если Вы имеете несколько Domino Directory расположенных на сервере, Вы можете изменять Domino Directory, управлять пользователями и группами редактировать документы из меню конфигурации. Эти установки не имеет никакого влияния на другие функции Web Administrator, например, при показе статистики, или при изменении списка контроля доступа баз данных.

*716 Запустить Web Administrator.

*717 Выбирайте – Preferences, затем выбирайте – Edit Preferences.

*718 Выбрать Domino Directory в поле Current Directory.

*719 Выбирайте – Set Preferences.

Изменение пользовательского интерфейса Web Administrator.

Web Administrator снабжен тремя интерфейсами пользователя: Button Interface, Dropdown Interface и Plain Interface. Интерфейс определяет отображение Web Administrator в Вашем браузере. Все функции доступны независимо от интерфейса, который Вы выбираете. Domino сохраняет интерфейс Domino Directory по умолчанию, в базе данных Web Administrator, в индивидуальном документе профиля для каждого администратора. Каждый

администратор может устанавливать предпочтение без изменения предпочтений других администраторов.

*720 Запустите Web Administrator.

*721 Выбирайте – Preferences, затем щелкайте – Edit Preferences.

*722 Выбрать интерфейс для пользователя:

- **Button Interface**, показывает графику для команд на левой стороне Вашего браузера. Кнопочный интерфейс установлен по умолчанию для всех браузеров. Используйте этот интерфейс, чтобы показать графическое представление команд, когда Вы используете больше чем 256 цветов, предпочтительно для высокого разрешения.

- **Dropdown Interface**, показывает команды в окне Dropdown, в верхней части браузера. Дополнительные поля DropDown появляются, когда Вы должны выбрать дополнительные команды. Используйте интерфейс DropDown, чтобы показать большее количество информации или когда Вы используете только 256 цветов.

- **Plain Interface**, показывает команды в окне DropDown, без использования рамок и графики. Используйте интерфейс с 16-цветным режимом, когда Вы хотите Web Administrator, работал быстро - например, когда Вы используете модем, чтобы соединиться. Установите по умолчанию для OS/2 и Windows3.1x браузеров, которые используют более ранние версии HTML.

*723 Выбирайте – Set Preferences.

2.11.5 Использование Web Administrator

После того как вы установили Web Administrator, вы можете контролировать следующие задачи из браузера:

*724 Мониторинг почты ждущей доставки и не доставленной почты

*725 Мониторинг памяти сервера и его дискового пространства

*726 Мониторинг запросов сервера и команд

*727 Анализ сообщений сервера и представлений файла LOG.NSF

*728 Вводить команды сервера на удаленной консоли сервера

*729 Создание групп и Person документов

*730 Управление ACL баз данных

*731 Управление базами данных

*732 Создание новых баз данных

*733 Редактирование системных файлов

*734 Создание тестовых почтовых сообщений (Track mail messages)

*735 Генерирование и использование почтовых отчетов

2.12 Установка Domino Web сервера

Глава описывает, как установить и настроить Domino сервер как Web сервер.

2.12.1 Web сервер Domino

Одна из особенностей Domino сервера, это объединение сервера приложений Domino и Web сервера. Поэтому приложения Web сервера Domino могут отвечать Web пользователям, которые через интернет или интранет, могут получить доступ к данным, которые сохранены, или в системных файлах, или в базах данных Domino.

Когда Web браузер запрашивает страницу в базе данных Domino, Domino конвертирует документ в формат HTML. Когда Web браузер запрашивает страницу в HTML, Domino читает ее непосредственно из файловой системы. Web сервер использует HTTP протокол, чтобы передать информацию Web браузеру. При использовании Domino, для хранения Web страниц в базе данных, имеется главное преимущество по хранению статических HTML страниц. При использовании Domino, любые изменение, которое Вы делаете в базе данных, автоматически будут отражены на Web сервере.

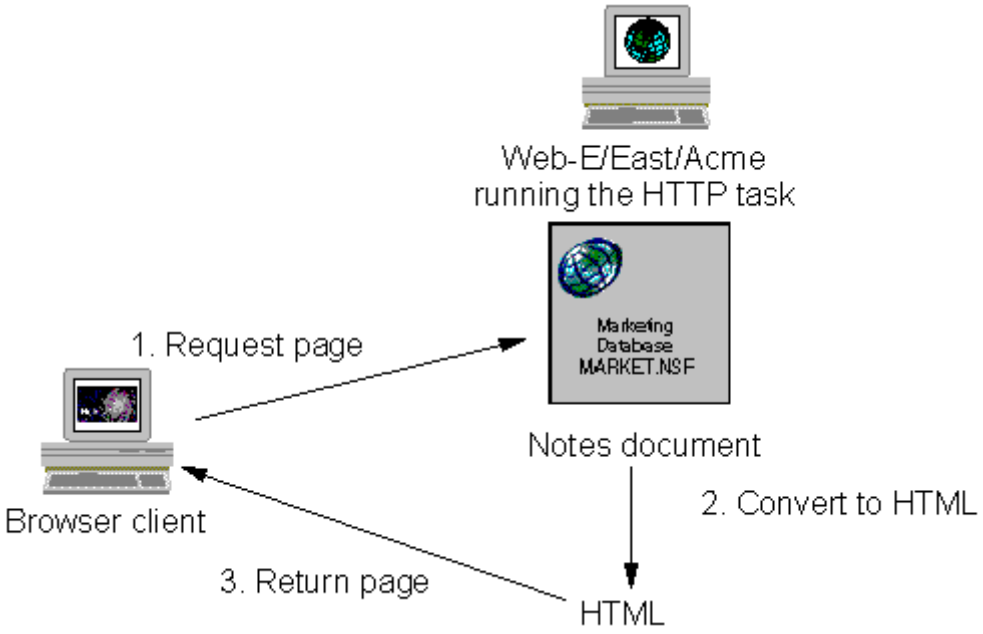


Рис. 44 Использование Domino Web сервера, для отображения документа Notes как HTML страницы - браузеру клиента.

Любое из приложений Domino может быть Web приложением. Прежде, чем Вы создаете Web приложение, ознакомьтесь с особенностями Domino, которые могут быть переведены в HTML и определите, будут ли Web пользователи и клиенты Notes получать доступ к приложениям одновременно. Вы можете использовать язык формул Notes, чтобы обнаружить, который тип пользователя обращается к приложению и затем, основываясь на типе пользователя, ввести изменения в отображении информации в приложении.

Domino Web сервер может состоять из единственной базы данных или нескольких баз данных. Вы можете также установить единственных сервер, который позволит Вам принимать запросы многих Web серверов на единственной машине (компьютере) и использовать различные имена хостов для доступа к серверу.

В дополнение к Web обязанностям, Web сервер может управлять другими серверными задачами, например маршрутизацией почты. Однако Вы должны тщательно проверить безопасность баз данных, если Вы не хотите пускать пользователей вне Вашей организации к базам данных на сервере.

Возможности Web сервера.

Domino поддерживает эти возможности Web сервера:

*736 Трансляция Notes в код HTML. Например, в код HTML, транслируются горячие точки Notes, они переводятся в <A> tags.

*737 Passthru HTML, Вы можете включать в форму, документ или документы About и Using. Domino интерпретирует их как HTML. Passthru HTML позволяет Вам использовать на Web - только форматированный текст, связи, изображения, команды, и программы. С использованием Passthru HTML, Вы может комбинировать возможности Domino и HTML код.

*738 Вы можете использовать безопасность Notes, как стандарт безопасности Web Domino. Вы можете использовать для безопасности ACL баз данных SSL и проверку имени и пароля.

*739 Поддерживаются Java апплеты с использованием Passthru HTML или вложения в документ.

*740 Поддерживается JavaScript, который может быть включен как Passthru HTML, или вложен непосредственно в документ.

*741 Поддерживаются CGI программы, которые могут быть включены в Passthru HTML в документе.

*742 Поддерживается статических HTML страниц, которые находятся в каталоге на диске сервера. Статические HTML страницы могут быть введены как Passthru HTML, включены в документ или могут использоваться, непосредственно используя URL.

*743 Поддерживается переадресация и ReMapping URLs и каталогов в другие места хранения файлов.

*744 Поддерживаются Virtual Servers, которые позволяют иметь несколько Web с отдельными именами DNS, на одном компьютере.

*745 Поддерживаются кластера серверов, которые позволяют переадресацию с сервера на другой сервер для балансирования загрузки

Создание Web серверов.

Вы могли бы установить один Web сервер для внутренних процессов, а другой Web сервер для внешних организаций. Web менеджеры могут делать изменения на сервере организации, без доступа на него пользователей. В конце концов, когда изменения будут сделаны, и будут удовлетворять менеджеров, внутренний сервер организации может быть реплицирован на сервер для внешнего использования. Кроме того, использование внутреннего сервера организации позволяет менеджерам, просмотреть изменения через браузер, перед их реплицированием на основной сервер.

Если Вы используете внутренний сервер организации, сделайте доступ на него только менеджерам. Также убедитесь, что дали менеджерам право репликаций на внешний сервер.

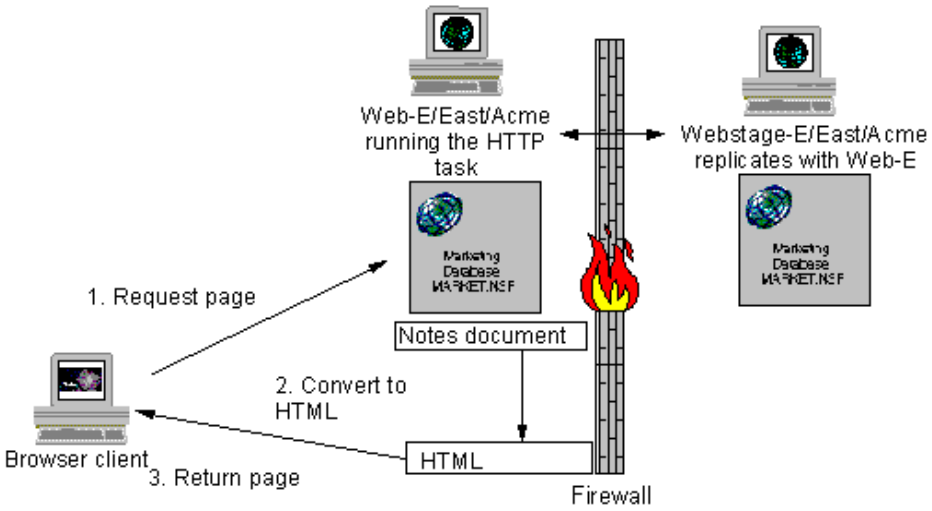


Рис. 45 Использование двух Domino Web серверов для подготовки и публикации документов Notes в интернете.

2.12.1.1 Как работает Domino Web сервер?

Domino Web сервер просматривает URL в поступающем запросе и определяет, запрашивается ли информация из базы данных Domino, или это запрос к файлу HTML. Если запрашивается HTML файл, Domino выполняет действия точно так же как любой другой Web сервер и предоставляет файл клиенту Web. Когда запрос сделан в базу данных Domino, Domino обращается к базе данных чтобы предоставить информацию Web клиенту, или поместить информацию от Web клиента в базу данных.

Domino поддерживает URL расширения, которые расширяют функциональные возможности клиента Web. Например, этот URL открывает базу данных Notes.net:

```
http://www.notes.net/welcome.nsf?OpenDatabase
```

В этом примере, запрос клиента - Notes документ, в базе данных. Сервер возвращает документ Notes - клиенту. Domino конвертирует документ в HTML и затем показывает его браузеру клиента.

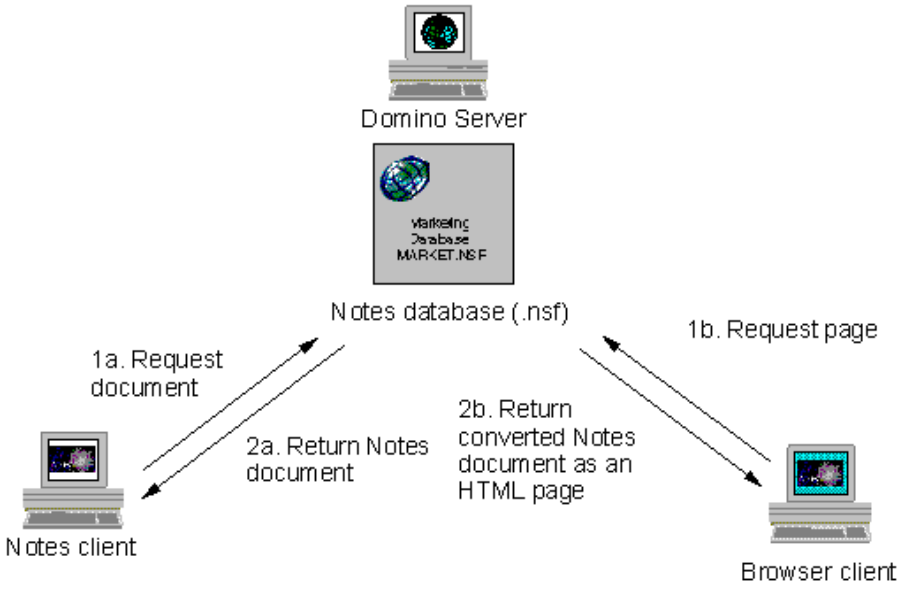


Рис. 46 Пример использования данных Domino сервера для разных типов клиентов.

2.12.2 Установка Domino Web сервера.

*746 Прежде, чем Вы установите Web сервер:

- Удостоверитесь, что Вы понимаете TCP/IP концепции, включая DNS имена хостов и IP адресование.
- Установите Domino сервер и настройте безопасность для сервера.

*747 Чтобы позволить пользователям соединиться с сервером по интернету, соедините сервер с Поставщиком Обслуживания Интернет (ISP) и зарегистрируйте имя домена сервера и адрес IP на DNS ISP's сервере. Если Вы хотите, чтобы пользователи соединились с сервером по внутренней сети, без соединения с интернетом, регистрируйте имя домена сервера и адрес IP на DNS сервере в Вашей организации.

*748 Из клиента Domino Administrator, выбирайте закладку Настройка, выбирайте Сервер и затем откройте Server документ для будущего сервера Web.

*749 Выбирайте закладку Ports – Internet Ports.

*750 Если Вы не используете SSL, удостоверьтесь, что запрещена эта опция в TCP/IP port status или SSL port status поля, на закладке Web.

*751 Сохраните документ.

*752 Запустите Domino сервер и запустите HTTP задачу.

*753 Чтобы проверить Ваши настройки сервера, запустите Ваш браузер и введите имя DNS или адрес IP сервера.

Обратите внимание, При регистрации имени на DNS Domino сервера и IP адреса, пользователи могут просматривать базы данных непосредственно через Web сервер.

2.12.2.1 Настройка параметров Domino Web сервера.

Server документ для Web сервера. Пользователи вводят www.acme.com , для доступа на сервер, это имя указано на сервере, в стеке протоколов TCP/IP, операционной системы.

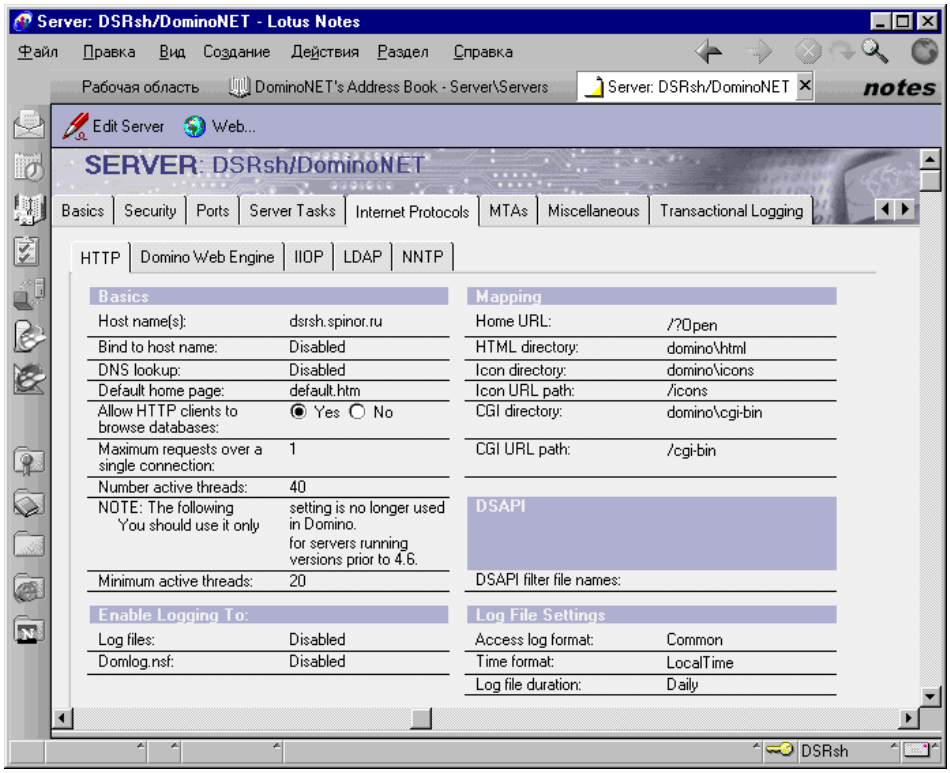


Рис. 47 Пример Server документа, секции HTTP.

2.12.3 Настройка Web сервера

Вы можете делать эти необязательные изменения в Server документе, чтобы изменить установки Web сервера.

*754 Из клиента Domino Administrator, выбирайте закладку Настройки, выбирайте сервер и затем откройте Server документ.

*755 Выбирайте закладку Ports – Internet Ports – Web, затем заполните поле:

Поле	**Значение**
TCP/IP port number	Номер порта, который должен быть больше чем 1024, если вы не изменяете номер порта, то стандарт 80 порт. Это - порт, на котором Domino слушает запросы HTTP. Номера портов меньше чем 1024, зарезервированы для других задач TCP/IP. Измените TCP/IP номер порта, только если это необходимо. Если Вы изменяете TCP/IP номер порта, клиенты должны включить определенный номер порта в запрос на Domino сервер. Номеру порта предшествует двоеточие и следует за именем DNS в URL. Например, URL http://www.lotus.com:8008/ запрашивает страницу по умолчанию, с хоста www.lotus.com, который работает по 8008 порту.

*756 Выбирайте закладку Internet Protocols – HTTP и заполните поля:

Поле	**Значение**
DNS lookup	Выбирайте одно: *757 Enabled - Domino посматривает имя DNS клиента. Domino LOG.NSF файл будет содержать имена хостов, соответствующие машине, используемой Web клиентов. *758 Disabled - (по умолчанию) Не просматривать DNS. Domino LOG.NSF файл и база данных будет содержать только IP адрес клиентов. **Примечание.** Выбор – Disabled существенно повышает производительность Domino сервера.
Bind to host name	Выбирайте одно: *759 Enabled – вы можете вводить имена псевдонимов названия в поля. Псевдонимы позволяют пользователям доступу к Web серверу с использованием другого имени (псевдонима), чем имя Domino сервера. *760 Disabled - (по умолчанию) запрещение всех псевдонимов.
Allow HTTP clients to browse databases	Выбирайте одно: *761 Yes - Web пользователям разрешается просмотр каталога Web сервера, командой ?OpenServer. Команда выводит список всех баз, расположенный на сервере. *762 No - (по умолчанию) просмотр каталога сервера, для Web пользователей запрещается.

*763 Выбирайте закладку Internet Protocols – Domino Web Engine, заполните эти поля, сохраните и закройте документ:

Поле	**Значение**

Make this site accessible to web site search crawlers	Выбирайте: *764 Enabled – использование знака “!” для генерации Domino URL команд *765 Disabled - (по умолчанию) использование знака “?” для генерации URL команд Использование знака “!” вместо вопроса, делает более легким поиск по Web, программами поиска для Web. Многие программы игнорируют знак “?” считая его CGI программой для запуска. Эти установки никак не влияют на URL команды для доступа на Domino сервер.

*766 Введите команду на консоли сервера для перезапуска сервера и вступлению изменений в силу:

```
tell http restart
```

2.12.4 Запуск и остановка Domino Web сервера.

Задача	**Ваши действия**
Запуск Web сервера вручную	Введите команду Load http на консоли сервера.
Запуск Web сервера автоматически, при старте сервера Domino	Редактируйте переменную ServerTasks в NOTES.INI и включите в нее имя задачи HTTP для автоматического запуска задачи при старте сервера
Остановка Web сервера	Введите Tell Http Quit, на консоли сервера.
Используйте эту команду для вступления в силу новых установок конфигурации сервера. (Перезапуск Web сервера)	Введите Tell Http Restart, на консоли сервера.

2.12.5 Поддержка нескольких Web серверов.

Если Вы - Поставщик Обслуживания Интернет (ISP) или администратор интернет, который обеспечивает услугами нескольких клиентов, Вы можете размещать виртуальные сервера на одном единственном Domino Web сервере. При этом единственный Domino Web сервер может поддерживать несколько Web участков. Использование виртуальных серверов позволяет Вам обслуживать отдельные участки сети, без несения дополнительных расходов, аппаратных средств и программного обеспечения.

Вы можете сконфигурировать каждый Web участок для Domino с собственным IP адресом, домашней страницей по умолчанию, настроить сообщения Web сервера, HTML, CGI и

каталоги для изображений. Каталог данных Domino сервера, однако, конфигурируется индивидуально для каждого виртуального сервера. Для конфигурирования виртуального сервера, используйте документ Virtual Server, из Domino Directory.

Перед конфигурированием виртуального сервера в Domino, Вы должны установить сетевое соединение для каждого виртуального сервера. Каждый виртуальный сервер может иметь собственный отдельный, постоянный IP адрес, или иметь несколько имен хостов, привязанных к одному и тому же IP адресу.

Domino не ограничивает число виртуальных серверов, которое Вы можете устанавливать. Число виртуальных серверов, которые Вы можете установить на Вашем Domino Web сервере, зависит от операционной системы и аппаратных средств Вашей системы. Некоторые аппаратные средства и операционные системы имеют ограничения, которые включают предел числа IP адресов, которые Вы можете связывать с операционной системой, и ограничения на использование числа сетевых карт, которые Вы можете использовать на компьютере.

Вы можете использовать SSL, если Вы устанавливаете несколько Web участков на одном сервере. Вы можете также требовать, чтобы пользователи вводили имена и пароли, для установки подлинности по TCP/IP.

В следующем примере, участки WWW.ACME.COM и WWW.ABC.COM существуют на одном и том же самом компьютере. Пользователи могут иметь доступ к любому Web участку на этой машине.

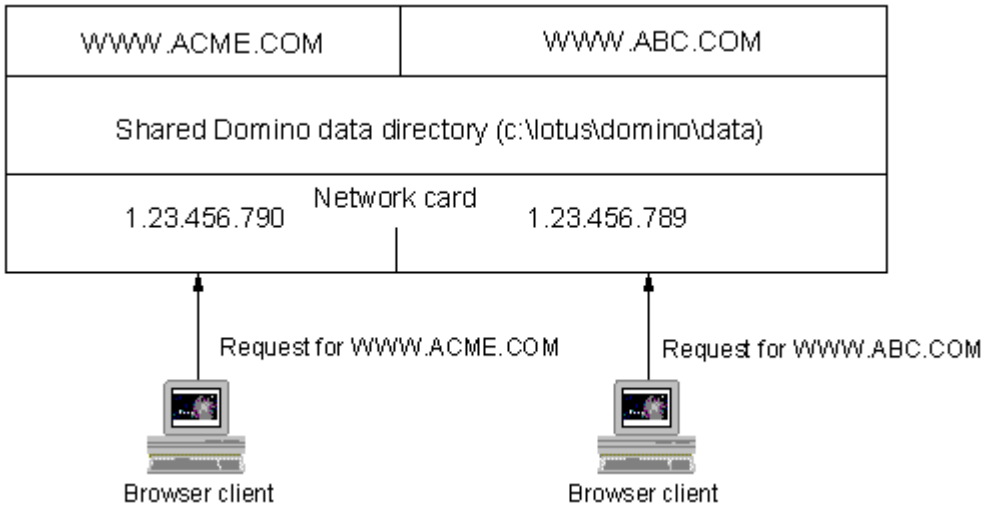


Рис. 48 Пример использования нескольких Web серверов на одном компьютере.

Поддержка нескольких Web серверов на одном сервере.

Для поддержки нескольких хостов Web на отдельном сервере, Вы должны закончить эти процедуры:

*767 Установить Web сервер.

*768 Установить политику безопасности для Web сервера.

2.12.5.1 Настройка поддержки нескольких Web серверов на одном сервере.

Чтобы установить новый сервер, с поддержкой нескольких Web серверов, создайте документ Virtual Server, в Domino Directory. Назначения, которые Вы определяете для Virtual Server документа, появляются в виде ответного документа к текущему Server документу. Чтобы показать документы Virtual Server, откройте представление Web – Конфигурации Web, из клиента Domino Administrator.

*769 Создайте каждый виртуальный сервер с собственным отдельным, постоянным IP адресом или с именем сетевой карты, к которому привязан IP адрес.

*770 Из клиента Domino Administrator, выбирайте закладку Настройка – Сервер – Все документы на сервере, выбирайте Server документ для сервера, на котором Вы хотите создать виртуальный сервер.

*771 Выбирайте кнопку Web и выбирайте Create Virtual Server.

*772 Выбирайте – Virtual Server.

*773 Выбирайте закладку - Basics заполните поля:

Поле	**Значение**
IP address	IP адрес для виртуального сервера.
Hostname	Имя хоста виртуального сервера. (Если нужно).
Default home page	HTML файл, который будет показан, когда пользователей соединяется с виртуальным сервером. Эта установка необязательна и используется только, если поле Home URL не заполнено.

*774 Выбирайте закладку Mapping, заполняйте поля и сохраните документ:

Поле	**Значение**
Home URL	Home URL - используется, когда пользователь получает доступ на виртуальный сервер. Команда URL может открыть базу данных или список баз данных на сервере. Home URL имеет приоритет над полем Default Home page. Команда /?Open показывает базы данных для всего виртуального сервера, так как Domino делит каталог данных со всем виртуальными серверами.

HTML directory, Icon directory, Icon URL path, CGI directory, CGI URL path	Каталог для HTML файлов, CGI программ и файлов иконок. Все виртуальные сервера используют общий каталог, или Вы можете определить отдельные каталоги для каждого сервера.

*775 Введите команду на консоли сервера, для вступления в силу Ваших установок:

```
tell http restart
```

Примечание. Вы можете настраивать сообщения, которые пользователи получат при обращении к Web участку на виртуальном сервере.

2.12.5.2 Настройка безопасности для виртуальных Web серверов.

Вы можете установить SSL сервер и использовать идентификацию клиентов по имени и паролю, или разрешить анонимный доступ для интернет клиентов, для доступа их на виртуальные сервера. Чтобы установить SSL, Вы должны создать Key Ring файл для каждого виртуального сервера на компьютере.

Вы должны быть знакомы с принципом SSL идентификации по имени и паролю, а также с использованием анонимного доступа, перед завершением этих шагов.

*776 Прежде, чем Вы установить опции безопасности для виртуальных серверов:

- Удостоверитесь, что Вы установили виртуальный сервер.
- Если Вы хотите установить SSL, установите SSL сервер. Запросите сервер Key Ring файл на каждый виртуальный сервер.

*777 Из клиента Domino Administrator, выбирайте закладку Настройка, выберите Web - Конфигурации Web, откройте документ Virtual Server.

*778 Выбирайте закладку Security, заполните поля, затем сохраните документ:

Поле	**Значение**
SSL key file	Имя файла Key Ring для виртуального сервера
Accept expired SSL certificates	Выбирайте одно: *779 Yes - позволять виртуальный сервер принимать просроченные сертификаты от пользователей. *780 No - не принимать просроченные сертификаты.
SSL ciphers	Выберите один или большее количество доступных шифров. Шифр используется, чтобы создавать шифрованные сессии. Ключ используется, чтобы шифровать передаваемую информацию с использованием – SSL.
Enable SSL V2	Разрешить пользователям присоединятся с использованием SSL версии 2.0.

Redirect TCP to SSL	Выбирайте одно: *781 Yes - требовать от клиентов и серверов, для доступа к виртуальным серверам использовать - SSL протокол. *782 No - разрешить клиентам и серверам, для доступа к виртуальным серверам - SSL или TCP/IP.
Name & password (TCP/IP)	Выбирайте одно: *783 Yes - запрашивать имя пользователя и пароль для интернета для доступа к базам виртуальных серверов. *784 No - не запрашивать имя и пароль.
Anonymous (TCP/IP)	Выбирайте одно: *785 Yes - разрешается анонимный доступ *786 No - запрещается анонимный доступ. Если разрешен анонимный доступ к базе данных, то сервер предоставляет пользователю анонимный доступ к базе данных. Если анонимный доступ не позволяется для базы данных, сервер запросит пользователя его имя и пароль.
Client certificate (SSL)	Выбирайте одно: *787 Yes - запросить сертификат пользователя при доступе к базам данных на виртуальном сервере. *788 No - не запрашивать сертификат клиента.
Name & password (SSL)	Выбирайте одно: *789 Yes - запросить имя и пароль клиента при доступе к базам на виртуальном сервере. *790 No – не запрашивать имя и пароль.
Anonymous (SSL)	Выбирайте одно: *791 Yes - разрешается анонимный доступ *792 No - запрещается анонимный доступ. Если разрешен анонимный доступ к базе данных, то сервер предоставляет пользователю анонимный доступ к базе данных. Если анонимный доступ не позволяется для базы данных, сервер запросит пользователя его имя и пароль.

*793 Введите команду на консоли сервера для перегрузки задачи:

```
tell http restart
```

2.12.6 Использование псевдонима для Web сервера.

Присвоение нескольких имен в DNS, назначает одному IP адресу нескольких Web имен. Это позволяет пользователям вводить различные URLs, для доступа к Web серверу. Например, Если Вы хотите, чтобы пользователи вводили www.acme.com или acme.com , для доступа к Web серверу Acme. Ввод псевдонимов также полезен, если Вы хотите изменить имя DNS для Web сервера - например, если название компании изменяется, но Вы не хотите нарушить связи с предыдущим именем DNS.

Псевдоним также известен как виртуальный хост. Для назначения псевдонима Web сервера:

*794 Установите Web сервер.

*795 Регистрируйте имя псевдонима на DNS сервере ISP или для Вашей внутренней сети.

*796 Из клиента Domino Administrator, выбирайте закладку Настройка – Сервер – Все документы на сервере, выбирайте Server документ для сервера, на котором Вы хотите создать виртуальный сервер.

*797 Выбирайте кнопку Web - Create Virtual Server.

*798 Выбирайте – Virtual Host.

*799 Выбирайте закладку – Basics, заполните поля:

Поле	**Значение**
Hostname	Введите имя псевдонима, для использования, для Вашего сервера
Comment	Комментарии
Default home page	HTML файл, который увидят пользователи по умолчанию при посещении сервера (не обязательно).

*800 Выбирайте закладку Mapping, заполняйте поля и сохраните документ:

Поле	**Значение**
Home URL	Home URL - используется, когда пользователь получает доступ на виртуальный сервер. Команда URL может открыть базу данных или список баз данных на сервере. Home URL имеет приоритет над полем Default Home page. Команда /?Open показывает базы данных для всего виртуального сервера, так как Domino делит каталог данных со всем виртуальными серверами.
HTML directory, Icon directory, Icon URL path, CGI directory, CGI URL path	Каталог для HTML файлов, CGI программ и файлов иконок. Все виртуальные сервера используют общий каталог, или Вы можете определить отдельные каталоги для каждого сервера.

*801 Введите команду на консоли сервера, для вступления в силу Ваших установок:

```
tell http restart
```

2.12.6.1 Настройка безопасности для псевдонимов Web сервера.

Псевдоним для Web сервера может иметь отдельные настройки для опознания пользователей. Например, Domino может требовать SSL связи, когда осуществляется доступ пользователя на www.acme.com и требовать - SSL вместе с TCP/IP, когда пользователи пытаются получить доступ к acme.com. Вы настраиваете безопасность для имени хоста DNS, Web сервера на закладке Ports – Internet Ports, в Security документе. Вы настраиваете безопасность для псевдонима в документе – Virtual Host.

*802 Прежде, чем Вы настроите безопасность,

- Удостоверитесь, что Вы назначили псевдоним для Web сервера.
- Если Вы хотите использовать SSL, установите SSL сервер, если Вы не сделали еще этого.

*803 Из клиента Domino Administrator, выбирайте закладку Настройки, выберите Web - Конфигурации Web и откройте документ - Virtual Host.

*804 Выбирайте закладку Security, заполните поля, затем сохраните документ:

Поле	**Значение**
Redirect TCP to SSL	Выбирайте одно: *805 Yes - вынуждать клиентов и сервера, для доступа к серверу, использовать SSL протокол. *806 No - разрешать использовать или SSL, или TCP/IP.
Name & password (TCP/IP)	Выбирайте одно: *807 Yes - запрашивать имя пользователя и интернет пароль для доступа к базам виртуального сервера. *808 No - не запрашивать имя и пароль.
Anonymous (TCP/IP)	Выбирайте одно: *809 Yes - разрешается анонимный доступ *810 No - запрещается анонимный доступ. Если разрешен анонимный доступ к базе данных, то сервер предоставляет пользователю анонимный доступ к базе данных. Если анонимный доступ не позволяется для базы данных, сервер запросит пользователя его имя и пароль.
Client certificate (SSL)	Выбирайте одно: *811 Yes - запросить сертификат пользователя при доступе к базе данных на виртуальном сервере. *812 No - не запрашивать сертификат клиента.

Name & password (SSL)	Выбирайте одно: *813 Yes - запросить имя и пароль клиента при доступе к базе данных на виртуальном сервере. *814 No - не запрашивать имя и пароль.
Anonymous (SSL)	Выбирайте одно: *815 Yes - разрешается анонимный доступ *816 No - запрещается анонимный доступ. Если разрешен анонимный доступ к базе данных, то сервер предоставляет пользователю анонимный доступ к базе данных. Если анонимный доступ не позволяется для базы данных, сервер запросит пользователя его имя и пароль.

*817 Введите команду на консоли сервера для перегрузки задачи:

```
tell http restart
```

2.12.7 Поддержка Java аппретов.

Для использование Java классов, Notes разработчики могут создавать апплеты которые исполняются задачей Domino, типа открытия сессии, получение информации из списка контроля управления доступа базы данных. Domino сервер может использовать апплеты и когда клиент запрашивает их и загружать апплеты в браузер.

Чтобы использовать Java апплеты, созданные на Java, Вы должны разрешить задачу DIIOP на сервере. Эта задача позволяет Domino и браузеру клиента использовать Domino серверную программу (ORB). Domino ORB обрабатывает апплет, запрашивает и передает информацию в браузер клиента. Вы должны позволить и задачу DIIOP и протокол IIOP на сервере прежде, чем пользователи могут получить доступ Domino ORB, чтобы запустить Java апплеты.

Проектировщики должны создать апплеты с Java классами Notes, кроме того, они должны определить, что апплеты могут использовать Domino ORB, чтобы связаться с браузерами клиентов. Проектировщики определяют эти установки, когда они добавляют апплеты к документам или форме.

Настройка Domino для использования ORB.

*818 Из клиента Domino Administrator, выбирайте закладку Настройка, выберите сервер и затем откройте Server документ.

*819 Выбирайте закладку Ports – Internet Ports – IIOP Server, заполните поля:

Поле	**Значение**
TCP/IP port number	Имя порта для задачи DIIOP listens. Не изменяйте это значение по умолчанию - 63148.

TCP/IP port status	Выбирайте одно: *820 Enabled (по умолчанию) - разрешить порт. *821 Disabled - запретить порт.

*822 Выбирайте закладку Internet Protocols – IIOP и заполните поле:

Поле	**Значение**
Number of threads	Кол-во нитей, которое Вы позволяете DIIOP задаче на сервере. По умолчанию - 10.

*823 Выбирайте закладку Security, заполните поля в секции IIOP Restrictions и сохраните документ:

Поле	**Значение**
Run restricted Java/Javascript	Имени или списку имен введенных в это поле, разрешается запуск программ, созданных с использованием всех возможностей Java и Javascript. Если апплет или приложение регистрируются анонимно, введите слово Anonymous в это поле.
Run unrestricted Java/Javascript	Именам или списку имен введенных в это поле, разрешается запуск программ, созданных с использованием ограниченных возможностей Java и Javascript. Если апплет или приложение регистрируются анонимно, введите слово Anonymous в это поле.

*824 Если необходимо, редактируйте переменную ServerTasks в NOTES.INI, чтобы включить в нее задачу DIIOP.

*825 Установите SSL сервер. Имя и пароля, анонимный доступ к IIOP порту для приложений или апплетам.

*826 Установите доступ к серверу для приложений или апплетов. Если апплет или приложение нуждаются в имени и пароле, введите имя для апплета или приложения. Иначе, используйте имя “Anonymous” при доступе к серверу.

*827 Перезапустите сервер.

2.12.8 Управление Java сервелетами на Web сервере.

Сервелет - Java программа, которая запускается на Web сервере в ответ на запрос браузера. Сервелеты для Domino должен быть - Java Servlet API Specification, фирмы Sun Microsystems Inc.

*828 Из клиента Domino Administrator, выбирайте закладку Настройки – Сервер, затем откройте Server документ.

*829 Выбирайте закладку Internet Protocols – Domino Web Engine, заполните эти поля, затем сохраните документ:

Поле	**Значение**
Java servlet support	Выбирайте одно: *830 None - (по умолчанию) не запускать Java Virtual Machine (JVM), или Servlet Manager, когда запускается задача HTTP. *831 Domino Servlet Manager - загрузить JVM и Servlet manager, поставляемый с Domino. *832 Third-Party Servlet Support - для запуска JVM, не Domino Servlet Manager. Вы можете использовать Servlet Manager, другого производителя, например IBM WebSphere.
Servlet URL path	URL путь к Domino сервелетам. По умолчанию - /servlet.
Class path	Один или несколько путей, где Servlet Manager и JVM будет искать сервелеты и Dependent Classes. Стандартные Java Libraries инсталлируются для Domino автоматически и заносятся в путь поиска. Здесь можно определить дополнительные пути поиска. Вы указываете каталоги, содержащие файлы – *.JAR и *.ZIP. Ваш путь может начинаться не обязательно с каталога данных Domino. Пример: c:\lotus\domino\data\domino\servlet c:\apps\myservlets c:\javamail\mail.jar domino\servlet\sql.zip По умолчанию - domino\servlet.
Servlet file extensions	Список файлов содержащих URL с окончаниями, которые указывают Domino, что URL предназначен для servlet. Вы должны мапировать (map) каждое расширение файла, через свойства сервелет файла. По умолчание нет, не одного окончания.

Session state tracking	Выбирайте одно: *833 Enabled - (по умолчанию) Domino Servlet Manager проверяет периодически активность пользователя для всех – HttpSession. Сессии, которые являются неактивными в течение периода времени, указанного в поле неактивных сессий, автоматически будут закрыты. Servlet Manager вызывает метод HttpSession.invalidate(), чтобы сообщить сервелету, что сессия будет закончена. *834 Disabled - не проверять деятельность пользователя. Domino использует эту установку и назначения ниже только, если сервелет использует Java Servlet API HttpSession интерфейс.
Idle session timeout	Время ожидания в минутах, после чего сессия будет разорвана. По умолчанию 30 минут.
Maximum active sessions	Максимальное число активных сессий. По умолчанию 1000. Если лимит будет превышен, придется ждать освобождения сессий.
Session persistence	Выбирайте одно: *835 Enabled - чтобы сохранять данные сессии в файле на диске, с названием sessdata.ser в каталоге данных Domino, когда HTTP задача завершается. Domino перезаписывает данные сессии, когда HTTP задача повторно начинается. *836 Disabled - (по умолчанию) отказываться от всех сессий, когда HTTP задача останавливается.

*837 Определение, кто имеет доступ к сервелет файлам.

2.12.9 Увеличение производительности Web сервера.

После того, как Вы установили Domino сервер и удостоверитесь, что он работает должным образом, проверьте работу сервера и время ответа сервера. Чтобы улучшать производительность сервера и время его ответа, сделаете любое из следующего действий:

*838 Измените настройки Кеш памяти

*839 Измените значение Time-Out

*840 Изменение номера нитей сервера

*841 Установка Domino Web сервера в кластер

*842 Оптимизация загрузки файлов для Web клиентов

*843 Определите метод, используемый для связи с внешними базами используемый для переадресации URL команд.

*844 Определите количество данных пользователей, позволяемых послать серверу с использованием команды HTTP POST.

2.12.9.1 Управление Кеш памятью Web сервера.

Чтобы оптимизировать время ответа, Domino использует память Кеш, также называемый Кеш команд. Этот отдел памяти хранить информацию о HTTP командах, базах данных и пользователей. Память Кеш хранит эту информацию, так что Domino сервер может получить к ней доступ очень быстро.

Domino кэширует страницы, которые содержат формулы @function также как страницы, которые не содержат формулы. Domino просматривают страницы для формул @function и затем оценивает изменение страниц, основанные на @function, используемые на странице. Например, Domino не кэширует страницы с формулой @New, но кэширует страницы с @Created формулами.

Чтобы контролировать эффективность Кеш памяти, смотрите статистику Кеш на Domino сервере.

Опции памяти Кеш расположены на закладке Protocols – Domino Web Engine, Server документа.

Поля	**Значение**
Maximum cached commands	Число команд HTTP сервера для кэширования анонимных пользователей. По умолчанию - 128. Domino должен конвертировать некоторые HTTP команды сервера типа OpenDatabase и OpenView в HTML прежде, чем сервер может обработать команды. Этот процесс требует некоторого времени. Это поле определяет, сколько команд Вы хотите хранить в памяти, когда следующий раз пользователь запускает команду на сервере, она немедленно будет доступна.
Maximum cached designs	Число элементов дизайна базы данных, для пользователей. По умолчанию - 128. Когда пользователь открывает базу данных, каждое имя модуля дизайна хранится в памяти. Используйте это поле, чтобы определить, сколько элементов, Вы хотите хранить в памяти. Когда пользователь запросит этот элемент, он появится немедленно.

Maximum cached users	Число пользователей Кеш. По умолчанию - 64. После того как пользователь успешно соединился с сервером, Domino хранит в памяти имя пользователя, пароль и список групп, к которым пользователь принадлежит. Используйте это поле, чтобы увеличить число кэшированных пользователей.
Cached user expiration interval	Интервал времени в секундах, в течение которых Domino регулярно удаляет имена пользователя, пароли, членство в группах из Кеша. По умолчанию - 120. Вы должны удалить имена пользователя, пароли и членство в группах из Кеша периодически, чтобы вынудить Domino искать пользователя в Directory, когда он получает доступ на сервер.

2.12.9.2 Настройка сетевого Time-Out для Web сервера.

Открытые, бездействующие сессии, могут мешать пользователям вызывать сервер. Определите сроки для действий между Domino Web сервером и клиентами или CGI программами, так чтобы связи не остаются открытыми, если не имеется никакой деятельности в сети между ними.

Настройки опций Time-Out определяются на закладке Internet Protocols – HTTP, Server документа.

Поле	**Значение**
Input timeout	Время в минутах, в течении которых клиент должен послать запрос после соединения с сервером. По умолчанию - 2. Сервер использует это поле, если клиент связанный с сервером не посылает команду Keep alive headers, на сервер в пределах количества указанного времени.
Output timeout	Максимальное время в минутах, в течении которых сервер должен послать ответ клиенту. По умолчанию - 20. Это поле применяется к локальным файлам и запросам. Установка не применяется к запросам, которые начинают CGI программу. Если сервер не посылает полный запрос в пределах этого времени, сервер закрывает связь.

CGI timeout	Максимально время в минутах определенное на выполнение CGI программ. По умолчанию - 5. Если время, указанное в этом поле завершается, сервер посылает сообщение CGI программы. По окончании этого времени сервер завершает программу.
Idle thread timeout	Это поле не имеет никакого влияния и остается в Server документе для совместимости.

2.12.9.3 Установка числа нитей, используемых Domino Web сервером.

Вы можете определить число нитей, которые Web сервер может обрабатывать или определять число запросов. Пользователь может делать единственный запрос на сервер. Вообще, число нитей указанный указывает на число пользователей, которые могут одновременно получить доступ на сервер.

Если число активных нитей достигнет установленного предела, Domino сервер не будет обрабатывать новые запросы, пока старые запросы не будут закончены. Чем большее мощнее Ваш компьютер, тем выше число нитей, Вы должны определить. Если Ваш компьютер тратит слишком много времени на задачах, типа свопирования памяти, определите более низкое число нитей.

Для определения количество нитей выбирайте закладку Internet Protocols – HTTP из Server документа.

Поле	**Значение**
Maximum requests over a single connection	Число запросов браузера, которые можно делать на сервере в то же самое время. По умолчанию - 1. Эта установка действует на браузеры, совместимые с HTTP 1.1 или выше, если браузер способен посылать несколько запросов на сервере без ожидания ответа от предыдущего запроса.
Number active threads	Число нитей активных в одно и тоже время на сервере По умолчанию - 40.
Minimum active threads	Поле не имеет никакого влияния и остается в Server документе для обратной совместимости.

2.12.9.4 Оптимизация загрузки файлов Web клиентами.

Клиенты Web могут скачать файл, который присоединен к странице, или находится в каталоге сервера, который является, связан с использованием URL. Если клиент использует программное обеспечение, которое поддерживает Byte-Range (доступный в HTTP 1.1) в

течение скачивания, файла. Если происходит разрыв, клиент может возобновлять копирования с той точки, где был разрыв. Без использования опции Byte-Range, пользователи должны будут повторить прерванное копирования с начала. Использование этой функции делает копирование файлов более эффективной.

Domino совместим с клиентами, которые твердо придерживаются HTTP 1.1 спецификации. Клиенты могут использовать эту функцию разными путями. Например, использовать браузер с различными дополнительными программами, поддерживающими докачку, использовать апплеты, или специальные программы. В настоящее время, только несколько коммерческих программ доступно и поддерживают Byte-Range. Одна из них GetRight 4.2 от фирмы Headlight. Domino автоматически использует функцию Byte-Range, если Web клиент может использовать эту особенность. Никакая конфигурация не необходима.

Присоединенные файлы должны быть несжатые, для клиентов которые будут использовать функцию Byte-Range, для доступа к этим файлам. Когда Вы присоединяете файл, Вы должны отменить опцию сжатия. Чтобы проверить, что существующее приложение не сжато, выбирайте Файл – Свойства документа, выбирайте поле $FILE и проверьте пункт - Тип сжатия: NONE.

Пример: Загрузка файла из файловой системы сервера.

Файл INSTALL.EXE находится в каталоге, из которого позволяется загрузка с использованием URL mapping. Клиент GetRight 4.2 может использовать следующий URL, чтобы разгрузить файл:

```
http://hostname/install.exe
```

Где hostname - имя хоста сервера.

Если разгрузка прервана, клиент может начинать разгрузку с точки, с которой сеанс был прерван.

Пример: Загрузка присоединенного файла.

Пользователь может разгружать *.PDF файл

Для доступа пользователя к файлу PROJECT.PDF, используйте следующий URL:

```
http://hostname/dbname/viewUNID/docUNID/$FILE/project.pdf
```

Где hostname - хоста сервера, dbname - название базы данных, которая хранит приложение, viewUNID - UNID представление для приложений, и docUNID - UNID документа, к которому присоединен файл.

2.12.10 Поиск ссылок для команд Redirect URL.

Вы используете команды Redirect URL, чтобы создавать связи, с документами, представлениями и связями с базами данных на Web странице. Эти связи могут направить пользователей к базам данных на том же самом сервере, или на другом сервере. Чтобы определить время сервера, для решений связей на других серверах, редактируйте опцию Redirect to resolve external links, на закладке Internet Protocols – Domino Web Engine, в Server документе. Разрешите эту опцию для любого сервера, который осуществляет поиском в домене и на серверах, для которых Вы хотите разрешить связи с другими серверами.

Поле	Значение

Redirect to resolve external links	Выбирайте одно: *845 Disabled - (по умолчанию) запретить серверу принятие команд Redirect URL и запретить серверу выполнение команд Redirect URL в результатах поиска по домену. *846 By Server - просматривает имя сервера, указанное в URL, в Domino Directory на Web сервере. Сервер ищет для имени сервера – в полях Host names, на закладке Internet Protocols – HTTP или в полях Fully qualified Internet host name, на закладке Basics. *847 By Database - чтобы найти сервер в Domino Directory на доступном сервере. Domino просматривает базы данных в каталоге домена, если доступно, или в локальном каталоге сервера. Удостоверитесь, что Catalog Domain содержит, свежую информацию относительно местоположения баз данных. Выбирая этот выбор, решение связи занимает большое количество времени, чем опция - By Server.

2.12.11 Ограничение данных пользователя, которые посылаются на сервер.

HTTP команда POST позволяет пользователям посылать данные на Domino сервер. Вы можете определить, количество пользовательских данных, позволяемых послать на сервер, сжимать ли файлы, посылаемые на сервер. Используйте это выбор, чтобы запретить пользователям, посылать большой объем данных на сервер.

Опция выбора для команды POST расположена на закладке Protocols – Domino Web Engine, в документе Server документ.

Поле	**Значение**
Maximum POST data	Количество данных в килобайтах, которое пользователю позволяется послать на сервер. По умолчанию – 0 (не ограниченно). Если пользователь пробуют послать больше чем максимум, позволенный данных, Domino возвращает сообщение в браузер.
File compression on upload	Определяет, сжимает ли Domino файлы перед добавлением их в базу данных. Сжатие файлов сохраняет место на диске сервера. По умолчанию – Disabled. Если клиенты используют браузер, который поддерживает опцию Byte-Range, выбирайте опцию – Disabled. В противном случае Вы не сможете разгружать сжатые файлы, используя функцию Domino Byte-Range.

2.12.12 Отображение информации Web сервером.

Domino дает Вам несколько различных настроек, для отображения информации на Web. Эти опции просмотра затрагивают все базы данных на сервере. Чтобы изменять просмотр индивидуальной базы данных, Вы должны изменить модули дизайна этой базы данных.

*848 Выбор домашней страницы Web сервера по умолчанию

*849 Выбор формата для хранения изображений - *.GIF или *.JPEG

*850 Выбор по умолчанию линий в представлении, для просмотра

*851 Настройка сообщений об ошибках для Web сервера

*852 Настройка кодовой страницы для отображения HTML текста

*853 Настройка по умолчанию, максимального числа документов, возвращаемых сервером как результат поиска.

2.12.12.1 Выбор домашней страницы по умолчанию для Web сервера.

Domino поддерживает два метода показа страницы, когда пользователь первый раз получает доступом к Web сервер. Вы можете определить HTML файл, чтобы показать его, или Вы можете вводить команду URL, чтобы показать список баз данных или содержание баз данных.

Domino придерживайтесь этих правил, при показе домашней страницы для Web сервера.

Поле Default home page	**Поле Home URL**	**Результат**
Содержит данные	Содержит данные	Domino показывает ссылку из поля Home URL.
Содержит данные	Пусто	Domino показывает ссылку из поля Default home page.
Пусто	Содержит данные	Domino показывает ссылку из поля Home URL.
Пусто	Пусто	Domino сообщает об ошибке
Содержит ссылку на файл, который не существует	Пусто	Domino сообщает об ошибке

Определение домашней страницы по умолчанию.

Опция - Default home page, находится на закладке Internet Protocols – HTTP, Server документа.

Поле	**Значение**
Default home page	Имя файла HTML , по умолчанию HTML каталог или подкаталог HTML.

Home URL	Команда URL. По умолчанию, Domino открывает файл HOMEPAGE.NSF Определение URL в этом поле, который начинается со знака / (слеш). Если Вы определяете URL, который открывает Domino базу данных, удостоверитесь, что пользователи имеют доступ к этой базе данных. Это поле имеет приоритет над полем Default home page.

Примечание. Выбранный URL в полях Home URL или Default home page стартует, если пользователь запрашивает UPL Вашего сервера http://someotherhost.domain.com/. Браузер исполняет запрос HTTP GET и показывает URL указанный в этом поле.

2.12.12.2 Пример использования домашней страницы по умолчанию.

Поле Home URL	**Результат**
dominodisc.nsf/?OpenDatabase	Показывает соответствующий документ или представление в базе данных DOMINODISC.NSF и показывает полный URL, включая /?OpenDatabase командует в URL окне браузера.
/dominodisc.nsf /dominodisc.nsf/By+Author /dominodisc.nsf/$About	Показывает соответствующий документ или представление в базе данных DOMINODISC.NSF, но не показывает команду URL в URL окне браузера.
http://myhost.domain.com/home/dominodisc.nsf	Переадресовывает браузер пользователя на сервер myhost.domain.com и показывает соответствующую страницу из базы данных DOMINODISC.NSF.

2.12.12.3 Выбор формата изображений *.GIF или *.JPEG

Вы можете управлять форматом и методом отображений, которые будут появляться в документах. Domino Web сервер поддерживает *.GIF и *.JPEG формат. Эта установка не имеет никакого влияния на упомянутые изображения, с использованием Passthru HTML.

Выбор преобразования изображений находится на закладке Protocols – Domino Web Engine, Server документа.

Когда Вы позволяете опцию Progressive или Interlaced предоставление изображений, пользователю кажется, что изображение загружается быстро и потом увеличивается резкость.

Опции преобразования для изображений формата *.GIF

Поле	**Значение**

Image conversion format	GIF - изображения в документах конвертируются в формат – *.GIF По умолчанию - GIF.
Interlaced rendering	Выбирайте одно: *854 Enabled - (по умолчанию) разрешить режим. *855 Disabled - запретить режим.

Опции преобразования для изображений формата *.JPEG

Поле	**Значение**
Image conversion format	JPEG - изображения в документах конвертируются в формат - *.JPEG По умолчанию - GIF.
Progressive rendering	Выбирайте одно: *856 Enabled - (по умолчанию) разрешить режим. *857 Disabled - запретить режим.
JPEG image quality	Можно указать уровень проработки деталей изображения, от 5 до 100 По умолчанию - 75.

2.12.12.4 Выбор числа строк для отображения представлений на сервере.

Вы можете определить максимальное число строк, чтобы отображать представления базы данных. Эта установка действует на все базы данных на сервере.

По умолчанию максимальное число строк представления можно установить на закладке Internet Protocols – Domino Web Engine, Server документа.

Поле	**Значение**
Default lines per view page	Число от 1 до числа, указанного в поле Maximum lines per view page. Это поле определяет, сколько строк будет показано, когда пользователи не указывают число строк в URL. Число строк, зависит от Вашего желания. Отображение большего количества строк в виде, делает более легким поиск в большом представлении. Представление меньшего количества строк в виде делает вид, более легким для чтения. По умолчанию - 30.
Maximum lines per view page	Число, которым ограничено программное обеспечение браузера. Это поле определяет максимальное число строк в виде, когда пользователь определяет индекс строк в URL. Введите 0, если Вы не хотите ограничивать число строк в виде. По умолчанию - 1000.

2.12.13 Настройка сообщений Web сервера.

Web сервер отображает страницу с сообщением об ошибке, когда пользователь сталкивается с ошибкой или когда на сервере документ не существует. Чтобы создать страницу сообщения об ошибке, Вы создаете форму в базе данных для каждого типа сообщений. Затем создаете документ Mapping в базе данных Конфигурации (DOMCFG.NSF), чтобы определить, как формируются сообщения. Любая база данных может хранить эти страницы сообщений об ошибках.

Вы можете настроить Ваш сервер, чтобы пользователь получал эти сообщения когда:

*858 Пользователь не опознан сервером.

*859 Пользователь не может получить доступ к одной из баз данных, который является частью Web сервера.

*860 Пользователь запускает команду удаления страницы, а сервер успешно стирает ее.

Кроме того, Вы можете определить общее сообщение, которое появляется для всех других типов ошибок или ответов, которые происходят на Web сервере.

Если Вы используете установку опознания пользователей, с использованием имени и пароля, Domino показывает HTML страницу, которую Вы определяете как регистрационную, для регистрации имени пользователя и ввода пароля.

В этом примере, форма для сообщения существует в базе данных ANYDB.NSF и возвращается пользователю, когда пользователь сталкивается с ошибкой сервера.

Пользователи должны иметь доступ читателя к базе Domino Конфигурации (DOMCFG.NSF) и любой из доступа к базе (ANYDB.NSF).

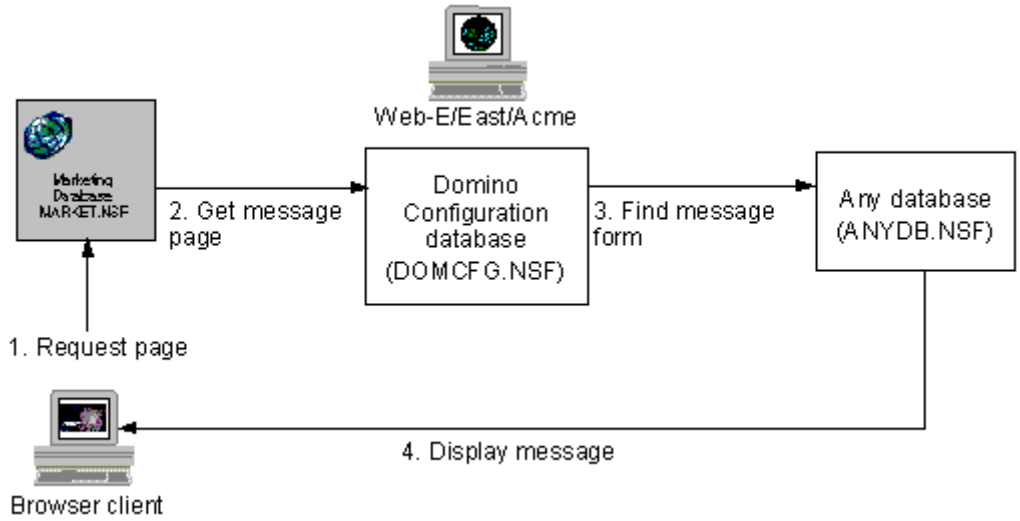


Рис. 49 Пример отображает процесс получения Web пользователем определенных Вами сообщений.

2.12.14 Создание базы данных Domino Configuration.

Вы используете базу данных Domino Configuration, чтобы настроить сообщения, которые будут возвращаться Web пользователям. Вы также используете эту базу данных при настройке HTML страниц, для регистрации Web пользователей на сервере. Используйте шаблон Domino Configuration Web Server (DOMCFG.NTF) для создания базы данных сообщений Domino. Добавьте запись для пользователя Anonymous в ACL базы и дайте ему доступ читателя.

2.12.15 Создание и настройка сообщений Web сервера.

*861 Удостоверится, что Вы уже создали базу данных Domino Configuration.

*862 После того как Вы определяете, какая база данных будет хранить настроенные сообщения, откройте базу данных и создайте форму, которая содержит сообщение для показа.

*863 Если Вы настраиваете, сообщение для виртуального сервера, в свойствах формы для формы, выбирайте - Available to Public Access users, на закладке безопасности.

*864 Сохраните форму.

*865 Повторите описанные шаги для каждой документа ответа, на каждую ошибку, для которого Вы хотите настроить страницу сообщения.

*866 В базе данных Domino Configuration, выбирайте – Create – Mapping Error Message.

*867 Если Вы настраиваете, сообщение для виртуального сервера, выбирайте – Virtual Server Settings и введите IP адрес сервера.

*868 (Необязательно) Введите любые комментарии.

*869 Для каждого типа ошибки или ответа, введите имя базы данных, которая содержит форму, которую Вы хотите показать в поле Target Database file name.

*870 Для каждого типа ошибки или ответа, введите имя формы, которую Вы хотите показать в поле Target Form name.

*871 Сохраните документы Error Message и Response Mapping.

*872 В ACL базы данных, которая содержит формы, введите доступ автора на сервере, который хранит базу данных.

2.12.15.1 Пример настройки сообщений Web сервера.

Следующий документ Error Message and Response Mapping использует формы, сохраненные в базе данных MESSAGES.NSF на текущем сервере. Имеются настроенные сообщения для регистрации Web пользователей, ответов на стирание документа и т.д. Domino показывает сообщение по умолчанию, сохраненные в базе данных Domino Configuration, для всех других сообщений которые может получить Web пользователь.

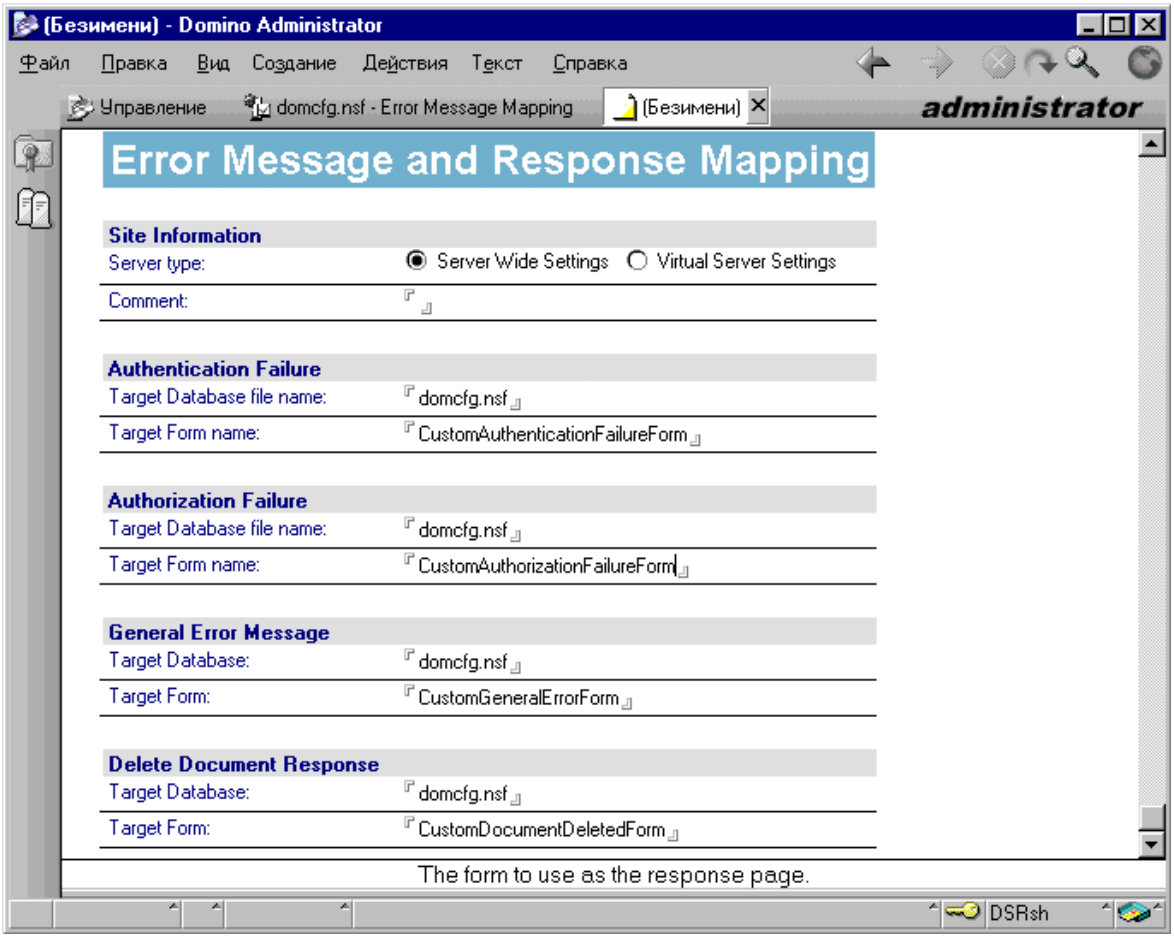


Рис. 50 Документ Error Message and Response Mapping.

2.12.16 Выбор набора интернациональных символов для затребованных страниц.

Domino использует набор символов по умолчанию. Набор символов устанавливает связь для генерации текста HTML для браузеров. Если Вы имеете пользователей, которые

должны видеть текст на не западных языках, вы должны сделать изменения в своих установках. Установка набора символов действует на все базы данных на сервере.

Установка набора интернациональных символов.

*873 Из клиента Domino Administrator, выбирайте закладку Настройка, выбирайте Сервер и затем откройте Server документ для Web сервера.

*874 Выбирайте закладку Internet Protocols – Domino Web Engine, заполняйте поля и сохраните документ:

Поля	**Значения**
Default character set group	Привилегированный набор символов, при создании или редактировании документов. По умолчанию – Western.
Convert resource strings to	Язык, используемый для сообщений HTML по умолчанию. Вы можете выбирать язык только для международных версий Domino сервера. По умолчанию – English.
Use UTF-8 for output	Выбирайте одно: *875 Yes – генерировать страницы с использованием UTF-8. *876 No - (по умолчанию) генерировать страницы с использованием Character Set Mapping, который Вы выбрали.
Use auto-detection if database has no language information	Выбирайте одно: *877 Yes – использовать автоматическое определение языка, для использования для базы данных, если никакой язык по умолчанию не выбран в свойствах базы данных. *878 No - (по умолчанию) использовать выбранный язык, использовать UTF-8. Если язык выбран для базы на закладке Design в свойствах базы данных, Domino использует этот язык для текста в базе.

Character set in header	Выбирайте одно: *879 Yes - (по умолчанию) добавлять строку Character, Content-Type HTTP, в заголовок HTML страницы. Если Вы выбрали - Yes, браузер находит строку и применяет эти установки для страницы. *880 No - не включать Characters в заголовок HTTP страницы HTML.
Meta character set	Выбирайте одно: *881 Yes - добавлять Character Set, в тег <META> на странице HTML. *882 No - (по умолчанию) не добавлять Character Set, в тег <META> на странице HTML.

*883 В полях, которые показывают имена групп наборов символов, выбирают один из доступных выборов символов, устанавливают – Mapping.

*884 Сохраните документ.

Набор символов для страниц Web сервера.

Набор символов по умолчанию. Доступный выбор символов устанавливают – Mapping. Если устанавливается группа символов, Вы должны выбрать какой набор символов использовать.

Группы наборов символов	**Значение набора символов**
Western Включает Windows и ANSI символы.	US-ASCII ISO-8859-1 (по умолчанию) ISO-8859-15 Windows-1252
Central European	ISO-8859-2 Windows 1250 (по умолчанию)
Japanese	SJIS (по умолчанию) JIS(ISO-2022-JP) EUC-JP
Traditional Chinese	Big5 (по умолчанию) EUC-TW
Simplified Chinese	GB

Korean	KSC5601(EUC)
Cyrillic	ISO-8859-5 Windows-1251 KOI8-R (по умолчанию)
Greek	ISO-8859-7 Windows-1253 (по умолчанию)
Turkish	ISO-8859-9 Windows-1254 (по умолчанию)
Thai	Windows-874
Baltic	Windows-1257
Arabic	Windows-1256 (по умолчанию) ISO-8859-6
Hebrew	ISO-8859-8 (по умолчанию) Windows-1255
Vietnamese	Windows-1258

2.12.17 Максимально число документов, возвращаемое поиском.

Вы можете определить максимальное число документов, показываемое в результате выполнения поиска по базе данных. Пользователи могут определить число документов для запроса поиска, чтобы использовать параметры SearchMax, с командами SearchView и SearchSite.

Измените этот выбор, чтобы удержать пользователей от перегрузки сервера результатами поиска.

Опции ограничения поиска можно настроить на закладке Protocols – Domino Web Engine, Server документа. Это установка действует на все базы данных на сервере.

Поле	**Значение**
Default search result limit	Число документов для показа, когда пользователи не определяют SearchMax параметр в URL. Введите 0, если Вы не хотите ограничить число показанных документов. По умолчанию - 250.

Maximum search result limit	Максимальное число документов, которое может быть показано пользователю с использованием SearchMax параметра в URL. Введите 0, если вы не хотите ограничивать число документов. По умолчанию - 1000.

2.12.18 Изменение запросов Web URLs, при изменении местоположения, каталогов и файлов Web сервера.

Иногда Вы должны переместить файлы и каталоги на Web сервере. Вы можете:

*885 Перенаправить запросы URLs и каталогов

*886 Изменить местоположение HTML, CGI и файлов иконок

2.12.18.1 Перенаправление запросов URL для каталогов.

Вы можете хранить файлы баз данных, HTML файлы, CGI сценарии и другие, связанные Web файлы в нескольких местах на жестком диске сервера. Вы можете перемещать их в новые каталоги без нарушения связей URL, действующих в Server документе.

Пример. Если Вы имеете Web приложение, с именем mysite.nsf, на сервере www.acme.com, но Вы хотите переместить это приложение на сервер www.abc.com, Вы можете переадресовывать всех пользователей на сервер www.abc.com, когда они получают доступ к приложению на www.acme.com

Переадресовывание URL показывает страницу с нового местоположения и показывает URL в окне местоположения для пользователя. Mapping URL или каталог показывает страницу в новом местоположении и скрывает URL от пользователя. Вы можете переадресовывать или URLs или каталоги для серверов единственного сайта и для виртуальных серверов на одном хосте на несколько серверов.

Чтобы переадресовывать URL или каталог, Вы создаете документ Mapping/Redirection, в Domino Directory. Domino показывает Mapping/Redirection документ, как ответный документ к Server документу на закладке представления Настройка – Web – Web Configuration Settingss.

*887 Из клиента Domino Administrator, выбирайте закладку Настройка, выберите сервер и откройте Server документ для сервера, на котором Вы хотите переадресовать URL или каталог.

*888 Выбирайте представление Все документы на сервере, нажмите – Web, выбирайте Create URL Mapping/Redirection.

*889 Щелкает на закладке Basics, заполняйте поля:

Поля	**Значения**

What do you want to setup	Выбирайте одно: *890 URL --> URL - карта перехода от одного URL к другому URL, так чтобы Вы могли создавать имена псевдонимов для длинных имен файлов, переименовывать каталоги, перемещать группы файлов, или хранит файлы на различных дисках сервера, без нарушения внешних связей или закладок пользователей. Domino не показывает URLs заднего плана пользователю. Вы не можете сделать этого со страницами, сохраненными в базе данных Domino. *891 URL --> Directory – каталоги URL в различные каталоги, так что Вы можете переименовывать каталоги, перемещать файлы, или хранит файлы на различных дисках. Domino не показывает URLs заднего плана пользователю. Вы не можете сделать этого со страницами, сохраненными в базе данных Domino. *892 Redirection --> URL – переход от URL к другому URL. Domino показывает переадресованный URL в браузере пользователя. Используйте этот выбор для переадресования URL, к определенному URL. Например, к странице сохраненной в базах данных Domino.

*893 Выбирайте закладку Site Information, заполните поля:

Поле	**Значение**
IP Address	Если Вы создаете Mapping for Virtual Server, определите уникальный адрес IP или имя хоста для сервера.

*894 Выбирайте закладку Mapping, заполните поля:

Поле	**Значение**
First URL path	Входящий URL путь, который Вы хотите отразить на другой каталог или URL.
Second URL path	Полный путь или имя каталога, на который Вы хотите отразить URL (новый URL). Для URL - > URL и URL - > Directory местоположения, к которому Вы должны перейти, на той же самой машине в каталог, указанный URL путь.

*895 Выбирайте закладку Access, заполните поля и сохраните документ:

Поле	**Значение**

Access	Если вы выбираете URL --> Directory, Определите тип доступа, который Вы хотите дать пользователям к каталогу. *896 Reader - позволяет браузеру читать файлы в каталоге. *897 Execute – позволяет браузеру выполнять файлы программ из этого каталога. Выбор читатель - доступ для любого каталога, который содержат файлы, типа HTML и изображений. Не установите доступ выполнения для этих каталогов. Выбор выполнить – доступ только для каталогов, которые содержат CGI сценарии и другие файлы, которые браузер может выполнять. Не устанавливайте доступ читателя для этих каталогов, пользователи не должны видеть то, что в этих каталогах содержится.

*898 Введите команду на консоли сервера и перегрузите сервер, для вступления изменений в действие:

```
tell http restart
```

2.12.18.1.1 Примеры для перенаправления URLs и каталогов

Перенаправление URL для каталога.

Эти примеры переадресовывают все запросы к файлам изображений по умолчанию хранящиеся в \domino\images каталоге. Если Вы имеете следующий HTML code в документе: [<body background=/images/icon.gif>] Domino ищет файлы *.Gif в каталоге c:\lotus\domino\data\domino\icons на сервере.

First URL path: /images

Second URL path: c:\lotus\domino\data\domino\icons

Access: Read

Этот пример для сценариев.

По умолчанию \domino\CGI каталог для одного виртуального сервера.

IP Адрес: 130.103.55.251

First URL path: /scripts

Second URL path: d:\lotus\domino\data\domino\cgi-bin

Access: Execute

Замена URL на другой URL.

Этот запрос примера для CGI программ в /cgi-bin URL.

First URL path: /scripts

Second URL path: /cgi-bin

Перенаправление URL.

Этот пример перемещает поступающий запрос новостей на самые актуальные сообщения страниц на Lotus Web.

First URL path: /news

Second URL path: http://www.lotus.com/home.nsf/tabs/topstories

2.12.18.2 Изменение места хранения файлов HTML, CGI, Icon.

Вы можете использовать Passthru HTML, чтобы ссылаться на индивидуальные HTML, CGI и файлы изображений. Domino ищет эти файлы в определенном каталоге диске.

Если Вы не хотите хранить эти файлы в каталогах по умолчанию, Вы должны изменить местоположения, указанные в Server документе для Web сервера, так чтобы Domino мог находить эти файлы.

Вы можете также изменять URL путь для изображений и CGI файлов. URL путь - то, где Domino ищет изображения или CGI программы, когда он сталкивается со ссылкой в коде HTML на один из этих пунктов.

Определение пути к изображениям и CGI URL полезно, если Вы изменяете, местоположение каталогов изображений или CGI программ и не хотите изменить HTML code, который ссылается на предыдущее место хранения этих файлов. Например, если Вы имеете каталог, названный \oldicons, и перемещаете содержание этого каталога в \icons подкаталог, Вы можете зайти в поле, где указано \oldicons - Icon URLs path и ввести значение domino\icons. Это назначения сообщает Domino искать файлы изображений в каталоге domino\icons всякий раз, когда он сталкивается со ссылкой на /oldicons в коде HTML.

Идентификация местоположения файлов HTML, CGI, Icon.

Вы можете определить местоположение HTML, CGI и файлов изображения для Domino Web сервера. Если Вы имеет несколько сайтов на одной машине, Virtual Server документ подменит эти назначения.

Когда Вы определяете каталоги для HTML, CGI, или файлов изображений, каталоги определяются - относительно Domino каталога данных, если Вы не определяете полный путь. Например, если Вы вводите в поле Icon URLs path значение domino\icons, Domino ищет файлы изображения в lotus\domino\data\domino\icons каталоге, если \lotus\domino\data - каталог данных сервера.

Вы определяете местоположение HTML, CGI и файлов изображения на закладке Internet Protocols – HTTP, Server документа. Эти назначения действует на все базы данных на сервере.

Поле	**Значение**
HTML directory	Каталог для файлов HTML. По умолчанию – domino\html.

Icon directory	Каталог для файлов изображений. По умолчанию - domino\icons.
Icon URL path	URL путь в каталог для иконок. По умолчанию - /icons.
CGI directory	Каталог для CGI программ. По умолчанию - domino\cgi-bin.
CGI URL path	URL путь для каталога CGI программ. По умолчанию - /cgi-bin.

2.13 Установка и настройка Domino для использования с Microsoft Internet Information Server.

Глава описывает, как установить и использовать Domino вместе с Microsoft IIS, чтобы обрабатывать HTTP запросы для баз данных Domino.

2.13.1 Domino и Microsoft IIS.

Domino позволяет Вам использовать Microsoft Internet Information Server (IIS), для обработки запросов HTTP для баз данных Domino и показывать их клиентам. IIS получает все URL, запрашивает и пропускает к Domino любые запросы. IIS обрабатывает любые другие запросы - например, HTML файлы и Activ Server Page (ASP).

Вы можете настроить эту необязательную конфигурацию Domino. Вы конфигурируете Domino сервер как ISAPI расширение для IIS. ISAPI - Internet Server Application Programming Interface, поддерживаемый IIS. Разработчики используют этот интерфейс, чтобы создать программы, называемые расширениями, которые расширяют функции IIS. Domino сервер устанавливает при инсталляции ISAPI расширение для Domino.

Domino сервер должен быть запущен, в то время когда Domino ISAPI расширение запускается. Domino сервер может использовать любые задачи, кроме родной HTTP задачи, которая будет конфликтовать с Domino ISAPI расширением. При этом Domino сервер позволяет клиентам Notes доступ на Domino сервер и позволяет Domino серверу управлять серверными задачами маршрутизации почты и репликациями.

Модель безопасности IIS и Domino работают вместе, когда пользователи обращаются к Domino приложениями. Это гарантирует высокий уровень безопасности Domino данных, сохраненных в Domino базах данных.

2.13.2 Настройка Domino для использования Microsoft IIS.

Чтобы настроить Domino для использования Microsoft IIS, Вы должны выполнить следующие процедуры:

*899 Удостоверьтесь, что Ваша система удовлетворяет базовым системным требованиям

*900 Сконфигурировать Domino для использования Microsoft IIS

*901 Настроить опции безопасности для Domino и Microsoft IIS

2.13.2.1 Базовые требования для Domino и Microsoft IIS.

Прежде, чем Вы установите Domino для Microsoft IIS, сделайте следующее:

*902 Установить Microsoft WindowsNT 4.0 с SP4.

*903 Установить Microsoft IIS4.

*904 Установите и настройте Domino сервер и удостоверитесь, что он работает правильно.

*905 Проверите следующее:

- NOTES.INI файл для сервера расположен в программном каталоге Domino, или в каталоге указанном в установке пути сервера.
- Если ID сервера не хранится в каталоге данных Domino, то NOTES.INI файл для сервера должен иметь полный путь к ID файлу сервера в параметре - ServerKeyFilename.
- ID файл сервера не должен использовать пароль. Вы не сможете вводить пароль, когда IIS запускает Domino ISAPI расширение.

*906 Удостоверитесь, Domino каталог и подкаталоги имеет, по крайней мере, доступ – Изменения файлов, для NT экаунтов пользователей, которые используют Domino для IIS. Типично, доступа к файлам по умолчанию достаточно. Однако если Вы должны изменить разрешения для файлов, имейте в виду, что пользователи Web, при обращении к серверу нуждаются в некоторых правах, чтобы делать изменения в базах данных и файлах на сервере.

*907 Вам надо понимать, как использовать Microsoft Management Console (MMC), которую Вы используете для конфигурирования IIS.

2.13.2.2 Конфигурирование Domino для Microsoft IIS.

После того, как Вы выполните базовые требования для Domino - Microsoft IIS, Вы должны сконфигурировать Domino для Microsoft IIS прежде, чем пользователи смогут использовать IIS для доступа к Domino приложениям. Чтобы настроить Domino для IIS, Вы должны закончить каждую процедуру, внесенную в список ниже:

Настройка ISAPI расширения.

Вы должны настроить Domino ISAPI расширение, чтобы использовать IIS для запросов на просмотр Domino приложений и определить файлы с расширением *.NSF. Вы используете Microsoft Management Console (MMC), чтобы настроить ISAPI расширение.

*908 Запустите MMC для – Web site.

*909 Выбирайте - IIS Web site и выбирайте – Setting.

*910 Выбирайте закладку Home Directory и выбирайте – Configurations.

*911 Выбирайте – Add.

*912 В поле Executable, введите полный путь, для файла ISAPI расширения. Файл находится в каталоге Domino и называется NIISEXTN.DLL . Например, если Вы установили Domino в каталог по умолчанию, то полный путь будет – c:\lotus\domino\niisextn.dll.

*913 В поле Extension введите значение – NSF

*914 В поле Methods Exclusions, введите HTTP методы, которые Domino для IIS не поддерживает: PUT, DELETE

*915 Выбирайте - Script Engine, запретите - Check that the File Exists.

*916 Выбирайте – OK.

Настройка фильтра IIS расширения.

Domino для IIS использует IIS фильтр расширения, чтобы гарантировать правильный доступ пользователей к Domino командам Domino (/?OpenServer).

*917 Запустите MMC и откройте – Web site.

*918 Выбирайте - IIS Web site, выбирайте – Setting.

*919 Выбирайте закладку - ISAPI Filters, выбирайте – Add.

*920 В поле Name Filters введите любой текст описания IIS фильтра, например – Domino.

*921 В поле Executable введите полный путь к файлу фильтра. Файл расположен в Domino каталоге и имеет имя NIISFILT.DLL. Например, если Вы установили Domino в каталог по умолчанию, полное имя пути – c:\lotus\domino\niisfilt.dll.

*922 Выбирайте – OK.

Укажите каталог для Domino Icons и Java applet.

Вы определяете местоположение приложений Domino изображений и файлов Java апплетов так, чтобы Domino для IIS показывал изображения и Java апплеты правильно.

*923 Запустите MMC и откройте - Web site.

*924 Щелкнуть правой кнопкой на IIS Web site, выбирайте New – Virtual Directory.

*925 В поле Virtual Directory Alias, введите – icon, выбирайте – Next.

*926 Введите полный путь к Domino каталогу для иконок. Например, если Вы установили Domino в каталог по умолчанию, ведите - c:\lotus\domino\data\domino\icons. Выбирайте – Next.

*927 Выбирайте – Finish. Вы не должны изменить назначения разрешений по умолчанию.

*928 Повторите шаги выше для определения каталогов, для Jawa апплетов. Введите псевдонима – domjava и полный путь к каталогу. По умолчанию – c:\lotus\domino\data\domino\java.

Запуск Domino для IIS.

*929 Запустите Domino сервер. Не запускайте HTTP задачу, на сервере Domino, так как IIS будет обрабатывать Domino HTTP запросы.

*930 Откройте MMC, и запустить IIS. IIS загружает Domino расширение, при первой попытке, когда пользователь запросит Domino URL.

*931 Закончите процедуру настройки безопасности для Domino и MS IIS.

Остановка Domino для IIS.

Вы должны остановить IIS сервер, чтобы остановить Domino для IIS.

2.13.2.3 Установка опций безопасности Domino для Microsoft IIS.

После того, как Вы настроили Domino для IIS, настройте опции безопасности для пользователей, обращающихся к Вашему серверу. Domino для IIS использует два уровня безопасности: для IIS и для Domino. После IIS идентификации пользователя, основанного на регистрации в NT, если пользователь успешно пропускается, обращается к опциям безопасности Domino.

Microsoft IIS поддерживает следующие методы установления подлинности пользователя:

*932 **Anonymous access** - пользователь не вводит имя или пароль

*933 **Basic Authentication** - пользователь вводит имя и пароль

*934 **WindowsNT Challenge/Response** - специальный протокол, поддерживаемый Microsoft Internet Explorer SSL

IIS требует установление подлинности пользователя, чтобы управлять доступом к ресурсам, принадлежащим IIS типа системным файла или Active Server Page. Если пользователь просит, доступ к Domino ресурсу, IIS пропустит введенную информацию на Domino сервер. Информация проходит и зависит от комбинации опознавательных методов, которые позволяются на IIS. После того, как информацию пропускают, Domino идентифицирует пользователя согласно процедурам, используемым родным Domino сервером и задачей HTTP. Все наборы каталогов, доступные родной HTTP задачей, типа использования нескольких Domino Directory, LDAP Directory, доступны для Domino с IIS.

Настройка опций безопасности.

*935 Запустите MMC для – Web site.

*936 Выбирайте - IIS Web site и выбирайте – Setting.

*937 Выбирайте закладку - Directory Security.

*938 Выбирайте – Edit Anonymous Access из Authentication Control section.

*939 Выбрать одну или большее количество опций опознания и выбирайте – OK.

2.14 Установка сервиса NNTP

Глава описывает, как настроить службу NNTP на Domino сервере. Как настроить и управлять группами новостей (newsgroups) и статьями новостей (newsfeeds).

2.14.1 Сервис NNTP

Вы можете установить службу новостей NNTP на Domino сервере. Она позволяет Вам посылать и получить статьи новостей из USENET, также как создавать и удалять

локальными группами новостей. USENET, это распределенная система информации, которая специализируется в диалоговых обсуждениях разнообразных тем. Набор тем и ответов, связанных с предметом обсуждений называется – группой новостей (newsgroup). Newsgroup, содержит отправленные по почте статьи. Отправление по почте, которое Вы посылаете в группу новостей или Вы их получаете, называется статьей. Любая статья, которая отправлена по почте в группу новостей, может получить пользователь, подписанный на эту группу новостей.

Служба NNTP использует TCP/IP для связи между серверами, которые периодически могут обмениваться группами новостей между собой. Служба NNTP может отправлять или получать группы новостей, также как читать статьи новостей удаленно. Отправка групп новостей происходит, когда сервер входит в контакт с клиентом и указывает, что имеются новости. Получение групп новостей происходит, когда клиент входит в контакт с сервером новостей и запрашивает их.

Использование Domino сервера, со службой NNTP, позволяет пользователям получить группы новостей с Domino сервера и читать статьи новостей в базе данных Notes. Администраторы могут использовать безопасность Domino, базирующуюся на ACL баз данных, чтобы управлять доступом к группам новостей.

Обратите внимание, что пользователи могут использования стандартного клиента для чтения групп новостей типа Netscape, Collabra или IE, или Web браузер, чтобы читать статьи новостей.

Сервис NNTP

Domino сервер поддерживает следующие функции службы NNTP:

*940 Поддержка клиентов Notes 4.6 и выше, стандартных клиентов NNTP, клиентов использующих Web браузер. Эти клиенты могут участвовать в обсуждении новостей.

*941 Поддержка USENET newsgroups Internet

*942 Поддержка для частных групп новостей, для использования в пределах Вашей организации

*943 Распределение статей новостей, использующих NNTP и схему Pull-Push для других NNTP серверов

*944 Безопасность для серверов, включая анонимный, парольный доступ и доступ с использованием – SSL

*945 Архивирование статей групп новостей.

2.14.2 Настройка Domino сервера и сервиса NNTP

*946 Настройка Domino сервера и настройка безопасности сервера.

*947 Запуск задачи NNTP на сервере.

*948 Настройка Server документа для сервиса NNTP.

*949 Настройка доступа клиентов на сервер.

*950 Создание документов подключений для сервера.

*951 Настройка установок портов сервера.

*952 Создание групп новостей, конфигурирование Domino сервера и сервиса NNTP, для автоматического создания групп новостей.

2.14.2.1 Настройка Server документа, для использования сервиса NNTP.

Domino сервер, с запущенной службой NNTP, может отправлять или принимать группы новостей, с удаленного сервера NNTP. Движение групп новостей может происходить в одном направлении или двух направлениях, то есть Domino сервер может “выталкивать” статьи на удаленный сервер, или статьи могут передаваться в обоих направлениях. Первый раз, когда Domino сервер принимает статьи групп новостей, установки по умолчанию требуют принимать только новые статьи, которые были отправлены по почте в течение прошедших трех дней.

Документ подключения сервера содержит информацию о домене, которая используется при соединении сервера для маршрутизации почты и репликаций. Например, в документе подключения Вы определяете имена групп новостей, которые Вы получаете.

Вы можете определить назначения для всех групп новостей NNTP между Domino сервером, со службой NNTP, и другим сервером NNTP, также как определяете дополнительные функции в документах News/NNTP подключений.

Вы также должны удостовериться, что служба NNTP разрешена в Вашем Server документе.

Настройка сервиса NNTP в Server документе.

*953 Из клиента Domino Administrator, выбирайте - Настройка – Сервер – Все документы на сервере.

*954 Выбирает сервер, чей документ Вы будете редактировать. Выбирайте – Edit Server.

*955 Выбирайте - Internet Protocols – NNTP.

*956 Заполните эти поля в секциях Basic и News Feed Parameters, затем сохраните документ:

Поле	**Значение**
NNTP Administrator's name	Имя NNTP администратора. По умолчанию, этот пользователь имеет доступ менеджера к этой базе
Default access	Выбирайте одно: *957 Grant - (по умолчанию) разрешено *958 Deny- запрещено
Exceptions to default access	IP адреса или имена хостов, которым не разрешен доступ По умолчанию - поле пустое.

Allow posting	Выбирайте одно из двух: *959 Yes (по умолчанию) - разрешено получение групп новостей *960 No - запрещено получение групп новостей
Maximum post size	Максимальный размер сообщения групп новостей. По умолчанию - 1024KB.
Maximum connection size	Максимальный лимит размера для соединений групп новостей. По умолчанию - 100MB.
Maximum connections	Максимальное число текущих соединений. По умолчанию - 5.

2.14.2.2 Контроль доступа на Domino сервер со службой NNTP.

Вы можете управлять тем, какой хост или внешние сервера со службой NNTP, могут получить доступ на Ваш Domino сервер со службой новостей NNTP. Если Вы хотите позволить доступ по умолчанию большинству хостов, используйте эту процедуру, чтобы ввести адреса IP тех хостов, которым вы хотите ограничить доступу на сервер.

*961 Из клиента Domino Administrator, выбирайте - Настройка – Сервер – Все документы на сервере.

*962 Выбирает сервер, чей документ Вы будете редактировать. Выбирайте – Edit Server.

*963 Щелкает - Internet Protocols – NNTP.

*964 Введите IP адреса или имя хостов в поле Exceptions to default access. Доступ на сервер для этих значений хостов будет ограничен. Сохраните документ.

Запрещение всем удаленным серверам NNTP принимать группы новостей.

Чтобы запретить всем удаленным NNTP серверам пулинг новых статей (забирать новости) с Вашего сервера, введите переменную в файл NOTES.INI:

```
NNTP_Prohibit_NEWNEWS_Command=1
```

2.14.2.3 Создание документа подключения для сервера Domino, сервисом NNTP.

Вы нуждаетесь в документе подключения для любого сервера, с которого Вы принимаете группы новостей. Если Вы только получаете группы новостей, Вы будете нуждаться только в этом типе документа подключения для каждого сервера, с которым Вы соединяете для обновления групп новостей.

Если вы планируете принимать и отсылать группы новостей, то Вам понадобиться два типа документов. Вы нуждаетесь в документе подключения для любого сервера, на который Вы будете выталкивать группы новостей, а также в документе подключения для любого

сервера, с которого Вы будете забирать группы новостей. В основном это будет связь по сети LAN, поэтому вы будете создавать документы подключения для LAN связи.

Если топология Вашей сети основана на типе связи Dial-Up для любого сервера, к которому Вы имеете доступ только через MS RAS. В этом случае, Вы будете также нуждаться в документах подключения для каждого сервера, с которого Вы будете забирать группы новостей, и документы подключений для каждого сервера, которому Вы будете передавать группы новостей.

Создание документа подключения сервера для соединения с сервером групп новостей.

*965 Из клиента Domino Administrator, выбирайте закладку Настройка.

*966 Выбирает вид Сервер – Подключения

*967 Делайте одно из двух:

- Чтобы создавать документ подключения, выбирайте – Add Connection.
- Чтобы редактировать документ подключения, выберите сервер, для которого Вы хотите редактировать документ подключения и выбирайте – Edit Connection.

*968 На закладке – Basics, заполните эти поля:

Поле	**Значение**
Connection type	Выбирайте тип – News/NNTP Feed

Source Server	Domino сервер, на котором запущен NNTP сервис.
	Пример:
	`Server1/Acme`
	Или IP сервера
	`192.168.220.123`

Connect via	Выбирайте тип соединения – Direct connection
Destination server	Полное имя интернет хоста сервера. Пример: `news.provider.com` Или IP адрес удаленного Domino сервера с сервисом NNTP

*969 Выбирайте закладку NNTP и заполняйте эти поля:

Поле	**Значение**

News feed type	Выбирает один из этих типов подключений: *970 Accept- чтобы разрешить удаленным серверам NNTP соединятся с Domino сервером с сервисом NNTP, и передавать новые статьи. *971 Pull - чтобы соединиться с удаленным сервером NNTP и запрашивать новые статьи с этого сервера *972 Push - чтобы соединиться с удаленным сервером NNTP и посылать новые статьи на этот сервер *973 Pull-Push - чтобы соединиться с удаленным сервером NNTP и обмениваться с ним новыми статьями в обоих направлениях
Authentication	Выбирайте одно из двух: *974 None - (по умолчанию) *975 Password - требовать имя пользователя и пароль для соединения
Username	Имя регистрации для сервера, с которого Вы будете принимать, или на который Вы будете отсылать статьи.
Password	Пароль для сервера, с которого Вы будете принимать, или на который Вы будете отсылать статьи.
Channel encryption	Выбирайте одно из двух: *976 None - (по умолчанию) *977 SSL - удаленный сервер со службой NNTP требует, чтобы Domino сервер с NNTP использовал протокол – SSL. Протокол нужно разрешить в Server документе на закладке Ports – Internet Ports – News, в поле SSL port status
Create newsgroups	Выбирайте одно из двух: *978 Automatic - (по умолчанию) новые группы создаются автоматически. *979 Manual - ручное создание групп на сервере
Newsgroup subdirectory	Имя подкаталога для хранения новостей По умолчанию – NNTP
Connection timeout	Максимальное время в минутах для завершения процесса обмена группами новостей По умолчанию - 0 минут
Newsgroups	Имена групп новостей (newsgroups) которые Вы хотите принимать к себе на сервер, или отсылать на другие сервера.

*980 Заполняйте остающиеся поля так, как Вы заполняете их для любого документа подключения, затем сохраните документ.

Создание документа подключения для типа соединения Network Dial-Up connection.

*981 Из клиента Domino Administrator, выбирайте закладку Настройка.

*982 Выбирает вид Сервер – Подключения

*983 Делайте одно из двух:

- Чтобы создавать документ подключения, выбирайте – Add Connection.
- Чтобы редактировать документ подключения, выберите сервер, для которого Вы хотите редактировать документ подключения и выбирайте – Edit Connection.

*984 На закладке Basics, в поле Connection type:, выбирайте – Network Dial-Up.

*985 Заполните оставшиеся поля на закладке Basics, как обычно для документа подключения.

*986 Щелкает на закладке – Network Dial-Up.

*987 В поле Choose a service type, выберите – Microsoft Dial-Up Networking.

*988 Заполните остающиеся поля, как обычно, затем сохраните документ.

Соединение с удаленным сервером с сервисом NNTP.

Вы можете использовать программное обеспечение службы удаленного доступа к сети LAN, чтобы соединиться с промежуточным сервером, который в свою очередь может, соединяется с удаленным сервером, на котором имеется служба NNTP.

Обратите внимание, если Вы установили Domino сервер со службой NNTP на платформу другую, чем WindowsNT или Windows95, Вы не можете конфигурировать, сервер для звонка на сервер с NNTP, через Domino сервер.

*989 Устанавливайте программное обеспечение для удаленного доступа к сети. Запустите программное обеспечение для удаленного соединения сети.

*990 Сконфигурируйте модем.

*991 Создайте документ подключения, для соединения с сервером с применением MS RAS.

Обратите внимание, что Вы должны создать в общем количестве три документа подключения.

2.14.2.4 Настройка портов по умолчанию для сервера, на котором запущен сервис NNTP.

TCP/IP порт 119 позволяется по умолчанию для службы NNTP. Используйте эту процедуру только, если Вы собираетесь изменить значения TCP/IP порта или хотите разрешить использование SSL порта, который по умолчанию запрещен. Если Вы используете SSL порт, используйте значение по умолчанию - 563.

Эти значения безопасности относятся к группам новостей для клиентов и удаленным серверам с NNTP, которые соединяются с Domino сервером с NNTP.

Обратите внимание, если Вы определяете другой порт, не 119 порт, для TCP/IP, введите новое значение порта, в Server документе, для этого сервера.

*992 Из клиента Domino Administrator, выбирайте - Настройка – Сервер – Все документы на сервере.

*993 Выбирает сервер, чей документ Вы будете редактировать. Выбирайте – Edit Server.

*994 Выбирайте закладку Ports – Internet Ports – News.

*995 Заполните эти поля и затем сохраните документ:

Поле	**Значение**
TCP/IP port number	Номер порта. По умолчанию – 119
TCP/IP port status	Выбирайте – Enabled
Name and Password	Yes - чтобы позволить клиентам групп новостей и удаленным NNTP серверам использовать пароль при соединении с Domino сервером с установленной службой NNTP. Это поле используется с опцией – SSL.
Anonymous	Yes - чтобы позволить клиентам групп новостей и удаленным серверам NNTP соединять с Domino сервером, с использованием анонимного доступа по TCP/IP. Все связи с группами новостей делаются согласно уровню доступа, позволенного анонимными пользователями. Это поле используется с опцией – SSL.
SSL port number	Номер порта. По умолчанию – 563

*996 Введенные значения для сервера NNTP вступают в силу при перегрузке сервера.

2.14.3 Настройка групп новостей.

Использование USENET newsfeeds может потребовать существенных ресурсов Вашей системы, если Вы подпишетесь на многие группы новостей. Прежде, чем Вы будете конфигурировать USENET newsfeed, удостоверьтесь в следующем:

*997 Что Вы рассмотрели все аспекты размещения групп новостей, без ущерба для Вашей системы передачи почты, репликаций и других задач сервера.

*998 CPU и ресурсы памяти сервера Вашей системы, удовлетворяют числу пользователей ожидаемых для доступа на Domino сервер

*999 Удаленный сервер сконфигурирован для каждого типа групп новостей. Настроите передачу новостей. Сконфигурируйте удаленный сервер так, чтобы он позволял Вашему Domino серверу NNTP, “тянут” группы новостей, которые Вы планируете получать. Для приема новостей, сконфигурируйте удаленный сервер NNTP, чтобы он принимал группы новостей, которые Вы будете “выталкивать” со своего сервера

Настройка групп новостей.

Прежде, чем Вы конфигурируете группы новостей, свяжитесь с администратором удаленного сервера NNTP, или Вашего поставщика новостей интернета. Договоритесь о:

*1000 Об именах или IP адресах для двух серверов NNTP, которые будут участвовать в передаче групп новостей.

Например:

```
servername.acme.com или news.isp.com
```

*1001 О группах новостей и о статьях, которые Вы планируете передавать между серверами.

*1002 О типах групп новостей.

Тип группы новостей	**Описание**
Accept	Удаленный NNTP сервер, является инициатором соединения с Domino сервером NNTP и посылает статьи. Выбирайте один из типов групп новостей, если Ваш Domino сервер NNTP будет инициатором соединений.
Pull*	Domino сервер NNTP соединяется с удаленным сервером NNTP и запрашивает новые статьи. Domino сервер NNTP не посылает свои статьи.
Push*	Domino сервер NNTP соединяется с удаленным сервером NNTP и посылает на него новые статьи. Domino сервер NNTP не принимает статьи.
Pull-Push*	Domino сервер NNTP соединяется с удаленным сервером NNTP и запрашивает новые статьи, а потом передает свои новые статьи.

* Удаленный сервер NNTP требует разрешение администратора до передачи сообщений. Проверите, что Вы имеете доступ к удаленному серверу NNTP.

*1003 Договоритесь о расписании передаче новых статей.

*1004 Договоритесь об информации по настройке порта и безопасности, чтобы настроить документы подключения. Вам нужна следующая информация:

- Номер порта NNTP
- Имя и пароль, для установления подлинности
- Информация об использовании SSL, для NNTP

*1005 Выделите свободное место на диске, для хранения групп новостей.

Служащие, которые отправляют по почте статьи с локальным адресом хоста, например - lerri@acme.com должны отражать имя Вашей компании. Поэтому, Вы должны создать политику для отправления по почте статей в группы USENET.

Перегрузка групп новостей.

Вы можете иногда повторно устанавливать группы новостей, если сервер предназначение недоступен. Переустановка групп новостей заставляет сервер отправлять или получать статьи новостей, как будто это происходит в первый раз.

Задача	**Установки файла NOTES.INI**
Reset a newsfeed	NNTP_Previous_*x_servername*
Request the transfer of all articles posted within a specific number of days during an initial newsfeed	NNTP_Initial_Feed_Days
Transfer all articles during an initial newsfeed	NNTP_Initial_Feed_All

```
Tell NNTP Reset servername
```

Эта команда переинициализирует все группы новостей.

2.14.4 Группы новостей.

Частные группы новостей и публичные новости USENET newsgroups.

Domino сервер, со службой NNTP, позволяет пользователям участвовать в частных группах обсуждений или публикациях группах новостей USENET newsgroups. Каждая группа новостей сохраняется как база данных Domino. Соглашение обозначения для базы данных следующие:

```
ND000000.NSF
```

Где 0 - число, автоматически назначенное при создании базы данных. Буквы в имени базы ND назначены как первые два знака, для каждого имени базы данных. Для первой базы данных назначается имя с пятью нулями и номером 1, второй назначается номер 2 и т.д.

Частные группы новостей.

Используя шаблон NNTPDI50.NTF, Вы можете создавать частные группы новостей, которые - не будут частью системы USENET. Они могут использоваться в пределах Вашей компании или в более широкой аудитории вне Вашей компании, которая охватывает интернет. Частные группы новостей позволяют Вам ограничивать доступ к обсуждениям. Вы выбираете из Вашего Domino Directory, имена тех пользователей, которые могут иметь доступ к частным группам новостей.

Если Вы устанавливаете несколько Domino серверов с сервисом NNTP в пределах Вашей организации, используете репликации, чтобы обмениваться недавно отправленными по почте статьями. Использование репликаций, Вы можете гарантировать, что все модули и списки контроля доступа ACL остаются в синхронизированном состоянии.

Не распространяйте частные группы новостей на USENET NNTP серверах в интернете.

Публичные группы новостей.

Когда Вы посылаете статью для публикации в USENET группы новостей, с Domino сервера NNTP, статья посылается Вашему поставщику USENET, а затем распределяется повсюду в системе USENET. Ваша статья может быть продублирована сотни раз.

Поддержка групп новостей.

Уменьшение групп новостей. Позвольте только одному человеку, модератору, отправлять по почте статьи в группы новостей. При конфигурировании Вашего Domino сервера для службы NNTP, Вы можете определить, хотите ли Вы, чтобы Domino сервер NNTP, автоматически создавал уменьшенные группы новостей только с доступом читателя.

2.14.5 Создание и поддержка групп новостей.

После того, как Вы создаете группы новостей, Вы должны регулярно архивировать и удалять статьи, также как и исполнять другие задачи обслуживания для баз данных.

2.14.5.1 Поддержка групп новостей.

Модератор групп новостей может принимать, отклонять, или отвечать на почтовые статьи.

Принятие или отклонение статей новостей.

*1006 Из клиента Domino Administrator, выберите - Файл – База данных – Открыть.

*1007 Открывайте базу данных группы новостей.

*1008 Выбирайте статью из представления Moderated View.

*1009 Просмотрите статьи, откройте нужную статью, затем щелкайте на кнопке Approve (принять), или на кнопке Reject (отклонить).

Отправка статьи новостей по почте.

Чтобы отправить по почте статью из клиента Notes или из Web браузера в группу новостей на сервере со службой NNTP, клиент Notes должен быть связан с этим сервером. На NNTP сервере Вы создаете базу данных NNTP, В которую можно отправлять почту (например, NNTPPOST.NSF) в каталоге данных. Когда клиент Notes или Web клиент отправляет по почте статью в больше чем один группу новостей, служба NNTP использует эту базу данных, чтобы хранить и затем отправить по почте статью в группу новостей в намеченный интервал времени.

2.14.5.2 Создание групп новостей.

Группы новостей могут быть созданы автоматически на Вашем Domino сервере с запущенной службой NNTP. Вы можете также использовать этот метод, чтобы создать вручную группы новостей. При назначении имени групп новостей, Вы не можете использовать пробелы, ?, !, [], или *. Для частных групп новостей, Вы не можете использовать категории USENET.

USENET использует иерархию, чтобы организовать группы с главной темой. Каждая группа новостей имеет собственное имя, в которое включено одно или большее количество частей, отделенное точкой. Имя группы новостей всегда начинается с имени иерархии.

Например, группы новостей для вопросов пользователей о системе USENET, может называться news.newusers.questions, где news - иерархия, newusers - первая категория, questions - подкатегория.

USENET иерархии - comp, misc, news, rec, sci, soc, chat, alt ...

Создание групп новостей.

Прежде, чем Вы создаете группу новостей, Вы определяете документ профиля для базы данных. В этом документе, Вы определяете, является ли группа новостей публичная или частная. Вы определяете права доступа для частных групп новостей.

Вы должны сохранить документ профиля базы данных прежде, чем Вы исполняете шаги по созданию групп новостей. Сохраните документа профиля базы данных, позволяет показать группу новостей, NNTP клиентам, клиентам Notes 4.6 и выше и Web пользователям.

В документе профиля базы данных, заполните эти поля и сохраните документ.

Поле	**Значение**
Database Profile editors	Имена пользователей, кому позволяют изменить профиль Базы данных. По умолчанию - имя создателя групп новостей. Пользователи, чьи имена Вы вводите - получают доступ менеджер к базе данных.
Private	Выбирайте одно из двух: *1010 Private – частная группа новостей Если опция не отмечена – публичная группа новостей
List of users who can access the database	Выбирайте одно из двух: Введите имена пользователей, которые могут получить доступ к Вашей базе данных. Эти пользователи будут иметь доступ автора к базе данных.
Moderated	Выберите пользователя – модератора для частных групп новостей и затем заполните эти поля: Name of Moderator: - имя пользователя, который отправляет по почте и удаляет статьи новостей. Этот пользователь – назначается редактором в ACL базы данных. E-mail of Moderator: - чтобы использовать адрес для рассылки статей и вопросов к модератору групп новостей. Если Вы оставляете поле незаполненным, Domino создает группу Moderated NewsGroup.

Вы можете разрешить отображение списка баз данных в каталогах:

Откройте окно свойств базы данных.

Выбирайте закладку - Design и выбирайте свойство - Включить в каталог баз данных.

Настройки ACL для групп новостей.

Вы можете использовать ACL баз данных, чтобы определить уровень доступа пользователей. Например, если Вы даете доступ пользователям интернета к частной группе новостей, определите их доступ базе только на чтение, но дайте доступ автора всем внутренним пользователям. Тогда внутренние пользователи могут отправить по почте статьи в группы новостей, а пользователи интернета могут только читать статьи.

Анонимный доступ к группам новостей.

Для доступа к частным группам новостей или любым группам новостей, к которым не позволяется анонимный доступ, сконфигурируйте NNTP сервис на сервере запрашивать имена пользователей для доступа к серверу новостей.

Автоматическое создание и управление группами новостей, доступных только для чтения.

*1011 От Вашего поставщика USENET, получите файл - active, который содержит список всех групп новостей на отдаленном сервере NNTP и указывает, являются ли группа новостей модерируемой, или позволяется ли отправлять статьи по почте.

*1012 Скопируйте этот файл в каталог данных и дайте имя ему - active. Когда Domino сервер с запущенной службой NNTP автоматически создает группу, сервер читает этот файл, чтобы определить, создать ли новую группу новостей с доступом только на чтение, по умолчанию.

2.14.5.3 Использование контрольных сообщений для администрирования групп новостей.

Сообщения контроля могут использоваться администратором Domino сервера NNTP при управлении группами новостей. Newsreader клиент может посылать сообщения контроля на Domino сервер, чтобы помогать координировать административные функции, типа создания и удаления групп новостей, удаления определенных статей из групп новостей.

Domino сервер с администратором NNTP службой может решать, действовать ли согласно инструкциям в сообщении контроля.

Все сообщения контроля сохраняются в уникальных группах новостей с приставкой control. Например, control.xxx, где xxx - тип сообщения контроля. Эти группы сообщений контроля создаются автоматически, когда Вы запускаете службу NNTP:

Контрольные сообщения	**Группы новостей**	**Сообщение**
Rmgroup	control.rmgroup	Удаление группы новостей
cancel	control.cancel	Удаление вставка статьи в группу новостей
newgroup	control.newgroup	Создание группы новостей

Если Вы удаляете одну из этих групп сообщений контроля, оно будет восстановлено следующий раз, когда Вы повторно начинаете службу NNTP.

Сообщение контроля, посланное из группы новостей клиента, сохраняется в соответствующей группе контроля, если она существует. Например, если клиент удаляет статью, удаляющееся сообщение будет сохранено в группе новостей – control.cancel.

Вы должны регулярно просматривать сообщения контроля, полученные Вашим Domino сервером NNTP. Чтобы получать автоматическое уведомление электронной почты, когда сервер получает сообщение контроля, Вы может создать агента.

Получение сообщений контроля.

Чтобы получать сообщения контроля через группы новостей, Вы должны добавить имена контрольных групп новостей в поле Newsgroup, в документе подключения для групп новостей. Например, чтобы получить новые сообщения группы контроля, добавьте имя control.newgroup, в поле Newsgroup, документа подключения для групп новостей.

2.14.5.4 Архивирование и удаление статей из групп новостей.

Управление группами новостей подразумевает удаление статей, когда они бездействуют или истекли их сроки. Из клиента Notes, Вы можете установить архивирование, чтобы удалять или архивировать статьи. Вы должны иметь доступ менеджера к базе данных новостей.

Архивирование статей.

Параметры в архивирования устанавливаются для баз данных, когда Вы определяете параметры архива через свойства базы данных. Параметры архива, которые Вы устанавливаете, применяются только к статьям в выбранной базе данных.

*1013 Откройте базу данных группы новостей, для которой Вы хотите изменить параметры архивирования.

*1014 Из клиента Notes выберите - Файл – База данных – Свойства.

*1015 Выбирайте – Настройка архива.

*1016 Выбирайте любую опцию из следующего выбора:

*1017 Выбирайте – OK.

Удаление статей из групп новостей.

По умолчанию, статьи из групп новостей, созданных на сервере автоматически - удаляются через пять дней.

Чтобы изменять эти установки, измените переменные в NOTES.INI:

Задача	**Установки NOTES.INI**
Определите число дней прежде, чем бездействующая статья будет удалена	NNTP_Delete_Days
Определите число дней, прежде чем просроченная статья будет удалена	NNTP_Delete_Days_Expired

Удаление групп новостей

*1018 Удостоверьтесь, что Вы имеете доступ менеджера в ACL групп новостей базы данных.

*1019 Введите на консоли сервера:

```
tell nntp newsgroup delete group_name(s)
```

Где group_name(s) - имя группы новостей.

Вы можете использовать звездочку (*), чтобы указать больше чем одну группы новостей. Вы можете использовать запятые, чтобы отделить имена групп новостей. Например, для group_name(s) Вы может определить rec.skiing или comp.groupware.

2.15 Transaction Logging.

Domino поддерживает опцию Transaction Logging и опции восстановления после сбоя системы. Если Вы включаете этой функции, система захватывает базу данных и отслеживает все изменения, записывая их в файл Transaction Log. В случае если Ваша система отказывает, Вы можете использовать файл Transaction Log и устройство резервного копирования, чтобы восстановить Ваши разрушенные базы данных.

Single Transaction - ряд изменений, сделанных в базе данных на сервере. Например, транзакция может включать открытие нового документа, добавление в него текста и сохранение документа.

Transaction logging - обеспечивает три главных выгоды:

*1020 В большинстве ситуаций, Вы больше не должны использовать задачу Fixup для обработки баз данных после отказа системы. Исключение использования задачи Fixup - более быстрый перезапуск сервера, так как Fixup должен сначала проверить каждый документ в каждой базе данных. Использование для восстановления Transaction Log более выгодно, так как вы можете восстанавливать или уничтожать только те транзакции, которые не записаны на диск, во время отказа системы.

*1021 Transaction logging экономит время, потому что позволяет Domino отложить модернизацию базы данных и запись на диск в течение периодов высокой занятости сервера. Транзакции регистрирует последовательно операций в файлах протоколах.

*1022 Использование Transaction logging упрощает Вашу ежедневную процедуру резервного копирования. Вы можете использовать утилиту резервного копирования, чтобы выполнять сохранение ежедневных изменений Transaction Logs, чем исполняют полную процедуру резервного копирования баз данных.

Transaction logging работает с базами данных Версии 5. После того, как Вы разрешаете использования опции Transaction Logging, все базы данных формата R5, автоматически будут зарегистрированы. Чтобы проверять формат баз данных, используйте закладку Файлы, из клиента Domino Administrator.

Чтобы использовать все функции Transaction logging и опций восстановления, Вы нуждаетесь в дополнительной утилите резервного копирования, которая поддерживает Transaction logging Domino R5.

2.15.1 Как работает Transaction logging?

*1023 Администратор системы, корпорации Acme, разрешает использование Transaction logging на почтовом сервере Mail-E/East/Acme. Перед использованием этой функции, администратор выбирает:

- Сохранять ли файлы Transaction Log на отдельном устройстве накопления информации с объемом не мене 1Гб.
- Выбирает способ архивирования транзакций.
- Настраивает утилиту резервного копирования, чтобы архивировать файлы протоколов. Утилита настроена на сохранение ежедневных Transaction Log и сохраняет все файлы транзакций каждую неделю.

*1024 Чтобы разрешить Transaction logging, администратор системы перезапускает Mail-E/East/Acme.

*1025 Когда сервер перезапускается, Domino делает следующее:

- Назначается Unique Database Instance ID (DBIID) для каждой базы данных формата R5, для того чтобы можно было отслеживать транзакции баз данных.
- Формирует файлы транзакций *.TXN и файл контроля.

Пример. Алан Джонес использует клиента Notes, чтобы создавать, редактировать и сохранять новые почтовые сообщение. Для новых почтовых сообщений:

- Делается запись в файлах Transaction Log.
- Сохраняется как изменение базы данных на сервере Mail-E/East/Acme.

В этот же день, Джуди Каплан использует Web браузер, чтобы создать и сохранить новую запись в ее календаре. Эта транзакция также будет зарегистрирован в Transaction Log прежде, чем назначение может быть сохранено к почтовой базе данных Джуди, Mail-E/East/Acme останавливается из-за отказа системы.

Когда администратор системы повторно запускает сервер Mail-E/East/Acme, Domino автоматически использует Transaction Log, чтобы исправить почтовую базу данных Джуди Каплана и восстанавливать календарное назначение.

Идентификатор базы данных DBIID.

Когда Вы включаете Transaction logging, Domino назначает каждой базе данных, формата R5, специальный идентификатор DBIID. Когда Domino делает запись в Transaction Log, он использует DBIID. В течение восстановления, Domino использует DBIID, чтобы связать транзакции и базу данных.

При выполнении некоторых действий, по обслуживанию баз данных, например запуск задачи Compact с некоторыми параметрами, заставляет Domino назначать новые DBIID для баз данных. С этого момента и далее, все новые транзакции, будут зарегистрированы в файлах протоколов, с использованием новых DBIID. Любые старые транзакции все еще имеет старый DBIID и больше не соответствуют новому DBIID баз данных. В результате, Domino не может восстановить эти старые транзакции в базах данных.

Чтобы избежать потери данных архивирования, Вы должны немедленно архивировать базу данных всякий раз, когда база данных получает новый идентификатор DBIID. Когда Вы выполняете эту процедуру, Вы захватываете всю базу данных транзакций, вплоть до момента, когда Domino получил новый DBIID, для восстановления базы данных.

Domino назначает новый идентификатор DBIID, когда:

*1026 Вы впервые запускаете Transaction logging.

*1027 Вы запускаете задачу Compact на сервере с любыми параметрами.

*1028 Вы запускаете задачу Fixup на испорченных базах данных.

*1029 Вы изменяете путь к файлам протоколов, или максимальный размер для файлов протоколов.

*1030 Вы перемещаете базы данных с одного сервера на другой.

2.15.2 Установка и настройка Transaction logging.

Все базы данных будут зарегистрированы в каталоге данных Domino и в подкаталогах.

*1031 Из клиента Domino Administrator, выбирайте закладку Настройка.

*1032 Открывайте Server документ.

*1033 Выбирайте закладку Transaction Logging.

*1034 Заполните эти поля, сохраните документ.

Поле	**Значение**
Transactional Logging	Выбирайте – Enabled, чтобы разрешить эту функцию. По умолчанию – Disabled.
Log path	Местоположение для файлов Transaction Log. По умолчанию поле пусто. Файлы будут помещаться в каталог данных Domino сервера. Настоятельно рекомендуется хранить файлы протоколов на отдельном устройстве, типа RAID. Определенное дисковое устройство должно иметь, по крайней мере, 1Гб свободного места. Если Вы используете это место исключительно для хранения файлов Transaction Log, установите значение – Yes, в поле Use all available space on log device.
Maximum log space	Максимальный размер в Мб, для файлов Transaction Log. По умолчанию - 192МБ. Максимум - 4096МБ (4GB). Domino форматирует, по крайней мере, от 3 до 64 файлов протоколов, в зависимости от максимально доступного места для этих файлов.

Use all available space on log device	Выбирайте одно: *1035 Yes - чтобы использовать все доступное место для файлов Transaction Log. Эта опция рекомендуются, если Вы используете отдельное устройство, для хранения файлов протоколов. Если Вы выбираете – Yes, Вы не должны вводить максимальное значение в поле Maximum log space. *1036 No - чтобы использовать значения по умолчанию или указать значения в поле Maximum log space.
Automatic fixup of corrupt databases	Выбирайте одно: *1037 Enabled - (по умолчанию). Если база данных испорчена и Domino не может использовать Transaction Log, чтобы исправить ее, Domino запустит задачу Fixup, назначает новый идентификатор DBIID и уведомляет администратора, что новая база данных требует резервного копирования. *1038 Disabled - Domino не запускает автоматически задачу Fixup и уведомляет администратора о факте разрушения базы с предложением запустить задачу с ключом (-J) на разрушенных базах данных.
Runtime/Restart performance	Это поле управляет, как часто Domino делает запись пунктов восстановления (recovery) в файл Transaction Log. Эта установка влияет на загрузку сервера. Чтобы делать запись пунктов восстановления, Domino оценивает каждую активно зарегистрированную базу данных, чтобы, определить, сколько, транзакций было бы необходимо для восстановления каждой базы данных после отказа системы: Создает отчет записей восстановления в файлах Transaction Log, внося в список каждую открытую базу данных, и отправную точку транзакций, необходимую для восстановления. Вынуждает базу данных при изменении, сохранятся на диске, если она не была еще сохранена. Выбирайте одно: *1039 Standard - (рекомендуемый по умолчанию). Сохранение пунктов происходят регулярно. *1040 Favor runtime – во время выполнения. Domino делает записи меньшего объема, улучшая производительность сервера. *1041 Favor restart recovery time - Domino делает запись большего объема, улучшая время восстановления, потому что меньшее количество транзакций требуется для восстановления.

Logging style	Выбирайте одно: *1042 Circular - (по умолчанию) непрерывное, повторное использование файлов протоколов и переписывать старые транзакции. Вы ограничены в восстановлении только транзакциями, сохраненными в Transaction Log. *1043 Archive - (рекомендуется) предотвращает повторное использование файлов протоколов, пока они не архивированы. Файл протоколов может быть архивирован, когда он закрыт или не захвачен. Используйте утилиту резервного копирования, чтобы копировать и архивировать существующие файлы. Когда Domino начинает использовать существующий файл снова, он увеличивает имя файла протоколов на единицу. Если все файлы протоколов станут бездействующими и не архивированы, Domino создает дополнительные файлы протоколов.

2.15.3 Запрещение Transaction logging для некоторых баз данных.

После того, как Вы установили Transaction logging, все базы данных, которые находятся в формате R5, будут зарегистрированы. Хотя это не рекомендуется, Вы можете запрещать Transaction logging для определенных баз данных.

Например, Вы могли бы запретить эту функцию для базы данных, которая хранит только присоединенные файлы, чтобы изменения этих файлов не регистрировались как транзакции.

В любом случае мы не рекомендуем этого, потому что Вы должны будете запускать задачу Fixup, чтобы править базы данных, после отказа системы.

Запрещение Transaction logging для выбранной базы данных.

*1044 Исполните любое из следующего:

- При создании новой базы данных, выберите опцию - Disable transaction logging, в окне диалога Advanced Databases Options.
- Для существующей базы данных, выберите - Disable transaction logging, в диалоге свойств базы данных.

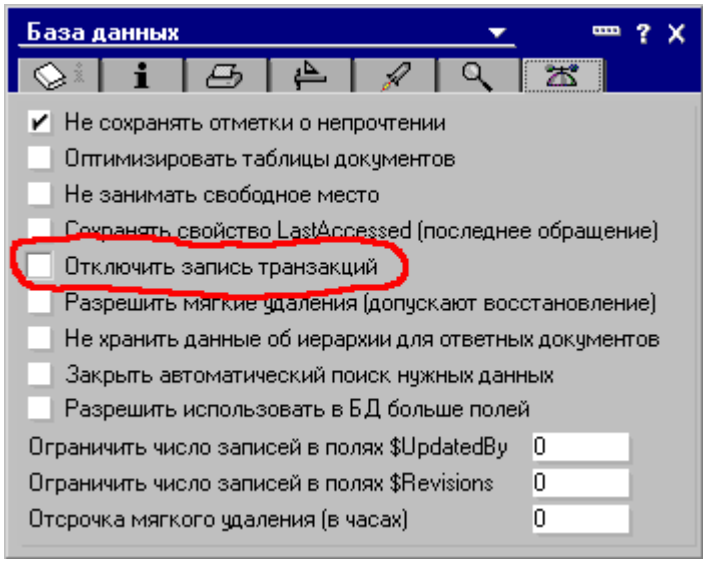


Рис. 51 Отключение записи транзакций, из окна свойств базы данных.

- Из клиента Domino Administrator, выберите базу данных на закладке Фалы, выберите из панели инструментов – Сервис – База данных – Дополнительные свойства, затем выберите опцию - Отключить запись транзакций.

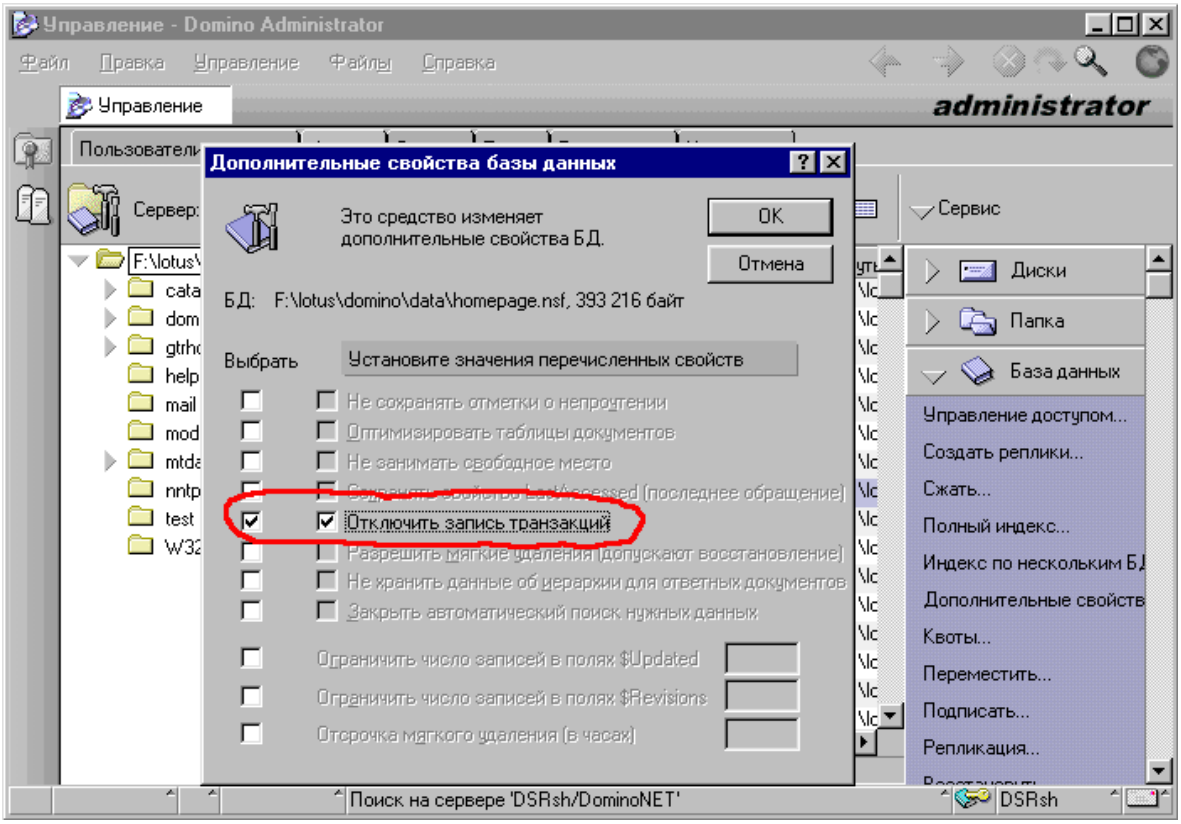


Рис. 52 Отключение записи транзакций, из клиента Domino Administrator.

- Используйте задачу Compact с параметром (-t).

*1045 Удостоверьтесь, что все пользователи закрыли базу данных.

*1046 Использовать команду dbcache, с параметром flush, чтобы закрыть базу данных в базе данных cache.

*1047 Откройте базу данных.

Для восстановления настроек Transaction logging исполните шаги, описанные выше, для отмены установленных свойств. Запустите задачу Compact с параметром (-T).

2.15.4 Расписание резервного копирования для Transaction Login.

Резервное копирование необходимо для восстановления баз данных после отказа диска сервера. Если Вы имеете утилиту для резервного копирования, Вы должны наметить следующее:

Обновление архивных файлов.

Используйте утилиту резервного копирования ежедневно для обновления Transaction Log.

Архивирование файлов протоколов.

Если Вы используете стиль архивирования Archive, используете утилиту резервного копирования, чтобы наметить архивирование файлов протоколов.

Полное резервное копирование.

В конце каждой недели, рекомендуется запускать задачу Compact с соответствующим ключом, чтобы уменьшить размер файла. Потому что задача Compact изменяет идентификатор DBIID каждой базы данных, Вы должны наметить выполнение полного резервного копирования баз данных после выполнения этой задачи.

2.15.5 Использование Transaction logging для восстановления.

Transaction logging - неотъемлемая часть процесса восстановления.

Восстановление системного отказа.

Отказ системы заставляет сервер останавливаться, и требуется повторный запуск сервера. В течение повторного запуска, Domino автоматически запускает восстановление баз данных. Система использует Transaction logs, чтобы применить или уничтожить данные транзакций, не записанных на диск, которые были открыты в течение отказа системы.

Domino также запускает задачу Fixup на базах данных, которые используют формат баз данных более ранних версий, на базах данных формата R5 с поврежденным Transaction logging, на испорченных базах данных. Fixup запускается, если вы установили опцию автоматического запуска, в поле Automatic fixup of corrupt databases.

2.16 Кластер серверов Lotus Domino.

Глава описывает кластер серверов Lotus Domino. Она научит Вас, как создать и конфигурировать кластер, объяснит выгоды от использования кластера серверов. Будут рассмотрены требования к программному обеспечению для использования кластера серверов.

2.16.1 Что такое кластер серверов Domino?

Domino кластер – это группа серверов, от двух до шести, которая позволяет Вам обеспечить пользователям постоянным доступом к данным, балансировать рабочую нагрузку между серверами, улучшать производительность серверов, когда Вы увеличиваете

размер Вашего предприятия. Сервера в кластере могут содержать реплики баз данных, которые будут готовы к использованию всегда. Если пользователь пробует открыть базу данных на сервере в кластере, который в данный момент не доступен, Domino открывает реплику этой базы данных на любом сервере в кластере, если реплика доступна. Domino непрерывно синхронизирует базы данных так, чтобы, какую бы ни открывал реплику пользователь, информация, будет всегда идентична.

Lotus Notes® клиенты могут иметь доступ ко всем серверам в Domino кластере. HTTP клиенты, клиенты, использующие интернет браузеры, могут получить доступ только к Domino Web серверам в Domino кластере.

2.16.1.1 Какие выгоды Вы получите от использования кластера серверов?

Когда происходят аппаратные сбои компьютера, или появляются проблемы с программным обеспечением, сервера в кластере переадресовывают запросы открытия баз данных, на другие сервера в кластере, для обеспечения пользователям непрерывного доступа к важным базам данных. Этот процесс называется Failover – переадресация или перенаправление. В кластере могут принимать участия Passthru сервера и выполнять такую же переадресацию на другие сервера в кластере. Failover также позволяет Вам выполнять обслуживание серверов.

Баланс рабочей нагрузки.

Когда пользователи пробуют получить доступ к базам данных на тяжело загруженных серверах, Domino может переадресовывать запросы пользователей на другие сервера кластера так, чтобы рабочая нагрузка была равномерно распределена по всему кластеру. Балансирование рабочей нагрузки на серверах в кластере, помогает Вашей системе достигнуть оптимального выполнения работ, которое ведет к более быстрому доступу к данным.

Расширяемость.

Когда число пользователей у Вас увеличивается, Вы можете легко добавлять сервера в кластер, чтобы поддержать высокое быстродействие Вашей системы. Вы можете также создавать многократные реплики баз данных, чтобы максимизировать готовность баз данных и перемещать пользователей на другие сервера кластера. Поскольку Ваше предприятие растет, Вы можете распределять пользователей в кластере и сбалансировать рабочую нагрузку в пределах кластера.

Синхронизация данных.

Ключ к эффективному использованию кластеров создание реплик на двух или более серверах кластера так, чтобы пользователи могли иметь доступ к данным, когда один из серверов закрывается или тяжело загружен. Репликации кластера гарантирует, что все изменения в базах данных, немедленно поступают в другие базы данных на сервера кластера. Таким образом, базы данных непрерывно синхронизируются, чтобы обеспечить высокую готовность информации.

Инструменты анализа и наблюдения за системой.

При использовании инструментов анализа кластера, а также файлов протоколов и базы данных Statistics & Events, Вы можете анализировать деятельность кластера и делать любые изменения необходимые для улучшения выполнения работ.

Простота обслуживания и модернизация системы серверов Domino.

Когда Вы хотите изменить аппаратные средства, операционную систему, или версию серверов Domino, Вы можете помечать сервер кластера опцией – RESTRICTED, чтобы запросы, перенаправлялись на другой сервер кластера. Это позволяет Вам делать Ваши изменения без остановки деловых процессов Ваших пользователей.

Система резервного копирования.

Вы можете настроить сервер в кластере, как резервный сервера, чтобы защитить критические данные. Вы можете запретить пользователям, обращаться к этому серверу, но кластерные репликации будут функционировать.

2.16.2 Системные требования к кластеру.

*1048 Все сервера в кластере должны быть Domino R5 или R4.62, с Enterprise лицензией сервера, или Domino R4.5 или R4.6, с лицензией Advanced Services.

*1049 Все сервера в кластере должны быть связаны, высокоскоростной локальной сетью LAN. Вы можете также установить отдельную, выделенную сеть LAN, только для использования серверами кластера.

*1050 Все сервера в кластере должны использовать TCP/IP, находиться в той же самой поименованной сети Notes и использовать тот же самый набор протоколов сети.

*1051 Все сервера в кластере должны быть в том же самом Domino домене и использовать общий Domino Directory.

*1052 Вы должны определить сервер администрирования для Domino Directory в домене. Если Вы не определяете сервер администрирования, процесс администрирования не сможет изменять членство в кластере. Сервер администрирования должна быть членом кластера или иметь Enterprise лицензию сервера.

*1053 Каждый сервер в кластере должен иметь иерархический ID сервера. Если любой из серверов имеет простой, неиерархический ID, Вы должны преобразовать его в иерархический ID, чтобы использовать сервер в кластере.

*1054 Сервер может быть членом только одного кластера одновременно.

*1055 Каждый сервер должен иметь достаточно места на диске, чтобы функционировать как член кластера. Потому что кластер обычно требуют больше места для реплик баз данных.

*1056 Каждый сервер должен иметь достаточную мощность и соответствующее количество памяти. Вообще, серверам кластера требуются больше мощности компьютера, чем обычным серверам.

Требования к клиенту.

*1057 Клиенты Notes должны работать использовать Notes R4.5 или выше, чтобы воспользоваться преимуществом переадресации кластера.

*1058 Клиенты, обращающиеся к серверу в кластере, должны использовать TCP/IP.

2.16.3 Как работает кластер Domino?

Все сервера в кластере непрерывно связывается друг с другом, чтобы синхронизировать реплики баз данных. Каждый сервер в кластере содержит компоненты кластера, которые

устанавливаются при инсталляции программного обеспечения Lotus Domino Enterprise Server. Эти компоненты и процесс администрирования, исполняют управление кластером, контролируют задачи кластера, позволяют Вам управлять кластером. Эти компоненты содержат в синхронизированном состоянии реплики баз данных, компоненты кластера постоянно связываются друг с другом, чтобы гарантировать правильную работу кластера. Компоненты также позволяют Вам устанавливать пределы для балансирования рабочей нагрузки на серверах и базах данных.

Чтобы воспользоваться преимуществом переадресации и балансирования рабочей нагрузки, Вы распределяете реплики баз данных повсюду в кластере. Вы не нуждаетесь в реплике каждой базы данных на каждом сервере. Число реплик, которые Вы создаете для базы данных, зависит от того, насколько заняты базы данных и насколько они важны для пользователей, чтобы иметь постоянный доступ к той базе данных.

2.16.3.1 Как работает переадресация запросов в кластере?

Способность кластера переадресовывать запросы с одного сервера на другой, при отказе первого, называется Failover. Когда пользователь пробует получить доступ к базе данных на сервер, который данный момент недоступен или тяжело загружен, Domino соединяет пользователя с репликой базы данных на другом сервере в кластере.

Cluster Manager - это задача, которая управляет всеми процессами в кластере. Она анализирует каждый сервер кластера, чтобы определить готовность каждого сервера кластера. Cluster Manager также проверяет непрерывно, какие базы данных и их реплики являются доступными на каждом из серверов. Когда пользователь пробует получить доступ к базе данных, которая не доступна, Cluster Manager переадресовывает запрос пользователя к репликам на различных серверах кластера. Хотя пользователь соединяется с базой данных на различных серверах, сам процесс Failover - прозрачен для пользователя.

Пример:

Этот пример описывает процесс, когда Domino использует кластер, переадресовывает запросы на другие сервера. Этот кластер содержит три сервера. Server1 в настоящее время недоступен. Cluster Managers на Server2 и Server3 знает, что Server1 недоступен.

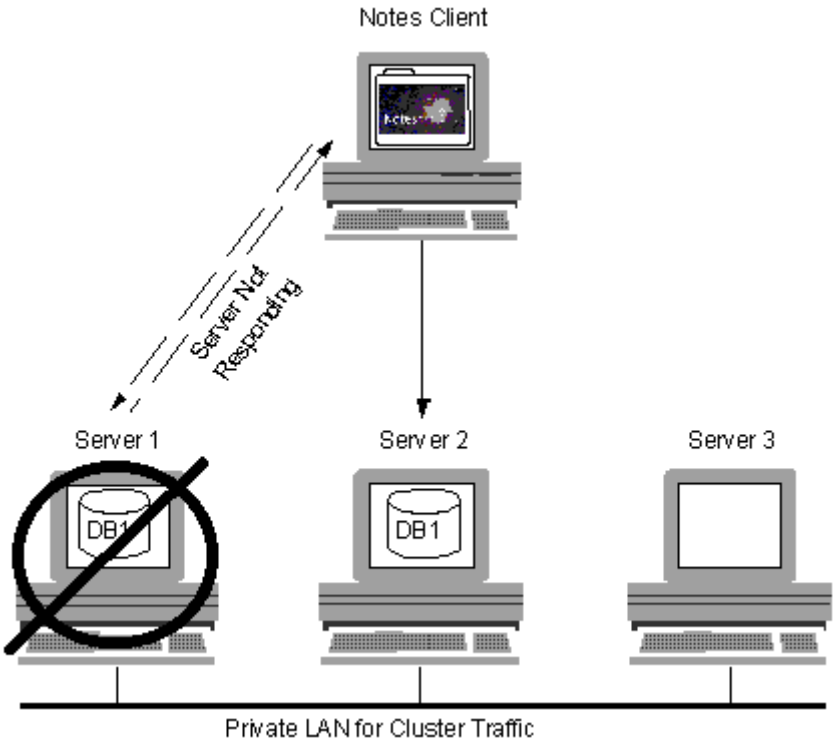


Рис. 53 Пример переадресации запросов пользователей в кластере Domino серверов.

*1059 Пользователь Notes пытается открывать базу данных на Server1.

*1060 Notes понимает, что Server1 не отвечает.

*1061 Вместо вывода сообщения, которое говорит, что сервер не отвечает, Notes просматривает кэш кластера, чтобы видеть, является ли сервер членом кластера, и находить имя другого сервера в кластере. Когда клиент Notes первые получает доступ на сервер в кластере, имена всех серверов кластера добавляется в кэш кластера клиента.

*1062 Cluster Managers на всех серверах, заносят все сервера, в список КЭШа кластера.

*1063 Cluster Manager определяет, какой сервер кластера содержит доступную реплики баз данных.

*1064 Cluster Manager сообщает эту информацию Notes, а Notes открывает эту реплику.

2.16.3.2 Когда происходит переадресация в кластере?

Переадресация происходит, когда пользователи не может получить доступ на сервер, который содержит базу данных, или он не может непосредственно получить доступ к базе данных. Следующая таблица описывает причины, по которым пользователь не может получить доступ на сервер или в базу данных.

Категория	**Причина**
Пользователь неспособен, получить доступ на сервер	Сервер выключен
	Есть проблемы с сетью

	Server достиг максимального значения позволенных пользователей, согласно установке Server_Maxusers из файла NOTES.INI
	Доступ к серверу ограничен администратором, согласно переменной Server_Restricted из файла NOTES.INI
	Сервер занят, находится в состоянии – BUSY, потому что он достиг максимального значения, позволенной нагрузки на сервер
Пользователь неспособен, получить доступ к базе данных	База данных помечена опцией Out of Service, в базе данных Cluster Database Directory
	База данных помечена Pending Delete", в базе данных Cluster Database Directory

Когда сервер или база данных не доступна, переадресация происходит, когда Вы пытаетесь использовать Notes, чтобы исполнить некоторые действия. Следующая таблица описывает действия, при выполнении которых происходит переадресация.

Категория	**Действия пользователя приводящие к переадресации**
Операции открытия базы данных	Пользователь открывает базу данных с закладок рабочего пространства
	Если пользователь нажимает на связи с документом, связь с видом или связь с базой данных
	Пользователь активизирует поле, акцию или кнопку содержащую команду @command (FileOpenDatabase)
	Пользователь запускает процедуру LotusScript®, содержащую OpenWithFailover метод NotesDatabase class
	Пользователь использует процедуры Java™, OpenDatabase метода DbDirectory class
	Репликация базы данных в кластере серверов не происходит, из-за проблем в сети
Операции, связанные с подготовкой и отправкой сообщений	Отправка почтового сообщения
	Поиск имени адресата
	Автоматический поиск имени адресата, при вводе первых символов его имени
	Передача почтового сообщения
	Выполнение почтового агента

	Планирование встречи, события
	Поиск свободного времени пользователя
	Поиск сервера
Операции с Web сервером	Выбор пиктограммы Open URL
	Пользователь нажимает ссылку URL
	Пользователь вводит адрес URL в Web браузере

2.16.3.3 Когда не происходит переадресации в кластере?

*1065 Когда сервер становится недоступным, но пользователь уже открыл базу данных

Обратите внимание, что пользователь может открыть базу данных снова, но только реплику, если она существует в кластере серверов. Если пользователь редактировал документ, когда сервер стал недоступным, пользователь может копировать документ в другую реплику.

*1066 Когда пользователь выбирает из меню Файл – База данных – Свойства, или Файл – База данных – Открыть.

*1067 Когда Router пытается доставить почту, в то время как переменная MailClusterFailover установлена в 0 (ноль)

*1068 Когда сервер шаблонов недоступен, при создании новой базы данных

*1069 При запуске любого агента, кроме почтового агента Pre-Delivery.

*1070 Когда сервер пытается делать репликацию, но сервер партнер достигает ограничения, максимального числа пользователей на сервере, установленное администратором. Или если сервер пытается реплицироваться с базой данных, которая помечена как Out of Service.

2.16.3.4 Как Domino находит нужную реплику при переадресации?

Когда пользователь пробует открыть базу данных, которая не доступна, Cluster Manager просматривает базы данных Cluster Database Directory и ищет реплику этой базы данных. Чтобы найти реплику, Cluster Manager ищет базу данных, которая имеет тот же самый ID реплики, как и у первоначальной базы данных.

Если имеются больше чем одна реплика базы данных на сервере, Cluster Manager предполагает, что отобранные реплики используются для репликаций. Cluster Manager выбирает реплику, которая имеет тот же самый путь, как и первоначальная база данных. Поэтому, если Вы помещаете несколько реплик на сервере, убедитесь, что все реплики в кластере, имеют тот же самый путь. Иначе, пользователи могут терпеть неудачу, при доступе к различным репликам.

Когда на сервере происходит переадресация, Domino производит соответствующую запись в протоколах сервера.

2.16.3.5 Как работает балансировка нагрузки в кластере?

Распределяя базы данных по кластеру серверов, Вы балансируете рабочую нагрузку в Вашей системе, чтобы никакой сервер не был перегружен. Кроме того, имеются несколько переменных в файле NOTES.INI, которые Вы можете устанавливать, чтобы помочь кластеру балансировать рабочую нагрузку. Например, Вы можете определить предел занятости, определяя порог готовности для серверов. Когда сервер достигает порога готовности, Cluster Manager помечает сервер, значением BUSY. Когда сервер помечен значением BUSY, запросы на открытие базы данных посылаются другим серверам, которые содержат реплики требуемых баз данных. Вы можете также определить максимальное число пользователей, для доступа на сервер. Когда сервер достигает этого предела, пользователи будут переадресованы на другой сервер. Этими действиями Вы поддерживаете сбалансированную рабочую нагрузку, на Ваши сервера.

Когда пользователь пробует открывать базу данных, которая находится на BUSY сервере, Cluster Manager просматривает в базу данных Cluster Database Directory для поиска реплики базы данных. Он проверяет готовность серверов, которые содержат реплику, и переадресовывает пользователя на другой, менее занятой сервер. Если никакой другой сервер кластера не содержит реплики, или все сервера находятся в состоянии BUSY, первоначальная база данных будет открыта, даже если сервер будет в состоянии BUSY.

Пример

Этот пример описывает, как Domino выполняет балансирование рабочей нагрузки на Вашу систему. Этот кластер содержит три сервера. Server2 - в настоящее время занят, находится в состоянии BUSY, потому что рабочая нагрузка достигла порога его готовности. Cluster Managers на Server1 и Server3 знает, что Server2 в состоянии BUSY.

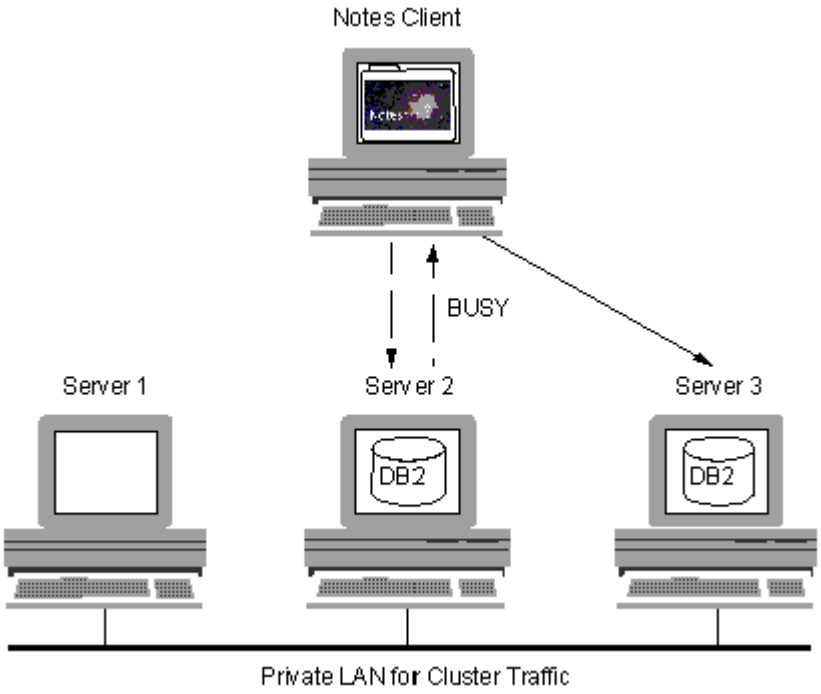


Рис. 54 Пример балансирования нагрузки на Domino сервера.

*1071 Пользователь Notes пытается открыть базу данных на Server2.

*1072 Domino посылает Notes сообщение, что сервер в состоянии BUSY.

*1073 Notes смотрит в кэш кластера, чтобы найти имена других серверов в кластере.

*1074 Cluster Manager определяет, какой сервер в кластере не занят и содержит реплику искомой базы данных.

*1075 Cluster Manager сообщает эту информацию Notes, и Notes открывает реплику.

2.16.4 Компоненты кластера.

Имеются несколько компонентов, которые работают вместе, чтобы кластер функционировал правильно. Они включают:

*1076 Cluster Manager

*1077 Cluster Database Directory

*1078 Cluster Database Directory Manager

*1079 Cluster Administrator

*1080 Cluster Replicator

*1081 Internet Cluster Manager

2.16.4.1 Cluster Manager.

Cluster Manager работает на каждом сервере в кластере. Этим действием он создается список серверов в кластере, в настоящее время доступных.

Когда Вы добавляете, сервер в кластере, Domino автоматически запускает задачу Cluster Manager на этом сервере. Пока сервер является частью кластера, Cluster Manager запускается каждый раз, когда Вы запускаете сервер.

Каждый Cluster Manager контролирует кластер. Cluster Manager определяет рабочую нагрузку и готовность другого сервера в кластере.

Задачи Cluster Manager занимаются следующим:

*1082 Определение, какие сервера принадлежат кластеру. Это делается периодически, контролируя Domino Directory на предмет изменений в поле ClusterName, Server документа и списков членов кластеров.

*1083 Контроль готовности сервера и рабочей нагрузки на кластер.

*1084 Информирование другого Cluster Managers, на предмет замен в кластере серверов и их готовности.

*1085 Переадресация запросов к базам данных, основанных на готовности серверов кластера.

*1086 Балансирование рабочей нагрузки на сервер в кластере.

*1087 Протоколирование переадресации и рабочей нагрузки, баланса в протоколах сервера.

Cluster Manager проверяет Domino Directory, чтобы определить, какой из серверов принадлежит к кластеру. Эта информация хранится в памяти КЭШа сервера (Cluster Name Cache). Cluster Manager использует эту информацию, чтобы обмениваться информацией, с другими Cluster Managers. Cluster Manager также использует Cluster Name Cache, для

хранения информации готовности серверов. Эта информация помогает Cluster Manager исполнить функции, балансирования рабочей нагрузки и для переадресации.

Чтобы рассматривать информацию, содержащуюся в Cluster Name Cache, введите на консоли сервера команду:

```
show cluster
```

2.16.4.2 Cluster Database Directory.

Cluster Database Directory – база данных CLDBDIR.NSF, которая находится на каждом сервере кластера. Cluster Database Directory содержит документ, для каждой реплики базы данных в кластере. Этот документ содержит информацию об имени базы данных, имени сервера, пути к базе данных, ID реплики. Компоненты кластера используют эту информацию, чтобы исполнить их функции.

2.16.4.3 Cluster Database Directory Manager.

Задача Cluster Database Directory Manager (CLDBDIR) на каждом сервере создает базу данных Cluster Database Directory и поддерживает ее актуальном состоянии. Когда Вы добавляете сервер в кластер, Cluster Database Directory Manager создает базу данных Cluster Database Directory на этом сервере. Когда Вы добавляете, какую либо базу данных на сервер в кластере, Cluster Database Directory Manager создает документ в базе данных Cluster Database Directory, который содержит информацию относительно новой базы данных. Когда Вы удаляете базу данных с сервера в кластере, Cluster Database Directory Manager удаляет этот документ. Cluster Database Directory Manager также отслеживает статус каждой базы данных, типа Out of Service или Pending Delete.

Когда имеется изменение в базе данных Cluster Database Directory, задача Cluster Replicator немедленно копирует это изменение на каждый сервер в кластере. Это гарантирует, что каждый член кластера имеет современную информацию относительно баз данных в кластере.

Cluster Administrator.

Cluster Administrator исполняет многие вспомогательные задачи, связанные с кластером. Например, когда Вы добавляете сервер в кластер, Cluster Administrator запускает задачи кластера, типа Cluster Database Directory Manager и Cluster Replicator. Он также добавляет имена задач CLDBDIR и CLREPL в переменную ServerTasks в файле NOTES.INI так, чтобы эти задачи запускались, каждый раз, когда Вы запускаете сервер. Cluster Administrator также запускает процесс администрирования, если он еще не работает. Когда Вы удаляете сервер из кластера, Cluster Administrator удаляет эти задачи из файла NOTES.INI и останавливает эти задачи, если они еще запущенны. Он также удаляет базу данных Cluster Database Directory на этом сервере и чистит записи сервера в кластере на других серверах.

Cluster Replicator.

Задача Cluster Replicator (CLREPL) постоянно синхронизирует данные среди реплик в кластере. Всякий раз, когда изменение происходят в базе данных в кластере, Cluster Replicator немедленно выталкивает изменение в другие реплики в кластере. Это гарантирует, что каждый раз, когда пользователь обращается к базам данных, они видит современную их версию. Cluster Replicator также копирует изменения личных папок, которые сохраняются в базе данных. Каждый сервер в кластере управляет одним Cluster Replicator по умолчанию, хотя Вы можете запускать и большее количество репликаторов, чтобы улучшить выполнение работ.

Cluster Replicator просматривает базу данных Cluster Database Directory (CLDBDIR.NSF), чтобы определить, какие базы данных, имеют реплики на других серверах, членах кластера. Cluster Replicator хранит эту информацию в памяти и использует ее, чтобы копировать изменения на другие сервера. Когда Cluster Replicator обнаруживает изменения в базе данных Cluster Database Directory, он модернизирует информацию в памяти.

Задача Cluster Replicator выталкивает изменения только на серверах кластера

2.16.5 Как работает кластерный репликатор?

Cluster Replication запускается чаще чем стандартный репликатор работающий по расписанию. Когда Cluster Replicator узнает об изменении в базе данных, он немедленно выталкивает это изменение в другие реплики в кластере. Если все-таки имеется разница в репликах, Cluster Replicator хранит их в памяти, пока не сможет их вытолкнуть на другие сервера в кластере. Если изменение в той же самой базе данных происходит прежде, чем предыдущее изменение было послано, Cluster Replicator объединяет эти изменения и посылает их вместе, чтобы экономить время обработки.

Потому что Domino хранит изменения реплик только в памяти, источник предназначение должен быть доступен для репликаций. Если сервер назначения не доступен, Cluster Replicator продолжает хранить изменения в памяти, пока сервер назначения не станет доступен.

Если сервер источник закрывается прежде, чем репликация заканчивается, изменения в памяти будут утеряны. По этой причине, Вы должны использовать стандартный репликатор, т.е. задачу REPLICA, чтобы исполнить немедленные репликации со всеми членами кластеров всякий раз, когда Вы повторно начинаете использование сервер кластера. Это также хорошая идея наметить репликации между серверами в кластере на регулярной основе, например один раз в час, гарантируя Вашим базам синхронизацию.

Когда Cluster Replicator регистрирует случай изменения любой базы данных, которые ожидают синхронизации, событие будет зарегистрировано в Replication Log. Это позволяет Вам видеть, какие базы данных в настоящее время не синхронизированы, и просматривать ошибки репликаций. После того, как ошибки исправлены и успешно закончена репликация, информация об ошибке больше не появится.

Cluster Replicator не обрабатывает формул репликаций стандартного репликатора. Потому что эти формулы могут использовать много ресурсов для обработки, чтобы минимизировать использования репликатора кластера. Если Вы используете выборочные репликации, база данных может временно получить документы, которые не соответствуют формуле отбора. Domino удаляет эти документы, когда Вы запускаете стандартный репликатор.

Кроме того, Cluster Replicator не обрабатывает назначения в группе Дополнительно, в окне установок репликаций. Поэтому, Вы не можете запретить репликации определенных элементов базы данных, типа ACL или агентов. Cluster Replicator всегда пытается делать все реплики идентичными, чтобы пользователи не заметили, что они обращаются к другим репликам.

Предостережение. Кластерный репликатор не может автоматически удалять изменения в определенных элементах баз данных, типа ACL, агентов. При ограничении репликаций этих элементов, важно для базы данных, рассмотреть использование только стандартного репликатора.

История репликации в кластере.

Потому что события репликаций происходят очень часто в кластере, Cluster Replicator не пишет истории репликации базы данных, каждый раз, когда происходит реплика баз данных. Cluster Replicator записывает информацию об истории реплик, приблизительно один раз в час.

Репликации личных папок в кластере.

Стандартный репликатор не копируют содержание и сами личные папки. В пределах кластера, однако, частные папки копируются в другие реплики в пределах кластера серверов. Это поведение кластер репликатора гарантирует Вам полную идентичность баз данных.

К личным папкам возможен доступ только создателям папки или серверам в пределах кластера. Только сервер определенный как сервер, или входящий в состав группы серверов, в списке контроля управления доступа к базе данных, может получить доступ и копировать лучные папки в пределах базы данных. Сервера, которые явно не включены в ACL, не могут копировать личные папки.

2.16.6 Перенаправление почты в кластере.

Если Вы создаете реплики почтовых баз данных в кластере серверов, то перенаправление пользователей к другим репликам происходит в следующих случаях:

*1088 Когда пользователь пробует открыть почтовую базу данных, которая является недоступной.

Перенаправление для почты работает так же как с любой базой данных

*1089 Когда пользователь пробует послать сообщение после того, как почтовый сервер пользователя стал недоступен

Если пользователь составляет сообщение, в то время когда его почтовый сервер недоступен, пользователь может все еще послать сообщение, если имеется реплика базы данных почты пользователя в кластере. Доставка терпит неудачу, если другой сервер в кластере, передает сообщение в MAIL.BOX.

*1090 Когда Router пробует доставить почту на сервер, который является недоступным в настоящее время

Если сервер, который содержит базу данных почты, недоступен, Router доставляет почту на сервер в кластере, который содержит реплику базы данных почты. Router использует следующий процесс, чтобы найти правильную базу данных почты.

Сначала Router проверяет, позволяется ли почте перенаправление для локального сервера, и находится ли почтовая база пользователя на другом сервере в кластере. Если локальный сервер находится в том же самом кластере, и имеет реплику почтовую базу данных пользователя, Router доставляет почту эту базу данных. Иначе, он запрашивает доступный член кластера относительно серверов, которые содержат реплики почтовой базы пользователя, и доставляет почту в эту базу данных. Если не имеется никакой доступной реплики, Router снова пробует доставить почту на почтовый сервер пользователя.

*1091 Когда пользователь использует Shared Mail

Вы можете получить доступ к базе данных сообщений Shared Mail, из каждой реплики почтовой базы данных таким же самый образом, как и к первичной почтовой базе данных. Когда Cluster Replicator реплицирует почтовые базы данных, он также реплицирует и

заголовки сообщений в почтовую базу данных пользователя, и тело сообщения в базу данных Shared Mail.

2.16.7 Как работает календарное планирование в кластере?

Domino поддерживает кластеринг календарей и баз данных Free Time. Когда кластерная система планирования работает, она немного по-другому выполняет работу, чем система не использующая кластер. Однако, эти различия не заметны для пользователей.

Каждый сервер, работающий вне кластера, содержит базу данных, с информацией планирования для всех пользователей, кто используют это сервер как почтовый сервер. Эта база данных имеет название BUSYTIME.NSF и известна как база данных свободного времени. Для серверов в кластере, имеется отдельная база данных свободного времени, для каждого пользователя. Эта база данных имеет название CLUBUSY.NSF и содержит всю информацию, о свободном времени, на всех серверов в кластере. Каждый сервер кластера содержит реплику этой базы данных.

Когда Вы добавляете сервер в кластер, Schedule Manager удаляет базу данных BUSYTIME.NSF на сервере, создает базу данных CLUBUSY.NSF, которая реплицируется на другие сервера в кластере. Когда пользователь в кластере ищет свободное время, сервер просматривает собственную базу CLUBUSY.NSF сначала, чтобы найти информацию для каждого пользователя в кластере. Для пользователей, чей почтовый сервер находится - вне кластера, запрос посылается этому серверу. Когда пользователь вне кластера делает запрос об информации пользователя в кластере и запрос терпит неудачу, запрос передается другому серверу в кластере. Всякий раз, когда имеется информация в CLUBUSY.NSF на любом сервере в кластере, Cluster Replicator реплицирует все изменения на другие сервера в кластере.

Когда Вы удаляете сервер из кластера, задача Schedule Manager удаляет CLUBUSY.NSF с сервера и создает новую базу BUSYTIME.NSF на сервере. Schedule Manager на каждом сервере в кластере, удаляет информацию из реплики CLUBUSY.NSF.

Обратите внимание, имеете ли вы версии 4.5 или 4.6 серверов в кластере. Эти сервера имеют BUSYTIME.NSF базу данных. Эти базы данных не преобразовываются в CLUBUSY.NSF. Планирования календаря для этих серверов в кластере, работает так же, как и на серверах, не объединенных в кластер.

2.16.8 Выделенная сеть для кластера, нужно ли это?

Чтобы сделать работу сильно загруженный серверов кластера более эффективной, Вы можете создать выделенную сеть, для использования Вашим кластером. Чтобы сделать это, устанавливаете дополнительные сетевые карты в каждый сервер кластера и соедините карты через отдельный сетевой концентратор.

Главная причина для создания выделенной сети для Вашего кластера состоит в том, чтобы отделить сетевое движение данных, от кластерных репликаций и передачи вспомогательных данных, между серверами кластера. Выделенная сеть может существенно разгрузить Вашу первичную сеть. Если Вы ожидаете тяжелые кластерные репликации, Вы должны создать выделенную сеть для кластера.

Вы можете также рассматривать создание выделенной сети с использованием интранет, чтобы гарантировать, что сервера кластера остаются на связи друг с другом, даже, когда происходят некоторые проблемы в сети. Добавляя выделенную сеть, все сервера в кластере связаны, по крайней мере, двумя разными сетями. При этом если одна из сетей отказывает,

имеется все еще сеть и соединение между всеми серверами в кластере. Это гарантирует Вам, что сервера кластера остаются связанными друг с другом, и что Cluster Replicator продолжает держать синхронизированными базы данных.

Если Вы создаете выделенную сеть для Вашего кластера, все члены кластера должны быть связаны, и с выделенной для кластера сетью, и с первичной сетью, для доступа клиентов.

2.16.9 Создание кластера серверов Domino.

Прежде, чем Вы создаете кластер, выполняете следующие задачи:

*1092 Определите сервера, которые будут входить в кластер и их названия.

*1093 Установите или модернизируйте программное обеспечение до Domino R5, с лицензией Enterprise Server на каждом сервере. Эта лицензия позволяет Вам установить сервера Domino R5 в кластер.

Примечание. Вы можете включать сервера в кластер и версии Domino R4.5, R4.6 с лицензией Advanced Services и Domino 4.62 с лицензией Enterprise Server. Однако эти сервера не будет иметь доступа к новым функциям кластера, которые появились в Domino R5.

*1094 Убедитесь, что Вы рассмотрели требования для кластера и что все сервера отвечают этим требованиям.

*1095 Распределите базы данных и реплики на серверах, которые Вы планируете включать в кластер.

*1096 Наметьте репликации между серверами кластера

Чтобы создавать кластер, Вы должны иметь, по крайней мере, доступ автора, с правом удаления документов в Domino Directory и, по крайней мере, доступ автора в базе данных Administration Requests. Если возможно, использование сервер администрирования при создании кластера. Это заставит быстрее обрабатывать запросы администрирования. Сервер администрирования не должен быть частью кластера.

Обратите внимание. Если сервера принадлежат различным кластерам, Вы не должны удалить их из этих кластеров. Cluster Administration Process сначала удалит сервер из первоначального кластера, а затем добавит его к новому кластеру.

*1097 Из клиента Domino Administrator удостоверитесь, что сервер администрирования или другой сервер является текущим.

*1098 Выбирайте закладку Настройка.

*1099 Выбирайте сервер, который Вы хотите добавить к кластеру.

*1100 Нажмите кнопку Add to Cluster.

*1101 На запрос выбора кластера, выбирайте – Create New Cluster, затем – OK.

*1102 Введите имя нового кластера и нажмите – OK.

*1103 Выбирайте - Да, чтобы добавить серверу к кластеру немедленно, или выбирайте – Нет, чтобы предоставить процессу администрирования, добавить сервер к кластеру.

2.16.10 Как убедиться, что кластер создан и работает корректно?

Вы можете делать следующий, чтобы проверить, что кластер был создан правильно.

Действие	Что Вы должны видеть
Из клиента Domino Administrator, выбирайте закладку Настройка, затем откройте секцию Кластер и выбирайте представление Кластеры.	Вы должны видеть имя кластера, сопровождаемое именем сервера кластера.
Выбирайте и откройте Server документ сервера, который Вы добавили в кластер.	Вы должны видеть имя кластера на закладке Basics, в поле Cluster Name.
Из клиента Domino Administrator, выбирайте закладку Сервер – Состояние.	В списке задач вы должны видеть запущенные задачи кластера: *1104 CLDBDIR (Cluster Database Directory Manager) *1105 CLREPL (Cluster Replicator)
Из клиента Domino Administrator, выбирайте закладку – Файлы.	В списке баз данных должна присутствовать база Cluster Directory (R4) (cldbdir.nsf), которая создается задачей Cluster Database Directory.
Сравните ID реплики базы данных Cluster Database Directories на каждом сервере кластера.	Вы должны иметь одинаковый ID реплики на каждом сервере кластера.

Вы можете также запустить Cluster Analysis, чтобы посмотреть полученные сообщения на предмет любых проблем в конфигурации кластера.

2.16.11 Запуск инструмента анализа кластера.

Когда Вы запускаете Cluster Analysis, Вы принимаете решение о типе сообщений, которые хотите создавать и типе детализации, которые хотите видеть в сообщениях. Во время, когда анализ кластера будет работать, будут появляться сообщения статуса в статусной строке. Для больших, занятых кластеров, анализ кластера может требовать нескольких часов или больше. Если Вы не имеете выделенный сервер для выполнения анализа, запускайте эту процедуру в течение не пиковых нагрузок.

*1106 Из клиента Domino Administrator, выберите сервер, на котором Вы хотите запустить анализ.

*1107 Выбирайте закладку Сервер – Анализ.

*1108 В стекле инструментов, выбирайте - Сервис – Анализ – Кластер…

*1109 Заполните любые поля и выбирайте нужные Вам типы отчетов и нажимайте ОК, для запуска анализа кластера серверов.

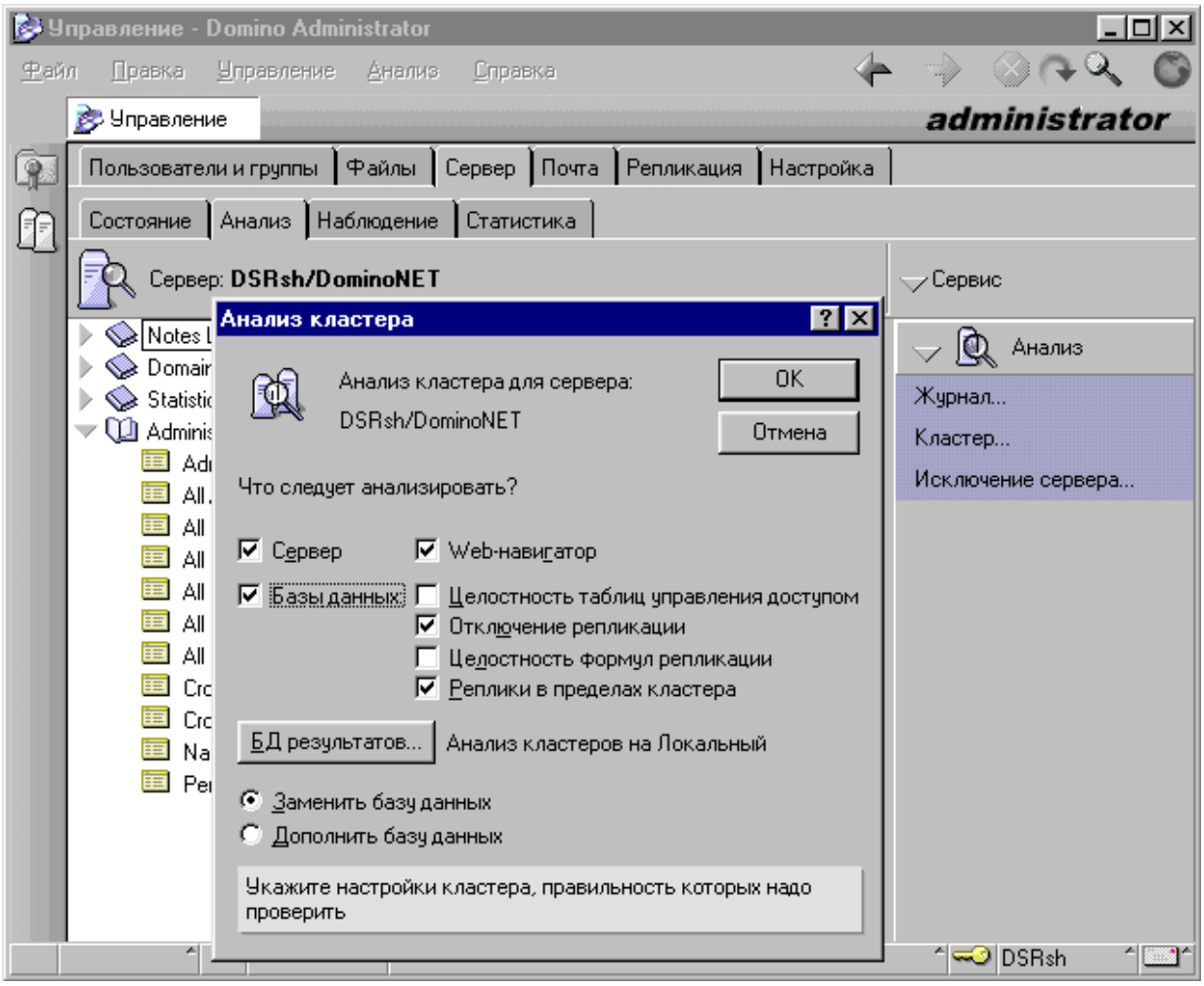


Рис. 55 Диалоговое окно настройки анализа кластера Domino сервера.

2.16.12 Управление доступом пользователей к базам данных.

Пользователи должны иметь те же самые права доступа во всех репликах баз данных в кластере. Иначе, пользователи не будут получать соответствующего доступа к репликам, для которых они имеют меньшее количество прав доступа. Они могут быть лишены доступа совсем, или они не смогут увидеть те же самые документы, не смогут выполнить те же самые действия, как в оригинальной базе данных, которую они использовали.

2.16.12.1 Поддержка ACL баз данных в кластере.

Один способ убедиться, что списки контроля и управления доступа синхронизированы во всех репликах, состоит в том, чтобы использовать следующую процедуру для каждой базы данных:

*1110 Выбирайте из меню Файл – База данных – Управление доступом.

*1111 Выбирайте закладку Дополнительно.

*1112 Выбирайте опцию Использовать единую таблицу управления доступом для всех реплик и затем – OK.

Эта установка гарантирует, что ACL всех реплик будет идентична.

Другой способ держать ACL баз данных, в синхронизированном состоянии, состоит в том, чтобы дать всем серверам кластера, доступ менеджера для всех баз, данных в кластере. Это гарантирует, что каждый сервер может модернизировать ACL каждой базы данных. Так что изменения в ACL одной реплики, будет автоматически копировать в другие базы данных, пока Вы не запретите репликации ACL для базы данных.

Чтобы дать доступ менеджера серверам кластера, для всех баз данных, Вы можете создать группу в Domino Directory, в которую включите все сервера кластера. Добавьте эту группу в ACL каждой базы данных и дайте ей доступ менеджера.

Важно, чтобы сервера кластера имели адекватный доступ, так чтобы они могли копировать все данные из одной реплики в другую. Если имеются любые ограничения в одной из реплик, то некоторая информация не будет доступна пользователям, когда происходит отказ одного из серверов. Поэтому, убедитесь, что сервера не только имеют доступ менеджера, но и что они могут копировать все данные, без ограничений.

Личные папки копируются по-другому в кластере, чем при использовании обычного репликатора. Обычно, личные папки и их содержание не копируют в течение репликаций сервер - сервер, но копируются в течение репликаций сервер - клиент. В кластере, личные папки копируются от сервера к серверу, чтобы пользователи могли получить доступ к своим личным папкам, в случае они одна из реплик становится недоступной. Чтобы гарантировать, что личные папки копируются между серверов в кластере, убедитесь, что установили тип пользователя для серверов в ACL баз данных Server или Server group.

2.16.12.2 Управление другими назначениями, которые ограничивают доступ к базам данных.

Имеются методы ограничения доступа к базам данных, в дополнение к ACL. Они включают следующее:

*1113 Ограничения для серверов. Разрешается или запрещается доступ сервера, в списках из Domino Directory

*1114 Списки доступа, для связей с базами данных или каталогами

*1115 Списки читателей, документов, представлений и папок

Например, если сервера в кластере содержит базу данных или связи с каталогами, которые имеют списки доступа, убедитесь, что сервера кластера находится в списках доступа. Иначе, они не будут иметь доступ к этим базам данных или каталогам, и не будут способны реплицировать данные с этими базами данных, даже если они имеют доступ менеджера в ACL.

Если документ в базе данных имеет поле Readers, сервера кластера должна быть внесены в список этого поля, или сервера не будут иметь доступ к этому документу, и не будут способны копировать этот документ. Это относится и к спискам доступа к папкам, представлениям.

2.16.13 Настройка почты в кластере.

Маршрутизация Почты терпит неудачу, если сервер почты получателя не доступен, когда Router пытается доставить почту. Пока почтовый сервер находится в кластере, Router доставляет почту другому серверу кластера, который содержит реплику почтовой базы данных получателя. Таким образом, получатель продолжает получать почту.

Предоставление возможности, перенаправления маршрутизации почты особенно полезно, если Вы используете Hub сервер для маршрутизации почты. Если этот Hub сервер становится недоступен, но он находится в кластере, Router доставляет почту другому Hub серверу кластера, и этот сервер посылать сообщение серверу назначения.

В следующем примере, Mail Server1 посылает сообщение на Mail Server2. Сервер делает попытку маршрутизации через Hub1, который является маршрутизатором для Mail Server2. В настоящее время Hub1 является недоступным. Потому что Hub1 находится в кластере, Domino маршрутизирует сообщение на сервер Hub2, который маршрутизирует сообщение на почтовый сервер пользователя - Mail Server2.

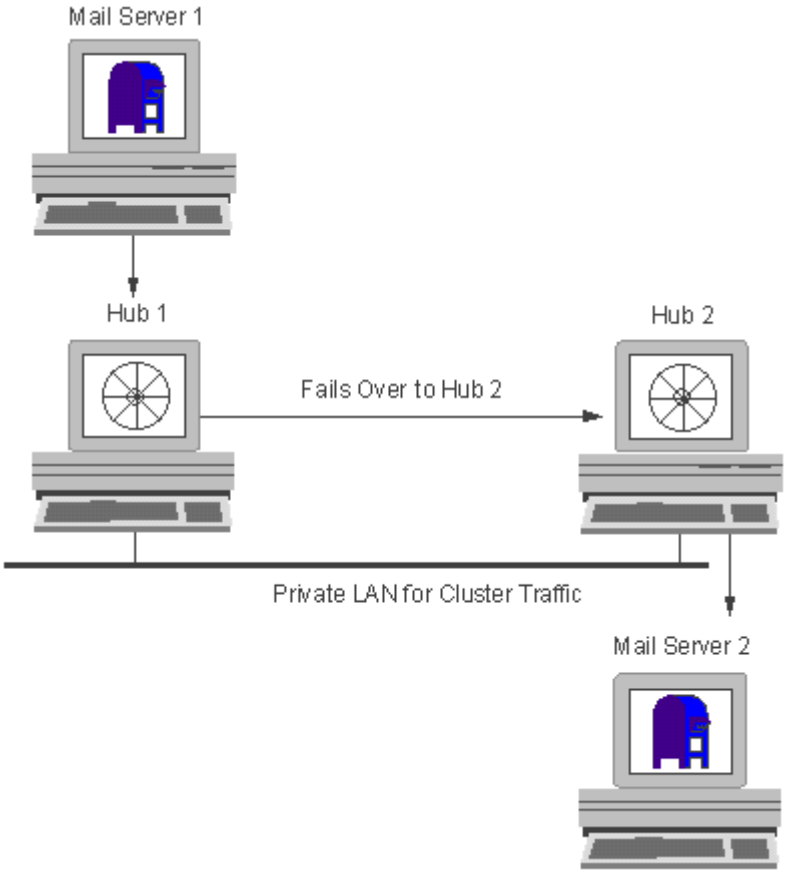


Рис. 56 Применение кластера для Hub серверов.

2.16.13.1 Изменение маршрутизации почты при отказе одного из серверов.

Чтобы изменять маршрутизацию почты по умолчанию при отказе одного из серверов, сделайте следующее изменение в Configuration документе, для каждого сервера в кластере, и каждом сервере в домене, который может маршрутизировать почту.

*1116 Из клиента Domino Administrator, выбирайте закладку Настройка, выбирайте представление Почта – Конфигурации.

*1117 Выбирайте нужный документ и откройте его для редактирования.

*1118 Выбирайте закладку Router/SMTP – Advanced – Controls.

*1119 В поле Cluster failover, выберите один из следующего:

- **Disabled** - запрещается

- **Enabled for last hop only** - (по умолчанию) разрешается только для последнего перелета
- **Enabled for all transfers in this domain** – разрешается для всех перемещений для этого домена

*1120 Сохраните и закройте Configuration Settings документ.

Обратите внимание, что это установка воздействует только на доставку почты клиенту, но не затрагивает рассылку сообщений от клиента, когда почтовый сервер недоступен. Если пользователь посылает сообщение и его почтовый сервер недоступен, доставка терпит неудачу.

2.16.13.2 Использование Shared Mail в кластере.

Вы можете использовать Shared Mail в кластере. Когда Вы делаете это, Cluster Replicator помещает тела сообщений в базу данных Shared Mail на сервер назначения, а заголовки сообщений в почтовые базы пользователей.

Чтобы установить Shared Mail в кластере, Вы используете ту же самую процедуру, которую Вы используете для организации репликаций Shared Mail, которые не находятся в кластере. Эта процедура включает всегда команду Load Object Set. Вы делаете это на каждом сервере в кластере, который содержит реплику почтовой базы данных. Когда Вы используете Shared Mail в кластере, Cluster Replicator распределяет почту базы данных Shared Mail на каждом сервере кластера.

2.16.14 Использование стандартного репликатора в кластере.

Вы должны использовать стандартные репликации на регулярной основе в кластере, чтобы убедиться, что все базы данных современны. Это особенно важно после аварий сервера.

2.16.14.1 Реплики по расписанию в кластере.

Это хорошая идея наметить репликации и запускать их, например, однажды час, что все базы данных были синхронизированы. Имеются много причин для запуска репликаций в кластере:

*1121 Реплицировать изменения, которые могут быть потеряны, когда сервер в кластере терпит крах.

Потому что события изменений репликаций кластера сохраняются только в памяти, они могут быть потеряны, когда сервер аварийно закрывается. Никакие данные не теряются, но события изменений репликаций кластера, теряются. Для синхронизации данных в репликах Вы запустите стандартный Domino репликатор.

*1122 Реплицировать базы данных, для которых Вы запретили репликации кластера

Вы можете иметь базы данных, которые Вы хотите реплицировать, но не на очень частой основе. Чтобы видеть, реплицируется ли база данных Cluster Replicator, обратитесь к полю Cluster Replication в базе данных Cluster Database Directory.

*1123 Репликации базирующиеся на критериях отбора по формулам

Cluster Replicator оставляет обработку формул отбора стандартному репликатору. Перед использованием формул отбора в кластере, Вы должны знать то, как они воздействует на репликации кластера.

*1124 Репликация реплики, которые находятся на том же самом сервере

Cluster Replicator выталкивает изменения на другой сервер в кластере, который содержит реплики, но не модернизирует одинаковые реплики на собственном сервере.

Обратите внимание. Если имеются несколько копий реплик на Вашем сервере, Cluster Manager использует оригинальный путь базы данных, чтобы выбрать реплику для пользователя и открыть ее в течение Failover. Если Вы помещаете многократные реплики в сервер, убедитесь, что все реплики в кластере, используют те же самые критерии формул отбора, и имеют тот же самый путь, что и оригинальные базы данных. Иначе, пользователи могут получить доступ в различные реплики, в процессе переадресации на другой сервер.

Чтобы убедиться, что все базы данных являются современными, хорошая идея реплицировать их всякий раз, когда Вы запускаете сервер. Вы можете создавать Program документ в Domino Directory, чтобы выполнять эту функцию.

2.16.14.2 Запрещение кластерных репликаций.

В кластере, все базы данных автоматически реплицируются в реальном масштабе времени, для синхронизации данных в базах данных. Однако репликации в реальном масштабе времени необходимы только для тех баз данных, которые требуют постоянной синхронизации. Для других баз данных, Вы можете запрещать кластерные репликации. Вы можете также запрещать кластерные репликации временно, чтобы исследовать некоторые проблемы. Вы можете запрещать кластерные репликации для всех баз данных, или для определенных баз данных на сервере. Эти установки не имеет никакого влияния на обычные, намеченные репликации, которые будут функционировать как обычно.

Запрещение кластерных репликаций для определенных баз данных.

*1125 Из клиента Domino Administrator, выбирайте закладку Настройка.

*1126 Откройте представление Кластер – Cluster Directory (R5).

*1127 Выбирайте одно из представлений:

- Databases by Pathname
- Databases by Replica ID
- Databases by Server

*1128 В представлении, выберите базы данных, для которых Вы хотите запретить репликации кластера.

*1129 Нажмите кнопку Tools… и выбирайте значение Disabled Cluster Replication on Selected Databases.

Примечание, чтобы просмотреть каким из баз данных разрешается кластерная репликация, а каким запрещается, выбирайте представление Databases by Pathname, колонку Cluster Replication.

Запрещение кластерных репликаций, для базы данных, запрещает только репликации этой базы данных на другие сервера в кластере. Эта установка не запрещает репликации в эту

базу данных с других серверов кластера. Запрещение кластерных репликаций, не имеет никакого влияния на стандартные репликации.

Создание агента, для запрещения кластерных репликаций для определенных баз данных.

Если Вы имеете много баз данных, для которых Вы не хотите использовать Cluster Replicator, Вы можете создать агента, чтобы запретить репликации кластера для этих баз данных.

*1130 На сервере администрирования кластера, откройте базу данных Cluster Database Directory (CLDBDIR.NSF).

*1131 Из меню выбирайте Создание – Агент…

*1132 В поле имени, введите имя агента.

*1133 В поле Когда этот агент должен выполнятся?, выберите значение Вручную из меню Действия.

*1134 В поле, Какие документы агент обрабатывает, выбирайте значение Выделенные документы.

*1135 В поле Запуск, выбирайте - Простые действия.

*1136 Нажмите кнопку Добавить действие.

*1137 В поле Действие, выбирайте значение Изменить поле.

*1138 Выбирайте поле ClusterReplicate.

*1139 В поле Значение, введите значение - 0 (ноль).

*1140 Выбирайте опцию Заменить значение, нажимайте – OK, сохраните агента.

*1141 Выбирайте базы данных, для которых Вы хотите запретить кластерные репликации, и затем запускайте агента из меню Действия.

Запрещение кластерных репликаций, для всего сервера.

Чтобы завершить задачу Cluster Replicator на сервере, делайте одно из следующего:

Из клиента Domino Administrator

*1142 Выбирайте закладки Сервер – Состояние.

*1143 В панели инструментов, выбирайте - Сервис – Задача – Stop.

Остановка репликатора с консоли сервера.

На консоли сервера введите следующее:

```
Tell clrepl quit
```

Эта команда останавливает задачу Cluster Replicator в течение активной сессии сервера. Следующий раз, когда Вы запускаете сервер, Cluster Replicator запускается снова.

Обратите внимание, что запрещение задачи CLREPL запрещают только репликации с этого сервера на другие сервера. Этим Вы не запрещаете обычные репликации с сервера на другие сервера кластера.

2.16.14.3 Разрешение протоколирования, для кластерных репликаций.

Чтобы позволять протоколирование событий кластерных репликаций, введите строку в файл NOTES.INI:

```
RTR_LOGGING=n
```

Где возможные значения для n:

1 - разрешение протоколирования событий кластерных репликаций

0 - запрещение протоколирования событий кластерных репликаций.

2.16.15 Установка выделенной сети LAN для Вашего кластера

Использование выделенной сети LAN для Вашего кластера отделяет кластерное движение данных сервера, репликаций в кластере, от остальной части Вашей сети. При использовании выделенной сети для кластера серверов разгружает Вашу первичную сеть.

Следуйте этой процедурой, чтобы установить выделенную сеть для Вашего кластера.

*1144 Установите дополнительную сетевую карту в каждом сервере кластера. Эти карты должны быть связаны, через выделенный концентратор и использовать отдельный кабель для связи.

*1145 Сконфигурируйте сеть LAN, для использования TCP/IP.

*1146 Назначьте второй IP адрес каждому серверу. В кластере, использующем два сервера, например, Вы могли бы использовать адреса 192.168.64.1 и 192.168.64.2.

*1147 Назначьте имена хостов, для новых адресов IP, в файле HOSTS или DNS. В кластере, использующем два сервера, например, Вы могли бы назвать сервера как – ACME_CLU и ACME2_CLU. Записи в файле HOSTS могли бы быть такими:

```
192.168.64.1      ACME_CLU

192.168.64.2      ACME2_CLU
```

*1148 Проверьте, что выделенная сеть LAN работает. Проверьте, каждый сервер кластера с использованием утилиты PING, с использованием IP адреса и имен хостов.

*1149 Определите новые порты в Server документе на закладке Ports, для каждого члена кластера и разрешите использование этих портов.

Например. Добавьте следующую информацию.

```
Port=CLUSTER

Notes Network=Cluster Network

Net Address=ACME_CLU

Enabled=ENABLED
```

*1150 Назначьте каждому порту IP адрес соответствующей подсетей и разместите эту информацию в файле NOTES.INI, в следующем формате:

```
PORT1_TCPIPADDRESS=0,b.c.d:1352

PORT2_TCPIPADDRESS=0,e.f.g.h:1352
```

Где PORT1 и PORT2 - имя порта, a.b.c.d и e.f.g.h - IP адреса для портов.

Пример. Если Вы имеете порты, с именами TCPIP и CLUSTER, эти строки мог бы быть следующие:

```
TCPIP_TCPIPADDRESS=0,192,114,32,5:1352

CLUSTER_TCPIPADDRESS=0,192.168.64.1:1352
```

*1151 Добавить следующую строку в файл NOTES.INI:

```
Server_Cluster_Default_Port=Cluster Port
```

Где Cluster Port - порт, который Вы создали для кластера.

Пример.

```
Server_Cluster_Default_Port=CLUSTER
```

Примечание. Вы может использовать Configuration Settings документ сервера, чтобы модернизировать файл NOTES.INI на всех серверах в кластере.

*1152 Перезапустите сервер.

Как убедится, что Domino использует выделенную сеть LAN?

Чтобы убедится, что Domino использует выделенную сеть LAN, Вы можете сделать следующее:

*1153 Введите на консоли сервера:

```
show cluster
```

*1154 В результатах, ищите строку - Server cluster default port: Cluster Port.

Cluster Port - порт, который Вы создали для кластера. В этом примере, эта строка была бы такой:

```
Server cluster default port: CLUSTER
```

Как удостоверится, что репликации кластера используют выделенную сеть LAN?

Это хорошая идея проверить кластер, чтобы убедиться, что репликации кластера используют выделенную сеть LAN. Чтобы сделать это, Вы можете смотреть некоторую статистику кластера.

*1155 Из клиента Domino Administrator, выбирайте закладку Сервер – Статистика.

*1156 Выбирайте секцию NET.

*1157 Откройте секцию с именем порта, который Вы определили для кластера.

*1158 Ищите следующую статистику для выделенного порта сети:

- BytesReceived
- BytesSent

*1159 Выбирайте секцию Replica – Cluster.

*1160 Выбирайте секцию SessionBytes и ищите следующую статистику для кластера:

- In
- Out

*1161 Сравните значения NET.portname.BytesReceived со значением Replica.Cluster.SessionBytes.In.

Эти значение должно быть близки друг к другу, хотя они не будут те же самыми.

*1162 Сравните значения NET.portname.BytesSent со значением Replica.Cluster.SessionBytes.Out.

Эти значения должны также быть близки друг к другу. Они не будут соответствовать точно, потому, что выделенная сеть используется не только репликаторами кластера.

2.16.16 Балансировка рабочей нагрузки на кластер

После контроля Вашего кластера и определения, что Вы хотите сделать в настройках, Вы можете делать следующее, чтобы лучше сбалансировать рабочую нагрузку на сервера в кластере:

*1163 Ограничите рабочую нагрузку на сервера, изменяя порог готовности сервера

*1164 Измените настройку максимального числа пользователей на сервере

*1165 Переместите базы данных на другой сервер

*1166 Создайте большее количество реплик занятых баз данных

*1167 Добавьте один или большее количество серверов к кластеру

Имейте в виду, что балансирование рабочей нагрузки не является решением недостатка мощности серверов в Вашей организации. Если Ваши Domino сервера сильно загружены и не имеется никаких дополнительных серверов, чтобы распределить нагрузку, то балансирование рабочей нагрузки не решит проблему. Балансировать рабочую нагрузку Вы должны, если имеются некоторые сервера, на которых постоянная загрузка сервера ниже, чем на других серверах

2.16.17 Ограничение рабочей нагрузки сервера

Чтобы лучше сбалансировать рабочую нагрузку между серверами в Вашем кластере, Вы можете ограничивать рабочую нагрузку каждого сервера, регулируя порог готовности сервера. Когда рабочая нагрузка сервера достигает порога готовности сервера, сервер будет обозначен как BUSY, занят. При этом запросы на доступ к серверу, будут перенаправляться на другой сервер в кластере. Если никакой другой сервер не будет доступен в это время, первоначальный сервер будет принимать запрос, даже если он находится в состоянии BUSY.

Чтобы определять, является ли сервер в состоянии BUSY, Domino сравнивает порог готовности сервера, с индексом готовности сервера, который является мерой текущей рабочей нагрузки на сервере. Когда порог готовности равен, или больше чем порог готовности, сервер переходит с состояние BUSY.

Обратите внимание, что порог готовности не затрагивает репликации. Репликации происходят даже, когда сервер находится в состоянии BUSY.

2.16.18 Индекс готовности сервера

Каждый сервер в кластере периодически определяет собственную рабочую нагрузку, основанную на среднем времени ответа запросов, которые сервер недавно обработал. Рабочая нагрузка отображается как число от 0 до 100, где 0 указывает, что сервер тяжело загружен, а 100 указывает слегка загруженный сервер. Это число называется индексом готовности сервера. Если увеличивается время ответа сервера, уменьшается индекс готовности сервера.

Диапазон чисел от 0 до 100 индекса готовности не процент производительности. Вместо этого, индекс готовности определяется как сравнение времени ответа текущей загрузки, со временем ответа той же самой функции, но с легкой грузкой и затем это значение вычитается из 100. Например, если база данных открывается за 3 секунды, но затрачивает только 0,3 секунды, при оптимальных условиях, индекс готовности будет равен выражению:

```
100-3/0,3
```

Таким образом, индекс готовности - 90.

Индекс готовности измеряет только время ответа сервера, который является обычно только маленькой частью времени ответа клиентам. Например, ответ сети между клиентом и сервером часто составляет существенную часть, ответа времени клиенту. Так, хотя индекс готовности и указывает - 90, опыт показывает, что время ответа сервера непосредственно в 10 раз больше, чем оптимальное значение времени.

2.16.18.1 Выбор порога готовности сервера

Настройка порога готовности сервера на каждом сервере - ключевой фактор в балансировании рабочей нагрузки в кластере. Настройка слишком высокого порога готовности сервера, может кончаться слишком частыми переадресациями запросов на другие сервера. Настройка слишком низкого значения этого порога, будет понижать эффективность использования Вашего сервера.

Чтобы определять надлежащее значение для порога готовности сервера, делайте следующее:

*1168 В течение периодов нормальных и тяжелых нагрузок на сервер, используйте один из следующих методов наблюдения за индексом готовности сервера:

- В панели серверов, из клиента Domino Administrator, выбирайте правой клавишей, свойства сервера и затем выбирайте закладку Кластер.
- Из клиента Domino Administrator, выбирайте закладку Сервер – Статистика и затем в списке статистики, выбирайте – Server.
- В консоли сервера, введите следующие команды:

```
show cluster

show stat server
```

- Из клиента Domino Administrator, выбирайте закладку Сервер – Анализ. Выбирайте имя сервера статистики, если оно доступно. Выбирайте представление Statistics Reports – Cluster.

- Вы можете просматривать представление Statistics Reports – Cluster из базы данных статистики STATREP.NSF.

- Если Ваш сервер работает под управлением WindowsNT, используйте Perfomance Monitor WindowsNT, чтобы проверить статистику с именем Server.AvailabilityIndex.

*1169 Установите начальный порог готовности, основанный на результатах Вашего наблюдения. Рассмотрите следующее, при настройке этого значения:

- Значение должно быть немного ниже конечного значения, которые Вы наблюдали, при исследованиях в Вашей системе.

- Повышайте или понижайте число порога готовности, приспосабливая ее к конкретному серверу.

- Когда какой либо сервер в кластере терпит крах, его рабочая нагрузка распределяется среди всех серверов в кластере. Если имеется только два сервера в кластере с одинаковой рабочей нагрузкой, то при отказе одного из серверов, рабочая нагрузка на другой, увеличится на 100%. Если имеется шесть серверов в кластере и один из серверов откажет, увеличение нагрузки на оставшиеся сервера ожидается только на 20%. Поэтому, Вы должны учитывать увеличение нагрузки на сервера, при аварийных ситуациях, когда устанавливаете порог готовности для сервера.

*1170 Отслеживайте другую статистику кластера, чтобы видеть сбалансирована ли рабочая нагрузка разумно. Следующая таблица содержит список некоторой статистики, которая является полезной в определении балансирования рабочей нагрузки.

Имя статистики	**Описание**
Server.AvailabilityIndex	Текущее значение индекса готовности. Значения от 0 до 100. Значение 0 указывает, что не имеется никаких ресурсов, доступных на сервере. Значение 100 - сервер полностью доступен.
Server.Cluster.OpenRedirects.LoadBalance.Successful	Количество времени, в течение которого, сервер помеченный как BUSY, успешно переадресовывает клиентов на другой сервер кластера.
Server.Cluster.OpenRedirects.LoadBalance.Unsuccessful	Количество времени, в течение которого, сервер помеченный как BUSY, безуспешно пытается переадресовывать клиентов на другой сервер кластера.
Server.Cluster.OpenRequest.ClusterBusy	Количество времени, в течение которого, сервер помеченный как BUSY, пробует переадресовывать запросы клиента, на другие сервера кластера, которые тоже находятся в состоянии BUSY.

Server.Cluster.OpenRequest.LoadBalanced	Количество времени, в течение которого пользователь пробовал открывать базу данных на этом сервере, когда сервер был в состоянии BUSY.

Эта совокупная статистика собирается с момента запуска сервера.

*1171 Сравнить эту статистику для всех серверов в кластере.

*1172 Регулируйте порог готовности сервера на любом сервере, если Вам кажется что она не сбалансирован.

Хотя может показаться естественным, установить тот же самый порог готовности на всех серверах кластера, это не оптимально для всех ситуациях. Если Ваши сервера значительно различаются по мощности, вместимости, или операционными системами, Вы должны учитывать эти различия.

2.16.18.2 Настройка порога готовности сервера.

Порог готовности сервера определяет самый низкий приемлемый индекс готовности сервера. Приблизительно один раз в минуту, Domino вычисляет индекс готовности сервера и сравнивает это значение с порогом готовности сервера, который Вы устанавливаете. Если индекс готовности - меньше чем порог готовности, сервер помечается состоянием BUSY. Когда сервер отмечен как BUSY, запросы на открытие баз данных будут переадресованы на другие доступные сервера в кластере. Когда индекс готовности становится выше, чем порог готовности снова, состояние BUSY снимается.

Чтобы устанавливать порог готовности сервера, добавьте следующую строку в файл NOTES.INI:

```
server_availability_threshold=a number from 0 to 100
```

Чем выше число Вы вводите, тем меньшее количество рабочей нагрузки, сервер может нести перед переходом в состояние BUSY. Значение – 100, автоматически помещает сервер в состояние BUSY, независимо от фактической готовности. Ввод числа – 0 (ноль) запрещает балансирование рабочей нагрузки, для того сервера. Значение по умолчанию – 0 (ноль).

Использование порога готовности, когда Вы перезапускаете сервер в кластере

Когда Вы перезапускаете, сервер в кластере, хорошая идея перевести сервер в состояние BUSY, пока все репликации на сервере не произойдут. Затем сделайте сервер доступным. Это гарантирует Вам, что доступ пользователей будет предоставлен, к самой современной информации. Вы можете перевести сервер в состояние BUSY, установив порог готовности равный - 100.

2.16.19 Настройка максимального числа пользователей на сервере.

Вы можете также балансировать рабочую нагрузку в кластере, используя переменную Server_MaxUsers в файле NOTES.INI. Эта настройка определяет максимальное число активных пользователей, подключенных к серверу одновременно. Когда сервер достигает этого предела, сервер переходит в состояние MAXUSERS и отклоняет любые дополнительные запросы пользователей, пока число активных пользователей снова упадет ниже предела переменной Server_MaxUsers. Когда Domino отклоняет запросы доступа, из-

за состояния MAXUSERS, Cluster Manager пытается переадресовывать запросы пользователей на другие сервера кластера, которые содержат соответствующие реплики. Если никакой другой сервер не доступен, Domino отклоняет запрос на доступ и показывает объяснительное сообщение.

Чтобы устанавливать максимальное число пользователей для сервера, добавьте следующую строку в файл NOTES.INI:

```
Server_MaxUsers=number
```

Где number - максимальное число пользователей, которым Вы хотите предоставить доступ на сервер одновременно

Обратите внимание, что настройка Server_MaxUsers не затрагивает репликации. Репликации происходят даже, когда сервер находится в состоянии MAXUSERS.

Примечание. Вы может использовать установку Server_MaxUsers с любым Domino сервером. Однако только сервера в кластере переадресовывает запросы доступа на другие сервера, когда сервер находится в состоянии MAXUSERS. Сервера, которые не входят в кластер, просто отклоняет запросы доступа.

2.16.20 Управление состоянием Failover в кластере.

Когда Вы устанавливаете кластер, Вы создаете реплики баз данных так, чтобы пользователи автоматически перенаправлялись к различным репликам, если оригинальная база данных или сервер, в данное время является недоступной. Кроме того, Вы можете захотеть применить опцию Failover преднамеренно:

*1173 Если вы модернизируйте программное обеспечение сервера или операционную систему

*1174 Исполняете профилактическое обслуживание на сервере

*1175 Заменяете сервер другим сервером

Как инициализировать событие Failover, для сервера.

Чтобы заставлять сервер эмулировать Failover, Вы можете использовать переменную Server_Restricted. Эта установка заставляет сервер, отрицать новые попытки на открытие баз данных и помещает сервер в состояние RESTRICTED. Установка запрещает новым пользователям вызывать сервер, хотя пользователи, которые имеют активные связи к базам данных на сервере, сохраняют их связи. Эта настройка полезна, когда Вы хотите сделать обслуживание на сервере, модернизировать сервер, или убрать сервер из обслуживания по другой причине.

Чтобы ограничить сервер от доступа на него новых пользователей, добавьте следующую строку в файл NOTES.INI:

```
Server_restricted=number
```

Где number 1 или 2.

1 - Сервер в состоянии RESTRICTED, для текущей сессии только. Перегрузка сервера очищает настройку.

2 - Сервер в состоянии RESTRICTED постоянно, даже после пере запусков сервера.

Когда сервер находится в состоянии RESTRICTED, Cluster Manager переадресовывает запросы на другой сервер кластера. Когда попытка переадресования неудачна, пользователь получает объяснительное сообщение и не может получить доступ на сервер. Для каждой попытки переназначения, Domino производит соответствующую запись в файле протоколов LOG.NSF.

Обратите внимание, что настройка Server_Restricted не затрагивает репликации. Репликации происходят даже, когда сервер находится в состоянии RESTRICTED.

Если Вы хотите ограничить сервер и не хотеть ждать всех пользователей, чтобы закрыть их существующие сессии, введите на консоли сервера команду Drop All, после того как Вы помещаете сервер в состояние RESTRICTED. Эта команда закрывает все существующие сессии на сервере. Когда пользователи пробуют повторно открыть базы данных, которые они использовали, они будут перенаправлены на другие сервера и реплики, если такие доступны.

Когда Вы хотите перевести сервер в обычный режим работы после режима RESTRICTED, делайте одно из следующего:

*1176 Если Вы установили значение - server_restricted=1, перезапустите сервер.

*1177 Если Вы установили значение - server_restricted=2, замените значение в файле NOTES.INI на следующее:

```
server_restricted=0
```

Замена сервера кластера другим сервером.

Если Вы хотите заменить сервер кластера другим сервером, делайте следующее:

*1178 Установить новый сервер, как сервер кластера.

*1179 Создайте реплики, которые Вы хотите иметь на новом сервере.

*1180 Добавить новый сервер в кластер.

*1181 Установите старый сервер в состояние RESTRICTED.

Это заставляет переадресовывать запросы пользователей, на новый сервер, и позволяет Вам удалить старый сервер, без остановки пользователей.

Другие способы управлять процессом Failover.

Вы можете устанавливать сервер как резервный сервер. Вы можете устанавливать порог готовности в 100 на резервном сервере, чтобы сервер находился в состоянии BUSY всегда. Учтите, что вторичный сервер принимает запросы на открытие баз данных только, когда первичный сервер недоступен.

Регулируя порог готовности на сервере в 100, Вы помещаете сервер в состояние BUSY. Это состояние подобно состоянию RESTRICTED. Кроме того, что сервера помеченные состоянием BUSY могут принимать новые запросы на открытые базы, если никакая другая реплика не доступна. Сервер, помеченный состоянием RESTRICTED, этого делать не может.

Примечание. Вы может использовать настройку Server_Restricted, для любой Domino сервера. Эта настройка не ограничена применением в кластере.

2.16.21 Управление доступностью баз данных в кластере.

Имеются три признака для баз данных, которые позволяют Вам определять, является ли база данных доступной для доступа пользователя. Они:

*1182 Out of Service

*1183 In Service

*1184 Pending Delete

2.16.21.1 Установка атрибута - Out of Service, для баз данных

В некоторых случаях, Вы можете отмечать базу данных признаком Out of Service. Вы делаете это, если Вы хотите сделать некоторое обслуживание базе данных, или если Вы хотите, чтобы пользователи не получали доступ к некоторым репликам баз данных, потому что сервер достигает высокого уровня использования.

Когда Вы помечаете базу данных как Out of Service, пользователи не могут открыть базу данных. Запрос на открытые базы данных терпят неудачу в этой реплике. Если никакая реплика не доступна, Domino отвергает запрос пользователей к базе данных и показывает объяснительное сообщение.

Пользователи, которые используют базу данных, когда Вы отмечаете ее признаком Out of Service, продолжают иметь доступ, пока они не закрывают базу данных. Если пользователи закрывают базу данных, но затем пробуют повторно открыть ее, они будут перенаправлены в другую доступную реплику. Это означает, что база данных постепенно перейдет в состояние Out of Service, без остановки пользователей, которые активно используют ее. Кроме того, репликации из других реплик продолжают происходить даже, когда база данных помечена как Out of Service.

Чтобы пометить базу данных признаком Out of Service, следуют этой процедурой:

*1185 В панели серверов, из клиента Domino Administrator, выберите сервер, который содержит базу данных, которую Вы хотите пометить как Out of Service.

*1186 Выбирайте закладку Файлы.

*1187 Выбирайте папку, которая содержит искомую базу данных и потом базу данных.

*1188 Из панели инструментов, справа, выбирайте - Сервис – База данных – Кластер.

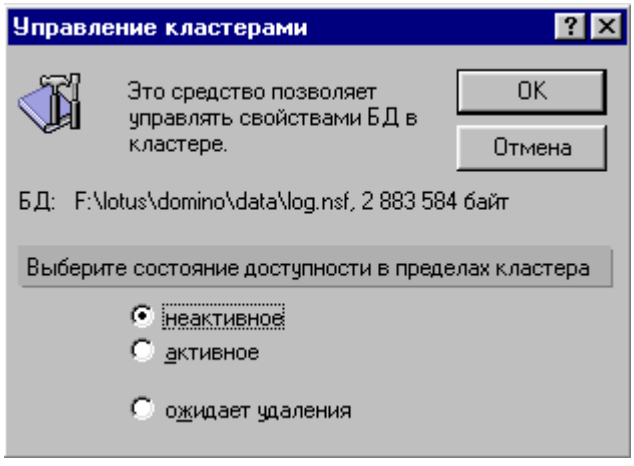


Рис. 57 Диалоговое окно управления базами данных в кластере.

*1189 Выбирайте значение “неактивное” (out of service), и затем – OK.

Вы можете пометить все базы данных признаком Out of Service, используя переменную Server_Restricted. При этом сервер не будет принимать новые запросы на открытия баз данных.

2.16.21.2 Установка атрибута - In Service, для баз данных.

Если вы пометили базу данных признаком Out of Service, но теперь хотите восстановить доступ к базе данных, Вы должны присвоить базе данных признак - In Service.

*1190 В панели серверов, из клиента Domino Administrator, выберите сервер, который содержит базу данных, которую Вы хотите пометить как Out of Service.

*1191 Выбирайте закладку Файлы.

*1192 Выбирайте папку, которая содержит искомую базу данных и потом базу данных.

*1193 Из панели инструментов, справа, выбирайте Сервис – База данных – Кластер.

*1194 Выбирайте значение “активное” (In Service), и затем – OK.

2.16.22 Использование кластера Domino серверов в интернете.

Глава описывает, как сконфигурировать для использования Internet Cluster Manager (ICM), чтобы расширить выгоду, от использования Domino кластеров, HTTP клиентами и Domino Web сервером.

2.16.22.1 Как работает Internet Cluster Manager?

Internet Cluster Manager (ICM) позволяет Вам использовать Domino кластеры, чтобы обеспечить переадресацию запросов клиентов, и балансирование рабочей нагрузки HTTP клиентам (Internet browsers), когда ими позволяется доступом на Domino Web сервера. Это делает Ваш Web сервер и базы данных, всегда доступными Web клиентам. Вы можете запустить ICM на любом сервере, который использует Domino R5, с лицензии Enterprise Server. Вы устанавливаете и конфигурируете Domino кластер как обычно, и затем конфигурируете ICM. ICM поддерживает протоколы HTTP и HTTPS.

ICM действует как посредник между HTTP клиентами и Domino Web серверами в кластере. Когда Domino Web сервера объединены в кластер, они производят URL, которые направляют запросы HTTP клиентов к ICM. ICM поддерживает информацию относительно готовности серверов и баз данных в кластере. Когда ICM получает запрос клиента, он переадресовывает клиента к наиболее доступному серверу, который содержит реплику требуемой базы данных.

ICM посылает периодические сигналы исследования Web серверам кластера, чтобы определить их статус и готовность. Когда ICM получает запрос клиента, он смотрит информацию в базе данных Cluster Database Directory, чтобы найти сервер, который содержит требуемую базу данных. ICM определяет наиболее доступный сервер, который содержит требуемую базу данных, и затем переадресовывает клиента на этот сервер. Клиент закрывает сессию с ICM и открывает новую сессию с выбранным сервером. Пользователь может видеть это как изменение (замена) имени хоста в URL. Пользователь

может также видеть измененный путь к базе данных в URL, потому что база данных может иметь различное место хранения на разных серверах.

Если страница, которая показана Web сервером, клиенту, включает связи с другими базам данных на том же самом сервере, или с другими базами данных в кластере, Web сервер, включает имя хоста ICM, в URL к этим базам данных. Это гарантирует, что пользователи, обращающиеся к этим связям, будут использовать ICM.

Следующий рисунок показывает HTTP клиента, который запрашивает у ICM, открытие базы данных. ICM переадресовывает клиента на лучший сервер, который содержит требуемую базу данных, Server2. Клиент соединяется непосредственно с Server2.

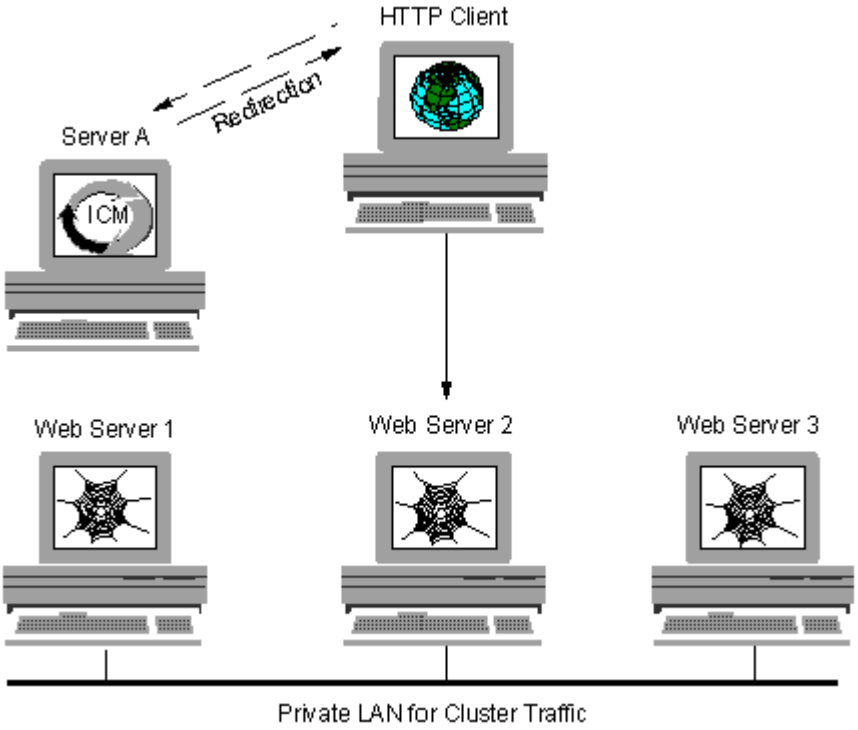


Рис. 58 Пример использования ICM.

ICM может запускаться на сервере кластера или вне его. Когда ICM работает на сервере в кластере, ему доступна локальная копия базы данных Cluster Database Directory. Когда ICM запущен на сервере вне кластера, это выбирает сервер в кластере, и получает доступ в базу данных Cluster Database Directory, на этом сервере. Если сервер, который ICM выбирает, становится недоступным, эта связь терпит неудачу, и запрос переадресовывается на другой сервер в кластере.

ICM всегда использует локальную копию Domino Directory. Поэтому, ICM должен быть в том же самом Domino домене, что и кластер.

Соображения о производительности ICM.

В большинстве случаев, пользователи замечают увеличение производительности, когда Вы начинаете использовать ICM. Эффект от использования ICM очень маленький, но выгода от балансирования рабочей нагрузки на сервера, может быть существенна. В случаях, где рабочая нагрузка на сервера, была уже сбалансирована, не будет иметься ни существенного увеличения, но уменьшения производительности.

2.16.22.2 Генерирование URLs, при использовании ICM.

Domino Web сервер, который находится в кластере, читает Server документ, чтобы найти имя хоста ICM. Web сервер производит URL, который включает имя хоста ICM. ICM принимает и обрабатывает все URL, поддерживаемые Domino Web сервером. Они включают URL, которые делают следующее:

*1195 Открытие сервера, базы данных, или представления

*1196 Открытые формы, навигатора, или агента

*1197 Открытие, редактирование, или удаление документа

*1198 Открытые документа по имени, из представления

*1199 Открытые файла изображения, приложения, или объекта OLE

*1200 Создание запросов поиска

Следующие условия могут затрагивать путь, с использованием которого ICM производит URL:

*1201 Если URL включает в себя путь, ICM не может решить этот URL, потому что несколько серверов могут содержать эту базу данных, с тем же самым путем и именем файла, но с разными ID реплик. Когда это происходит, ICM показывает список возможных баз данных, из которых пользователь может выбирать нужную базу данных.

*1202 Если URL включает ID реплики, ICM не может быть способен решить этот URL, для единственной базы данных, если имеются несколько копий реплик баз данных на сервере. Когда это происходит, ICM переадресовывает запрос клиента к серверу, который содержит, по крайней мере, одну реплику требуемой базы данных, и Web сервер выбирает реплику, чтобы представить ее пользователю. Для доступа к определенной реплике, пользователи должны определить путь к этой реплике.

*1203 Если URL включает NoteID, ICM может давать не правильные результаты при обработке URL. Это происходит потому, что NoteID объект, не может быть тот же самый во всех репликах. В отличие от NoteID, ID реплики - идентичны во всех репликах баз данных.

2.16.22.3 Конфигурирование ICM.

Вы конфигурируете ICM, делая записи в секции Internet Cluster Manager в Server документе. Вы можете также устанавливать отдельный IP адрес для ICM.

Вы можете конфигурировать ICM на одном сервере, и иметь больше чем один ICM с доступом, к этими настройкам. Это позволяет ICM на различных серверах, использовать общую конфигурацию. Вы должны включить в ICM информацию относительно каждого Web сервера кластера. Вы делаете это, потому что каждый Web сервер использует собственный Server документ, чтобы определить, как производить URL, который будет обращаться к ICM. Web сервер получает имя хоста ICM из Server документа. Web Сервер использует это имя хоста, чтобы произвести URL, который ссылается на ICM.

Конфигурирование ICM

*1204 Из клиента Domino Administrator, выбирайте закладку Настройка.

*1205 Выбирайте Server документ сервера, на котором Вы хотите запустить ICM и переведите его в режим редактирования.

*1206 Выбирайте Server Tasks – Internet Cluster Manager.

*1207 Заполните следующие поля:

Секция	**Имя поля**	**Описание**
Basics	Cluster name	Имя кластера, который ICM обслуживает. Если это поле не заполнено, Domino использует имя кластера, к которому принадлежит этот сервер.
	ICM Notes port	Имя порта Notes, который ICM будет использовать, чтобы связаться с HTTP клиентами. Если Вы оставляете это поле незаполненным по умолчанию, ICM может использовать любой порт Notes, чтобы связаться с HTTP клиентами. Вводите название порта, только, если Вы хотите ограничить ICM связь, по одному определенному порту.
	ICM SSL keyfile	Имя файла KeyFile, для SSL, который содержит сертификаты, для идентификации ICM связей HTTP клиентов.
	Allow users to browse databases in the cluster over HTTP	Позволяется ли HTTP клиентам просматривать список баз данных в кластере. Когда Вы позволяете эту опцию, пользователи могут вводить команду http://icmhostname/?OpenServer Ввод этого URL показывает список баз данных на сервере в кластере, связанном с ICM именем хоста.
Configuration	Get configuration from	Позволяет Вам определять различные Server документы, чтобы получить информацию конфигурации из них. Это поле позволяет нескольким ICM использовать ту же самую конфигурацию.
	Obtain ICM configuration from	Это поле появляется, когда Вы выбираете Another server document в поле Get configuration from. Введите имя сервера, чей Server документ содержит конфигурацию, которую Вы хотите использовать.
	ICM hostname	Полное имя хоста, которое клиенты должны использовать, чтобы связаться с ICM. Это может быть зарегистрированное имя DNS или адрес IP. Domino сервер Web использует это поле, чтобы создать URL, который ссылается на ICM. Если это поле не заполнено, Web сервер не будет способен произвести URL, которые будут обращаться к ICM.

ICM HTTP Port Settings	TCP/IP port number	Введите номер порта для использования ICM. Если Вы запускаете ICM на том же самом сервере, что и Web сервер, Вы должны избежать конфликтов портов и адреса. Если Вы не даете ICM собственный адрес IP, убедитесь, номер порта ICM, отличается от любого из других номеров порта, которые Вы используете на сервере.
	TCP/IP port status	*1208 Enabled - Чтобы позволять HTTP связь с ICM *1209 Disabled - Для запрещения HTTP связей с ICM
	SSL port number	Введите номер порта, для использования SSL. Если Вы запускаете ICM на том же самом сервере, что и Web сервер, и Вы не даете ICM собственный IP адрес, убедитесь, что номер SSL порта, отличается от любого из других номеров порта, которые Вы используете на сервере.
	SSL port status	Чтобы разрешить HTTPS связь с ICM, выберите значение – Enabled.

*1210 Сохраните и закройте Server документ.

Когда Вы запускаете ICM, он смотрит в Server документ, на котором он запущен, чтобы найти ICM имя кластера и адрес сети. Задача получает имя хоста и назначения порта из того же самого Server документа или из Server документа, указанного в поле Obtain ICM configuration from.

Если Вы запускаете ICM на той же самой системе, что и Domino Web сервер, Вы должны избежали конфликтов IP адреса или конфликтов номеров портов. Лучший подход состоит в том, чтобы назначить ICM собственный адрес IP. Вы можете также иметь ICM, разделяют адрес IP с Web сервером, если Вы определяете различные номера порта, для ICM и других протоколов на Web сервере.

2.16.22.3.1 Определение выделенного IP адреса для ICM

Когда Вы запускаете ICM на Web сервере, Вы можете определить ICM, собственный IP адрес, чтобы избежать конфликтов.

*1211 Использовать Вашу операционную систему, чтобы определить новый IP адрес и сделать его доступным.

*1212 Из клиента Domino Administrator, на сервере который содержит ICM, устанавливают порт, делая следующее:

- Выберите из меню Файл – Параметры – Параметры настройки.
- Выбирайте закладку Порты.
- Выбирайте - Создать.

- Определите Имя для нового порта, например – ICMPORT.
- Выбирайте - TCP, драйвер порта.
- Нажмите дважды – OK.

Обратите внимание, если ли Вы не используете Domino Administrator на сервере, который содержит ICM, сделайте следующее, чтобы установить порт:

Добавьте следующую строку в файле NOTES.INI:

Portname=TCP, номер адаптера или номер сети, номер сессий, размер буфера данных

Пример:

```
ICMPORT=TCP,0,15,0
```

Добавьте имя порта, типа ICMPORT, к настройке портов в файл NOTES.INI

*1213 Добавить следующую строку в файл NOTES.INI:

```
Portname_TcpipAddress=0,IPADDRESS
```

Где portname - имя порта, который Вы конфигурировали из Domino Administrator, типа ICMPORT, а IPADDRESS - адрес IP, который Вы используете для ICM.

Пример:

```
ICMPORT_TCPIPADDRESS=0,192.94.222.169
```

*1214 В поле ICM Notes port на Server Tasks – Internet Cluster Manager в Server документе, введите имя порта, который Вы сконфигурировали, типа – ICMPORT.

*1215 Если Вы хотите использовать порт 80, и для ICM, и для Web сервера, Вы должны сделать следующее:

- В Server документе, выбирайте закладку Internet Protocol – HTTP.
- В поле Host name(s), введите адрес IP или имя хоста Web сервера.
- В поле Bind to host name, выбирайте – Enabled.

2.16.22.3.2 Запуск ICM

Чтобы запускать ICM каждый раз, когда Вы запускаете сервер, добавляете в конец строки переменной ServerTasks имя задачи ICM в NOTES.INI. Например:

```
ServerTasks=ROUTER,REPLICA,ADMINP,CLDBDIR,CLREPL,HTTP,ICM
```

Чтобы запустить задачу ICM вручную, введите на консоли сервера следующую команду:

```
load icm
```

Вы можете запустить ICM задачу многократно на сервере, чтобы гарантировать, что ICM запускается всегда. Когда Вы запускаете больше чем одну копию задачи ICM, Вы типично используете те же самые назначения конфигурации для каждого ICM.

2.16.22.4 Failover и балансирование рабочей нагрузки на сервера.

При использовании ICM, процесс Failover и балансирование рабочей нагрузки работает точно так же, как и стандартный Domino кластер. Domino вычисляет индекс готовности сервера, основанный на всех открытых сессиях клиентов Notes, HTTP клиентов, или другой Domino сервера. В конфигурации балансирования рабочей нагрузки и Failover, Вы используете те же самые переменные, Server_Restricted, Server_Availability_Threshold и Server_MaxUsers. Для готовности баз данных, Вы также используете те же самые назначения, типа маркировки базы данных Out of service или Pending delete.

Обратите внимание. В отличие от стандартного Domino на кластера, ICM может перенаправлять клиентов к серверу, который находится в состоянии MAXUSERS или RESTRICTED, если никакой другой сервер не доступен.

ICM использует следующий тип информации, чтобы задача могла находить реплику, когда клиент просит об этом:

*1216 Информация, относительно каждой базы данных, является доступной в кластере и где они сохранена. ICM получает эту информацию из базы данных Cluster Database Directory.

*1217 Информация, относительно готовности каждого сервера. ICM получает эту информацию, каждый раз, когда задача исследует сервера в кластере.

*1218 Информация, относительно конфигурирования Web сервера. Какой из серверов сконфигурирован для HTTP, а какой для работы с использованием HTTPS. ICM получает эту информацию из Server документов, каждого сервера кластера.

Чтобы определить, какая реплика базы данных должна быть открыта, ICM делает следующее:

*1219 Определяет, где реплики расположены и помечены ли они Out of Service или Pending Delete.

*1220 Проверяет индекс готовности каждого сервера, который содержит базу данных.

*1221 Проверяет готовность порта сервера (pinging port) HTTP или HTTPS, в зависимости от запроса клиента.

*1222 Исключает любые сервера, которые являются недоступными или помеченные как RESTRICTED.

*1223 Исключает любые сервера, которые помечены как BUSY или MAXUSERS.

*1224 Выбирает сервер из оставшихся, доступных серверов. Если не имеется никаких доступных серверов, ICM выбирает сервер, который находится в состоянии BUSY, MAXUSERS, или RESTRICTED. Если имеется несколько серверов, ICM выбирает сервер с самой легкой текущей рабочей нагрузкой.

После выбора сервера, ICM просматривает Server документ, чтобы определить порт для доступа на сервер.

Когда сервер терпит неудачу.

Когда HTTP клиент связан с сервером, который терпит неудачу, клиент получает сообщение, говорящее, что сервер не отвечает. Чтобы обратится к другой реплике,

пользователь, должен войти в контакт ICM снова. Пользователь может сделать это следующим способом:

*1225 Щелкните кнопкой Back в браузере, чтобы соединиться с главной страницей через ICM

*1226 Использовать соответствующую закладку

*1227 Ввести URL

Пользователю придется повторно подтвердить свою подлинность на новом сервере. Это определяется следующими факторами:

*1228 Если пользователь, уже зарегистрирован на новом сервере в течение этой сессии, никакое установление подлинности ненужно

*1229 Если HTTP клиент и сервер оба поддерживают SSL3, проверка подлинности происходит автоматически

2.16.22.5 Безопасность.

ICM поддерживает SSL. ICM может использовать те же самые SSL сертификаты, которые Domino Web сервер использует, или Вы можете определить различный набор SSL сертификатов для ICM. Вы можете сконфигурировать ICM, чтобы требовать SSL в секции Internet Cluster Manager документа сервера. ICM использует назначения секции Internet Ports, документа сервера, чтобы разрешить соответствующую версию SSL протокола и принимать ли истекшие сертификаты.

Кроме того, обычные функции безопасности Domino сервера, для баз данных, могут использоваться с использованием ICM. Однако ICM не участвует в процессе безопасности в прямом смысле слова. Когда HTTP клиент хочет получить доступ к базе данных, он посылает анонимный запрос к ICM. ICM сообщает клиенту имя сервера, на который он может получить доступ. Запрос клиента автоматически переадресовывается на соответствующий сервер. Сервер устанавливает диалог с клиентом и может использовать любые меры безопасности, которые доступны Вам. Если Вы хотите защитить ICM непосредственно от неправомочного доступа, Вы можете использовать Firewall сервер.

2.16.22.6 Управление и контроль ICM.

ICM делает соответствующие записи всех событий, чтобы найти эти события, просмотрите представление Miscellaneous Events, в файле протоколов LOG.NSF.

Вы можете просмотреть статистику ICM с консоли сервера, введите команду на консоли:

```
show stat icm
```

Вы можете использовать эту статистику, в совокупности со стандартной статистикой кластера, чтобы определить, который из серверов в кластере является самым занятым. После этого Вы можете сбалансировать рабочую нагрузку в кластере.

2.16.22.7 Совместимость с предыдущими версиями серверов Domino.

ICM перенаправляет запросы клиентов на любой Domino Web сервер в кластере, не зависимо от версии этого сервера Domino. Поэтому, использование ICM в смешанном кластере не имеет никаких отрицательных результатов для клиентов. Только R5 Web сервера, однако, производят URL, которые включаются ссылки на ICM. Когда

пользователь выбирает URL, которые содержит эти ссылки, ICM способен балансировать рабочую нагрузку и переадресовывать пользователя к соответствующему серверу.

Если ICM переадресовывает запрос клиента на сервер, версия которого ниже Domino R5, URL, который производит сервер, не будет содержать ссылки на ICM. Клиент может передвигаться по Web страницам только на этом сервере. Чтобы воспользоваться преимуществом ICM, пользователь должен ввести URL, который содержит ссылку на ICM.

2.17 Команды Domino сервера.

Вы можете использовать команды сервера, чтобы выполнить все задачи администрирования. Глава описывает как вводить команды сервера, и содержит полную информации относительно использования каждой команды.

2.17.1 Ввод команд сервера

Консоль сервера показывает события сервера, ответы на ввод команд. Для некоторых команд, типа Load, сервер не выдает ответ на консоль. Вместо этого, в файле LOG.NSF сервер делает запись. Вы можете просматривать файл LOG.NSF с закладки Сервер – Анализ, клиента Domino Administrator.

Вы можете также использовать клиента Domino Administrator, чтобы ввести команды предназначенные удаленному серверу. Многие из закладок клиента Domino Administrator автоматически показывают информацию, которую Вы обычно видели, как результат ввода команд сервера на консоли сервера.

Например, когда Вы щелкаете на закладке Сервер – Состояние, эквивалент команды Show Tasks появится. Кроме того, несколько закладок имеют панели инструментов, которые позволяют Вам вводить команду через окно диалога пользователя.

Имеются несколько способов ввести команды сервера:

*1230 Ввести команду на консоли сервера

*1231 Ввести команду из клиента Domino Administrator

*1232 Запустить командный файл (BAT), использую консоль сервера

2.17.1.1 Ввод команды с консоли сервера.

*1233 Запустите Domino сервер, если сервер еще не запущен.

*1234 Нажмите – ENTER, чтобы показать на консоли знак приглашения (>).

*1235 Введите команду сервера.

Если параметр команды содержит пробел, заключите команду в кавычки - например:

```
Pull Acme Server
```

Примечание, чтобы сэкономить время, вводите сокращения для команд сервера. Вы можете также нажимать стрелку курсора, чтобы показать команду, которую Вы предварительно вводили.

*1236 (Необязательно) Используйте эти ключевые комбинации клавиш, по мере необходимости:

CTRL+Q, или **PAUSE**, чтобы остановить вывод на экран информации и приостановить дальнейшее выполнение вывода информации.

CTRL+R, чтобы возобновить отображение информации и доступа к серверу.

2.17.1.2 Ввод команд сервера с использованием Domino Administrator.

*1237 Удостоверьтесь, что вы внесены в список в поле Администраторов сервер документа.

*1238 Из клиента Domino Administrator, выбирайте Сервер – Состояние.

*1239 Выбирайте – Консоль.

*1240 Делайте одно из следующего:

- Введите команду, в командную строку сервера.
- Выбирайте кнопку Команды, затем выбирайте команду.
- Выберите команду из списка, и затем пошлите, или измените ее.
- Если надо, введите аргументы команды.

Команда может содержать до 255 знаков. Если аргумент команды содержит пробел, заключите его в кавычки. Например:

```
PULL Acme Server
```

нажмите – ENTER.

*1241 (Необязательно) Делайте любое из следующего, по мере необходимости:

*1242 Выбирайте - Пуск, чтобы показать записи.

*1243 Выбирайте - Стоп.

*1244 Выбирайте – Stop, чтобы остановить вывод записей.

2.17.1.3 Запуск Batch-файла на консоли сервера.

Вы можете запускать несколько команд на консоли сразу. Синтаксис для команд

```
< Batchfilename
```

В каталоге данных, создайте командный текстовый файл - например, COMMANDS.TXT - содержащий список команд сервера. На консоли сервера, введите

```
< COMMANDS.TXT
```

Если Вы создаете *.TXT файл не в каталоге данных Notes, включаете в команду полный путь с именем файла.

Внимание! Обратите внимание на синтаксис ввода команды **< commands.txt**

2.17.1.4 Вывод ответа команды сервера в файл.

Некоторые команды сервера показывает информацию, которую Вы могли бы захватить в файл. Введите команду сервера и на той же самой строке, введите пробел и затем следующее:

```
> Filename.ext
```

Где `filename.ext` - имя файла, в котором Вы хотите сохранить ответ команды. Ведите пробел после команды сервера, но после символа переназначения (>). Например, эта команда пишет ответ команды Show Tasks в файл TASKS.OUT в Notes directory:

```
Show Tasks > TASKS.OUT
```

Чтобы сохранить вывод, в файл в другом каталоге данных, определите полный путь к файлу.

2.17.2 Команды Domino сервера.

2.17.2.1 Broadcast

Посылается сообщение определенному пользователю или всем пользователям этого сервера. Используйте эту команду, чтобы предупредить пользователей, когда сервер будет остановлен для обслуживания. Сообщение, которое Вы вводите, покажется в панели статуса пользователя.

2.17.2.2 Dbcache Flush

Закрывает все базы данных, которые являются в настоящее время открытыми в памяти сервера. Используйте эту команду, для обслуживания баз данных

2.17.2.3 Drop

Закрытие, одного или большего количества сессий сервера. Чтобы визуально подтверждать, закрытие сессии, Вы должны присвоить переменной Log_Sessions=1 (значение единицы) в NOTES.INI файле сервера.

2.17.2.4 Exit

Останавливает сервер. Эта команда идентична - Quit.

Прежде чем Вы используете команду Exit, используйте команду Broadcast, чтобы предупредить пользователей об остановке сервера.

Если Вы останавливаете сервер, в то время как он копирует базы данных или передает почту, эти задачи запустятся после того, как Вы повторно запустите сервер. Репликации или передача почты продолжится, пока базы данных полностью не закончат репликации, и пока не произойдет полная передача почты.

2.17.2.5 Help

Показывает список команд сервера, с кратким описанием, аргументов и надлежащим синтаксисом для каждой.

2.17.2.6 Load

Загружает указанную задачу или программу на сервере. Вы можете запустить программу на сервере, которая должна быть в пути поиска сервера.

2.17.2.7 Pull

Вынуждает одностороннюю репликацию с указанного сервера на Ваш сервер. Вы можете также реплицировать отдельную базу данных с указанного сервера на Ваш сервер, включением имени базы данных в командную строку. Вводите полное иерархическое имя серверов.

Вы можете реплицировать базы немедленно, если база данных важна вам.

Для выполнения репликаций, удостовериться, что:

*1245 Domino Directory содержит Server документ для каждого сервера в домене

*1246 Domino Directory содержит документ подключения, чтобы соединиться с удаленным сервером

*1247 ID файл каждого сервера содержит сертификат, который другой сервер признает и доверяет ему

*1248 База данных ACL позволяет репликации, а источник сервер имеет достаточный доступ в ACL, чтобы копировать изменения. Если вы используете группы серверов в списках доступа, сервер должен иметь надлежащий доступ в документе сервера.

Если сервер - в настоящее время реплицирует, Domino не выполняет Pull команды, пока текущая задача не заканчивается. Чтобы проверять статус Репликатора, перед использованием Pull, войдите в эту команду на консоли сервера:

```
Show Tasks
```

Сервер показывает одно из следующих сообщений:

*1249 Если сервер не реплицирует, слово Idle появляется рядом с задачей Репликатора.

*1250 Если server реплицирует, получите сообщение типа Replicating CONTRACT.NSF from MARKETING\CONTRACT.NSF.

2.17.2.8 Push

Вынуждает одностороннюю репликацию с Вашего сервера на указанный сервер. Вы можете также реплицировать отдельную базу данных с Вашего сервера, на указанный сервер, включая имя базы данных в командную строку. Ваш сервер посылает данные на названый сервер, но не запрашивает данные.

В действительности, Push команда - функционирует, как противоположная команде Pull.

2.17.2.9 Quit

Останавливает сервер. Эта команда идентична команде Exit. Однако Quit команда имеет боле расширенный синтаксис. Она может использоваться с командой Tell, которую Вы используете, чтобы остановить выбранную задачу сервера, без остановки сервера.

Если Вы останавливаете сервер, во время репликации данных или передачи почты, эти задачи будут продолжены после того, как Вы повторно перезапустите сервер. Репликации или передача почты продолжатся, пока базы данных полностью не реплицируются и, пока полностью не будет передана почта.

Прежде, чем Вы используете команду сервера Quit, используете Broadcast, чтобы предупредить своих пользователей.

2.17.2.10 Replicate

Вынуждает репликацию между двумя серверами. Используйте полное иерархическое имя серверов. Если название сервера - больше чем одно слово, имя заключается в кавычках. Чтобы вынуждать репликацию специфической базы данных, имя базы данных, указывается после имени сервера.

Обратите внимание, что если существует график репликаций между серверами и работает запланированная реплика, в момент ввода вами команды для вынуждения реплики, Ваша реплика устанавливается в очередь. Ваша реплика начинает работать после завершения всех запланированных реплик.

Чтобы проверить статус Репликатора, введите эту команду на консоли сервера:

```
Show Tasks
```

Сервер показывает одно из следующих сообщений:

*1251 Если server не реплицирует, слово Idle появляется рядом с задачей Репликатора.

*1252 Если server реплицирует, получите сообщение типа Replicating CONTRACT.NSF from MARKETING\CONTRACT.NSF.

Чтобы оптимизировать ресурсы Domino реплицируйте только то, что необходимо. Чтобы вынудить репликацию только в одном направлении, используйте команду Pull или Push.

2.17.2.11 Restart

Останавливает сервер и затем повторно его запускает, после краткой задержки.

Если Вы останавливаете сервер, во время репликации баз данных или передачи почты, то при повторном запуске сервера репликации или передача почты продолжится, пока все не завершится.

Прежде, чем Вы используете команду Restart, используете Broadcast, чтобы предупредить пользователей об этом.

2.17.2.12 Route

Начинает передачу почты на определенный сервер. Команда Route перекрывает любые графики передачи почты, которые Вы создаете в документах подключения в Domino Directory. Используйте команду Route для серверов, которые сконфигурированы как Pull, Pull-Push, Push, или Push Wait в документах подключения. Используйте полное иерархическое имя серверов. Если имя сервера - состоит из нескольких слов, заключайте название сервера в кавычки, при вводе его имени в командной строке.

Используйте команду Route при проблемах с передачей почты или если Вам необходимо передать почту с сервера немедленно.

Если никакой почты не имеется в очереди для передачи, Domino игнорирует команду Route. Для проверки серверов на наличие очереди почты на передачу, введите эту команду на консоли сервера:

```
Tell Router Show
```

2.17.2.13 Set Configuration

Добавляет или изменяет установку в NOTES.INI файле.

2.17.2.14 Set Secure

Защищает консоль сервера паролем.

После того, как Вы ввели пароль и защитили консоль, Вы не можете использовать команды Load, Tell, Exit, Quit и Set Configuration или другие программы, которые не запускаются автоматически через Program documents Domino Directory, или через NOTES.INI, пока Вы не введете пароль заново. Акция Безопасности консоли сервера остается в силе, пока Вы не очищаете пароль, вводом вторично команду Set Secure с тем же самым паролем.

Даже если консоль защищена паролем, держите сервер в физически защищенном месте, чтобы предотвратить вторжение в операционную систему.

2.17.2.15 Show Allports

Показывает конфигурацию всех разрешенных и запрещенных портов на сервере.

2.17.2.16 Show Cluster

Показывает Кластер локальных серверов, в который включен список всех членов кластера и их статуса, полученной в течение работы Кластера серверов.

2.17.2.17 Show Configuration

Показывает текущее значение установок NOTES.INI. Используйте Show Configuration и Set Configuration server команды вместе, чтобы гарантировать, что Вы правильно устанавливаете NOTES.INI значения.

2.17.2.18 Show Directory

Выводит список всех файлов баз данных (например, .NSF и .NTF) из каталога данных и определяет, содержатся ли в каталоге данные реплики баз данных. Эта команда работает только для каталога данных; Вы не можете определить другой каталог.

2.17.2.19 Show Diskspace

Показывается свободное место на диске сервера, в байтах (WindowsNT, OS/2, UNIX). Если Вы не определяете, местоположение, Domino показывает место, доступное на диске системных файлов, содержащих Domino Directory. Если доступного места окажется мало - например, 10МБ - удалите документы, базы данных, и другие файлы, в которых Вы не нуждаетесь.

Domino сервер установленный на WindowsNT 3.51 сервере при использовании TCP/IP и Netbios не может видеть смапированые диски, на другом NT сервере, с использованием

команды Show Diskspace на Domino сервере сразу. Для того чтобы команда Show Diskspace заработала, необходимо одно из следующих условий:

*1253 Domino сервер запущен как приложение

*1254 Domino сервер запущен как задача NT сервера

Обратите внимание, если Domino сервер запущен прежде, чем диски сервера смапированы, и Вы пытаетесь использовать команду Show Diskspace - задача терпит неудачу. Чтобы увидеть смапированые диски, остановите и повторно запустите Domino сервер, или поместите Domino сервер в группу – Startup group.

Domino может делать запросы по сети Redirector в системе, если это включено. Notes сервер может видеть диски по сети, если они показываются в Сетевом окружении сервера.

2.17.2.20 Show Memory

На OS/2 сервере команда Show Memory показывает количество доступной памяти - RAM, плюс количество памяти обмена, доступной на загрузочном диске Domino сервера. Если число, показанное здесь и число, когда Вы вводите команду Show Diskspace, равно или близко к равенству, сервер может нуждаться в большем количестве RAM.

2.17.2.21 Show Port

Показывает трафик сети, через сетевую карту, статистику ошибок и ресурсов. PortName может быть любой сконфигурированный порт. Например - LAN0, LAN1, COM1, COM2.

Чтобы проверить статус порта с рабочего места Notes, выбирайте из меню Файл – Параметры – Параметры настройки – Порты. Выбирайте порт, и выберите Состояние. Чтобы проверять статус порта из клиента Domino Administrator, Выбирайте - Сервер – Статистика и затем выбирайте – NET, выбирайте порт для просмотра статистики.

2.17.2.22 Show Schedule

Показывает расписание задач намеченных на сервере, включая тип задачи и время ее запуска.

2.17.2.23 Show Server

Показывает информацию статуса сервера, включая имя сервера, данные о каталоге сервера, время работы сервера, оперативную статистику, статус задач, ожидаемую, и “мертвую” почту.

2.17.2.24 Show Stat

При использовании без аргументов, показывает список статистики сервера: место на диске, память, почты, репликации, движение по сети. Чтобы показать отдельную статистику, введите аргумент для команды Statistic, как необязательный аргумент.

Вы можете вводить эту команду на консоли сервера, чтобы показать статистику для локального сервера или, на удаленной консоли сервера, чтобы показать статистику для удаленного сервера.

2.17.2.25 Show Tasks

Показывает имя сервера, путь к каталогу Domino Directory и статус активных задач сервера.

2.17.2.26 Show Users

Показать пользователей работающих с сервером.

2.17.2.27 Start Port

Разрешается использование указанного порта. Используйте эту команду после того, как Вы запретили порт командой - Stop Port.

Обратите внимание. Команды Stop Port и Start Port не имеют никакого влияния на Domino Web сервер.

2.17.2.28 Stop Port

Запрещает использование указанного порта. Порт, который Вы запрещаете, определяется из меню Файл – Параметры – Параметры настройки – Порты и удалите “галочку” - Порт включен. Эта команда позволяет Вам делать изменения в настройках порта, которые вступают в силу немедленно без остановки Domino сервера. Когда вы закончили изменения в настройках порта, используете команду - Состояние, чтобы заново разрешить его использование.

2.17.2.29 Tell

Управляющая команду для задач сервера. Команда особенно полезна для остановки задач сервера без остановки самого сервера.

Administration Process Tell Commands

Команда	**Результат**
Tell Adminp Process All	Обрабатывает все новые и запросы на изменение, немедленно, интервал, ежедневно и отсроченные запросы. Эта команда не перекрывает запланированные запросы.
Tell Adminp Process Daily	Обрабатывает запросы: *1255 Все новые и ежедневно измененные запросы, чтобы модернизировать документы Person в Domino Directory. *1256 Любые невыполненные запросы Rename Person in Unread List.
Tell Adminp Process Delayed	Обрабатывает все новые и изменения отсроченных запросов. Запросы, которые обычно выполняются согласно Start executing on и с назначениями Start executing at из Server документа.

Tell Adminp Process Interval	Обрабатывает немедленно все запросы и все запросы, которые обычно обрабатываются согласно Interval setting в Server документе.
Tell Adminp Process New	Обрабатывает все новые запросы.
Tell Adminp Process People	Обрабатывает все новые и запросы на изменение, документов Person в Domino Directory.
Tell Adminp Process Time	Обрабатывает все новые и запросы изменения, чтобы удалить файлы Unlinked Mail.
Tell Adminp Show Databases	Отображает, делает запись в файле LOG.NSF сервера этой информации: *1257 Базы данных, Particular administration server updates *1258 Местоположения базы данных, в которых модернизируются поля Readers And Authors в базах данных. *1259 Базы данных, которые не имеют сервера администрирования назначенного для них.
Tell Adminp Quit	Останавливает задачу Administration Process на сервере.

Agent Manager Tell commands

Команда	**Результат**
Tell Amgr Pause	Приостановка расписаний для агентов.
Tell Amgr Resume	Возобновление расписаний для агентов.

Tell Amgr Schedule	Показывает список всех агентов, намеченных на текущий день. Кроме того, команда показывает тип запуска агента, время намеченное для агента, имя агента, имя базы данных, на которой будет запущен агент. При проверке менеджера агента список позволяет Вам видеть, ожидает ли агент в очереди менеджера агентов. Agent Manger queues: E - Agents eligible to run S - Agents scheduled to run V - Event-triggered agents waiting for their events to occur Trigger types: S - Agent is scheduled to run M - Agent is a new mail-triggered agent U - Agent is a new/updated document-triggered agent
Tell Amgr Status	Эта команда показывает “слепок” очереди менеджера агентов и показывает назначения менеджера агента в Server документе.
Tell Amgr Quit	Остановка Agent Manager на сервере.

Cluster Replicator Tell commands

Команда	**Результат**
Tell Clrepl Log	Делает запись информации в файл сервера LOG.NSF немедленно, не дожидаясь запланированного интервала log. LOG.NSF включает информацию относительно всех кластерных репликаций ожидающего повторения. Если Replica.Cluster.Retry.Waiting statistic не равна нулю, это означает, что некоторые репликации не закончены и ожидают повторения. После того, как Вы исправляете ошибки - например, перезапускаете сервер, который был недоступен - Cluster Replicator будет запущен на следующее повторение Replica.Cluster.Retry.Waiting statistic, установится в ноль.

Tell Clrepl Quit	Останавливает все Cluster Replicator на сервере. Чтобы запретить задачу Clrepl в будущих сессиях, удалите все упоминания Clrepl из ServerTasks в NOTES.INI файле. Запрещение Clrepl task на одном сервере, только останавливает репликации этого сервера на другие сервера, но не запрещает реплики на сервер, от других серверов в кластере.

LDAP Tell commands

Команда	**Результат**
Tell LDAP reloadschema	Модернизирует схему directory на LDAP сервере, чтобы отразить изменения, которые Вы настраиваете для Domino Directory.

NNTP Tell commands

Команда	**Результат**
Tell NNTP Newgroup *groupname*	Создание новой NewsGroup используйте эту команду для сознания NewsGroup, если она автоматически не создано в течение сессии.
Tell NNTP Newgroup Delete *group_name(s)*	Удаление указанной NewsGroup.
Tell NNTP Newgroup *groupname pathname*	Tells NNTP, чтобы добавить группу в Cache, с указанным NewsGroup и путем. Используется, когда группа создается на базу шаблона.
Tell NNTP print cache list	Отображается текущий список NNTP discussion groups и соответствующие им базы Notes.
Tell NNTP Print config	Отображение текущего списка значений NNTP.
Tell NNTP Quit	Остановка задачи NNTP.
Tell NNTP Reset *servername*	Повторная установка всех статей на сервере.
Tell NNTP Show Config	Показывает NNTP сервер конфигурацию, из секции NNTP документа сервера.
Tell NNTP Show Groups	Показывает имена и путь для NewsGroup на сервере.

Router Tell commands

Команда	**Результат**
Tell Router Delivery Stats	Показать статистику доставки задачи Router.

Tell Router Compact	Уплотняет MAIL.BOX и чистит открытые очереди задачи Router. Вы можете использовать эту команду, чтобы уплотнить MAIL.BOX в любое время. Если существует более чем один MAIL.BOX, сконфигурированный для сервера. Каждый MAIL.BOX будет уплотнен последовательно. По умолчанию, MAIL.BOX автоматически уплотняется в 4 часа утра.
Tell Router Show Queues	Показывает почту ожидающую доставки.
Tell Router Exit	Остановка задачи Router на сервере.
Tell Router Use *databasename*	Создает базу данных Shared Mail, которую Вы определяете, и устанавливает в NOTES.INI переменную Shared_Mail=2, которая разрешает Shared Mail для доставки и перемещения почты на этот сервер. Databasename - полное имя базы данных shared mail, которую Вы выбрали для использования на этом сервере, включая каталог, например, SHARED.NSF. В дополнение к созданию базы данных Shared Mail, Domino автоматически создает файл по имени MAILOBJ.NSF в каталоге данных. MAILOBJ.NSF - связь баз данных, которая всегда указывает на фактическую базу данных Shared Mail, которую Router использует, чтобы хранить новую почту, доставляемую на сервер, во время разрешения Shared Mail.
Tell Router Quit	Остановка задачи Router на сервере.

Schedule Manager Tell commands

Команда	**Результат**
Tell Sched Stats	Показывает общее количество Reservations и Appointments в базе данных Free Time.
Tell Sched Show *username*	Показывает график для указанного пользователя на консоли сервера. Используйте эту команду, чтобы исследовать проблемы в базе данных Free Ttime.

Tell Sched Validate	Обновление значений базы данных Free Time на сервере. Обновление происходит по умолчанию в 2 часа утра; однако, Вы можете использовать эту команду, чтобы вынудить это происходить скорее. Другой способ вынуждать обновление, состоит в том, чтобы останавливать и повторно начать задачу Schedule Manager. Обновление может занимать некоторое время. Вы должны запускать эту команду на всех серверах, где файлы почты были удалены и или добавлены, чтобы гарантировать, что старая информация Free time удалялась, а новая добавлялась в базу. Не используйте эту команду, когда Вы добавляете нового пользователя. Процесс администрирования создаст документы Person для пользователей в Domino Directory перед созданием их почтовых файлов на их почтовом сервере. Schedule Manager наблюдает за созданием баз данных и автоматически обрабатывает файлы почты новых пользователей.
Tell Sched Validate *username*	Validates - информации для указанного пользователя. Эта команда быстрее, чем использование команды Tell Sched Validate, потому что позволяет Вам обрабатывать пользователей индивидуально, чем обработка всех данных на сервере.
Tell Sched Quit	Остановка задачи Schedule Manager на сервере.

Statistic Collector Tell Commands

Команда	**Результат**
Tell Collector Collect	Запуск Statistic Collection на всех указанных серверах и собирает сообщения статистики.
Tell Collector Quit	Остановка задачи Collect на сервере.

Web Navigator Tell commands

Команда	**Результат**
Tell Web Help	Просмотр всех команд Web Navigator на консоли сервера.
Tell Web Refresh	Переинициализация всех глобальных назначений Web Navigator. Используйте эту команду, если Вы редактировали документ администрирования, во время работы задачи Web сервера

Tell Web Quit	Остановка всех запущенных копий Web Navigator.

Web Server Tell commands

Команда	**Результат**
Tell HTTP Restart	Переинициализирует Web сервер с изменениями, сделанными в: *1260 Документе сервера для Web сервера *1261 File Protection, Virtual Server и URL Mapping документах в Domino Directory. *1262 NOTES.INI файл, которые затрагивают задачу HTTP *1263 HTTPD.CNF и BROWSER.CNF файлы *1264 Изменения Java servlets или servlets.properties файлов Эта команда имеет тот же самые результаты как остановка и рестарт Web Server. Однако, эта команда Tell быстрее, чем остановка или рестарт, потому что, когда Вы используете команду Tell, задача HTTP остается в памяти. Если любые процессы HTTP активны, когда Вы запускаете команду, Domino ждет до конца процессов перед рестартом HTTP. HTTP не будет, однако, принимать никакие новые запросы, пока команда рестарта не заканчивает работу. Эта команда удаляет из памяти кэшированные станицы пользователя.
Tell HTTP Show File Access	Показывает информацию относительно защиты системных файлов на машине и на виртуальных серверах, если Вы имеете такие.
Tell HTTP Show Security	Показывает информацию по SSL и файлу Key Ring сервера, включая информацию относительно того, запущена ли серверная задача SSL на машине. Показывает информацию относительно SSL для виртуальных серверов, если Вы имеете такие.
Tell HTTP Show Users	Показывает имена пользователей и их IP адреса, истечения времени сессий для пользователей зарегистрированных на сервере, только которые использует базовую идентификацию.
Tell HTTP Show Virtual Servers	Показывает виртуальные сервера, запущенные на Вашем сервере.
Tell HTTP Quit	Остановка задачи Web сервер.

2.17.2.30 Trace

Используйте команду Trace, чтобы проверить связь с сервером. Эта команда показывает детальную информацию относительно каждого перехода через сервер и полезна при поиске проблем и поиска неисправностей сети. Эта команда работает так же как Трассировка, когда Вы выбираете - Файл – Параметры – Параметры настройки.

Чтобы проследить путь к серверу, введите:

```
Trace servername
```

Чтобы проследить определенный порт, введите

```
Trace portname!!!servername
```

Когда Вы пытаетесь соединяться с сервером, значок сети автоматически появляется в строке статуса, рабочего места Notes или на консоли сервера, в зависимости от того, где Вы ввели команду попытки связи. Вы можете использовать установку NOTES.INI – Console_LogLevel, чтобы управлять уровней деталей информации, которая будет выводится в строке статуса. Информация будет регистрироваться в файле log (LOG.NSF).

2.18 Задачи сервера.

Задачи сервера Domino исполняют сложные процедуры администрирования - например, уплотнение баз данных или обновление индексов. Вы можете запускать задачи вручную, загружая их с консоли сервера. Или Вы можете запускать эти же задачи автоматически, когда запускаете сервер, добавляя имя в переменную ServerTasks или ServerTasksAt файла NOTES.INI файл. Кроме того, Вы можете создавать документ типа - Program document в Domino Directory, чтобы запускать задачу в намеченный Вами интервал времени.

Запуск задач из NOTES.INI.

Многие задач запускаются по умолчанию в определенное время. Вы можете наметить дополнительные задачи для запуска, редактируя одно из этих назначений в NOTES.INI файле:

*1265 **ServerTasks** - запуск задач автоматически, при запуске сервера

*1266 **ServerTasksAt** - запуск задач в указанное время

Запуск задач с консоли сервера.

*1267 Из клиента Domino Administrator, откройте консоль сервера, выбирайте - Консоль на закладке Сервер – Состояние.

*1268 Введите:

```
load taskname
```

Где `taskname` - имя задачи сервера, которой Вы хотите запустить.

Запуск задач, из документа Program document.

Чтобы запускать задачу на сервере в регулярно намеченное время или при запуске сервера, создайте Program document в Domino Directory. Вы можете также использовать Program document, чтобы управлять командным файлом OS/2, UNIX или программой API.

Если Вы создаете командный файл OS/2, UNIX, API программу, Вы можете использовать любые знаки в имени A-Z, 0-9, - _ /. Не используйте \ (наклонную черту влево) или любые другие знаки.

*1269 Из клиента Domino Administrator, откройте Domino Directory. Выбирайте представление Сервер и откройте документ сервера.

*1270 Выбирайте – Create – Server Program.

*1271 На закладке Basics заполните эти поля:

Поля	**Значения**
Program name	Имя задачи сервера, которую Вы хотите запустить. Для OS/2 сервера, Вы используете CMD.EXE как имя программы, включите описание ключей управления для команды.
Command line	Командная линия для запуска задачи, включая любые аргументы команды.
Server to run on	Полное иерархическое имя сервера, на котором вы планируете запустить задачу.
Comments	Комментарии

*1272 Выбирайте закладку Schedule и затем заполните эти поля:

Поля	**Значения**
Enabled/disabled	Выбирайте одно: *1273 Запуск программы при запуске сервера. *1274 Разрешение графика запуска для задачи в определенном промежутке времени.
Run at times	Время первого запуска программы.
Repeat interval of	Интервал повторения.
Days of week	Дни недели для запуска Вашей программы

*1275 (Необязательно) Щелкают на закладке Administration и вводят в поля имена администраторов.

*1276 Сохраните и закройте документ.

Примечание, чтобы просмотреть все задачи, намеченные для выполнения на сервере, используйте команду – Show Schedule.

3 Администрирование пользователей и групп.

3.1 Пользователи Notes.

Пользователи Notes - люди, кто используют клиента Notes Domino для доступа к серверам и базам данных. Они имеют ID файл Notes, Person документ и если они используют почту Notes, то почтовый файл.

Чтобы зарегистрировать пользователей Notes рассмотрите следующие вопросы. Регистрировать ли их в Notes или мигрировать их из другой, внешней почтовой системы или каталога. Прежде, чем Вы начинаете добавлять пользователей, лучше определить назначения по умолчанию, которые Notes применит в течении процесса регистрации.

Чтобы добавить пользователей, Вы регистрируете их соответствующим ID сертификатора. При регистрации создается ID пользователя, который позволяет Вашим пользователям соответствующий доступ к системе. После регистрации пользователей Notes, Вы должны подготовить файлы установки, для установки Notes на рабочих станциях.

Чтобы разрешить использовать пользователям Notes, Вы исполняете эти задачи:

*1277 Определяете назначения по умолчанию, для рабочего пространства пользователя и регистрации пользователей.

*1278 Регистрируете пользователей.

*1279 Сделайте, доступ к файлам установки Notes, чтобы пользователи смогли устанавливать Notes.

В дополнение к пользователям Notes, Domino сервер может поддерживать и других пользователей:

*1280 IMAP

*1281 LDAP

*1282 NNTP

*1283 POP3

*1284 Web

3.1.1 Определение установок по умолчанию для пользователей.

Прежде, чем Вы будете регистрировать новых пользователей Notes, Вы можете определить некоторые установки по умолчанию, которые Notes будет применять для всех пользователей регистрируемых Вами. Назначения по умолчанию делают регистрацию пользователей более легкой и быстрой.

Вы можете определять по умолчанию - почтовый сервер пользователи, ID сертификатора, используемый для регистрации пользователей. Вы можете также определить по умолчанию список контроля управления для рабочей станции (ECL), чтобы защитить данные, от неправомочного доступа к рабочей станции.

После того, как Вы определяете назначения по умолчанию, имеются много способов изменить их. Вы можете редактировать документы, в которых Вы определили установки по умолчанию - например, документ профиля пользователя или предпочтения при

регистрации. Вы можете изменять эти назначения в диалоге регистрации для пользователей.

Чтобы определить назначения по умолчанию, используйте любую из этих задач:

*1285 Создайте Профиль установки пользователя, чтобы определить назначения для рабочего пространства пользователя по умолчанию.

*1286 Создайте список контроля управления для рабочей станции (ECL) - по умолчанию, чтобы управлять доступом к данным рабочей станции.

*1287 Определите предпочтение регистрации (в Administration Preferences) чтобы определить назначения для регистрации пользователя по умолчанию.

*1288 Определите назначения пользователя по умолчанию в диалоге регистрации пользователей.

3.1.2 Что такое - профиль установки пользователя?

Перед регистрацией пользователей, Вы можете создать - Профиль установки пользователя, который можно будет использовать в документе пользователя Место вызова, рабочей станции. Назначения по умолчанию, которые Вы определяете, могут включать интернет и Passthru сервера назначения, также как набор определенных баз данных, которые появляются на рабочем пространстве каждого пользователя. Профили установки пользователя, делают регистрацию пользователей легкой.

Когда Вы регистрируете пользователей, Вы связываете их с определенным профилем, так что они получают определенную группу назначений по умолчанию. Вы можете создать несколько профилей в Вашей организации, каждый будет уникальным для определенной группы пользователей. Например, Вы можете создать профили, для регистрации людей в отдел Маркетинга, или людей работающих на Восточном побережье.

Прежде, чем Вы создадите профиль, удостоверитесь, что Вы уже установили Вашу Domino систему и сделали следующего:

*1289 Установили Domain search сервер.

*1290 Web Navigator и InterNotes™ сервер (сервер хранит странички в базе Web Navigator)

*1291 Базы данных, которые Вы хотите, добавлять в рабочее пространство пользователя

*1292 Mobile directory каталоги (или клиент каталога)

*1293 Passthru сервера, LAN сервера, интернет сервера и удаленные сервера. Программа установки пользователя создает документы подключения в персональной адресной книге каждого пользователя, для серверов, которые Вы определяете в Профиле.

*1294 TCP/IP и NDS Notes name сервера

*1295 Host domains where Java applets are assumed to be safe

*1296 Proxy сервера

После создания профиля установки пользователя, Вы можете изменять или добавлять назначения и затем распределять новый профиль пользователям.

3.1.3 Что такое ECL рабочей станции?

ECL – список управления безопасность данных на рабочей станции. ECL ограничивает действия формул и скриптов, запущенных на рабочей станции. Например, ECL может запрещать некоторым пользователям, работающим на компьютере - стирать данные. Как администратор, Вы можете позволить пользователям изменять ECL, или управлять защитой рабочей станции сами.

Чтобы ограничивать доступ к рабочей станции, ECL ищет подпись в базах данных и шаблонах прежде, чем они будут открыты на рабочей станции. ECL проверяет эту подпись, чтобы определить уровень доступа. Каждая система и шаблоны приложений, поставляемых с Notes, содержат подпись. Каждый шаблон или база данных Ваших проектов должна содержать подпись разработчика приложения или администратора.

Чтобы создать ECL рабочей станции, программа Установки копирует ECL из Domino Directory на клиент Notes. Прежде, чем Вы регистрируете пользователей, редактируете ECL, чтобы создать ECL рабочей станции для пользователей.

ECL рабочей станции и опции безопасности.

Выберите из этих опций нужные Вам, для ECL рабочей станции:

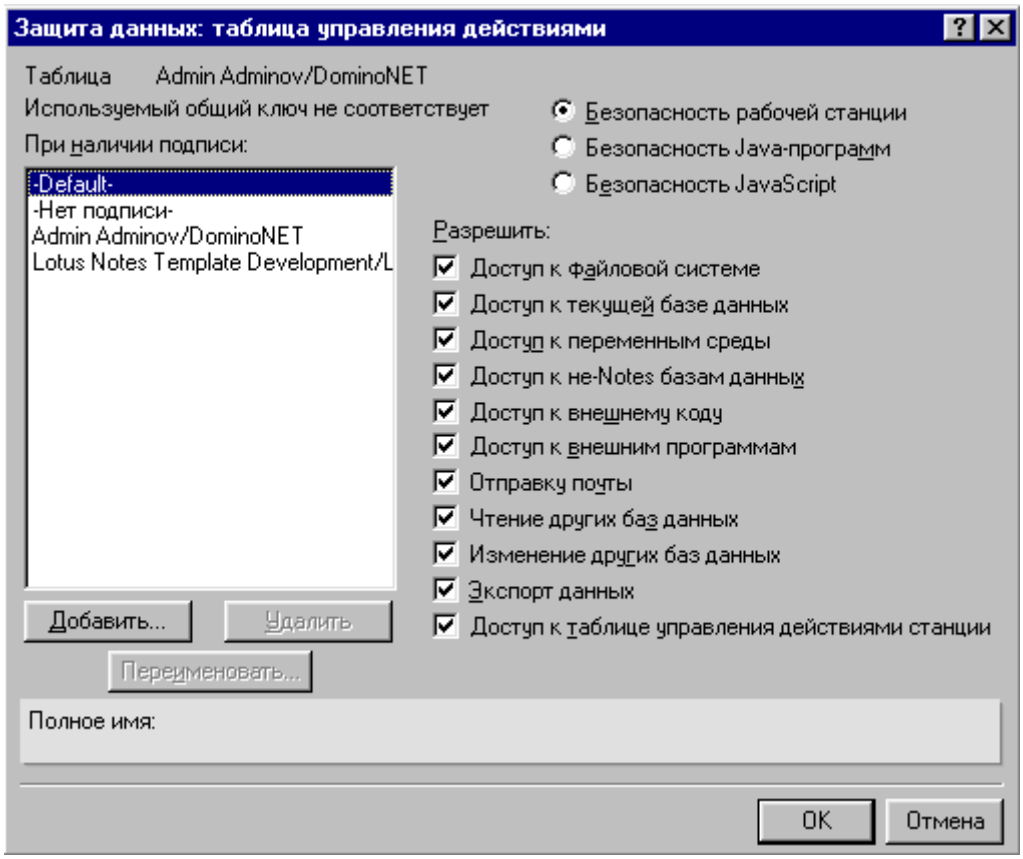


Рис. 59 Диалоговое окно настройки безопасности рабочей станции Notes.

3.1.3.1 Пример ECL.

Таблица описывает доступ для пользователей:

*1297 -Default-

*1298 -No Signature-

*1299 */Acme

*1300 Lotus Notes Development/Lotus Notes

*1301 Phyllis Spera/Sales/East/Acme

Подпись	**Применяются к**	**Пример**
-Default-	Формулы и коды, которые содержит подпись, не соответствуют никакой записи в ECL	Если пользователь – John Andrews/Atlas, ECL использует -Default- тип подписи, чтобы назначить доступ, потому что, хотя база данных содержит подпись, она не соответствует никакой записи в ECL.
-No Signature-	Формулы и коды, которые не содержат подписи	Если лицо содержит не действительную или не доступную подпись, ECL иденфицирует ее как -No Signature-.
Lotus Notes Template Development / Lotus Notes	Каждый шаблон, отправленный с Domino, содержит эту подпись	Подпись лица соответствует Lotus Notes Template Development / Lotus Notes signature.
*/Acme	Формулы и коды, содержащие подписи */Acme	Если подпись *anyname*/Acme, для примера Emily Marks/Acme или Alan Jones/Sales/East/Acme – ECL сопоставляет ее с */Acme.
Phyllis Spera/Sales/East/Acme	Формулы и коды подписанные Phyllis Spera/Sales/East/Acme	Подпись сопоставляется только с Phyllis Spera/Sales/East/Acme.

3.1.3.2 Создание ECL для рабочей станции.

*1302 Из клиента Domino Administrator, выбирайте закладку – Файлы.

*1303 Из панели Сервера, выбирайте сервер, с которым хотите работать.

*1304 Открывайте Domino Directory (NAMES.NSF).

*1305 Выбирайте из меню Действия – Edit Administration ECL.

*1306 Выбирайте – Default - и затем выбирает опции доступа.

*1307 Выбирайте – No Signature - и затем выбирайте опции доступа.

*1308 Выбирайте – Добавить, введите имя пользователя или сервера и затем - OK.

*1309 Введите звездочку (*), чтобы позволить доступ всем пользователям, даже тем которые не внесенные в “Domino Directory”. Введите звездочку (*) сопровождаемую

именем сертификатора - например, */Acme - чтобы позволить только пользователям сертифицированным иметь доступ.

*1310 Позволяйте пользователям изменять ECL на их рабочий станциях, или позволяют Java applets от доверенных отправителей. Выбор Позволяет пользователям изменять и выбирать соответствующий выбор.

*1311 Выбирайте - OK.

Запрещение опций безопасности для рабочей станции.

Если Вы работаете в хорошо защищенной среде, Вы можете запретить акция безопасности данных на рабочей станции. Однако, знайте, что после того, как Вы запретите ECL на рабочей станции, данные окажутся уязвимы для вмешательства из вне.

Чтобы запретить опцию безопасности на рабочей станции. Нужно изменить администраторские настройки ECL. Разрешите в ECL все опции, для типа подписей - Default-, -No Signature-, Lotus Notes Template Development/Lotus Notes и других имен подписей внесенных в список.

Обновление ECL для рабочей станции.

Если Вы изменяете, административные настройки ECL после пользовательской установки, которая автоматически копирует ECL на их рабочие станции, Вы можете заменить ECL.

*1312 Удостоверитесь, что Domino Directory, с изменениями ECL реплицировалась по домену.

*1313 Напишите записку пользователям, чьи ECL Вы изменили.

*1314 Добавьте кнопку в записку, которая выполнит формулу при нажатии.

```
RefreshEcl (" "; " ")
```

*1315 Опишите цель записки и инструктируйте пользователей, что делает эта кнопка.

*1316 Отправьте записку пользователю.

3.1.4 Процесс регистрации пользователей.

Вы должны регистрировать пользователей прежде, чем они устанавливают Notes на их рабочих станциях. Для каждого пользователя, в процессе регистрации создает:

*1317 Документ Person в Domino Directory

*1318 ID пользователя, содержащий сертификат Вашей организации

*1319 Почтовый файл пользователя

Notes предлагает различные опции для регистрации пользователей. Например, использование базовой регистрации пользователя. Он быстр и легок, потому что он автоматически делает многие назначений по умолчанию для пользователей. Если Вы используете регистрацию пользователя Выборочного типа, Вы можете назначать более продвинутые значения, типа добавления пользователя к группе WindowsNT. Вы можете также регистрировать пользователей, импортируя их из текстового файла или мигрируя их из других почтовых каталогов.

Если Вы используете процесс регистрации пользователей, чтобы регистрировать пользователей, Вы можете просматривать и изменять назначения пользователя базы данных Очереди Регистрации Пользователя (USERREG.NSF), которая появляется в диалоге регистрации. Эта база данных содержит информацию относительно пользователей, ожидающих регистрации. Когда Вы выходите из диалога регистрации пользователей, Вы можете сохранять всех пользователей, ожидающих регистрации и регистрировать их позже. Когда Вы открываете базу снова, база данных Очереди Регистрации Пользователя автоматически открывается, чтобы показать всех пользователей, ожидающих регистрации. Не пробуйте изменить информацию пользователя, открывая базу данных, непосредственно, Вы рискуете нарушить целостность данных при регистрации.

Прежде, чем Вы зарегистрируете пользователей, рассмотрите иерархическую схему имен Вашей организации и решите, где каждый пользователь будет располагаться в этой схеме. Просмотрев схему имен, Вы определите, какой ID сертификатора использовать, для регистрации пользователей, какой сервер использовать, как Сервер Регистрации, и какой сервер будет хранить почтовые файлы пользователей. Когда Вы регистрируете пользователей, Вы должны иметь соответствующий доступ к каждому серверу, который Вы используете, Вы должны знать пароль для каждого ID сертификатора, который используете.

Пример регистрации Notes пользователей.

Далее описывается, как администраторы в корпорации Acme зарегистрировали двух пользователей, использую принцип основанный на месте положения каждого пользователя в иерархии организации. Пользователи работают в различных отделах.

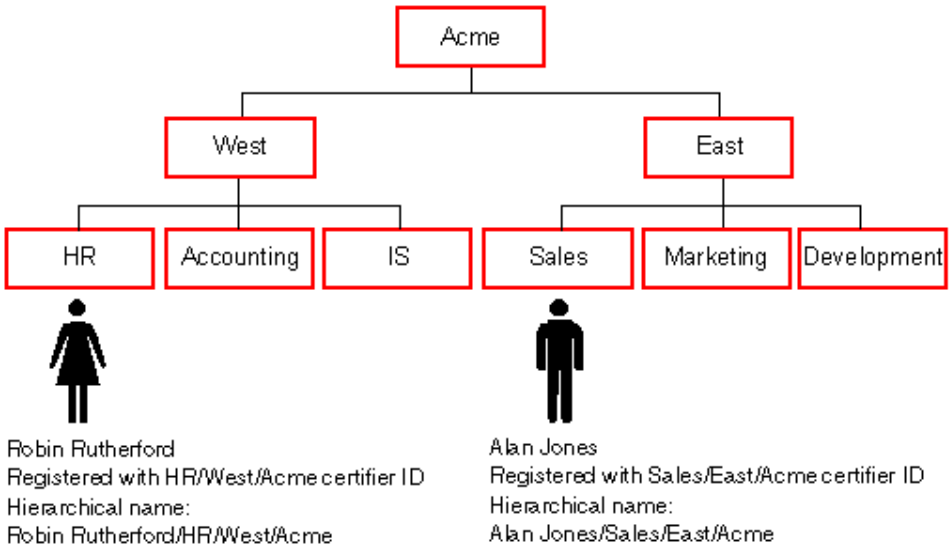


Рис. 60 Пример регистрации пользователей с использованием разных сертификатов в Acme.

Alan Jones работает в коммерческом отделе восточного побережья Acme. Чтобы дать Alan, соответствующий доступ в пределах системы, администратор использует ID сертификатора Sales/East/Acme, чтобы зарегистрировать его. Полное иерархическое имя Alan Jones, становится Alan Jones/Sales/East/Acme.

Администратор назначает Mail-E сервер, расположенный в сети восточного побережья Acme, как почтовый сервер для Alan Jones. Почтовый сервер Alan находится в той же

самой сети LAN, что и его рабочая станция, он получает и посылает почту, он может соединяться непосредственно с сервером, который хранит его почтовый файл.

Robin Rutherford работает в отделе бухгалтерского учета, на западном побережье. Acme Администратор использует ID сертификатора Accounting/West/Acme, чтобы регистрировать пользователя Robin. Mail-W - почтовый сервер для Robin, а ее полное иерархическое имя - Robin Rutherford/Accounting/West/Acme.

3.1.5 Методы регистрации пользователей.

Вы можете использовать любой из этих методов для регистрации пользователей Notes:

*1320 Базовая (по умолчанию) регистрация пользователей

*1321 Выборочная регистрация пользователя

*1322 Регистрация пользователей из текстового файла

*1323 Инструменты Миграции пользователей из других почтовых систем

Метод, который Вы используете, чтобы регистрировать людей, зависит от ряда причин включая такие опции, как:

*1324 Определили ли Вы назначения по умолчанию

*1325 Хотите ли Вы назначить пользователям дополнительные опции (типа дополнительных имен)

*1326 Должны ли Вы импортировать пользователей из внешней почтовой системы или почтовых каталогов, и находятся ли Ваши пользователи в текстовом файле.

Обратите внимание. При регистрации пользователей, в именах которых содержатся не-ASCII символы, модуль регистрации пытаются преобразовать любые не-ASCII в символы ASCII, чтобы создать адрес для интернет формата. Это не относится к нелатинским знакам, типа Арабского языка, Китайского, Кириллицы, Греческого, Иврит. Для этих языков, адрес интернета автоматически не присваивается. Администратор должен вручную создать адрес интернета для этих пользователей.

Базовая регистрация.

Для быстрой и легкой регистрации, используйте регистрацию по умолчанию. Основная регистрация требует, чтобы Вы определили имя пользователя и пароль, но также и предлагает Вам удобство, для некоторых назначений по умолчанию для пользователя. Вы можете определять назначения по умолчанию. Вы можете определять назначения в диалоге регистрации пользователей; или Вы можете использовать Notes назначения по умолчанию. Вы можете также назначать пользователей в определенные группы.

Все назначения, доступные в основной регистрации, доступны для Выборочной регистрации. Вы можете выбирать рассматривать и исполнять Выборочную регистрацию в любое время, щелкая на кнопке – Больше в окне диалога регистрации пользователей.

Выборочная регистрация.

Выборочная регистрация предлагает Вам все назначения, включенные в основную регистрацию, а также позволяет Вам изменять назначения по умолчанию. Определять дополнительные назначения - например, назначать дополнительное имя пользователю или добавить пользователя в группу WindowsNT.

Регистрация пользователей из текстового файла.

Имеются два способа регистрировать пользователей из текстового файла - файл, который содержит информацию об одном, или большего количества пользователей. Вы можете использовать диалог регистрации пользователя, который создает запись, для каждого пользователя в очереди регистрации и позволяет Вам изменять назначения индивидуально. Альтернативно, Вы можете регистрировать их непосредственно так, чтобы введенные персоны никогда не появился в очереди регистрации пользователя. Если Вы регистрируете их непосредственно, Вы назначаете пользователям определенные назначения прежде, чем Вы импортируете их и регистрируете их. Notes применяет назначения всем пользователям и не позволяет Вам изменять назначения пользователя индивидуально.

Миграция пользователей из других почтовых систем.

Вы можете мигрировать пользователи, из внешней почтовой системы или каталога в Notes. Вы регистрируете их, используя утилиту - Migration Tools. Обратится к меню, можно через кнопку – перенести пользователей в окне регистрации пользователей. После перемещения их, Вы можете изменять их назначения. Следующие типы пользователей Вы можете мигрировать в Notes:

*1327 Lotus cc:Mail

*1328 Microsoft Exchange

*1329 LDIF (LDAP Directory)

*1330 Microsoft Mail

*1331 WindowsNT

*1332 Novell GroupWise 4.1

*1333 Novell GroupWise 5

*1334 Netscape Messaging Server

3.1.5.1 Использование Базовой регистрации пользователей.

Используйте базовую регистрацию пользователей, чтобы зарегистрировать пользователей и добавить пользователей к существующим группам. Чтобы сделать регистрацию, быстрой и легкой, базовая регистрация использует установки по умолчанию для всех пользователей.

Имена пользователей.

При добавлении пользователей, имена пользователя могут состоять из верхнего регистра и нижнего, алфавитных знаков (A- Z), чисел (0- 9), амперсанта (&), черты (-), точки (.), пробела ( ) или подчеркивания (_).

*1335 Для выполнения базовой регистрации, удостоверьтесь, что Вы имеете следующее, прежде чем Вы начинаете регистрацию:

*1336 Доступ к ID сертификатора и его паролю.

*1337 Доступ к Domino Directory с Вашего компьютера

*1338 Доступ Редактора или роль UserCreator к Domino Directory на сервере регистрации

*1339 Можете создавать новые базы на почтовом сервере, если Вы планируете создавать почтовые файлы пользователя в течение регистрации

*1340 Доступ к CERTLOG.NSF на регистрационном сервере

*1341 Из клиента Domino Administrator, выбирайте закладку – Пользователи и группы.

*1342 Из панели Сервер, выбирайте сервер, с которым будете работать.

*1343 Выбрать Domino Directory, и затем выбирайте – People.

*1344 Выбирайте - Domino Directory, затем выбирайте – Сервис – Пользователи – Зарегистрировать, из панели инструментов.

*1345 Введите пароль для ID сертификатора и выбирайте - OK.

Обратите внимание, что Notes использует ID сертификатора указанный в административных настройках, если таких не имеется, используется ID указанный в переменной CertifierIDFile из NOTES.INI.

(Необязательно) измените регистрационный сервер, выбирайте кнопку – Регистрационный Сервер, выбирайте сервер, который регистрирует всех новых пользователей, затем выбирайте - OK. Если Вы не определили регистрационный сервер в административных настройках, это сервер - по умолчанию:

*1346 Локальный сервер, содержащий Domino Directory

*1347 Сервер, указанный в переменной NewUserRegServer из NOTES.INI

*1348 Сервер администрирования

*1349 Введите короткое имя пользователя, для адреса интернета, которое автоматически будет подставлено в адрес. Чтобы изменить короткое имя или адрес интернета, выбирайте имя и введите новый текст.

*1350 Введите пароль для ID пользователя и выбирайте - OK.

*1351 Выбирайте – Добавить пользователя. Имя пользователя появляется в окне Очередь на регистрацию.

*1352 (Необязательно) добавлять пользователя к существующей группе:

*1353 Выбирайте – Группы

*1354 Выберите группу, или группы, чтобы назначить в нее пользователя и выбирайте – Добавить и затем щелкают кнопку – Применить.

*1355 Выбирайте – Регистрировать и затем - OK.

3.1.5.2 Использование выборочной регистрации пользователей.

Выборочная регистрация, предлагает все функции Базовой регистрации, но также позволяет Вам изменять назначения по умолчанию и применять некоторые расширенные назначения для пользователей.

Примечание. Вы можете изменять назначения пользователей в любое время, как только Вы добавите пользователя к очереди регистрации пользователей. Выбирайте пользователей из очереди и затем делайте необходимые изменения. Вы можете также изменять некоторые

назначения для нескольких пользователей сразу, выбирая пользователей в очереди и делая изменения.

Для выборочной регистрации пользователей, заполните поля в базовом окне регистрации пользователей:

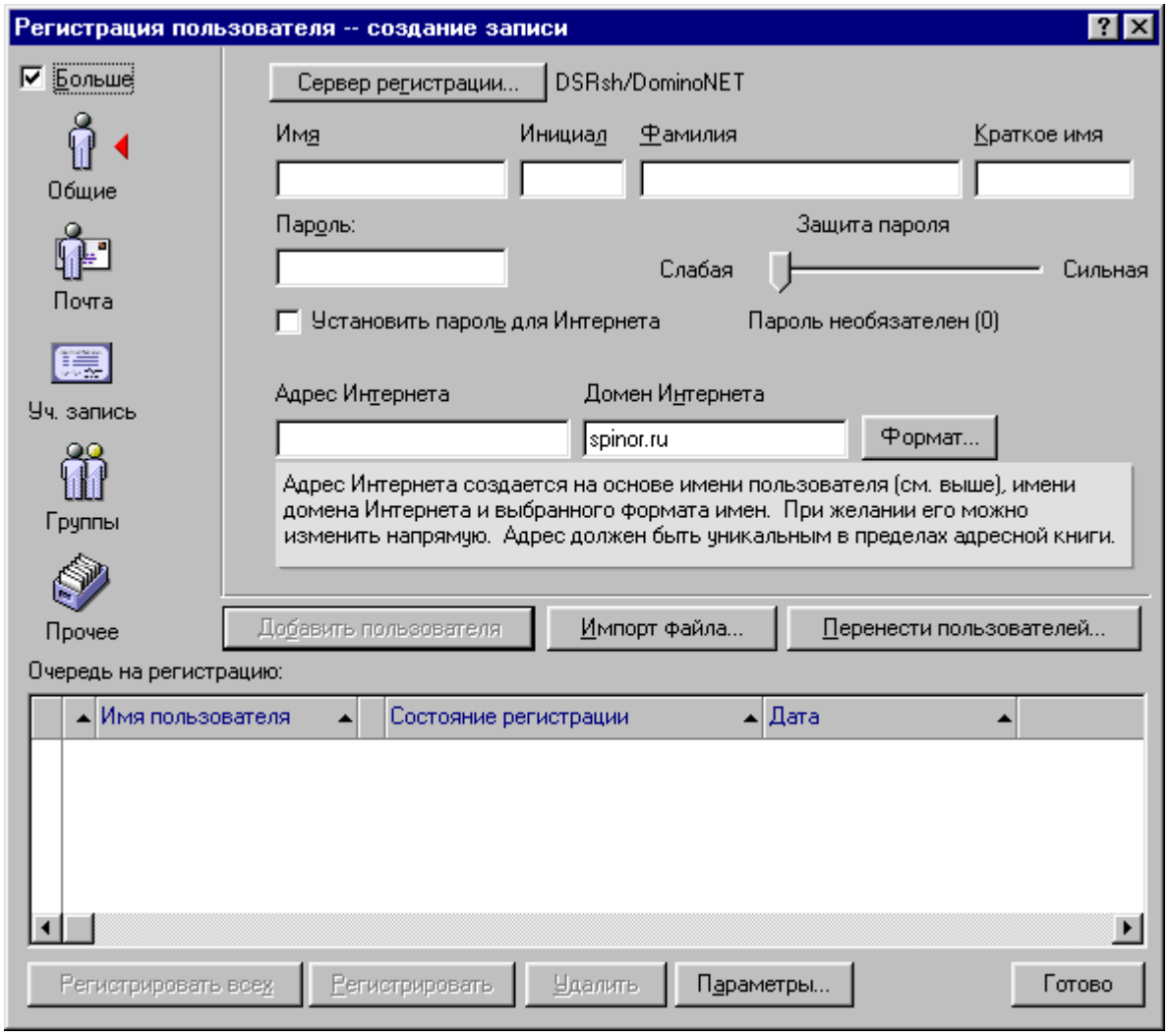


Рис. 61 Диалоговое окно регистрации пользователей, закладка Общие.

*1356 Выбирайте – Добавить пользователя. Имя пользователя появляется в окне Очередь на регистрацию.

*1357 Выбирайте – Почта и заполните любое из этих полей. Domino использует для любых полей, значения по умолчанию.

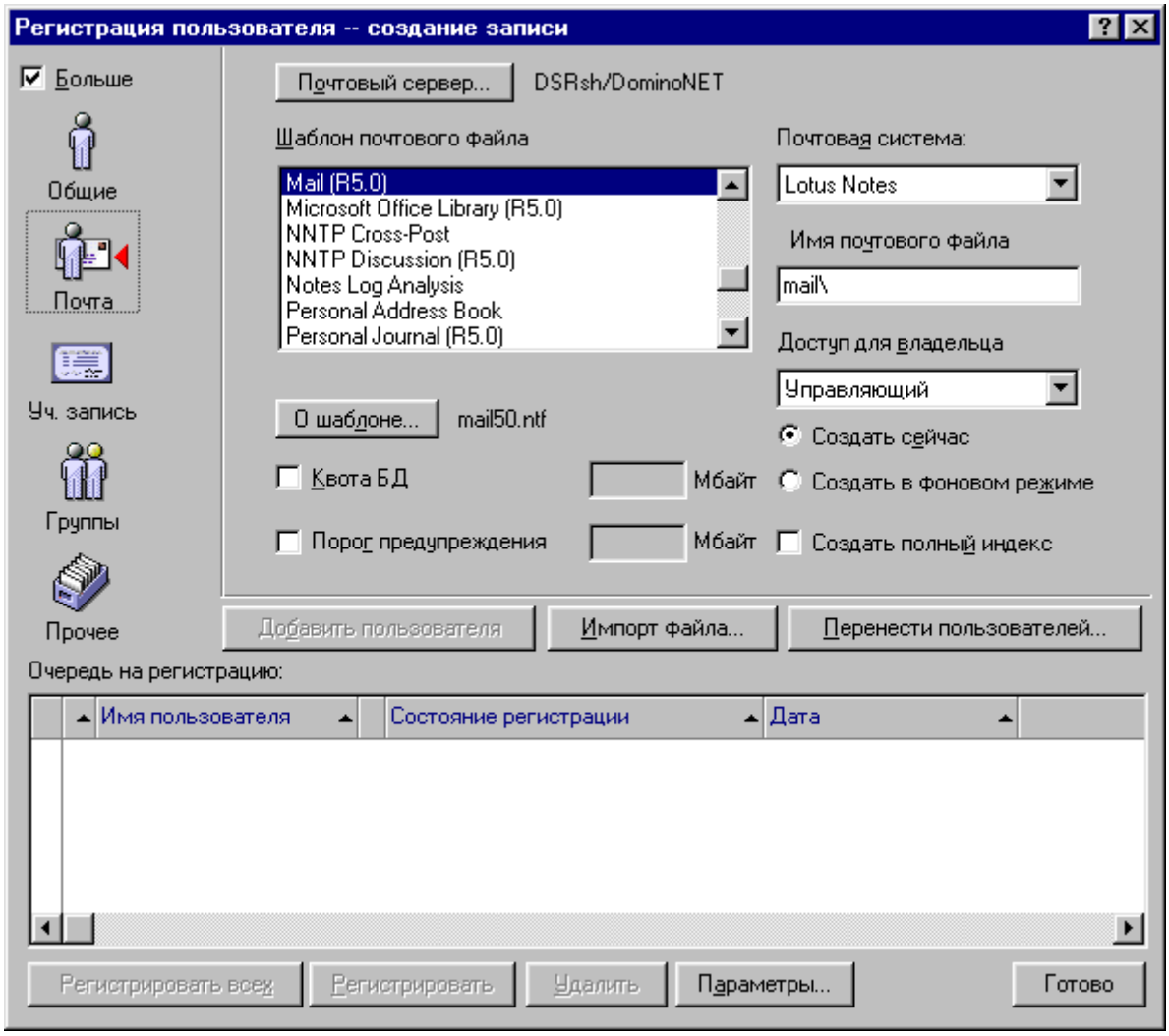


Рис. 62 Диалоговое окно регистрации пользователей, закладка Почта.

Поля	**Значения**
Почтовый сервер	Почтовый сервер для пользователя
О шаблоне	Шаблон для почтового файла по умолчанию MAIL50.NTF.
Почтовая система	Выбирайте тип почтовой системы для пользователя: *1358 Lotus Notes (по умолчанию) *1359 POP *1360 IMAP *1361 Other Internet *1362 Other *1363 None
Имя почтового файла	Имя почтового файла. По умолчанию почтовые файлы находятся в каталоге … Data\Mail\

Доступ для владельца	Уровень доступа к почтовому файлу пользователя. По умолчанию – Менеджер. Это поле может использоваться, чтобы предотвратить удаление собственного почтового файла. Если доступ владельца почтовому файлу будет немного ниже – Дизайнера, или Редактор - пользователь не сможет по ошибке удалить свой почтовый файл.
Квота БД	Выбирайте - Enable, если хотите ограничить размер почтовой базы пользователя (Maximum 10Гб).
Порог предупреждения	Выбирайте опцию, если хотите, чтобы Domino предупреждал вас о приближении к максимальному размеру почтового файла (Maximum 10Гб).
Создать сейчас/Создать в фоновом режиме	Выбирайте одно из двух: *1364 Создать сейчас (по умолчанию) *1365 Создать в фоновом режиме При выборе второй опции создание почтовых файлов вынуждает Процесс Администрации создавать файлы и экономит время процесса регистрации пользователя.
Создать полный индекс	Опция создание полнотекстового индекса.

*1366 Выбирайте - Уч. Запись и введите любые значения в поля. Domino использует значения по умолчанию, если это возможно.

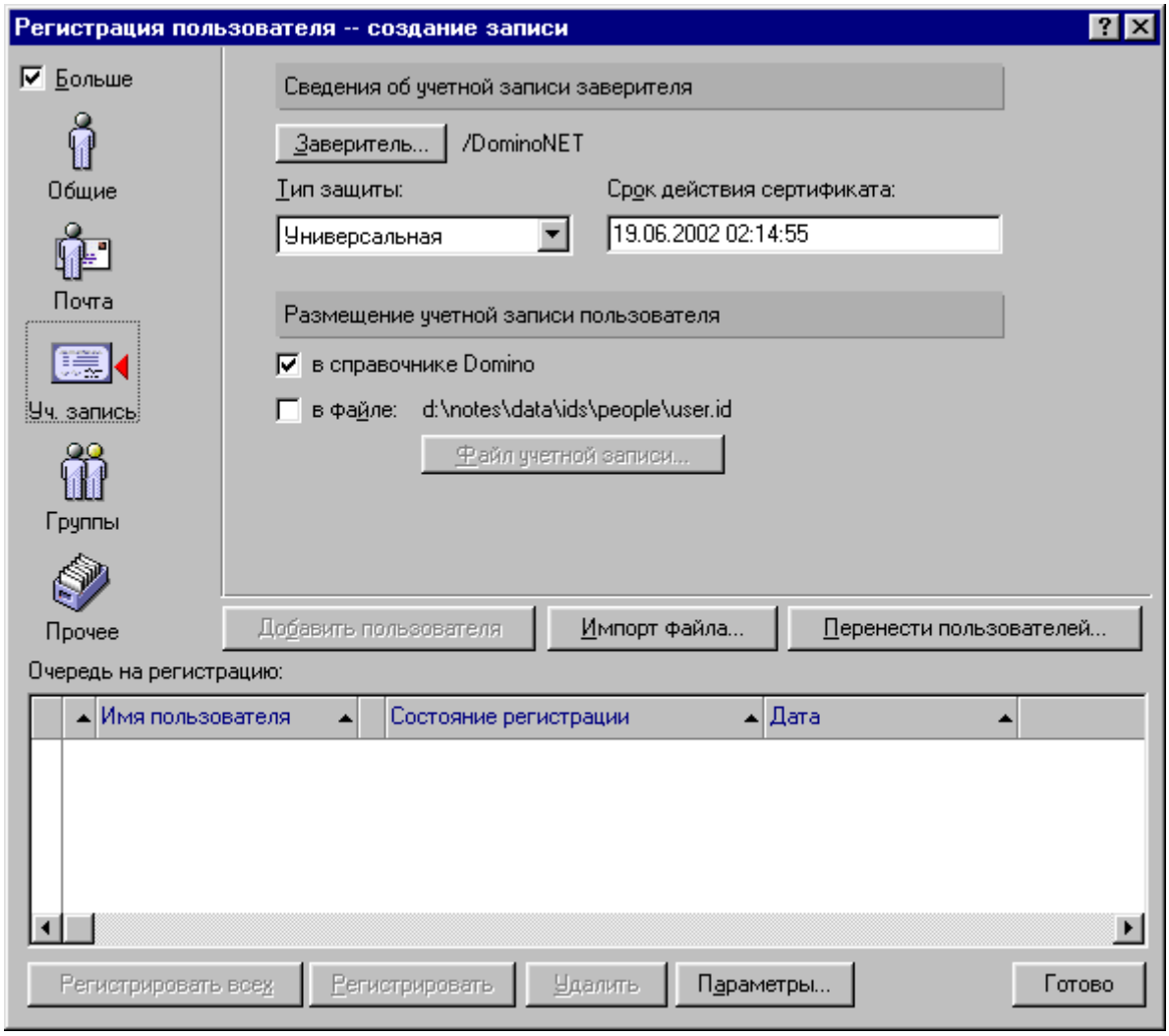


Рис. 63 Диалоговое окно регистрации пользователей, закладка Уч. запись.

Поля	**Значения**
Заверитель	Выбор используемого для регистрации сертификата.
Тип защиты	Тип лицензии: *1367 Северной Америки *1368 Универсальная *** Начиная с версии 5.0.4 – Global ***
Срок действия сертификата	Дата истечения Сертификата выданного пользователю.

Размещение учетной записи пользователя	Выбирайте одно из двух: *1369 По умолчанию в Domino Directory, присоединяет его к документу Person. *1370 В файл. По умолчанию: (<*datadirectory*>\ids\people*user.id*).

*1371 (Необязательно) вы можете добавить пользователя к существующей группе:

*1372 Выбирайте – Группы

*1373 Выберите Группу, или группы, чтобы назначать пользователю и щелкайте – Добавить.

*1374 Выбирайте – Прочие и заполните любые из этих полей. Domino использует установки по умолчанию, если они доступны, для полей.

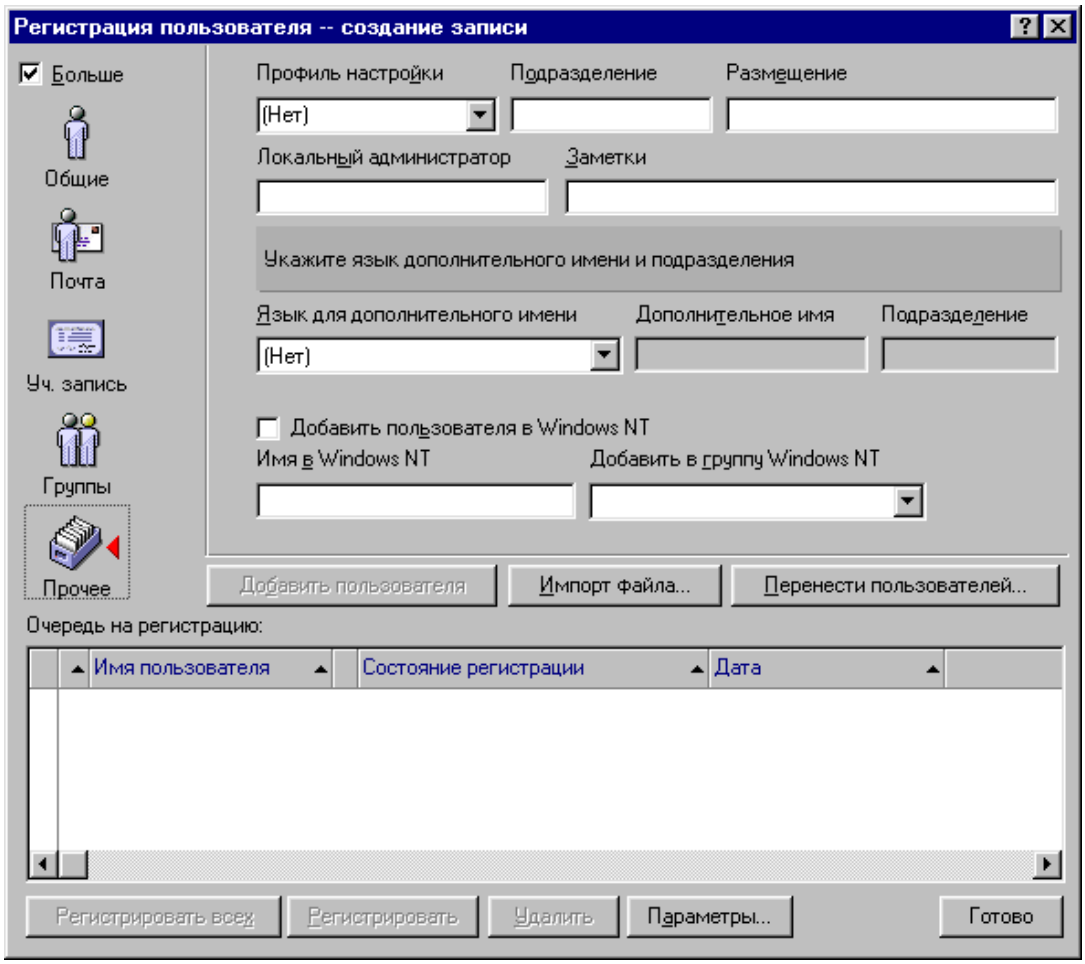


Рис. 64 Диалоговое окно регистрации пользователей, закладка Прочие.

Поле	**Значения**
Профиль настройки	Имя Профиля настроек

Подразделение	Вспомогательное слово, которое отличает пользователей с одинаковыми именами и работающими в одной организации.
Размещение	Местоположение пользователя
Локальный Администратор	Локальный Администратор, который будет иметь доступ автора к Domino Directory, Person документу.
Заметки	Любые комментарии
Язык для дополнительного имени	Альтернативное имя, с использованием другого языка.
Дополнительное имя	Альтернативное имя
Подразделение	Слово, которое отличает двух пользователей, имеющих то же самое имя и сертифицированных тем же самым ID сертификатором.
Добавить пользователя WindowsNT	Добавить пользователя в WindowsNT.
Имя в WindowsNT	Имя для WindowsNT
Добавить в группу WindowsNT	Добавить Имя в группу WindowsNT.

*1375 Выбирайте – Регистрировать и затем - OK.

3.1.5.3 Регистрация пользователей из текстового файла.

При регистрации пользователей из текстового файла, Вы можете импортировать их двумя путями:

*1376 Вы можете использовать диалог Регистрации Пользователей, который размещает пользователей в очереди на регистрацию, и позволяет Вам изменять назначения для пользователя индивидуально.

*1377 Через меню, которое обходит, очередь регистрации и регистрирует пользователей без разрешения, что-либо изменять. При использовании этого метода, Вы назначаете параметры, перед импортированием пользователей и Notes применит их ко всем пользователям.

Если Вы хотите добавить текстовый файл в NOTES.INI так, чтобы Notes не спрашивал Вас ничего, введите переменную BatchRegFile=filename в NOTES.INI. Вы можете все еще вводить имя файла.

Вы можете также определять разделитель для текстового файла, добавляя переменную BatchRegSeparator=(знак) в NOTES.INI. Если Вы не определяете переменную BatchRegSeparator, то точка с запятой (;) будет используется.

Все, описанные выше назначения для пользователей доступны Вам, перед использованием меню импорта для пользователей. Notes применяет назначения всем пользователям в группе регистрации из текстового файла.

Создание текстового файла для регистрации пользователей.

При создании текстового файла, создайте для каждого пользователя строку с параметрами. Введите в параметры для каждого пользователя в порядке, показанном в таблице ниже. Используйте точку с запятой, чтобы отделить параметры.

Например, эта строка в файле, определяет только фамилию и пароль:

```
Alexis;;;;password1
```

Эта строка в файле, определяет полное имя, домашний сервер, профиль установки пользователя:

```
Alexis;Catherine;R.;;password1;;;Marketing/Acme;;;;;;Marketing Profile
```

Обратите внимание, что минимальные параметры, это имя и пароль.

Позиция	**Параметр**	**Значение**
1	Last name	Фамилия пользователя
2	First name	Имя пользователя
3	Middle initial	Инициалы отчества
4	Organizational unit	Иерархическое имя организации
5	Password	Пароль
6	ID file directory	Каталог для ИД файла пользователя
7	ID file name	Имя ИД файла пользователя
8	Mail server name	Имя Почтового сервера
9	Mail file directory	Каталог почтового файла
10	Mail file name	Имя почтового файла
11	Location	Наглядная информация местоположения пользователя, которая добавляется к документу Персоны пользователя. Если кто-то адресует почту этому пользователю и имеется другой пользователь с тем же самым именем, Notes показывает местоположение, чтобы помочь отправителю отличить двух пользователей.
12	Comment	Комментарии
13	Forwarding address	Перенаправление всей почты на другой адрес, JSmith@acme.com
14	Profile name	Имя Профиля установки
15	Local administrator	Локальный Администратор. Доступ автора к Domino Directory, возможность редактирования Person document.

16	Internet address	интернет адрес для пользователя. Параметр нужен для пользователей Lotus Notes, POP3, IMAP почты.
17	Short name	Короткое имя. Используется для формирования интернет адреса
18	Alternate name	Альтернативное имя
19	Alternate org unit	Альтернативное название организации. Notes использует это для различия двух пользователей с одинаковыми именами
20	Mail template file	Шаблон для почтового файла

*1378 Из клиента Domino Administrator, выбирайте – Пользователи и группы.

*1379 Из панели Серверов, выбирайте сервер, с которым Вы собираетесь работать.

*1380 Выбрать Domino Directory и затем выберите – People.

В зависимости от того, как Вы хотите импортировать и регистрировать пользователей, Ваши шаги могут отличаться.

a) Регистрировать пользователей и применять индивидуальные назначения:

*1381 Из панели инструментов, выбирайте – Сервис – Пользователи – Зарегистрировать

*1382 Введите пароль для ID сертификатора и выбирайте - OK.

*1383 Выбирайте кнопку – Импорт из файла. Выбирайте текстовый файл – Открыть.

*1384 Чтобы изменять параметры пользователя, выберите пользователя из очереди регистрации и делайте Ваши изменения.

*1385 Выбирайте – Регистрировать, чтобы регистрировать отмеченных пользователей, в очереди регистрации.

b) Регистрировать пользователей группой:

*1386 Из панели инструментов, выбирайте – Сервис – Пользователи – Зарегистрировать из файла

*1387 Введите пароль для ID сертификатора и выбирайте - OK.

*1388 Выбирайте текстовый файл - Открыть.

*1389 Назначите глобальные назначения для пользователей если необходимо.

*1390 Выбирайте – Регистрировать.

3.1.6 Для чего используются группы?

Группы - списки пользователей, групп и серверов, которые имеют общие черты свойств. Они полезны для списков адресов и списков контроля доступа. Использование групп может упростить задачи администрации.

Например, если Вы создаете группу с именем - Terminations и внесете в нее всех уволенных служащих, Вы можете использовать имя группы в полях, Server документа, для запрещения доступа к этому серверу. Когда служащий увольняется из компании, Вы добавляете его имя к группе Terminators, затем реплицируете Domino Directory на другие сервера Вашего домена. Использование группы Terminations, экономит Ваше время, когда вы вручную добавляете имена в каждый Server документ.

Чтобы создать группу, создаете документ Group в Domino Directory. Вы можете добавить зарегистрированных пользователей в группу, в документ Group. Вы можете добавлять новых пользователей к группе, когда Вы регистрируете их. Предела числу имен, которые Вы можете добавлять к группе - нет. Однако общее количество знаков, используемых для имени группы, не может превышать 15КБ. Чтобы Вашими группами легче было управлять, распределите большой список Ваших пользователей на две или более групп.

По умолчанию, Domino Directory содержит две группы: LocalDomainServers и OtherDomainServers. LocalDomainServers включает в себя все сервера Вашего домена. Domino автоматически добавляет сервера, которые Вы регистрируете в домене к группе LocalDomainServers. Группа OtherDomainServers содержит имена всех серверов, которые не принадлежат Вашему домену. В группу OtherDomainServers, могут быт включены имена серверов других компаний, с которыми Ваша компания связывается.

Каждая группа должна иметь владельца, кто обычно является менеджером баз данных или администраторов.

Обротите внимание, что группа действует в пределах одного домена !

3.1.6.1 Создание и модификация групп

Вы можете создавать и изменять группы из клиента Domino Administrator. Вы также можете использовать Web Administrator, чтобы создавать и изменить группы. Вы можете включать одну или большее групп в пределы существующей группы, то есть создать группу и затем добавить одну или большее количество существующих групп, как членов новой группы. Для маршрутизации почты, Вы можете включать до пяти уровней групп. Для всех других целей, Вы можете включать до шести уровней групп.

Для создания Группы.

*1391 Удостоверитесь, что Вы имеете доступ Редактора или роль GroupCreator к Domino Directory на сервере.

*1392 Из клиента Domino Administrator, выбирайте закладку – Пользователи и Группы.

*1393 Из панели Серверов, выберите сервер, чтобы работать с ним.

*1394 Выбрать Domino Directory и затем выберите – Группы.

*1395 Выбирайте – Создать.

*1396 Введите название группы в поле Названия группы. Используйте любые из этих знаков: A-Z, 0-9, (амперсант, черта, пробел, подчеркивание, апостроф) для Имени. Название Группы может быть максимум 64 символов по длине. Для более легкого администрирования, используйте Имя без пробелов. Не используйте Имена, которое уже используются как название Орг. Единиц в иерархической схеме имен.

*1397 Выбирайте тип группы. Тип групп определяет цель группы и определяет представление в Domino Directory, где название группы появляется.

Тип групп	Описание
Многоцелевая	Универсальная группа для использования в mail, ACLs и т.д.
Управление доступом	Используется только для ACLs
Почта	Используется только для почты
Только серверы	Используется только для Групп Серверов
Отказ в доступе	Используется только для запрещения доступа. Administration Process не может удалить эту группу.

*1398 (Необязательно) Введите описание группы, в поле Описания.

*1399 Выбирайте кнопку Члены, выбирайте пользователей, сервера или группы, выбирайте – Добавить и затем - OK.

*1400 Выбирайте – Сохранить и Закрыть.

3.1.7 Как добавить альтернативный язык и альтернативное имя пользователю?

Альтернативное имя - позволяет Вам назначать два имени для пользователя, первичное имя и альтернативное имя. Первичное имя - интернационально, альтернативное имя распознается на родном языке пользователя. Прежде, чем Вы сможете добавить альтернативное имя пользователю, Вы должны добавить альтернативный язык и имя к ID сертификатора, которым Вы, потом заверяете существующий ID. Вы не можете добавить альтернативные имена серверам.

Дополнительные имена полезны, потому что они позволяют пользователям использовать их родной язык для отображения и поиска имен. Например, пользователь может вводить имя на родном языке, посылая почту или выбирать и показывать все документы в базе данных на родном языке.

Каждое альтернативное имя связано со спецификатором языка, который опознает родной язык имени. Типично, альтернативное имя вводится на родном языке пользователя, но Первичное имя определено интернациональным набором символов. Оба типа имен обеспечивается ту же самую безопасность в пределах Domino системы. Например, Вы можете использовать альтернативные или первичные имена в ACL или в группах.

Вы можете добавлять несколько альтернативных имен для сертификатора организации.

ID пользователя может содержать только одно альтернативное имя. Когда Вы назначаете альтернативное имя пользователю, альтернативное имя и спецификатор языка добавляется к пользовательскому ID, к сертификатам Notes, выпущенным для пользователя и, к Person документу.

3.1.7.1 Как добавить альтернативное имя – ID сертификатору?

В этой процедуре, Вы назначаете альтернативное имя и связываете с выбранным языком, сертификат организации ID и орг. Единицы, с использованием процесса сертификации. Вы сначала повторно сертифицируете сертификатора организации, а затем используете сертификат, чтобы повторно сертифицировать сертификат орг. единицы.

*1401 Вы должны иметь ID сертификатора, которому Вы хотите добавить альтернативное имя.

*1402 Из клиента Domino Administrator, выбирайте закладку – Настройка.

*1403 Выбирайте – Сервис и затем выбирайте – Заверение – Заверить.

*1404 Выбрать ID сертификатора и введите пароль.

*1405 Выбрать ID, который Вы хотите повторно сертифицировать, и введите пароль. Чтобы добавить Альтернативное имя к сертификатору организации, выбирайте тот же самый ID.

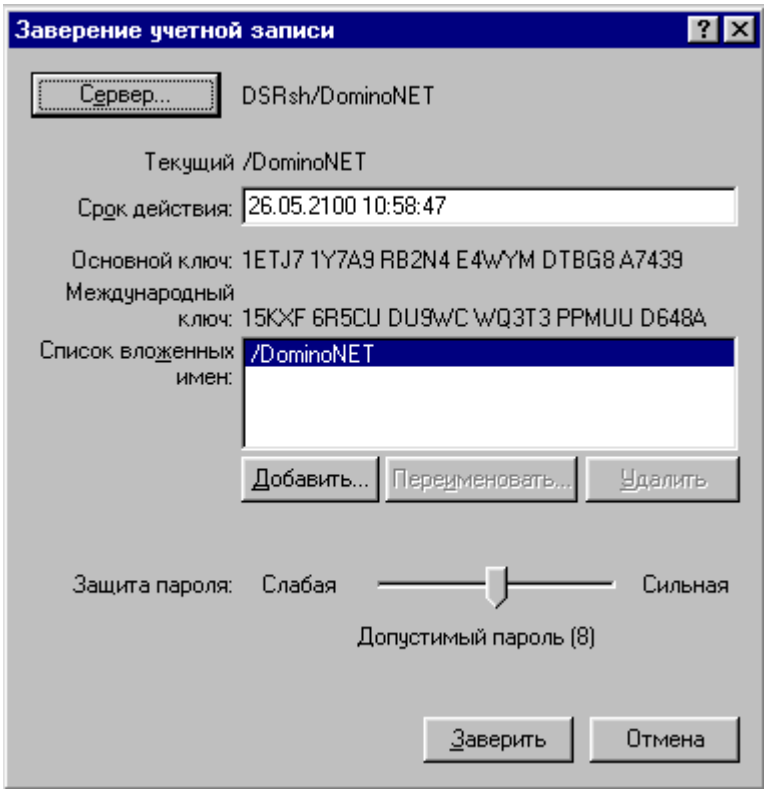


Рис. 65 Диалоговое окно ресертификации сертификатора.

*1406 Выбирайте – Добавить.

*1407 Выбирайте альтернативный язык в поле языка. Если Вы повторно сертифицируете орг. единицу сертификатора, доступные языки включают все языки, связанные с ID сертификатора организации.

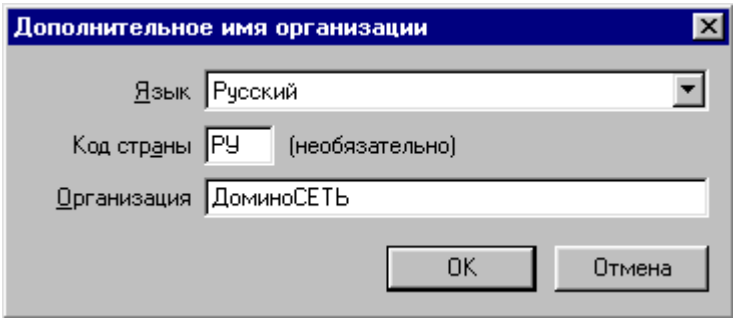


Рис. 66 Диалоговое окно выбора альтернативного языка для сертификатора.

*1408 (Необязательно) Входят признак страны для организации. Этот выбор доступен только для ID сертификатора организации.

*1409 Введите имя для орг. единицы в поле Организация.

*1410 Выбирайте - OK.

*1411 (Необязательно) добавьте другой альтернативный язык, выбирайте – Добавить.

*1412 Выбирайте – Заверить.

3.1.7.2 Как добавить Альтернативное имя конечному пользователю?

Используйте ID сертификатора, чтобы повторно сертифицировать пользователя.

*1413 Удостоверитесь, что ID сертификатора содержит альтернативное имя со спецификатором языка, который Вы хотите использовать.

*1414 Из клиента Domino Administrator, выбирайте закладку – Пользователи и Группы.

*1415 Из панели Серверов, выберите сервер, чтобы работать с ним.

*1416 Выбирайте Domino Directory, затем выберите представление – People.

*1417 Выбирайте соответствующий Person документ.

*1418 Выбирайте – Редактировать. Выбирайте закладку – Administration, заполните эти поля и затем щелкают – Сохранить и Закрыть:

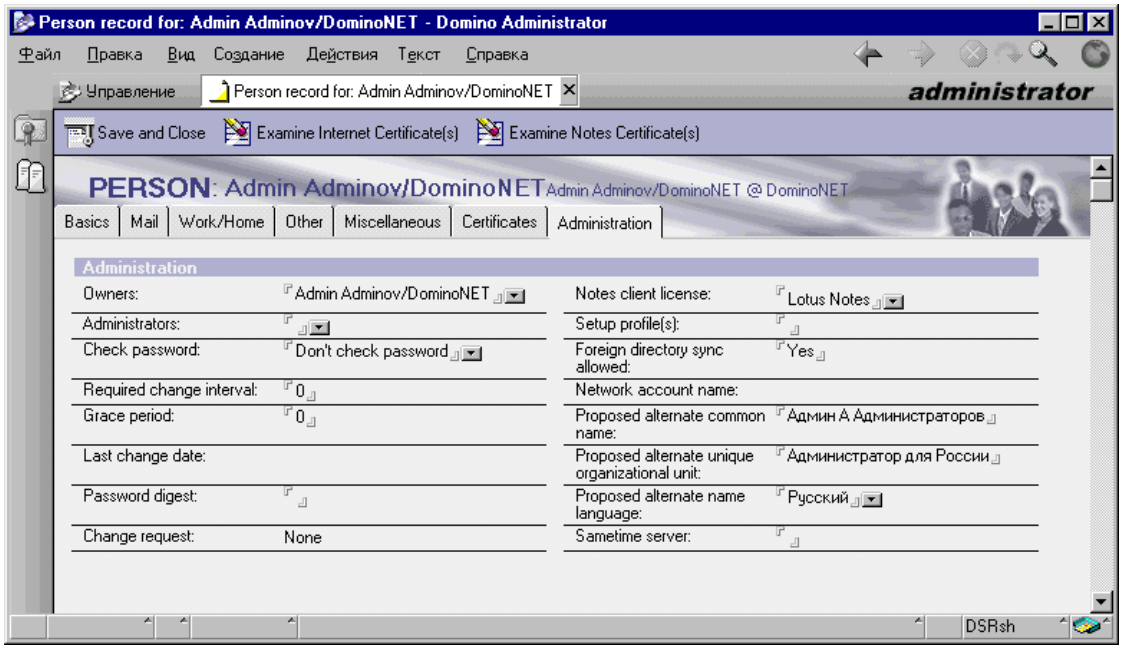


Рис. 67 Пример альтернативного языка в Person документе пользователя.

Поля	Значения

Proposed Alternate Common Name	Полное альтернативное имя (включая имя, первая буква отчества и фамилия). Не войдите иерархические компоненты имени здесь. Пользователь унаследует иерархические компоненты имени из ID сертификатора.
Proposed Alternate Organizational Unit	(Необязательно) Введите значение в поле подразделение. Это поле отличает двух пользователей с тем же самым именем. Это не связано с фактическим сертификатором орг. Единицы.
Proposed Alternate Name Language	Выбирайте альтернативный язык в этом поле.

*1419 Продолжите эти последние шаги, для каждого пользователя, чтобы назначить Альтернативное имя и затем отметьте все Person документы, чтобы сертифицировать их.

*1420 Выбирайте пользователей - Для ресертификации, выбирайте ID сертификатора и введите пароль. Этот процесс генерирует запрос Процесса Администрирования, запрашивает базу данных, чтобы при запуске Процесса Администрирования, он изменял документы Персон для каждого пользователя, и копировал эти изменения во все базы данных в домене.

3.1.7.3 Как добавить альтернативное имя при регистрации нового пользователя?

Прежде, чем Вы добавляете Альтернативное имя новому пользователю, удостоверитесь, что Вы имеете ID сертификатора, который содержит альтернативное имя и спецификатор языка, который Вы хотите использовать. Вы назначаете имя и язык в панели Прочее диалога регистрации пользователей.

3.2 Как выполнить миграцию пользователей из WindowsNT домена в Notes?

При использовании специального инструмента Notes Migration Tools for Microsoft WindowsNT из клиента Domino Administrator, Вы можете импортировать пользователей и группы пользователей из выбранного WindowsNT домена и регистрировать их как пользователей Notes.

Процесс перемещения включает в себя импортирование пользователей и группы из WindowsNT домена. При этом создаются записи для этих пользователей в Domino Directory, создаются Notes ID файлы и почтовые файлы пользователей.

3.2.1 Выбор WindowsNT домена, для импорта пользователей в Notes

Следующая процедура объясняет, как соединиться с WindowsNT доменам и получить список пользователей домена. После того, как Вы получите список, Вы можете импортировать пользователей, групп, для регистрации. Вы должны быть администратором или принадлежать к группе Account Operator, чтобы выполнить эту процедуру.

Обратите внимание, чтобы мигрировать пользователей WindowsNT в Notes, на компьютере, где запущен клиент Domino Administrator, должен иметь операционную систему WindowsNT. На компьютерах, с Windows 95 пользователи и группы не появятся среди списка доступных источников.

*1421 С рабочей станции администратора, где Вы установили клиента Domino Administrator, вставьте дискету, содержащую соответствующий ID Сертификаторов, для организаций или орг. единиц, в которых Вы будете регистрировать пользователей.

*1422 Из клиента Domino Administrator, выбирайте закладку – Пользователи и группы.

*1423 Из правой панели выбирайте – Сервис – Пользователи – Зарегистрировать.

*1424 Введите пароль для ID Сертификатора.

*1425 Удалите дискету, содержащую ID сертификатора, выбирайте - OK.

*1426 (Необязательно) Нажмите кнопку – Сервер регистрации - определите Сервер регистрации, если это необходимо и выбирайте - OK.

*1427 Выбирайте кнопку – Перенести пользователей.

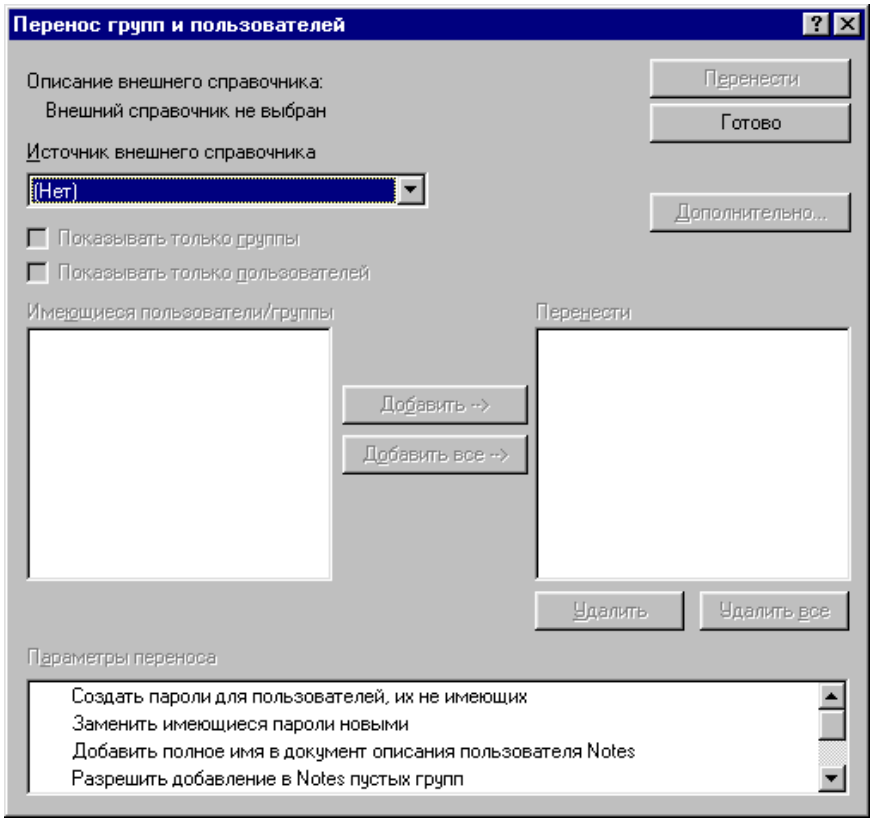


Рис. 68 Окно переноса пользователей из домена WindowsNT.

*1428 Из окна – Источник внешнего справочника, выбирайте – Пользователи/группы WindowsNT.

*1429 Определите WindowsNT домен, чтобы импортировать пользователей и выбирайте - OK. Вы можете выбирать домен из списка, или ввести имя различных доменов.

Обратите внимание, Если не появится диспетчер доменов для выбранного WindowsNT домена или он - не доступен, Вы увидите сообщение об ошибке.

3.2.2 Импортирование пользователей WindowsNT для регистрации в Notes

После того, как вы получите список пользователей и групп WindowsNT домена, выбирайте пользователей для перемещения, которых вы собираетесь переместить в Notes.

*1430 Из окна диалога Имеющиеся пользователи/группы, выбирайте пользователей, которых Вы планируете импортировать в течение текущей сессии и перенесите их кнопкой – Добавить ->, в правое окно с названием - Перенести.

*1431 Выбирайте кнопку Дополнительно, чтобы открыть окно диалога, которое позволяет Вам определять некоторые дополнительные опции для миграции пользователей из WindowsNT.

*1432 Выбирайте – ОК, когда Вы закончите определять пользователей.

*1433 Выбирайте – Перенести, чтобы перенести выбранных пользователей в очередь на регистрацию и выбирайте – Готово и потом - ОК, чтобы закрыть сообщение, которое указывает на статус и число пользователей добавленных в очередь на регистрацию.

*1434 Пользователи для регистрации теперь появляются в окне Очередь на регистрацию. Вы теперь готовы регистрировать пользователей.

3.2.3 Настройка опций миграции для пользователей WindowsNT

Вы можете настроить дополнительные опции, для определения информации, которая будет импортирована из WindowsNT домена. Опции, которые Вы определяете, относятся ко всем пользователям и группам, для импортирования из WindowsNT в течение текущей сессии.

В окне Параметры переноса, когда вы выбираете пользователей WindowsNT, Вы можете выбрать нужные опции. Чтобы отменить выбор опции, выбирайте ее второй раз.

Следующая таблица содержит список опций, доступных для мигрирования пользователей из WindowsNT домена:

Выбор	**Статус по умолчанию**
Создать пароли для пользователей их не имеющих	Вкл.
Добавить полное имя в документ описания пользователя Notes	Откл.
Заменить имеющиеся пароли новыми	Откл.
Разрешить добавление в Notes пустых групп	Откл.

Обратите внимание, что существующие пароли WindowsNT не импортируются. Если Вы запрещаете выбор назначения паролей, Вы должны будете назначить пароли для каждого пользователя, импортированного в очередь регистрации прежде, чем Вы можете регистрировать их.

Продолжайте процедуру импорта, определяйте дополнительные установки, нажимая кнопку Дополнительно. Вы устанавливаете Дополнительные Опции независимо для выбранного инструмента миграции. Вы можете применять различный набор опций для

системы. Опции, которые Вы выбираете, применяется ко всем пользователям, импортированным из данного домена в течение сессии.

3.2.4 Выбор способа конвертирования поля Full Names пользователя WindowsNT в Notes имя пользователя

Вы можете определить опцию для миграции, с использованием дополнительных параметров, как Имя Фамилия. Определение формата преобразования, позволяет интеллектуально преобразовать полные имена пользователей в имена Notes. Вы определяете формат преобразования следующим образом:

Из окна диалога Параметры обновления для пользователей WindowsNT, выбирайте формат из окна Имя Фамилия. Инструмент перемещения автоматически преобразует импортированные полные имена WindowsNT, в имена Notes с компонентами фамилии согласно указанному формату. Следующие форматы доступны:

Формат имени Notes	**Пример**
Имя Фамилия	Susan Salani
Обращение Имя Фамилия	Dr. Susan Salani
Имя Инициалы Фамилия	Susan R. Salani
Обращение Имя Инициалы Фамилия	Dr. Susan R. Salani
Имя Фамилия1 Фамилия2	Susan Miranda Salani
Обращение Имя Фамилия! Фамилия2	Dr. Susan Miranda Salani
Обращение Фамилия	Dr. Salani
Фамилия Имя	Salani Susan
Обращение Фамилия Имя	Dr. Salani Susan
Фамилия, Имя	Salani, Susan
Фамилия, Обращение Имя	Salani, Dr. Susan
Фамилия, Обращение Имя Инициалы	Salani, Dr. Susan R.
Фамилия 1 Фамилия 2, Имя	Miranda Salani, Susan
Фамилия 1 Фамилия 2, Обращение Имя	Miranda Salani, Dr. Susan

Понимание различий между именем WindowsNT компонентами имени Notes.

В WindowsNT, имеются два типа имен, связанных с пользовательским экаунтом, имя Unique User и Full Name. Имя пользователя WindowsNT состоит из набора символов (до 20) знаков и не имеет никакого формата. Full Name – имя необязательно и вообще представляет полное имя пользователя, сформатировано согласно соглашениям в Вашей организации, типа фамилия имя. Например, в WindowsNT, пользователь Susan Salani могла бы иметь пользователя, с именем ssalani, и полное имя Susan Salani.

В Notes, информация об имени сохранена как отдельное имя, буквы инициалов и фамилии. Например, имя Susan Salani сохраняется не как полное имя, а как отдельное имя Susan и фамилия Salani. Когда Вы импортируете имена из WindowsNT домена, Вы должны определить, как будут преобразованы полные имена пользователей NT, в компоненты имен Notes.

Выбор формата преобразования.

Когда Вы импортируете пользователей из WindowsNT домена, Вам доступен выбор формата преобразования, чтобы использовать его в преобразовании полного имени пользователя WindowsNT в компоненты имени Notes (Имя, Инициалы и Фамилия).

По умолчанию формат преобразования предполагает, что полные имена из WindowsNT домена преобразовывается в формат Имя Фамилия (например, Susan Salani). Если это вас не устраивает, используйте другой формат и выбирайте наиболее совместимый формат преобразования.

Если инструмент миграции не может преобразовать имя пользователя правильно - например, если число компонентов имени Full Name в WindowsNT, не равняется числу компонентов имени в указанном формате преобразования - появится окно предупреждения, диалога компонентов имени пользователя WindowsNT. Окно диалога предупредит Вас о том, что в полном имени слишком мало или содержит слишком много компонентов, для выбранного формат преобразования.

Пример. Если Вы определяете формат преобразования как Имя Фамилия, а поле Full Name содержится значение Susan Salani, диалоговое окно указывает, что компоненты были определены как, Susan поле имени, Salani поле фамилии. С другой стороны, если Вы выбираете тип преобразования как Фамилия Имя, а поле Full Name содержит значение Susan P. Salani, окно диалога указывает, что имеются слишком много компонентов, для преобразования в выбранный формат преобразования. Скорее всего, придется отказаться от некоторых дополнительных компонентов имени. Инструмент миграции определит компоненты имени пользователя в следующем порядке, Susan в поле фамилии, R. Salani в поле имени.

Несовместимый формат преобразования, может потребовать, значительного времени на редактирование имени, в формат Notes. Если Вы не проверили имена пользователей добавленных к очереди регистрации, убедитесь, что каждое имя имеет компонент фамилии. Notes требует, чтобы компонент фамилии присутствовал в имени пользователя WindowsNT.

Обратите внимание, что инструмент миграции только проверяет имя, НО пропускает компоненты имени при преобразовании компоненты для указанного формата. Он не проверяет компоненты в соответствующих полях и не проверяет поля на наличие недопустимых в применении символов. Например, инструмент миграции не проверяет, содержит ли первый компонент имени информацию или нет.

Импорт пользователей, у которых поле полного имени - пусто.

Если имеется пустое поле Full Name при импортировании из WindowsNT, инструмент миграции не заставляет Вас делать любые поправки. Вместо этого, автоматически добавляет имя пользователя WindowsNT в поле Фамилии Notes, независимо от указанного формата преобразования.

Пример. Если Вы импортируете пользователя с именем ssalani из WindowsNT домена, пользователь добавляется к очереди регистрации, при этом в поле фамилии вставляется ssalani, поле имени - пусто. Вы можете редактировать имя для этого пользователя, в

очереди регистрации, добавляя, например S или Susan в первую часть имени и в поле Фамилии – Salani.

3.2.5 Создание короткого имени Notes (Short Names) для пользователей WindowsNT.

Вы можете генерировать короткие имена Notes, для импортированных пользователей, основываясь на их именах в WindowsNT. По умолчанию имя пользователя WindowsNT будет добавлено как в поле Short Names и документы Person пользователя, но Вы его можете изменить в окне параметров пользователя перед регистрацией.

Short Name - по умолчанию назначается как имя почтового файла и ID файла пользователя.

Если Вы не выбрали значение для Short Name, Notes назначает Short Name первую букву имени пользователя, плюс первые семь букв фамилии, например ssalani, для Пользователя Susan Salani.

3.2.6 Регистрация пользователей и завершение миграции из WindowsNT.

После того, как Вы успешно импортируете пользователей в очередь регистрации, Вы готовы регистрировать их и закончить перемещение. В зависимости от опций Вы выбираете, процесс регистрации:

*1435 Создавать Notes Person документ и Notes ID для каждого мигрированного пользователя

*1436 Создавать файл почты Notes

Вы можете определить дополнительную информацию при регистрации пользователей для Notes, включая имя почтового сервера, тип лицензии, принадлежность к группам, имя орг. единицы, и т.д.

Обратите внимание. После того, как процесс регистрации начался, Вы не можете использовать рабочую станцию NT для запуска любой другой задачи, пока процесс не закончится. Если необходимо, Вы можете останавливать процесс регистрации, нажимая комбинацию клавиш CTRL+Break.

Процесс регистрации.

*1437 Из окна диалога регистрации пользователей, просмотрите информацию регистрации для каждого имени, которое находится в окне статуса регистрации, проверьте, что все введено правильно.

*1438 (Необязательно) Щелкают кнопкой – Параметры..., для выбора дополнительных опций, для этой сессии и щелкайте – ОК.

*1439 (Необязательно) Определите дополнительную информацию для регистрации пользователей, по мере необходимости. Если Вы создавали группу для перемещенных, открывайте панель групп и назначайте пользователей в эту группу.

*1440 Из окна Очередь на регистрацию, выберите пользователей и выбирайте кнопку – Регистрировать. Domino Administrator попытается регистрировать выбранных пользователей в порядке, в котором они были добавлены в очередь. Пользователи, которых Вы не выбираете, остаются в очереди для более поздней регистрации.

*1441 Процесс регистрации может требовать значительное количество времени, в зависимости от числа регистрируемых пользователей.

*1442 После того, как регистрация заканчивается, появляется сообщение, которое сообщает Вам о статусе регистрации. В случае неудачной регистрации пользователя, он остается в списке окна статуса регистрации, с сообщением статуса, указывающего на причину неудачи.

Проверьте, что перемещение было успешно для выбранных пользователей.

3.3 Как использовать WindowsNT User Manager для управления пользователями Domino сервера?

Когда Вы создаете новых пользователей, или группы в WindowsNT User Manager, Вы можете одновременно регистрировать пользователей или группы в Notes. Для пользователей, это означает создание Person документов, Notes ID, пароля и почтового файла для пользователя. Для групп, это означает создание Group документа и произвольную, регистрацию членов группы как пользователей Notes. Вы можете также регистрировать существующих пользователей WindowsNT или групп в Notes. Кроме того, Вы можете удалять пользователей Notes или группы, когда Вы удаляете их учетную запись пользователя, группы. Далее Вы можете синхронизировать существующих пользователей WindowsNT с пользователями Notes, для будущих действий.

Чтобы настроить WindowsNT User Manager, Вы должны закончить эти процедуры:

*1443 Разрешить опцию синхронизации в Notes.

*1444 Синхронизация пользователей WindowsNT и Notes.

3.3.1.1 Синхронизация пользователей и групп Domino и WindowsNT.

Если Вы запускаете Domino сервер на платформе WindowsNT, Вы можете синхронизировать пользователей и группы в Domino и WindowsNT. Тогда, Вы можете выполнять многие задачи администрирования или в Domino или в WindowsNT.

Когда Вы используете Domino, чтобы регистрировать, или удалить пользователя Notes или удалять группу Notes, Вы можете автоматически сделать обновление из User Manager for Domains (USRMGR.EXE). Наоборот, специальное меню опций, добавляется в WindowsNT, оно позволяет Вам определять, добавлять ли имена для пользователей сделанные в User Manager пользователь или группы в Domino Directory. Вы можете также добавлять существующего пользователя WindowsNT или группы в Domino Directory.

Например. Когда Вы добавляете, удаляете, или изменяете других пользователей при работе в WindowsNT. Все эти изменения автоматически будут сделаны в Domino Directory. Плюс, почтовый файл, ID пользователя Notes пароль, Notes пароль для интернет экаунта в WindowsNT, может быть создан, для каждого нового пользователя.

Эти особенности синхронизации каталога позволяют Вам держать, и Domino Directory и User Manager, без необходимости обновления, когда любые изменения будут сделаны.

Обратите внимание, чтобы использовать особенности синхронизации в WindowsNT User Manager, Вы, должно, установить WindowsNT Services для Domino. Вы можете получить доступ к этим опциям в течение установки программного обеспечения сервера.

3.3.1.2 Разрешение операции синхронизации Notes и WindowsNT User Manager.

Вы должны разрешить опцию синхронизации Notes, чтобы сделать Notes команды доступными Вам из меню Notes и WindowsNT User Manager.

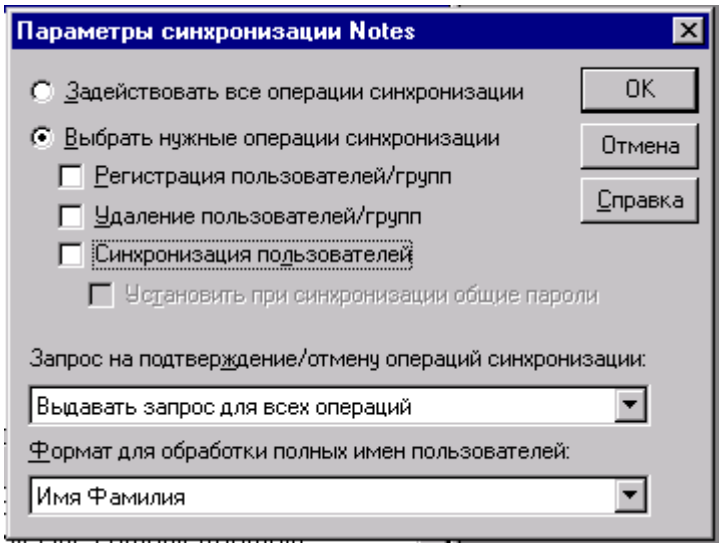


Рис. 69 Диалоговое окно параметров синхронизации пользователей Notes.

Примечание. По умолчанию, действия синхронизации не разрешены.

*1445 Из User Manager, выбирайте - Notes – опцию Notes Synchronization.

*1446 Заполните эти поля, затем выбирайте - OK:

Поле	**Значение**
Задействовать все операции синхронизации	Разрешите все действия синхронизации Notes, внесенные в список в поле Select synchronization operations to enable. Всякий раз, когда Вы исполняете одно из этих действий синхронизации в User Manager для домена, Вы разрешите исполнить те же самое действие в Notes.
Выбрать нужные операции синхронизации	Выберите одно из этого действия синхронизации Notes: *1447 Регистрация пользователей/групп новых или существующих пользователей WindowsNT и групп в Notes. Этот выбор позволяет добавлять отобранных NT пользователей/групп в Notes. *1448 Удаление пользователей/групп из WindowsNT, удаленных из Domino Directory. *1449 Синхронизация пользователей, в User Manager, которые изменяют имя в экаунте и в поле Person документа из Domino Directory.
Установить при синхронизации общие пароли	Синхронизировать пароль WindowsNT и Notes пароль интернета, когда Вы синхронизируете пользователей.

Запрос на подтверждение/отмену операции синхронизации	Запрос на подтверждение/отмену операций синхронизации: *1450 Выдавать запрос для всех операций (по умолчанию) *1451 Выдавать запрос для только для удаляемых пользователей/групп *1452 Не выдавать запрос для любых операций
Формат для обработки полных имен пользователей.	Формат для обработки полных имен пользователей: По умолчанию – Имя Фамилия.

Чтобы сохранить и применить изменения для следующей сессии в User Manager, выберите – Options – Save Settings on exit.

3.3.2 Синхронизация пользователей WindowsNT и Notes пользователей.

Если Ваша система имеет WindowsNT пользовательские экаунты, которые соответствуют Person документам в Domino Directory, Вы можете держать эту информацию в синхронизированном состоянии. Когда Вы синхронизируете WindowsNT и Person документы, эти изменения происходят:

*1453 Поле Network account name из документа Person пользователя, обновляется с именем экаунта пользователя WindowsNT.

*1454 Информация из поля Full name, пользователя WindowsNT, добавляется в поле User name документа Person, если это имя еще не существует в списке имен. Существующее полное имя в Person документе не изменяется.

*1455 (Необязательно) Пароль WindowsNT и пароль интернета в Person документе заменяется обычным паролем, который работает и для WindowsNT и для Domino Web доступа. Пароль интернета шифруется в Person документе.

Синхронизация пользователей также имеет место, когда NT пользователь переименован, с использованием User Manager. В этом случае, имя пользователя NT и поле Network account name, из документа Person обновляется, но пароли не синхронизируются.

Синхронизация пользователей не регистрирует пользователя Notes - то есть не создает Person документа, Notes ID и почтовый файл. Синхронизация пользователей может только изменять информацию в существующем документе Person.

Обратите внимание, если происходит ошибка в течение синхронизации пользователя - например, документ Person не может быть найден для NT сервера, сообщение ошибки будет появляться. Детали относительно ошибки также будут выведены в NT LOG файла.

Если Вы изменяете в WindowsNT имя пользовательского экаунта или полное имя пользователя, Вы можете запустить синхронизацию снова. Вы должны также запускать синхронизацию, если Вы хотите синхронизировать пароль WindowsNT с паролем Notes. Синхронизация пользователей будет успешна, если эти условия существуют:

*1456 Имя NT экаунта пользователя соответствует имени в поле Short name, имени в Person документе

*1457 Полное имя пользователя WindowsNT, соответствует полю User name, в Person документе

*1458 Имя Last name WindowsNT, соответствует имени в поле Last Name, в Person документе

*1459 Имя в поле Network account name, если имеется в Person документе, соответствует WindowsNT имени User Account.

Синхронизация пользователей WindowsNT и Notes пользователей.

Синхронизация пользователей WindowsNT и пользователей Notes должно закончится изменениями Person документов в Domino Directory.

*1460 Удостоверитесь, что Вы уже разрешили использование синхронизацию пользователей WindowsNT в User Manager.

*1461 В окне User Manager, выберите UserName пользователей, которых Вы хотите синхронизировать.

*1462 Выбирайте из меню – Notes – Синхронизировать выделенных пользователей NT с Notes.

*1463 Когда Вас запросят продолжать, выбирайте – Да.

*1464 Если Вы позволили синхронизирование пароля, введите и подтвердите пароль для первого пользователя, синхронизируете пользователя и затем щелкаете - OK.

*1465 Введите и подтвердите пароль для других пользователей, которых Вы синхронизируете, затем щелкайте - OK.

3.3.3 Использование WindowsNT User Manager, для домена Domino.

Вы можете выполнять следующие задачи для Domino сервера или WindowsNT:

*1466 Регистрировать новых пользователей. Вы можете добавлять пользователей в WindowsNT и регистрировать их в Domino как Domino пользователей или интернет пользователей. Для Domino пользователей, Domino создает Person документ, почтовый файл и ID пользователя. Для интернет пользователей, Domino создает Person документ, который содержит пароль интернета.

*1467 Удалять пользователей или групп

*1468 Переименовывать пользователей Domino, и автоматически переименовывать пользовательские экаунты WindowsNT

*1469 Создавать новые группы экаунтов WindowsNT и автоматически создавать их для Domino

*1470 Добавлять существующие группы WindowsNT в Domino и регистрировать пользователей этих групп в Domino

*1471 Создавать пароль для Domino и WindowsNT

*1472 Регистрировать существующих пользователей WindowsNT в Domino и включать их в группы

3.3.4 Изменение установок регистрации Notes для WindowsNT пользователей.

Каждый раз, когда Вы регистрируете пользователей, Вы можете изменять по умолчанию регистрацию для пользователя WindowsNT. Если Вы изменяете опции регистрации, User Manager не сохраняет назначения, когда Вы выходите из программы. Каждый раз, когда Вы запускаете User Manager, назначения возвращаются к первоначальным установкам по умолчанию.

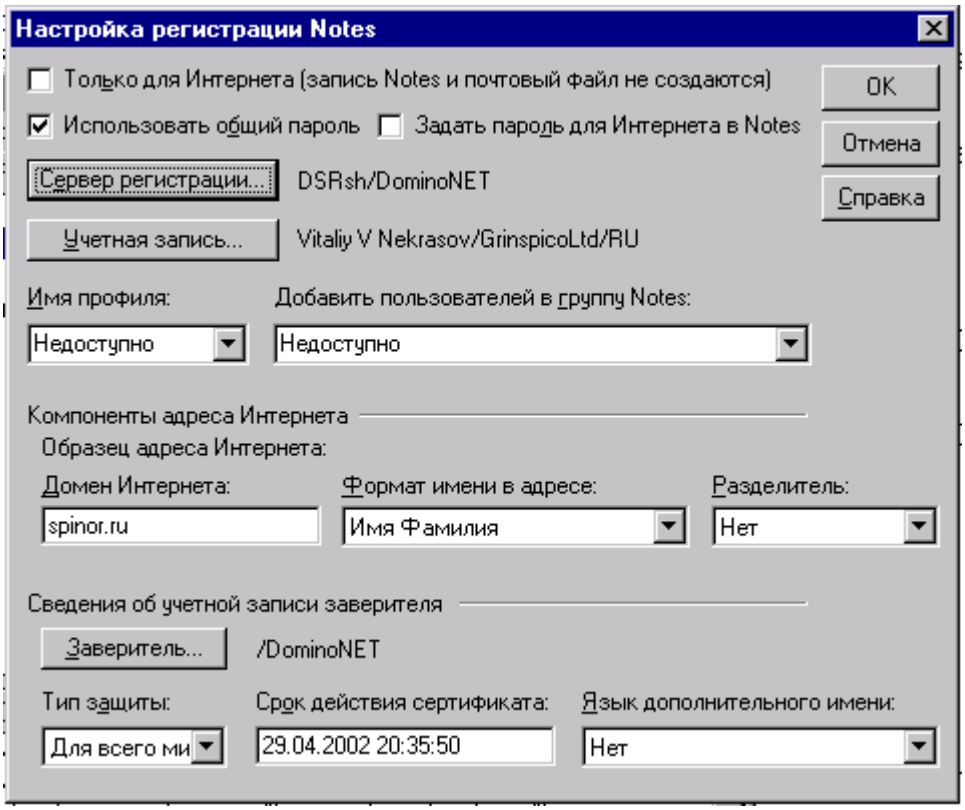


Рис. 70 Диалоговое окно настройки регистрации пользователей.

Поля Только для интернета (запись Notes и почтовый файл не создается) и Использовать общий пароль устанавливаются следующим образом:

*1473 Если опции Только для интернета (запись Notes и почтовый файл не создается) не выбрана, а Использовать общий пароль выбрана, поля компонентов интернет адреса и ID сертификатора показывают информационные поля.

*1474 Если опции Только для интернета (запись Notes и почтовый файл не создается) и Использовать общий пароль выбраны, информационные поля, об ID сертификатора - не показываются.

*1475 Если опции Только для интернета (запись Notes и почтовый файл не создается) выбрана, а Использовать общий пароль не выбрана, поля компонентов интернет адреса и ID сертификатора не показывают информационные поля.

Изменения опций регистрации по умолчанию.

Перед изменением опций регистрации по умолчанию, Вы должны разрешить опцию регистрации пользователей.

*1476 Из окна WindowsNT User Manager, выберите – Notes – Registration Setup.

*1477 Заполните, или измените, любые из этих полей и затем выбирайте - OK.

Поле	**Значение**
Только для интернета (запись Notes и почтовый файл, не создается)	Создается Person документы в Domino Directory с паролем интернета, но ID пользователя и почтовые файлы не создается. Позволяет Web, LDAP, или NNTP пользователям получать доступ к Domino Web серверу без рабочей станции Notes. Скрывает диалоги, связанные с Notes ID и с почтовыми средствами, типа полей адреса интернета. По умолчанию – не разрешено
Использовать общий пароль	Создается единственный пароль для WindowsNT и Notes. Вы можете изменить этот выбор для некоторых пользователей во время регистрации. Этот существующий NT пароль для NT пользователя, может быть заменен, общим NT/NOTES паролем, когда пользователи будут зарегистрированы. Это поле не видно, когда существующие пользователи зарегистрированы со случайными паролями. По умолчанию – разрешено
Задать пароль для интернета в Notes	Устанавливает пароль для интернет доступа для Domino Web сервера. Пароль интернета шифруется и устанавливается в поле пароля интернета в Person документе. Этот пароль обязателен, если выбрана опция Только для интернета (запись Notes и почтовый файл не создается) или если выбран тип почты - Другая почта интернет, POP3 или IMAP По умолчанию - не разрешено
Сервер регистрации	Регистрационный сервер для этой сессии, то есть Domino сервер, на котором будет создан Person документ в Domino Directory. Пользователи автоматически назначаются в тот же самый Notes домен выбранного сервера. Вы должны иметь соответствующий сертификат Notes ID, с соответствующим доступом к указанному серверу, чтобы регистрировать пользователей Notes. По умолчанию - локальный
Учетная запись	Введите ID администратора и затем введите пароль для него. Выбирайте - OK.

Имя профиля	Имя пользовательского профиля. По умолчанию - нет
Добавить пользователя в группу Notes	Назначения пользователей в группы По умолчанию – нет
Домен интернета	Правая часть адреса интернета для каждого пользователя. По умолчанию - текущий домен хоста (пример: acme.com)
Формат имени в адресе	Формат интернет адреса
Разделитель	Выбирайте одно их следующего: *1478 Нет *1479 Подчеркивание *1480 Точка *1481 Равенство Эти поля показываются, если выбраны почтовые системы – Notes, POP3 или IMAP.
Заверитель	ID Сертификатора По умолчанию, текущий ID сертификатора, указанный в NOTES.INI
Тип защиты	Выбирайте одно их следующего: *1482 Северной Америки *1483 Универсальная *** Начиная с версии 5.0.4 – Global ***
Срок действия сертификата	Дата истечения действия сертификата По умолчанию - два года начиная с текущей даты
Язык дополнительного имени	Альтернативное имя, при условии, что ID сертификатора содержит альтернативный язык

Изменение установок по умолчанию для почты и ID пользователей.

Опции почтовых настроек и настроек для ID не доступны, если Вы выбрали тип регистрации Только для интернет, в окне диалога Установок Регистрации.

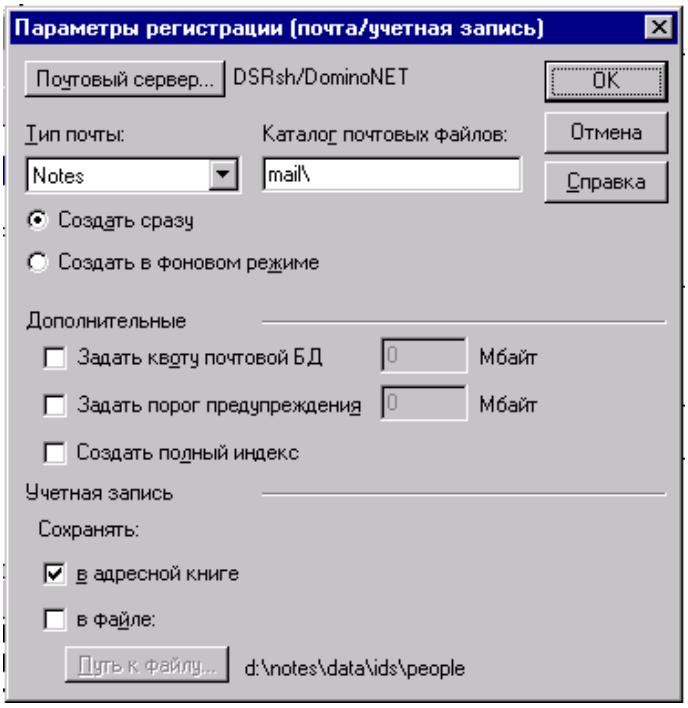


Рис. 71 Диалоговое окно параметров регистрации пользователей.

Перед изменением опций сделайте следующее:

*1484 Разрешите регистрацию пользователей и групп из WindowsNT User Manager.

*1485 Из User Manager, выберите – Notes – Параметры регистрации.

*1486 (Необязательно) Если необходимо создать почтовый файл на другом сервере, выбирайте кнопку – Почтовый сервер и выбирайте другой сервер, затем выбирайте - OK.

*1487 Измените, любые назначения и затем выбирайте - OK:

Поле	**Значение**

Тип почты	Выбирайте одно их следующего: *1488 Notes - Для использования почты Notes *1489 Other Internet Mail - Для использования почты интернета, если сервер Вашей организации используется как сервер интернет почты. Если используется эта опция, Domino не создает почтового файла для пользователя. *1490 POP – Для использования почтового клиента POP3, для доступа к почтовому файлу на Domino сервере. *1491 IMAP - Для использования почтового клиента IMAP, для доступа к почтовому файлу на Domino сервере. *1492 Other - Используется для перенаправления почты на другой адрес не Notes адрес. Почтовый файл не создается. *1493 None -Не используется почта По умолчанию – Notes
Каталог почтовых файлов	Каталог для почтовых файлов пользователей Notes. По умолчанию – почтовые файлы создаются в каталоге /mail каталога данных сервера Domino
Создать сразу	Создание почтового файла в процессе регистрации Notes пользователя По умолчанию – выбрано
Создать в фоновом режиме	Для создания почтовых файлов пользователя используется Administration Process. При этом создается запрос процесса администрирования в базе данных Administration Requests.
Задать квоту почтовой БД	Определение максимального значения размера для почтового файла пользователя. Введите планируемый размер в мегабайтах, для ограничения размера базы данных.
Задать порог предупреждения	Вы можете использовать это значение, для оповещения администратора, что почтовая база пользователя достигает указанного значения.
Создать полный индекс	Выбирайте эту опцию, если хотите создать полный индекс, при создании почтовой базы пользователя.

Сохранять ID в ...	Выбирайте одно их следующего: *1494 Почтовый файл пользователя, по умолчанию, сохраняется в Domino Directory. *1495 Вы можете сохранять файл в другом месте.
Путь к файлу ID	Вы можете сохранять пользовательские ID файлы в каталогах сервера. Если Вы выбираете опцию Сохранить ID в файле, укажите путь к месту хранения файлов. По умолчанию ID файлы сохраняются в каталоге: <Data directory>\ids\people

3.3.5 Использование WindowsNT для создания экаунта пользователя и регистрация Notes пользователя.

Вы можете создавать новый экаунт пользователя в WindowsNT и регистрировать нового пользователя в Notes одновременно. Вы можете также регистрировать существующих пользователей WindowsNT в Notes. Регистрация типично включает создание Person документа, Notes ID, почтового файла и пароля. Однако пользователи могут быть зарегистрированы и без почтового файла и Notes ID файла, чтобы получить доступ на Domino Web сервер без использования клиента Notes.

Вы можете регистрировать NT пользователей в Notes, используя установки по умолчанию или использовать опции регистрации, которые Вы можете определять. Если Вы используете установки по умолчанию, компьютер, на котором Вы это делаете должен иметь ОС - WindowsNT. Экаунт должен быть - экаунтом Domino сервера и этот сервер должен быть сервером регистрации.

Создание нового пользовательского экаунта WindowsNT и регистрация Notes пользователя.

*1496 Чтобы создавать новых пользователей в WindowsNT, из User Manager следуйте инструкциям или документации по созданию пользователей для WindowsNT.

*1497 После того, как Вы заканчиваете создание пользовательского экаунта, заполните эти поля и затем щелкать - OK:

Поля	**Значения**
Имя Отчество Фамилия	Принимайте имена по умолчанию, полученные из полей Full Name пользователя для WindowsNT

Подразделение	Название огр. Единицы пользователя, включаемого в его полное имя. Например, если Пользователь John Smith, а орг. единица - Eng. Имя пользователя было бы быть John Smith/Eng. Орг. единицы полезны для идентификации пользователей с одинаковыми именами. Например, John Smith/Eng/Acme и John Smith/Doc/Acme, где один служащий - член группы разработчиков, а другой - член группы разработки документации. Каждому назначено различное имя орг. единицы.
Использовать общий пароль	Назначает пользователю пароль для Notes и WindowsNT, а также для Notes интернет. Чтобы сохранить существующий пароль WindowsNT, введите Ваш обычный пароль. Если использование, общего пароля не выбрано, активизируется пароль Notes для имени пользователя.
Notes пароль для имени пользователя	Пароль для пользователя Notes
Подтверждение ввода пароля	Подтверждение пароля пользователя
Назначение интернет пароля для Notes	Введите адрес интернета, в Person документ, Domino Directory. Это поле применяется, только если пользователь зарегистрирован и использует почту Notes, активизируются следующие поля: *1498 Адрес интернета *1499 Пароль интернета для пользователя *1500 Подтвердите пароль интернета
Адрес интернета	интернет адрес пользователя. Для примера, KCarter@domain.com Поле показывается для POP3, IMAP, Notes типа почтовой системы.
Пароль интернета для ...	Введите интернет пароль
Подтверждение пароля интернета	Подтверждение пароля

*1501 Если Вы создаете больше чем один экаунт пользователя, щелкаете – Закрыть.

- Делайте одно из следующего:

Выбирайте – Начать Регистрацию, чтобы регистрировать новых пользователей. После того, как регистрация начала, щелкайте – Остановить Регистрацию в любое время, чтобы остановить регистрацию.

Выбирайте – Отменить, чтобы регистрировать новых пользователей позже. Информация о пользователях, которую Вы ввели, не сохраняется, если Вы выходите из User Manager.

*1502 Чтобы закончить процесс регистрации выбирайте - OK.

Примечание Вы может зарегистрировать экаунты в Notes в любое время, выбирая меню – Notes – Добавить выделенные группы/пользователей NT в Notes.

Domino ошибки не имеют никакого влияния на User Manager. Если Domino выдает ошибку и не регистрирует пользователя в Notes, пользователь все еще будет присутствовать в окне User Manager.

3.3.6 Регистрация существующих экаунтов пользователей WindowsNT в Notes.

*1503 В окне User Manager, выбирайте экаунт пользователя, который Вы хотите зарегистрировать в Notes.

*1504 Выбирайте из меню - Notes – Добавить выделенные группы/пользователей NT в Notes.

*1505 Если Вы регистрируете несколько пользователей, Вам будет предложено выбирать одно из следующего, затем щелкайте - OK:

- Запрашивать имя и пароль для каждого пользователя, чтобы вводить информацию для каждого пользователя вручную.
- Регистрировать пользователей без дополнительных запросов, использовать Full Names WindowsNT как имя пользователя Notes и генерировать, случайный пароль Notes в базе данных NTSYNC45.NSF. Если вы делаете этот выбор, Вы можете пропустить пункты для дополнительных опций регистрации для пользователей.

*1506 Если Вы регистрируете только одного пользователя, или если Вы выбрали вводить информацию пользователя вручную, заполните значения полей в окне регистрации пользователя.

*1507 Когда User Manager запрашивает Вас, хотите ли Вы регистрировать новых пользователей WindowsNT в Notes, делайте один из следующего:

- Выбирайте – Начать Регистрацию, чтобы регистрировать новых пользователей немедленно.
- Выбирайте - Отменить, чтобы регистрировать новых пользователей позже.

*1508 Если Вы выбрали опцию Регистрировать пользователей без дополнительных запросов, распространите пароли среди пользователей, так что бы они могли устанавливать их рабочие станции Notes. После установки, пользователи могут создавать новые пароли.

Обратите внимание. Автоматически произведенные пароли, применяются только для пользователей Notes ID, но не к WindowsNT.

3.3.7 Добавление WindowsNT групп в Notes.

Когда Вы добавляете NT группу в Notes, Вы можете также создавать документ Group в Notes и зарегистрировать членов группы. Если NT группа - группа локальная и содержит глобальные группы как членов группы, Вы можете добавлять эти глобальные группы в

Notes и зарегистрировать ее членов как пользователи Notes. Вы можете изменять членство группы перед добавлением их к Notes без того, чтобы воздействовать на NT группу.

Создание новой группы WindowsNT и регистрация ее в Notes.

*1509 Создать новую группу WindowsNT как указано в документации по WindowsNT.

*1510 Если вы будете запрошены, введите пароль для Вашего ID пользователя Notes.

*1511 Выбирайте - Создать группу со следующими параметрами и заполните эти поля, затем щелкайте - OK:

Поля	**Значения**
Имя группы Notes	Имя Группы
Тип группы	Тип Группы: *1512 Многоцелевая (по умолчанию) *1513 Только для почты *1514 Только для ACL *1515 Только для Отказов
Описание	Описание для группы
Зарегистрировать пользователей NT в Notes	Члены группы будут зарегистрированные как пользователи Notes. Person документы, Пользовательские ID и почтовые файлы будут созданы для пользователей. Запретите опцию, если Вы не хотите регистрировать членов группы как пользователи Notes.

*1516 Выбирайте на кнопке – Состав, если Вы хотите добавлять, или удалить членов групп из NT, затем заполните эти поля:

Поля	**Значения**
Входят	Удалите из этого списка, тех пользователи, кто больше не будет членом группы этой группы, или добавляют к этому списку имена новых пользователей.

Не входят	Добавьте к этому списку тех пользователей, кто не будут членом группы, или удалите из этого списка имена пользователей, если хотите включить их в список членов группы.

Обратите внимание, имеются ли глобальные группы в списке членов группы, если Вы хотите добавить эти группы в Domino Directory, выбирайте синхронизировать группы.

Добавление существующих WindowsNT групп в Notes.

*1517 В окне User Manager Groups, выберите группу, которую Вы хотите добавить в Notes.

*1518 Выбирайте из меню Notes – Добавить выделенные группы/пользователей NT в Notes.

Далее следует процедура регистрации группы описанная в предыдущем пункте.

3.3.8 Использование WindowsNT User Manager для удаления групп пользователей.

Когда пользователь Notes удаляется, все ссылки на его имя удаляются Administration Process, на Domino сервере.

Для удаления экаунта пользователя или группы.

Вы можете удалять пользователя или группу из User Manager и автоматически удалять соответствующего пользователя или документ группы в Domino Directory. Вы можете также автоматически удалять почтовые файлы пользователя.

*1519 Из User Manager, выберите – Notes – Параметры удаления/синхронизации пользователей Notes.

*1520 Заполните эти поля, затем выбирайте - OK.

Поле	**Значение**
Сервер	Имя сервера, содержащего Domino Directory из которого пользователь или группа будет удалена.
Параметры удаления пользователей	Выберите следующее: *1521 Не удалять почтовый файл *1522 Удалять только почтовый файл, указанный в Person документе *1523 Удалять только почтовый файл, указанный в Person документе и все его реплики
Выбирайте сервер для синхронизации пользователей	Имя локального сервера или удаленного Notes сервера.

*1524 Удалить пользователя или группу как указано в Вашей документации по WindowsNT.

*1525 Если вас спросят, удалять ли пользователя или группу из Domino Directory, выбирайте - OK.

3.4 Управление пользователями, серверами и группами.

Эта глава описывает как ресертифицировать ID сертификатора, переименовать его. Обратите внимание на управление пользователей. Как удалять пользователей, переименовывать их, удалять группы, или Domino сервера.

3.4.1 Управление пользователями.

Чтобы управлять пользователями, Вы можете делать любую из следующих задач:

*1526 Изменять имя пользователя Notes

*1527 Перемещать пользователей в различные иерархии имен организации

*1528 Изменять общее имя пользователя

*1529 Повторно сертифицировать ID пользователя

*1530 Удаление имени пользователя

*1531 Преобразование имени пользователя в иерархические

*1532 Перемещение почтового файла пользователя

3.4.1.1 Изменение имени Notes пользователя с использованием Administration Process.

Вы можете использовать процесс администрирования, чтобы изменить имя пользователя Notes или переместить имя пользователя Notes, в различные иерархические организации. Administration Process автоматизирует изменение имени повсюду в базах данных, в пределах домена Domino серверов. Процесс администрирования производит и выполняет ряд запросов, отправляемых по почте в базу данных Administration Requests (ADMIN4.NSF). Процесс администрирования может изменять имена пользователей только, если базе данных назначен сервер администрирования.

Процесс администрирования может автоматизировать изменение имен только пользователей Notes. Вы должны вручную изменить имена пользователя интернета для тех, кто имеет Person документ в Domino Directory, например для пользователей Web браузеров.

Сертификат, который Вы используете или любой предок сертификата, должен иметь Certifier документ в представлении Certificates из Domino Directory. Например, если Вы используете ID сертификатора /Sales/NYC/ACME, Domino Directory должен содержать Certifier документы для /ACME, /NYC/ACME и /Sales/NYC/ACME.

Публичный ключ в Person документе должен соответствовать ключу в ID пользователя. Если публичный ключ был изменен или разрушен, Вы увидите сообщение в базе данных Administration Requests – The name to act on was not found in the Address Book.

3.4.1.2 Как изменить общее имя пользователя?

Используйте эти шаги, чтобы изменить общее имя пользователя.

*1533 Чтобы переименовать пользователя Вы должны иметь:

- Доступ редактора с созданием документов или роль UserModifier, к Domino Directory
- По крайней мере, доступ автора с созданием документов к базе данных Certification Log

*1534 Из клиента Domino Administrator, выбирайте закладку Пользователи и группы".

*1535 Выбирайте имя пользователя.

*1536 Из панели инструментов, выбирайте - Сервис – Пользователи – Переименовать.

*1537 Нажимайте кнопку Изменить имя пользователя.

*1538 Выбирайте ID сертификатора, которым был сертифицирован ID пользователя, выбирайте - Открыть.

Например, чтобы переименовать Joe Smith/Sales/NYC/ACME, используйте ID сертификатора с именем - /Sales/NYC/ACME.

*1539 Введите пароль для ID сертификатора и выбирайте – ОК.

*1540 Согласитесь или измените дату истечения сертификата. По умолчанию, два года начиная с текущей даты.

*1541 Изменяйте имя пользователя, фамилию, по мере необходимости.

*1542 (Необязательно) В поле Новое подразделение введите значение. Тем самым Вы добавляете компоненту, которая появляется между именем пользователя и именем сертификата.

*1543 Нажмите кнопку Переименовать и затем – ОК.

3.4.1.3 Как переместить имя пользователя в иерархии имен?

Вы можете использовать процесс администрирования, чтобы переместить имя пользователя в различные иерархические схемы имен или перемещать имена в различные организации в целом.

Перемещение имени пользователя.

*1544 Из клиента Domino Administrator, выбирайте закладку Пользователи и группы.

*1545 Выбирайте имя пользователя.

*1546 Из панели инструментов, выбирайте - Сервис – Пользователи – Переименовать.

*1547 Нажимайте кнопку Запросить переход к другому заверителю.

*1548 Выбирайте ID сертификатора, которым был сертифицирован ID пользователя, выбирайте - Открыть.

*1549 Введите пароль для ID сертификатора и выбирайте – ОК.

*1550 Введите имя сертификата, чтобы использовать его иерархическое имя в поле Новый заверитель.

*1551 Нажмите кнопку Запросить, затем - ОК.

*1552 Выбирайте закладку Файлы, открывайте базу данных Administration Requests.

*1553 Выбирайте представление Name Move Requests, выбирайте пользователя, которого собираетесь переименовать.

*1554 Выбирайте из меню Действия – Complete Move for selected entries.

*1555 Выбирайте ID сертификатора, которым будет сертифицировано имя пользователя, и выбирайте – Открыть.

*1556 Введите пароль для ID сертификатора и выбирайте – ОК.

*1557 Принимайте дату истечения сертификата по умолчанию (два года начиная с текущей даты) или вводите другую дату.

*1558 (Необязательно) В поле Новое подразделение, введите имя, для уникальной идентификации пользователя. Этим Вы добавляет компоненту, который появляется между именем пользователя и именем сертификата.

*1559 Выбирайте кнопку – Заверить. Если Ваша локальная адресная книга не содержит взаимного сертификата для сертификата, Вы будете запрошены на предмет его создания.

*1560 Выбирайте кнопку – ОК.

3.4.1.4 Как преобразовать простые имена пользователей - в иерархические?

Используйте эти шаги, чтобы преобразовать простые имена пользователя в иерархический формат.

*1561 Чтобы преобразовать имя пользователей Вы должны иметь:

- Доступ редактора с созданием документов или роль UserModifier, к Domino Directory
- По крайней мере, доступ автора с созданием документов к базе данных Certification Log

*1562 Из клиента Domino Administrator, выдирайте закладку Пользователи и группы.

*1563 Выбирайте имя пользователя.

*1564 Из панели инструментов, выбирайте - Сервис – Пользователи – Переименовать.

*1565 Нажимайте кнопку - Обновить до иерархических.

*1566 Выбирайте ID сертификатора, которым будет сертифицировано имя пользователя, и выбирайте – Открыть.

*1567 Введите пароль для ID сертификатора и выбирайте – ОК.

*1568 Принимает дату истечения сертификата по умолчанию (два года начиная с текущей даты) или введите новую дату.

*1569 (Необязательно) В поле Новое подразделение введите имя, для уникальной идентификации пользователя. Этим Вы добавляет компоненту, который появляется между именем пользователя и именем сертификата.

*1570 Выбирайте – Обновить, затем – ОК.

3.4.1.5 Как удалить имя пользователей из Domino системы?

Вы можете удалять имя пользователя с помощью процесса администрирования. Вы можете начинать удаление пользователя, из клиента используя Domino Administrator, Web Administrator, или используя User Manager WindowsNT. Когда Вы удаляете пользователя, Вы можете добавить этого пользователя в группу Termination, чтобы запретить вызов сервера этим пользователем. Когда Вы создаете группу Termination, назначаете группе тип группы Deny Only.

Если сервер запущен на платформе WindowsNT, и пользователь имеет экаунт пользователя WindowsNT, Вы можете удалить и этот счет, также.

Удаление пользователя.

*1571 Чтобы удалить пользователя, Вы должны иметь:

- Право автора с удалением документов и роль UserModifier, или доступ редактора к Domino Directory
- Доступ автора с созданием документов к базе данных Certification Log.

*1572 Из клиента Domino Administrator, выдирайте закладку Пользователи и группы.

*1573 Выбирайте имя пользователя, которое Вы хотите удалить.

*1574 Из панели инструментов, выбирайте - Сервис – Пользователи – Delete.

*1575 Выбирайте – Да, чтобы удалить Person документы.

*1576 Заполните поля, по Вашему усмотрению:

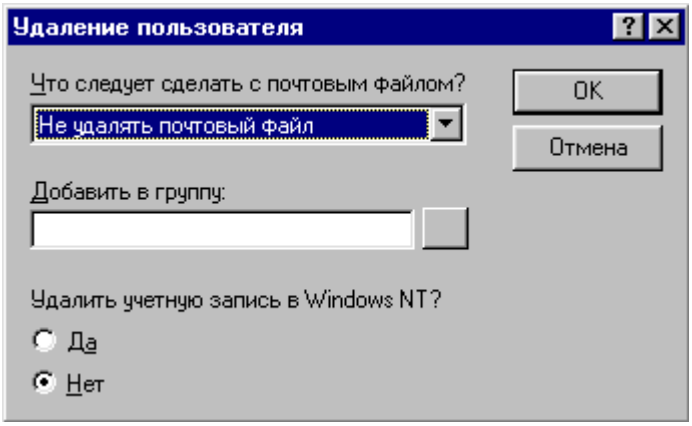


Рис. 72 Диалоговое окно удаления пользователей.

Поле	Значение

Что следует делать с почтовым файлом?	Выбирайте одно: *1577 Не удалять почтовый файл - удалять Person документ, но почтовый файл остается *1578 Удалить только почтовый файл – удалить только почтовый файл, указанный в Person документе *1579 Удалить почтовый файл и реплики - удалить почтовый файл, указанный в Person документе и все его реплики **Примечание.** Если Вы выбираете опцию, использовать процесс администрирования, для удаления почтового файла пользователя, просмотрите в представлении Pending Administrators Approval, запрос Approve File Deletion request, в базе данных Administration Requests. В режиме редактирования, выбирайте опцию – Approve File Deletion, чтобы запрос администрирования удалил почтовый файл пользователя. Если Вы выбираете не использовать запрос администрирования, для удаления почтового файла пользователя, Вам пройдется удалить файл вручную.
Добавить в группу	Вы можете добавить удаляемого пользователя в группу, например – Termination
Удалить учетную запись в WindowsNT	Выбирайте одно: *1580 Да *1581 Нет

Обратите внимание, если Вы выбираете удалять почтовый файл пользователя, Вы должны иметь, по крайней мере, доступ редактора с удалением документов к базе данных Administration Requests и право удалять документы из Domino Directory.

*1582 Выбирайте – ОК.

*1583 Делает одно из следующего:

- Выбирайте – Да, чтобы заставить процесс администрирования, немедленно удалить все ссылки на пользователя в этой реплике Domino Directory и отправить по почте запрос Delete in Access Control List.
- Выбирайте – Нет, чтобы отправить по почте запрос Delete in Address Book в базу данных Administration Requests, чтобы запустить процесс администрирования, удалять ссылки на пользователя в Domino Directory, ACL базах данных, согласно установке Interval, для Administration Process.

3.4.1.6 Ресертификация ID пользователя.

Следуйте этой процедурой, чтобы использовать оригинальный ID сертификатора для ресертификации ID пользователя, который имеет сертификат, срок действия которого истекает в ближайшее время.

Ресертификация ID пользователя.

Следуйте этими шагами, чтобы использовать процесс администрирования, для ресертификации иерархического ID файла, срок которого истекает в ближайшее время.

*1584 Для ресертификации пользовательского ID, Вы должны иметь:

- Доступ автора с созданием документов и роль UserModifier или доступ редактора в Domino Directory
- По крайней мере, доступ автора с созданием документов к базе данных Certification Log.

*1585 Из клиента Domino Administrator, выдирайте закладку Пользователи и группы.

*1586 Выбирайте имя пользователя, которое Вы хотите ресертифицировать.

*1587 Из панели инструментов, выбирайте - Сервис – Пользователи – Заверить заново.

*1588 Выбирайте ID сертификатора, использованного первоначально при сертификации Вашего ID файла и нажмите – Открыть.

*1589 Введите пароль для ID сертификатора и нажмите – ОК.

*1590 Принимайте дату истечения сертификата по умолчанию (два года начиная с текущей даты) или введите новую дату.

*1591 (Необязательно) Введите дату истечения сертификата ID пользователя.

*1592 Нажмите кнопку Заверить, затем – ОК.

3.4.1.7 Как перенести почтовый файла пользователя на другой сервер, или в другой каталог?

Вы может переместить некоторый почтовые файлы для высвобождения места на диске сервера или, когда пользователи изменяют свое место работы. Если Вы используете Shared Mail, и Вы хотите удалить почтовый файл пользователя из системы, Вы должны сначала удалить все связи с почтовым файлом из любых баз данных Shared Mail.

Когда почтовый файл перемещается, поля Почтовый файл и Главный/почтовый сервер будут изменены в документе Место вызова.

*1593 Из клиента Domino Administrator, выдирайте закладку Пользователи и группы.

*1594 Выбирайте имя пользователя, почтовый файл которого Вы хотите перенести.

*1595 Выбирайте кнопку из меню – Move Mail File.

*1596 Нажмите – Да, для подтверждения перемещения почтового файла.

*1597 Введите, имя нового почтового сервера для пользователя и нажмите – ОК.

*1598 Отредактируйте Person документ пользователя в Domino Directory, чтобы ввести новое имя почтового сервера. Вам потребует доступ редактора к Domino Directory. Если Вы перемещаете почтовый файл пользователя в другой домен, “вырежьте” Person документ из Domino Directory своего домена и “вставьте” этот документ в Domino Directory нового домена и затем исправьте имя почтового сервера пользователя и домена.

Перемещение почтового файла пользователя, из панели инструментов клиента Domino Administrator.

*1599 Из клиента Domino Administrator, выдирайте закладку Пользователи и группы.

*1600 Выбирайте имя пользователя, почтовый файл которого Вы хотите перенести.

*1601 Из панели инструментов, выбирайте - Сервис – Пользователи – Переместить.

*1602 Введите имя сервера и выбирайте сервер, на который Вы перемещаете пользователя.

*1603 Выбирайте – ОК.

*1604 Выбирайте каталог для нового почтового файла и затем нажимайте – ОК.

3.4.2 Управление серверами.

Чтобы управлять серверами, Вы должны уметь делать любую из следующих задач:

*1605 Изменять администратора сервера

*1606 Decommission server (сравнение серверов, например, для замены одного сервера другим)

*1607 Удалять имя сервера

*1608 Повторно сертифицировать ID сервера

*1609 Преобразовать имя сервера - в иерархическое

При управлении серверами, Вы можете нуждаться в ресертификации ID сертификатора.

3.4.2.1 Как изменить имя администратора сервера?

Если имя прежнего администратора явно внесено в список контроля управления доступа, для Domino Directory, удалите имя из ACL. Добавьте имя нового администратора и назначите доступ менеджера новому администратору.

Если имя прежнего администратора включено в любые группы, удалите имя прежнего администратора из Group документов. Добавьте имя нового администратора.

*1610 Из клиента Domino Administrator, выбирайте закладку Настройка.

*1611 Выбирайте документ сервера и откройте документ в режиме редактирования.

*1612 Выбирайте закладку Administration.

*1613 В поле Administrator, введите имя администратора, или выбирайте его из адресной книги.

*1614 Нажимайте клавишу ОК, затем сохраните и закройте Server документ.

*1615 Использовать серверную команду Replicate, с консоли сервера, чтобы распространить изменение быстро на другие сервера.

3.4.2.2 Сравнивание серверов (Decommissioning a server)

Вы можете использовать инструмент - Анализа для исключения сервера, когда Вы объединяете существующий сервер, с другим сервером, или удаляете сервер из Вашей системы серверов. Объединяете ли Вы сервера в один сервер, или переименовываете сервер, результат один и тот же - старое имя сервера заменяется на новое. Инструмент анализа может помочь Вам избежать потери сервисов, для Вашего Domino сервера. Инструмент анализа сравнивает исходный сервер с новым сервером назначения и сообщает различия между ними, которые могли причинить возможную потерю служб обслуживания.

Когда Вы запускаете инструмент анализа, из клиента Domino Administrator, Вы создаете базу данных результатов анализ (decomsrv.nsf), содержащую детальную информацию сравнения для двух сравниваемых серверов. Исходный сервер – сервер, который удаляется из обслуживания, и новый сервер - сервер который будет работать вместо исходного сервера, должны быть иерархическими серверами Notes, того же самого домена. Сервера не обязательно должен быть Domino R5 серверами. Только клиент Domino Administrator R5 необходим для использования инструментом анализа серверов.

Несоответствия между сервером источником и целевым сервером будут отмечены в базе данных результатов соответствующими документами. Ознакомьтесь с этими документами прежде, чем Вы исключите сервер из Вашей системы. Каждое сравнение, инструмент анализа делает индивидуально. Поэтому, Вы должны просмотреть каждое сообщение и сделать Ваши собственные выводы перед любыми действиями. Вы можете делать сравнения между двумя серверами в любой момент. Не все различия должны быть решены прежде, чем Вы замените сервера.

Прежде Вы исключите сервер, Вы должны выполнить следующие действия:

*1616 Проверьте каждую базу данных и формулы, которые содержат определенные ссылки на названия серверов

*1617 Проверьте документы из Domino Directory, особенно документы типа Подключения и Programs документы.

*1618 Если старый сервер имел взаимные сертификаты, удостоверитесь, что новый сервер имеет те же самые взаимные сертификаты

*1619 Уведомите другие домены, что доступ на сервер изменяется, в связи с изменением имени сервера

*1620 Сообщите пользователям о новом местоположении баз данных, если это необходимо

*1621 Проверьте протоколы сети на старом и новом сервере

*1622 Реплицируйте все базы данных со старого сервера на новый сервер

*1623 Переопределите таблицы маршрутизации почты, чтобы почта доставляется правильно

Запуск инструмента сравнения серверов.

*1624 Чтобы использовать инструмент сравнения, Вы должны иметь доступ администратора к старому и к новому серверу. Если Вы не имеете права администратора, некоторые части анализа могут быть незавершенны должным образом.

*1625 Из клиента Domino Administrator, выбирайте закладку Сервер – Анализ.

*1626 Из панели инструментов, выбирайте - Сервер – Исключение сервера.

*1627 Заполните следующие поля:

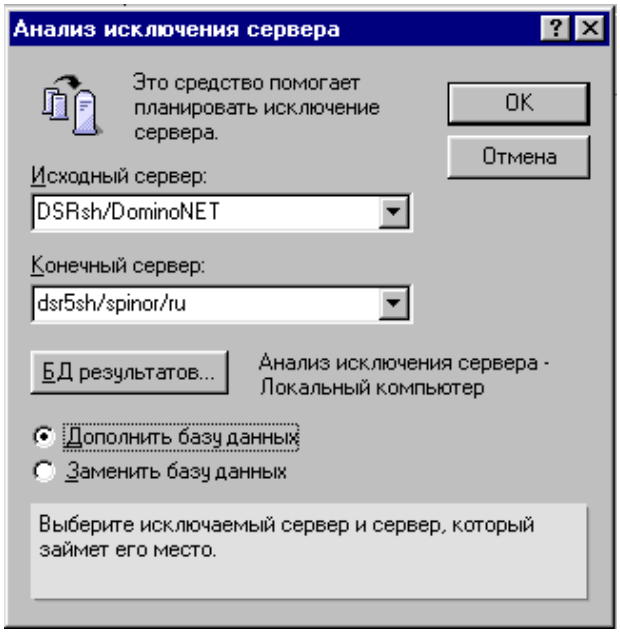


Рис. 73 Диалоговое окно анализа исключений сервера.

*1628 Если Вы не используете имя по умолчанию DECOMSRV.NSF - Заполните эти поля, нажимая кнопку ДБ результатов:

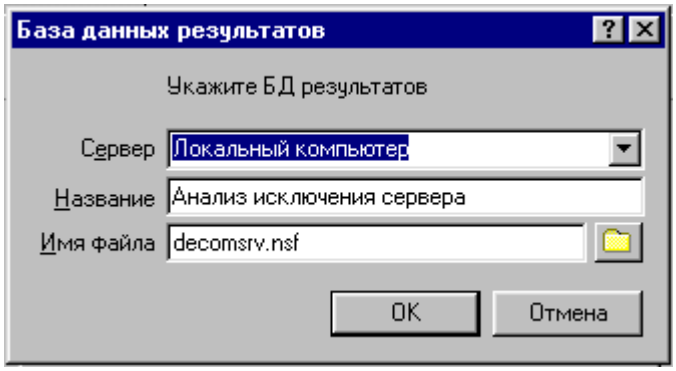


Рис. 74 Диалоговое окно определения места хранения результатов анализа серверов.

*1629 Нажимайте – ОК, затем опять – ОК.

Когда анализ завершается, база данных Результатов открывается. Это может продолжаться несколько минут в зависимости от загрузки сети и числа баз данных, на обоих серверах.

Примечание Вы можете создавать несколько сообщений в одной и той же базе данных или в различных базах данных и затем, использует эти сообщения, чтобы проверить, различия между двумя серверами. Вы можете заново запускать инструмент анализа.

Просмотр отчета в базе данных Анализ исключения сервера.

Инструмент сравнения серверов производит список пунктов, которые Вы можете в последствии анализировать. Каждая категория представляет различный аспект конфигурации серверов, который нуждается во внимании. Каждый пункт вносит в список

любые различия между серверами. В базе данных Результатов, Вы можете рассматривать список пунктов.

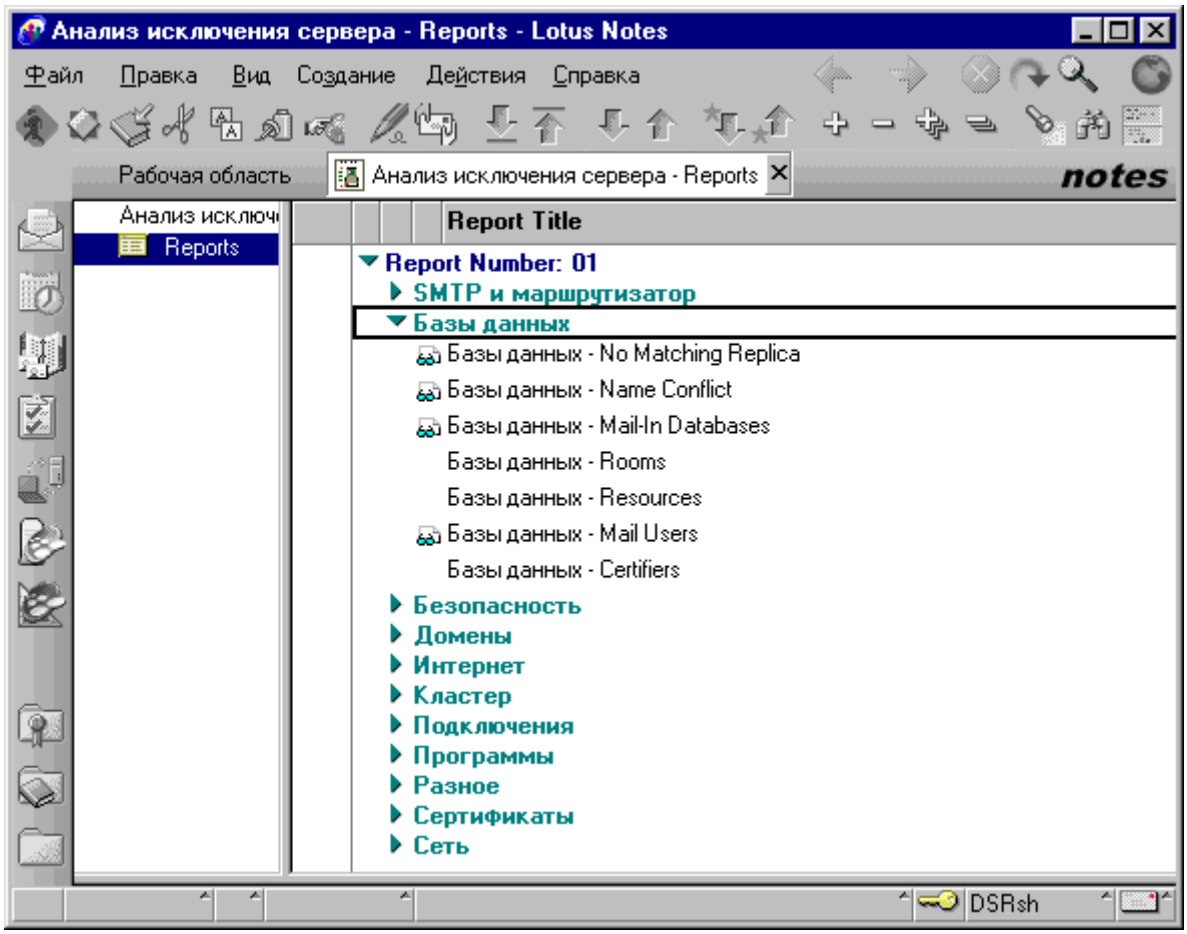


Рис. 75 Пример результата сравнения серверов.

Каждый пункт представлен в соответствии с документом. Статус документа обозначен изображением слева от документа следующим образом:

Иконка	**Описание**
	Различие было найдено при выполнении сравнений и может требовать внимания администратора
	Ошибка при выполнении или попытке исполнить сравнение
No icon	Никакое внимание не требуется, потому что сравниваемые поля эквиваленты, источнику

Выбирайте документ, чтобы открыть документ и рассматривать фактическое сообщение. Так выглядит типичный документ:

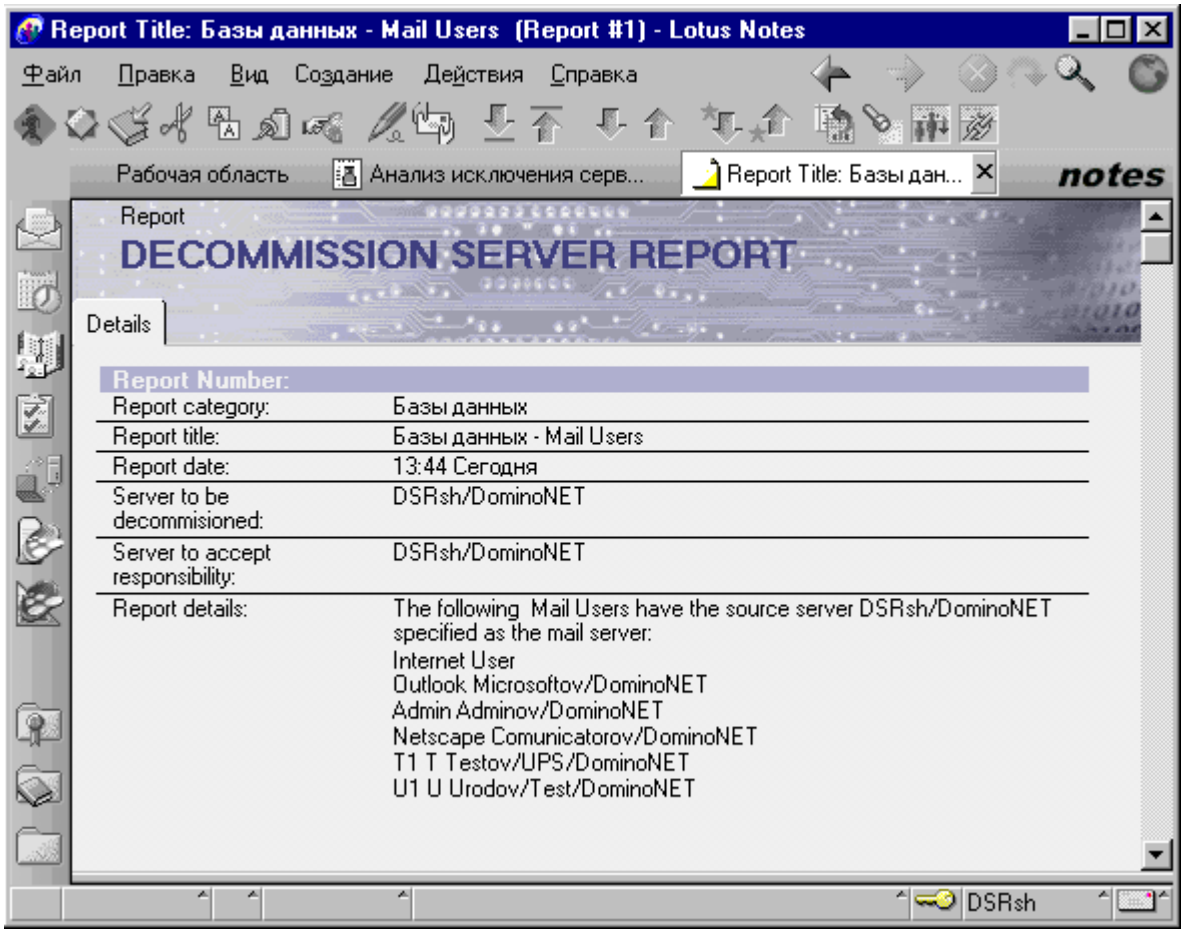


Рис. 76 Типичный документ отчета, сравнения серверов.

Поле	**Описание**
Report category	Секция или категория, которой документ принадлежит. Эти категории: Сертификаты, Кластер, Подключения, Базы данных, Домены, интернет, Инструменты, Сеть, Программы, Безопасность, SMTP и маршрутизаторы.
Report title	Определенное поле или пункт, который анализируется. Например, Базы данных – Mail Users или Базы данных -- No Matching Replica.
Report date	Дата генерации отчета
Server to be decommissioned (source server)	Имя сервера, который будет удален
Server to accept responsibility (target server)	Имя сервера, который будет выполнять обязанности нового сервера
Errors	Ошибки, которые происходят в течение анализа в этом пункте или поле. Эта поле не заполнено, если не имеется никаких ошибок.

Report details	Информация, которая указывает проблему или несогласованность, которая существует между двумя серверами

Сравнительный отчет.

Следующие типы сравнений полей, выполняемые между двумя Server документами и Configuration Settings документами:

Сравниваемые поля	**Описание**
Boolean	Содержание из двух сравниваемых полей должно быть идентично. В некоторых случаях, если поля на сервере источнике нет, никакое сравнение не выполняется для сервера назначения.
Numeric	Два поля сравняются
Text list	Два текстовых списка сравниваются и если поля не равны, производится сообщение
Name list	Два списка имен сравниваются, дубликаты будут удалены, сообщение будет произведено, если источник имеет не полный список.
Special cases	В некоторых случаях, незаполненные поля имеет специальное значение. В этих случаях, определенная интерпретация незаполненных полей будет учтена, когда сравнения будут выполнены.

Сравнения делаются следующим документам:

Сравниваемые документы	**Описание**
Connection document	Сравнение выполняется на любых Connection документах, где сервер источник, внесен в список в поле Source Server в Connection документах. Сравнение делается, чтобы гарантировать, что все сервера назначения в этих документах также были включены в отчеты связи сервера назначения. Сообщение производится, если задачи отличаются.
Program records	Все записи программ, которые внесены в список на сервере источнике, включены в сообщение. Никакое сравнение между источником и целевым сервером в отчеты не включаются, потому что не имеется никакого способа гарантировать, что выполняемые программы существуют на сервере назначения.

Domain records	Все отчеты о документах Foreign Domain проверяются, чтобы видеть имеется ли Gateway сервер для сервера источника. Если сервер найден, будет произведено сообщение, указывая, что в документе Foreign Domain есть сервер посредник.
Cross Certificates	Любой взаимный сертификат, который имеется на сервере источнике.

Эти сравнения делаются для баз данных:

Сравниваемые базы данных	**Описание**
Mail-in Databases, Rooms, Resources, Certifiers, Person documents	Каждый документ, который содержит сервер назначения, как почтовый сервер.
Replicas	Любая база данных на сервере источнике, которая не имеет соответствующей реплики на сервере назначения, будет отображена. Имя файлов для всех баз данных, которые не имеют реплики на сервере назначения, будут отражены в отчете. Любая база данных на сервере источнике, который имеет другое название базы данных, чем название реплики базы данных на сервере назначения будет внесена в список.

Эти сравнения делаются с документами сетевых протоколов сервера:

Сравнение документов сети	**Описание**
Enabled ports	Сравнение выполняется, для имен портов и протоколов. Сообщение производится для любых различий.
Notes Named Networks	Если источник и целевой сервер не имеют той же самой Notes поименованной сети, сообщение будут произведены.

3.4.2.3 Как удалить имя сервера из Domino системы?

Для удаления имени сервера из Вашей сети Domino серверов лучше использовать процесс администрирования, чтобы удалить все ссылки на сервер, из Domino Directory и из ACL баз данных.

Чтобы удалять имя сервера, Вы должны иметь:

- По крайней мере, доступ автора с правом удаления документов и роль ServerModifier, или доступ редактора к Domino Directory.

- По крайней мере, доступ автора с созданием документов к базе данных Certification Log.

*1630 Из клиента Domino Administrator, выбирайте закладку Настройка.

*1631 Выбирайте имя сервера, которое Вы будете удалять.

*1632 Нажмите кнопку Delete Server, затем – Да, чтобы подтвердить удаление записи сервера.

*1633 Сделайте одно из следующего:

- Выбирайте опцию – Да, чтобы заставить процесс администрирования, немедленно удалить все ссылки на сервер в этой реплике Domino Directory и отправить по почте запрос Delete in Access Control List.

- Выбирайте опцию – Нет, чтобы отправить по почте запрос Delete in Address Book, в базу данных Administration Requests. Этим Вы заставляете процесс администрирования, удалить все ссылки на сервер из Domino Directory и ACL баз данных, согласно значению Interval, для Administration Process.

*1634 Нажмите кнопку – ОК.

3.4.2.4 Ресертификация ID файла сервера.

Вы должны использовать оригинальный ID файл сертификатора, для ресертификации ID файла сервера, который имеет этот сертификат, но время действия, которого истекает в ближайшее время.

*1635 При ресертификации ID сервера, Вы должны иметь:

- Доступ автора с правом создания документов и роль ServerModifier, или доступом редактора к Domino Directory

- По крайне мере доступ автора с созданием документов к базе данных Certification Log.

*1636 Из клиента Domino Administrator, выбирайте закладку Настройка.

*1637 Выбирайте имя сервера, ID файл которого собираетесь ресертифицировать.

*1638 Выбирайте из меню Действия – Recertify Selected Servers.

*1639 Выбрать ID сертификатора, которым первоначально был сертифицирован сервер, и нажимайте – ОК.

*1640 Введите пароль для сертификатора и нажимайте кнопку Открыть.

*1641 Принимайте дату истечения сертификата по умолчанию (два года начиная с текущей даты), или введите другую дату.

*1642 Нажимайте – Заверить, затем – ОК.

Примечание. Вы может использовать функцию @Certificate, чтобы создать личное представление, которое будет содержать ID имена и даты истечения сертификатов. Если Вы создаете вид, убедитесь, что включили в меню акций кнопку Recertify Servers.

3.4.2.5 Преобразование простого имени (Flat Name) сервера - в иерархическое.

*1643 Из клиента Domino Administrator, выбирайте сервер, который Вы хотите преобразовать из представления - Сервер.

*1644 Выбирайте из меню Действия – Upgrade Server to Hierarchical.

*1645 Выбирайте новый ID файл сертификатора.

*1646 Введите пароль для ID файла сертификатора и затем – OK.

*1647 (Необязательно) Вводят имя орг. единицы.

*1648 Принимайте или изменить дату истечения сертификата для ID файла.

*1649 Выбирайте – Заверить, затем – OK.

3.4.3 Использование инструмента управления группами.

Вы можете использовать инструмент управления группами из панели инструментов, клиента Domino Administrator. Этот инструмент обеспечивает Вас быстрым и легким методом управления существующими группами в Domino Directory. Вы можете добавлять, удалять пользователей и группы, из групп, по мере необходимости. Вы можете также детально рассматривать описания для групп.

*1650 Из клиента Domino Administrator, выбирайте закладку Пользователи и группы.

*1651 Из панели инструментов, выбирайте - Сервис – Группы – Управление.

*1652 Вы можете выполнять любые операции просмотра с группами и членами групп:

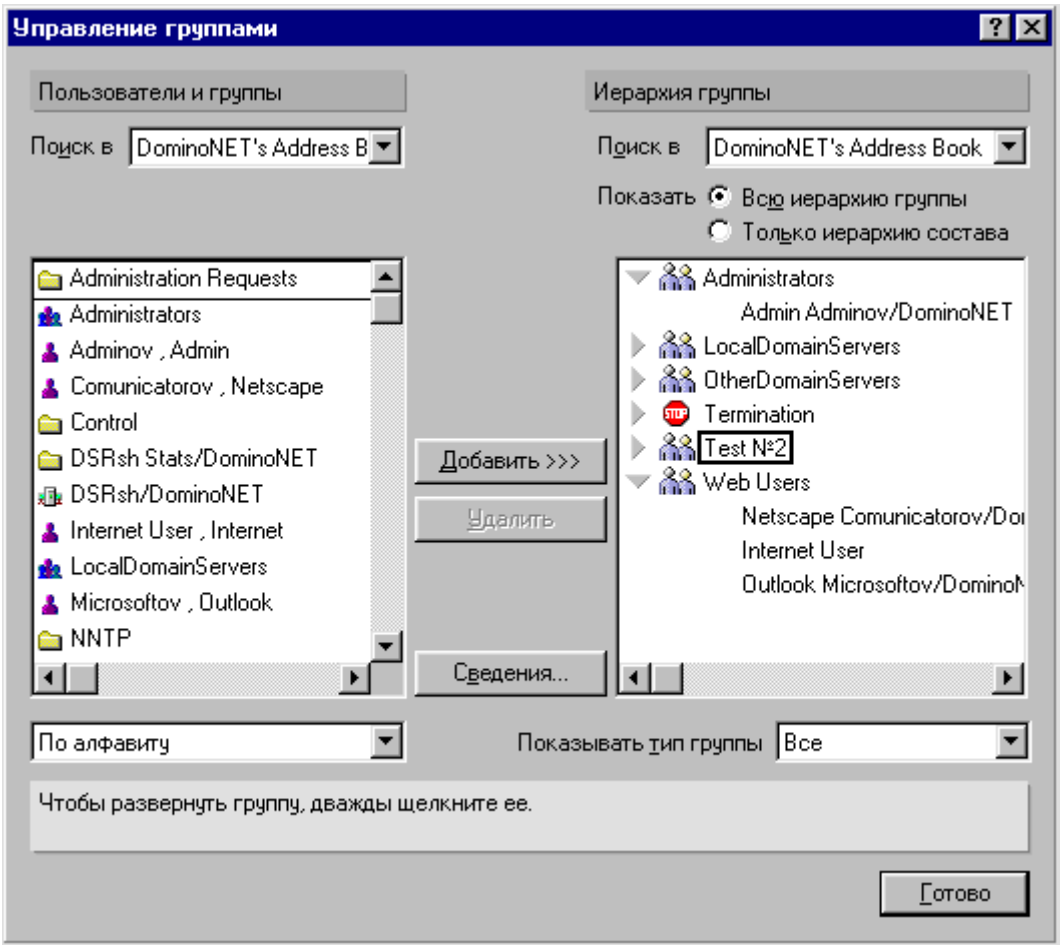


Рис. 77 Диалоговое окно инструмента управления группами.

*1653 Делайте любое из следующего:

- Чтобы добавить пользователей к группе, выбирайте группу в окне Иерархия группы, затем выберите пользователя или группу из окна Пользователи и группы и нажмите кнопку – Добавить >>>.
- Чтобы удалить пользователя из группы, выберите члена группы из окна Иерархия группы и нажмите кнопку Удалить.
- Чтобы просмотреть документ группы, выберите группу из окна Иерархия группы и нажмите кнопку Сведения….

*1654 Когда Вы закончили настройку групп, нажмите кнопку ОК.

4 Почтовая система Domino сервера.

Почтовый сервер Domino - основа почтовой инфраструктуры Вашей организации. Domino поддерживает стандарты интернет почты типа Simple Mail Transfer Protocol (SMTP), Post Office Protocol v.3 (POP3), Internet Message Access Protocol (IMAP) и Multipurpose Internet Mail Extensions (MIME). Domino маршрутизирует почту по SMTP и Notes почту и в формате Notes MIME. Domino сервер действует, как почтовый сервер интернет, используя SMTP, MIME, POP3, IMAP, но и как почтовый сервер Notes. Ваша организация может использовать Domino для рассылки почты интернет, в формате интернета, для маршрутизации почты Notes в формате Notes rich text формат, а также как помесь обоих форматов. Domino Router и клиент R5 оптимизирует формат сообщения, основываясь на предпочтении получателя, но если преобразование между форматами необходимо, Domino исполняет преобразование автоматически.

4.1 Обзор возможностей.

Domino предлагает мощные инструменты для контроля почты, для управления коммерческой электронной почтой (UCE), и может предотвратить злоупотребления ей.

Domino почтовая система имеет три основных компонента: почтовый сервер Domino, почтовые файлы Domino и почтовые клиенты. Каждый пользователь почты в Domino системе имеет файл почты, на почтовом сервере Domino. Вы можете создавать реплики почтовых файлов на других серверах для перенаправления запросов пользователей, в случае, если первичный сервер окажется недоступен. Пользователи создают почтовые сообщения, используют клиента, Lotus Notes и посылают почту через почтовый сервер Domino, который маршрутизируют сообщение получателю. Получатель использует клиента, чтобы читать сообщение.

Почтовый сервер Domino и маршрутизация почты.

Domino маршрутизирует почту по SMTP, по Notes и в формате Notes и MIME. Маршрутизация почты начинается, когда пользователь посылает сообщение с клиента, который связан с Domino сервером. Сообщение передается от клиента до базы данных MAIL.BOX на почтовом сервере пользователя. Серверная задача Router, доставляет почту, проверяет адрес сообщения, чтобы определить, по какому маршруту доставить сообщение получателю и что использовать Notes или SMTP протокол, для доставки сообщения.

Если пользователь посылает почту в формате Notes, адресует ее в интернет, используя для этого клиента Notes R4, Router автоматически конвертирует сообщение в формат MIME.

Рассылка почты за пределы Вашей организации.

Почтовый сервер Domino может маршрутизировать почту, которая адресована получателям вне Вашей организации непосредственно в интернет, или на промежуточный хост сервер, или Firewall. Если почтовый сервер Domino не использует SMTP для маршрутизации, почты во внешние домены, Domino использует SMTP или Notes для маршрутизации сообщений на почтовый сервер, который может доставлять почту в интернет. Вы можете настроить все сервера, или только некоторые, или только один сервер в Вашей организации для маршрутизации почты по SMTP. Так как почта интернет может маршрутизироваться с использованием Notes, каждый пользователь может посылать и получать интернет почту, даже если Вы устанавливаете только

один сервер для маршрутизации почты по SMTP. Эта гибкость гарантирует, что Domino может маршрутизировать почту безопасным способом. Вы можете настроить Вашу почтовую систему так, чтобы только один сервер обращался с интернет. На этом сервере Вы можете установить антивирусное программное обеспечение и ограничивать получение почты от некоторых доменов. Или, Вы можете сбалансировать нагрузку почты и настроить каждый сервер на маршрутизирование интернет почты по SMTP.

Даже если Вы настраиваете только несколько серверов, для маршрутизации интернет почты получателям вне Вашей организации, все сервера могут все еще маршрутизировать сообщения MIME и SMTP получателям в пределах Вашей организации. Вы можете использовать интернет почту для внутренних получателей на всех серверах, но посылать и получать почту, от внешних получателей на несколько серверов.

Почтовый сервер Domino.

Вся почта в Domino системе сохраняется в почтовых файлах, независимо от ее формата Notes или MIME. Пользователь может обращаться к почтовым файлам любым клиентом - Notes, POP3 Web браузером, или IMAP. почтовые файлы Domino хранят сообщения в формате Notes или в формате MIME. Если интернет клиент или IMAP клиент, открывает или разгружает сообщение, сохраненное в формате Notes, Domino автоматически конвертирует сообщение в MIME формат.

Безопасность почты.

Чтобы гарантировать безопасность при передаче сообщений между серверами, почтовый сервер Domino поддерживает SSL для передачи почты по SMTP и поддерживает шифрование Notes, когда почта использует Notes маршрутизацию.

Чтобы шифровать и подписывать сообщения, клиенты Notes могут использовать сертификаты Notes и шифрование, или X.509 сертификаты. Другие почтовые клиенты могут использовать X.509 сертификаты. Клиенты Notes могут использовать интернет почту с X.509 сертификатами.

Работа с другими почтовыми системами.

Domino работает с другими почтовыми серверами и системами, используя и агентов передачи сообщений (MTA) X.400 и cc:Mail систем. Domino может обмениваться почтой с другими SMTP серверами и маршрутизировать почту X.400 и cc:Mail систем, через X.400 MTA и cc:Mail MTA.

4.1.1 Передача сообщений и протоколы доступа к почте.

Domino поддерживает протоколы передачи сообщений для интернет, а также предлагает мощную почтовую систему Notes. Domino маршрутизирует почту с использованием SMTP и Notes. Пользователи могут посылать почту в формате Notes или в формате MIME. Таким образом, Вы можете использовать SMTP или Notes для маршрутизации сообщений MIME, с клиента Notes или использовать SMTP для маршрутизирования сообщений MIME от IMAP клиентов, POP3 клиентам.

Потому что Domino автоматически конвертирует сообщения между Notes форматом и MIME, если это необходимо, клиенты могут посылать и получать почту, не беспокоясь о формате. Если клиент Notes посылает сообщение в формате Notes, IMAP клиенту, Domino конвертирует сообщение в MIME для IMAP клиента. Если

POP3 клиент посылает сообщение MIME клиенту Notes R4, который не может читать сообщения в формате MIME, Domino конвертирует сообщение MIME в формат Notes.

Комбинация маршрутизаций SMTP и Notes и, автоматического преобразования сообщений из одного формата в другой, предлагает Вам широкий выбор и гибкость в Вашей почтовой инфраструктуре. Например, Вы можете настроить почтовую систему, которая будет полностью удовлетворять стандартам интернет и использовать Router для маршрутизации сообщений MIME по SMTP. Вы можете настроить почтовую систему, которая полностью будет базироваться на почте Notes и использовать Router для маршрутизации сообщений формата Notes. Вы можете так же настроить почтовую систему, которая будет использовать и SMTP, и Notes.

Domino поддерживают интернет протоколы доступа к почте IMAP и POP3, а также предлагают доступ клиентам Notes. IMAP, POP3 и клиенты Notes соединяются с использованием почтового сервера Domino, чтобы читать почту и посылать ответы. Если IMAP или POP3 клиент нуждается в доступе к сообщениям в формате Notes, Domino конвертирует сообщение для этих клиентов.

4.1.2 Как передаются сообщения в системе Domino?

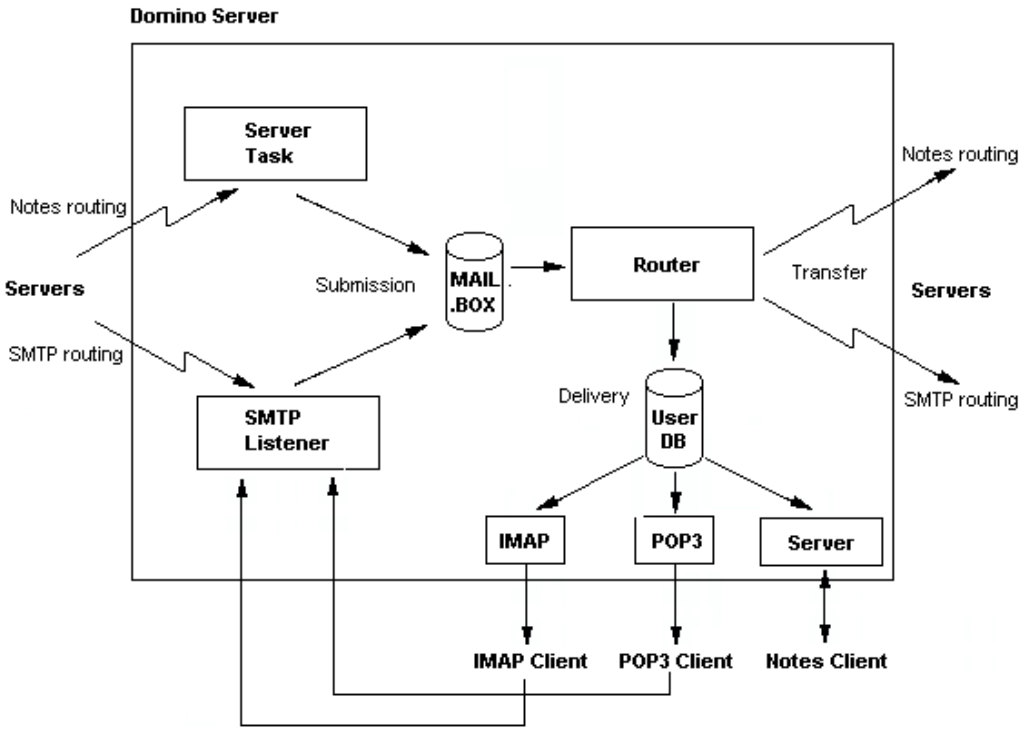


Рис. 78 Схема маршрутизации сообщений в почтовой системе Domino.

Эта секция описывает процесс маршрутизации почты в почтовой системе Domino.

*1655 Пользователь создает и адресует сообщение получателю.

*1656 Пользователь посылает сообщение.

*1657 Программное обеспечение клиента пользователя может:

- Использовать протоколы Notes, чтобы переместить сообщение в почтовую базу MAIL.BOX Domino сервера.

- Использовать SMTP, чтобы послать почтовое сообщение пользователя на Domino сервер, на котором запущена задача SMTP Listener. Задача SMTP Listener заносит сообщение в MAIL.BOX (Lotus Notes, IMAP клиенты, POP3 клиенты).

- Использовать HTTP, чтобы послать почтовые сообщения пользователя на Domino сервер, на котором должна быть запущена HTTP задача. HTTP задача заносит сообщение в MAIL.BOX (Web клиенты).

*1658 Router находит сообщение в MAIL.BOX и решает, куда послать сообщение для каждого получателя. Router вычисляет следующий Hop (перелет), для сообщения на пути к получателю и использует или SMTP, или Notes - чтобы передать сообщение.

- При использовании SMTP, Router соединяется с сервером назначения, почтовым сервером получателя, Relay Host, Smart Host, или с одним из серверов в интернете домена получателя - и передает копию сообщения.

- При использовании Notes, Router перемещает сообщение в MAIL.BOX базу данных на сервере, который является следующим в цепочке, до почтового сервера получателя.

*1659 Router на сервере получателя находит сообщение в базе данных MAIL.BOX на Domino сервере и доставляет его в почтовый файл получателя.

*1660 Получатель использует клиента, который поддерживает протоколы Notes, POP3, IMAP, или Web доступ (HTTP), чтобы читать сообщение, которое сохранено в его почтовом файле.

4.1.3 Domino Directory и маршрутизация почты.

Domino Directory содержит всю информацию, необходимую для маршрутизации почты в Вашей инфраструктуре исключая DNS, который поддерживается отдельно. Domino Directory поддерживает LDAP сервис так, чтобы интернет почтовые клиенты могут использовать LDAP, чтобы отыскивать информацию в Domino Directory, если они имеют доступ к нему.

Таблица маршрутизации.

Когда Вы запускаете Router на сервере, сервер собирает информацию из документов подключений, документов доменов и Server документов, из Domino Directory. Когда пользователь посылает почту, получателю в локальном домене, Router просматривает Domino Directory (или вторичный Directory) и ищет Person документ получателя, который содержит запись о домашнем сервере получателя. Router проверяет таблицу маршрутизации, чтобы определить оптимальный путь к этому серверу и маршрутизирует сообщение согласно этому пути. Если Вы перегружаете сервер, Router повторно вычисляете таблицу маршрутизации.

Имя хоста в системе Domino.

Lotus рекомендует в Domino системе, использовать полные имена хостов, вместо IP адресов. В то время как IP адреса работают и полностью поддерживаются, т.к. IP изменяются более часто, чем имена хостов. Domino не может работать должным образом, если адреса должным образом не обновляются. Например, изменение или реорганизация

может потребовать изменения в адресации серверов. В этом случае, если Server документ использует имена хостов, обновления документов не нужны, однако обновление необходимо, если документы содержат IP адреса.

4.1.4 Domain Name Service (DNS) и маршрутизация почты.

Domain Name Service (DNS) - используется задачей SMTP, чтобы конвертировать имена, типа acme.com, в IP адрес сервера. Сервер получает IP сервера назначения от DNS и посылает должным образом сообщение получателю. Вы должны правильно сконфигурировать DNS, чтобы поддерживать использование SMTP. Чтобы определять адрес IP почтового сервера назначения, Domino делает следующее:

*1661 Просматривает серверную часть домена и адреса каждого получателя в DNS.

*1662 Если DNS находит запись MX, сервер пробует соединять с сервером, из списка записей MX. Если имеются больше чем одна запись MX, сервер пробует соединяться с записью, которая имеет самую низкую стоимость. Если больше чем одна запись MX имеют низкую стоимость, сервер беспорядочно выбирает одну и пробует соединиться с этим сервером.

Обратите внимание, что могут иметься больше чем одна запись MX определяемая для имени домена. Каждая запись содержит адрес IP для хоста сервера.

*1663 Если DNS находит запись, Domino маршрутизирует сообщение по IP адресу.

*1664 Если DNS не находит запись, Domino не может доставить сообщение и посылает сообщение недоставке отправителю.

Вы можете также использовать DNS, чтобы сопоставить IP адрес имени хоста, или имя хоста - IP адресу, чтобы проверить, кто фактически посылает сообщение. Используйте эту проверку, чтобы ограничить доступ Releу через Ваш сервер или запрещать незапрашиваемую коммерческую электронную почту (UCE).

MX записи сопоставляют имени домена одну или большее количество имен хостов. Удобнее использовать имена хостов в записях MX по некоторым соображениям:

*1665 Некоторые инструменты Third-Party признают только имена хостов, а не IP адреса.

*1666 Если Вы должны заменять или переместить компьютер, Вы можете назначать существующее имя хоста и IP адрес новому компьютеру. Эта замена прозрачна для пользователей и сообщения продолжают маршрутизироваться должным образом.

Когда Вы устанавливаете больше чем одну запись MX имен, Вы можете устанавливать приоритет, который управляют, как DNS выбирает записи. DNS выбирает записи с более низким значением сначала. Например, DNS выбирают 5, а потом 10. Если Вы, имеете больше чем одну запись MX. Если имеются записи с той же самую стоимостью, DNS беспорядочно, выбираете из этих записей MX. Если одна из этих записей MX терпит неудачу - например, потому что сервер недоступен - DNS переходит к следующей записи MX, которая имеет ту же самую стоимость.

Например, acme.com домен имеет четыре MX записи:

```
MX record: acme.com IN MX 5 mail1.acme.com

MX record: acme.com IN MX 5 mail2.acme.com

MX record: acme.com IN MX 10 mail3.acme.com
```

```
MX record: acme.com IN MX 10 mail4.acme.com
```

Когда сервер пробует соединяться с acme.com, DNS сначала использует запись MX с предпочтением 5. Так как имеется две записи MX с предпочтением 5, DNS беспорядочно выбирает между записью MX mail1.acme.com и mail2.acme.com. Если DNS возвращает запись MX mail1.acme.com, но mail1.acme.com недоступен, DNS возвращается к записи MX mail2.acme.com. Если mail2.acme.com недоступен, обе записи MX со стоимостью 5 потерпят неудачу. DNS тогда выбирает запись MX, которые имеют стоимость 10.

4.1.4.1 Примеры использования нескольких записей MX records.

Использование одного интернет домена с одним именем сервера.

Вы можете определить в записях MX единственный интернет домен - например, acme.com. Используйте полное хост имя сервера в MX записях - например, mail1.acme.com.

Например, сконфигурируйте резервный SMTP сервер mail2.acme.com для получения или отправки почты, когда первичный SMTP сервер mail1.acme.com недоступен:

```
MX record: acme.com IN MX 5 mail1.acme.com

A record: mail1.acme.com IN A 192.168.10.17

MX record: acme.com IN MX 10 mail2.acme.com

A record: mail2.acme.com IN A 192.168.10.18
```

Сообщения, адресованные acme.com сначала маршрутизируются на mail1.acme.com, потому что стоимость (5), более низкая. Если mail1.acme.com недоступен, mail2.acme.com получает почту.

Использование одного интернет домена с двумя серверами.

Если Вы даете двум серверам равную стоимость, DNS беспорядочно выбирает сервер, чтобы сбалансировать нагрузку прихода почты.

```
MX record: acme.com IN MX 5 mail1.acme.com

A record: mail1.acme.com IN A 192.168.10.17

MX record: acme.com IN MX 5 mail2.acme.com

A record: mail2.acme.com IN A 192.168.10.18
```

Использование нескольких имен доменов в Вашей системе.

Вы можете создавать записи MX для нескольких интернет доменов - например, acme.com acme.com, qrs.com и xyz.com.

Примечание. Пользователи могут адресовать почту любому из доменов. Каждый домен имеет резервный SMTP сервер.

```
MX record: acme.com IN MX 5 mail1.acme.com

MX record: acme.com IN MX 10 mail2.acme.com

MX record: qrs.com IN MX 5 mail1.acme.com

MX record: qrs.com IN MX 10 mail2.acme.com

MX record: qrs.com IN MX 5 mail1.acme.com
```

```
MX record: xyz.com IN MX 10 mail2.acme.com
```

4.2 Почтовая адресация в версии R5.

Domino просматривает почтовый адрес интернет в Domino Directory R5, Domino проверяет скрытый вид $Users для создания или проверки адреса. Если он находит полный интернет адрес получателя (например, jdoe@acme.com) или Короткое имя пользователя, Domino доставляет сообщение этому пользователю. Domino также сопоставляет знак подчеркивания (_) в любой части адреса – пробелу (например, jane_doe), из любого из полей Person документа. Например, если сообщение адресовано jone_doe@acme.com, и Domino находит, что Person документ Jone Doe, в поле Имени Пользователя, Domino доставляет сообщение в почтовый файл - Jone Doe.

Примечание. Domino конвертирует, знак подчеркивания в пробел. В этом примере, jone_doe становится Jone Doe. Domino конвертирует двойное подчеркивание в подчеркивание, подчеркивание в пробелы. Поиск нечувствителен к регистру, поиск jone doe все равно, что Jone Doe, в Person документах.

Исчерпывающий поиск Domino в виде $Users гарантирует, что любой адрес R4 MTA, для пользователя в Вашем Directory будет найден и идентифицирован должным образом. Вы можете использовать интернет адрес пользователя в R5, из Person документа и стандартный Notes адрес, чтобы стандартизировать адрес интернета в Вашей организации, но этот шаг необязательный. Domino, не видит различия между R4 и адресацией R5 и использует оба адреса одинаково хорошо.

4.2.1 Поля Address Internet в Person документах.

Когда Вы модернизируете систему до R5, Вы можете использовать интернет адрес в адресации сообщений. Используйте следующую последовательность, чтобы заполнить поля Address Internet для всех Person документов, в которых это поле еще пусто.

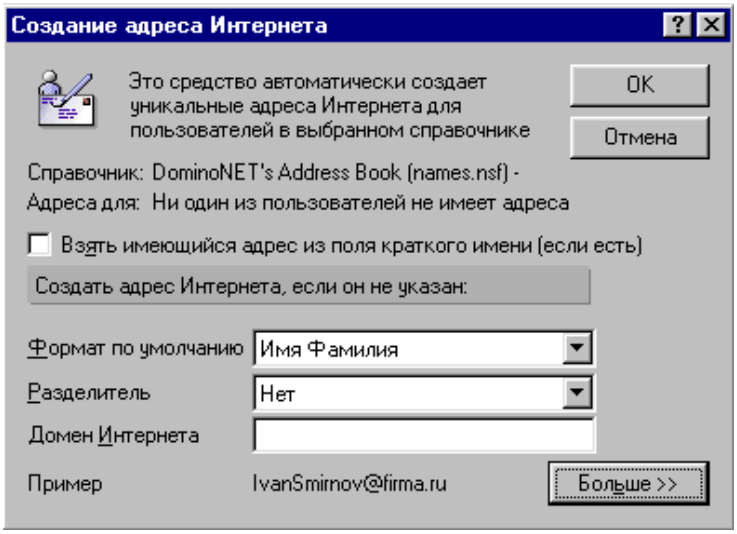
*1667 Запустите клиента Domino Administrator.

*1668 Выбирайте закладку Пользователи и группы.

*1669 Выбирайте нужный сервер и Domino Directory, для которого Вы желаете заполнить поля Address Internet.

*1670 Выбирайте закладку Сервис – Пользователи.

*1671 Выбирайте – Адрес интернета.



*1672

Рис. 79 Диалоговое окно создания интернет адреса пользователя (заполнение поля Internet Address).

*1673 В окне Создание адреса интернета, выберите формат адреса интернета.

*1674 Выбирайте разделитель для Адрес интернета. Этот знак, отделяющий слова, знаки в интернет адресе, в поле Разделитель.

*1675 Введите Домен интернета для Вашей компании.

Обратите внимание. Если Вы выбираете опцию в поле - Взять имя Домена интернета из поля краткого имени (если есть)**,** функция ищет поле Short Name в каждом Person документе. Если поле содержит интернет адрес, например jdoe@acme.com, Domino использует этот адрес, чтобы закончить заполнение поля Address Internet, вместо создания нового, базируясь на информации диалогового окна.

*1676 (Необязательно...) Щелкайте на кнопке Больше >>:

*1677 Выбирайте - Помещать разделители между словами в именах, чтобы вставить разделитель, который Вы определяете, между словами в составном имени.

*1678 Выбирайте - Создать адреса только для выбранного домена Notes, чтобы установить Адрес интернета только для пользователей в данном домене Notes. Введите имя Домена Notes, в котором Вы хотите установить Адрес интернета.

*1679 Выбирайте - При конфликте использовать дополнительный шаблон формата, чтобы определить второй признак Адреса интернета, если Notes находит одинаковый адрес для двух пользователей. Определите альтернативный образец формата. Это позволяет Вам так же использовать альтернативный формат адреса, если первичный не может быть использован. Причина может быть разной. Например, в адресе используются не ASCII символы или адрес уже используется, или содержит недопустимые в интернете символы.

Окно Создание адреса интернета определяется сервер и Domino Directory. Она также отображает пример для каждого адреса и формат разделителя.

Обратите внимание, что диалог не дает примеров, для всех комбинаций выборочного формата.

Инструмент Адрес интернета, проверяет все Person документы Domino Directory. Когда он находит документ с пустым полем Address Internet, он заполняет его согласно правил,

изложенных выше. Проверяет его, чтобы запись имела формат RFC 821, проверяет также запись на предмет уникальности, выполняя поиск имени на всех Domino Directory на сервере. Если запись существует в поле Address Internet, инструмент оставляет поле, неизмененное и выводит ошибку в файл LOG.NSF.

Обратите внимание, что все ошибки выводится в файл LOG.NSF.

Предостережение, Инструмент анализа Адрес интернета выполняет исчерпывающий поиск имени для каждого нового адреса интернета и не должен запускаться на каталогах сервера, который сильно загружен.

4.2.1.1 Как форматируется Адрес интернета?

Вы можете выбирать один из следующих формата адреса:

*1680 **Имя Фамилия.** Используется поля Имени и поля Фамилии, чтобы формировать адрес.

*1681 **Имя первая буква отчества. Фамилия.** Использует содержание поля Имени, поле Инициалов и поле Фамилии, чтобы формировать адрес.

*1682 **Первая буква Имени. Фамилия.** Использует первую букву поля Имени пользователя и поле Фамилии, чтобы формировать адрес.

*1683 **Первая буква Имени. Первая буква Отчества Фамилия.** Использует первую букву поля Имени пользователя, Середина – первая буква Отчества и поле Фамилии, чтобы формировать адрес.

*1684 **Фамилия Имя.** Использует поле Фамилии и поле Имени, чтобы формировать адрес.

*1685 **Фамилия Имя первая буква отчества.** Использует содержание поля Фамилии, поле Имени и поле Инициалов, чтобы формировать адрес.

*1686 **Фамилия первая буква имени.** Использует содержание поля Фамилии и первую букву поля Имени пользователя, чтобы формировать адрес.

*1687 **Фамилия первая буква имени первая буква отчества.** Использует поле Фамилии, первое букву поля Имени пользователя, и поле Инициалов, чтобы формировать адрес.

*1688 **Фамилия первая буква имени.** Использует поле Имени и первую букву поля Фамилии, чтобы формировать адрес.

*1689 **Настаиваемый шаблон.** Используется свободный формат, позволяет Вам определить свой формат Internet address.

Вы можете выбирать один из разделителей для формирования адресов:

*1690 Нет

*1691 Подчеркивание _

*1692 Знак равенства =

*1693 Знак процента %

Примечание Вы должны определить интернет домен в поле Домен интернета, из диалогового окна.

4.2.2 Выбор формата интернет адреса для Вашей организации

Имя пользователя	**Поле Имя**	**Поле Фамилия**	**Поле инициал Отчества**	**интернет домен**
Jane R. Jones	Jane	Jones	R	acme.com

Теперь Вы можете использовать специальный встроенный инструмент R5, для формирования уникального формата интернет адреса для Вашей организации. Пример:

Используемые поля	**Разделитель**	**Формат интернет адреса**
Имя_Фамилия	_	Jane_Jones@acme.com
Имя_первая буква отчества_Фамилия	_	Jane_R_Jones@acme.com
Первая буква Имя_Фамилия	%	J%Jones@acme.com
Первая буква имя_первая буква отчества_Фамилия	%	J%R%Jones@acme.com
Фамилия_Имя	=	Jones=Jane@acme.com
Фамилия_Имя_первая буква отчества	=	Jones=Jane=R@acme.com
Фамилия_первая буква имя	_	Jones_J@acme.com
Фамилия_первая буква имя_первая буква отчества	_	Jones_J_R@acme.com
Имя_первая буква Фамилии	%	Jane%J@acme.com

Примечание. Вы должны определить интернет домен в поле Домен интернета.

4.2.3 Формирование нестандартного интернет адреса.

Если Вас все-таки не устаивает ни один из предложенного выше адреса, выбираете - Настаиваемый шаблон в диалоговом окне инструмента формирования адреса интернета. Вы можете определить, как Domino будет формировать интернет адрес в Person документ, поля Address интернет. Используйте следующие знаки, чтобы определить, как адрес должен выглядеть:

Абривиатура	**Значение**
Fn	Имя name, *n* - число знаков имени
Ln	Фамилия, *n* – число знаков имени

M	Первая буква Отчества
T	Титул
G	Generational qualifier
I	Employee ID
C	Местоположения
D	Департамент
V	Сервер
O	Орг. Единица
S	Использование значения поля Short name
=	Разделитель
_	Разделитель
%	Разделитель

Объединяя и комбинируя знаки и разделители, указанные выше, Вы можете определить формат интернет адреса для Вашей организации.

Пример. Интернет адрес для пользователя Jane R. Jones:

Титул	**Имя**	**Первая буква Отчества**	**Фамилия**	**Местоположение**	**Организация**	**Сервер**
Ms	Jane	R	Jones	Tampa	Acme	MailT1

Пример написания адреса	**Адрес**
FL	JaneJones@acme.com
F2L	JaJones@acme.com
F_L=C	Jane_Jones=Tampa@acme.com
T_F_M_L%V	Ms_Jane_R_Jones%MailT1@acme.com

4.2.4 Проверка интернет адреса на уникальность.

Вы можете использовать этот инструмент, чтобы проверить, поля Address Internet всех Person документов в одном или в нескольких Domino Directory на уникальность. Инструмент гарантирует, что каждый адрес интернета не имеет аналогов в Вашей системе. Чтобы воспользоваться этим, сделайте следующее:

*1694 Запустите клиента Domino Administrator.

*1695 Выбирайте закладке Пользователи и группы.

*1696 Выбирайте сервер и Domino Directory, для которого Вы желаете проверить записи в полях Address Internet.

*1697 Щелкаете на закладке Пользователи, справа.

*1698 Выбирайте опцию – Проверить адрес...

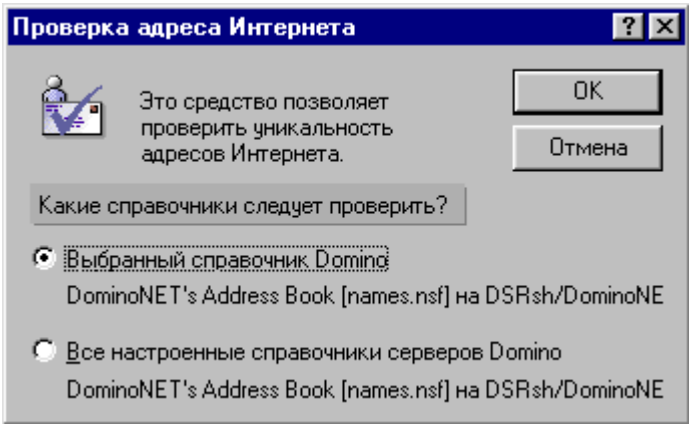


Рис. 80 Диалоговое окно проверки уникальности интернет адреса.

*1699 Выбираете проверку адреса интернета в текущем Domino Directory, или во всех доступных Domino Directory на сервере, затем – OK.

Инструмент проверяет каждое поле Address Internet в Domino Directory или всех каталогах, указанных в базе данных Directory Assistance (DA50.NSF). Если адрес не уникален, появится запись в файле LOG.NSF, Вашего сервера.

Обратите внимание, что поиск повторяющегося адреса затрачивает существенные ресурсы сервера. Не используйте этот инструмент, когда сервер сильно загружен. Lotus рекомендует пользоваться этим инструментом в то время, когда сервер не загружен.

4.3 Какой тип маршрутизации почты выбрать и как ее настроить?

4.3.1 Планирование топологии почтовой маршрутизации.

Domino представляет много возможностей для конфигурирования Вашей почтовой системы. Конфигурация может использовать Notes или SMTP маршрутизацию, или оба типа для внутренних и внешних систем передачи сообщений. Однако прежде чем Вы установите маршрутизацию почты, имеется множество факторов, которые могут повлиять на решение какой тип маршрутизации выбрать:

4.3.1.1 Какие типы почтовых клиентов поддерживает сервер Domino?

Когда Вы планируете топологию передачи почты, продумайте какие типы клиентов, Вы будете использовать для доступа пользователей, на Domino сервер. Domino поддерживает следующие типы клиентов - Notes, IMAP, POP3, NNTP и Web клиентов.

Notes клиенты.

Для доступа клиентов Notes к серверу, могут использоваться протоколы Notes, POP3, IMAP и NNTP. Если Ваша организация использует клиентов Notes, выберите любой из этих

протоколов для доступа клиентов к серверу. Разрешите выбранный Вами протокол на сервере.

IMAP клиенты.

Для доступа клиентов IMAP на почтовые сервера используются два протокола IMAP и SMTP. Клиент посылать почту на сервер по SMTP, а читает сообщения с использованием IMAP. Разрешите IMAP сервис на сервере и используйте Router для доставки сообщений IMAP клиентам.

POP3 клиенты.

Для доступа почтовых клиентов POP3 на сервер и чтения сообщений, используется POP3 протокол. Клиент посылает почту на сервер с использованием протокола SMTP. Разрешите POP3 задачу и используйте Router для доставки сообщений POP3 клиентам.

NNTP клиенты.

Вы можете использовать NNTP клиентов для доступа к группам новостей и базам данных обсуждений на сервере Domino, использую для этого NNTP службу. NNTP протокол не обеспечивает функциональные возможности передачи почты, хотя многие NNTP клиенты также включают в себя IMAP и POP3 возможности. Разрешите службу NNTP на сервере, чтобы использовать Domino сервер для чтения новостей.

Web клиенты.

За доступ Web клиентов на почтовый сервер Domino отвечает HTTP задача. Клиенты этого типа посылают почту с использованием протокола SMTP, а читают свои почтовые сообщение. Разрешите HTTP задачу и используйте Router для Web клиентов, чтобы использовать Domino сервер для передачи почты. Разрешите задачу SMTP Listener на Domino сервере.

4.3.1.2 Маршрутизация внутренней почты.

Для передачи почты в пределах Вашей организации Вы можете использовать локальные интернет домены. Решите, как клиенты будут получать доступ к их почтовым файлам на Domino серверах, и как сервера будут маршрутизировать почту. Router использует SMTP и Notes протоколы для маршрутизации почты с MIME и форматом Notes.

Domino может использовать стандартные протоколы интернет для передачи почты. Для доступа к почте, Domino может использовать POP3, IMAP, или HTTP. Чтобы посылать и передавать почту, Domino может использовать SMTP протокол.

Domino может использовать протоколы Notes для передачи почты. Протоколы Notes разрешены по умолчанию, когда Вы загружаете Router. Domino маршрутизирует сообщения MIME и Notes rich text формата, по протоколам Notes. Клиенты Notes используют протоколы Notes, которые разрешены по умолчанию, для доступа к почте на Domino сервере.

Domino может использовать и интернет, и протоколы Notes для передачи почты. Чтобы использовать протоколы Notes для передачи почты, разрешите следующие опции:

*1700 Протоколы доступа клиентов интернет на всех почтовых серверах. Протоколы доступа клиентам Notes позволяются по умолчанию.

*1701 Загрузите Router на каждом сервере

*1702 Разрешите задачу SMTP Listener, в Server документе для каждого сервера, на котором Вы хотите получать почту по SMTP протоколу

*1703 Выбирайте SMTP allowed within the local Internet domain, для MIME messages only, в документе Configuration Settings, для каждого сервера, с которого Вы хотите послать почту через SMTP.

*1704 Если Ваши сервера находятся в больше чем одной поименованной сети Notes, разрешите опцию Servers within the local Notes domain are reachable via SMTP over TCPIP, в документе Configuration Settings для каждого сервера, если хотите посылать и получить почту через SMTP.

Domino маршрутизирует MIME и Notes rich text формат сообщений, по протоколам Notes и маршрутизирует формат MIME по SMTP. Например, если получатель использует IMAP клиента, то для этого получателя создает сообщение формата MIME. Программное обеспечение клиента может создавать сообщение в обоих форматах, когда это необходимо. Например, программное обеспечение клиента создает сообщение в формате Notes rich text, для получателя, который использует клиента Notes R4 и создает сообщение MIME для получателя POP3 клиента.

Если и SMTP и Notes формат позволяется, Router сам выбирает оптимальный протокол, для перемещения сообщения на сервер назначения. Например, если SMTP позволяется для локального интернет домена, Router использует SMTP для маршрутизации копии MIME сообщения на сервер для POP3 получателя, но использует протокол Notes для маршрутизации Notes rich text копии, на сервер получателя Notes.

Smart Host.

Если не все пользователи Вашей системы внесены в Domino Directory, сконфигурируйте Smart Host, который имеет свой почтовый каталог пользователей. Router может передавать сообщения получателям из этого каталога, которые находятся в локальном интернет домене.

4.3.1.3 Маршрутизация внешней почты.

Для маршрутизации почты во внешние интернет домены, Вы должны настроить, по крайней мере, один сервер для соединения его с интернетом и маршрутизированием почты по SMTP. Вы можете так же настраивать несколько серверов, которые будут маршрутизировать почту в интернет.

Все сервера могут маршрутизировать почту во внешние домены.

В этой конфигурации, каждый почтовый сервер соединяется с интернетом по TCP/IP протоколу. Каждый сервер имеет разрешенную установку SMTP used when sending messages outside of the local Internet domain, в документе Configuration Settings. Когда пользователь посылает сообщение получателю во внешний интернет домен, Router просматривает записи DNS, для получения адреса IP сервера назначения. Он использует SMTP, для соединиться с сервером получателя. Router передает сообщение и закрывает сеанс связи SMTP.

Только некоторые сервера могут маршрутизировать почту во внешние домены.

В этой конфигурации, только некоторые выбранные почтовые сервера, соединены с интернетом. Другие почтовые сервера маршрутизируют сообщения, адресованные получателям во внешние интернет домены, на эти сервера. Чтобы устанавливать эту конфигурацию с использованием SMTP, сконфигурируйте сервера связанные с интернет, в

качестве Relay Hosts. Например, создайте имя DNS, для домена acme.com, сделайте несколько MX записей. Каждая запись MX описывает один из серверов. Введите имя DNS в поле Relay host for messages leaving the local Internet domain, в документе Configuration Settings, для всех серверов, которые не соединяются непосредственно с интернетом. Когда Router на этих серверах находит сообщение, адресованное получателю во внешнем интернет домене, это сообщение передается на один из серверов, которые внесены в список в DNS и соответствуют этим именам.

Чтобы установить эту конфигурацию, используя протоколы Notes, создайте документы Foreign SMTP Domain и SMTP Connection. Когда Router на сервере, не связанном непосредственно с интернетом находит сообщение, адресованное получателю во внешнем интернет домене, Router передает сообщением в домен, указанный в документах документы Foreign SMTP Domain и SMTP Connection. Router, одного из серверов, получивших сообщение, соединяется с внешним интернет доменом и передает сообщение.

Dial-Up тип соединение.

Ваша организация может соединяться с интернетом через Dial-Up соединение. Чтобы установить Dial-Up связь в Вашей Domino почтовой системе, создайте документ подключения Notes Direct Dial-Up и затем сконфигурируйте, как Domino будет, обменивается сообщениями.

Relay Host.

Вы можете маршрутизировать всю почту, через некоторый сервер SMTP. Укажите его имя в поле Relay Host, и все сообщения адресованные в интернет, будут передаваться на этот хост. Далее этот сервер будет заниматься передачей всей почты, получателям интернета.

4.3.2 Какие конфигурации можно использовать для маршрутизации почты?

Мы рассмотрим типичные конфигурации маршрутизации почты. Эти типовые конфигурации, помогут Вам спланировать почтовую инфраструктуру Вашей организации. Типичные конфигурации:

*1705 Использование одного сервера для передачи всех сообщений в интернет

*1706 Использование одного сервера для входящих и одного сервера для исходящих сообщений

*1707 Использование двух серверов, для сбалансирования интернет нагрузки

*1708 Установите маршрутизацию почты в локальном интернет домене

*1709 Установите маршрутизацию почты между Third-Party серверами и Domino, в том же самом интернет домене

*1710 Использование Smart Host

*1711 Использование всех серверов для маршрутизации исходящей почты и одного для маршрутизации внутренней почты

4.3.2.1 Использование одного сервера для всех рассылки и получения почтовых сообщений интернета.

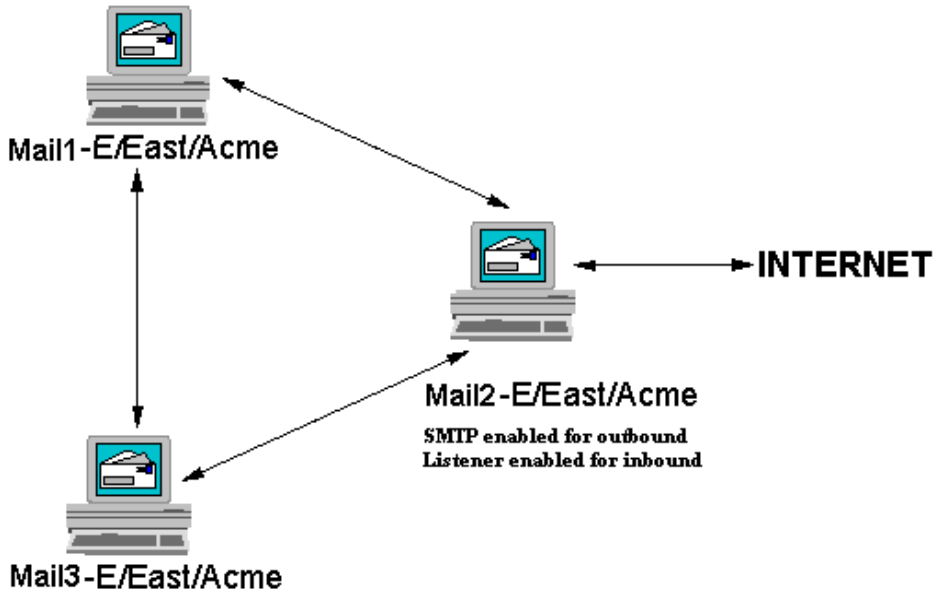


Рис. 81 Пример использования одного сервера для всех рассылки и получения почтовых сообщений интернета.

В этом примере единственный Domino сервер Mail2-E/East/Acme принимает и передает сообщения для организации Acme. Этот сервер передает почту в другие интернет домены и получает всю почту, адресованную на домен acme.com. Mail2-E/East/Acme имеет разрешение в поле SMTP used when sending messages outside of the local Internet domain, на закладке Router/SMTP – Basics, в документе Configuration Settings. Имеет запущенную задачу SMTP Listener, на закладке Basics, Server документа.

Если пользователи из двух Acme внутренних почтовых серверов, Mail1-E/East/Acme или Mail3-E/East/Acme, посылает сообщение внешнему адресату в интернет, сервера маршрутизируют сообщения на сервер Mail2-E/East/Acme, который может маршрутизировать почту во внешние домены. Любая почта из внешних интернет доменов, адресованная домену - acme.com, получает один сервер - Mail2-E/East/Acme, который определен в DNS как почтовый сервер для домена acme.com. Как только почта достигает Mail2-E/East/Acme, сервер маршрутизирует ее на сервер назначения.

Два внутренних почтовых сервера, Mail1-E/East/Acme и Mail3-E/East/Acme, могут маршрутизировать интернет почту на сервер, с использованием SMTP, или через Notes. Используя документы Foreign SMTP Domain и SMTP Connection, сервера связываются с Mail2-E/East/Acme, или через SMTP, сконфигурированного как Relay Host.

Конфигурирование этих серверов требует:

*1712 Разрешение SMTP used when sending messages outside of the local Internet domain, для Mail2-E/East/Acme

*1713 Разрешение задачи SMTP Listener, для сервера Mail2-E/East/Acme

*1714 Добавления в записи в DNS имени хоста компьютера, на котором запущен сервер Mail2-E/East/Acme, как почтовый сервер для домена acme.com

*1715 Разрешение опций SMTP allowed outside of the local Internet domain, для Mail1-E/East/Acme и Mail3-E/East/Acme. Определение Mail2-E/East/Acme как Relay Host, или создание документов Foreign SMTP Domain и SMTP Connection, для сервера Mail2-E/East/Acme

4.3.2.2 Использование одного сервера для отправки и одного сервера для принятия интернет сообщений.

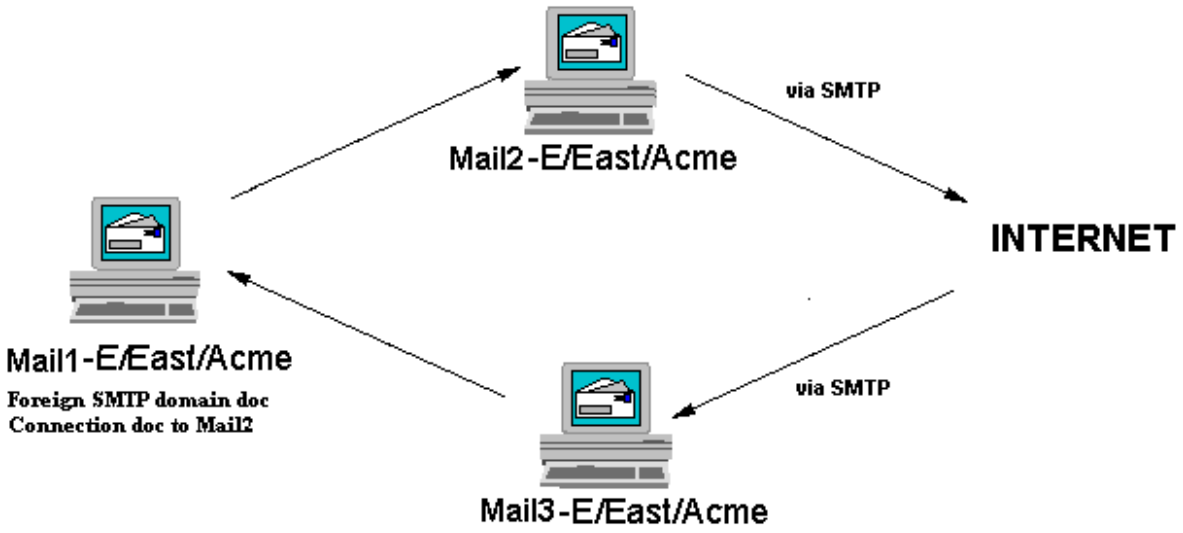


Рис. 82 Пример использования одного сервера для отправки и одного сервера для приема интернет сообщений.

В этом примере один Domino сервер Mail2-E/East/Acme предназначен для маршрутизации сообщений из организации Acme в интернет домены, а другой Domino сервер Mail3-E/East/Acme получат почту, адресованную интернет домену acme.com. Mail2-E/East/Acme имеет установку разрешения в поле SMTP used when sending messages outside of the local Internet domain, на закладке Router/SMTP – Basics, в документе Configuration Settings, который применяется только к этому серверу. Mail3-E/East/Acme имеет разрешенную задачу SMTP Listener, на закладке Basics, Server документа.

Если пользователь сервера, Mail1-E/East/Acme, посылает сообщение внешнему интернет адресату, сервер маршрутизирует сообщение на Mail2-E/East/Acme, который может маршрутизировать почту во внешние интернет домены. Любая почта из внешнего интернет домена, адресованная acme.com - доставляется на сервер Mail3-E/East/Acme, который определен в DNS, как почтовый сервер для домена acme.com. Как только почта достигает Mail3-E/East/Acme, сервер маршрутизирует ее на сервер назначения.

Внутренний почтовый сервер Mail1-E/East/Acme может маршрутизировать интернет почту на сервер Mail2-E/East/Acme определенный как Relay Host, с использованием SMTP, для внешних пользователей. Он может использовать маршрутизацию Notes, с использованием документов Foreign SMTP Domain и SMTP Connection.

Конфигурирование этих серверов требует:

*1716 Разрешение опции SMTP used when sending messages outside of the local Internet domain для сервера Mail2-E/East/Acme

*1717 Разрешение задачи SMTP Listener, на сервере Mail3-E/East/Acme

*1718 Настройте DNS, чтобы определить сервер Mail3-E/East/Acme, как почтовый сервер для домена acme.com

*1719 Разрешите опцию SMTP allowed outside of the local Internet domain, для Mail1-E/East/Acme. Определите сервер Mail2-E/East/Acme как Relay Host, или создайте документы Foreign SMTP Domain и SMTP Connection, для связи с Mail2-E/East/Acme

4.3.2.3 Использование двух серверов для сбалансирования нагрузки интернет почты.

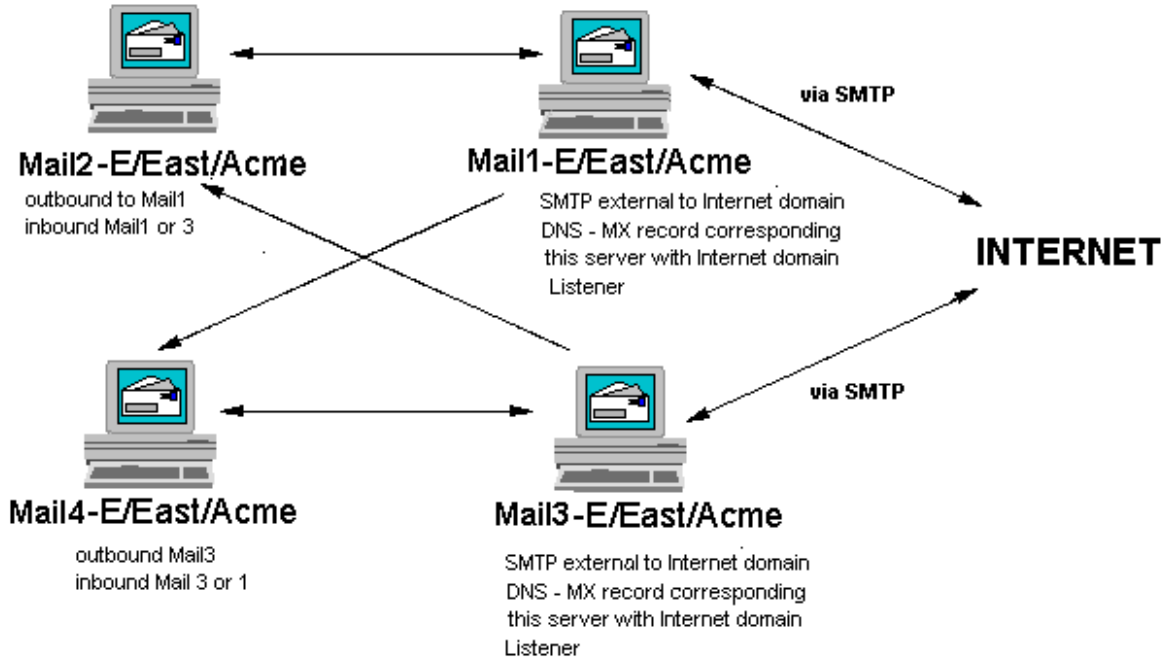


Рис. 83 Пример использования двух серверов для сбалансирования нагрузки интернет почты.

В этом примере, два Domino сервера, Mail1-E/East/Acme и Mail3-E/East/Acme, маршрутизируют сообщения из организации Acme в интернет домены. Сервера также получают почту, адресованную интернет домену acme.com. Mail1-E/East/Acme и Mail3-E/East/Acme имеют разрешение в поле SMTP used when sending messages outside of the local Internet domain, на закладке Router/SMTP – Basics, документа Configuration Settings. На обоих серверах разрешена задача SMTP Listener, на закладке Basics, Server документа.

Если пользователь Acme, внутреннего почтового сервера Mail2-E/East/Acme посылает сообщение внешнему адресату, сервер маршрутизирует сообщение на Mail1-E/East/Acme, который может передавать почту на внешние домены интернет. Если пользователь Acme, внутреннего почтового сервера Mail4-E/East/Acme посылает сообщение внешнему адресату, сервер маршрутизирует сообщение на Mail3-E/East/Acme, который может маршрутизировать почту во внешние домены. Таким образом, исходящая почта распределяется между серверами Mail1-E/East/Acme и Mail3-E/East/Acme.

Любая почта из внешних интернет доменов распределяется между Mail1-E/East/Acme и Mail3-E/East/Acme. DNS имеет две записи MX, одна для Mail1-E/East/Acme и одна для Mail3-E/East/Acme. Оба сервера определяются как почтовые хосты для домена acme.com. Когда интернет почтовый сервер пробует соединяться с доменом acme.com, чтобы передать сообщение, он посматривает записи для acme.com в DNS. Server находит записи MX acme.com и возвращает адрес IP Mail1-E/East/Acme или Mail3-E/East/Acme. Если записи

MX имеют равный приоритет, интернет сервер выбирает одну из записей и возвращает адрес IP сервера. Если этот, сервер недоступен, другая запись MX, будет обработана и адрес IP другого сервера будет возвращен. Такой подход обеспечивает сбалансирование нагрузки, используя случайный выбор записей MX, когда предпочтения для записей MX равны.

Внутренние почтовые сервера могут маршрутизировать интернет почту на сервера, т. к. у них разрешена опция - SMTP allowed outside of the local Internet domain.

Конфигурирование этих серверов требует:

*1720 Разрешения опций SMTP used when sending messages outside of the local Internet domain, для Mail1-E/East/Acme и Mail3-E/East/Acme

*1721 Разрешения задачи SMTP Listener, для серверов Mail1-E/East/Acme и Mail3-E/East/Acme

*1722 Настройте записи DNS, чтобы определить сервера Mail1-E/East/Acme и Mail3-E/East/Acme, как почтовые сервера для домена acme.com

*1723 Разрешите опцию SMTP allowed outside of the local Internet domain, для серверов Mail2-E/East/Acme и Mail4-E/East/Acme. Занесите в поля Relay Host, сервера Mail1-E/East/Acme или Mail3-E/East/Acme или создайте документы Foreign SMTP Domain и SMTP Connection, чтобы связываться с серверами Mail1-E/East/Acme или Mail3-E/East/Acme.

4.3.2.4 Маршрутизация почты в локальном интернет домене.

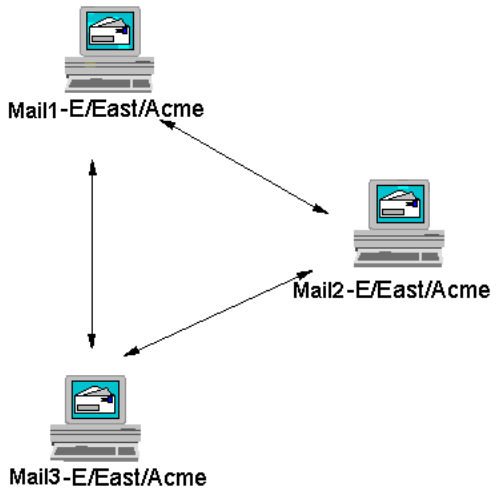


Рис. 84 Пример маршрутизации почты в локальном интернет домене.

В этом примере, пользователи Acme посылают сообщения в домен acme.com (внутренние сообщения) по SMTP. Mail1-E/East/Acme, Mail2-E/East/Acme и Mail3-E/East/Acme. Почтовые сервера Domino имеют разрешенную опцию - SMTP allowed within the local Internet domain, для MIME messages only, на закладке Router/SMTP – Basic, документа Configuration Settings, который применяется для всех серверов. Должна быть разрешена задача SMTP Listener, на закладке Basics, их Server документов. Это позволяет серверам посылать почту друг другу по SMTP и получать почту по SMTP.

Сервера должны быть в той же самой поименованной сети Notes, с сетевым протоколом TCP/IP. Каждый сервер в поле Servers within the local Notes domain are reachable via SMTP

over TCPIP, должен иметь разрешение, в документе Configuration Settings, который применяется к нему.

Если пользователь посылает сообщение MIME другому пользователю в домен acme.com, его почтовый сервер определяет, где находится почтовый сервер получателя, соединяется с этим сервером по TCP/IP и передает сообщение, используя SMTP. Если сообщение находится в формате Notes, например, а пользователь использует клиента Notes R4 - сообщение будет преобразовано в Notes формат.

Конфигурирование этих серверов требует:

*1724 Разрешение задачи SMTP Listener для серверов Mail1-E/East/Acme, Mail2-E/East/Acme и Mail3-E/East/Acme

*1725 Настройте DNS, чтобы определить сервер Mail3-E/East/Acme, как почтового сервер, для домена acme.com

*1726 Разрешите опцию SMTP allowed within the local Internet domain, для MIME messages only, для серверов Mail1-E/East/Acme, Mail2-E/East/Acme и Mail3-E/East/Acme

*1727 Если все три сервера находятся в той же самой поименованной сети Notes, разрешите опцию Servers within the local Notes domain are reachable via SMTP over TCPIP, для каждого сервера

4.3.2.5 Маршрутизация почты с использованием Third-Party сервера и внутреннего интернет домена серверов Domino.

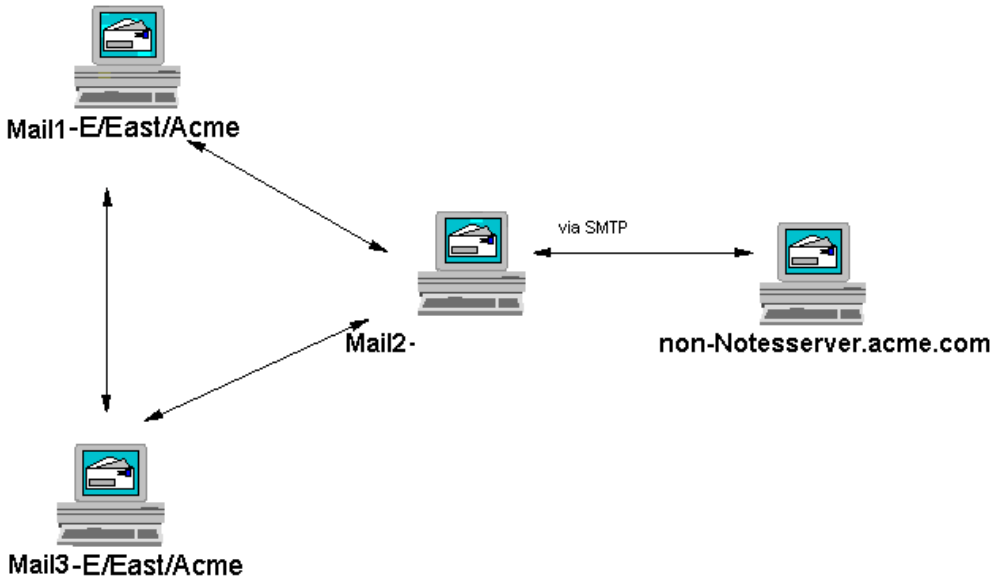


Рис. 85 Пример маршрутизации почты с использованием Third-Party сервера и внутреннего интернет домена серверов Domino.

В этом примере, Acme имеет три Domino сервера и Third-Party SMTP Host, в локальном интернетом домене, который используется как почтовый сервер для некоторых пользователей. Все пользователи имеют записи в Domino Directory.

Когда пользователь посылает почту другому пользователю в домене acme.com, Domino сервер посматривает получатель в Domino Directory. Если получатель имеет почтовый файл на одном почтовых серверов Domino Mail1-E/East/Acme, Mail2-E/East/Acme или Mail3-E/East/Acme, сервера используют для маршрутизации Notes протокол передачи

сообщений. Notes тип маршрутизация используется и с MIME, и с форматом Notes. Если получатель имеет почтовый файл на сервере Third-Party, non-Notesserver.acme.com, их документ Person имеет адрес в формате SMTP. На серверах Mail1-E/East/Acme и Mail3-E/East/Acme есть документы типа Foreign SMTP Domain, для *.non-Notesserver.acme.com, который соответствует документу подключения типа SMTP, и определяют Mail2-E/East/Acme сервер, для передачи сообщений. Сервера посылают сообщения с использованием Notes, на сервер Mail2-E/East/Acme, который имеет разрешение в поле SMTP used when sending messages outside of the local Internet domain, на закладке Router/SMTP – Basics, в документе Configuration Settings, который применяется к этому серверу. На этом же сервере разрешена задача SMTP Listener, на закладке Basics, Server документа. Если сообщение находится в формате Notes, Mail2-E/East/Acme конвертирует его в MIME. Mail2-E/East/Acme соединяется с non-Notesserver.acme.com по TCP/IP и передает сообщение по SMTP.

Если пользователь из non-Notesserver.acme.com посылает сообщение пользователю на Mail1-E/East/Acme, Mail2-E/East/Acme, или Mail3-E/East/Acme, server передает сообщение на Mail2-E/East/Acme по SMTP, а Mail2-E/East/Acme маршрутизирует сообщение на сервер назначения по Notes протоколу.

Конфигурирование этих серверов требует:

*1728 Разрешение задачи SMTP Listener, для сервера Mail2-E/East/Acme

*1729 Настройка записей DNS

*1730 Создание документов Foreign SMTP Domain для *.non-Notesserver.acme.com и документа SMTP Connection, для Mail2-E/East/Acme

4.3.2.6 Использование Smart Host.

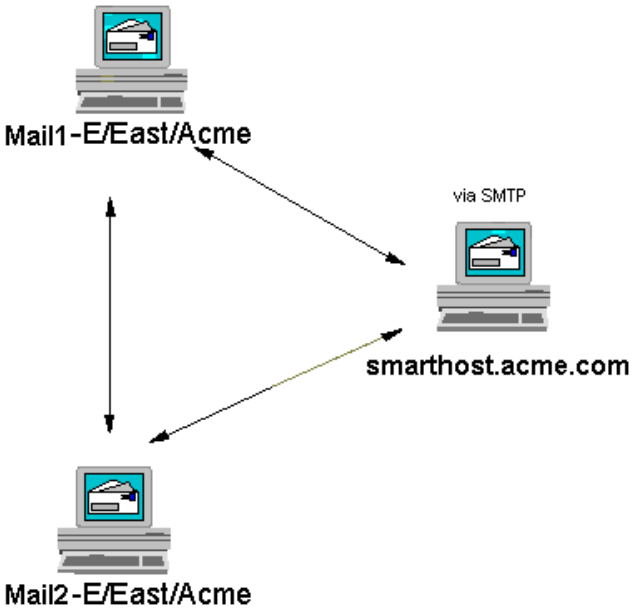


Рис. 85 Пример использования Smart Host.

В этом примере, Acme имеет три сервера: Mail1-E/East/Acme, Mail2-E/East/Acme и smarthost.acme.com Third-Party SMTP Host, имеют почтовые файлы некоторых пользователей. Сервера в этом примере, по существу те же самые что и описанные в предыдущем параграфе, за исключением того, что не все пользователи внесены в Domino

Directory. Smart Host сервер, smarthost.acme.com имеет каталог, для этих пользователей. Mail1-E/East/Acme и Mail2-E/East/Acme имеют разрешение в поле SMTP allowed within the local Internet domain и имеют запись smarthost.acme.com, внесенную в поле Local Internet domain smart host, на Router/SMTP – Basic, из документа Configuration Settings, который применяется для серверов.

Если пользователь на одном из почтовых серверов Domino посылает сообщение пользователю в acme.com интернет домене и Router не может найти получателя в Domino Directory, Router передает сообщение на smarthost.acme.com, с использованием SMTP.

Конфигурирование этих серверов требует:

*1731 Настройки записей DNS

*1732 Разрешение опции SMTP allowed within the local Internet domain, для MIME messages only, для Mail1-E/East/Acme, Mail2-E/East/Acme

*1733 Введение имени сервера smarthost.acme.com в поле Local Internet domain smart host, для Mail1-E/East/Acme и Mail2-E/East/Acme

4.3.2.7 Использование всеми серверами маршрутизации исходящей интернет почты.

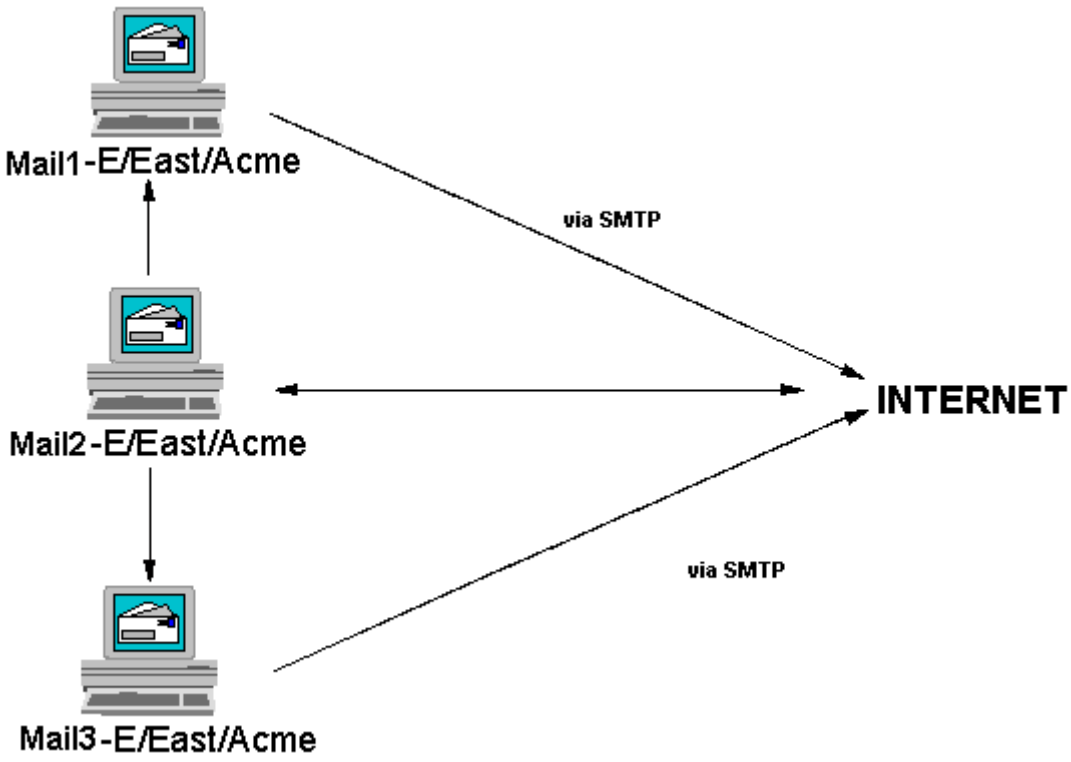


Рис. 86 Пример использования всеми серверами маршрутизации исходящей интернет почты.

В этом примере, Acme имеет три почтовых сервера, Mail1-E/East/Acme, Mail2-E/East/Acme, и Mail3-E/East/Acme, каждый из которого может маршрутизировать сообщения из Acme организации, во внешние интернет домены. Mail1-E/East/Acme, Mail2-E/East/Acme и Mail3-E/East/Acme имеют разрешение в поле SMTP used when sending messages outside of the local Internet domain, на закладке Router/SMTP – Basics, документа Configuration Settings. Один

сервер, Mail2-E/East/Acme, получает почту, адресованную домену Acme (acme.com). На сервере Mail2-E/East/Acme разрешена задача SMTP Listener, на закладке Basics, Server документа.

Если пользователь на одном из почтовых сервере посылает сообщение внешнему адресату - сервер просматривает домен назначения в DNS, соединяется с ним по TCP/IP, устанавливает SMTP сессию и передает сообщение.

Любая почта из внешних интернет доменов - поступает на сервер Mail2-E/East/Acme. В DNS Mail2-E/East/Acme определен как почтовый сервер, для домена acme.com. Как только почта достигает Mail2-E/East/Acme, сервер маршрутизирует сообщения на сервер назначения.

Так как каждый из серверов может посылать сообщения непосредственно во внешние домены, никакие поля Relay Host не заполняются и документы Foreign SMTP Domain или SMTP Connection - не нужны.

Конфигурирование этих серверов требует:

*1734 Разрешение опций SMTP used when sending messages outside of the local Internet domain, для всех серверов

*1735 Разрешение задачи SMTP Listener, для сервера Mail2-E/East/Acme

*1736 В записи DNS должен быть внесен сервер Mail2-E/East/Acme, как почтовый сервер для домена acme.com

4.3.3 Для чего используется документ Configuration Settings?

При использовании документов Configuration Settings, Вы можете настраивать маршрутизацию почты для нескольких Domino серверов, одним документом. Документ Configuration Settings включает в себя назначения серверов и Notes или SMTP маршрутизацию. Используйте один документ Configuration Settings для:

*1737 Для всех Domino серверов в Notes домене.

*1738 Для серверов в определенной группе.

*1739 Для определенного сервера.

Вы можете выбрать опцию настроек для всех серверов в Notes домене. Это дает Вам контроль над Вашей системой и может экономить время, потому что Вы можете использовать один документ, чтобы изменить назначения для всего домена.

Каждая установка, которую Вы определяете, применяется к каждому серверу, включенному в документ Configuration Settings. Поэтому, Вы будете нуждаться в нескольких документах конфигураций, если Вы нуждаетесь в различных назначениях для определенных серверов. Например, если Ваш Notes домен включает три географически разделенных сервера, Вы может создать Configuration Settings документ для каждого сервера. Вы можете создавать группы, которые включают все сервера определенного местоположения и использовать место расположения - как имя группы.

Чтобы определить дополнительные ограничения для сервера, который включен в группу, создают отдельный документ Configuration Settings, для определенного сервера. Например, Вы имеете документ Configuration Settings для группы серверов, или для всех серверов. Если в Вашей компании Вы хотите ограничить, или наоборот предоставить некоторые

права, определенному серверу, создайте документ Configuration Settings для этого сервера. Документ конфигурации для конкретного сервера, будет иметь приоритет, по отношению к документу конфигурации для группы.

Каждый сервер проверяет документы Configuration Settings в следующем порядке:

*1740 Документ, определенный для сервера

*1741 Документ группы серверов

*1742 Документ по умолчанию

Если имеется несколько документов Configuration Settings для групп, содержащих один и тот же самый сервер, результат будет неопределенный. Например, Вы имеете сервер А и две группы с именем группа 1 и группа 2. Обе группы содержат сервер А. Если Вы создаете документ Configuration Settings для сервера А, все назначения, которые будут установлены в этом документе, будут использоваться сервером А. Если не имеются документа для сервера назначения А, то просматриваются документы Configuration Settings для групп 1 и 2. Однако любые назначения, которые были определены в документе сервера А, не будут действовать в группах 1 и 2. Если после поиска документов для групп 1 и 2, документы не найдены, применяются назначения по умолчанию.

Обратите внимание на использование полных имен хостов в полях документов Configuration Settings вместо IP адресов. Хотя IP адресы будут работать и полностью поддерживаются.

Создания документов Configuration Settings.

*1743 Из клиента Domino Administrator, выбирайте закладку – Настройка, затем откройте секцию Почта.

*1744 Выбирайте представление – Конфигурации.

*1745 Выбирайте – Add Configuration, чтобы создать новый документ Configuration Settings.

*1746 Выбирайте закладку – Basics.

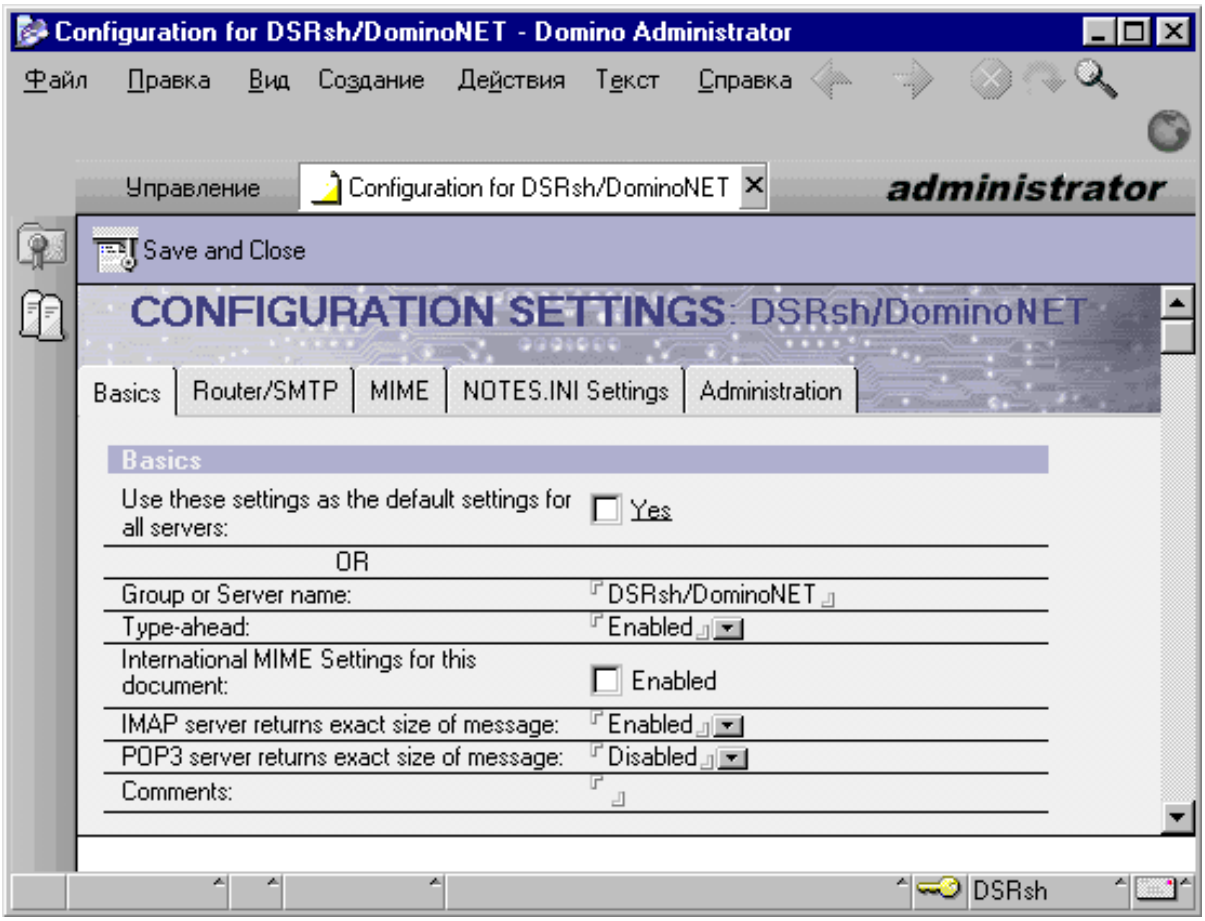


Рис. 87 Пример Configuration Settings документа.

*1747 Заполните любые поля и сохраните документ.

4.3.4 Настройка Notes маршрутизации.

Вы создаете документы в Domino Directory, чтобы настроить Notes маршрутизацию. Потому что Domino автоматически маршрутизирует почту, между серверами в той же самой поименованной сети Notes, и Вы не должны создавать документы подключения, чтобы вынуждать маршрутизацию почты между серверами в поименованной сети Notes. Однако если сервера находятся не в той же самой поименованной сети Notes, Вы должны создать документы подключения в Domino Directory, чтобы определить, как будет маршрутизирована почта в пределах системы Notes. Как Вы будете создаете связи для маршрутизации Notes, зависит от:

*1748 Местоположения двух серверов: та же самая поименованная сеть Notes, тот же самый Notes домен, Adjacent Notes домен, Non-Adjacent Notes домен

*1749 Тип связи требуемой для двух серверов: LAN, Notes Direct Dial-Up, Network Dial-Up, или Passthru server.

Кроме того, маршрутизация почты - определяет, сколько документов подключений Вы должны создать. В большинстве случаев, вы будете маршрутизировать почту в обоих направлениях, поэтому Вы создаете два документа подключения с каждой стороны.

Если Вы уже настроили репликации, Вы возможно уже создали документы подключения, в которых Вы нуждаетесь. Вы можете использовать тот же самый документ подключения

для репликаций и передачи почты, или Вы можете создать отдельный документ подключения для каждой задачи.

Эта таблица описывает типы связей и документов, требуемых для установки связей.

Места расположения серверов	**Документы, которые нужно создать**
Если нет поименованной сети Notes, для серверов в Notes домене	Создается два документа подключения, для маршрутизации почты в обоих направлениях.
Adjacent Notes домены (соседний домен)	Создается два документа подключения, для каждого Notes домена, если планируется двухсторонняя передача почты. Один документ домена Adjacent Domain, если хотите ограничиться только одним направлением передачи почты.
Non-adjacent Notes домены (не соседний домен)	Создается два документа подключения, по одному на каждый Notes домен. Два документа Non-Adjacent Domain, по одному для каждого Notes not adjacent домена, чтобы связаться, через сервер посредник (для первого и последнего сервера).
Шлюз использующий foreign домен (не-notes)	Один документ Foreign domain, для идентификации Foreign Domain, для передачи сообщений системам Fax или Pagers.
SMTP сервер	Один документ Foreign SMTP domain, для идентификации местоположения и передачи почты в интернет на промежуточный почтовый сервер интернет SMTP. Один документ SMTP connection, для SMTP значение – Enabled.

Примечание. Когда Вы создаете документ подключение, маршрутизация Notes позволяется по умолчанию.

4.3.4.1 Создание документа Adjacent Domain.

Вы создаете Adjacent Domain документ, когда Вы должны применить ограничения для направления сообщений в соседний домен. Ограничения действуют и применяются только для этих доменов.

Создание документа Adjacent Domain.

*1750 Из клиента Domino Administrator, выбирайте закладку Настройка, затем откройте секцию Почта.

*1751 Выбирайте – Домены.

*1752 Выбирайте – Add Domain.

*1753 На закладке Basics заполните нужные поля:

Поля	**Значения**
Domain type	Выбирайте Adjacent Domain
Adjacent Domain name	Имя Adjacent Notes domain
Domain description	Описание домена

*1754 Выбирайте закладку Restrictions, заполните, если нужно поля, сохраните документ:

Поля	**Значения**
Allow mail only from domains	Имена Notes доменов, из которых разрешена отправка почты в Adjacent Domain
Deny mail from domains	Имена Notes доменов, из которых не разрешается передача почты в Adjacent Domain

4.3.4.2 Создание документа Non-Adjacent Domain.

Вы создаете документ Non-Adjacent Domain, чтобы указать путь между серверами, которые расположены в Notes доменах, которые подключаются друг к другу только с использованием домена посредника, известного как Adjacent Domain. Вы также используете документы Adjacent Domain, чтобы подключиться к домену посреднику. Если применяется предположение, что все серверы в домене используют тот же самый Domino Directory, Вы нуждаетесь только в одном документе Non-Adjacent Domain, для каждого Non-Adjacent Domain.

Ограничения, которые Вы устанавливаете для документа Non-Adjacent Domain, применяются только к предыдущему домену. Эти ограничения работают вместе с теми, которые вы найдете в документе Configuration Settings.

Создания документа Non-Adjacent Domain.

*1755 Из клиента Domino Administrator, выбирайте закладку Настройка, затем откройте секцию Почта.

*1756 Выбирайте – Домены.

*1757 Выбирайте – Add Domain.

*1758 На закладке Basics заполните нужные поля:

Поля	Значения
Domain type	Выбирайте Non-Adjacent Domain
Mail sent to domain	Имя Notes домена назначения
Route through domain	Имя домена посредника
Domain description	Описание домена

*1759 Выбирайте закладку Restrictions, заполните, если нужно любые поля и сохраните документ.

4.3.4.3 Создание документа Foreign domain.

Вы создаете документ Foreign domain, чтобы указать путь между Notes доменом и внешним приложением типа шлюза для факса или пейджера. Документ Foreign domain обозначает сервер, который направляет сообщения в шлюз. Так же, как Domino обрабатывает группу серверов, как домен, он обрабатывает группу компьютеров в Foreign системе, как домен. Foreign domains, главным образом используется для разработок третьих лиц, но может использоваться для передачи сообщений между R5 сервера и R3 сервера SMTP.

Приложения типа X.400, cc:Mail отделяют документы Foreign domain, чтобы направлять сообщения через агента MTA. Для получения дополнительной информации относительно MTAs, см. документацию.

Создания документа Foreign domain.

*1760 Из клиента Domino Administrator, выбирайте закладку Настройка, затем откройте секцию Почта.

*1761 Выбирайте – Домены.

*1762 Выбирайте – Add Domain.

*1763 На закладке Basics заполните нужные поля:

Поля	Значения
Domain type	Выбирайте Foreign domain.
Foreign Domain Name	Имя домена для foreign почтовой системы. Это имя выбирается, если MTA шлюз инсталлирован.
Domain description	Описание шлюза или MTA.

*1764 Выбирайте закладку Restrictions и заполняйте нужные поля.

*1765 Выбирайте закладку Mail Information и заполните эти поля, после чего сохраните, и закройте документ:

Поля	Значения
Gateway server name	Имя Domino сервера использующегося как шлюз.

Gateway mail filename	Имя файла почтовой системы шлюза.

4.3.4.4 Создание документа Foreign SMTP domain.

Вы создаете документ Foreign SMTP domain для любого сервера, который должен посылать сообщения SMTP, но сам он не установлен как SMTP сервер.

В документе Foreign SMTP domain, Вы определяете, куда направить сообщения, адресованные в интернет. Например, Вы можете указать в документе Foreign SMTP domain, чтобы направить всю исходящую почту SMTP, в другой Notes домен. Тогда сервер, который находится в этом домене и определенный как SMTP сервер, будет маршрутизировать почту SMTP в интернет.

Если в документе Foreign SMTP domain определен тип почты как *.*, то вся почта, соответствующая маске *.* - например, acme.com или mail1.acme.com - маршрутизируется адресату, указанному в документе Foreign SMTP domain. Если Вы используете подстановочный знак, Вы можете все еще ограничить сообщения определенным интернет доменам, определяя ограничения в документе Configuration Settings.

Создания документа Foreign SMTP domain.

*1766 Из клиента Domino Administrator, выбирайте закладку Настройка, затем откройте секцию Почта.

*1767 Выбирайте – Домены.

*1768 Выбирайте – Add Domain.

*1769 На закладке Basics заполните нужные поля:

Поля	**Значения**
Domain type	Выбирайте Foreign SMTP Domain

*1770 Выбирайте закладку Routing, заполняйте нужные поля.

Поля	**Значения**
Internet Domain	Имя интернет домена, к которому этот документ применяется, или ко всем доменам (*.*)
Domain name	Имя виртуального домена.

*1771 Создайте документ SMTP Connection, для соединения с сервером, на котором установлен и SMTP.

4.3.4.5 Создание документа SMTP Connection.

Документ SMTP Connection определяет, как сообщения направляются с сервера, который не может посылать сообщения SMTP, на сервер который это умеет. Документ SMTP Connection определяет подключение между Notes доменом и серверами SMTP.

Создания документа SMTP Connection.

*1772 Из клиента Domino Administrator, выбирайте закладку Настройка и затем откройте секцию Почта.

*1773 Выбирайте – Подключения и выбирайте – Add Connection.

*1774 На закладке Basics, заполните нужные поля и затем сохраните документ:

Поля	**Значения**
Connection type	SMTP
Source server	Имя non-SMTP сервера
Source domain	Имя non-SMTP домена серверов
Connect via	Direct connection
Destination server	Имя виртуального сервера, например – All_Internet_hosts
Destination domain	Имя виртуального домена, указанного в поле интернет Domain name, документа Foreign SMTP domain.

4.3.5 Настройка SMTP маршрутизации.

Чтобы разрешить маршрутизацию SMTP, Вы должны подготовить Вашу систему для рассылки сообщений в интернет и затем сделайте любое из следующего:

*1775 Настроить маршрутизацию SMTP, для рассылки почты за пределы локального интернет домена

*1776 Настроить маршрутизацию SMTP, для рассылки почты адресатам локального интернет домена

*1777 Настроить сервера для получения почты, посланной с использованием маршрутизации SMTP

4.3.5.1 Настройка получения и отправки интернет почты

Используйте следующий порядок, чтобы удостоверится, что Ваша система готова к получению и отправке почты в интернета или другую частную сети, с использованием SMTP.

*1778 Удостоверитесь, что Вы имеете подключение к интернет через ISP или прямое подключение.

*1779 Использовать команду PING, чтобы проверить связь между сервером, с разрешенным SMTP и любым внешним компьютером. Проверите подключение между компьютерами, с которых сообщения будут посылаться и серверами, с которых Вы посылаете почту во внешний мир. PING проверяет только доступность компьютера, а не существование или надлежащее конфигурирование на нем SMTP.

*1780 Определить список интернет доменов, которые зарегистрированы за Вашей организацией. В некоторых случаях, компания может иметь несколько интернет доменов. Введите эти имена как псевдонимы в документе Global domain.

*1781 Удостоверитесь что DNS установлен, для определения всех имен хостов интернет доменов, которые Ваша компания использует.

*1782 Если Ваша компания использует почтовый сервер Relay или Firewall, узнайте их имена хостов.

4.3.5.2 Настройка SMTP маршрутизации во внешние интернет домены из локального интернет домена.

Вы должны разрешить опцию SMTP routing to send messages outside of the local Internet domain, для разрешения передачи сообщений в интернет или другую частную сеть.

Для разрешения опции SMTP routing outside of the local Internet domain, удостоверитесь, что Вы подготовили Вашу систему для рассылки почты интернет.

*1783 Удостоверитесь, что Вы уже имеете документ Configuration Settings для сервера(ов).

*1784 Из клиента Domino Administrator, выбирайте закладку Настройка, затем откройте представление Конфигурации

*1785 Выбирайте документ Configuration Settings, затем выбирайте – Edit Configuration.

*1786 На закладке Routing/SMTP - Basics, измените, если это необходимо значение следующенго поля и затем сохраните документ:

Поле	**Значение**
SMTP used when sending messages outside the local Internet domain	Выбирайте одно из двух: *1787 Enabled – для использования SMTP маршрутизации почты интернет *1788 Disabled - (по умолчанию) маршрутизация почты во внешние домены запрещена

4.3.5.3 Настройка SMTP маршрутизации в пределах локального интернет домена.

Вы можете использовать SMTP маршрутизацию, для рассылки сообщений другим серверам, в пределах Вашего локального интернет домена.

Однако Вы можете разрешить SMTP маршрутизацию, не на каждом сервере. Как правило, используются только некоторые сервера, для передачи почты, вне поименованной сети Notes. Например, Вы не можете иметь прямое подключение между всеми серверами, в

одной TCP/IP поименованной сети Notes. Вы можете определить, чтобы все сообщения из одной Notes поименованной сети перемещались в другую, через сервера посредники.

Для разрешения опции SMTP routing within the local Internet domain:

*1789 Удостоверитесь, что Вы уже имеете документы Configuration Settings для сервера(ов).

*1790 Из клиента Domino Administrator, выбирайте закладку Настройка, затем откройте секцию Конфигурации.

*1791 Выбирайте документ Configuration Settings, затем выбирайте – Edit Configuration.

*1792 Выбирайте закладку Router/SMTP – Basics.

*1793 Проверьте значения указанных полей, измените их значения, если это необходимо и затем сохраните документ:

Поле	**Значение**
SMTP allowed within the local Internet domain	Выбирайте одно: *1794 MIME messages only - только сообщения MIME должны маршрутизироваться по SMTP, в пределах поименованной сети Notes *1795 Disabled - (по умолчанию) использовать Notes маршрутизацию для передачи почты на другие сервера в поименованной сети Notes *1796 All messages - для всех сообщений использовать SMTP маршрутизацию, для передачи сообщений Notes формата и MIME формата сообщений. Это означает что все сообщения, включая Notes формат сообщений, будут конвертированы в MIME формат, для передачи.
Servers within the local domain are reachable via SMTP over TCPIP	Выбирайте одно: *1797 Always - (по умолчанию) всегда использовать маршрутизацию SMTP для передачи почты на другие Domino сервера, которые находятся в одном и тоже интернет домене. Эта установка разрешает прием почты и маршрутизацию с использованием SMTP. *1798 Only if in same Notes Named Network – только для той же самой поименованной сети Notes. Для использования маршрутизации Notes, для передачи почты на сервера в другие поименованные сети Notes, даже если разрешена опция рассылки SMTP within the local Internet domain.

4.3.5.4 Настройка серверов для получения почты посланной с использованием SMTP маршрутизации.

Чтобы сервер мог получать SMTP сообщения, Вы должны разрешить задачу SMTP Listener. Тогда сервер сможет прослушивать SMTP порт TCP/IP (обычно на порту 25) и получать сообщения SMTP в базу данных MAIL.BOX.

Примечание. Не добавляйте SMTP задачу в список задач в файл Notes.INI, или эта задача не будет работать.

Разрешения задачи SMTP Listener:

*1799 Из клиента Domino Administrator, выбирайте закладку Настройка, затем откройте секцию Сервера – Все документы на сервере.

*1800 Выбирайте сервер документ, затем выбирайте – Edit Server.

*1801 На закладке Basics, разрешите задачу - SMTP lister task и затем сохраните документ.

4.3.6 Настройка решения адресов.

Чтобы сообщения должным образом доставлялись адресатам, Вы можете конфигурировать следующее:

*1802 **Переадресация сообщений** - для пользователей, которые не имеют почтового файла Notes

*1803 **Smart host** - хост, который содержит адресные книги для организации

*1804 **Любой псевдоним** – имя псевдонима для интернет домена, используемого Вашей организацией

*1805 **Входящий интернет адрес** – Person документа

*1806 **Хост имя** - Имя хоста для исходящих сообщений

4.3.6.1 Настройка опции Forwarding Address.

Forwarding address позволяет пользователям, которые имеют Person документы в Domino Directory, переадресовывать почту на другой адрес. Имеются различные причины, почему это бывает полезно:

*1807 Пользователи изменяют свои имена. Например, из-за вступления в брак - но все еще хотят получить все сообщения.

*1808 Пользователь меняет место работы. Например, пользователь может уйти в отставку из компании, он определяет значение поля Forwarding Address, чтобы почта направлялась по старому адресу и отправлялась на новое местоположение.

*1809 Пользователи используют различные почтовые системы и не имеют почтовых файлов Notes.

Сконфигурируйте Forwarding Address, для Person документа пользователя.

4.3.6.2 Настройка опции Smart Host.

Smart Host – это хост, которому SMTP перенаправляет сообщения посланные получателю которого не удалось найти в локальном Domino Diorectory интернет домена. Когда сообщение получено, Router ищет адрес получателя, чтобы определить находится ли он в локальном домене интернета. Router проверяет Person документы, чтобы определить, куда послать сообщение. Иногда организация использует другие системы почты, пользователи этих систем не могут находится в Domino Directory. В том случае, Вы можете определить почтовый сервер такой системы как Smart Host. Например, если некоторые пользователи находятся в системе UNIX SendMail, но их сообщения - маршрутизируются через систему почты Domino, Вы можете определять Smart Host.

Определение значения поля Smart Host

*1810 Удостоверитесь, что Вы уже имеете документ Configuration Settings, для сервера(ов).

*1811 Откройте его для редактирования и перейдите на закладку Router/SMTP – Basics.

*1812 Заполните следующие поля и затем сохраните и закройте документ:

Поля	**Значения**
Local Internet domain smart host	Имя хоста сервера, для SMTP пользователей, которые находятся в адресной книге отличной от Domino Directory.
Smart host is used for all local Internet domain recipients	Выберите одно из двух: *1813 Enabled – разрешить маршрутизацию всех SMTP сообщений на Smart Host, для поиска пользователей, перед направлением их в другое место. *1814 Disabled - запретить маршрутизацию сообщений, чьи адреса не найдены в Domino Directory.

4.3.6.3 Использование нескольких имен интернет доменов в одной организации.

Ваша организация должна иметь единственное имя интернет домена - например, acme.com. Однако некоторые организации могут использовать несколько имен интернет доменов. Использование нескольких имен интернет доменов может использоваться когда:

*1815 Организация изменяет имя

*1816 Организация приобретает другую компанию, которая уже имеет существующее имя интернет домена и пользователи продолжают использовать другой интернет домен в своих адресах

*1817 Вы устанавливаете почтовую топологию, с маршрутизацией сообщений, в другие филиалы через Ваш Firewall в интернет, или другую частную сеть

*1818 Вы настраиваете топологию почты, чтобы использовать более чем одно имя интернет домен

Если Ваша организация использует больше чем одно имя интернет домена, Вы должны создать документ Global domain, чтобы определить различные имена интернет доменов, для которых может быть получена почта из интернета. Вы должны также сконфигурировать записи DNS для включения всех имен интернет доменов, которые Ваша компания использует.

Настройки использования нескольких имен интернет доменов в организации.

*1819 Удостоверитесь, что Вы уже имеете документ Configuration Settings для сервера(ов).

*1820 Из клиента Domino Administrator, выбирайте закладку Настройка, затем откройте секцию – Почта.

*1821 Выбирайте – Домены – Add Domain.

*1822 На закладке – Basics заполните поля:

Поле	**Значения**
Domain type	Выбирайте Global Domain
Global domain name	Любое описание домена
Global domain role	Выбирайте R5 интернет Domain или R4.x SMTP MTA

*1823 Выбирайте закладку – Conversions и заполните эти поля. Сохраните и закройте документ:

Поле	**Значения**
Local primary Internet domain	Имя первичного интернет домена, которое Ваша компания использует. Например, ACME.COM
Alternate Internet domain aliases	Дополнительные имена интернет домена, используемые Вашей компанией. Например, ANOTHER.COM

4.3.6.4 Способы поиска адреса в Person документах пользователей

Вы можете определить, как локальные пользователи будут искаться адреса в Domino Directory. Имеются три выбора:

*1824 **Fullname only** - ищется полное имя SMTP, в Domino Directory (First_Last Acme.com)

*1825 **Local Part only** - чтобы искать локальную часть адреса в Domino Directory

*1826 **Fullname then Local Part** - чтобы искать полный адрес сначала, а затем локальную часть, если не имеется первого.

Обратите внимание, Если Вы заполнили поле интернет адреса в Person документах пользователей для всех Ваших пользователей, выбирайте только – Fullname.

Для выбора способа поиска адресов.

*1827 Удостоверитесь, что Вы уже имеете документ Configuration Settings для сервера(ов).

*1828 Откройте его для редактирования на закладке Router/SMTP – Basics.

*1829 Заполните эти поля и затем сохраните и закройте документ:

Поле	**Значение**
Address lookup	Выбирайте одну функцию: *1830 Fullname then Local Part - (по умолчанию) искать сначала интернет адрес, а затем локальный. *1831 Fullname only - чтобы посмотреть полный адрес интернета *1832 Local Part only - искать только, для определения адреса Notes пользователя
Exhaustive lookup	Выбирайте одно: *1833 Enable - разрешается поиск во всех Directories *1834 Disabled - (по умолчанию) ограничивается поиск только первым Directory.

4.3.6.5 Настройка Router, для разрешения IP адреса SMTP сервера назначения.

Вы можете определить, как Router будет определять IP адрес(а) для SMTP систем. Вы можете настраивать метод разрешения адреса, для задачи Router. Методы разрешения адреса:

*1835 Только динамический поиск (DNS только)

*1836 Только локальный поиск

*1837 Динамически, потом локально

Если Вы сконфигурировали TCP/IP, чтобы использовать DNS, выберите динамическое разрешение или динамический, а потом локальный. Для динамического поиска, Router просматривает DNS записи и находит имя хоста и получает IP адрес.

При использовании динамического, а потом локального поиска, Router сначала просматривает DNS, а затем проверяет локальные HOSTS файлы. Файл известный как HOSTS, содержит имена и IP адреса хостов. Динамический, а потом локальный выбор может быть полезен, если Вы должны соединиться с внутренними хостами, которые не внесены в записи DNS.

Если Вы сконфигурировали TCP/IP, чтобы использовать поиск в локальных Hosts файлах, выберите опцию Local lookup only. Если Вы используете этот выбор, IP адрес и полное имя хостов для каждого сервера назначения должно быть указано в HOSTS файле. Выбор данной опции требует внимательного администрирования, потому что Вы должны следить и своевременно обновлять HOSTS файлы.

Если DNS не содержит список имен хостов назначения, Router определяет сообщение как не доставленное. Если DNS недоступен, Router повторяет отправку, согласно числу и времени обозначенном в соответствующих полях документов Configuration Settings.

Определения способа решения адресов.

*1838 Удостоверитесь, что Вы уже имеете документ Configuration Settings для сервера(ов).

*1839 Откройте его для редактирования, на закладке Router/SMTP – Basics.

*1840 Заполните эти поля и затем сохраните и закройте документ:

Поле	**Значение**
Host name lookup	Выбирайте одно: *1841 Dynamic lookup only (DNS only) - (по умолчанию) просмотр только DNS, для решения IP адресов *1842 Local lookup only (host files only) – использование только HOSTS файлов *1843 Dynamic then local – DNS потом HOSTS файлы

*1844 Перегрузите систему, чтобы изменение вступили в силу.

4.3.7 Настройки Relay Host или Firewall.

Relay Host может быть сервером, в пределах Вашей организации, или сервер Вашего провайдера (ISP), чтобы сообщения маршрутизировались из локального интернет домена. Часто тот же самый сервер действует как Firewall, через который Ваша организация направляет все сообщения в интернет. Это может быть Domino сервер или другой тип сервера - например, сервер UNIX SendMail.

Настройка Relay Host.

*1845 Удостоверитесь, что Вы уже имеете Configuration Settings документ для сервера(ов), чтобы сконфигурировать его.

*1846 Откройте его для редактирования, на закладке Router/SMTP – Basics.

*1847 Заполните поле и затем сохраните и закройте документ:

Поле	**Значение**
Relay host for messages leaving the local Internet domain	Имя хоста или имя домена для передачи сообщений через него в интернет

*1848 После того, как Вы настроили Relay Host, Вы можете настроить и ограничения для некоторых серверов.

4.3.8 Настройка передачи сообщений с использованием Dial-Up connection.

Вы можете определить, как передавать сообщения с серверов Вашей организации, на удаленный сервер (часто ISP), с использованием Dial-Up. По умолчанию, когда сервер связывается с другим сервером, он выталкивает сообщения на этот сервер. Сервер инициатор не может забирать (Pull), накапливаемые для него сообщения с другого сервера. Вместо этого сервер ждет, пока другой сервер не установит связь и маршрутизирует сообщения для него. Чтобы изменить это поведение сервера по умолчанию и затребовать сообщения с другого сервера, Вы можете настроить сервер инициатор, чтобы послать запрос типа Pull Request другому серверу.

Когда сервер инициатор - сконфигурирован посылать запрос Pull Request, он посылает запрос серверу, на котором временно хранятся сообщения для сервера инициатора. Как правило это почтовый сервер Вашего провайдера. Сервер провайдера получив запрос Pull Request, доставляет любые сообщения, которые ожидают доставки, на сервер инициатор.

Если Вы используете SMTP, Вы должны удостовериться, что ETRN расширение протокола поддерживается и разрешено на сервере, получающим запрос Pull Request, в противном случае он не будет способен получить запрос Pull Request. Этот режим доставки сообщений в интернет требует, чтобы сервер источник использовал статический адрес IP и адрес должен быть прописан в записях DNS.

Обратите внимание, Если удаленная система провайдера назначает новый IP адрес, каждый раз, когда Вы соединяетесь с ней, Вы не должны использовать значение – Pull.

Вы можете указывать, продолжительность нахождения на линии сервера при соединении. Это функция предотвращает “бросание” трубки сервером прежде, чем удаленный сервер попытается передать почту, для Вашего сервера. Сервер инициатор посылает запрос Pull Request, а затем выталкивает любые сообщения, которые он имеет для удаленного сервера, затем ждет сообщения, которые находится на удаленном сервере.

Когда сервер инициатор посылает запрос Pull Request, сервер может также запрашивать сообщения для других серверов, доменов, хостов, или любого имени очереди, в пределах Вашей организации, для которых сервер инициатор является домашним.

Если удаленный сервер - Domino сервер, Вы можете сконфигурировать его, чтобы он хранил любую почту для сервера инициатора, пока это он не получит запрос Pull Request от сервера инициатора. Это предотвращает удаленный сервер от попыток передать почту на сервер инициатор, когда он не связан с сетью. Он будет ждать запрос Push Wait Router.

Для определения опций обработки сообщений.

*1849 Удостоверитесь, что Вы уже создали документ Notes Direct Dial-Up Connection

*1850 Из клиента Domino Administrator, выбирайте закладку Настройка, затем откройте секцию - Почта – Подключения.

*1851 Откройте нужный документ подключения в режиме редактирования и перейдите на закладку Routing and Replication, заполните нужные поля и затем сохраните и закройте документ:

Поле	**Значение**

Router type	Выбирайте одно: *1852 Push/Wait – выбирайте эту опцию, чтобы Ваш сервер ждал от другого сервера запрос Pull Request, для передачи почты на этот сервер. *1853 Push Only (по умолчанию) - выбирайте эту функцию, если Ваш сервер должен соединится с сервером назначения и передавать на него почту. *1854 Pull Push - опция для соединения с сервером назначения, передачи на него почты и передачи запроса Pull Request на сервер, для того, чтобы сервер назначения, передал почту на сервер инициатор. *1855 Pull Only - опция, только для передачи на сервер назначения команды запроса Pull Request и принятия ожидаемой для сервера инициатора.
Pull routing request protocol	Выбирайте одно: *1856 Notes RPC - использовать Notes маршрутизацию для посылки запроса Pull Request. *1857 SMTP - использовать SMTP маршрутизацию для посылки запроса Pull Request. **Примечание.** Выбранный протокол не применяется, если удаленный сервер, является Domino сервер и тип маршрутизации – Pull Push. В этом случае, Pull Request посылается с использованием протокола используемого для передачи сообщений на сервер назначения.
Request the following when issuing a Pull Request	Выбирайте: *1858 Имя сервера источника (Notes и DNS host name по умолчанию), указание сервера инициатора (для примера, CN=Server/Org=ACME и server1.acme.com). *1859 All local primary Internet domains – перечисленные в документе Global Domain (Ваш интернет домен, для примера acme.com). *1860 All local alternate Internet domains - перечисленные в документе Global domain. *1861 The following servers/domains/hosts - чтобы запросить сообщения для этих серверов. Внесите в список определенные сервера, домены или хосты на чье имя сделан запрос Pull Request. Это может быть полезно, если удаленный сервер требует определенного синтаксиса, или имени определенного сервера для ETRN Pull Request, для инициализации передачи сообщения.

Pull router timeout	Число секунд, которое сервер инициатор ждет ответа сервера назначения, чтобы ответить на запрос Pull Request перед разрывом соединения. По умолчанию - 30 секунд.

4.4 Настройка почтовой системы Domino.

Эта глава объясняет, как настроить Вашу систему Domino после того, как Вы установили маршрутизацию почты.

4.4.1 Настройка почты.

После того, как Вы установили базовую маршрутизацию почты, Вы можете настраивать Вашу почтовую систему Domino, чтобы улучшить производительность почтовой системы. Например, Вы можете установить ограничения на нежелательную коммерческую почту (UCE), которая поступает в Вашу систему. Вы можете ограничить размер сообщения и, или использовать квоты для баз данных, чтобы вынуждать пользователей быстро удаляют старые сообщения. Вы можете определить политику безопасности, ограничивая возможность посылки электронной почты в интернет или шифровать все сообщения, доставленные на сервер.

Прежде, чем Вы настроите Вашу почтовую систему, Вы должны:

*1862 Удостоверится, что Ваша система почты должным образом установлена.

*1863 Оценить Ваши настройки, и решите, что Вы хотите осуществить.

4.4.2 Требование для работы почтовой системы.

Удостоверитесь, что Ваша система Domino работает должным образом:

*1864 Установленный Domino сервер, работает без ошибок.

*1865 Задача Router запущенна и работает должным образом.

*1866 Созданы файлы почты для каждого пользователя и Person документы, в Domino Directory для каждого пользователя Domino.

*1867 Настройте Notes и, или SMTP маршрутизацию почты.

Требование к маршрутизации SMTP почты

*1868 Установите DNS, локальные HOSTS файлы или Relay Host.

*1869 Разрешите задачу SMTP Lister.

*1870 Разрешите маршрутизацию SMTP, в пределах локального интернет домена.

*1871 Разрешите маршрутизацию SMTP, для посылки сообщения за пределы Вашего локального интернет домена.

Требование к маршрутизации Notes почты

*1872 Создайте нужные документы подключений.

В зависимости от топологии Вашей почтовой системы, создайте эти документы, по мере необходимости:

*1873 Документы Non-Adjacent Domain.

*1874 Документы Adjacent Domain.

*1875 Документы Foreign SMTP domain.

*1876 Документы SMTP Connection.

Требования для обмена почтой с другими системами в Вашей организации

*1877 Если Вы имеете некоторых пользователей, которые используют Lotus cc:Mail, Вы нуждаетесь, по крайней мере, в одном сервере, с установленным на нем агентом MTA cc:Mail, чтобы соединить Вашу Domino систему, с cc:Mail системой.

*1878 Если Вы имеете некоторых пользователей, которые используют X.400 почтовую систему, Вы нуждаетесь, по крайней мере, в одном сервере, с агентом X.400 MTA, чтобы соединить Вашу Domino системой с X.400.

*1879 Установите Smart Host.

4.4.3 Настройка системы передачи сообщений

После того, как Вы создаете базовую маршрутизацию почты, Вы можете изменить или подстроить любую из этих настроек:

*1880 Улучшить производительность Вашей системы

*1881 Настройка Notes маршрутизации

*1882 Контроль передачи сообщений

*1883 Ограничения для входящих сообщений

*1884 Ограничения для исходящих сообщений

*1885 Конфигурирование опций доставки сообщений

Кроме того, при настройке Вашей почтовой системы, Вы можете столкнуться с некоторыми проблемами. Процедуры, описанные ниже, помогут Вам в поиске неисправностей:

*1886 Запись дополнительной информации относительно Вашей почтовой системы в файл LOG.NSF.

*1887 Временное запрещение маршрутизации почты.

4.4.3.1 Оптимизация настроек Вашей почтовой системы.

4.4.3.1.1 Создать несколько баз данных MAIL.BOX.

Каждый Domino сервер, использует базу MAIL.BOX, для временного хранения сообщений. Пользователи и сервера используют SMTP или Notes протоколы, чтобы заносить сообщения в базу данных MAIL.BOX, для временного хранения. Router на сервере читает

сообщения и доставляет их в почтовые файлы пользователей на этом сервере, или перемещает их в MAIL.BOX на другие сервера.

В предыдущих версиях Domino, Router использовал только одну базу данных MAIL.BOX. В R5 Вы можете продолжать использовать единственную базу данных MAIL.BOX. Вы можете заметно увеличить производительность, для этого создайте несколько баз данных MAIL.BOX. Любой процесс, пробующий записать данные в MAIL.BOX, включая сервер и Router, нуждается в монопольном доступе к этой базе данных. Кроме того, когда Router читает новые сообщения из MAIL.BOX, другие процессы должны ждать, пока база не освободится. Когда у Вас имеется большое количество почты, с тяжелым почтовым трафиком - много время уходит на этот процесс.

При использовании нескольких баз данных MAIL.BOX, Domino использует несколько параллельных процессов. При чтении одного MAIL.BOX, Router помечает эту базу данных признаком - В использовании, так что другие сервера, пробующие занести почту, переходят к следующей базе данных MAIL.BOX. Такой подход значительно улучшает производительность почтовой системы.

При многократной записи в базы данных нередко возникают проблемы с MAIL.BOX, поэтому Вы должны помещать базы MAIL.BOX и почтовые файлы пользователей на различных дисках.

Если Вы добавляете только одну дополнительную базу данных MAIL.BOX, Вы почувствуете увеличение производительности Вашей почтовой системы. Вы получаете дополнительную выгоду от применения каждой дополнительной базы данных MAIL.BOX, хотя общая производительность компьютера уменьшается с каждым дополнительным почтовым ящиком MAIL.BOX.

Примечание. Вы определяет число MAIL.BOX баз данных в документе Configuration Settings. Если Вы используете одну конфигурацию для нескольких серверов, Domino создает число почтовых ящиков установленное в этом документе на каждом сервере.

Для создания нескольких баз данных MAIL.BOX сделайте следующее:

*1888 Удостоверитесь, что Вы уже имеете документ Configuration Settings для сервера(ов).

*1889 Из клиента Domino Administrator, выбирайте закладку – Настройка, откройте секцию - Почта.

*1890 Выбирайте представление – Конфигурации.

*1891 Выбирайте документ Configuration Settings, для почтового сервера или серверов, которым Вы хотите ограничить почту и выбирайте – Edit Configuration.

*1892 Выбирайте закладку Router/SMTP – Basics.

*1893 Заполните это поле и затем сохраните документ:

Поле	**Значение**
Number of mailboxes	Число от 1 до 10, чтобы установить число почтовых ящиков для каждого сервера, который использует этот документ конфигурации. По умолчанию - 1

4.4.3.1.2 Запрещение автоматического поиска адреса, основанного на вводе нескольких символов адреса.

Адресация типа Type-ahead ищет имена, которые соответствуют, введенным буквам в полях - To, Cc и Bcc. Например, если Вы введете Джейн Д в поле To, для адресации почты, Domino находит документ пользователя Джейн Доe/Акм в Domino Directory. Domino автоматически заканчивает остальную часть адреса получателя за Вас. Вы можете изменять или повторно вводить адрес, если это необходимо. Чтобы сэкономить время, Domino разрешает этот тип адресации по умолчанию.

Чтобы увеличить производительность сервера, Вы можете запретить эту функцию адресации. Если Вы запрещаете Type-ahead адресацию на почтовом сервере, пользователи все еще используют опцию Type-ahead, чтобы найти адреса в своих персональных адресных книгах, или в Domino Catalog.

Откройте документ Configuration Settings, на закладке Basics, измените значение поля, если это необходимо, затем сохраните и закройте документ:

Поле	**Значение**
Type-ahead	Выбирайте одно: *1894 Enabled – разрешение автоматической подстановки адресата в поля To, Cc или Bcc. *1895 Disabled – запрещение функции. Пользователи все еще могут использовать эту функцию, используя персональные адресные книги или Directory Catalog.

4.4.4 Запись дополнительной информации относительно передачи почты в файл LOG.NSF

По умолчанию, Domino записывает в файл LOG.NSF неудачные попытки доставки почтовых сообщений. Когда у Вас возникают проблемы с почтовой системой, Вы можете делать дополнительные записи в файле LOG.NSF.

Откройте документ Configuration Settings, для почтового сервера или серверов, для которого Вы хотите изменить уровень протоколирования. Переведите документ в режим редактирования. Перейдите на закладку Router/SMTP – Advanced – Controls. Измените значение поле в секции Miscellaneous Controls и сохраните документ:

Поле	**Значение**

Logging level	Выбирайте одно: *1896 Minimal – Запись сообщений только о фатальных ошибках почты. *1897 Normal - (по умолчанию) Регистрируются все сообщения предупреждений, которые указывают на состояние системы. *1898 Informational – Регистрируются все информационные сообщения доступа к файлу MAIL.BOX, обработки сообщений. Регистрируются события конвертирования сообщений и статуса доставки. *1899 Verbose – Наиболее полное протоколирование событий почтовой системы. Этот режим может помочь Вам при решении проблем с Вашей почтовой системы. **Примечание.** Выбирайте установку Verbose, только если Вы решаете проблемы с Вашей почтовой системой, иначе файл протокола может сильно увеличится в размерах.

4.4.5 Временное запрещение маршрутизации почты.

Вы можете временно запретить маршрутизацию почты на сервере, для устранения проблем с почтой.

Остановка задачи Router с консоли сервера.

Введите эту команду на консоли сервера:

```
tell router quit
```

Этой командой Вы остановите Router на сервере. Почта будет накапливается в MAIL.BOX, так как другие сервера и клиенты будут продолжать заносить почтовые сообщения базу данных MAIL.BOX, но Router не будет их доставлять.

Чтобы запустить Router, введите в эту команду на консоли сервера:

```
load router
```

Задача Router начинает работать и начинает доставлять почту.

Запрещение задачи Router из файла NOTES.INI.

Чтобы запретить загрузку задачи Router при старте сервера, удалите запись Router из переменной ServerTasks файла NOTES.INI.

*1900 Остановите сервер

*1901 Отредактируйте NOTES.INI, чтобы удалить задачу Router, из строки ServerTasks.

*1902 Повторно запустите сервер, чтобы изменения вступили в силу.

Когда Вы повторно запускаете сервер Router, задача не запускается.

4.4.6 Настройка маршрутизации Notes почты.

Чтобы настроить маршрутизацию Notes почты в Вашей организации, Вы можете:

*1903 Составить расписание маршрутизации для оптимизации эффективности системы

*1904 Измените стоимость маршрутизации подключений между Domino серверами

*1905 Маршрутизируйте сообщений согласно приоритетам

4.4.6.1 Расписание маршрутизации почты Notes.

Notes маршрутизация, использует расписание для доставки почты, основанное на документах подключения в Domino Directory. Вы можете настраивать документы подключения, чтобы управлять маршрутизацией Domino, для отправки Notes почты. Вы можете также использовать команду Route на консоли сервера, чтобы вынудить сервер маршрутизировать почту на другой сервер.

Для установки расписания маршрутизации Notes почты.

*1906 Удостоверитесь, что Вы уже создавали необходимые документы подключений.

*1907 Из клиента Domino Administrator, выбирайте закладку – Настройка и откройте секцию – Почта.

*1908 Выбирайте представление – Подключения.

*1909 Выбирайте документ подключения для связи сервера, которой Вы хотите сконфигурировать и выбирайте – Изменить подключение.

*1910 Перейдите на закладку – Schedule.

*1911 Заполните эти поля в секции Scheduled Connection:

Поле	**Значение**
Schedule	Выбирайте одно из значений: *1912 Enabled – для разрешения использования подключения для сервера. *1913 Disabled – игнорирование расписания сервером.
Call at times	Интервал времени для передачи почты Пример, 8:00 AM - 5:00 PM, 11:00 PM, 2:00 AM. По умолчанию 8:00 AM - 10:00 PM.
Repeat interval	Интервал повторения По умолчанию 360 минут.
Days of week	Дни недели для расписания передачи почты

*1914 Выбирайте закладку Replication/Routing.

*1915 Заполните поля секции Routing и сохраните документ:

Поле	Значение
Routing task	Выбирайте одно из значений: *1916 Mail Routing (по умолчанию) – разрешение маршрутизации Notes почты между серверами *1917 X400 Mail Routing – разрешение маршрутизации почты между серверами по X.400, использованием X.400 Message Transfer Agent *1918 SMTP Mail Routing – разрешить серверам версии R4 маршрутизировать почту в интернет *1919 cc:Mail Routing – разрешение маршрутизации сообщений между серверами с использованием cc:Mail Message Transfer Agent *1920 None – запрещается любая маршрутизация между серверами
Route at once	Минимальное число сообщений для передачи, при нормальном приоритете. По умолчанию - 5.
Routing cost	Относительная стоимость этой связи сервера. Изменяйте это значение, если Вы опытный Domino администратор.
Router type	Тип Domino маршрутизации между серверами.

Обратите внимание, что высокий приоритет для SMTP маршрутизирует сообщения немедленно. Маршрутизация сообщений низкого приоритета, происходит только в течение низкоприоритетного интервала маршрутизации. Сообщения для получателя на сервере, в той же самой поименованной сети Notes, сервер маршрутизирует немедленно, независимо от приоритета сообщения.

4.4.6.2 Изменение стоимости маршрутизации подключений между Domino серверами.

Маршрутизация Notes назначает стоимость направления на каждую связь и использует эти данные, чтобы выбрать наиболее эффективный путь, при маршруте почте от одного сервера к другому. Router вычисляет и хранит информацию относительно этих затрат, в таблицах маршрутизации. Если имеются больше чем один возможный маршрут для передачи почты между сервером источником и сервером назначения, Router просматривает информацию в таблицах маршрутизации, чтобы вычислить маршрут наименьшей стоимости, для передачи сообщений.

Router использует информацию из документов домена сервера и документов подключений, чтобы создать таблицы маршрутизации. Имеется приоритет для разных видов связи. Связь по сети LAN имеет цену ниже, чем Duial-Up соединение с использованием модема. По умолчанию, каждая связь по LAN имеет стоимость равную - 1, в то время как каждое соединение Dial-Up (модемное соединение) имеет стоимость равную - 5.

Если связь между серверами прерывается, или сетевое соединение не удается, Router выбирает альтернативный путь и увеличивает стоимость этого соединения пути на – 1 (единицу).

Как Router выбирает маршрут.

*1921 Router вычисляет и выбирает маршрут с наименьшей стоимости маршрута.

*1922 Если маршрут с наименьшей стоимостью маршрута терпит неудачу, например, если не имеется никакого ответа от сервера назначения, Router увеличивает стоимость начального маршрута на единицу. Например, если соединение по LAN между сервером A и сервером B первоначально имеет стоимость равную единице, но связь терпит неудачу, в течение предпринятой попытке, Router увеличивает стоимость этого соединения между сервером A и сервером B до двух.

*1923 Следующий раз, когда Router пробует передать почту между серверами, он снова определяет маршрут с наименьшей стоимости маршрута между серверами. Если имеется дополнительный маршрут, который является равным в стоимости, и требует меньшего количества Hops (перелетов), Router выбирает дополнительный маршрут. Например, если имеются два пути между сервером A и сервером B, каждый с общей стоимостью 4, Router исследует число Hops (перелетов) в каждом пути. Если один из маршрутов требует, три Hops (перелетов), а другой требует два Hops (перелета), Router использует путь, который требует только двух Hops (перелетов), так как затраты равны.

Router повторно устанавливает стоимость для связи когда:

*1924 Сервер получает запрос на связь при неудавшейся попытки

*1925 Происходит поиск динамического интервала стоимости

*1926 Вы останавливаете и повторно запускаете Router

Таблица маршрутов хранится в памяти динамически. Когда Вы повторно запускаете сервер или изменяете, документы подключений, сервера, конфигурации, или документы доменов, Router пересчитывает таблицу маршрутизации заново.

Для изменения установок по умолчанию.

Вы можете изменять установки по умолчанию, для стоимости маршрутов, только для связей между серверами в различных поименованных сетях Notes. Изменяйте стоимость по умолчанию только, если Вы - опытный Domino администратор. Ошибочные назначения изменение затрат, может создать петли маршрутизации, а Router не сможет выбирать дополнительные маршруты.

*1927 Удостоверитесь, что Вы уже создавали необходимые документы подключений.

*1928 Выбирайте нужный документ подключения, откройте его для редактирования.

*1929 Выбирайте закладку – Replication/Routing.

*1930 Заполните это поле и сохраните документ:

Поле	**Значение**

Routing cost	Число от 1 до 10. По умолчанию - 1. Router выбирает связи с более низкой стоимостью сначала. **Например.** Router выбирает связь со стоимостью – 2, а затем со стоимостью - 3.

4.4.6.3 Маршрутизация сообщений согласно приоритета.

Пользователи Notes могут выбирать приоритет доставки сообщения. Для этого нужно щелкнуть на кнопке Delivery Options, из клиента Notes и определить приоритет - высокий, нормальный или низкий. Уровень приоритетов определяет, как быстро Domino маршрутизирует сообщение. Если Вы не определяете приоритет для сообщения, сервер определяет сообщение, как сообщение нормального приоритета - по умолчанию.

Уровень Приоритета	**Маршрутизация Notes по умолчанию**
High	Сервер доставляет сообщение немедленно.
Normal	Сервер доставляет сообщение в ближайшее время, определенное расписанием передачи почты между серверами.
Low	Сервер доставляет сообщение ночью, согласно расписанию с низким приоритетом (с 12 ночи по 6 утра).

Примечание. Вы может заставлять Domino игнорировать приоритет сообщения. Сообщения для получателя на сервере в той же самом поименованной сети Notes, сервер маршрутизирует немедленно, независимо от приоритета сообщения.

4.4.7 Контроль передачи сообщений.

Чтобы управлять способом передачи сообщений между серверами в Вашей Domino системе, Вы можете:

*1931 Ограничивать передачу сообщений по размеру сообщения.

*1932 Маршрутизировать сообщения большого размера, в течение низкоприоритетного диапазон времени.

*1933 Настроить средство управления передачи - например, изменить число передачи и интервала повторения попыток.

*1934 Настраивать дополнительные средства управления - например, изменить уровень протоколирования, или когда можно игнорировать приоритет сообщения.

*1935 Настроить текст сообщения в случае неудачной попытки.

4.4.7.1 Ограничения размера почтовых сообщений пользователей.

Чтобы ограничить размер сообщения и определять, как Domino будет обрабатывать большие сообщения, Вы можете настраивать поведение Router. Вы можете заставить Router отклонять сообщения, которые окажутся большими, чем некоторый размер, или определять большие сообщения - как низкоприоритетные. Такие сообщения будут маршрутизироваться во время, определенное для сообщений низкого приоритета. После отклонения сообщения большого размера, Domino возвращает сообщение с отказом доставки отправителю. Ограничения размера сообщения относятся и к MIME, и к сообщениям формата Notes, и к SMTP и Notes маршрутизации.

Определить ограничения вы можете в документе Configuration Settings для сервера(ов) из Domino Directory.

*1936 Откройте нужный документ Configuration Settings для редактирования. Выбирайте закладку – Router/SMTP – Restrictions and Controls – Restrictions.

*1937 Заполните поля на закладке Router Restrictions, которые хотите использовать, сохраните и закройте документ:

Поле	**Значение**
Maximum message size	Максимальный размер сообщения в КБ, которые сервер может принимает. Router отклоняет любые сообщения, которые превышают этот размер. По умолчанию - 0KB, нет ограничения на размер сообщения.
Send all messages as low priority if message size is between	Выбирайте одно: *1938 Enabled *1939 Disabled (по умолчанию) **Примечание.** Если Вы, разрешаете эту функцию, все сообщения больше определенного вами размера в КБ - доставляется в низко приоритетное время. По умолчанию - 0KB, не устанавливать никаких изменений приоритетов доставки.

4.4.7.2 Настройка контроля передачи сообщений.

Transfer controls затрагивает передачу сообщений между серверами. Они управляют числом используемых нитей, числом позволенных Hops (перелетов) прежде, чем сообщение терпит неудачу, интервалов чистки и временем TimeOut.

Определить ограничения вы можете в документе Configuration Settings, для сервера(ов) из Domino Directory.

*1940 Откройте нужный документ Configuration Settings для редактирования. Выбирайте закладку – Router/SMTP – Restrictions and Controls – Transfer Control.

*1941 Заполните эти поля на закладке Transfer Controls и затем сохраните документ:

Поле	**Значение**
Maximum transfer threads	Максимальное значение нитей сервера, которое Domino создает, для передачи сообщений на другие сервера.
Maximum concurrent transfer threads	Максимальное число параллельных нитей, которые Domino создает для перемещения сообщений отдельным серверам назначения. По умолчанию – половина максимального числа нитей передачи. Например, если максимальное количество нитей передачи - 5, максимальное число параллельных нитей по умолчанию - 2.
Maximum hop count	Максимальное число времени, для передачи сообщений между серверами, по истечению, которого и Domino посылает сообщение о недоставке.
Low priority mail routing time range	Диапазон времени для передачи почты с низким приоритетом По умолчанию с 12 AM до 6 AM.
Initial transfer retry interval	Временной интервал между попытками, передачи почты. По умолчанию 15 минут.
Expired message purge interval	Частота (в минутах) проверки истечения сообщений, чтобы производит чистку. По умолчанию - 15 минут.

Обратите внимание, что Router устанавливает максимального число нитей передачи по умолчанию, основываясь на памяти сервера. Router выбирает максимальное число обычно лучше всего. Если Вы устанавливаете максимальный число вручную, Lotus рекомендует устанавливать максимум между одной нитью и 25 нитями, согласно загрузки сервера.

4.4.7.3 Настройка дополнительных параметров передачи сообщений.

Удостоверитесь, что Вы уже создали документ Configuration Settings для сервера(ов).

*1942 Из клиента Domino Administrator, выбирайте закладку Настройка и открывайте секцию – Почта.

*1943 Выбирайте – Конфигурации.

*1944 Выбирайте документ Configuration Settings, для почтового сервера или серверов, которым Вы хотите редактировать.

*1945 Выбирайте закладку Router/SMTP – Advanced – Controls.

*1946 Заполните эти поля в секции Advanced Transfer Controls:

Поле	**Значение**
Ignore message priority	Выбирайте одно: *1947 Enabled - чтобы установить все приоритеты сообщения в нормальный приоритет, независимо от первоначального приоритета, назначенного отправителем. *1948 Disabled - (по умолчанию), чтобы не изменять приоритеты сообщения, оставляя их первоначальный, назначенный отправителем.
Dynamic cost reset interval	Число минут, после которого Router наращивает стоимость соединения, при неудачной попытке. Например, если значение интервала - 15 минут, Router увеличивать стоимость связи с 1 до 2, после истечения этого периода. Router повторно увеличивает стоимость на 1 после каждых 15 минут, неудачного соединения.

Заполните следующие поля в секции Additional Controls section и сохраните документ:

Поле	**Значение**
Restrict name lookups to primary directory only	Выбирайте одно: *1949 Enabled - позволить пользователям посматривать имена групп и пользователей только в Domino Directory для Notes домена серверов. Если Вы выбираете этот выбор, пользователи не могут осуществлять поиск имен групп и пользователей в Directories, которые являются доступными через Directory Assistance. *1950 Disabled - (по умолчанию), позволить пользователям, просматривать имена групп и пользователей в любом Directories, доступном на сервер.

Cluster failover	Выбирайте одно: *1951 Disabled - не позволять Router обнаруживать другой сервер кластера, если сервер назначения недоступен. Эта функция запрещает Router направлять почту на другой сервер в кластере. *1952 Enabled - (по умолчанию), чтобы позволять Router определять неисправность сервера назначения, для последующего перехода на другой сервер кластера. Это установка позволяет Router обнаруживать, что почтовый сервер получателя в прошлый раз при передаче почты был недоступен, и затем пытаться определять другой почтовый сервер кластера, для передачи сообщения этому серверу. Если Router находит другой сервер кластера, он передает сообщение этому серверу. Если сервер член кластера серверов, и имеется реплику почтового файла получателя, Router доставляет сообщение в эту базу. **Пример**. Server1/Acme маршрутизирует сообщение, адресованное Джейн Доe/Acme, чей файл почты находится на Server3/Acme. Server1 будет не в состоянии соединяться с Server3, который является недоступным. Server1 проверяет Domino Directory, чтобы определить, имеется ли любой другой сервер в кластере с Server3. Server2/Acme - находится в кластере с Server3, так что Router с Server1 пытается соединяться с Server2. Если связь успешна, Router передает сообщение на Server2.
Hold undeliverable mail	*1953 Enabled – при задержке почты в MAIL.BOX, не генерировать сообщения о недоставке. *1954 Disabled - (по умолчанию) генерировать сообщение Non-Delivery Report.

Задержка не доставленной почты в базе данных MAIL.BOX.

Когда Router не может доставить сообщение, например, когда адрес введен неправильно, он доставляет сообщение о недоставке отправителю. Вы можете заставлять Router задерживать эти не доставленные сообщения в базе данных MAIL.BOX, как поврежденные сообщения. Вы можете просматривать эти сообщения, определять какое действие с ними предпринять. Если Вы выбираете опцию хранения не доставленных сообщений в MAIL.BOX, проверяйте MAIL.BOX базу данных, на наличие таких сообщений. MAIL.BOX также содержит мертвые сообщения, которые Router неспособен доставить, или для которых Router не мог доставить сообщение отказа отправителю, например, когда адрес получателя был введен неправильно, или сервер отправителя недоступен.

Проверка наличия не доставленной почты.

Из клиента Domino Administrator откройте базу данных MAIL.BOX. Проверьте сообщения, которые помечены в представлении как Мертвые.

Когда Вы находите не доставленное сообщение - Вы можете делать одну из трех вещей:

*1955 Исправьте адрес получателей сообщения

*1956 Отправить заново сообщения

*1957 Удалите сообщения

Кнопка Release в базе данных MAIL.BOX имеет несколько расширенных функций, которые будут Вам доступны из открывающегося меню, если Вы нажмете на правый край кнопки, помеченный треугольником. Исследуйте эти опции для работы с Вашими не доставленными сообщениями.

Когда Вы выполнили, обработали все, не доставленные сообщения, закрываете базу данных MAIL.BOX.

4.4.7.4 Настройка текстовых сообщений при сбое в доставки почты.

Вы можете настраивать текст сообщения, который Domino посылает, когда происходят различные неудачные попытки доставки почты. Текст, который Вы определяете, добавляется к тексту по умолчанию к сообщению. Вы можете добавлять текст на разных языках или вводить текст, который дает пользователю дополнительную информацию. Например, если почтовый сервер использует процессы электронной торговли участка Web сети, добавьте текст, телефонные номера, для связи с Вашими клиентами, если почтовые сообщение не достигает Вашего сервера.

*1958 Из клиента Domino Administrator, выбирайте закладку – Настройка, откройте секцию – Почта.

*1959 Выбирайте – Конфигурации.

*1960 Выбирайте документ Configuration Settings для почтового сервера или серверов, которым Вы хотите редактировать.

*1961 Выбирайте закладку Router/SMTP – Advanced – Controls.

*1962 Заполните эти поля в секции Failure Messages, затем сохраните документ:

Поле	**Значение**
Transfer failure text file	Имя файла, содержащего сообщение о неудаче передачи сообщения Пример C:\DOMINO\DATA\TRANSFER.TXT. Отказы передачи почты происходят, когда имеется проблема или отказ связи между серверами.
Delivery failure text file	Имя файла, содержащего сообщение о недоставке сообщения Пример C:\DOMINO\DATA\DELIVER.TXT. Недоставка происходят, когда сервер неспособен, доставить сообщение в файл почты получателя, например, если почтовый файл получателя перемещен, а Domino Directory не был должным образом обновлен.

Message expiration text file	Имя файла, содержащего сообщение о недоставке сообщения в определенный Вами период времени Примера, C:\DOMINO\DATA\EXPIRE.TXT. Неудача передачи сообщения по истечении определенного времени. Происходит, когда Domino не может передать сообщение в данный период времени.
Domain failure text file	Название файла, содержащего сообщение отказа при передаче почты в домен Пример C:\DOMINO\DATA\DOMAIN.TXT. Отказ, неудача передачи почты в домен происходят, когда Domino не может идентифицировать домен назначение для получателя сообщения. Например, если Вы посылаете сообщение jdoe@lotus.com, но Domino не может определить домен lotus.com, или в Domino Directory или на DNS сервере, сервер не может найти имя домена.
Server failure text file	Название файла, содержащее сообщение отказа при отказе сервера Пример, C:\DOMINO\DATA\SERVER.TXT. Отказы сервера происходят, когда Domino не может соединяться с сервером назначением. Например, если Вы посылаете сообщение jdoe@lotus.com и DNS сообщает, что Вы должны послать почту домена lotus.com на сервер mail1.lotus.com , НО Domino не можете соединяться с сервером mail1.lotus.com, Domino сервер генерирует сообщение отказа.
Username failure text file	Название файла, содержащего сообщение отказа при отказе по Имени пользователя Пример C:\DOMINO\DATA\USER.TXT. Отказы по имени пользователя происходят, когда Domino не может найти соответствий с адресом получателю. Например, если Вы посылаете сообщение jdoe@lotus.com, но Domino не может найти jdoe в Domino Directory, сервер возвращает сообщение отказа по имени пользователя.

Size failure text file	Название файла, содержащего сообщение отказа для отказов по размеру файла Пример C:\DOMINO\DATA\SIZE.TXT. Отказы по размеру файла происходят, когда Domino отклоняет сообщение, потому что размер сообщения больше чем максимальный размер сообщения, который Вы может определять в поле Maximum message size, на закладках Restrictions и Controls-Restrictions - ограничений для сервера, в документах Configuration Settings. В этом случае генерируется сообщение отказа передачи сообщения по размеру...
Restriction failure text file	Название файла, содержащего сообщение отказа, для отказов по ограничению Пример C:\DOMINO\DATA\RESTRICT.TXT. Отказы по ограничению происходят, когда Domino отклоняет сообщение, основанное на SMTP ограничениях. Например, если Вы посылаете сообщение jdoe@lotus.com, но lotus.com внесен в список в поле Deny messages from the following Internet addresses/domains, на закладке Router/SMTP-Restrictions и Controls-SMTP Inbound Controls, в документе Configuration Settings, Domino отклоняет сообщение и возвращает сообщение отказа по ограничению.

4.4.8 Ограничения маршрутизации входящей почты.

Вы можете настраивать Вашу Domino систему, чтобы управлять и ограничивать почту для входящих сообщений (inbound). Ограничение входящей маршрутизации почты, ограничивает Ваших пользователей и организация от ненужной Вам коммерческой почты (UCE) и уменьшает нагрузку на Вашу систему. Вы можете устанавливать следующие ограничения:

*1963 Проверьте и ограничьте входящие соединения

*1964 Настройте входящий Releу почты

*1965 Ограничьте маршрутизацию почты, основанную на Notes доменах организаций и орг. единицах

*1966 Проверите и ограничьте, кто может посылать электронную почту в интернет Вашим пользователям

*1967 Ограничьте, кто может получать электронную почту из интернет в Вашей организации

*1968 Проверьте набор расширенных SMTP функций для входящих сессий

Если Вы устанавливаете ограничение, которое заставляет Domino отклонять входящие сообщение, Domino посылает сообщение отказа отправителю. Это сообщение называет причину для отказа. Сообщения отказа содержат текст по умолчанию, который Вы можете настроить.

4.4.8.1 Ограничения для входящих SMTP соединений.

Некоторые пользователи и организации могут пытаться посылать Вам нежелательную почту. Чтобы предотвратить принятие нежелательной почты и ограничить Ваши сервера от перегрузок можно ограничить соединения с Вашей почтовой системой.

*1969 Удостоверитесь, что Вы уже имеете документ Configuration Settings для сервера, чтобы сконфигурировать его.

*1970 Из клиента Domino Administrator, выбирайте закладку и откройте секцию - Почта.

*1971 Выбирайте представление – Конфигурации.

*1972 Выбирайте документ Configuration Settings, для почтового сервера или серверов, которым Вы хотите ограничить почту, откройте его для редактирования.

*1973 Выбирайте закладку Router/SMTP – Restrictions and Controls – SMTP Inbound Controls.

*1974 Заполните нужные поля в секции Inbound Connection Controls, затем сохраните документ:

Поле	**Значение**
Verify connecting host name in DNS	Выдирайте одно из двух: *1975 Enabled - проверять имя соединяющегося хоста в DNS *1976 Disabled - (по умолчанию) не проверять Когда эта опция позволяется, Domino просматривает IP адрес соединяющегося хоста в DNS. Если адрес IP не соответствует имени хоста, Domino принимает связь, но не позволяет хосту передавать почту. Domino возвращает ошибку хосту инициатору, в процессе передачи команды MAIL FROM, SMTP протокола и не принимает никакую входящую почту.
Allow connections only from the following SMTP Internet host names/IP addresses	Имя хоста и или IP адреса серверов, которым позволяют соединиться с Вашим сервером и никакие кроме этих серверов. Если Вы вводите имена хостов и или IP адреса в этом поле, то только эти сервера, будут соединяться с Вашим сервером по SMTP. Запросы связи от всех других серверов будут отклонены. Например, Вы вводите Lotus.com, ibm.com в это поле. Domino принимает связи только от серверов в именах хоста которых, содержится Lotus.com или ibm.com домены. Domino отклоняет все другие запросы связи. **Примечание**. Вводите IP адреса в скобках, например [192.168.10.17]

Deny connections from the following SMTP Internet host names/IP addresses	Имена хостов и или IP адреса, которым не позволяется соединиться с Вашим сервером. Если Вы вводите имена хостов и или IP адреса в это поле, все сервера, кроме указанных в этом поле смогут соединяться с Вашим сервером по SMTP. Запросы связи будут отклонены только для серверов введенных в эти поля. Например, Вы вводите Lotus.com в поле. Domino принимает связи от всех серверов кроме тех, в домене которых имеется Lotus.com. Domino отвергает связи от серверов с именами хостов, заканчивающихся на Lotus.com. **Примечание**. Вводите IP адреса в скобках, например [192.168.10.17]

4.4.8.2 Настройка ограничения для Вашего сервера, при передаче почты через него (ограничение использования Relay).

Вы можете управлять, поступающими сообщениями от хостов, не Вашего локального интернет домена, принятых для получателей, не Вашего локального интернет домена. Установка ограничения запрещает попытки использовать Вашу почтовую систему как Reley сервер, чтобы экономить деньги или обеспечить анонимность. Посылая сообщение через Вашу систему, фактически предназначено для другой системы. Ваша система оказывается как последний хост инициатор передачи сообщения.

Вы можете запретить неправомочное использование Вашей системы, в качестве Reley-хоста, Router проверяет, является ли сервер, посылающий сообщение сервером локального интернет домена. Router проверяет поля Local primary Internet domain и Alternate Internet domain aliases, в документе Global Domain, чтобы определить имена интернет доменов, использующихся Вашей компанией. Если сообщение передается с сервера Вашей организации, Router проверяет имя каждого получателя, чтобы видеть, находится ли получатель в пределах локального интернет домена. Если нет, Domino использует ограничения, которые Вы можете сконфигурировать, чтобы определить Reley доступ.

Формат для ввода IP адресов - [a.b.c.d], где a, b, c, d - числа от 0 до 255 включительно. Вы можете включать звездочку (*) в Ваши записи, но они должно применяться для полной секции адреса - например, 192.168.17.*. Вводите IP адреса в скобках - например, [192.168.10.17]

Для ограничения Relay доступа.

*1977 Удостоверитесь, что Вы уже имеете документ Configuration Settings для сервера, чтобы сконфигурировать его.

*1978 Из клиента Domino Administrator, выбирайте закладку Почта.

*1979 Выбирайте представление Конфигурации.

*1980 Выбирайте документ Configuration Settings для почтового сервера или серверов, которым Вы хотите ограничить почту, откройте его для редактирования.

*1981 Выбирайте закладку Router/SMTP – Restrictions and Controls – SMTP Inbound Controls.

*1982 Заполните эти поля в секции Inbound Relay Controls, затем сохраните документ:

Поле	**Значение**
Allow messages from external Internet domains to be sent only to the following Internet domains	Только этим интернет доменам, разрешается использовать Вашу систему сообщений как Reley. Если Вы вводите в это поле домен, то только сообщения для этого домена, будет принято для передачи, через Вашу систему. Сообщения пользователей для другого внешнего интернет домена будут отклонены. **Например**, Вы вводите Lotus.com, ibm.com в это поле. Domino принимает только сообщения этих адресатов lotus.com или ibm.com доменов. Domino отвергает все другие сообщения для передачи в другие внешние домены.
Deny messages from external Internet domains to be sent to the following Internet domains	Интернет домены, для которых Ваша система не будет принимать сообщения. Если Вы вводите в это поле домен, все сообщения для этого домена не будут приниматься для передачи через Ваш хост. Сообщения будут отклонены только для получателей с этими адресами, соответствующими записям в этом поле. **Например**, Вы вводите Lotus.com в поле. Сообщения для всех получателей во всем внешнем интернете домене, кроме Lotus.com могут быть переданы через Вашу систему. Domino отвергает сообщения для получателей домена Lotus.com.
Allow messages only from the following external Internet hosts to be sent to external Internet domains	Имя хоста и или IP адрес, от которого разрешается Reley через Вашу систему, получателям с адресами вне локального интернет домена. Если Вы вводите имя хоста и или IP адрес в это поле, только сообщения от этих серверов могут использовать Reley через Вашу систему. Сообщения от других серверов будут отклонены. **Например**, Вы вводите Lotus.com, ibm.com в поле. Domino принимает только сообщения от серверов с именами хостов, заканчивающимися на Lotus.com или ibm.com. Domino отклоняет сообщения для этих получателей от всех других серверов.
Deny messages from the following external Internet hosts to be sent to external Internet domains	Имена хостов и или IP адресов, от которых Ваша система не будет принимать сообщения Reley, получателям вне локального интернет домена. Если Вы вводите имена хостов и или IP адрес в этом поле, то от всех серверов будет приниматься Reley, кроме этих соответствий, через Вашу систему. Сообщения будут отклонены только от серверов в этом поле. **Например**, Вы вводите Lotus.com в поле. Domino принимает сообщения получателям во внешние интернет домены от всех серверов кроме тех хостов, которые заканчиваются на Lotus.com. Domino отвергает эти сообщения от серверов домена Lotus.com.

Обратите внимание, если вы определяете тот же самый хост для разрешения в поле и, для запрещения в другом поле и, имеется конфликт между двумя полями, то установки запрещения имеет приоритет из соображений безопасности. Будьте осторожны в заполнении этих полей.

Примечание. Вы может использовать звездочку (*), чтобы указать значение - Все домены. Например, помещение (*) в поле разрешения, позволяет всем доменам исполнять это действие.

4.4.8.3 Ограничения базовой маршрутизации почты Notes доменов для организации и Орг. Единиц.

Вы можете использовать два метода ограничения маршрутизации почты и ограничение Notes маршрутизации в Вашей инфраструктуре.

Создайте документ Adjacent Domain в Domino Directory, чтобы запретить пользователям передачу почты через Ваш домен, в другой домен. Например, если Вы имеете документы подключения с Вашего домена Acme, на домен Lotus и домен IBM, Вы можете создать документ Adjacent Domain, чтобы запретить пользователям из домена Lotus, направлять почту в домен IBM, через Ваш домен Acme. Использование этих ограничений уменьшает нагрузку на Вашу систему. Документ Adjacent Domain запрещает пользователям использования Вашего домена в качестве Reley, для Notes почты.

Определите ограничения в документе Configuration Settings в Domino Directory, чтобы ограничить почту из указанного Notes домена.

Ограничение маршрутизации почты с использованием документа Configuration Settings.

*1983 Удостоверитесь, что Вы уже имеете документ Configuration Settings для сервера.

*1984 Из клиента Domino Administrator, выбирайте закладку - Почта.

*1985 Выбирайте представление – Конфигурации.

*1986 Выбирайте документ Configuration Settings, для почтового сервера или серверов, которым Вы хотите ограничить почту, откройте его для редактирования.

*1987 Выбирайте закладку Router/SMTP – Restrictions and Controls – Restrictions.

*1988 Заполните эти поля в секции Router Restrictions, затем сохраните документ:

Поле	**Значение**

Allow mail only from domains	Notes домены, от которых сервер будет принимать почту. Если Вы вводите в это поле Notes домены, то только сообщения от этих доменов могут быть переданы на Ваш домен с использованием Notes маршрутизации. Domino отвергает почту от всех других Notes доменов. **Например**, Вы вводите Lotus в поле. Domino принимает сообщения, только посланные от Lotus домена, для Ваших пользователей. Domino отвергает сообщения, посланные от всех других Notes доменов. **Обратите внимание**, что эти ограничения не затрагивает почту в локальном Notes домене.
Deny mail from domains	Notes домены, от которых сервер не будет принимать почту. Если Вы вводите в это поле Notes домены, сообщения от этих доменов не могут быть переданы на Ваш домен с использованием Notes маршрутизации. Domino принимает почту от всех других Notes доменов. **Например**, Вы вводите Lotus в поле. Domino не принимает сообщения, посланные из Lotus домена, для Ваших пользователей. Domino принимает сообщения, посланные от всех других Notes доменов. **Обратите внимание**, что это ограничение не затрагивает почту в локальном Notes домене.
Allow mail only from the following organizations and organizational units	Организации и или орг. единицы, от которых сервер принимает почту. Если Вы вводите в поле организации и или орг. единицы, только сообщения от пользователей в этих организациях и или орг. единицах могут передаваться в Ваш домен с использованием Notes маршрутизации. Domino отвергает почту от всех других организаций и или орг. единиц. **Например**, Вы вводите */East/Lotus в это поле. Domino принимает только сообщения от /East/Lotus орг. единицы, для Ваших пользователей. Domino отвергает сообщения от других организаций и или орг. единиц.
Deny mail only from the following organizations and organizational units	Организации и или орг. единицы, от которых сервер не будет принимать почту. Если Вы вводите в поле организацию и или орг. единицу, то сообщения от пользователей в этих организациях и или орг. единицах не смогут передавать почту в Ваш домен с использованием Notes маршрутизации. Domino принимает почту от всех других организаций и или орг. единиц. **Например**, Вы вводите */East/Lotus в это поле. Domino не будет принимать сообщения от /East/Lotus орг. единицы, для Ваших пользователей. Domino принимает сообщения от всех других организаций и или орг. единиц.

Примечание. Если Вы определяете ту же самую запись в поле разрешения и поле запрещения, и имеется конфликт между двумя полями, то отрицающая установка имеет приоритет, из соображений безопасности. Будьте осторожны, чтобы не иметь одинаковых значений в полях и запрещения и разрешения.

4.4.8.4 Ограничения по отправителям интернет почты, для Ваших пользователей.

Незапрашиваемая коммерческая электронная почта (UCE) часто засоряет Ваши сервера многочисленными копиями сообщений. Принятие ее существенно затрудняет работу сервера и потребляет ресурсы системы. Вы можете определить ограничения, для UCE для Вашего сервера. Определение ограничений оградит Вашу систему от ненужной почты UCE.

Чтобы экономить ресурсы Вашей системы, Domino проверяет поле получателя To: и поле автора From:. Если Вы заставляете Domino сервер отвергать некоторого отправителя, Domino отвергает его всякий раз, когда с ним сталкиваются. Например, если пользователи из отклоненного домена посылают почту через Reley, Domino отвергает передачу почты, основываясь на запрещении для этого домена. Domino создает запись в файле LOG.NSF всякий раз, когда сообщение было отклонено.

Чтобы ограничить получение почты интернет, для Ваших пользователей.

*1989 Удостоверитесь, что Вы уже имеете документ Configuration Settings для сервера, чтобы сконфигурировать его.

*1990 Из клиента Domino Administrator, выбирайте закладку Почта.

*1991 Выбирайте представление Конфигурации.

*1992 Выбирайте документ Configuration Settings, для почтового сервера или серверов, которым Вы хотите ограничить почту, откройте его для редактирования.

*1993 Выбирайте закладку Router/SMTP – Restrictions and Controls – SMTP Inbound Controls.

*1994 Заполните эти поля в секции Inbound Sender Controls и затем сохраните документ:

Поле	**Значение**
Verify sender's domain in DNS	Выбирайте одно: *1995 Enabled – чтобы проверять домен отправителя в DNS и убедится, что домен отправителя существует, перед отправкой почты. *1996 Disabled - (по умолчанию) не проверять.

Allow messages only from the following Internet addresses/domains	Интернет адреса, от которых сервер принимает сообщения. Если Вы вводите адреса в это поле, только сообщения от этого отправителя, могут посылать почту из интернета, пользователям в Вашем локальном интернет домене. Почта от всех других адресатов будет отклонена. **Например**, Вы вводите Lotus.com в это поле. Domino принимает только сообщения, посланные от пользователей, чей адрес заканчивается в Lotus.com. Domino отвергает сообщения от всех других адресатов интернета.
Deny messages from the following Internet addresses/domains	интернет адреса, от которых сервер не будет принимать сообщения. Если Вы вводите адреса в это поле, только сообщения от этого отправителя, не могут посылать почту из интернета, пользователям в Вашем локальном интернет домене. Почта от всех других адресов будет приниматься. **Например**, Вы вводите Lotus.com в поле. Domino не принимает только эти сообщения, посланные от пользователей, чей адрес заканчивается на Lotus.com. Domino принимает сообщения от всех других адресов интернета.

4.4.8.5 Ограничение на то, кто может получать почту из интернета из Вашей Организации.

Ваша компания может вести политику, которая ограничивает служащих от получения сообщений из интернета. Вы можете управлять этой опцией, кто в Вашей организации может получать почту из интернета. Domino имеет два выбора: Вы можете указывать, какие пользователи могут получать почту интернет и запретить получение почты интернета для всех других пользователей. Вы можете указывать, какие пользователи не могут получать почту интернет, и позволять использовать почту интернет для всех других пользователей.

Обратите внимание на то, что Вы можете неумышленно блокировать нужную почту, будьте осторожными, когда Вы используете эти поля.

*1997 Удостоверитесь, что Вы уже имеете документ Configuration Settings для сервера, чтобы сконфигурировать его.

*1998 Из клиента Domino Administrator, выбирайте закладку Почта.

*1999 Выбирайте представление Конфигурации.

*2000 Выбирайте документ Configuration Settings, для почтового сервера или серверов, которым Вы хотите ограничить почту, откройте его для редактирования.

*2001 Выбирайте закладку Router/SMTP – Restrictions and Controls – SMTP Inbound Controls.

*2002 Заполните эти поля в секции Inbound Intended Recipients Controls и затем сохраните документ:

Поле	Значение
Allow messages intended only for the following Internet addresses	Адреса интернета, которые находятся в пределах локального интернет домена и им позволяется получить почту из интернета. Если Вы вводите адреса в это поле, то только эти получатели могут получать почту интернета. Domino отвергает почту для всех других получателей.
Deny messages intended for the following Internet addresses	Интернет адреса в пределах локального интернет домена, которым запрещено получение почты из интернета. Если Вы вводите в это поле адреса, все получатели, кроме тех, кого вы внесли в список в этом поле, могут получать почту интернета. Domino отвергает почту только для получателей, перечисленных в этом поле.

4.4.8.6 Поддержка расширений SMTP для входящих сессий.

Domino поддерживает множество расширений SMTP (ESMTP) функций. Они включают способность комбинировать, объединять команды, заставляя сервер проверять размер сообщений перед их принятием / передачей, создавать безопасную SSL связь с другим сервером и создавать уведомления статуса доставки в формате MIME. Вы можете позволять или запрещаете любой из этих функций в документе Configuration Settings, для серверов, к которым Вы хотите использовать эти функции.

*2003 Удостоверитесь, что Вы уже имеете документ Configuration Settings для сервера, чтобы сконфигурировать его.

*2004 Из клиента Domino Administrator, выбирайте закладку - Почта.

*2005 Выбирайте представление Конфигурации.

*2006 Выбирайте документ Configuration Settings, для почтового сервера или серверов, которым Вы хотите ограничить почту, откройте его для редактирования.

*2007 Выбирайте закладку Router/SMTP – Advanced – Commands and Extensions.

*2008 Заполните эти поля в секции Inbound SMTP Commands and Extensions и затем сохраните документ:

Поле	Значение

SIZE extension	Выбирайте одно: *2009 Enabled - (по умолчанию) разрешение проверки входящих сообщений перед перемещением его на сервер. Эта опция гарантирует, что сообщение не превышает максимальный размер ограничения. Если сообщение больше чем максимальный размер, Domino не принимает сообщение. *2010 Disabled - не проверять входящие сообщения перед передачей их на Ваш сервер.
Pipelining extension	Выбирайте одно: *2011 Enabled - (по умолчанию) чтобы улучшить выполнение работ и разрешить посылку нескольких SMTP команд в одном пакете. *2012 Disabled - посылать SMTP команды в отдельных пакетах
DSN extension	Выбирайте одно: *2013 Enabled - посылать уведомление статуса доставки отправителю сообщения для SMTP сообщения, если отправитель запрашивает DSN *2014 Disabled - (по умолчанию) не посылать уведомление статуса доставки.
8-bit MIME extension	Выбирайте одно: *2015 Enabled – посылать Multi-National Characters, без Encoding *2016 Disabled - (по умолчанию) посылать Characters с Encoding
HELP command	Выбирайте одно: *2017 Enabled - (по умолчанию) разрешить команду – Help *2018 Disabled - запретить команду – Help
VRFY command	Выбирайте одно: *2019 Enabled - принимать входящие запросы для верификации имени пользователей *2020 Disabled - (по умолчанию) не принимать запросы для проверки имени пользователей
EXPN command	Выбирайте одно: *2021 Enabled – просматривать списки и группы, для отображения пользователей, входящих в них. *2022 Disabled - (по умолчанию) не просматривать списки и группы.
ETRN command	Выбирайте одно: *2023 Enabled – позволять серверу принимать входящие запросы Pull для вытягивания исходящих сообщений *2024 Disabled - (по умолчанию) не принимать входящие Pull запросы

SSL negotiated over TCP/IP port	Выбирайте одно: *2025 Enabled – позволять Domino надежно соединятся с другими серверами для организации шифрованного канала SSL, по TCP/IP порту, используемого двумя серверами *2026 Disabled - (по умолчанию) не позволять secure SSL соединения

Примечание. Предоставление возможности VRFY и EXPN позволяет людям не Вашей организации легко получить доступ к именам групп и проверять адреса электронной почты в Вашей организации. Вы не разрешаете эти расширения из соображений безопасности.

4.4.9 Ограничения для исходящих сообщений сервера.

Вы можете управлять исходящими сообщениями Вашей системы, которые отправляются во внешние интернет домены. Вы можете ограничивать пользователей, кто может посылать эти сообщения или позволять использование расширений SMTP (ESMTP). Вы можете устанавливать эти ограничения:

*2027 Ограничивать, кто может посылать почту в интернет.

*2028 Определять набор исходящих SMTP расширений.

4.4.9.1 Ограничения на рассылку почты в интернет.

Ваша компания может придерживаться политики, которая ограничивает служащих от рассылки сообщений в интернет. Вы можете определять, кому в Вашей организации разрешать посылать почту в интернет. Domino имеет два выбора: Вы можете определить, кто из пользователей может посылать почту в интернет и запретить почту интернет для всех других пользователей. Вы можете определить, кто из пользователей не может посылать почту в интернет и позволяют почту интернет для всех других пользователей.

Обратите внимание, Вы можете неумышленно блокировать нужную почту, будьте осторожны, когда используете эти поля.

*2029 Удостоверитесь, что Вы уже имеете документ Configuration Settings, для сервера, чтобы сконфигурировать его.

*2030 Из клиента Domino Administrator, выбирайте закладку Почта.

*2031 Выбирайте представление Конфигурации.

*2032 Выбирайте документ Configuration Settings, для почтового сервера или серверов, которым Вы хотите ограничить почту, откройте его для редактирования.

*2033 Выбирайте закладку Router/SMTP – Restrictions and Controls – SMTP Outbound Controls.

*2034 Заполните эти поля и затем сохраните документ:

Поле	**Значение**

Allow messages only from the following Internet addresses to be sent to the Internet	Адреса интернета, которые находятся в локальном интернет домене и которым позволяют послать почту в интернет. Если Вы вводите адреса в это поле, то только эти получатели могут посылать почту в интернет. Domino отвергает почту от всех других пользователей.
Deny messages from the following Internet addresses to be sent to the Internet	Адреса интернета, которые находятся в локальном интернет домене, которым не позволяется посылать почту в интернет. Если Вы вводите адреса в эти поля, то только эти получатели не могут посылать почту в интернет. Domino позволяет передавать почту от всех других пользователей.
Allow messages only from the following Notes addresses to be sent to the Internet	Адреса Notes, которые находятся в локальном интернет домене, которым позволяется послать почту в интернет. Если Вы вводите адреса в это поле, то только эти пользователи могут посылать почту в интернет. Domino отвергает почту от всех других пользователей.
Deny messages from the following Notes addresses to be sent to the Internet	Адреса Notes, которые находятся в локальном интернет домене, которым не позволяется посылать почту в интернет. Если Вы вводите адреса в эти поля, то только этим пользователи не могут посылать почту в интернет. Domino позволяет передавать почту от всех других пользователей.

Примечание. Domino проверяет каждый адрес, чтобы определить, является ли этот адрес интернета или адрес Notes локальным, после чего Router применяет ограничения, указанные для этого типа адреса.

4.4.9.2 Поддержка исходящих SMTP расширений.

Domino поддерживает множество расширений SMTP (ESMTP) функций. Они включают способность комбинировать, объединять команды, заставляя сервер проверять размер сообщения перед отправкой - передачи, создавать безопасную SSL связь с другим сервером, или создавать уведомления статуса доставки в формате MIME. Вы позволяете или запрещаете любой из этого выбора из документа Configuration Settings, для сервера или серверов, для которого Вы хотите использовать эти расширения.

*2035 Удостоверитесь, что Вы уже имеете документ Configuration Settings для сервера, чтобы сконфигурировать его.

*2036 Из клиента Domino Administrator, выбирайте закладку - Почта.

*2037 Выбирайте представление Конфигурации.

*2038 Выбирайте документ Configuration Settings для почтового сервера или серверов, которым Вы хотите ограничить почту, откройте его для редактирования.

*2039 Выбирайте закладку Router/SMTP – Advanced – Commands and Extensions.

*2040 Заполните эти поля в секции Outbound SMTP Commands and Extensions, затем сохраните документ:

Поле	**Значение**

SIZE extension	Выбирайте одно: *2041 Enabled - (по умолчанию) разрешение проверки исходящих сообщений перед перемещением его с сервера, это гарантирует, что сообщение не превышает максимального ограничения размера. Если сообщение больше чем максимальный размер, Domino не отправляет сообщение. *2042 Disabled – не проверять исходящие сообщения перед передачей его с Вашего сервера.
Pipelining extension	Выбирайте одно: *2043 Enabled - (по умолчанию) чтобы улучшить выполнение работ и разрешить посылку нескольких SMTP команд в одном пакете. *2044 Disabled – посылать SMTP команды в отдельных пакетах
DSN extension	Выбирайте одно: *2045 Enabled - посылать уведомление статуса доставки отправителю сообщения для SMTP сообщения, если отправитель запрашивает DSN *2046 Disabled - (по умолчанию) не посылать уведомление статуса доставки.
8-bit MIME extension	Выбирайте одно: *2047 Enabled – посылать Multi-National Characters, без Encoding *2048 Disabled - (по умолчанию) посылать Characters", с Encoding

4.4.10 Конфигурирование опций доставки сообщений.

Вы можете управлять процессом доставки сообщений с Вашей системы Domino. Эта опция так же определяет шифрование сообщений, сколько нитей Router может использовать, чтобы доставить сообщения. Будет ли Router повиноваться квотам баз данных, и не будет доставлять почту пользователям, чьи файлы почты большие, чем позволенный размер. Вы можете сконфигурировать этот выбор доставки сообщения:

*2049 Настройте средство управления доставки сообщения

*2050 Ограничьте маршрутизацию почты, основанную на квотах баз данных

4.4.10.1 Настройка опций доставки сообщений.

Вы можете настраивать опции доставки для Domino серверов, включая сколько нитей, использует Router, для доставки сообщения, должны ли сообщения быть зашифрованы, и как долго сервер ждет запуска агента Pre-Delivery.

*2051 Удостоверитесь, что Вы уже имеете документ Configuration Settings для сервера.

*2052 Из клиента Domino Administrator, выбирайте закладку Почта.

*2053 Выбирайте представление Конфигурации.

*2054 Выбирайте документ Configuration Settings для почтового сервера или серверов, которым Вы хотите ограничить передачу почты, откройте его для редактирования.

*2055 Выбирайте закладку Router/SMTP – Restrictions and Controls – Delivery Controls.

*2056 Заполните эти поля в секции Delivery Controls, затем сохраните документ:

Поле	**Значение**
Maximum delivery threads	Максимальное число нитей, которое Domino может создавать для доставки почты в MAIL.BOX.
Encrypt all delivered mail	Выбирайте одно: *2057 Enabled – шифровать все сообщения. *2058 Disabled - (по умолчанию) шифровать сообщение, только если в установках пользователя установлена опция шифровать сообщения.
Pre-delivery agent timeout	Количество секунд, которое сервер ждет запуска агента Pre-Delivery, по умолчанию - 30 секунд.

Примечание. Router устанавливает число максимума по умолчанию нитей доставки, основываясь на памяти сервера. Если Вы устанавливаете максимальное число вручную, Lotus рекомендует установить максимум между 1 (одной) и 25 нитями, основываясь на загрузке сервера, опытным путем.

4.4.10.2 Ограничения маршрутизации почты базирующейся на квотах баз данных.

Чтобы сохранить ресурсы сервера установите предел размера или квоту баз данных, на почтовые файлы пользователей. Этой установкой Вы вынуждаете пользователей уменьшать размер файла. Сконфигурируйте Router, чтобы он не доставлял пользователям сообщения, чьи почтовые файлы большие, чем установлена квота. Будьте осторожное в использовании этой установки, потому что она вызывает отказ доставки сообщений, посланных таким пользователям, и пользователи не смогут получать важные для них сообщения.

Удостоверитесь, что Вы уже имеете Configuration Settings документ для сервера(ов).

*2059 Из клиента Domino Administrator, выбирайте закладку - Почта.

*2060 Выбирайте представление – Конфигурации.

*2061 Выбирайте документ Configuration Settings для почтового сервера или серверов, которым Вы хотите ограничить почту, откройте его для редактирования.

*2062 Выбирайте закладку Router/SMTP – Restrictions and Controls – Restrictions.

Заполните нужные поля в секции Router Restrictions, затем сохраните документ.

Поле	**Значение**
Obey database quotas during message delivery	Выбирайте одно: *2063 Enabled – чтобы вынудить Router повиноваться квотам баз данных и, не доставлять сообщения пользователям, чьи почтовые файлы больше чем предел размера квоты. *2064 Disabled - (по умолчанию) доставлять сообщения не обращая внимание на квоты баз данных. **Примечание.** Даже если Вы не позволяете этот выбор, пользователи, чьи почтовые файлы большие, чем квота баз данных, не могут создавать или сохранять новые почтовые сообщения. Использование квот, для баз данных, вынуждает пользователей уменьшать размер почтового файла

4.5 Использование Shared Mail.

База данных Shared Mail - экономит место на диске Вашего сервера Domino. База хранит единственную копию почтовых сообщений, которые адресованы нескольким получателям. Когда получатели, чьи почтовые файлы находятся на одном сервере, получают сообщение – сообщение сохраняется в базе данных Shared Mail, а почтовые файлы каждого получателя хранят заголовок сообщения. Использование базы данных Shared Mail полностью прозрачно для пользователей. Когда пользователь открывает сообщение, срабатывает связь между почтовым файлом и базой данных Shared Mail и сообщение появится в полном объеме. Пользователи могут удалять, отвечать, изменять сообщения, представление или папку, редактировать, сохранять, повторно посылать и выполнять все почтовые задачи. Каждый пользователь может редактировать, сохранять и повторно посылать сообщения, без воздействия на сообщения других пользователей.

Shared Mail использует с все почтовые файлы, расположенные на Вашем Domino сервере и не зависит от почтового клиента. Это означает что пользователи, которые используют клиентов POP3, IMAP или Notes имеющие почтовые файлы на Domino сервере, могут использовать базу Shared Mail.

Shared Mail использует опции безопасности характерные для баз данных сервера. Они гарантируют Вам, что только пользователи, которые должны иметь доступ к данному сообщению, фактически имеют доступ к этому сообщению:

*2065 Список контроля доступа (ACL) базы данных Shared Mail установлен так, чтобы только сервер, используя ID сервера, может получить доступ к базе данных. Т.к. ID сервера имеет доступ менеджера к базе данных Shared Mail, и тип пользователя – Сервер, злоумышленник не сможет использовать этот ID сервера для доступа к базе данных с рабочего места Notes, и не сможет создать реплику базы данных на другом сервере.

*2066 База данных Shared Mail шифруется с использованием ID сервера. Только ID сервера, который создал базу данных, может получить доступ к ней.

*2067 База данных Shared Mail не появляется в меню - Открыть – База данных.

*2068 База данных Shared Mail не содержит никакие представления и ни одно не может быть добавлено в нее.

*2069 База данных Shared Mail включает связи с заголовками сообщения. Когда пользователь читает сообщение, Domino проверяет, что заголовок сообщения соответствует содержанию, сохраненному в базе данных Shared Mail.

*2070 Сообщения, полученные пользователями, для которых выбрана опция шифрования - не может быть сохранено в базе данных Shared Mail.

4.5.1 Как работает Shared Mail?

Когда Router получает почтовое сообщение, адресованное двум или большему количеству получателей, чьи почтовые файлы находятся на этом сервере, Router делит поступающее сообщение в две части: заголовок и содержание. Заголовок состоит из полей сообщения To, Cc, Bcc, Subject и From. Содержание включает в себя только тело сообщения и любые присоединенные файлы. Router сохраняет копию заголовка в почтовом файле каждого получателя, а единственную копию тела сообщения хранит в базе данных Shared Mail.

Когда получатель открывает сообщение, заголовок активизирует связь с содержанием сообщения из базы данных Shared Mail. Сообщение появляется, как если бы полное сообщение было сохранено в почтовом файле получателя.

Если получатель удаляет сообщение, Domino удаляет только заголовок в почтовом файле получателя. Удаление не воздействуют на содержание сообщения, потому оно сохранено в базе данных Shared Mail. Серверная задача на сервере производит чистку устаревших сообщений, включая тела сообщений из базы данных Shared Mail. Эта задача запускается ежедневно в 2AM, по умолчанию.

4.5.2 Как установить Shared Mail?

Прежде, чем Вы создаете базу данных Shared Mail, решите, где она будет храниться. База данных Shared Mail должна быть в пределах логической структуры сервера. Учитывайте, что база данных может стать весьма большой по объему, выбираете диск сервера, на котором достаточно свободного места. Если Вы выбираете каталог, который не является каталогом данных Domino, Вы должны создать связь с базой данных Shared Mail. Иначе, когда Вы запустите сервер, он не найти базу данных Shared Mail.

Router может доставлять почту только в одну базу данных Shared Mail. Поэтому, используете только одну активную базу данных Shared Mail одновременно. После того, как сообщение сохраняется в базе данных Shared Mail, оно остается там пока оно не будет очищено.

Если база данных Shared Mail становится слишком большой, можно создать новую базу данных Shared Mail и заставить Router использовать ее. Связи между почтой пользователя и старым оригиналом базы данных Shared Mail продолжают работать, а новая база данных Shared Mail, будет хранить все вновь поступающие сообщения.

4.5.2.1 Создание и активация базы данных Shared Mail.

Когда Вы разрешаете использование базы данных Shared Mail, Domino устанавливает переменную Shared_Mail, из файла NOTES.INI - в значение 2 (два). Определение этого значения разрешает доставку и передачу почты в базу Shared Mail. Domino также автоматически создает файл с именем MAILOBJ.NSF в каталоге данных. MAILOBJ.NSF - файл связи, который всегда указывает на активную базу данных Shared Mail. Router использует установки из нее, чтобы сохранять новые сообщения в базе данных Shared Mail.

*2071 Удостоверитесь, что задача Router запущена.

*2072 Введите в эту команду на консоли сервера:

```
Tell Router Use SHARED.NSF
```

Где SHARED.NSF - полное название базы данных Shared Mail, которую Вы будете использовать. Если база данных находится в подкаталоге, включите в эту командную строку путь к каталогу. Если файл, еще не существует, Domino используя это имя, создаст его.

4.5.2.2 Создание и разрешение использования дополнительной базы данных Shared Mail.

Задача Object Collect, которая запускается ежедневно и производит чистку устаревших сообщений, ограничивая рост базы данных Shared Mail. Поэтому, Вы не должны создавать дополнительных баз данных Shared Mail пока имеются достаточно свободного места на диске.

Вы можете создать дополнительную базу данных Shared Mail на сервере, если размер базы данных Shared Mail становится слишком большим, или если Вы хотите связать определенные файлы почты с определенной базой данных Shared Mail. После того, как Вы создаете новую базу данных Shared Mail, она будет, хранит все новые сообщения. Старые, существующие сообщения будут находится в старой базе данных.

*2073 Введите эту команду на консоли сервера:

```
Load Object Create NEWOBJ.NSF
```

Где NEWOBJ.NSF - имя новой базы данных Shared Mail. Если необходимо, Вы можете также определить полный путь ней. Для простоты управления, держите все базы данных Shared Mail в одном каталоге.

*2074 Используйте команду Link, для связи почтовых файлов с новой базой Shared Mail.

4.5.3 Управление базой данных Shared Mail.

Используйте для управления базой данных Shared Mail и почтовыми файлами пользователей, которые связаны с базой, следующие процедуры:

*2075 Связывания (Link) , разрыв связей (unlink) или восстановление связей (relink) с почтовыми файлами пользователя

*2076 Включение (Include) или исключение (exclude) почтовых файлов пользователей

*2077 Разрешение использования Shared Mail, для реплицированных почтовых файлов

*2078 Очистка сообщений (obsolete shared mail messages)

*2079 Восстановление базы данных Shared Mail

*2080 Удаление базы данных Shared Mail

4.5.3.1 Связывание (Linking) почтовых файлов с базой данных Shared Mail.

После того, как Вы создаете базу данных Shared Mail на сервере, Domino автоматически сохраняет все новые сообщения в этой базе. Однако Вам может понадобится, чтобы база данных Shared Mail содержала сообщения, которые были доставлены до того, как Вы установили базу данных Shared Mail на сервере. Чтобы сохранить эти сообщения в базе данных Shared Mail, Вы используете команду Object Link, чтобы связать почтовые файлы пользователя с базой данных Shared Mail.

По умолчанию, команда Object Link автоматически перемещает содержание каждого сообщения из почтового файла пользователя в базу данных Shared Mail. Если эта команда связывает больше чем пять файлов сообщений, с базой данных Shared Mail, задача автоматически уплотняет почтовый файл пользователя, чтобы высвободить место на диске, которое было занято содержанием удаленных сообщений.

Связывание почтового файла пользователя с Shared Mail.

Введите эту команду на консоли сервера:

```
Load Object Link USERMAIL.NSF SHARED.NSF
```

Где USERMAIL.NSF - имя почтового файла пользователя или каталог, содержащий почтовые файлы. SHARED.NSF - имя базы данных Shared Mail.

Связывание почтового файла с исключением опции сжатия.

-Nocompact - ключ запрещает уплотнение почтового файла, даже если больше чем пять файлов сообщений будут связаны.

Введите эту команду на консоли сервера:

```
Load Object Link -Nocompact USERMAIL.NSF SHARED.NSF
```

Где USERMAIL.NSF - имя почтового файла или каталог, содержащий почтовые файлы. SHARED.NSF - имя база данных Shared Mail.

Повторно связывает почтовый файл с различными базами Shared Mail.

Повторно связывает почтовые сообщения пользователя с различными копиями баз данных Shared Mail.

Введите эту команду на консоли сервера:

```
Load Object Link -Relink USERMAIL.NSF SHARED.NSF
```

Где USERMAIL.NSF - имя файла почты или каталог, содержащий почтовые файлы. SHARED.NSF - имя базы данных Shared Mail.

Разрыв связей с почтовым файлом пользователей.

Введите эту команду на консоли сервера:

```
Load Object Unlink USERMAIL.NSF
```

Где USERMAIL.NSF - имя файла почты или каталог.

Разрыв связей с базой данных Shared Mail.

Введите эту команду на консоли сервера:

```
Load Object Unlink SHARED.NSF
```

Где SHARED.NSF - имя базы данных Shared Mail.

4.5.3.2 Включение или исключение почтового файла в базу данных Shared Mail.

Вы можете исключать определенный почтовый файл из Shared Mail, или включать ранее исключенный почтовый файл, в Shared Mail.

Исключение почтового файла.

Введите эту команду на консоли сервера:

```
Load Object Set -Never USERMAIL.NSF
```

Где USERMAIL.NSF - имя почтового файла или имя каталога, который содержит почтовые файлы.

Включение, ранее исключенного почтового файла.

Введите эту команду на консоли сервера:

```
Load Object Reset -Never USERMAIL.NSF
```

Где USERMAIL.NSF - имя почтового файла или название каталога, который содержит почтовые файлы.

4.5.3.3 Очистка устаревших сообщений в базе данных Shared Mail.

Устаревшие сообщения – это сообщения, которое все получатели удалили из своих почтовых файлов. Задача Object Collect автоматически производит чистку устаревших сообщений из баз данных Shared Mail ежедневно в 2AM. Однако Вы можете использовать задачу Object Collect, чтобы произвести чистку сообщений из почтовых файлов пользователя.

Например, если база данных Shared Mail теряет данные, Вы не можете восстановить все сообщения в базе данных. Если это происходит, почтовые файлы пользователя будут содержать сообщения, которые пользователи не могут прочитать, потому что содержание сообщения отсутствует в базе данных Shared Mail. Чтобы произвести чистку этих неполных сообщений из почтовых файлов пользователей, Вы можете использовать задачу Object Collect. При этом если реплика почтового файла есть на другом сервере, и содержит очищенное сообщение, сообщение будет восстановлено при репликации в следующий раз с этого сервера.

Когда Вы запускаете задачу Object Collect, Domino автоматически производит статистику Shared Mail.

Предварительный просмотр сообщений, которые будут удалены.

Прежде, чем Вы фактически произведете чистку устаревших сообщений, введите эту команду на консоли сервера, для просмотра документов которые будут удалены. Вы можете просмотреть, сколько места высвободится:

```
Load Object Collect -Nodelete
```

Чистка устаревших сообщений из базы данных Shared Mail.

Введите эти команды на консоли сервера:

```
Load Object Collect SHARED.NSF
```

```
Load Object Collect -Force SHARED.NSF
```

Где SHARED.NSF - имя базы данных Shared Mail

-Force ключ, который Вы используете только после того, как Вы удаляете почтовые файлы пользователя и хотите использовать место на диске, занятое ранее сообщениями.

Для очистки сообщений из почтовых файлов пользователей.

Введите эту команду на консоли сервера:

```
Load Object Collect USERMAIL.NSF
```

Где USERMAIL.NSF - имя почтового файла пользователя.

4.5.3.4 Восстановление базы данных Shared Mail.

Потеря Данных - необычное явление, но это может произойти в любой системе. Чтобы предотвратить потерю данных из базы данных Shared Mail, проверяйте базу данных, по крайней мере, один раз в день. Продумайте создание больше чем одной базы данных Shared Mail на сервере. При использовании нескольких баз данных на сервере уменьшается количество сообщений Shared Mail, которые могли бы быть потеряны. Например, Вы можете создавать новую базу данных на сервере каждую неделю и использовать ее как базу данных для вновь поступающей почты.

Если потеря данных все-таки происходит, и Вы восстанавливаете базу данных Shared Mail, возможно, что не все сообщения будут восстановлены, в этой базе данных. Поэтому почтовые файлы пользователей могут все еще содержать заголовки сообщений, которые Вам не удалось восстановить в базе Shared Mail. Ваши пользователи не смогут читать эти сообщения, потому что база данных Shared Mail не содержит содержание этих сообщений.

Процедура восстановления базы данных Shared Mail.

*2081 Загрузите самую современную резервную копию базы данных Shared Mail в каталог, который не является каталогом Domino сервера. Этот каталог может быть сетевым диском, если не имеется достаточно места на локальных дисках сервера.

*2082 На консоли, введите команду Push, чтобы вытолкнуть изменения из резервной базы данных Shared Mail, в текущую базу данных Shared Mail. Например, после разгрузки резервной копии базы данных в каталог h:\backup, введите команду:

```
Push Manufacturing h:\backup\SHARE1.NSF
```

Где Manufacturing - имя сервера, SHARE1.NSF - имя базы данных Shared Mail.

*2083 Удалите резервную копию базы данных Shared Mail.

*2084 В почтовых файлах пользователя, произведите чистку сообщений, которые больше не имеют соответствующего содержание сообщений в файле Shared Mail.

4.5.3.5 Удаление базы данных Shared Mail.

По некоторым причинам Ваша организация может решить прекратить использование базы данных Shared Mail. Чтобы удалить базу данных Shared Mail, Вы должны сначала разорвать все связи с почтовыми файлами пользователей. После этого Domino сохранят все сообщения в почтовых файлах пользователей. Если Вы не разорвете связи с почтовыми файлами пользователей прежде, чем удаляете базу данных Shared Mail, задача Object Collect не сможет произвести чистку содержания сообщений в базе данных Shared Mail.

Прежде, чем Вы разорвете связи, проверяете число и размер сообщений в ней. Вы сможете определять, имеется ли достаточно места на диске, для сохранения полных копии сообщений в почтовых файлах каждого получателя.

Удаления базы данных Shared Mail.

*2085 Введите эту команду на консоли сервера:

```
Load Object Info USERMAIL.NSF
```

Где USERMAIL.NSF - имя файла почты пользователя или имя каталога, который содержит почтовые файлы.

*2086 Введите эту команду на консоли сервера:

```
Load Object Unlink USERMAIL.NSF
```

Где USERMAIL.NSF - имя файла почты пользователя или имя каталога, который содержит почтовые файлы.

*2087 Введите эту команду на консоли сервера:

```
Load Object Unlink SHARED.NSF
```

Где SHARED.NSF - имя базы данных Shared Mail.

*2088 Удалите файл базы данных Shared Mail.

4.6 Использование сервиса POP3 на Domino сервере.

POP3 - протокол передачи интернет почты (3 версии), который позволяет пользователю имеющего почтового POP3 клиента, например, Netscape Navigator, Eudora или Microsoft Internet Explorer - получать почту с сервера, на котором запущена служба POP3. Вы можете использовать Domino сервер для запуска этой службы POP3. Ваши пользователи смогут периодически соединяться с Domino сервером, чтобы забирать свою почту.

Пользователи могут использовать только POP3 клиента или, POP3 и Notes для отправки сообщений клиентов. Для каждого POP3 пользователя, Вы создаете Person документ и почтовый файл. Так как эти пользователи не имеют полного ID Notes, они не могут получить доступ к Notes (Domino). Пользователи POP3 не могут получать шифрованную почту Notes, для этого они должны иметь публичный ключ, который не содержит их ID. Прежде чем пользователь POP3 получит доступ к своему почтовому файлу, он должны зарегистрироваться на Domino сервере. Domino сервер поддерживает базовую идентификацию с использованием имени и пароля, а так же SSL идентификацию и SSL шифрование.

POP3 клиенты могут посылать почту другим POP3 и IMAP клиентам, независимо от того, отправляет ли они почту из Notes или из другой почтовой системы. POP3 пользователи

могут также посылать почту пользователям Notes. Router использует SMTP для доставки сообщений в почтовый файлу получателя, на Domino сервер.

Domino сервер только хранит и позволяет исправление почты, полученной POP3 клиентами. Чтобы позволять POP3 клиентам посылать почту, Вы должны установить и сконфигурировать протокол SMTP.

Служба POP3 поддерживает следующие стандарты:

*2089 RFC 1725 – Post Office Protocol, версии 3

*2090 RFC 822 - Стандарт для формата ARPA текстового сообщения интернет

*2091 RFC 1521 - MIME (Multipurpose Internet Mail Extensions) и

*2092 RFC 1522 - MIME (Multipurpose Internet Mail Extensions), который поддерживает почтовые сообщения содержащие с присоединенной графикой, видео и аудио.

4.6.1 Установка сервиса POP3 на Domino сервере.

Чтобы установить службу POP3 на Domino сервере, нужно выполните следующие процедуры:

*2093 Прежде, чем Вы установите службу POP3:

- Удостоверитесь, что Вы понимаете TCP/IP концепцию, включая имена DNS хостов и IP адресование.
- Установите Domino сервер и настройте безопасность для сервера.

*2094 Чтобы позволить пользователям, соединиться с Вашим сервером с использованием интернета, необходимо соединить Ваш сервер с интернетом, зарегистрировать имя и IP адрес сервера, на сервере DNS Вашего поставщика услуг интернета.

*2095 Запустите POP3 задачу на Domino сервере.

*2096 (Необязательно) Изменение POP3 порт по умолчанию.

*2097 Запустите SMTP, по крайней мере, одном Domino сервере и включите SMTP Listener.

4.6.1.1 Запуск и остановка сервиса POP3.

Вы можете загрузить службу POP3 вручную, или запускать ее автоматически при старте Domino сервера.

Задача	**Как это сделать**
Ручной запуск сервиса POP3	Введите на консоли сервера: `load pop3.`
Автоматический запуск сервиса POP3 при старте сервера Domino	Отредактируйте установки переменной ServerTasks в NOTES.INI. добавьте имя задачи POP3 в эту строку. Domino добавляет имя задачи POP3 по умолчанию, если Вы выбираете при инсталляции этот сервис.

Остановка сервиса POP3	Введите на консоли сервера: `tell pop3 quit`

4.6.1.2 Изменение значения порта, для задачи POP3.

По умолчанию задаче POP3 назначается 110 порт TCP/IP. Если Вы планируете использовать нестандартный порт для задачи POP3, или Вы хотите временно запретить POP3 клиентам соединения с Domino сервером, используйте следующую последовательность действий.

*2098 Из клиента Domino Administrator, выбирайте закладку Настройка, откройте Server документ для Вашего сервера, на котором запущена служба POP3.

*2099 Выбирайте закладку Ports – Internet Ports – Mail

*2100 В колонке – Mail (POP3), измените значения этих полей, если это необходимо и затем сохраните документ:

Поле	**Значение**
TCP/IP port number	Номер порта для задачи POP3
TCP/IP port status	Выбирайте одно: *2101 Enabled - (по умолчанию) разрешить POP3 клиентам соединятся с почтовым Domino сервером *2102 Disabled - запретить POP3 клиентам соединятся с почтовым Domino сервером

*2103 Если Вы изменили номер порта или статус порта для POP3 задачи, чтобы изменение вступило в силу, перезапустите задачу.

4.6.2 Настройки для пользователей POP3.

Для пользователей POP3 необходимо выполнить следующие настройки:

*2104 Проверить и изменить установки в Person документах, если это необходимо.

*2105 Создать почтового файла, если они еще не созданы.

*2106 Конфигурирование программного обеспечения POP3 клиента.

4.6.2.1 Установки в Person документах, для POP3 пользователей

Для каждого POP3 пользователя Вы должны создать Person документ, или отредактировать существующий. В большинстве случаев, Вы создаете Person документ в течение регистрации пользователя.

*2107 Из клиента Domino Administrator выбирайте закладку - Пользователи и группы.

*2108 Выбирайте Domino Directory – Пользователи.

*2109 Выбирайте нужное имя пользователя и затем, переведите документ в режим редактирования. Если пользователь не был предварительно зарегистрирован как пользователь Notes, выбирайте кнопку – Add Person.

*2110 Выбирайте закладку – Basics и затем заполните следующие поля:

Поля	**Значения**
First name Last name User name	Введите имя отчество и фамилию пользователя для клиента POP3.
Internet password	Пароль, который пользователь будет использовать для доступа к Domino серверу.

*2111 На закладке Mail заполните следующие поля, потом сохранить документ:

Поле	**Значение**
Mail system	Почтовая система для пользователя – POP3.
Domain	Введите имя домена Notes.
Mail server	Имя сервера для POP3 пользователя – почтового сервера Domino.
Mail file	Имя пользовательского файла, с указанием подкаталога. Пример: MAIL\AJONES.NSF
Forwarding address	Перенаправление почты на адрес.
Internet message storage	Выбирайте одно: *2112 Notes - сохраняет сообщение только в формате Notes. *2113 Notes и интернет присоединения сохраняются в Notes и MIME формате *2114 Только MIME - сохраняются в MIME формате
Internet address	интернет адрес для POP3 клиента.
Encrypt incoming mail	Выбирайте – No. POP3 клиенты не могут читать шифрованную почту Notes.

4.6.2.2 Создание почтового файла для пользователя POP3.

Каждый POP3 пользователь должен иметь почтовый файл на Domino сервере. Вы можете создавать почтовые файлы в течение регистрации пользователя, или Вы можете вручную создавать почтовые файлы. Если пользователь уже зарегистрированный пользователь Notes и имеет существующий почтовый файл Notes, чтобы использовать POP3 систему, пользователь может использовать POP3 клиента для доступу к файлу почты.

Вы можете иметь зарегистрированных пользователей Notes, которые не используют почту Notes. Поэтому Вы должны создать новый почтовый файл для этих пользователей.

Создание почтового файла - в ручную.

*2115 Убедитесь, что Вы создали Person документ для пользователя POP3.

*2116 Выбирайте из меню Файл – База данных – Новый.

*2117 Определите настройки для почты пользователя:

Поле	**Значение**
Server	Имя почтового сервера.
Title	Описание почтового файла. Пример: Alan Jones' Mail.
File name	Путь к файлу пользователя. Пример: MAIL\AJONES.NSF

*2118 Выбирайте шаблон для почтового файла - MAIL.NTF.

*2119 После создания почтового файла отредактируйте ACL базы данных. Присвойте доступ менеджера с удалением документов будущему пользователю. Удалите свое имя из ACL, если это необходимо.

4.6.2.3 Конфигурирование программного обеспечения клиента POP3.

Вы конфигурируете программное обеспечение клиента POP3 в зависимости от его изготовителя. Эта таблица представляет общие требования.

Требования	**Описание**
Fully qualified name of the Domino server that runs SMTP	Полное имя хоста сервера SMTP.
Fully qualified name of Domino POP3 server	Полное имя хоста сервера с запущенным сервисом POP3.

POP3 client user name	Имя клиента POP3.
Automatically delete mail documents on from the POP3 server after the client copies them locally.	Эта опция сохраняет ресурсы сервера, минимизируя место на диске Domino сервера. Не удаляйте документы, если пользователь также имеет доступ к почте через клиента Notes.
POP3 client should check for mail no more than every five (5) minutes.	Период проверки почты клиентом.

4.7 Установка сервиса IMAP.

Глава описывает, как настроить Domino сервер, чтобы использовать службу IMAP и как создать и настроить IMAP пользователей.

4.7.1 Сервис IMAP.

Ваш Domino сервер может поддерживать службу IMAP, определенную в документе RFC 2060, для чтения почты IMAP пользователями. Пользователи сервиса могут:

*2120 Читать сообщения с Domino сервера, на котором запущена служба IMAP, сохранять эти сообщения локально

*2121 Иметь доступ к сообщениям непосредственно на сервере

*2122 Копировать сообщения, для локального использования и затем синхронизировать их с почтовым сервером

*2123 Иметь общие почтовые ящики, которые являются эквивалентом папок почты Notes

После того как Вы установили Domino сервер и запустили службу IMAP, пользователи, используя почтового клиента IMAP, могут получить доступ к своим почтовым файлам, на Domino сервере. Служба IMAP не может посылать почту. Вместо этого Вы настаиваете Domino сервер для использования маршрутизации SMTP, для рассылки исходящий сообщений.

Служба IMAP поддерживает всех IMAP-клиентов, например Outlook Express, Netscape Messenger, PC-Pine 3.0 или Simeon 4.1.

IMAP клиенты должны ввести пароль, прежде чем они смогут получить доступ на почтовый сервер. Domino сервер поддерживает идентификацию пользователей с использованием имени и пароля, SSL, а также SSL шифрование.

Папки Notes появляются в IMAP, как IMAP почтовые ящики. Когда пользователи получают или удаляют документы в IMAP почтовом ящике, изменения также происходят в папках Notes и наоборот.

Пользователь может использовать и IMAP клиента и Notes клиента, для доступа к своему почтовому ящику. IMAP клиент может посылать почту другим IMAP или POP3 клиентам, независимо от того, используют ли он почту Notes, или другую почтовую систему. IMAP пользователи могут также посылать почту не - IMAP пользователям Notes. Router использует SMTP, для доставки сообщение в почтовый файл получателей на Domino

сервере. Этот процесс похож на тот, когда IMAP клиент посылает почту не-IMAP пользователям Notes.

4.7.2 Установки сервиса IMAP.

Чтобы настроить службу IMAP, исполните следующие процедуры:

*2124 Прежде, чем Вы установите службу IMAP:

- Удостоверитесь, что Вы понимаете концепцию TCP/IP, DNS имен хостов и IP адресацию.
- Установите Domino сервер и настройте безопасность для сервера.

*2125 Чтобы позволить пользователям, не использующим Вашу сеть, соединятся с сервером по интернету, соедините Ваш сервер с Поставщиком Обслуживания интернета (ISP) и зарегистрируют имя DNS сервера и IP адрес в записях DNS Вашего провайдера.

*2126 Запустите IMAP задачу на Domino сервере.

*2127 (Необязательно) Измените по умолчанию порт для сервиса IMAP.

*2128 Запустите SMTP и SMTP Lister, по крайней мере, на одном Domino сервере.

4.7.2.1 Запуск и остановка задачи IMAP.

Вы можете загружать IMAP задачу вручную или запускать ее автоматически при старте Domino сервера.

Задача	**Решение**
Ручной запуск задачи IMAP	Введите на консоли сервера: `load imap.`
Автоматический запуск сервиса IMAP при запуске Domino сервера	Редактируйте переменную ServerTasks в файле NOTES.INI, добавьте задачу IMAP для автоматического запуска задачи на Domino сервере при его старте.
Остановка сервиса IMAP	Введите на консоли сервера: `Tell imap quit.`

4.7.2.2 Изменение значения порта по умолчанию, для задачи IMAP.

TCP/IP порт 143 определяется по умолчанию, для сервиса IMAP. Если Вы планируете использовать нестандартный порт, или хотите запретить IMAP клиентам соединятся с Domino сервером, выполните следующее:

*2129 Из клиента Domino Administrator, выбирайте закладку Настройка, и откройте Server документ сервера, на котором запущен сервис IMAP.

*2130 Выбирайте закладку Ports – Internet Ports – Mail.

*2131 В колонке Mail (IMAP), если это необходимо, измените значения полей, затем сохраните документ:

Поле	**Значение**
TCP/IP port number	Номер порта
TCP/IP port status	Выбирайте одно: *2132 Enabled - (по умолчанию) разрешить IMAP клиентам соединится с Domino сервером без использования SSL *2133 Disabled - запретить IMAP клиентам соединятся с Domino сервером *2134 Redirect to SSL – требовать соединения с использованием SSL

*2135 Если Вы изменили номер порта, перезапустите задачу IMAP.

4.7.3 Настройки для пользователей IMAP.

Для настройки IMAP пользователей, исполните эти процедуры:

*2136 Настройте Person документ для пользователей.

*2137 Создайте почтовый файл для пользователей IMAP.

*2138 Разрешите доступ к почтовым файлам, пользователей IMAP.

*2139 Сконфигурируйте программное обеспечение IMAP клиентов.

*2140 (Не обязательно) Создайте полнотекстовый индекс для почтового файла, чтобы IMAP пользователь мог искать информацию в почтовом файле. Когда Вы создаете индекс, выбираете опцию Индексировать вложения, что позволить пользователю искать информацию в присоединенных файлах, которые находятся в формате MIME.

4.7.3.1 Настройки Person документов, для пользователей IMAP.

Для каждого IMAP пользователя, Вы должны создать Person документы или редактировать существующие. Во многих случаях Вы создаете Person документы в течение регистрации пользователей.

*2141 Из клиента Domino Administrator, выбирайте закладку - Пользователи и группы.

*2142 Выбирайте - Справочники Domino – Пользователи.

*2143 Выбирайте нужный Person документ пользователя. Если пользователь не был предварительно зарегистрирован в Notes, выбирайте кнопку – Add Person.

*2144 Выбирайте закладку – Basics, заполните или измените поля, если это необходимо:

Поле	**Значение**
First name Last name User name	Введите имя, отчество, фамилию, пользователя IMAP.
Internet password	Пароль, который пользователь будет использовать для доступа к Domino серверу.

*2145 На закладке Mail, заполните или измените значения полей и сохраните документ:

Поле	**Значение**
Mail system	Выбирайте тип почтовой системы для пользователя – IMAP.
Domain	Введите имя домена Notes.
Mail server	Имя почтового сервера, для IMAP пользователя – Почтовый сервер Domino.
Mail file	Имя пользовательского почтового файла, с указанием подкаталога Пример: MAIL\AJONES.NSF.
Forwarding address	Перенаправление почты на адрес …
Internet message storage	Выбирайте одно: *2146 Notes - сохраняет сообщение только в формате Notes. *2147 Notes и интернет присоединения сохраняются в Notes и MIME формате *2148 Только MIME – сохраняются в MIME формате
Internet address	интернет адрес для IMAP клиента.
Encrypt incoming mail	Выбирайте – No. IMAP клиенты не могут читать шифрованную почту Notes.

4.7.3.2 Создание почтового файла для пользователя IMAP вручную.

Каждый IMAP пользователь должен иметь почтовый файл на Domino сервере. Вы можете создавать почтовые файлы автоматически, в течение регистрации пользователя, или Вы можете вручную создавать почтовые файлы. Если пользователь, уже зарегистрирован как пользователь Notes, пользователь может использовать IMAP клиента для доступа к почтовому файлу.

Создание почтового файла вручную:

*2149 Удостоверитесь, что Вы создали Person документ, для IMAP пользователя.

*2150 Выбирайте из меню Файл – База данных – Новый.

*2151 Определите настройки пользователя:

Поле	**Значения**
Server	Имя почтового сервера.
Title	Описание почтового файла, например: Alan Jones's Mail.
File name	Путь к файлу пользователя (MAIL\AJONES.NSF).

*2152 Выбирайте почтовый шаблон MAIL50.NTF …

4.7.3.3 Конвертирование почтового файла IMAP.

После того, как Вы создали почтовый файл для IMAP пользователя, Вы должны конвертировать его, чтобы пользователи могли обращаться к нему с использованием IMAP клиента. Когда Вы создаете реплику файла почты, ссылки на папки по умолчанию не работают. Поэтому Вы должны их немедленно конвертировать, если Вы планируете использовать IMAP, для доступа к репликам файла.

Папки Входящие, Мусорная корзина и любые общие папки, в файле почты Notes, появляются в IMAP как почтовые ящики. Скрытые и личные папки будут не видны IMAP пользователям. Также, IMAP пользователи не будет видеть Черновики и Отправленные. IMAP и клиенты Notes поддерживают функцию Непрочитанных сообщений независимо друг от друга. Сообщение, помеченное как прочитанные в Notes, может все еще быть помечено как непрочитанные для IMAP клиента и наоборот. Domino IMAP сервер не поддерживает переименование папки Inbox в почтовом файле Notes из IMAP клиента.

Обратите внимание, что увеличение размера почтового файла замедляет быстродействия папок.

Почтовые файл пользователей IMAP, должны быть созданы по почтовому шаблону - MAIL50.NTF. Если необходимо, Вы можете использовать утилиту, для преобразования почтового файла, когда Вы планируете использовать почтовый файл, для IMAP пользователя. Вы можете запускать утилиту на отдельном файле, или на всех файлах в каталоге.

Конвертирование почтового файла пользователя для использования его с сервисом IMAP.

*2153 Удостоверитесь что Вы:

- Создали Person документ для IMAP пользователя
- Создали почтовый файл для IMAP пользователя

*2154 На консоли сервера введите:

```
load convert -m path mailfile * mail50.ntf
```

Где:

-m - Указывает путь к файлу(ам), относительно каталога данных

Mailfile - Имя определенного почтового файла, или *.NSF, чтобы указать все файлы в каталоге

Mail50.ntf - Имя файла шаблона

Пример. Чтобы определить все файлы в каталоге, удостоверитесь, что каталог содержит только почтовые файлы. Введите на консоли сервера:

```
load convert -m path mail\*.nsf
```

Чтобы позволить доступ сервиса IMAP к определенному почтовому файлу в каталоге и, конвертировать почтовый файл, с использованием текущего почтового шаблона, введите на консоли сервера:

```
load convert -m path imap\ajones.nsf * mail50.ntf
```

Обратите внимание, в UNIX используется знак - (/), вместо - (\). Например:

```
load convert -m path mail/*.nsf
```

Конфигурирование программного обеспечения IMAP клиента

Вы конфигурируете программное обеспечение клиента IMAP, в зависимости его изготовителя. Эта таблица показывает общие требования.

Требования	**Комментарии**
Fully qualified name of the Domino server running SMTP	DNS имя хоста
Fully qualified name of Domino IMAP server	Это может быть такое же самое имя как имя Domino сервера, на котором запущен сервис SMTP.
IMAP client user name	Имя клиента
Folder prefixes	Путь к Root Folder, для IMAP клиентов. Domino не использует префиксы пользовательских папок.

5 Каталог Domino сервера. База данных Domino Directory.

Глава содержит описание базы данных Domino Directory и объясняет, как настроить Domino Directory для Notes домена.

5.1 Domino Directory

Domino Directory – новое название базы данных Public Address Book или Name Address Book. Domino автоматически создает эту базу на каждом сервере, или реплицирует его с другого сервера. Domino Directory на серверах Domino выполняет две главные цели:

*2155 Это домино каталог, содержит информацию относительно пользователей, серверов, групп и других объектов, которые Вы можете включать в каталог самостоятельно - например, принтеры.

*2156 Эта база данных так же является также инструментом, который администраторы используют, чтобы управлять Domino системой. Администраторы создают документы в Domino Directory, для соединения серверов для репликаций или передачи почты. Регистрируют пользователей и сервера, намечают серверные задачи, для запуска их на сервере Domino.

Типично, Domino Directory связан с Notes доменом. Когда Вы регистрируете пользователей и сервера в домене, Вы создаете Person документы, Server документы в Domino Directory. Эти документы содержат детальную информацию о каждом пользователе или сервере.

Когда Вы устанавливаете первый сервер в Notes домене, Domino автоматически создает на нем базу данных Domino Directory, называет его NAMES.NSF. Когда Вы добавляете, новый сервер в домен, Domino автоматически создает реплику Domino Directory на новом сервере.

Дополнительные сервисы Directory.

В дополнение, Domino Directory предоставляет Вам три службами каталога: Directory Catalog, Directory Assistance и LDAP Service. Эти функции помогают пользователям найти имена пользователя, для адрессования им почты и другую информацию из Domino Directory.

Directory Catalog - объединяет информацию о пользователях, группах из одного или нескольких Domino Directory в маленькую, легкую базу данных. Пользователи Notes, которые используют копию Local Directory Catalog – Mobile Directory Catalog - могут быстро адресовать почту пользователям во всей Вашей организации, даже если организация использует большой каталог, или несколько каталогов пользователей. В организациях, которые используют несколько Domino каталогов, Directory Catalog на сервере объединяет эти каталоги в одну базу данных так, чтобы сервер смог просматривать имена в одной базе данных намного быстрее, чем в нескольких Domino каталогах.

Directory Assistance – эта функция, которая помогает управлять поиском имен в организациях, которые используют несколько Domino каталогов, или адресных книг производителей других почтовых систем (Third-Party). База данных Directory Assistance связывает каждый Domino Directory/LDAP, с определенными иерархическими именами. В процессе поиска Domino сначала просматривает каталог, который содержит имена из этой определенной иерархии.

Lightweight Directory Access Protocol. Вы можете настроить Domino сервер, чтобы он использовал службу LDAP. Вы можете разрешить LDAP клиентам, поиск и изменения информации в базе данных Domino Directory.

5.1.1 Настройки Domino Directory для домена Notes.

Domino Directory содержит документы, которые управляют задачами Domino каталога, управляют задачами серверов, определяют взаимоотношение между серверами. Domino автоматически создает некоторые документы, когда Вы исполняете некоторые задачи администрирования. Например, Domino создает новый Person документ, когда Вы регистрируете пользователя. Вы можете вручную создавать документы, в которых нуждаетесь. Например, Вы создаете документ подключения, чтобы определить, как два сервера будут передавать почту или реплицировать данные между собой. Вы можете использовать закладки, клиента Domino Administrator, для доступа к документам из Domino Directory.

После того, как Вы установите и запускаете Domino сервера в Notes домене, исполняете эти процедуры, чтобы настроить Domino Directory для домена.

*2157 Назначьте нужный доступ к базе данных Domino Directory.

*2158 Наметьте репликации для базы данных Domino Directory.

*2159 (Необязательно) Настраивайте профиль для Domino Directory.

*2160 (Необязательно) Создайте базу данных Mobile Directory Catalog.

5.1.1.1 Настройка ACL для Domino Directory.

Чтобы управлять доступом к базе данных Domino Directory, Вы настраиваете список управления контроля доступа. Вы можете управлять общим доступом к Domino Directory и доступом к определенным формам, а так же управлять доступом к определенным документам. Кроме того, если Вы разрешаете анонимный доступ к Domino серверу, для LDAP сервиса, Вы можете указать, к каким из полей, в каталоге, могут получить доступ анонимные пользователи LDAP.

Управление общим доступом к каталогу.

Назначьте ACL базы Domino Directory, чтобы определить доступ пользователям и серверам к Domino Directory. Эта таблица описывает доступ по умолчанию к базе данных Domino Directory:

Запись	Уровень доступа	Тип пользователя
- Default -	Доступ автора, без ролей, с привилегией Create documents	Не определен
Administrators group	Доступ менеджера, без ролей	Не определен
LocalDomainServers	Доступ менеджера со всеми ролями	Группа серверов
OtherDomainServers	Доступ читателя	Группа серверов
Сервер, на котором каталог был создан	Доступ менеджера со всеми ролями	Сервер

Администратор, который был определен в течение установки сервера	Доступ менеджера со всеми ролями	Пользователь

Назначение доступа к определенным формам.

Domino Directory имеет роли Creator и Modifier, которые Вы можете назначать, чтобы делегировать полномочие для управления определенными типами документов в Domino Directory. Вместо использования доступа Editor, который позволяет пользователям изменять все документы в Domino Directory, Вы можете использовать роль Modifier, чтобы позволить пользователям с доступом Author, изменять определенные виды документов в Domino Directory.

Например. Вы определяете некоторых администраторов ответственными за поддержку пользователей и назначаете им роль UserModifier. Роль Modifier применяются для пользователей с доступом Author. Пользователи с доступом к базе - Editor или выше, могут изменять любой документ в Domino Directory, без этой роли.

Роль Creator, с привилегией Create documents, позволяют Вам управлять пользователями. Эти пользователи могут использовать меню Create, чтобы создавать определенные типы документов в Domino Directory. Роль Creator используется со всеми уровнями доступа пользователей, включенных в ACL базы данных Domino Directory.

Предостережение. Роль Creator создана скорее для удобства, чем для безопасности, так как Domino игнорирует роль Creator, когда пользователи создают документы без использования меню Create, например, если документы создаются программно.

Используя роль Modifier, позволяет Вам определять, какой пользователь с доступом Author, может изменять документы. В отличие от роли Creator, роль Modifier относится к акциям безопасности.

Доступ, определенный ролью, никогда не превышает общий уровень доступа. Например, пользователь с доступом Reader не может использовать меню Create, чтобы создать Person документы, даже если пользователь включен в роль UserCreator.

Если в Вашей организации только несколько администраторов управляют Domino Directory, Вы можете не использовать роли.

Описание ролей:

Роль	**Что позволяет делать эта роль**
GroupCreator	Пользователям с привилегией Create documents, разрешается использование меню Create, для создания новых Group документов
GroupModifier	Пользователям с доступом Author, разрешается редактировать Group документы*
NetCreator	Пользователям с привилегией Create documents, разрешается использование меню Create, для создания новых Person документов, Group документов и Server документов

NetModifier	Пользователям с доступом Author, разрешается редактировать все существующие Person документы, Group и Server документы*
ServerCreator	Пользователям с привилегией Create documents, разрешается использование меню Create, для создания новых Server документов
ServerModifier	Пользователям с доступом Author, разрешается редактировать Server документы*
UserCreator	Пользователям с привилегией Create documents, разрешается использование меню Create, для создания новых Person документов
UserModifier	Пользователям с доступом Author, разрешается редактировать Person документы*

* Чтобы удалять документы из Domino Directory, пользователи должны иметь привилегию Delete documents в ACL, независимо от их уровня доступа или роли.

Доступ к выбранным документам.

Каждый документ в Domino Directory содержит закладку администрирования с полем администрирования. Чтобы позволить пользователю доступ только к определенному документу, а не ко всем документам, введите имя пользователя в поле администрирования.

5.1.1.2 Расписание репликаций для базы данных Domino Directory.

Создайте документы подключений, для определения репликаций Domino Directory для всех серверов в Notes домене. Так как Domino Directory является самой важной базой данных в Domino системе, важно реплицировать ее как можно чаще. Реплицируйте Directory, по крайней мере, каждые 30 минут, или если каталог большой и изменяется часто, наметьте репликации каждые 10 - 15 минут.

Реплицируйте базу данных Administration Requests (ADMIN4.NSF), также часто, как Вы реплицируете Domino Directory. Задача Adminp, упрощает некоторые задачи администрирования и использует базы данных Administration Requests и Domino Directory, чтобы выполнять эти задачи. Если Domino Directory большой, создайте документы подключений, чтобы наметить репликации только для Domino Directory и базы данных Administration Requests.

5.1.1.3 Использование профиля для Domino Directory.

Используйте профиль для Domiono Directory, чтобы определить некоторые назначения для Domino Directory.

*2161 Из клиента Domino Administrator, из панели сервера, слева, выбирайте сервер, который хранит реплику Domino Directory, который Вы хотите изменить. Если Вы не видите панель сервера, выбирайте изображение сервера.

*2162 Выбирайте закладку Файлы.

*2163 Выбирайте Domino Directory и откройте базу данных.

*2164 Выбирайте из меню Действия – Edit Directory Profile.

*2165 Заполните любые из этих полей и затем выбирайте – Сохранить и Закрыть:

Поля	**Значения**
Domain defined by this Public Directory	Имя Notes домена для Domino каталога. Domino заполняет это поле автоматически, когда Вы устанавливаете Domino сервер.
Directory Catalog file name for domain	Имя файла Directory Catalog для домена. Каждый сервер в домене, который имеет реплику Directory Catalog, должен использовать это имя файла для реплик.
Sort all new groups by default	Выбирайте одно из следующего: *2166 Yes – сортировка в алфавитном порядке, для каждой новой группы которую Вы создаете. *2167 No - (по умолчанию), чтобы показать членов группы в порядке, в котором Вы их добавляете.
Use more secure Internet Passwords	Выбирайте одно из следующего: *2168 Yes - (по умолчанию) использовать усиленное шифрование для паролей интернета. *2169 No - использовать менее безопасное шифрование, доступное предыдущим версиям Domino.
Allow the creation of Alternate Language Information documents	Выбирайте одно из следующего: *2170 Yes - (по умолчанию) Позволять Вам создавать документы Alternate Language, чтобы разрешить LDAP клиентам, искать информацию о пользователях на определенном Вами, родном языке. *2171 No – не разрешается создание документов Alternate Language.
List of administrators who are allowed to create Cross Domain Configuration documents in the Administration Process Requests database	Введите имена пользователей, тех, кто может создавать документы Cross Domain Configuration, чтобы позволить Administration Process обрабатывать запросы между Notes доменами.

5.1.2 Оптимизация производительности Domino Directory.

Чтобы оптимизировать производительность базы данных Domino Directory Вы можете изменить некоторые свойства базы данных, установленные по умолчанию. Вы можете изменить значения по умолчанию, для следующих опций:

*2172 Оптимизировать таблицы документов - чтобы увеличить производительность маленьких представлений, при их обновлении.

*2173 Не сохранять отметки о не прочтении - чтобы увеличить производительность базы данных и уменьшать ее размер.

5.2 Использование нескольких Domino Directories.

Когда Вы устанавливаете первый сервер в организации, Вы создаете Notes домен и Domino Directory. Большинство организаций использует один Notes домен, и регистрируют все сервера и пользователей в одной базе данных Domino Directory. Однако имеются несколько причин, по которым вы можете использовать несколько доменов и несколько баз Domino Directory.

Пример. В большой организации, в которой ответственность за администрирование системы распределена, создавая несколько отдельных доменов и используя несколько отдельных Domino Directories, Вы определяете безопасность системы, основываясь на ACL каждого Domino Directory. Вы можете ограничить доступ, к серверам и адресным книгам, таким группам как OtherDomainServers, или любой другой группе, определить им доступ только на чтение информации, или вообще запретить доступ.

Другая причина, по которой Вы можете использовать несколько доменов и Domino Directories - если Ваша организация сливается с другой организацией, которая использует Domino. В этом случае, Вы можете решить сохранить свой домен и Domino Directories, по крайней мере, временно. Чтобы создать дополнительный домен и Domino Directory, Вы должны выполнить установку сервера.

Некоторые организации создают дополнительные Domino Directory для пользователей, которые не входят Notes домен. Вы можете сделать это, для определения не-Notes пользователей, например для Web пользователей. Чтобы создать дополнительный Domino Directory, Вы создаете базу данных используя шаблон PUBNAMES.NTF. Например, если Ваша компания использует электронную почту и переписывается с другими компаниями, которые используют Domino, Вы могли бы создать отдельный Domino Directory, который бы содержал их адреса.

В системе с несколькими Domino Directories, первичный Domino Directory тот, в котором зарегистрирован Ваш сервер. Первичный Domino Directory использует имя файла - NAMES.NSF. С точки зрения Вашего сервера, любой другой Domino Directory, в пределах организации является вторичным, по отношения к Вашему серверу и Domino Directory.

Организация может также использовать Domino Directory наряду с Third-Party и LDAP Directory. Например, организация может иметь Domino Directory на Domino Web сервере, но использовать данные Third-Party, LDAP Directory, для идентификации Web пользователей, которые соединяются с Domino сервером. Если Вы используете Domino LDAP сервис, Вы можете также выделить этих LDAP клиентов, которые используют службу Third-Party, LDAP Directory, в отдельный каталог.

Важно планировать стратегию использования нескольких Domino Directories. Вы можете создавать Directory Catalog и Directory Assistance, чтобы сделать более легким поиск имен и идентификацию клиентов, во всех Domino Directory.

5.2.1.1 Как планировать использование нескольких Domino Directory.

Создание Directory Catalog и конфигурирование Directory Assistance, при использовании нескольких Domino Directory помогает Вам управлять Вашей системой.

Directory Catalog.

Directory Catalog объединяет наиболее часто используемую информацию из одного или нескольких Domino Directory, в единственную легкую, с быстрым доступом базу данных. Вы должны создать базу данных каталога, с использованием шаблона DIRCAT5.NTF. Имеются два типа Directory Catalog: Mobile Directory Catalog и Server Directory Catalog.

Пользователи Notes могут хранить локальные реплики базы Mobile Directory Catalog, при этом они могут быстро адресовать почту любому пользователю в Вашей организации, даже когда эти пользователи отсоединены от сети. Такой тип адресации, автоматически ищет нужных пользователей, при вводе нескольких символов имен получателей в Mobile Directory Catalog. Таким образом, уменьшается движение данных по сети, так как поиск имен не происходить на сервере.

Server Directory Catalog ускоряют поиск имен во вторичных Domino Directory, которые находятся на сервере.

Directory assistance.

Directory Assistance расширяет поиск имен Notes, LDAP поиск, идентификацию Web клиентов во вторичных Domino Directory и LDAP Directories. Для использования Directory Assistance, создайте базу данных из шаблона DA50.NTF. В этой базе данных Вы создаете документы для каждого каталога (Directory), в котором Вы планируете искать нужную Вам информацию. В документе, Вы определяете, среди других вещей, местоположения каталога и правила обработки имен (Rule Naming), которые отражают имена пользователей на их каталоги (Directory).

Lotus рекомендует, использование Directory Assistance вместо использования каскадных Domino Directory, которые все еще поддерживается только для обратной совместимости версий серверов.

Сравнение Directory Catalogs и Directory Assistance.

Mobile Directory Catalog, Server Directory Catalog и Directory Assistance предоставляет Вам похожие функциональные возможности. Этот таблица сравнивает эти задачи.

Задача	**Mobile Directory Catalog**	**Server Directory Catalog**	**Directory assistance**
Находит записи во вторичных Domino Directories имена пользователей Notes, для адресации почты	Да	Да	Да
Находит записи в LDAP Directory имена Notes пользователей, для адресации почты	Нет	Нет	Да
Находит записи во вторичных Domino Directories для LDAP клиентов	Нет	Да	Да
Обращение LDAP клиентов к LDAP Directory	Нет	Нет	Да

Идентификация Web клиентов с использованием записей, вторичных Domino Directory	Нет	Да	Да
Идентификация Web клиентов с использованием записей из LDAP Directories	Нет	Нет	Да
Возможность адрессования Recipient name type ahead *(Поиск имени по нескольким введенным символам)*	Да	Да*	Да

*Только для клиентов Notes, которые не используют Mobile Directory Catalog.

Lotus рекомендует использовать и Server Directory Catalog, и Directory Assistance.

Сервер поиска в домене/каталоге (Directory servers).

Directory server – выделенный Domino сервер. Directory Server уменьшает рабочую нагрузку на сервера домена, особенно на почтовые сервера. Вы можете создать User Setup Profile, чтобы создавать пользователей Notes, с использованием Directory server. При таком подходе, когда пользователь вводит имя, при адресации почты, поиск происходит на выделенном для этой цели Directory сервер, скорее, чем на почтовом сервере пользователя.

5.2.1.2 Как Domino просматривает Domino Directories при поиске.

Инициализация поиска на Notes клиенте происходит, когда пользователь Notes пытается ввести адресата письма. Поиск имен Domino зависит от того, как пользователь сконфигурировал свой документ Место вызова. Последовательность поиска имеет следующий приоритет:

*2174 Персональная адресная книга пользователя, сохраненная локально, на рабочем месте Notes.

*2175 Mobile Directory Catalog, сохраненный на рабочем месте Notes.

Обратите внимание. Если в поле Автонабор имени получателя, установлено значение Локальный компьютер затем сервер, в текущем документе Место вызова, имя для адресации почты ищется сначала в Mobile Directory Catalog, вместо поиска на сервере. Поиск будет продолжен на сервере только тогда, когда пользователь Notes нажимает клавишу - F9, перед отправкой почты.

*2176 Первичный Domino Directory указанный в качестве пользовательского почтового сервера или Directory сервер.

Обратите внимание, что для поиска в первичном Domino Directory, текущего документа Место вызова, в поле Место почтового файла, должно быть установлено значение - На сервере, иначе поиск будет остановлен.

*2177 Directory Catalog, на сервере.

*2178 В каталогах определенных базой данных Directory Assistance.

Инициализация поиска на сервере происходят в следующей последовательности:

*2179 Первичный Domino Directory, на сервере.

*2180 В Directory Catalog, на сервере.

*2181 В каталогах определенных базой данных Directory Assistance.

5.3 Directory Catalogs.

Directory Catalog - объединяет записи о пользователях, группах, почтовых базах данных и ресурсах, из одного или нескольких Domino Directories, в отдельную легкую базу данных, с быстрым доступом. Вы можете использовать User Setup Profile, чтобы создать реплику Directory Catalog на клиентских компьютерах Notes, известных как Mobile Directory Catalog. При этом пользователи Notes могут быстро адресовать почту, любому пользователю Вашей организации, даже когда они отключены от сети. Автоматический поиск просматривает Mobile Directory Catalog быстрее, чем Domino Directory на сервере, уменьшая при этом нагрузку на сеть. Вы можете также создать Directory Catalog на сервере, чтобы сервер мог использовать одну базу данных, чтобы искать имена в нескольких Domino Directories. Типично, Вы создаете два Directory Catalogs: Mobile Directory Catalog и Server Directory Catalog.

Directory Catalog может объединять записи нескольких Domino Directories и быть при этом очень маленьким. Например, несколько Domino Directories, которые содержат, больше чем 350,000 пользователей и имеют общее дисковое пространство в 3GB, при объединении в Directory Catalog, вероятно, будут иметь объем только - 50МБ. Вообще, каждая запись в Directory Catalog занимает - 100 байт.

По умолчанию, в записи Directory Catalog включаются следующие поля, которые требуются для поиска почтовых адресов. Вы можете включать и другие поля в каталог.

Поля, включенные по умолчанию	**Записи, которые используют эти поля**
FullName	Person, Mail-In Database, Resource
ListName	Group
Type	Person, Mail-In Database, Resource, Group
FirstName	Person
MiddleInitial	Person
LastName	Person
Location	Person
MailAddress	Person
Shortname	Person
MailDomain	Person, Mail-In Database, Resource
InternetAddress	Person, Mail-In Database

MessageStorage	Person, Mail-In Database

Чтобы создать Directory Catalog, Вы создаете базу данных Directory Catalog, используя шаблон базы данных - DIRCAT5.NTF. Потом Вы создаете документ конфигурации в этой базе данных, в котором Вы определяете имена файлов Directories, чтобы объединить в каталоге поля, которые Вы включили в каталог и другие опции конфигурации. Сервер, на котором хранится Directory Catalog типично, хранит все реплики Directories, объединенные в каталоге.

После конфигурирования базы Directory Catalog, Вы запускаете задачу Directory Cataloger (DirCat) на сервере, который хранит базу Directory Catalog. Задача DirCat суммирует записи для пользователей, групп, почтовых баз данных и ресурсах планирования, из всех сконфигурированных Domino Directories и объединяет записи в Directory Catalog. Если Вы создаете Mobile Directory Catalog, Вы используете User Setup Profile, для репликации клиентам этой базы Notes. Если Вы построили Server Directory Catalog, реплицируете его на все Domino сервера, чтобы использовать его. Чтобы использовать Server Directory Catalog, Вы должны включить его имя файла, в Public Directory Profile в Server документах.

Запускайте задачу DirCat регулярно, чтобы держать Directory Catalog, в синхронизированном состоянии со всеми Directories. создайте график регулярных репликаций для Directory Catalog клиентам и серверам повсюду в Вашей организации.

5.3.1.1 Mobile Directory Catalog.

При создании Mobile Directory Catalog Вы получите следующие выгоды:

*2182 Пользователи могут иметь доступ к информации в каталоге даже, когда они отключены от сети Notes.

*2183 Когда пользователи адресуют почту, они могут быстро проверять имена любого в Вашей организации. Проверка адреса работает даже, когда пользователи отключены от сети и даже если Ваша организация использует несколько Notes доменов.

*2184 Пользователи могут использовать шифрованную почту, даже, когда они отключены от сети. Почта шифруется позже, когда клиент передает почту на почтовый сервер, в то время, когда клиент посматривает публичный ключ и шифрует почту.

*2185 Имена групп включаются в каталог, так что пользователи могут адресовать почту и группам.

*2186 Автоматический поиск отвечает мгновенно, потому что связь с сервером не нужна.

*2187 Пользователи могут искать адресатов в Directory Catalog тем же самым способом, которым они искали в персональной адресной книге. Например, если пользователь хочет послать почту пользователю с именем Робин в Лос-Анджелесе, но не помнит фамилию Робина, пользователь может искать имя Робин по местоположению - Лос-Анджелес, чтобы найти имя из каталога. LDAP протокол используется для этого поиска.

*2188 Пользователи могут использовать окно диалога почтовой адресации, чтобы открыть и просмотреть имена в Directory Catalog.

*2189 Пользователи могут использовать Soundex поиск, для поиска имен. Эта функция позволяет пользователям вводить записи имен, которые они не знают, как писать.

*2190 Движение в сети уменьшается, потому что решение имен происходит в локальном режиме быстрее, чем на сервере.

Обратите внимание. Создание Mobile Directory Catalog выгоден, даже если Ваша организация использует только один Domino Directory.

5.3.1.1.1 Пример использования Mobile Directory Catalog.

Корпорация Acme состоит из двух Notes доменов, AcmeEast и AcmeWest. Acme создает Mobile Directory Catalog, чтобы сделать его легким в использовании для пользователей во всей организации, для адресации почты. Acme делает все на сервере Mail/West/Acme расположенном в AcmeWest домене.

*2191 Создает реплику AcmeEast Directory

*2192 Постройте первичный Directory Catalog

*2193 Запускает задачу DirCat

Acme реплицирует Directory Catalog на сервер Mail/East/Acme в AcmeEast домене, и клиентам Notes в обоих доменах

Пользователь Notes Susan Salani/HR/West/Acme имеет Mobile Directory Catalog, сохранный на его на локальном компьютере. Когда она посылает почту Phyllis Spera /Sales/East/Acme в AcmeEast домене, Notes использует Mobile Directory Catalog, чтобы проверить адрес почты Phyllis. Подобный процесс происходит, когда Phyllis посылает почту Susan.

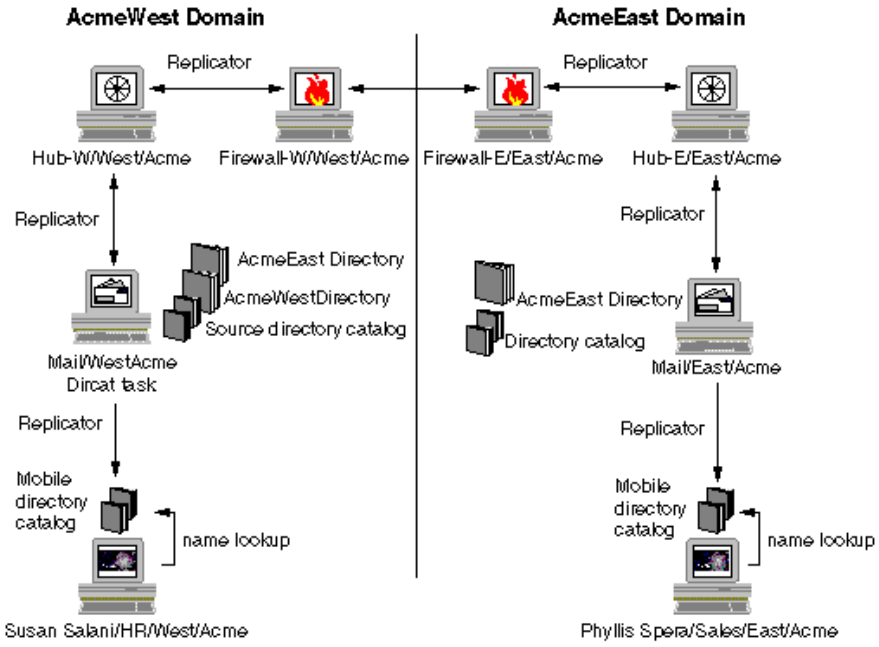


Рис. 88 Пример использования Mobile Directory Catalog.

5.3.1.2 Server Directory Catalog.

Вы можете использовать Server Directory Catalog, чтобы облегчить идентификацию Web клиентов, зарегистрированных во вторичных Domino Directories. Вы можете решать адреса в LDAP каталогах, первичных и вторичных Domino Directories для пользователей Notes, которые не используют Mobile Directory Catalog. Вы можете использовать только один сервер каталога.

Облегчение идентификации Web пользователей.

Когда Web клиенты соединяются с Domino Web сервером, Вы можете использовать опцию Credentials (доверия), во вторичном Domino Directory, чтобы идентифицировать клиентов. Вы используете Directory Assistance, чтобы определить правила обработки имен, которые указывают на название Directory пользователя, при этом Web сервер может идентифицировать клиента.

Server Directory Catalog может работать с Directory Assistance, чтобы облегчить идентификацию Web клиентов. Использование Server Directory Catalog выгодно потому, что Domino может быстро найти имя из вторичного Directory в одной базе данных – Directory Catalog, скорее чем искать в нескольких Directories.

Если Вы используете имя и пароль для Web клиентов, Вы можете хранить пароли в Directory Catalog. Чтобы сделать это, Вы добавляете поле HTTPPassword в конфигурацию каталога. Вы должны все еще использовать Directory Assistance, чтобы определить правила опознания проверки пароля, происходит непосредственно в каталоге, чтобы посмотреть пароль.

Примечание. Вы можете также хранить X.509 сертификаты в Server Directory Catalog, но это увеличивает размер Directory Catalog и поэтому, Lotus не рекомендует делать это.

Расширенный поиск LDAP.

Если Вы используете Domino LDAP сервис, Вы можете установить Server Directory Catalog на том же самом сервере, на котором запущен LDAP. После того, как LDAP сервис проверит первичный Domino Directory, он ищет записи в Directory Catalog даже если поиск был успешен в первичном Domino Directory.

Использование сервера Directory Catalog для решения почтового адреса.

Для пользователей Notes, кто не используют Mobile Directory Catalog, Domino использует Server Directory Catalog на домашнем почтовом сервере пользователя. Начиная с конфигурации по умолчанию, Directory Catalog включает поля, необходимые для решения почтового адреса, Вы не нуждаетесь в Directory Assistance для этой цели.

5.3.1.3 Настройка Directory Catalog.

Чтобы установить Directory Catalog для использования на сервере, или Mobile Directory Catalog выполните эти процедуры.

*2194 Подготовьте сервер к построению Directory Catalog.

*2195 Настройте Directory Catalog.

*2196 Постройте записи Directory Catalog.

Далее делайте одно из следующего:

*2197 Если Вы сконфигурировали Directory Catalog для использования на сервере, реплицируйте Directory Catalog на другие сервера.

*2198 Если Вы сконфигурировали Directory Catalog для использования в мобильном режиме, установите Directory Catalog на клиентах Notes.

*2199 (Рекомендуется) Настройте Directory Assistance.

5.3.1.3.1 Подготовка сервера к построению первичного Directory Catalogs.

Создайте и настройте Directory Catalogs для использования на сервере и рабочих станциях пользователей, на одном и том же сервере.

*2200 Выбирайте сервер, чтобы создать первичный Directory Catalog. Если возможно используйте Hub сервер, для более легкого создания реплик Directory Catalog, после того как Вы установите его. Если Вы включаете несколько Domino Directories в каталог, рассмотрите использование выделенного Directory сервера.

*2201 На сервере, который Вы выбрали, создайте реплики каждого вторичного Domino Directory, который Вы планируете включить в Directory Catalog. Вы должны создать реплики всех каталогов на сервере, назначая им уникальные имена файлов. Directory Cataloger использует реплики вторичных Directories, чтобы строить первичный Directory Catalog. Когда изменения происходят в репликах, задача DirCat обновляет данные первичного каталога Directory Catalog. Как альтернатива создания реплик для вторичных Directories, Вы можете настроить систему для доступа к вторичным Directories по сети. Однако этот подход не рекомендуется, потому что обновление первичного Directory Catalog будет более длинным

*2202 Создайте документ подключения для репликаций между серверами, которые имеют реплики базы данных Directory Catalog, по крайней мере, на одном сервере, в каждом вторичном домене. Расписание репликаций гарантирует, что реплики вторичных Directories всегда находятся в современном состоянии, а данные для построения Directory Catalog всегда будут актуальны.

5.3.1.3.2 Настройки первичного Directory Catalog.

Создайте один первичный Directory Catalog для использования сервером, а другой для использования мобильными пользователями.

Обратите внимание. После того как Вы первоначально построите Source Directory Catalog, а потом измените любые из полей в секции Basics, Directory Catalog, Configuration Settings, за исключением Restrict aggregation to this server, Send Directory Catalog reports to и Comments – после следующего запуска задачи DirCat, каталог будет обновлен полностью. Кроме того, когда Directory Catalog следующий раз будет реплицироваться, например, когда пользователь Notes реплицирует Directory Catalog – полной репликации не происходит. Выполнение полной репликации - более медленный процесс, особенно если она осуществляется по модемному соединению.

Удостоверитесь, что Вы уже подготовили сервер к созданию Directory Catalog.

*2203 Выберите из меню Файл – База данных. Создать.

*2204 Выберите сервер, который Вы подготовили как Source Directory Catalog.

*2205 Введите название каталога. Вы можете использовать любое название.

*2206 Введите имя файла для каталога. Вы можете использовать любое имя файла, например sdc.nsf для Directory Catalog, используемого для серверов, а mdc.nsf для Mobile Directory Catalog.

*2207 Выбирайте опцию - Create full-text index for searching

*2208 Выбирайте сервер шаблона. Выберите сервер, который содержит шаблон DIRCAT5.NTF, а затем щелкают - OK.

*2209 Выберите шаблон для Directory Catalog и затем выбирайте - OK.

*2210 Не выберите шаблон Catalog(5.0) (CATALOG.NTF).

*2211 Установите доступ к базе по умолчанию – Читатель.

*2212 Откройте базу данных, которую Вы только что создали и выбирайте – Создать – Configuration.

*2213 Заполните поле Directories to include. Введите имена файлов вторичных Domino Directories, чтобы включить их в Directory Catalog. Также введите имя первичного Domino Directory (NAMES.NSF), если Вы хотите использовать другой Notes домен, используйте Directory Catalog.

Местоположение вторичных Domino Directory	**Введите**
Локально (рекомендуется)	Имя файла - для примера, EASTNAMES.NSF
Локально в подкаталоге, каталога данных Domino	Имя файла и каталог. **Пример:** `DIRECTORIES\EASTNAMES. NSF`
В сети на смапированом диске	Имя файла и путь. **Пример:** `U:\DIRSERVER\NAMES.NSF`
В сети Domino	Имя файла, синтаксис: portname!!!servername!!filename Где: Portname - имя, которое Вы дали порту Servername – иерархическое имя сервера, который хранит базу данных Domino Directory Filename - имя файла для Domino Directory на сервере **Примера:** TCPIP!!dirserv/east/acme!!names.nsf **Внимание.** Для доступа Domino сервера ко вторичным Domino Directory сохраненных на других Domino серверах, эти Domino сервера должны иметь соответствующие сертификаты или взаимные сертификаты.

*2214 (Необязательно) На закладке Basics, редактируйте поле Additional fields to include, чтобы настроить поля, включаемые в каталог. Лучше не удалять поля из конфигурации по умолчанию, потому что они используются для оптимизированного быстрого адресования почты.

Если Directory Catalog будет использоваться на сервере, добавьте поля AltFullName и AltFullNameLanguage, даже если пользователи не используют альтернативные имена. Также добавьте поле Members, чтобы Directory Catalog мог использоваться его для поиска свободного времени для календарей. Чтобы хранить пароли Web клиентов сервера, в Directory Catalog, добавьте поле HTTPPassword.

Если Directory Catalog будет использоваться как Mobile Directory Catalog, добавьте поля AltFullName и AltFullNameLanguage, только если пользователи используют эти альтернативные имена.

Помните, что Вы можете добавить поле Members, если большинство пользователей хотят искать свободное время своих коллег, когда они работают вне сети. Учтите, что добавление этого поля, увеличивает размер Mobile Directory Catalog, а это в свою очередь увеличит время репликации.

*2215 (Необязательно) В закладке Basics, измените, назначения по умолчанию для этих полей. Убедитесь, что Вы правильно понимаете, настройки для Directory Catalog и понимаете, как он работает с поиском имен прежде, чем Вы изменяете эти назначения.

Поля	**Значения**
Sort by	Выбирайте один из типов сортировки: *2216 Distinguished name (по умолчанию) - если Вы ожидаете, что пользователи будут вводить имена потом фамилии. *2217 Last name – если Вы ожидаете, что пользователи будут вводить фамилии. *2218 Alternate Fullname – если Ваша организация использует альтернативные имена. Если Directory Catalog будет использоваться на почтовом сервере, для оптимизации выполнения работ по передаче почты, оставьте значения поля по умолчанию.
Use Soundex	Выбирайте одно из значений: *2219 Yes - (по умолчанию) помогать пользователю вводить имя, если он не знает, как оно правильно пишется *2220 No – не использовать эту опцию
Remove duplicate users	Выбирайте одно из значений: *2221 Yes - (по умолчанию) чтобы удалять двойные записи при идентичных именах и отображать только первые, с которыми сталкивается Directory Cataloger, согласно порядку в списке Directories в поле Directories to include. *2222 No – заставить пользователя выбирать имена из найденных дубликатов

Group types	Выбирайте одно из значений: *2223 Mail and Multi-purpose (по умолчанию) - включать только эти типы групп в Directory Catalog. *2224 All - чтобы включить все группы в Directory Catalog.
Comments	Введите в любые комментарии

*2225 (Необязательно). Если этот Directory Catalog используется сервером, выбирайте закладку Advanced, для оптимизации настроек

*2226 (Рекомендуется). В поле Restrict aggregation to this server, определяют имя сервера источника, который вы подготовили для Directory Catalog и на котором будет запускаться задача DirCat, для построения Directory Catalog. Если Вы заполняете это поле, когда пользователь пытается запустить задачу DirCat на другой реплике Directory Catalog на другом сервере, сервер возвратит соответствующее сообщение ошибки.

*2227 (Необязательно). В поле Send Directory Catalog reports to, введите имена пользователей и или групп, для получения почтовых сообщений.

*2228 Закройте и сохраните документ.

5.3.1.3.3 Построение и модернизация первичного Directory Catalogs.

После того, как Вы сконфигурировали первичный Directory Catalogs, Вы запускаете задачу DirCat, чтобы обработать его. После первой обработки Directory Catalog, Вы должны наметить ежедневный запуск задачи DirCat, для обновления записей первичного Directory Catalog и синхронизировать его записи с исходными каталогами пользователей.

Задача DirCat суммирует записи из Domino Directories и объединяет записи в совокупные документы первичного Directory Catalog. Каждый совокупный документ содержит поля Directory Catalog, а каждое поле может содержать максимум 255 записей. Записи в совокупных документах сортируются в алфавитном порядке согласно имени по умолчанию.

Скрытое представление $Users хранит совокупные документы. Однако эти документы не предназначены для просмотра. Вы не должны открывать их, поскольку их форматирование будет занимать значительное время.

Первоначально при создании Directory Catalog, задача DirCat тратит приблизительно один час, для каждых 75,000 записей на сервере, с процессором Pentium 200. Последующие обновления будет занимать меньшее количество времени.

Предостережение. Всегда запускайте задачу DirCat на сервере, который хранит Source Directory Catalogs. Если Вы запустите ее на больше чем одном сервере, происходят конфликты репликаций. Используйте поле конфигурации Restrict aggregation to this server, чтобы гарантировать, что задача DirCat запускается только на одном сервере.

Замечание. Вы можете щелкнуть на кнопке Clear History, на закладке Advanced, документа Configurationt, чтобы заново перестроить первичный Directory Catalog в следующий раз, когда будет запущена задача DirCat. Вы можете сделать это, если подозреваете, что Directory Catalog содержит не все записи, или часть записей, кажется Вам устаревшими.

Расписание для автоматического запуска задачи DirCat.

Используйте эти шаги, чтобы наметить расписание выполнение задачи DirCat. По умолчанию, задача запускается ежедневно, каждые 6 часов, с 8 AM до 10 PM.

Удостоверитесь, что Вы уже создали первичный Directory Catalog.

*2229 Из клиента Domino Administrator, выбирайте сервер, который хранит базу данных Directory Catalogs.

*2230 Выбирайте закладку Настройка.

*2231 Выбирайте Server документ

*2232 Переведите Server документ в режим редактирования.

*2233 Выбирайте закладку Server Tasks – Directory Cataloger.

*2234 Заполните эти поля, сохраните и затем закройте документ:

Поля	**Значения**
Directory catalog file names	Имя файла первичного Directory Catalogs.
Schedule	Выбирайте значение – Enabled, для разрешения расписания модернизации

*2235 Если Вы все же не создали Directory Catalog для сервера, или для мобильного использования, выполните эти процедуры:

*2236 Настройте для использования Directory Catalog на сервере.

*2237 Настройте для использования Directory Catalog для мобильной работы.

Запуск задачи DirCat в - ручную.

Если Вы вручную запускаете задачу DirCat, когда она уже запущенна, могут возникнуть конфликты между двумя задачами. Поэтому, если задача DirCat запущена, например согласно графика, Вы должны остановить задачу, прежде чем Вы сможете запустить ее вторую копию вручную.

*2238 Из клиента Domino Administrator, в панели сервера выбирайте сервер, который хранит Directory Catalog.

*2239 Выбирайте закладку Сервер – Состояние.

*2240 Выбирайте кнопку Консоль в верхней части окна, и введите эту команду в командную строку, затем нажмите ENTER

```
tell Dircat quit
```

*2241 После выгрузки задачи, запустите ее снова, следующей командой:

```
load Dircat dc.nsf
```

Где dc.nsf - имя файла первичного Directory Catalog.

5.3.1.4 Настройка использования Directory Catalog на серверах.

Когда Вы построили первичный Directory Catalog для использования серверами, настройте Directory Catalog на серверах, повсюду в Вашей организации. В дополнение к Directory Catalog, мы также рекомендуем, чтобы Вы установили Directory Assistance.

Обратите внимание, что следующие процедуры описывают, как добавить имя файла Directory Catalog для домена в Public Directory Profile. В дополнение, или вместо этого, Lotus рекомендует добавить имя файла Directory Catalog для домена, в документы серверов, которые будет использовать Directory Catalog. Это гарантирует, что сервера могут продолжать использовать сервер Directory Catalog, даже если запись имени файла в Public Directory Profile неосторожно изменяется. Добавьте имя файла Directory Catalog, в поле Directory Catalog filename for this domain on this server, на закладке Basics, Server документа в Domino Directory.

Настройки Directory Catalog на серверах, того же самого домена, что и первичный Directory Catalog.

Удостоверитесь, что Вы уже построили первичный Directory Catalog для использования сервером.

*2242 Создайте реплики Directory Catalog на другие сервера в домене, который будут использовать этот каталог. Используйте то же самое имя файла для каждой реплики. Domino автоматически создает полнотекстовый индекс для каждой реплики.

*2243 Из клиента Domino Administrator, в панели сервер, выбирайте сервер, который хранит реплику Domino Directory.

*2244 Выбирайте закладку Файлы.

*2245 Выбирайте Domino Directory и затем откройте его.

*2246 Выбирайте из меню Действия – Edit Directory Profile.

*2247 В поле Directory catalog file name for domain, введите имя файла, которым Вы выбрали для Directory Catalog. Сохраните и закройте документ.

*2248 Убедитесь, что имеются документы подключений, которые намечают репликации между серверами.

Настройки Directory Catalog на серверах, в разных доменах.

Для настройки серверов, находящихся в разных доменах, повторите шаги описанные выше. Убедитесь, что сервера хранящие первичный Directory Catalog и сервера других доменов, имеют реплики каталога. Если сервера в двух доменах не имеют сертификатов, реплики происходить не будут.

5.3.1.5 Настройки Mobile Directory Catalog.

Если Вы установили и построили первичный Directory Catalog для использования на рабочих станциях пользователей, Вы можете создать User Setup Profile, чтобы создавать Mobile Directory Catalog на клиентах Notes. User Setup Profile исполняет две задачи. Сначала, он создает “окурок” реплики Directory Catalog, в рабочем пространстве каждого пользователя. Во вторых, он добавляет имя файла каталога, к содержанию поля Local address books, в установках пользователя для почты. Если Вы не используете User Setup Profile, каждый пользователь Notes должен вручную исполнить эти две процедуры.

Настройки Mobile Directory Catalog для клиентов того же самого домена, что и сервер хранящий первичный Directory Catalog.

Удостоверитесь, что Вы уже построили первичный Mobile Directory Catalog, для использования сервером.

*2249 Создайте реплики Mobile Directory Catalog на других серверах в домене, который будут использовать этот каталог. Используйте другое имя файла, чем имя каталога для серверов, для каждой реплики. Domino автоматически создает полнотекстовый индекс для каждой реплики.

*2250 Выбирайте закладку Файлы, откройте базу Mobile Directory Catalog.

*2251 Выбирайте из меню Правка – Копировать как связь – с базой данных.

*2252 Из Клиента Domino Administrator, в панели сервер, выбирайте сервер, который хранит реплику Domino Directory, который Вы хотите использовать для профиля установки.

*2253 Выбирайте закладку Пользователи и группы.

*2254 Откройте секцию Профили настройки.

*2255 Сделайте одно из следующего:

*2256 Чтобы изменять существующий User Setup Profile, выберите профиль и выбирайте – Edit Setup Profile.

*2257 Чтобы создавать новый User Setup Profile, выбирайте - Edit Setup Profile и введите имя для профиля в поле названия.

*2258 Выбирайте закладку Databases и затем выбирайте поле Mobile directory catalogs.

*2259 Выбирайте – Правка – Вставить.

*2260 Сделать другие записи в User Setup Profile и затем выбирайте, сохранить и закрыть.

*2261 Когда пользователи затем соединяются с их почтовыми серверами, чтобы подтвердить свою подлинность, они получают реплику профиля с сервера и “окурок” реплики Directory Catalog, с разрешенным графиком репликаций. Пользователи должны регулярно реплицировать их мобильные каталоги с сервера.

Настройки Mobile Directory Catalog для клиентов из другого домена, что и сервер хранящий первичный Directory Catalog.

Для настройки серверов, находящихся в разных доменах, повторите шаги описанные выше. Убедитесь, что сервера хранящие Mobile Directory Catalog и сервера других доменов, имеют реплики каталога. Если сервера в двух доменах не имеют сертификатов, реплики происходить не будут.

5.3.1.5.1 Настройка расписания для запуска задачи обновления Directory Catalogs.

Domino имеет расписание по умолчанию, которое Вы можете использовать для задачи DirCat. График по умолчанию, изменяет записи ежедневно, каждые шесть часов, с 8 AM по 10 PM. Однако Вы можете настроить график расписания по своему усмотрению.

Измените, значения полей на закладке Directory Cataloger, документа сервера.

Поля	**Значения**
Schedule	Выбирайте – Enabled, для разрешения расписания
Run Directory Catalog aggregator at	Диапазон времени, для запуска модернизации Directory Catalog.
Repeat interval of	Интервал повторения запуска
Days of week	Дни недели, для запуска программы

5.3.1.5.2 Добавление и удаление полей из Directory Catalog.

По умолчанию, Directory Catalog предлагает определенный набор полей; Person, Group, Mail-In Database и Resource documents, из Domino Directory. Однако, Вы можете добавлять поля и удалять поля из Directory Catalog. Например, чтобы посматривать пароли Web клиентов в Directory Catalog, используемым сервером, Вы добавляете поле HTTPPassword к каталогу.

Обратите внимание, что Вы не должны добавить это поле к Mobile Directory Catalog.

По умолчанию, конфигурация Directory Catalog включает поля, которые позволяют пользователям быстро адресовать почту. Лучше оставить эти поля без изменения. Вообще, не добавьте много полей, потому что размер Directory Catalog увеличится. Сделайте Directory Catalog как можно меньше, особенно Mobile Directory Catalog. Добавляйте поля только из форм: Person, Group, Mail-In Database и Resource.

Если Вы настраиваете шаблон Domino Directory, используя подформы, чтобы добавить поля к Person или Group, Вы можете добавить некоторые из этих полей в Directory Catalog. Чтобы сделать это, Вы должны сначала копировать и вставить эти подформы в базу данных Directory Catalog. Чтобы избежать ошибки, используйте клиента Domino Designer, для копирования и вставки полей из форм в шаблон Domino Directory.

Вообще, не добавьте поля, которые изменяются часто, это требует что бы Domino часто модернизировал записи в первичном Directory Catalog, а затем реплицировал изменения.

Всегда добавьте поля AltFullName и AltFullNameLanguage, из форм Person, даже если пользователи не используют альтернативные имена. Добавьте поле Members, из формы Group, чтобы позволить пользователям использовать сервер Directory Catalog для поиска свободное времени.

Чтобы добавить или удалить поля в Directory Catalog сделайте следующее:

*2262 Откройте в режиме редактирования базу данных первичного Directory Catalog.

*2263 В поле Additional fields to include добавьте новые поля, или удалите существующие значения.

*2264 Сохраните и закройте документ.

5.3.1.5.3 Оптимизация производительности Directory Catalog.

Назначения по умолчанию для Directory Catalog, полностью оптимизированы для оптимальной производительности.

По умолчанию, каждое поле в совокупном документе хранит до 255 записей из Domino Directories. Это означает, например, что поле FullName в совокупном документе может содержать до 255 записей Domino Directories. Если Вы используете Domino Directories на сервере с LDAP сервисом, этот поиск используют индекс Domino Directories. Если Ваши запросы выполняются медленно, уплотните базу.

Потому что единственное поле, в совокупном документе содержит значения из многих записей, вероятно, что в любой момент каждое поле может требовать обновления, и поэтому нуждается в репликации. Управлять изменениями полей в Domino Directories, Domino, использует возрастающий сливающий процесс, который хранит изменения во временных полях, в совокупных документах до 5 процентов от полного изменения полей. После чего Domino сливает изменения, сохраненные во временных полях, в оригинальные поля, совокупных документов, он удаляет временные поля. Этот процесс происходит беспорядочно, поэтому в любое время, только несколько совокупных документов нуждаются в репликации. Когда Domino Directories реплицируется с клиентом или сервером Domino Directories, только обновленные поля реплицируются. Этот принцип возрастающей репликации, улучшает производительность репликаций, особенно когда репликации происходят по модемному соединению.

Изменения установок производительности.

*2265 Откройте в режиме редактирования базу данных первичного Directory Catalog.

*2266 Выбирайте и открывайте для редактирования документ Configuration, из представления Configuration, базы Directory Catalog.

*2267 Заполните следующие поля на закладке – Advansed, после чего сохраните, и закройте документ.

Поля	**Значения**
Packing density	Максимальное Количество записей в полях документов. По умолчанию - 255.
Incremental fields	Выбирайте одно из двух: *2268 Yes - (по умолчанию) временное сохранение записей во временных полях (Duplicate Fields). *2269 No - сохранение записей сразу в оригинальных полях.
Merge factor	Значение процента, от полного изменения, которые должны произойти, прежде чем Domino сливает изменения сохраненные во временных полях, в оригинальные поля, совокупных документах. По умолчанию - 5 процентов. **Предостережение.** Не изменяйте этот параметр.

5.3.1.6 Мониторинг Directory Catalogs.

Используйте переменную Log_DirCat в файле NOTES.INI, чтобы сделать записи в файле LOG.NSF, когда задача DirCat начинается и заканчивается, и на каком каталоге она запускается.

Почтовое извещение Directory Catalog.

Directory Catalog имеет агента Directory Catalog Status Report. Этот агент отправляет сообщения один раз в неделю людям, которых Вы определили в документе Configuration. Сообщения включает следующее:

*2270 Связи с базой данных Directory Catalog, информацию относительно первичного Directory Catalog, включая название базы данных, местоположение сервера, путь к файлу, размер, число записей и установки конфигурации. Агент получает эту информацию от задачи DirCat.

*2271 Связь с базой данных каждого каталога, содержит информацию о каждом каталоге, включая его название, местоположение сервера, путь к файлу, размер, дата последнего обновления в Directory Catalog.

*2272 Размер первичного Directory Catalog, как процент от размера каталогов. Хотя размер Directory Catalog будет типично очень маленьким, в сравнении с размером каталогов источников, реплицируйте Directory Catalog даже маленький, потому что он не содержит определенное скрытое представление, созданное только в первичном Directory Catalog.

Запуск агента Directory Catalog Status Report:

*2273 Убедитесь, что Вам позволено запускать ограниченных агентов на сервере типа LotusScript/Java.

*2274 Из клиента Domino Administrator, откройте нужный Вам первичный Directory Catalog.

*2275 Откройте документ Configuration в режиме редактирования.

*2276 В поле Send Directory Catalog reports to, введите имена людей и или группы, которые будут получать почтовые сообщения.

*2277 Сохраните и закройте документ.

По умолчанию, агент отправляет сообщениям один раз в неделю, но Вы может изменять этот интервал.

5.4 Настройка сервиса LDAP.

LDAP или Lightweight Directory Access Protocol, является протоколом, который использует TCP/IP, для доступа клиентов к информации из каталога Domino. LDAP определяет стандартный способ поиска и управляет записями в каталоге.

Имя - CN=Phyllis Spera, OU=Sales, OU=East, O=Acme - является именем, которое уникально опознает запись в пределах дерева каталога. Каталог может содержать много типов записей - например, записи для пользователей, групп, устройств, и данных приложений.

Разрешая LDAP сервис на сервере, Вы запускаете LDAP задачу на нем. Клиенты, которые могут использовать LDAP протокол, чтобы соединиться с сервером, могут искать

информацию и записи в Domino Directory, Domino сервера. Вы можете использовать Notes R5 клиента, который имеют экаунт на сервере, клиента Microsoft Outlook Express и Netscape Communicator клиента с сервисом LDAP. Например, LDAP клиент может искать адреса электронной почты, номера телефонов для людей, которых клиент разыскивает.

Domino LDAP сервис поддерживает следующие функции:

*2278 LDAP v3 и v2

*2279 Анонимный доступ к полям, которые Вы определяете

*2280 Расширенный поиск LDAP, во вторичных Domino Directory

*2281 LDAP клиенты могут использовать LDAP каталоги

*2282 Использование LDAP совместимый сервер - типа Netscape Enterprise Web сервер, чтобы идентифицировать пользователей, которые имеют имена и пароли с X.509 сертификатами, сохраненными в Domino Directory на Domino сервере, на котором запущен сервис LDAP.

*2283 Использование LDAP клиентов для добавления, изменения и удаления записей каталога

*2284 Использование базового поиска имен и поиска с использованием альтернативных языков

Domino также поддерживает функции, которые не требуют сервиса LDAP:

*2285 Утилиты командной строки для поиска в каталогах LDAP

*2286 Инструменты миграции, использующихся для импорта записей в LDAP каталог Domino

*2287 Хотя в Domino R5 не входят LDAP API, Вы можете использовать стандарт LDAP C+, Java и JNDI библиотеки.

5.4.1 Как сервис LDAP обрабатывает запросы поиска интернет адреса.

Domino возвращает интернет адрес пользователей зарегистрированных в Domino Directory, LDAP клиентам, как:

*2288 Полный адрес интернета, из списка в одном из этих полей Person документа в следующем порядке:

- Адрес интернета
- Короткое имя - если поле Internet Address Lookup, секции преобразования адреса SMTP Global Domain документа стоит, запрещено - то LDAP сервис не просматривает короткие имена.

*2289 Адрес перенаправления (Forwarding address) - значение этого поля. Однако это значение зависит от выбранной почтовой системы пользователя. Например, значение - Forwarding address может использоваться для Notes почты пользователя.

*2290 Правила, указанные в поле Internet address lookup, Global Domain документа. Если Ваша организация использует больше чем один документ типа Global Domain, Вы должны

выбрать – Yes, в поле Use as default Global Domain, документа Global Domain, который Вы хотите использовать.

*2291 Имя DNS домена, определенное операционной системой Domino сервера компьютера. Синтаксис:

user's hierarchical name%notesdomain@hostname

Например, Randi Bowker/Marketing/East/Acme%Acme@acme.com

Обратите внимание. В Domino R4.62, или ниже, LDAP сервис не может возвращать интернет адреса LDAP клиентам

5.4.2 Установка сервиса LDAP.

Прежде, чем Вы установите Domino LDAP сервис, удостоверитесь, что Вы используете TCP/IP, включая DNS имена хостов и адресование с использованием IP. Установите и настройте Domino сервер.

*2292 Чтобы позволить клиентам соединяться с LDAP сервисом по интернету, соедините Domino сервер, с запущенным сервисом LDAP с интернетом и зарегистрируйте его имя в DNS и адрес IP.

*2293 Создать полнотекстовый индекс для реплики Domino Directory на сервере с сервисом LDAP. Lotus настоятельно рекомендует создать полнотекстовый индекс.

*2294 Запускайте Domino сервер и затем LDAP задачу.

*2295 Если Ваша организация использует больше чем один документ Global Domain, Вы должны определить тот документ, который будет использовать сервис LDAP. Откройте Global Domain документ и поле Use as default Global Domain, выбирайте – Yes.

*2296 Настройте LDAP клиентов.

*2297 (Необязательно) Настраивайте конфигурацию LDAP сервиса, изменяя установки по умолчанию. В большинстве случаев, сервис LDAP функционирует правильно при использовании назначений по умолчанию.

*2298 Чтобы проверять Ваши установки сервиса LDAP, используйте LDAP клиента или утилиту Lsearch, чтобы построить запрос к сервису LDAP.

5.4.2.1 Запуск и остановка сервиса LDAP.

Задача	Решение
Запуск сервиса LDAP автоматически при старте сервера Domino	Редактируйте переменную ServerTasks в NOTES.INI и включите в нее имя задачи LDAP. Domino добавит сервис LDAP по умолчанию в NOTES.INI, если Вы выбрали LDAP сервис при установке сервера.

Ручной запуск сервиса LDAP	Введите команду на консоли сервера: `Load ldap`
Остановка сервиса LDAP	Введите команду на консоли сервера: `Tell ldap quit`

5.4.2.2 Настройка пользователей для использования сервиса LDAP.

Чтобы использовать Domino LDAP сервис, каждый LDAP пользователь Notes или не-Notes, должен настроить клиента для соединения с сервисом LDAP.

Настройка не-Notes LDAP пользователей для соединения с сервисом LDAP.

Настройте не-Notes LDAP пользователя, чтобы соединиться с сервисом LDAP. В LDAP конфигурации клиента определите имя хоста Domino сервера с сервисом LDAP. Например, ldap.acme.com, или IP адрес для сервера. Если Вы хотите, чтобы LDAP пользователь соединялся с использованием имени и пароля, пользователь должен иметь Person документ в первичном Domino Directory. Для LDAP сервиса включите опцию безопасности с использованием пароля пользователя или сертификата клиента.

По умолчанию, LDAP пользователи, которые соединяются с LDAP сервисом, с использованием имени и пароля, могут использовать любое имя из полей FullName или ShortName, Person документа - как LDAP имя клиента. Однако чтобы требовать использования полного имени, определенные в документах RFCS 2251-2254, используется переменная из NOTES.INI - LDAP_STRICT_RFC_ADHERENCE.

Настройка пользователей Notes для соединения с сервисом LDAP.

Чтобы настроить пользователей Notes, для автоматического соединения с сервисом LDAP, Вы создаете или изменяете User Setup Profile. Если Вы не используете User Setup Profile, для настройки пользователей, каждый пользователь Notes, который хочет использовать LDAP сервис, должен создать экаунт, чтобы соединиться с сервером.

*2299 Из клиента Domino Administrator, панели сервера слева, выбирают нужный сервер. Если Вы не видите панели сервера, выбирайте изображение серверов.

*2300 Выбирайте - Пользователи и группы.

*2301 Откройте секцию – Domino Directories, затем выбирайте - Профили настройки.

*2302 Делайте одно из следующего:

*2303 Чтобы изменять существующий Профиль Установки Пользователя, выберите профиль и затем выбирайте – Edit Setup Profile.

*2304 Чтобы создавать новый Профиль Установки Пользователя, выбирайте – Add Setup Profile и введите имя для профиля в поле Profile Name.

*2305 Выбирайте закладку – Accounts и затем заполните поля секции Default Accounts to Internet Servers

Примечание, чтобы создать несколько интернет экаунтов, введите несколько значений, в поля и разделяйте значения запятыми (,).

Поля	**Значения**
Account Names	Наглядное имя для этого экаунта LDAP сервиса. Пользователи видят это имя, когда они хотят использовать LDAP сервис для поиска. Если Вы определяете больше чем один экаунт – например, экаунт для других служб интернета - отделите имена экаунтов запятыми (,).
Server Addresses	Введите имя хоста сервера с запущенным сервисом LDAP Пример: ldap.acme.com.
Protocols	Выбирайте – LDAP Protocol.
Use SSL Connection	Выбирайте - Yes, если Вы используете SSL, если нет – No.

*2306 Заполните другие поля в профиле установки пользователя и затем выбирайте – Сохранить и Закрыть.

5.4.3 Оптимизирование настроек сервиса LDAP.

По умолчанию LDAP конфигурация работает без модификации. Однако Вы можете настраивать LDAP конфигурацию, чтобы удовлетворить Ваши потребности:

2307 Настроить поля, к которым можно получить доступ, используя анонимный доступ, сервиса LDAP

2308 Оптимизировать выполнение поиска LDAP сервисом

*2309 Оптимизировать процесс поиска LDAP сервиса. Вы можете изменять значения TimeOut, чтобы ограничить максимальное число возвращаемых записей, определять минимальное значение знаков для поиска.

2310 Позволить LDAP пользователям добавлять, изменять и удалять записи в Domino Directory

*2311 Настроить процесс обработки LDAP сервисом дублирующихся имен

2312 Разрешить LDAP поиск с использованием альтернативных имен

*2313 Изменить по умолчанию порт и настройки безопасности для LDAP сервиса

*Если Ваша организация использует несколько Domino Directory и Вы используете Directory Assistance во вторичных Domino Directory.

Например, Вы можете позволить LDAP пользователям изменять первичный Domino Directory, LDAP сервиса, но не изменять вторичный Domino Directory.

5.4.3.1 Конфигурирование полей для анонимного доступа LDAP сервиса.

По умолчанию, LDAP пользователи, имеющие анонимный доступ к Domino серверу, могут получить доступ к полям, в Person документах и Group документам, перечисленных в таблице ниже. Кроме того, по умолчанию анонимные LDAP пользователи могут искать поля FullName в Certifier документах.

Обратите внимание, что LDAP клиенты, имеют, по крайней мере, доступ читателя к Domino Directory и могут получить информацию только по документам Domino Directory, созданным по формам: Person, Group, Server, Certifier и форм, которые используют схему Directory Schema.

Поля Person документов.

Имя поля	**Описание поля**
FirstName	Имя пользователя
FullName	Полное имя
LastName	Фамилия
MailAddress	Адрес перенаправления/X.400 адрес/Другой адрес
ShortName	Короткое имя и/или интернет адрес для R4.x SMTP MTA
MailDomain	Домен
Location	Место вызова
InternetAddress	интернет адрес
AltFullName	Альтернативное имя
Certificate	Сертифицированный публичный ключ
PublicKey	Имя простого ключа
UserCertificate	Нет

Поля Group документ.

Имя поля	**Описание поля**
ListName	Имя группы
Members	Члены группы

Вы можете определять различные поля для анонимного доступа. Например, Вы могли бы захотеть анонимным пользователям доступ к полям, в дополнительных документах Domino Directory.

Если Вы используете поиск LDAP, во вторичных Domino Directory, Вы можете использовать эти поля, этих каталогов.

Выбор полей доступных анонимным пользователям сервиса LDAP.

*2314 Из клиента Domino Administrator, выбирайте закладку Настройка.

*2315 В поле Справочник с, выбирайте сервер, который хранит нужную реплику Domino Directory, которую Вы хотите изменить.

*2316 Если имеется документ Configuration Settings, для всех серверов в домене, откройте его в режиме редактирования.

*2317 Если Вы не имеете документа Configuration Settings, для всех серверов в домене, создайте его. Выбирайте кнопку Add Configuration, в поле Use these settings as the default settings for all servers установите опцию Yes.

*2318 Выбирайте закладку LDAP.

*2319 Выбирайте кнопку Choose fields that anonymous users can query via LDAP и сделайте следующее:

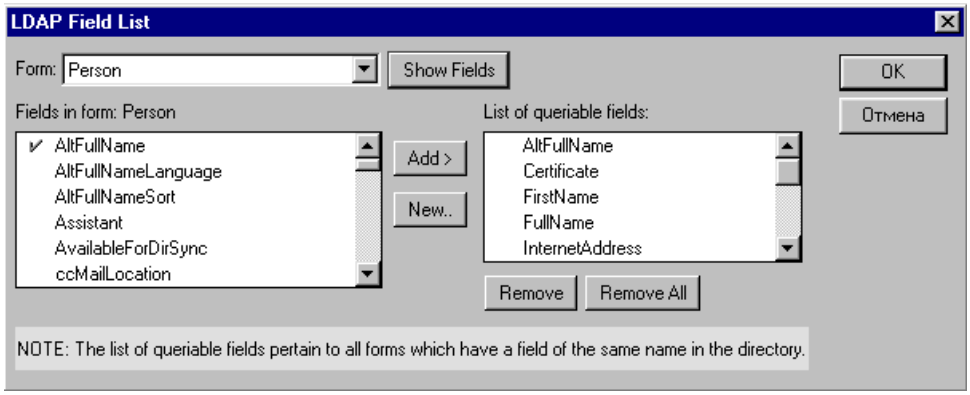


Рис. 89 Диалоговое окно определения полей поиска для LDAP.

- В окне формы, выберите определенную форму или подформу. Выбирайте только формы Person, Group, Server, Certifier, если хотите расширить схему поиска для каталога.

- Выбирайте - Show Fields, чтобы показать в левом окне, связанном с выбранной формой или подформой. Маркер появляется рядом с полями, в настоящее время отобранными для анонимного доступа.

- (Необязательно) Чтобы добавить новое поле к форме или подформы, щелкают на кнопке Новый и введите имя нового поля, затем щелкают - OK.

- Выбирайте поля в левом окне, которое Вы хотите предоставить анонимным пользователям, и затем выбирайте – Add>. Domino добавляет поле в окно List of queriable fields. Если Вы выбираете поле, которое используется в нескольких формах, поле позволяется для всех форм.

- Чтобы удалять поле из окна List of queriable fields, выбирайте поле в окне и Выбирайте – Remove. Чтобы удалять все поля в окне, выбирайте – Remove All.
- Повторите вышеупомянутые шаги для каждой формы или подформы, которую Вы хотите сконфигурировать для анонимного доступа.
- Выбирайте - OK.

*2320 Выбирайте – Сохранить и Закрыть.

*2321 Остановите и перезапустите Domino сервер с запущенным LDAP сервисом.

5.4.3.2 Оптимизация поиска LDAP.

Когда Вы оптимизируете LDAP поиск, Domino строит четыре скрытых представления – $LDAPS, $LDAPG, $LDAPCN, $LDAPHIER - в Domino Directory. LDAP сервис использует эти представления:

*2322 Для поиска по общим именам, фамилиям

*2323 Увеличения производительности на документах созданных по формам, которые были добавлены в Domino Directory

*2324 Позволяется поиск информации в документах Alternate Language Information

*2325 Позволяется LDAP клиентам видеть результаты поиска согласно иерархии имен в дереве каталога, если клиент позволяет делать этого

*2326 Позволяется обработка Server документов.

*2327 Вы можете разрешить выбор Optimize LDAP queries, для определенных серверов или для всех серверов в Notes домене.

*2328 Вы могли бы оптимизировать поиск только на репликах первичных Domino Directory, использующих LDAP сервис. Если Вы используете Directory Assistance, чтобы расширить поиск LDAP во вторичных Domino Directory, Вы могли бы разрешить выбор Optimize LDAP queries, только на репликах вторичных Domino Directory, используемых в Directory Assistance.

Обратите внимание, что разрешение поиска в документах Alternate Language Information, требует, чтобы все сервера домена использовали выбор Optimize LDAP queries. Когда Вы разрешаете использование альтернативного языка, Domino также автоматически позволяет опцию Optimize LDAP queries на всех серверах в домене.

Для оптимизации поиска LDAP, сделайте следующее:

*2329 Из клиента Domino Administrator, в панели сервера, выбирают сервер в домене.

*2330 Выбирайте закладку – Настройка.

*2331 В поле Справочник с:, выбирайте сервер, который хранит нужную реплику Domino Directory, которую Вы хотите изменить.

*2332 Если имеется документ Configuration Settings, для всех серверов в домене, откройте его в режиме редактирования.

*2333 Если не имеется документа Configuration Settings для всех серверов в домене, создайте его. Выбирайте кнопку Add Configuration, чтобы создать новый документ. В поле Use these settings as the default settings for all servers установите опцию – Yes.

*2334 На закладке Basics, в поле Optimize LDAP queries, выбирайте - Yes.

*2335 Выбирайте – Сохранить и Закрыть.

Остановите и повторно запустите каждый Domino сервер, на котором запущен LDAP сервис.

5.4.3.3 Как можно изменять и настраивать процесс поиска LDAP сервиса.

Чтобы улучшить производительность LDAP сервиса, Вы можете настраивать, как служба будет обрабатывать запросы. По умолчанию, LDAP сервис позволяет брать необходимые записи в таком порядке, как она их находит. Если LDAP сервис выполняется медленно, измените значения TimeOut. Вы можете также определить минимальное число знаков, которые пользователи должны использовать перед первым вводом в запросе поиска. По умолчанию - 1 знак. Чем больше количество знаков, тем боле ограничиваются запросы типа Wildcard. Если LDAP сервис выполняет запросы медленно, увеличьте минимальное количества знаков, для поиска Wildcard до двух.

Измените эти назначения в репликах только для первичных Domino Directory – LDAP сервиса.

Изменения настроек процесса поиска LDAP сервиса.

*2336 Из клиента Domino Administrator, выбирайте закладку Настройка.

*2337 В поле Справочник с:, выбирайте сервер, который хранит нужную реплику Domino Directory, которую Вы хотите изменить.

*2338 Если имеется документ Configuration Settings, для всех серверов в домене, откройте его в режиме редактирования.

*2339 Если не имеется документа Configuration Settings для всех серверов в домене, создайте его.

*2340 Выбирайте закладку LDAP.

*2341 Заполните любые из этих полей или измените их значение:

Поле	**Значение**
Timeout	Максимальное время, в секундах, для LDAP запроса клиентов. По умолчанию - 0. Например, определите - 60 секунд.

Maximum number of entries returned	Максимальное число возвращаемых записей Максимальное число записей в Directory, который LDAP сервис, возвращает LDAP клиентам. По умолчанию - 0, означая, что не имеется никакого предела. Например, определите - 100.
Minimum characters for wildcard search	Минимальное число знаков, которые должны ввести, для первого поиска Wildcard запроса; По умолчанию - 1.

*2342 Остановите и повторно запустите каждый Domino сервер, на котором запущен LDAP сервис. Если необходимо, ждите, пока Domino Directory изменит данные в репликах на всех серверах, перед остановкой и рестартом сервера.

5.4.3.4 Настройка действий LDAP сервиса, при нахождении имен дубликатов в документах и в правилах обработки имен из Directory Assistance.

Вы можете сконфигурировать LDAP сервис, для обработки, дублирующихся имен в Domino Directory. Выбор, который Вы определяете, определяет действия службы на запросы:

*2343 Когда дубликат имени найден при попытке удаления или изменения документов

*2344 Когда дубликат имени найден при сравнении двух документов

*2345 Когда дубликат имени найден в правиле базы данных Directory Assistance

*2346 Измените эти назначения в реплике первичного Domino Directory LDAP сервиса.

Определения опций настроек.

*2347 Из клиента Domino Administrator, выбирайте закладку Настройка.

*2348 В поле Справочник с:, выбирайте сервер, который хранит нужную реплику Domino Directory, которую Вы хотите изменить.

*2349 Если имеется документ Configuration Settings, для всех серверов в домене, откройте его в режиме редактирования.

*2350 Выбирайте закладку LDAP.

*2351 В поле Rules to follow when this directory is the primary directory and there are multiple matches on the distinguished name being compared/modified, выбирайте одно из следующего:

- **Don't modify any** (по умолчанию) - чтобы не делать ни каких действий. Выберите этот выбор, если Вы не будете обрабатывать двойные имена. LDAP сервис будет возвращать ошибку, и Вы можете просматривать и анализировать двойные имена.
- **Modify first match** - чтобы выполнить действие на первом имени или в правиле обработке имен.

- **Modify all matches** - чтобы выполнить действие на всех именах или правилах обработки имен.

*2352 Остановите и повторно запустите каждый Domino сервер, на котором запущен LDAP сервис.

5.4.3.5 Разрешение поиска с использованием Alternate Language.

Чтобы разрешить LDAP клиентам исполнять поиск в Alternate Language, Вы можете связывать Person документы с Alternate Language Information документами. Когда Вы создаете Alternate Language Information, документ связывается по признаку, с документом Person. Например, если поле FirstName в Person документе содержит имя Steven, Вы можете создавать документ Alternate Language Information, который использует значение Etienne, для французского языка. Domino хранит документы Alternate Language Information в виде Alternate Language Information, Domino Directory.

Обратите внимание, что в настоящее время клиент Notes и большинство других LDAP клиентов не может определить Alternate Language, в запросах поиска LDAP. Например, если вы ищете первое имя Steven и французское имя Etienne, LDAP клиенты могут получить результаты при поиске имени Etienne, но большинство клиентов не могут получить результат при поиске французского имени Etienne.

Если Вы решили использовать LDAP поиск во вторичных Domino Directory и хотите разрешить поиск, с использованием Alternate Language во вторичных каталогах, Вы должны разрешить просмотр Alternate Language, для вторичных Directory.

Разрешение поиска с использованием Alternate Language.

*2353 Из клиента Domino Administrator, выбирайте закладку Настройка.

*2354 Если не имеется документа Configuration Settings для всех серверов в домене, создайте его.

*2355 Выбирайте закладку LDAP.

*2356 В поле Allow Alternate Language Information processing, выбирайте Yes, затем сохраняют и закрывают документ. Этот выбор, автоматически разрешает опцию Optimize LDAP queries, для всех серверов в домене.

Остановите и повторно запустите LDAP задачу на каждом сервере в домене, на котором запущен LDAP сервис.

Создание документа Alternate Language Information.

Удостоверитесь, что Вы позволили поиск Alternate Language для Вашего Directory.

*2357 Из клиента Domino Administrator выбирайте закладку - Пользователи и группы.

*2358 Открывайте Person документ и затем выберите – Действия – Add Alternate Language Information.

*2359 Выбирайте закладку Basics и сделайте следующее:

*2360 Выбирайте значение для поля Language.

*2361 (Необязательно) Определите значения полей Common name, First name и других полей.

Обратите внимание, что имя пользователя (FullName), наследуется из Person документа. Если Person документ включает один или большее количество альтернативных сертификатов имени, и Вы создаете документ Alternate Language Information, который содержит альтернативный язык, связанный с сертификатом, общее имя в документе Alternate Language Information наследует общее имя.

*2362 Выбирайте закладку Work/Home и затем заполните поля для Work и Home в выбранном документе.

*2363 Выбирайте – Сохранить и Закрыть.

*2364 Повторить эти шаги, для каждого документа Alternate Language Information, который Вы хотите добавить к Person документу.

Примечание. Чтобы просмотреть документы Alternate Language Information, откройте Domino Directory, на закладке Файлы, откройте секцию - People - Alternate Language Information.

*2365 Остановите и повторно запустите каждый Domino сервер, который управляет LDAP сервисом.

5.4.3.6 Изменение значения порта сервиса LDAP и его конфигурирование.

По умолчанию, LDAP клиенты могут соединяться с сервисом LDAP Domino сервера анонимно или с использованием имени и пароля по TCP/IP порту 389. Измените эти назначения, по умолчанию редактируя Server документ для сервера, на котором запущен LDAP сервис.

Для изменения конфигурации порта TCP/IP сделайте следующее:

*2366 Ознакомьтесь с опциями безопасности для TCP/IP.

*2367 Из клиента Domino Administrator, выбирайте закладку Настройка.

*2368 Выбирайте сервер, на котором запущен сервис LDAP, в панели сервера слева.

*2369 Откройте нужный Server документ для редактирования.

*2370 Выбирайте закладки Ports – Internet Ports – Directory.

*2371 Заполните поля:

Поля	**Значение**
TCP/IP port number	Выбирайте - 389 (по умолчанию) для использования сервиса LDAP.
TCP/IP port status	Выбирайте одно из следующего: *2372 Enabled (по умолчанию) - для разрешения LDAP клиентам присоединятся к серверу с использованием TCP/IP *2373 Disabled - запрещение соединений LDAP клиентов.
Authentication options: Name & password	Если в поле TCP/IP port status установлено – Enabled, выбирайте – Yes (по умолчанию), чтобы разрешить LDAP клиентам использовать имя и пароль для идентификации их

Authentication options: Anonymous	Если в поле TCP/IP port status установлено – Enabled, выбирайте – Yes (по умолчанию), чтобы разрешить LDAP клиентам регистрироваться на сервере АНОНИМНО
SSL port number	Выбирайте - 636 (по умолчанию) для использования стандартного значения порта для LDAP при использовании SSL.
SSL port status	Выбирайте одно: *2374 Enabled - LDAP клиентам разрешается соединятся с сервисом LDAP, с использованием SSL. *2375 Disabled - (по умолчанию), запрещение использования SSL.
Authentication options: Client certificate	*2376 Если SSL port status установлен – Enabled, выбирайте – Yes для разрешения LDAP клиентам соединятся с использованием Crtificate Authentication. *2377 Выбирайте – No (по умолчанию), для запрещения использования сертификатов
Authentication options: Name & password	*2378 Если SSL port status установлено – Enabled, выбирайте – Yes для разрешения LDAP клиентам использовать имя и пароль для идентификации *2379 Выбирайте – No (по умолчанию), для запрещения использования имен и паролей для идентификации с использованием SSL.
Authentication options: Anonymous	*2380 Если SSL port status установлено – Enabled, выбирайте – Yes (по умолчанию) разрешение LDAP клиентам присоединения к сервису LDAP только АНОНИМНО. *2381 Выбирайте – No, для запрещения использования анонимной регистрации с использованием SSL.

*2382 Остановите и перезапустите сервер.

5.4.4 Мониторинг сервиса LDAP.

Чтобы показывать число активных сессий LDAP сервиса, используйте эту команду:

```
show tasks
```

Чтобы просмотреть статистику ошибок по TCP/IP порту, используйте эту команду:

```
show port portname
```

Где portname - имя TCP/IP порта LDAP сервиса на Domino сервере. По умолчанию имя порта - TCPIP.

Чтобы показывать статистику LDAP сервиса, используйте эту команду:

```
show stat ldap
```

Статистика сервиса LDAP:

```
LDAP.Total LDAP Connections

LDAP.Simple LDAP Connections
```

```
LDAP.Anonymous LDAP Connections

LDAP.Failed LDAP Connections

LDAP.Total LDAP Searches

LDAP.Longest LDAP Search time

LDAP.Average LDAP Search time

LDAP.Longest LDAP Search request

LDAP.TotalLDAPConnections

LDAP.Total LDAP Modifies

LDAP.Total LDAP Compares

LDAP.Total LDAP Adds

LDAP.Total LDAP Deletes

LDAP.Total LDAP ModifyDNs

LDAP.Total LDAP Extended Operations

LDAP.Total LDAP Abandons

LDAP.Total LDAP Searches for Subschema

LDAP.Total LDAP Searches for Root DSE

LDAP.Sessions.Accept.Queue

LDAP.Sessions.Active

LDAP.Sessions.Inbound.non-SSL

LDAP.Sessions.Inbound.Total

LDAP.Sessions.Incoming.BytesReceived

LDAP.Sessions.Incoming.BytesSent

LDAP.Sessions.Peak

LDAP.Sessions.Threads.Busy

LDAP.Sessions.Threads.Idle

LDAP.Sessions.Total
```

5.5 Directory Assistance

Первый сервер, который был зарегистрирован в домене, содержит Domino Directory и связан с Notes серверами домена. Каждый сервер хранит собственный первичный Domino Directory файл, который называется NAMES.NSF. Directory Assistance - функция, которая позволяет пользователям и серверам использовать информацию из других Directory, которые - не являются первичными для серверов. Вы можете создавать Directory Assistance, для вторичных Domino Directories и для LDAP Directories - например, для Third-Party, LDAP Directories.

Вы создаете базу данных Directory Assistance по шаблону DA50.NTF. Для каждого Directory, который Вы хотите использовать в Directory Assistance, Вы создаете документ Directory Assistance, который описывает Directory и настраивает сервер, чтобы использовать Directory Assistance database.

5.5.1 Вторичные Domino Directories и Directory Assistance.

С точки зрения сервера, любой Domino Directory, который не является первичным для сервера, рассматривается как вторичный Domino Directory. Вторичный Domino Directory может быть связан с другим Notes доменом, или это может быть не принадлежащий ни к какому Notes домену файл.

Вы создаете один документ Directory Assistance, чтобы определить местоположение одного вторичного Domino Directory.

5.5.1.1 Сервер Directory Catalog и Directory Assistance.

Сервер всегда ищет первичный Domino Directory, а затем ищет Directory Catalog на сервере, если Directory Catalog сконфигурирован на сервере, прежде чем используется Directory Assistance. Вообще, лучше создавать на сервере и Directory Catalog и Directory Assistance. Сервер Directory Catalog может выполнять запросы поиска почтовых адресов, только в Directory Catalog и не трогает вторичные Directories.

Каждая запись в Directory Catalog включает в себя реплику ID Domino Directory, из которого был получен UNID для записи. Уникальный ID связан с реплицируемым документом. В случаях, когда Directory Catalog не может выполнить поиск - например, чтобы обработать LDAP поля, не включенные в каталог - сервер использует информацию из Directory Assistance и очень быстро получает доступ к вторичным Domino Directory.

Нет необходимости создавать те же самые вторичные Domino Directories и в Directory Catalog, и в Directory Assistance. Если Вы создаете вторичный Domino Directory в Directory Assistance, а не в Directory Catalog, сервер ищет вторичные Domino Directory, после поиска в Directory Catalog.

5.5.1.2 Идентификация Web клиентов во вторичных Domino Directory.

Когда Web клиенты соединяются с Domino Web сервером, сервер может искать их сертификаты, во вторичных Domino Directory, чтобы идентифицировать клиентов. Когда Вы устанавливаете Directory Assistance для вторичных Directory, Вы определяете одни или более правил обработки имен. Тогда Domino подтверждает подлинность только Web клиентов из Person документов, которые имеют иерархические имена, которые соответствуют правилу обработки имен.

Чтобы идентифицировать Web клиентов, зарегистрированных во вторичных Domino Directory, Вы можете использовать или X.509 сертификаты, или имя и пароль.

После того, как Web сервер идентифицировал Web клиента, сервер не может использовать вторичный Domino Directory, чтобы проверить членство Web клиента в группе. Если Вы используете группы в ACLs базе данных на Web сервере, убедитесь что включили группы в первичные Domino Directory серверов.

Вы не можете идентифицировать других клиентов интернета, зарегистрированных во вторичных Domino Directory - только Web клиентов.

Вы можете также идентифицировать Web клиентов, с сертификатами, в LDAP Directory, например Third-Party, LDAP Directory.

Использование Directory Catalog для идентификации Web клиентов.

Чтобы использовать Directory Catalog и облегчить идентификацию Web клиентов, по крайней мере, одна из реплик вторичного Domino Directory, указанного в документе Directory Assistance, должна иметь реплику Directory Catalog.

Если Вы используете имя и пароль, для идентификации Web клиентов зарегистрированных во вторичных Domino Directory, Вы можете добавить поле HTTPPassword, в документ Directory Catalog Configuration, для хранения паролей в Directory Catalog. Если Directory Catalog хранит пароли, Web сервер не нуждается в доступе ко вторичным Directory.

Хотя Вы можете хранить X.509 сертификаты в Directory Catalog, для идентификации клиентов, делать этого не стоит, Вы значительно увеличите размер Directory Catalog.

5.5.1.2.1 Пример. Как сервер просматривает пароль Web клиента, с использованием Directory Catalog.

Организация Acme использует имя и пароль, для идентификации Web клиентов, которые соединяются с Domino Web сервером, Web/West/Acme. Acme регистрирует Web пользователей и их пароли в Directory - Webusers Directory на сервере Directory-W/West/Acme. Имя Пользователя, находятся в формате ou=Web/ ou=West/ o=Acme. Acme запускает задачу DirCat, строит первичный Directory Catalog, на сервере Directory-W/West/Acme. Конфигурация каталога включает Webusers Directory и дополнительное поле HTTPPassword. Acme создает Directory Assistance документ для Directory Webusers, в базе данных Directory Assistance и включает в документ правило ou=/ ou=/ ou=Web/ ou=West/ o=Acme/ c=*. Это правило гарантирует, что только пользователи, которые зарегистрированы в Directory и имеют имена, которые соответствуют указанному формату, могут быть идентифицированы. В секции Replicas, Directory Assistance документа, Acme определяет реплику Webusers Directory на сервере Directory-W/West/Acme.

Acme реплицирует Directory Catalog и базы данных Directory Assistance на сервер Web/West/Acme. Acme не делает реплик Webusers Directory.

Когда Web пользователь Linda Bell, соединяется с сервером Web/West/Acme. Сервер делает следующее:

*2383 Ищет запись пользователя в реплике Directory Catalog, для Linda Bell.

*2384 Определяет имя как Linda Bell/Web/West/Acme, используя информацию из Directory Catalog.

*2385 Использует информацию из Directory Catalog, чтобы решить, что запись для Linda Bell/Web/West/Acme в каталоге, получена из реплики Webusers Directory на сервере Directory-W/West/Acme.

*2386 Ищет документ Directory Assistance, для Webusers Directory, в реплике базы данных Directory Assistance.

2387 Видит правило ou=/ ou=/ ou=Web/ ou=West/ o=Acme/ c=, которому доверяет для идентификации клиентов и решает, что имя Linda Bell/Web/West/Acme соответствует этому правилу.

*2388 Видит, что реплика Webusers Directory, которая определена в документе Directory Assistance, соответствует реплике, из записи которой Linda Bell в каталоге был получен.

*2389 Смотрит в Directory Catalog, на Web/West/Acme, чтобы проверить пароль Linda Bell.

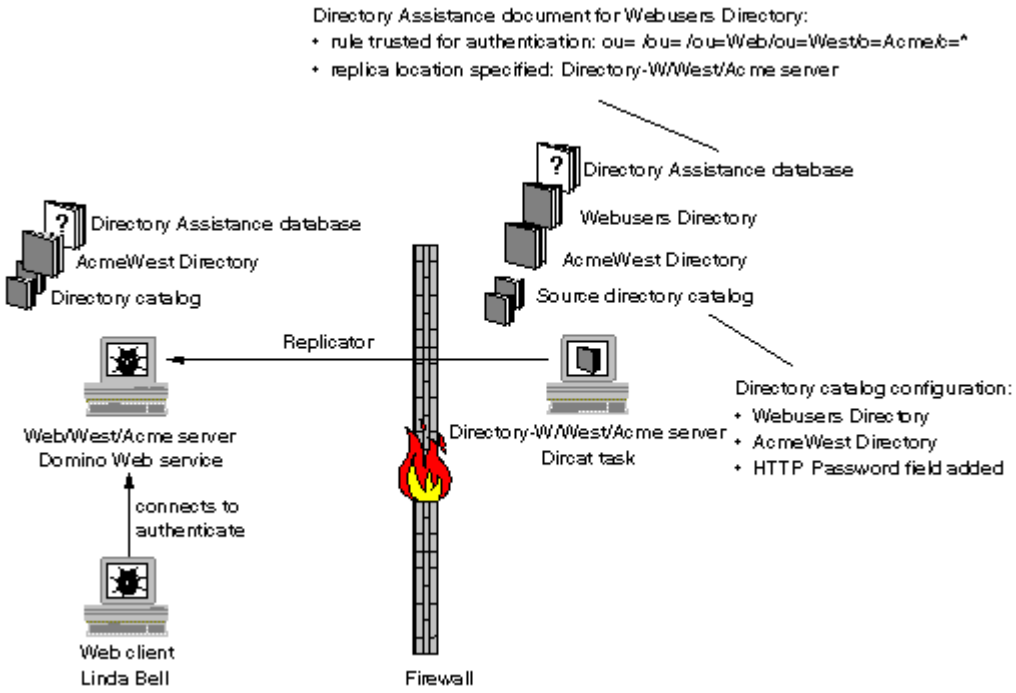


Рис. 90 Логика поиска пароля Web пользователя, сервером, с использованием Directory Catalog.

5.5.1.2.2 Пример просмотра сертификата Web клиента, во вторичном Domino Directory.

В этом примере, организация Acme использует X.509 сертификаты, чтобы идентифицировать Web клиентов, которые соединяются с Domino Web сервером, Web/West/Acme. Acme регистрирует Web пользователей и их сертификаты, в Directory Webusers Directory на сервере Directory-W/West/Acme. Имена Web пользователей находятся в формате ou=Web/ ou=West/ o=Acme. Acme реплицирует Webusers Directory на Web/West/Acme сервер.

Acme запускает задачу DirCat, для строительства первичного Directory Catalog на сервере Directory-W/West/Acme. Конфигурация каталога включает Webusers Directory и AcmeWest Directory. Acme реплицирует и устанавливает Directory Catalog, на сервер Web/West/Acme.

Acme создает документ Directory Assistance для Webusers Directory, в базе данных Directory Assistance и включает в документ правило ou=/ ou=/ ou=Web/ ou=West/ o=Acme/ c=*, которому “доверяет” для идентификации. Это правило определяет, что только пользователи, которые зарегистрированы в Directory, с именем в этом формате, могут быть идентифицированы. В секции Replicas, документа Directory Assistance, Acme определяет две реплики Webusers Directory: реплика на Directory-W/West/Acme и на сервере Web/West/Acme.

Когда Web пользователь Alan Kenny, соединяется с Web/West/Acme. Сервер делает следующее:

*2390 Пробует найти имя Alan Kenny и X.509 сертификат клиента в первичном Domino Directory, AcmeWest Directory, но не находит имя.

*2391 Находит имя Alan Kenny в реплике Directory Catalog.

*2392 Используя информацию из каталога, решает, что запись для Alan Kenny/Web/West/Acme в каталоге получена из реплики Webusers Directory на Directory-W/West/Acme.

*2393 Используя информацию из каталога, просматривает документ Directory Assistance, для Webusers Directory в реплике базы данных Directory Assistance.

2394 Видит правило ou=/ ou=/ ou=Web/ ou=West/ o=Acme/ c=, в документе Directory Assistance, которому “доверяют” для идентификации и решает, что имя Alan Kenny/Web/West/Acme соответствует этому правилу.

*2395 Находит, что в одной из реплик Webusers Directory, указанная в документе Directory Assistance, есть запись для Alan Kenny.

*2396 Использует реплику Webusers Directory на Web/West/Acme сервере, указанную в документе Directory Assistance, чтобы найти Person документ, для Alan Kenny, который содержит иерархическое имя Alan Kenny/Web/West/Acme.

*2397 Сравнивает X.509 сертификат, сохраненный в Webusers Directory, чтобы проверить сертификат.

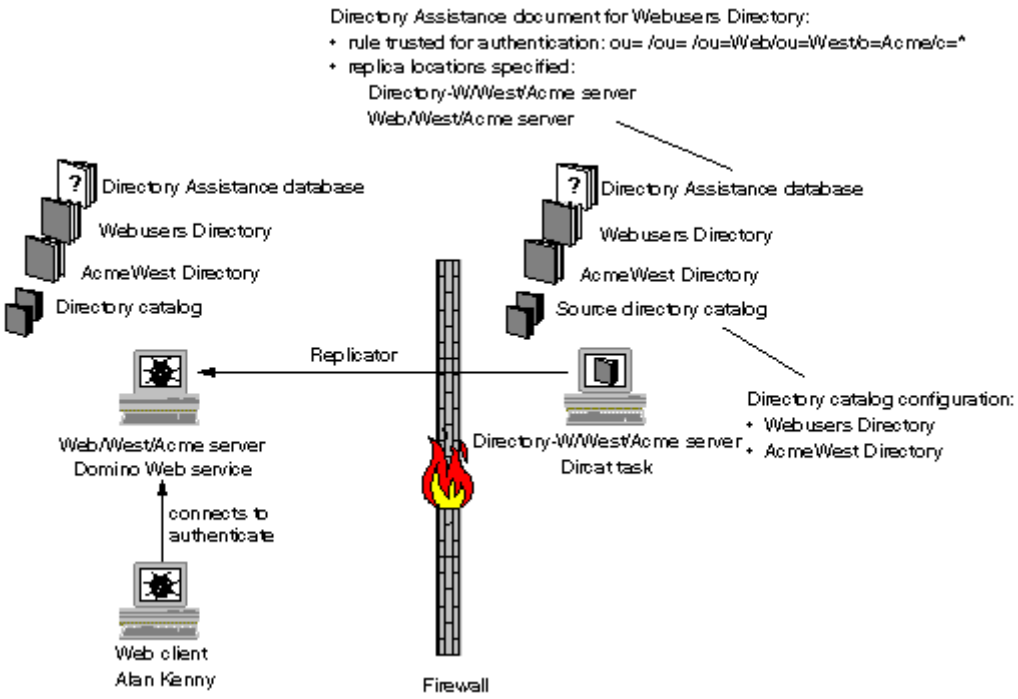


Рис. 91 Логика поиска сертификата Web пользователя, сервером, во вторичном Domino Directory.

5.5.1.3 Поиск LDAP, во вторичных Domino Directory.

Если один или большее количество Ваших серверов имеют LDAP сервис, Вы можете настроить Directory Assistance, чтобы расширить поиск во вторичных Domino Directories. Тогда, когда LDAP клиент начинает поиск, LDAP сервис может искать информацию во вторичных Domino Directories.

Вы можете использовать Directory Catalog вместе с Directory Assistance. При этом если Directory Catalog не удовлетворяет поиск, LDAP сервис использует Directory Assistance, чтобы искать во всех вторичных Directories. Если Вы используете сервис Directory Catalog, включаете поля, которые LDAP клиенты ищут наиболее часто.

LDAP поиск распространяется на Directory Catalog, и или Directory Assistance, даже когда первичный LDAP сервер Domino Directory удовлетворяет запрос клиента.

5.5.1.3.1 Пример расширенного поиска LDAP во вторичных Domino Directory.

Корпорация Acme запускает LDAP сервис на Domino сервере Directory-W/West/Acme. Пользователи Acme использующие LDAP клиентов, соединяются с сервером, чтобы искать AcmeWest Directory, который является первичным сервером Domino Directory.

Чтобы позволить LDAP поиск клиентам в AcmeEast Directory, Acme создает документ Directory Assistance типа Notes, для Directory. Acme определяет сервер Directory-W/West/Acme как место хранения реплики Directory. Имя пользователя AcmeEast Directory, находятся в формате ou=East/ o=Acme, поэтому, Acme использует это правило решения имен для документа Directory Assistance, для AcmeEast:

```
ou=/ ou=/ ou=/ ou=East/ o=Acme/ c=*
```

Acme запускает задачу DirCat и строит первичный Directory Catalog на сервере Directory-W/West/Acme. Конфигурация каталога включает в себя AcmeEast Directory и AcmeWest Directory.

LDAP пользователь Barbara Fischer соединяется с сервером Directory-W/West/Acme и ищет адреса электронной почты для всех записей, которые соответствуют имени Alex Davidson. Имеется Alex Davidson/West/Acme, зарегистрированный в AcmeWest Directory и Alex Davidson/East/Acme, зарегистрированный в AcmeEast Directory. Чтобы закончить поиск, Directory-W/West/Acme сервер действует следующим образом:

*2398 Ищет AcmeWest, первичный Domino Directory и находит запись для Alex Davidson/West/Acme и адрес электронной почты.

*2399 Ищет Directory Catalog и находит запись каталога для Alex Davidson/East/Acme и адрес электронной почты.

*2400 Возвращает адреса электронной почты двух пользователей, записями Barbara Fischer.

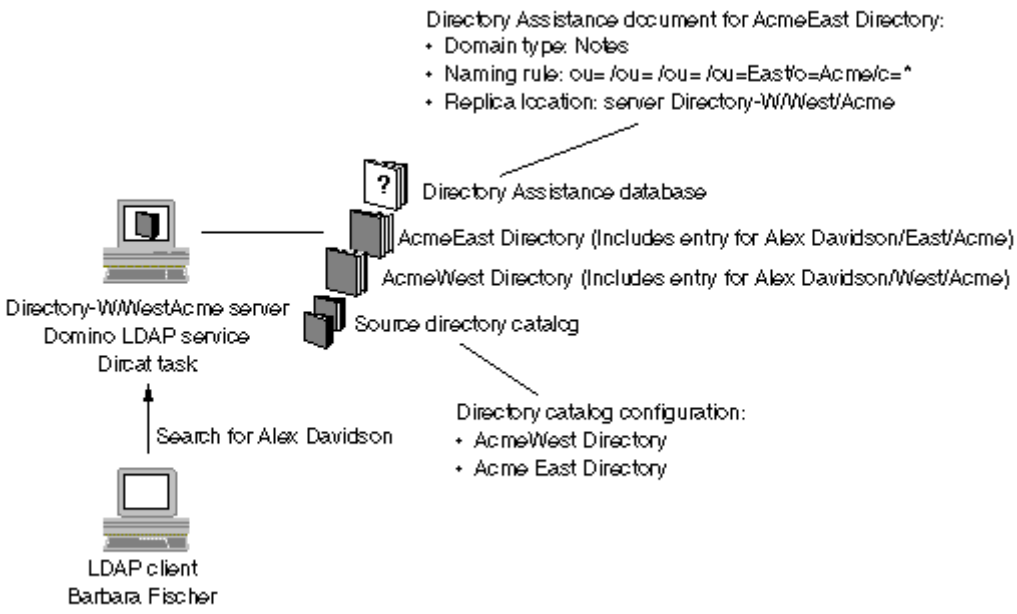


Рис. 92 Логика расширенного поиска LDAP во вторичных Domino Directory.

5.5.1.4 Проверка адреса Notes во вторичных Domino Directory.

Чтобы проверить имя для адресации Notes почты, когда пользователь Notes вводит адреса и нажимает клавишу F9, Notes просматривает первичный Domino Directory на почтовом сервере пользователя или сервер каталога. Вы можете сконфигурировать Directory Assistance, чтобы клиентам Notes позволялся поиск имен и во вторичных Domino Directory.

Как альтернатива использования Directory Assistance, Вы можете использовать Mobile Directory Catalog и или Server Directory Catalog. По умолчанию конфигурация Directory Catalog включает в себя все поля, необходимые для решения почтового адреса, если Вы используете Directory Catalog, если Вы не используете Directory Assistance для решения почтовых адресов.

Для пользователей Notes, чтобы воспользоваться преимуществом Directory Assistance или Server Directory Catalog для проверки, вы должны выбрать в поле Место почтового файла - значение На сервере, для активных документов Место вызова.

5.5.2 Разрешение поиска в LDAP Directories из Directory Assistance.

LDAP или Lightweight Directory Access Protocol, является стандартным протоколом, используемым для сервиса каталогов TCP/IP. Вы можете настроить Directory Assistance для доступа к LDAP-совместимым каталогам. LDAP Directory могут располагаться как на серверах, с запущенным Domino LDAP сервисом, так и на других серверах поддерживающих LDAP Directory сервисы ...

Установки Directory Assistance, для LDAP Directories:

*2401 Используйте сертификат в LDAP Directories, чтобы идентифицировать Web клиентов, которые используют Domino Web сервер.

*2402 Проверите членство в группах, зарегистрированных в LDAP Directory.

*2403 Определите LDAP клиентов, которые соединяются с Domino LDAP сервисом.

*2404 Позволите пользователям Notes проверять почтовые адреса пользователей в LDAP Directories.

Используйте один документ Directory Assistance, для одного определенного Вами LDAP Directory. Если это необходимо, создайте несколько документов Directory Assistance.

5.5.2.1 Идентификация Web клиентов из LDAP Directory.

Вы можете настроить Directory Assistance так, чтобы Domino Web сервер мог идентифицировать Web клиентов, чьи сертификаты сохранены в LDAP Directory. Например, если Ваша организация регистрирует пользователей в Third-Party, LDAP Directory, когда пользователи соединяются с Domino Web сервером, сервер может посматривать имена пользователей, пароли или сертификаты в этих LDAP Directory. Web сервер не должен иметь сервис Domino LDAP, он только должен быть способен установить связь по сети с сервером LDAP Directory.

Когда Вы настаиваете Directory Assistance, для использования LDAP Directory, чтобы идентифицировать Web пользователей, мы настоятельно рекомендуем, чтобы Вы сконфигурировали документ Directory Assistance использовать X.509 сертификат, для идентификации сервером LDAP Directory.

Вы не можете идентифицировать других клиентов интернет, зарегистрированных в LDAP Directory - только Web клиентов.

5.5.2.1.1 Пример использования LDAP Directory для идентификации Web клиентов

Предположим, что корпорация Acme регистрирует пользователей в Third-Party, LDAP Directory ldap.acme.com. Когда Web клиенты соединяют с Domino Web сервером Web/Acme, сервер использует X.509 сертификаты, сохраненные на ldap.acme.com, для идентификации этих пользователей. Имена Web пользователей зарегистрированных на ldap.acme.com, находятся в формате ou=Web, o=Acme.

Acme создает документ Directory Assistance для ldap.acme.com, на сервере Web/Acme. Acme включает правило ou=/ ou=/ ou=/ ou=Web/ o=Acme/ c=*, которому доверяет. Acme позволяет SSL шифрование канала, в документе Directory Assistance, чтобы гарантировать, проверку идентичности ldap.acme.com.

Когда Web пользователь Karen Wright, зарегистрированный на ldap.acme.com как cn=Karen Wright, ou=Web, o=Acme, соединяет с Domino сервером Web/Acme, сервер делает следующее:

*2405 Просматривает имя и зарегистрированный X.509 сертификат, в первичном Domino Directory, AcmeWeb Directory, но не находит имя.

*2406 Находит документ Directory Assistance для ldap.acme.com.

2407 Видит, правило ou=/ ou=/ ou=/ ou=Web/ o= Acme/ c=, доверяет ему, для установления подлинности.

*2408 Соединяется с ldap.acme.com и находит имя cn=Karen Wright, ou= Web, o=Acme, в каталоге ldap.acme.com.

2409 Найденное доверительное правило ou=/ ou=/ ou=/ ou=Web/ o=Acme/ c=, в документе Directory Assistance, для ldap.acme.com и подтверждает, что запись, найденная для Karen Wright соответствует правилу.

*2410 Сравнивает X.509 сертификат, сохраненный на ldap.acme.com.

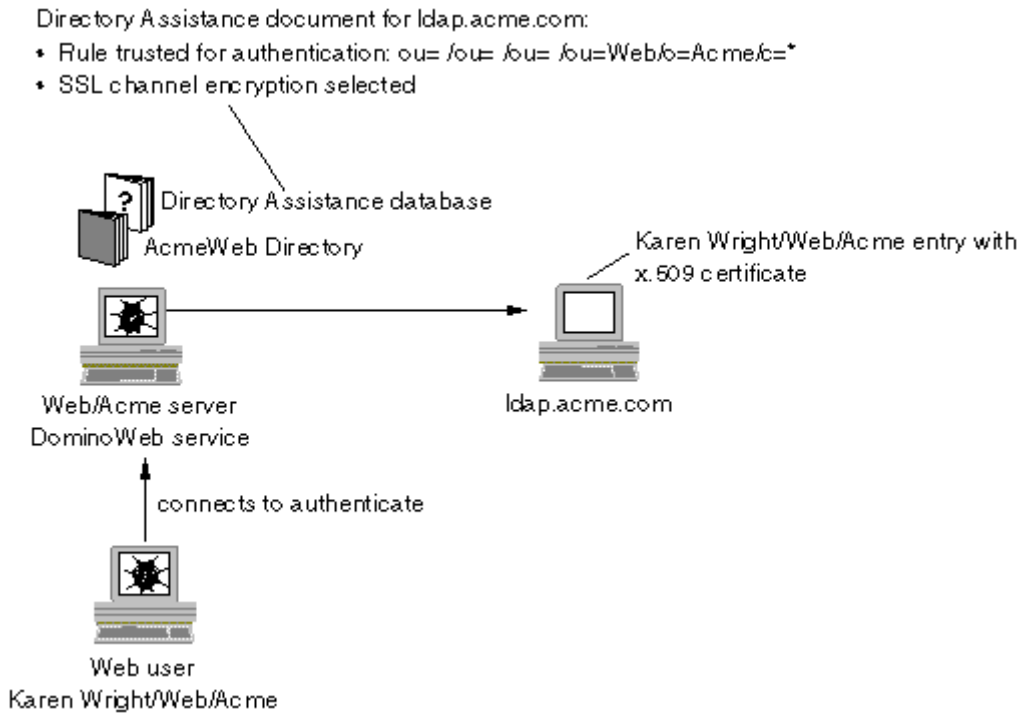


Рис. 93 Логика использования LDAP Directory для идентификации Web клиентов.

5.5.2.2 Использование групп пользователей с LDAP Directory.

Вы можете вводить имена групп, зарегистрированных в LDAP Directory, в ACL баз данных на Domino серверах, для использования с Directory Assistance. При этом, когда Notes или Web пользователи пытается открыть базы данных на сервере, сервер будет искать группы в каталогах LDAP Directory. Сервера, которые используют Directory Assistance, не должны управлять сервисом LDAP, они должны уметь связываться по сети с сервером LDAP Directory.

Чтобы искать группы в LDAP Directory, Вы создаете для LDAP, документ Directory Assistance, выбираете – Yes в поле Group expansion, разрешаете по крайней мере одно правило обработки имен для группы, которому Вы доверяете для идентификации.

Также можно писать Notes API программы, которые использует эту особенность, чтобы посматривать членов групп в LDAP Directory.

Вы можете запрашивать поиск группы в только одном LDAP Directory.

5.5.3 Правила обработки имен в Directory Assistance.

Когда Вы создаете документ Directory Assistance, в базе данных Directory Assistance, Вы определяете один или большее количество правил, которые соответствуют иерархическим именам записей в Directory. Directory Assistance использует правила, чтобы определить порядок поиска в Directories, когда пользователи вводят иерархические имена, и имеется несколько конфигураций в Directory Assistance.

Вы можете использовать Directory Assistance, чтобы переопределять LDAP клиентов, которые используют Domino LDAP сервис на другие LDAP Directory, когда клиент ищет имена, по дереву каталогов.

Вы также используете правила обработки имен, чтобы идентифицировать Web клиентов, зарегистрированных во вторичных Domino Directory или LDAP Directory. Когда Вы создаете правило, Вы устанавливаете опцию “доверять” этому правилу. Использование “доверия” правилу гарантирует, что Domino подтверждает подлинность только пользователей, которые имеют имена в Directory, которые соответствуют правилу.

Когда пользователи вводят общие имена или иерархические имена, которые соответствует больше чем в одном документу Directory Assistance, Directory Assistance решает в каком каталоге искать, согласно порядку поиска, назначенному каждому каталогу.

Обратите внимание, когда Вы устанавливаете Directory Catalog для использования на сервере, Directory Assistance не должен искать адреса в нескольких вторичный Domino Directories, потому что сервера могут находить записи в Directory Catalog.

Перечисление правил использует X.500, различные модели имен, которые назначаются Organizational Units, Organization и компоненты страны. Каждый компонент правила должен содержать один из следующего:

*2411 Имя для компоненты - например, для компонента организации Acme

*2412 Звездочка (*) - чтобы включить все названия на определенном уровне иерархии имен

*2413 Пробел - чтобы исключить имена на определенном уровне иерархии имени

Следующая таблица содержит примеры правил и иллюстрирует, как каждое правило включает или исключает эти имена:

```
Marilyn Jenkins/Omega

Alan Jones/Sales/East/Acme

Randi Bowker/Marketing/East/Acme

Cheryl Lordan/IS/West/Acme

Derek Malone/Accounting/West/Acme

Deborah Jones/West/Acme
```

Пример	**Выбор**	**Исключение имен**
//*/*/*/*	Все Имена и Directory	Нет
//*/*/Acme/*	Alan Jones/Sales/East/Acme Randi Bowker/Marketing/East/Acme Cheryl Lordan/IS/West/Acme Derek Malone/Accounting/West/Acme Deborah Jones/West/Acme	Marilyn Jenkins/Omega

//*/West/Acme/*	Cheryl Lordan/IS/West/Acme Derek Malone/Accounting/West/Acme Deborah Jones/West/Acme	Marilyn Jenkins/Omega Alan Jones/Sales/East/Acme Randi Bowker/Marketing/East/Acme
//IS/West/Acme/*	Cheryl Lordan/IS/West/Acme	Marilyn Jenkins/Omega Alan Jones/Sales/East/Acme Randi Bowker/Marketing/East/Acme Derek Malone/Accounting/West/Acme Deborah Jones/West/Acme
//*/West/Acme/*	Deborah Jones/West/Acme	Marilyn Jenkins/Omega Alan Jones/Sales/East/Acme Randi Bowker/Marketing/East/Acme Derek Malone/Accounting/West/Acme Cheryl Lordan/IS/West/Acme

5.5.4 Порядок поиска в Directory Assistance.

Иногда при использовании поиска в Directory Assistance, с использованием общего или иерархического имя, имя может соответствовать нескольким правилам обработки, больше чем в одном документе Directory Assistance. Вы можете определять порядок поиска в документах.

Пример. Если следующее истина:

*2414 Имеются Domino Directory, для Notes доменов AcmeEast и AcmeWest. Имеется два определенных Вами правила */*/Sales/East/Acme/*

*2415 Для AcmeWest Directory определено значение приоритета поиска - 2

*2416 Для AcmeEast Directory определено значение приоритета поиска - 3

В этом случая Directory Assistance ищет пользователя Alan Jones/Sales/East/Acme сначала в AcmeWest Directory, а затем в AcmeEast Directory.

Если Вы не определяете порядок поиска, или если Вы назначаете одно значение приоритета поиска двум Domino Directory, Directory Assistance просматривает каталоги пользователей в алфавитном порядке, согласно именам, указанным в поле Domain Name каждого документа Directory Assistance.

Представление Directory Assistance, из базы данных Directory Assistance, всегда показывает текущий порядок поиска в Directories.

5.5.5 Создание базы данных Directory Assistance.

Чтобы создать базу данных Directory Assistance для Notes домена, создайте базу данных на одном из серверов домена. Создайте реплики этой базы данных на всех серверах Вашего домена. Используйте для базы шаблон DA50.NTF. Создайте документы подключений, чтобы наметить репликации баз данных на всех серверах.

5.5.5.1 Идентификация базы данных Directory Assistance на серверах.

Чтобы настроить сервера для использования Directory Assistance, добавьте имя файла базы данных Directory Assistance, в Server документы базы данных Domino Directory. Вы можете вручную ввести имя файла баз данных Directory Assistance в Server документ, или использовать для этой цели процесс администрирования (Process Administration). Administration Process создает запрос Set Directory Assistance database, который копирует имя файла Directory Assistance, в поле Directory Assistance database name из Servers документов.

Для определения базы данных на сервере или серверах сделайте следующее:

*2417 Удостоверитесь, что Вы сделали это:

- Создали и реплицировали базу данных Directory Assistance.
- Имеете доступ автора и роль ServerModifier, или доступ редактора в Domino Directory, к которому Вы хотите добавить имена файла.
- Уже основали Administration Process.

*2418 Из клиента Domino Administrator, выбирайте закладку Настройка.

*2419 Выбирайте Server документы для серверов, которые будут использовать Directory Assistance. Маркируйте эти документы.

*2420 Из меню Действия, выбирайте опцию Set Directory Assistance Information.

*2421 Введите имя файла, которое Вы дали базе данных Directory Assistance на этих серверах - например, DA.NSF. Если база данных Directory Assistance находится в подкаталоге, введите путь, например DIRECTORIES\DA.NSF и выбирайте - OK.

*2422 Повторите эти шаги для каждого набора серверов, которые используют те же самые имена файлов и путь к ним для реплик баз данных Directory Assistance.

5.5.6 Настройка Directory Assistance, для использования вторичных Domino Directory.

После того, как Вы создаете и настраиваете базу данных Directory Assistance, для настройки Directory Assistance, для вторичных Domino Directory, сделайте следующее:

*2423 Определите место хранения реплик вторичных каталогов пользователей.

*2424 Разрешите серверам и пользователям доступ к выбранным вторичным Directory.

*2425 Создайте документы Directory Assistance для вторичных Domino Directory.

*2426 (Рекомендуется) Установите Directory Catalog на серверах, которые используют Directory Assistance.

5.5.6.1 Планирование места хранения реплик вторичных Domino Directory.

Чтобы осуществлять поиск во вторичных Domino Directory, Directory Assistance должен знать расположение реплик Directory. Поэтому, прежде, чем Вы создаете документы Directory Assistance для вторичных Domino Directory, решаете где хранить реплики вторичных Domino Directory.

Если сервера Вашего домена и вторичные домены связаны медленным соединениями WAN или модемом, создайте реплики вторичных Domino Directory на одном из серверов в домене. При создании реплик в Вашем домене гарантирует, что поиск в Directory происходят быстро.

Если Ваши сервера и вторичном домены связаны быстрыми WAN соединениями или LAN связью, Вы можете не создавать реплики вторичных Directory в своем домене. Вместо этого, Вы можете создать Directory Assistance, с доступом к вторичным Directory, на сервере во вторичном домене.

Расширенные функции для одной реплики вторичного Directory.

В документе Directory Assistance, Вы можете определить больше чем одну реплику для вторичного Domino Directory. Тогда, если одна реплика будет недоступна, Directory Assistance может искать данные в другой реплике. Если Вы определяете больше чем одну реплику вторичного Directory, Directory Assistance ищет реплики, в той же самой поименованной сети Notes. Если поиск неудачен, сервер ищет реплики в том же самом домене Notes. Если местоположение не найдено, сервер использует первую реплику, указанную в документе Directory Assistance.

Обратите внимание. Если Вы определяете реплику вторичного Directory, которая находится в кластере серверов, Directory Assistance будет автоматически перенаправлять пользователей к другой реплике Directory в кластере, при перегрузке указанного сервера в кластере. Вы должны явно конфигурировать все реплики в пределах кластера, которые Вы хотите использовать в Directory Assistance.

5.5.6.2 Разрешение доступа к Domino Directory.

После того как Вы решаете где расположить реплики вторичных Domino Directory, которые Вы хотите включить в Directory Assistance, Вы должны удостовериться что сервер в домене имеет доступ к нему.

*2427 Удостоверитесь каждый сервер использующий Directory Assistance:

- имеет доступ к каждому серверу, который хранит реплику вторичного Directory.
- имеет, по крайней мере, доступ читателя, в ACL каждой реплики вторичного Directory.

*2428 (Необязательно) позвольте пользователям Notes, просмотр и выбор имен из Directory. Удостоверитесь, что каждый пользователь:

- Имеет доступ к каждому серверу, который хранит реплику вторичного Directory.
- Имеет, по крайней мере, доступ читателя в ACL каждой реплики вторичного Directory.

Обратите внимание, что пользователи Notes могут использовать клавишу F9, или вводить адреса по буквам, чтобы решать адреса пользователей во вторичном Directory.

5.5.6.3 Создание документа Directory Assistance для вторичного Domino Directory.

Если Вы планируете использовать вторичный Domino Directory, чтобы идентифицировать Web клиентов, настройте для этого Directory Assistance.

Если Вы используете сервер Directory Catalog, создайте Directory Catalog, чтобы включить в него вторичные Domino Directory. Если Вы используете имя и пароль для идентификации Web клиентов, зарегистрированных в Directory, и Вы хотите хранить пароль в Directory Catalog, добавьте поле HTTPPassword, в документ конфигурации Directory Catalog.

Если Вы хотите использовать LDAP поиск в первичном Domino Directory, создайте полнотекстовый индекс, используемого Directory Assistance. Также произвольно делайте любые настройки LDAP конфигурации для этого каталога:

*2429 Определите поля для анонимного доступа пользователей с использованием сервиса LDAP

*2430 Оптимизируйте поиск реплик Directory, используемых в Directory Assistance

*2431 Позволите LDAP пользователям добавлять, изменять и удалять записи в Directory.

*2432 Позволите LDAP пользователям поиск, с использованием альтернативных языков

Обратите внимание, если вы разрешаете LDAP клиентам изменять записи во вторичном Domino Directory, не используйте Directory Catalog на Domino сервере, на котором запущен LDAP сервис.

*2433 Для создания документов Directory Assistance, из клиента Domino Administrator выбирают сервер, который хранит базу данных Directory Assistance.

*2434 Откройте базу данных Directory Assistance.

*2435 Выбирайте – Add Directory Assistance.

*2436 На закладке Basics заполните поля:

Поле	**Значение**
Domain Type	Выбирайте Notes
Domain Name	Имя Notes домена связанного с вторичным Directory. Имя домена должно отличаться от первичного Notes домена и от всех других доменов в конфигурации Directory Assistance. Если вторичный Directory не связан с Notes доменом, выбирайте имя домена, не определяя первичный Notes домен.
Company Name	Имя компании связанное с этим Directory. Несколько документов Directory Assistance, могут использовать то же самое название компании.
Search Order	Число, определяющее порядок поиска в базе данных Directory Assistance.

Enabled	Выбирайте – Yes, для разрешения использования документа.

*2437 На закладке Rules заполните следующие поля:

Поле	**Значение**
Rule #	Одно или несколько правил, которые описывают имена в Directory. По умолчанию, первое правило содержит все звездочки, указывая все имена в Directory.
Enabled	Выбирайте одно из двух: *2438 No – запрещение выбранного правила *2439 Yes – разрешение выбранного правила По умолчанию, разрешено первое правило.
Trusted for Credentials	Выбирайте одно из двух: *2440 Yes – позволить Domino, использовать этот Directory для идентификации Web имен клиентов, соответствующие этому правилу *2441 No - не разрешать Domino использовать этого Directory идентификации Web имен клиентов, соответствующие этому правилу

*2442 Выбирайте закладку Replicas и заполните следующие поля, чтобы определить до пяти реплик вторичных Directory, для использования Directory Assistance.

Обратите внимание. Если вы идентифицируете Web клиентов, зарегистрированных во вторичных Directory, а также используете Directory Catalog, убедитесь, что определили реплики вторичных Domino Directory, которые Вы использовали для строительства Source Directory Catalog.

Поле	**Значение**
Database links	Откройте реплику вторичного Directory и затем выберите - Правка – Копировать как связь – с базой данных. Выберите поле Database links и затем выбирайте - Правка – Вставить. Использования связей с базами данных, работает только в Domino R5 серверах. Использование связей баз данных может задерживать запуск серверов, потому что, когда Вы запускаете сервер, который использует Directory Assistance, задачи сервера должны восстановить информацию базы данных с удаленных серверов.

Replica #	Имя сервера и имя файла реплики вторичного Directory Server name: Mail1/West/Acme Directory file name: EASTNAMES.NSF Выбирайте – Yes, рядом с каждой репликой.

Примечание. Если Вы определяете реплику в поле Database links и в поле Replica, поле Replica имеет приоритет.

*2443 Сохраните и закройте документ.

5.5.7 Настройка Directory Assistance для LDAP Directory.

Создайте Directory Assistance для LDAP Directory, Вы конфигурируете единственный документ Directory Assistance для Directory, чтобы определить следующее:

*2444 Идентификация Web клиентов использующих LDAP Directory

*2445 Проверка групп из LDAP Directory

*2446 Обращение LDAP клиентов, к LDAP Directory

*2447 Использование LDAP Directory, для проверки почтовых адресов от имени Notes пользователей

Когда Вы используете LDAP Directory, чтобы идентифицировать Web клиентов, или проверить их членство в группе, мы настоятельно рекомендуем использование SSL, для соединения с LDAP Directory сервером.

5.5.7.1 Идентификация Web клиентов с использованием LDAP Directory.

Вы можете сконфигурировать Directory Assistance, чтобы использовать LDAP Directory для идентификации Web клиентов.

Примечание, чтобы дать Web пользователям доступ к базам данных, Вы может включать их имена в ACL баз данных. Когда Вы добавляете имя Web пользователя, зарегистрированного в LDAP Directory, используете полное имя, но используете, разделители (/) вместо запятых (,). Например, если имя пользователя в LDAP Directory:

```
Oid=Karen Мастер, ou=Web, o=Acme
```

В ACL базы данных вводят имя:

```
Oid=Karen Wright/ ou=Web/ o=acme
```

Для настройки идентификации Web пользователей создайте документ, в базе Directory Assistance и заполните поля, как указано ниже.

*2448 На закладке Basics, заполните эти поля:

Поле	**Значение**
Domain Type	Выбирайте – LDAP

Domain Name	Имя домена
Company Name	Имя компании.
Search Order	Номер, определяющий порядок поиска в базе данных Directory Assistance.
Enabled	Выбирайте – Yes, для разрешения использования документа.

*2449 Выбирайте закладку Rules и заполните поля:

Поле	**Значение**
Rule #	Одно или несколько правил, которые описывают имена в Directory. По умолчанию, первое правило содержит все звездочки, указывая все имена в Directory.
Enabled	Выбирайте одно из двух: *2450 No – запрещение выбранного правила *2451 Yes – разрешение выбранного правила По умолчанию, разрешено первое правило.
Trusted for Credentials	Выбирайте одно из двух: *2452 Yes – чтобы позволить Domino, использовать этот Directory для идентификации Web имен клиентов, соответствующие этому правилу *2453 No - не разрешать Domino использовать этого Directory идентификацию Web имен клиентов, соответствующие этому правилу

*2454 Выбирайте закладку LDAP, заполните поля и нажмите сохранить и закрыть:

Поле	**Значения**
Hostname	Имя хоста сервера LDAP Directory. Пример: ldap.acme.com.

Base DN for search	Базовый поиск, если сервер LDAP Directory требует этого.
	Пример:
	`o=Ace Industry`
	`o=Ace Industry,c=US`

Perform LDAP search for	Выбирайте опцию – Notes clients/Web Authentication.

Channel encryption	(Настоятельно рекомендуем) Выбирайте – SSL, для использования SSL, при соединении с Domino сервером Заполните поля: Accept expired SSL certificates, SSL protocol version, Verify server name with remote server's certificate.
Port	Номер порта, для соединения LDAP Directory сервер: Если выбрано - SSL, порт по умолчанию - 636. Если выбрано - None, используется по умолчанию - 389.
Timeout	Максимальное число в секундах, для поиска в LDAP Directory. По умолчанию - 60 секунд.
Maximum number of entries returned	Максимальное число имен, которые сервер LDAP Directory возвратит для отыскания имен. По умолчанию - 100.

5.5.7.2 Идентификация пользователей в группах из LDAP Directory.

Вы можете включать имена групп, расположенных в LDAP Directory, в ACL баз данных на Domino серверах. Когда Web пользователи пытается открыть базу данных на сервере, который использует Directory Assistance, настройте Directory Assistance так, чтобы Domino мог иметь доступ LDAP Directory, чтобы проверять членство пользователей в группах. Вы можете разрешить эту опцию только для одного LDAP Directory, сконфигурированного в Directory Assistance.

Для разрешения поиска в группах LDAP Directory серверов, установите в поле Group expansion значение –Yes, на закладке Basics, документа Directory Assistance.

Если Вы изменили имя группы, используйте команду остановки, для каждого Domino сервера, который использует Directory Assistance для проверки групп. Запустите каждый сервер повторно. Если это необходимо, ждите пока Directory Assistance реплицирует изменения на другие сервера.

5.5.7.3 Использование SSL в установках Directory assistance для LDAP Directory.

Когда Вы создаете Directory Assistance, для идентификации Web клиентов, или проверки членства пользователя в группах LDAP Directory, для баз данных ACL, настоятельно рекомендуется, чтобы Вы использовали SSL, при соединении с LDAP Directory сервером.

*2455 Из клиента Domino Administrator, открывайте Directory Assistance

*2456 Выбирайте закладку LDAP. В поле Perform LDAP search, выбирайте - Notes Clients/Web Authentication

*2457 В поле Channel encryption, выберите – SSL.

*2458 В поле Port, введите номер порта, который будет использоваться для соединения с LDAP сервером. По умолчанию - 636.

*2459 В поле Accept expired SSL certificates, выберите – Yes (по умолчанию), чтобы принять сертификат от LDAP Directory сервера, даже если дата сертификата истекла. Для увеличения уровня безопасности, установите значение – Yes.

*2460 В поле SSL protocol version, выберите номер версии SSL протокола, чтобы использовать, его следующим образом:

Версия SSL протокола	**Описание**
V2.0 only	Использовать только SSL версии 2.0 соединения.
V3.0 handshake	Делается попытка использовать SSL версии 3.0 для соединения. Если попытка неудачна, пробуется SSL версии 2.0.
V3.0 only	Использовать только SSL версии 3.0.
V3.0 and V2.0 handshake	Делается попытка установить связь с использованием SSL версии 3.0, но начинается попытка с SSL версии 2.0. Если получено сообщения об ошибке, делается попытка использовать SSL версии 3.0. Используйте V3.0 и V2.0 установку Handshake, чтобы получить V2.0 сообщение об ошибке. Эти сообщения об ошибке могли бы предоставить Вам информацию относительно любых проблем совместимости, найденных в течение связи.

*2461 В поле Verify server name with remote server's certificate установите – Enabled, чтобы требовать, проверки сертификатов и имени удаленных серверов, LDAP Directory и имени хоста. По умолчанию эта опция разрешена. Чтобы работать должным образом, удаленные сервера должны быть включены в DNS. Мы рекомендуем, чтобы Вы не запрещали этот выбор, если Вы уверены в X.509 сертификатах с удаленных серверов, с которыми Ваш сервер соединяется, содержит удаленное имя хоста в соответствующем формате.

Обратите внимание, что Domino CA и некоторые другие CAs требуют ввода дополнительной информации пользователями. Например, Domino CA требует от каждого пользователя вводить информацию об удаленном сервере, типа, обычного названия, имени орг. единицы, названия организации, признака страны. Domino CA размещает эту информацию в Subject Lines и добавляет соответствующую приставку (cn=, ou=, o=, и так далее) к каждому полю. Если Вы использовали Domino CA, для создания сертификата удаленного сервера, мы настоятельно рекомендуем вводить имя хоста в поле Common Name, при использовании выбора - Verify server name with remote server's certificate. Например, Domino CA позволяет пользователям вводить, следующие имеющие значения в Subject Lines (mailserver.acme.com - DNS имя хоста сервера):

```
cn=mailserver.acme.com, ou=sales, ou=marketing, o=acme, st=mass, c=us

cn=mailserver, ou=sales - mailserver.acme.com o=acme, st=mass, c=us
```

Чтобы пользователи вводили имя хоста DNS должным образом, мы рекомендуем, чтобы они вводили его как общее имя, при требовании сертификата от Domino CA. Другие CA's могут иметь различные диалоги для ввода в поле Subject Lines; пользователи должны следить за этими диалогами, чтобы ввести в имя хоста удаленного сервера DNS.

*2462 Заполните оставшиеся поля в документе Directory Assistance, сохраните его и закройте.

5.5.8 Каскадные Domino Directory.

До версии Domino R4.5, организации использовали каскадные Domino Directory. Использование каскадных Domino Directories все еще поддерживается для обратной совместимости, рекомендуется, чтобы Вы конвертировали их в Directory Assistance. Следующая таблица сравнивает Directory Assistance с каскадными Domino Directories.

Возможности	**Directory Assistance**	**Cascading Directory**
Находит записи во вторичных Domino Directories по имени пользователей Notes для адресования почты	Да	Да
Находить записи в LDAP Directories по имени пользователей Notes для адресования почты	Да	Нет
Находить записи во вторичных Domino Directories по имени для LDAP клиентов	Да	Да
Сравнивать LDAP клиентов в LDAP Directories	Да	Нет
Использует имя и пароль, для идентификации Web клиентов, зарегистрированных во вторичных Domino Directories	Да	Нет
Использует X.509 сертификаты, для идентификации Web клиентов, зарегистрированных во вторичных Domino Directories	Да	Нет
Идентификация Web клиентов зарегистрированных в LDAP Directories	Да	Нет
Переадресация в другие реплики вторичных Domino Directory	Да	Нет
Использование правила обработки имен для эффективного поиска во вторичных Domino Directories	Да	Нет
Поддержка неограниченного числа вторичных Domino Directories	Да	Нет (NAMES = setting has a 256-character limit)
Поддержка адресации Recipient name type ahead	Да	Да
Совместная работа с Directory Catalog на сервере	Да	Да

Примечание. Вы не может использовать Directory Assistance вместе с каскадными Domino Directories. Имеются два способа использовать каскадные Domino Directories. Вы можете создавать реплики для каждого вторичного Directory в первичном Notes Directory домена, или Вы можете настраивать сервера, для доступу ко вторичным Directory по сети.

Использование реплик каскадных Directories на Вашем сервере

В этой конфигурации, каждый сервер хранят реплики вторичных Domino Directories и реплики первичных Domino Directory. Преимущество для этого подхода состоит в том, что при вводе имени, имя ищется в первичном и вторичных Domino Directories. Неудобства - дополнительное место на диске, для реплик.

Исполните эту процедуру для каждого сервера, который Вы используете:

*2463 Убедитесь, что первичный Directory внесен в список имен АК, файла NOTES.INI, и у Вас имеются следующие документы:

- Документы групп, только для групп в первичном домене
- Документы серверов, только для серверов в первичном домене
- Документы подключения только для подключения серверов в первичном домене

*2464 Создайте реплики каждого вторичного Domino Directory на сервере. Дайте каждой реплике Domino Directory различные имена файлов.

2465 Добавьте названия файла реплик, в установку имен в файле NOTES.INI. Установите название файлов для первичного Domino Directory вначале списка. Не включите расширение файлов (.NSF) в переменную. Отделите список Directories запятыми. Например, определите:

```
Names=NAMES, EASTNAME, WESTNAME
```

*2466 Перезапустите сервер, чтобы изменения вступили в силу.

*2467 Наметьте репликации для Domino Directory каждого домена.

Использование реплик каскадных Directories с доступом к ним по сети

В этой конфигурации, каждый сервер использует сеть, для доступа ко вторичным Domino Directory. При использовании этого подхода, Вы не нуждаетесь в репликах в домене. Однако пользователи не могут использовать ввод адресов, для решения имен, а сессии между доменами остаются постоянно открытым.

*2468 Добавьте имена вторичных Domino Directory в переменную NOTES.INI файле. Держите имя файла первичного Domino Directory в начале списка. Определите местоположение для вторичного Directory следующим образом:

```
Servername!! Filename
```

Например, ввод имен мог бы быть такой:

```
Names=NAMES,serverwest/west/acme!!NAMES, servereast/east/acme!!NAMES
```

Не включите расширение (*.NSF) при определении имени файла. Отделите список серверов и Directories запятыми.

Если удаленный сервер – Hub сервер, и он хранит несколько Domino Directories, Вы должны указывать для каждого Directory - сервер. Вы должны повторить имя сервера для каждого Directory.

Например:

```
Names=NAMES,serverhub/acme!!NAMES1, serverhub/acme!!NAMES2
```

*2469 Перезапустите сервер, чтобы изменения вступили в силу.

5.5.9 Сервер Каталогов

Directory server - Domino сервер, который Вы сконфигурировали как сервер каталога. Сервер каталога уменьшает рабочую нагрузку на почтовые сервера. Вы можете создавать реплики вторичных Domino Directories на сервере каталога, так, чтобы другие сервера в Вашей организации не должны хранить эти реплики.

Используйте Setup Profile, чтобы заставить пользователей Notes, использовать сервер каталога.

Directory Catalog и Directory servers

Если Вы используете Directory Catalog, храните его базу данных и реплики, вторичных Domino Directory, на сервере каталога. Настройте почтовые сервера, чтобы использовать Directory Catalog так, чтобы почтовые сервера могли быстро находить адреса пользователей во вторичном Domino Directory, вместо поиска в нескольких Directory.

Directory Assistance и Directory servers

Сконфигурируйте Directory Assistance так, чтобы его документы указывали на реплики вторичных Directories расположенные на сервере каталога. Создайте реплики баз данных Directory Assistance на почтовых серверах, так что бы почтовый сервер мог просматривать адреса пользователей во вторичном Domino Directory.

Domino LDAP сервис и Directory servers

Запускайте LDAP сервисы на Directory servers.

5.5.9.1 Конфигурируйте сервер каталога для Notes пользователей.

После того, как Вы установите сервер каталога, Вы можете настроить пользователей Notes, чтобы использовать его. Notes будет использовать Directory сервер, чтобы решать почтовый адресы.

Обратите внимание, чтобы искать на сервере каталога, пользователи Notes не должны использовать Mobile Directory Catalog. Сервер каталога не используется для LDAP поиска.

Имеются два способа, чтобы настраивать клиентов Notes, для использования Directory сервера. Как администратор, Вы можете создавать User Setup Profile для клиентов Notes, или пользователи Notes могут вводить имя сервер каталога в поле Сервер справочника, в документе Место вызова. Тогда, Notes использует указанный сервер каталога, скорее, чем почтовый сервер пользователя, для решения адреса.

6 Безопасность и контроль доступа на Domino сервера.

6.1 Защита ID файлов и работа с ними.

Domino использует ID файлы, чтобы идентифицировать пользователей и управлять доступом к серверам. Каждый Domino сервер, сертификатор Notes и пользователь Notes должен иметь ID файл. Когда Вы регистрируете пользователей или сервера, Domino автоматически создает для них ID файлы. ID файл содержит:

*2470 Имя владельца. Пользовательский ID файл может также содержать одно дополнительное имя. Сертификатор ID может содержать несколько дополнительных имен.

*2471 Постоянный номер лицензии. Этот номер указывает, что владелец юридический определен, имеет Северо-Американскую, Международную или Glabal лицензию.

*2472 По крайней мере, один сертификат Notes от Сертификатора ID. Сертификат Notes, это электронная печать, добавляется к ID пользователя или ID сервера. Эта печать, производится из личного ключа ID сертификатора. Она подтверждает, что имя владельца ID правильно связано с определенным публичным ключом.

*2473 Личный ключ. Notes использует личный ключ, чтобы подписывать сообщения, посланные владельцем сообщения,

*2474 (Необязательно для клиента Notes) Может иметь интернет сертификат. Это сертификат используется для связей SSL, шифрования и подписи почтовых сообщений S/MIME. интернет Сертификат выпускается от имени Certification Authority (CA) и подтверждает идентичность пользователя.

*2475 (Необязательно) Ключи шифрования, чтобы позволить пользователям шифровать и дешифровать поля в документах.

*2476 (Необязательно) Пароль, если владелец ID создает его. Пароль производит ключ, который шифрует личные данные ID.

6.1.1 Сертификаты.

Сертификаты - уникальная электронная печать, которая опознает пользователя или сервер. ID сервера и пользователя содержат один, или несколько Notes сертификатов. Кроме того, ID пользователя может содержать интернет сертификат, который опознает пользователей, когда они используют SSL, для соединения с интернет сервером или при рассылке подписанных или зашифрованных почтовых сообщений S/MIME.

Сертификат содержит:

*2477 Имя сертификатора, который выпустил сертификат.

*2478 Имя пользователя или сервера от имени, кого сертификат был выпущен.

*2479 Публичный ключ, который сохраняется в Domino Directory и в ID файле. Notes использует публичный ключ, чтобы шифровать сообщения, которые будут посланы владельцу и шифруются с использованием публичного ключа, для проверки подлинности ID владельца.

*2480 Электронную подпись.

*2481 Дата истечения сертификата.

Сертификаты сохраняются в ID файлах пользователей, серверов и в Certifier документах, из Domino Directory.

Публичный ключ - не тайна. Любой пользователь может просмотреть публичный ключ другого пользователя и может использовать его, чтобы послать шифрованное письмо. Пользователи должны иметь возможность получить публичный ключ сертификатора, прежде чем они могут идентифицировать владельца сертификата. Если пользователь имеет сертификат выпущенный тем же самым сертификатором, что и другой пользователь или сервер, первый пользователь может проверить публичный ключ для сертификата, и знать публичный ключ, связанный с именем пользователя или сервера. Если пользователь не имеет сертификата, выпущенного тем же самым сертификатором, пользователь нуждается во взаимном сертификате для идентификации.

Когда Вы регистрируете пользователей и сервера, Domino автоматически создает сертификат Notes для каждого ID пользователя или сервера. Кроме того, Вы можете создавать интернет сертификаты пользователей, или получить сертификат от уполномоченных для этой цели CA. Domino создает сертификат интернета X.509 формата.

Сертификаты Notes имеют даты истечения. Поэтому, Вы должны повторно сертифицировать ID Notes, когда приближаются их дата истечения. Кроме того, если пользователь или сервер изменяет имя, Вы должны повторно сертифицировать соответствующий ID Notes так, чтобы новый сертификат будет связан с публичным ключом и новым именем. Однако изменение имени ID пользователя не затрагивает интернет сертификаты.

6.1.2 Просмотр сертификатов ID файла.

Вы можете просматривать Notes сертификаты и интернет сертификаты, связанные с ID и просматривать информацию о сертификате. Например, можно просмотреть информацию о публичном ключе, просмотреть дату создания сертификата, просмотреть дату истечения сертификата и информацию о сертификатор.

Например, окно сертификатов показывает сертификаты для ID пользователя Notes с именем Alan Jones/Sales/East/Acme. Первый сертификат из списка ниже – выпущен для Alan Jones международного типа использования. Второй сертификат из списка - выпущен для Alan Jones Северо-Американского типа использования. После них - сертификат, выпущенный сертификатором ID и любым предком сертификатора. Последний сертификат из списка - сертификат интернета, выпущенный для Alan Jones.

Сертификат	**Для кого выпущен сертификат**
/Sales/East/Acme (International)	Alan Jones/Sales/East/Acme
/Sales/East/Acme (North American)	Alan Jones/Sales/East/Acme
/East/Acme	/Sales/East/Acme
/Acme	/East/Acme
/Acme	/Acme

CN=AcmeCA/OU=East/O=Acme/L=Cambridge/ST=Massachusetts/C=US	EMAIL=alan_jones@acme.com/CN=Alan Jones/OU=East/O=Acme/L=Cambridge/ST=Massachusetts/C=US

Просмотр сертификатов

*2482 Из клиента Domino Administrator, выбирайте закладку Настройка

*2483 Выбираем из меню Заверения – Свойства учетной записи и выбираем нужный ID.

*2484 Введите пароль и выбирайте – OK.

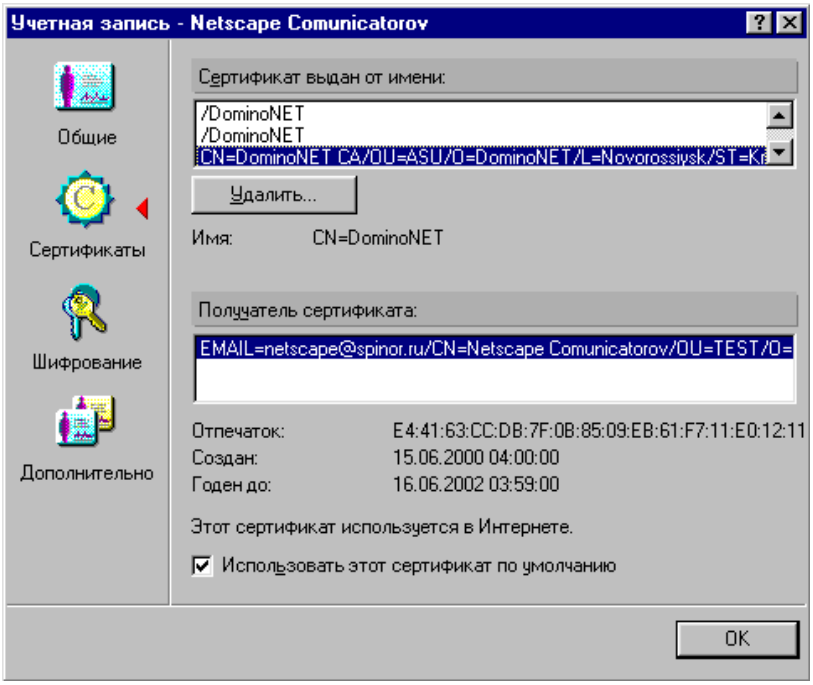


Рис. 94 Диалоговое окно свойств учетной записи пользователя, закладка Сертификаты.

*2485 Делает следующее:

- Выбирайте закладку - Сертификаты, чтобы просмотреть список всех Notes и сертификатов интернета, выпущенных для этого ID файла.
- Выберите сертификат в окне Сертификаты, чтобы просмотреть дополнительную информацию относительно сертификатора.

6.1.3 Защита ID файлов Notes и Domino серверов паролем.

Чтобы гарантировать безопасность Domino системы, защищайте паролем все ID Notes и Domino сертификаторов, серверов и пользователей. Когда Вы защищаете ID паролем, ключ, который получен из пароля, зашифрует данные об ID. Когда Вы делаете попытку доступа к почте, сервер исследует ID информацию файла и вынуждает Вас ввести пароль.

6.1.3.1 Особенности защиты паролем.

Проверка качества пароля.

Когда Вы регистрируете пользователя или сервер или создаете ID сертификатора, Вы используете шкалу от 0 до 16, чтобы определить уровень сложности пароля для ID. Чем выше уровень, тем более сложен пароль и поэтому более труден для подбора. Для оптимальной безопасности, определите пароль, не менее 8 знаков. Не записывайте Ваш пароль, и не оставляйте копию Вашего пароля, чтобы никто не мог найти его.

Запрос качественного уровня пароля требуется, когда Вы вводите пароль для нового ID файла, или когда пользователи изменяют пароль для существующего ID файла. Когда пользователи изменяют пароли, Notes показывает информацию о пароле, требуемого для ID файла. Пользователи должны вводить пароль, который выполняет критерии уровня защиты, иначе им не позволяется изменить пароль.

При выборе пароля, лучше определять случайную, алфавитно-цифровую строку, которая включает смешанный, верхний и нижний регистр, числа и знаки пунктуации. Рассмотрите в качестве пароля применение определение фразы. Фраза для пароля легка для запоминания, но трудна для подбора.

Чтобы изменять пароль для ID, Вы должны повторно сертифицировать ID.

Механизмы задержки по времени, для ввода пароля и защита от перехвата пароля другими программами.

Все пароли для Notes ID имеют встроенную задержку времени и механизм Anti-Spoofing. Оба механизма созданы для предотвращения перехвата пароля.

Пароль и проверка публичного ключа при идентификации пользователей.

По умолчанию, Notes и Domino использует только пароли, для защиты информации, сохраненную в ID файлах. Однако Вы можете сконфигурировать сервера, чтобы проверять пароли и публичные ключи в течение идентификации. Пароль и проверка публичных ключей увеличивает безопасность использования ID файлов. Если Вы настраиваете сервер, для проверки пароля, но некоторый пользователь получает ID и пароль, хозяин ID должен только изменить пароль для ID. В следующий раз, когда неправомочный пользователь пытается зарегистрироваться, доступ для этого пользователя не будет разрешен на сервер.

Наряду с проверкой паролей, Вы можете настроить сервер, чтобы он требовал, изменения пароля периодически.

Использование нескольких паролей для одного ID файла.

Чтобы обеспечивать более плотный уровень безопасности для ID сертификаторов и серверов, Вы можете назначить многоуровневые пароли для них. Использование, которых требуют, чтобы группа администраторов работала вместе для доступа к ID файлу. Эта особенность полезна, когда Вы хотите избежать, давать полномочие для ID сертификатора одному человеку. Вы можете определить, что только определенное количество назначенных паролей требуется для доступа к ID. Например, Вы можете назначать четыре пароля для ID файла, но требовать, чтобы только любые два, из четырех паролей, были введены для доступа к ID файлу.

ID и восстановление пароля.

Если Вы имеете ID и пароль восстановления, Вы можете восстановить пароль, если пользователь теряет ID файл или забывает пароль ID файла. Группа администраторов может работать вместе, чтобы поправить ID файл. Потеря ID файла обычно сопровождается потерей доступа пользователя для чтения сообщений и других данных, которые он шифровал с использованием своего ID. Используйте новую функцию

восстановления ID файла, при котором администраторы могут поправить эту потерю доступа и восстанавливать ID файл.

6.1.4 Проверка пароля пользователя при идентификации пользователя.

Вы можете позволить проверку пароля, чтобы пользователь Notes мог подтверждать подлинность с сервером только после ввода правильного пароля, который связан с пользовательским ID. Если неправомочный пользователь получает ID и подбирает пароль для ID, владелец ID может использовать проверку пароля, чтобы изменить пароль. Этими действиями Вы можете блокировать использования украденного ID. Следующий раз, когда неправомочный пользователь пробует использовать ID со старым паролем для доступа на сервер, сервер проверяет пароль, решает, что введенный пароль не соответствует новому паролю и отвергнет доступ пользователя на сервер. Без проверки пароля, неправомочный пользователь может использовать ID и пароль даже после того, как пользователь изменяет пароль для ID. Это происходит потому, что по умолчанию, пароль используется только для дешифрации ID файла. По умолчанию пароль не сравнивается с сохраненным паролем в Domino Directory.

Если Вы устанавливаете проверку пароля, требуете, чтобы пользователи изменяли пароли для ID файлов регулярно. Когда пользователи изменяют пароль, текущий ID и Person документ обновляется новым паролем.

Обратите внимание, что эти действия не изменяют поле пароля для интернета в Person документе пользователя в Domino Directory.

Если пользователь имеет несколько ID файлов, пользователь должен заменить устаревшие ID, новой копией обновленного ID. Вы не можете использовать проверку пароля на ID файлах, которые защищены несколькими паролями.

Каждый раз, когда пользователь изменяет пароль, пользователь должен определить уникальный пароль. Domino помнит до 50 старых паролей, которые пользователь использовал.

Просроченный пароль не запрещает пользователю чтение шифрованной почты или создания новых подписанных документов, шифрование локальных реплик, однако, без определения нового пароля, пользователь не сможет получить доступ на сервера.

Обратите внимание, что проверка пароля в течение идентифицикации не работает для интернет пользователей, потому что они не имеют ID пользователя Notes.

Процесс администрирования и проверка пароля.

Проверка пароля требует, чтобы процесс администрирования модернизировал документы в Domino Directory. Когда Вы позволяете проверку пароля для пользователя, процесс администрирования создает запрос Set Password Information, в базе данных Administration Requests. Domino выполняет этот запрос согласно установке в поле Interval, в секции Administration Process, Server документа. Этот запрос позволяет проверять значения полей Check password, Required change interval и Grace period, из секции Administration Person документа.

Первый раз, когда пользователь регистрируется на сервере, который требует проверки пароля, процесс администрирования генерирует запрос Change User Password in Domino Directory, в базе Administration Requests. Этот запрос передает пароль в поле Password digest в секции Administration, Person документа. Также делается запись даты, когда пользователь ввел пароль в последней раз, в поле Last change date, секции Administration,

Person документа. Чтобы подтверждать подлинность с серверами, которые позволяются проверки пароля, пользователь, должен вводить пароль, который соответствует полю Password digest.

После того, когда пользователь изменяет пароль, процесс администрирования производит новый запрос Change User Password in Domino Directory. Этот запрос модернизирует поля даты изменения в Person документе.

Изменения интервала и периода на требование изменить пароль пользователя.

Вы можете настроить сервер, чтобы проверять пароли пользователей в течение идентификации, без требования, изменения их паролей. Если Вы требуете изменения пароля, Вы можете определить период, который определяет интервал истечения пароля. Если требуемый интервал изменения истекает прежде, чем пользователь изменяет пароль, пользователь не сможет соединиться с сервером, который требуют проверки пароля, пока не создаст новый пароль. Если, период истекает, но пользователь все еще, не изменил пароль, пользователь не может пройти процесс идентификации, пока администратор вручную не удалит данные из поля Password digest, в Person документе и пользователь создает новый пароль.

Если неправомочный пользователь изменяет пароль в ID прежде, чем уполномоченный владелец ID сделает это, уполномоченный владелец не сможет подтверждать подлинность и увидит это сообщение:

```
You have a different password on another copy of your ID file and you must
change the password on this copy to match.
```

В этом случае, удалите запись из поля Password digest и просите пользователя войти в систему и немедленно ввести новый пароль.

Обратите внимание, что требование интервалов изменения паролей, не относятся к паролю интернет, которые используются клиентами интернета.

6.1.4.1 Установка проверки пароля.

Чтобы использовать проверку пароля для пользователей Notes, Вы должны позволить проверку пароля для обоих пользователей и серверов.

*2486 Удостоверится, что процесс администрирования настроен и запущен на сервере и что Вы имеете, по крайней мере, доступ автора и роль UserModifier к Domino Directory.

*2487 Из клиента Domino Administrator, выбирайте закладку - Пользователи и группы, используя для доступа к Domino Directory сеть.

*2488 Выбирайте Person документ, для которого пользователя, которому Вы хотите позволить проверку пароля.

*2489 Выбирайте - Действия – Set Password Fields, затем – Yes, для продолжения.

*2490 Выбирайте опцию – Check password.

*2491 Заполните эти поля, и затем выбирайте – OK:

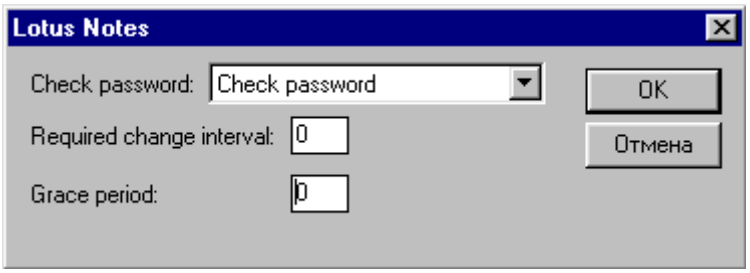


Рис. 95 Диалоговое окно установки проверки пароля сервером.

Поле	**Значение**
Required change interval	Число дней, спустя которые пользователю будет предложено ввести новый пароль; По умолчанию – 0 Не требует, чтобы пользователи изменили их пароли, и игнорирует любые значения в поле Grace period.
Grace period	Число дней в течении которых сервер все еще будут просить изменить пароль и все еще пропускать пользователей. По умолчанию – 0 Позволяет пользователям неограниченное количество времени на изменение их пароля после того, как интервал изменения истекает. Рекомендуется значение между 3 и 7 днями.

*2492 Делайте следующее, чтобы позволить проверку пароля на каждом сервере, с которым эти пользователи работают:

- Выбирайте закладку Настройка, откройте каждый Server документ.
- Выбирайте закладку Security.
- В поле Check passwords on Notes Ids выберите – Enabled.

Эта опция разрешает проверку пароля пользователям, для которого установка проверки пароля разрешена. Когда Вы запрещаете проверку пароля для пользователя, Domino не проверяет пароли для пользователя, даже если проверка пароля позволяется для сервера.

Запрещение проверки пароля.

*2493 Удостоверится, что процесс администрирования настроен и запущен на сервере и что Вы имеете, по крайней мере, доступ автора и роль UserModifier к Domino Directory".

*2494 Из клиента Domino Administrator, выбирайте закладку - Пользователи и группы, используя для доступа к Domino Directory сеть.

*2495 Выбирайте Person документ, для которого пользователя, которому Вы хотите позволить проверку пароля.

*2496 Выбирайте опцию – Don't check password, затем – OK.

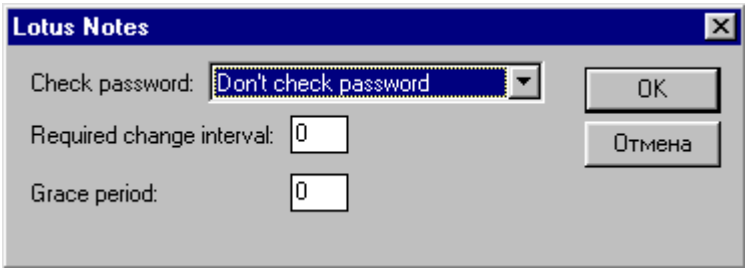


Рис. 96 Диалоговое окно запрещения проверки пароля сервером.

Когда Вы запрещаете проверку пароля для сервера, Domino не проверяет пароли для любых пользователей, которые имеет доступ на сервер, даже если пользователь имеет установленную опцию проверки пароля разрешенной.

*2497 Выбирайте закладку Настройка, откройте каждый Server документ.

*2498 Выбирайте закладку Security.

*2499 В поле Check passwords on Notes Ids выберите – Disabled.

6.1.5 Назначение нескольких паролей для ID сервера или сертификатора.

Чтобы закончить следующие процедуры, Вы должны собрать вместе всех администраторов, чьи пароли будут назначены на ID файл. Каждый администратор должен выполнить ряд шагов. Любой пароль, который был назначен на ID прежде, чем Вы назначаете новые пароли, больше не будет иметь силу.

*2500 Из клиента Domino Administrator, выбирайте закладку - Настройка, затем инструмент справа - Заверение

*2501 Выбирает из панели инструментов – Изменить набор паролей

*2502 Выбирайте ID, которому Вы хотите назначить несколько паролей, и затем выбирайте – Открыть.

*2503 Введите пароль для ID файла (если требуется).

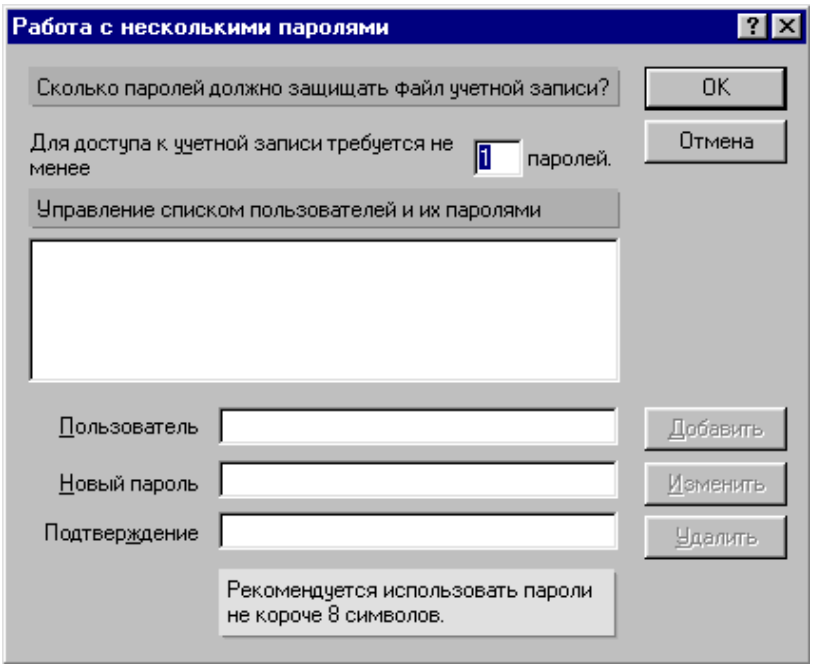


Рис. 97 Диалоговое окно назначения нескольких паролей ID файлу.

*2504 Каждый администратор в свою очередь заканчивает эти шаги:

- В поле Пользователь, вводится имя пользователя.
- В поле Новый пароль, вводится пароль.
- В поле Подтверждение, повторно вводится пароль.
- Выбирайте – Добавить, чтобы добавить Ваше имя в пароль ID файл.

*2505 Вводят минимальное число паролей, требуемых для доступа к ID файлу. Введите число, которое является меньше или равное числу администраторов.

*2506 Выбирайте – OK.

Удаление паролей из ID файла

*2507 Из клиента Domino Administrator, выбирайте закладку Настройка, затем инструмент справа - Заверение

*2508 Выбирает из панели инструментов – Изменить набор паролей

*2509 Выбирайте ID, из которого Вы хотите удалить пароль.

*2510 Вводите требуемые пароли.

*2511 Выбирает пользователя, и затем выбирайте – Удалить.

*2512 Повторите эти шаги, чтобы удалить пароли для каждого пользователя.

*2513 Выбирайте – OK.

6.1.6 Восстановление пароля ID файла.

Чтобы предохранится от потери или повреждения ID файла, рекомендуйте, чтобы все пользователи имели резервные копии своих ID файлов в безопасном месте - например, на диске, сохраненные в недоступной области. Потеря или повреждение ID файла, или забытие пароля имеет серьезные последствия. Без ID пользователи Вы не можете получить доступ на сервера, или читать сообщения и другие данные, которые они зашифровали с использованием потерянного ID. Чтобы предотвратить эти проблемы, когда пользователи теряют или повреждают ID файлы или забывают пароли, настройте Domino, для восстановления ID файлов.

Вы должны определять несколько администраторов, которые будут действовать как группа, для восстановления ID и пароли. Вы можете определять единственного администратора, чтобы управлять ID файлами и восстанавливать пароли. Мы рекомендуем, по крайней мере, присутствия трех администраторов, для работы вместе, по восстановлению ID файлов. Наличие группы администраторов помогает предотвращать нарушение безопасности одним администратором, который имеет доступ ко всем ID файлам. Когда Вы определяете группу администраторов, Вы можете определить, что только минимальный набор их присутствия, в течение фактического восстановления ID.

Например, если Вы определяете пять администраторов для восстановления ID, но требуете присутствия только троих администраторов, для отпирания ID файла. Любые три из пяти администраторов могут отпирать ID файл. При обозначении группы администраторов и при требовании присутствия только нескольких человек, также предотвращает проблемы, которые происходят, если один администратор недоступен или оставляет компанию.

Прежде, чем Вы можете отпирать ID файлы, Вы должны делать следующее:

*2514 Администратор, который имеет доступ к файлу ID сертификатора, должен определить информацию восстановления.

*2515 Пользователи должны принять информацию восстановления в их ID файл, или ID файл должен быть создан с ID сертификатора, который содержит информацию восстановления. После принятия информации восстановления или регистрации нового пользователя, Notes автоматически отправляет зашифрованную резервную копию ID файлов в специальную централизованную базу данных. ID файлы, которые не содержат информации восстановления, не может быть восстановлен.

Domino хранит ID информацию восстановления в ID файле сертификатора. Сохраненная информация включает имена администраторов, кому позволяется отпирать ID файлов, адрес почтовой базы данных, или Mail-In базы данных, куда пользователи посылают зашифрованную резервную копию их ID файлов, число администраторов, требуемых, чтобы отпереть ID файл. База данных Mail-In содержит документы, которые хранят присоединенные файлы, с шифрованной резервной копией ID файлов. Эти файлы шифруются с использованием случайного ключа и не могут использоваться с Notes, пока они не будут восстановлены.

Зашифрованная резервная копия ID файла требуется, чтобы заменить потерянный или разрушенный ID файл. Восстановление ID файла, для которого пароль был забыт, немного легче. Если оригинал ID файла содержит информацию восстановления, администраторы могут восстановить ID файл, даже если зашифрованный резервный ID файл не существует.

6.1.6.1 Как работает функция восстановления ID файла?

Для каждого ID администратора или пользователя, файл содержит пароль восстановления, который создан и зашифрован с использованием публичного ключа администратора. Пароль уникален для каждого администратора и пользователя. Например, Bowker Randi администратор имеет уникальный пароль восстановления для пользователя Alan Jones, и этот пароль сохранен в ID файле Alan Jones. Администратор Bowker Randi имеет уникальный пароль восстановления для Пользователя Susan Salani, и этот пароль сохранен в ID файле Susan Salani.

Восстановление ID:

*2516 Пользователь обращается к администратору, чтобы получить пароль восстановления администратора.

*2517 Администратор получает запрос на восстановление, дешифрует пароль восстановления, сохраненный в ID файле пользователя, используя личный ключ администратора.

*2518 Администратор, после чего дает пароль восстановления пользователю.

*2519 Шаги описанные выше, повторяются пользователем, пока не будет достигнуто минимальное число администраторов, для восстановления ID файла.

*2520 После того, как файл отпирают, пользователь должен ввести новый пароль, чтобы защитить ID файл.

Тот же самый ID файл может быть восстановлен снова, используя те же самые пароли восстановления.

Когда пользователи генерирует новый публичный ключ, изменяет имя, или принимают или создает ключ шифрования, Domino автоматически посылает, зашифрованный резервный ID файл в централизованную базу данных.

Чтобы запретить неправомочным пользователям, восстанавливать ID, удостоверитесь, что проверка пароля позволяется для пользователей и серверов.

Как дополнительная предосторожность, после восстановления ID файла, обычно просят, чтобы пользователи заново приняли информацию восстановления, а затем изменяют публичный ключ на их ID файлах.

6.1.6.2 Настройки необходимые для восстановления пароля ID файлов.

Прежде чем пользователи могут восстанавливать свои ID файлы, Вы должны создать централизованную почтовую базу данных или Mail-Iin базу данных. Эта база данных будет хранить зашифрованные резервные копии ID файлов, и определять информацию, которой администраторы будут пользоваться для восстановления ID файлов. Вы должны исполнить эти шаги прежде, чем любой пользователь потеряет или разрушит свой ID файл.

*2521 Создайте почтовую базу или Mail-In базу данных на сервере, к которому все пользователи и сервера могут получить доступ. Вы можете использовать любой шаблон, чтобы создать базу данных.

*2522 В ACL базы данных, установите доступ по умолчанию – Нет Доступа. Администраторам дайте доступ читателя.

*2523 Из клиента Domino Administrator, выбирайте закладку Настройка, затем выбирайте из панели инструментов справа - Заверение.

*2524 Выбирайте – Данные для восстановления.

*2525 Выбирайте ID файл сертификатора и введите пароль.

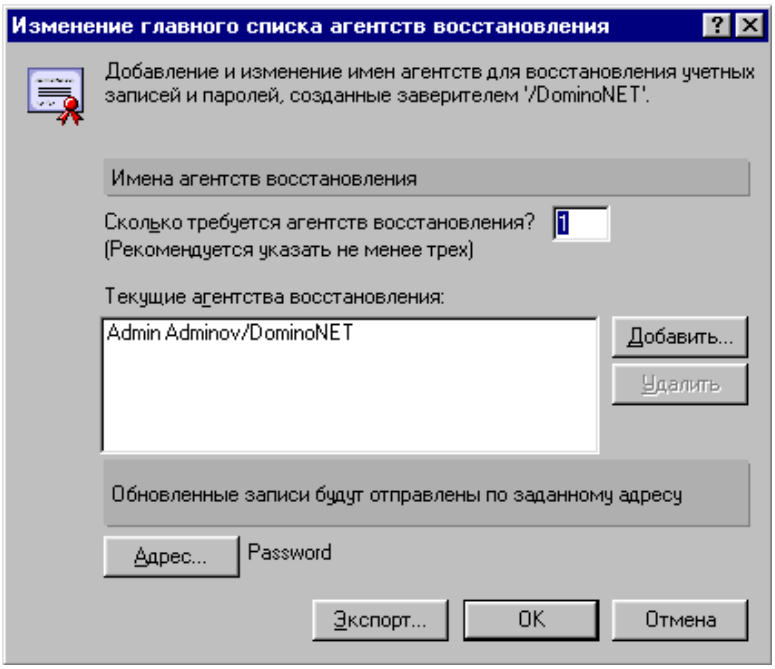


Рис. 98 Диалоговое окно определения администраторов для восстановления пароля ID файла.

*2526 Выбирайте кнопку Добавить и выбирайте имена администраторов, которых Вы назначаете восстанавливать ID файлы.

*2527 Выбирайте кнопку Адрес и выбирайте адрес электронной почты или базу данных Mail-In, которая будет хранить зашифрованные ID файлы.

*2528 Введите число администраторов, требуемых, для отпирания ID файла.

*2529 Щелкает – OK.

*2530 Если пользовательский ID файл еще не содержит информации, для восстановления, выполните процедуру подготовки ID для восстановления.

6.1.6.3 Подготовка к восстановлению ID файлов.

После того, как Вы определяете информацию восстановления в ID файле сертификатора, когда Вы регистрируете пользователей, пользователь IDs автоматически содержит информацию восстановления. Однако если Вы определили информацию восстановления после создания ID пользователя, пользователи должны модернизировать свои ID, для использования информации восстановления. Обновление ID файла информацией восстановления автоматически посылает зашифрованный ID пользователя, в централизованную почтовую базу данных или в Mail-In базу данных. Вы должны закончить эти шаги прежде, чем пользователь потеряет или повредит ID или забудет пароль.

Рассылка информации восстановления пользователям.

Администратор выполняет эти шаги:

*2531 Из клиента Domino Administrator, выбирайте закладку Настройка, затем выбирайте из панели инструментов справа - Заверение.

*2532 Выбирайте – Данные для восстановления.

*2533 Выбирайте ID файл сертификатора и введите пароль.

*2534 Выбирайте кнопку – Экспорт, затем вводят пароль для ID сертификатора.

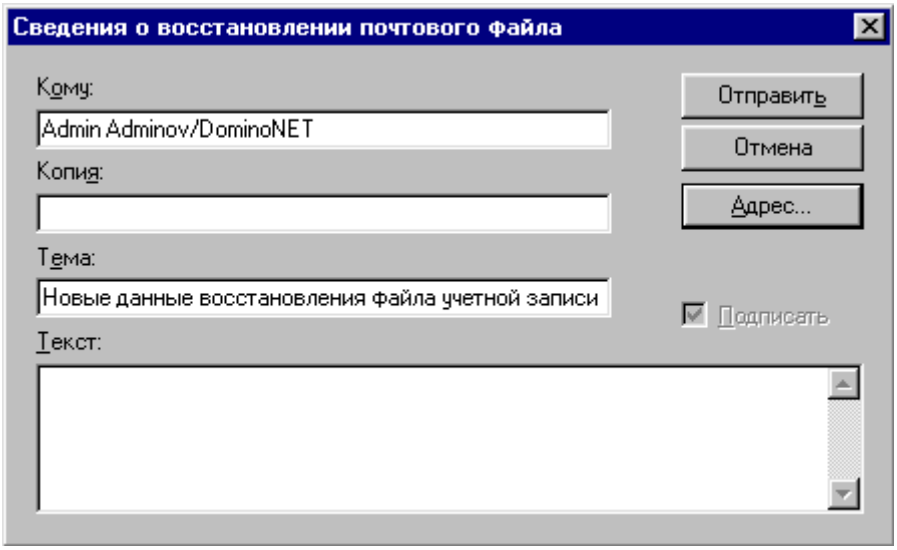


Рис. 99 Диалоговое окно сведений о восстановлении пароля ID файла.

*2535 Заполните эти поля, и затем выбирайте – Отправить

Поле	**Значение**
Кому:	Имена пользователей и групп, чьи ID файлы Вы хотите сохранить.
Копия:	Имена пользователей и групп, кому Вы хотите послать копию сообщения.
Тема:	Информация для пользователей и группы, которая будут появляться в поле Тема сообщения. Если это поле не заполнено, Notes использует следующее: Новые данные восстановления файла учетной записи находятся во вложении. Добавьте их в Вашу учетную запись с помощью команды – Ввод данных для восстановления
Текст:	Информация для пользователей и групп, которая будет появляться в поле сообщения. Domino автоматически прилагает зашифрованную резервную копию файла к сообщению - Вы не должны определить ничего в это поле.

Принятие информации восстановления ID файла

Пользователь заканчивает эти шаги.

*2536 После того, как администратор посылает информацию восстановления, открывайте сообщение в Вашей почтовой базе данных.

*2537 Выбирайте – Действие – Ввод данных для восстановления, затем вводите Ваш пароль.

*2538 Заполните эти поля, затем выбирайте – Отправить.

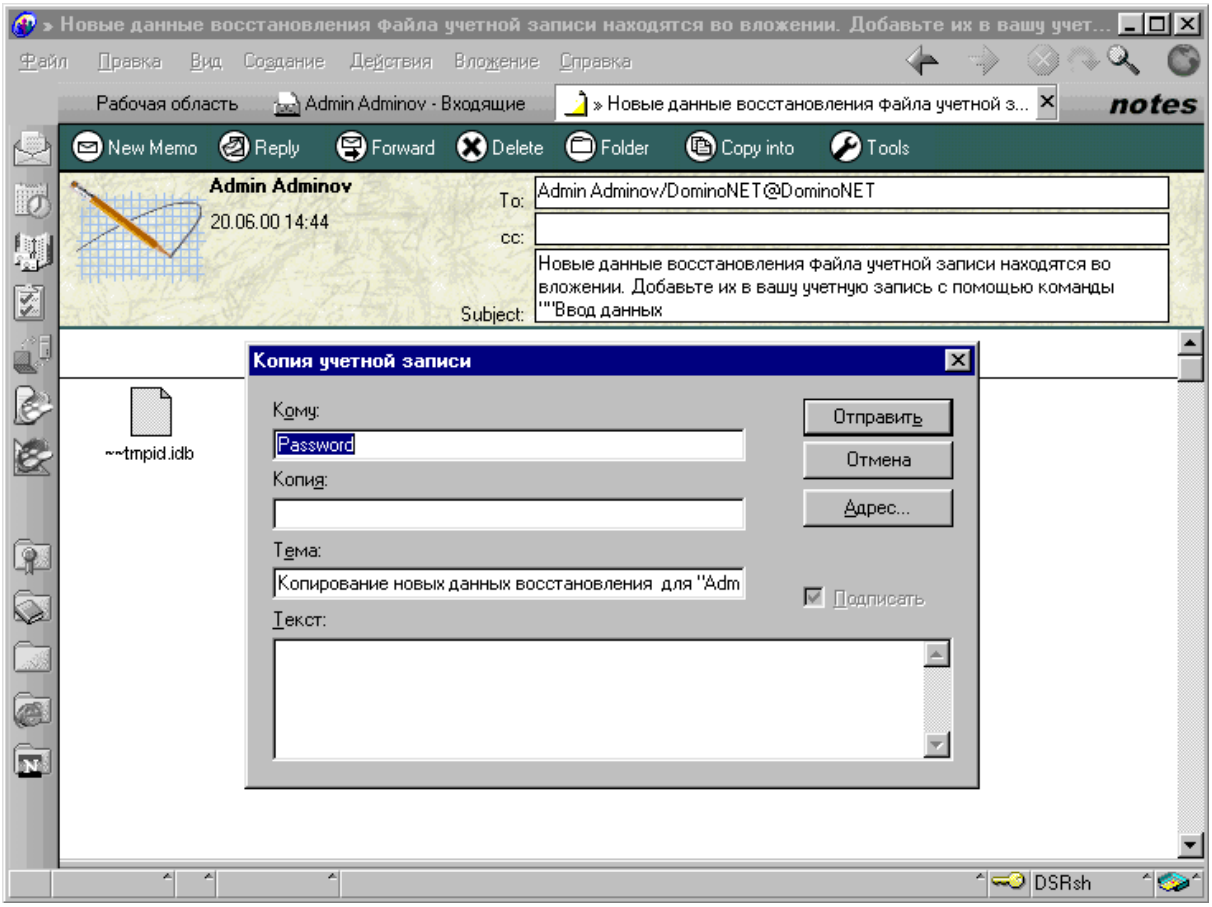


Рис. 100 Пример принятия информации для восстановления пароля в ID файл пользователем.

Поле	**Значение**
Кому:	Имя почтовой базы или Mail-In базы данных, которая будет хранить резервную копию Вашего ID. Domino вводит название базы данных, указанной Вашим администратором.
Копия:	Имена пользователей и групп, которым Вы хотите послать копию сообщения.
Тема:	Информация для администраторов, которая будут появляться в поле Тема сообщения. Если поле не заполнено, Notes использует одно из следующего: Копирование новых данных восстановления для UserName

Текст:	Информация для администраторов, которые будут появляться в поле сообщения. Domino автоматически прилагает резервный из ID файл к сообщению - Вы не должны определить ничего в этом поле.

Domino автоматически посылает зашифрованный резервный ID файл в централизованную почтовую базу или Mail-In базу данных, указанную администратором.

Примечание. Вы может хранить несколько копий ID файлов в централизованной почтовой базе или Mail-In базе данных. Domino создает каждый раз новый документ, с сохраненным ID файлом. При попытке восстановить ID файла, используйте самый последний резервный файл.

6.1.6.4 Восстановление пароля для ID файла.

Если пользователь теряет или портит свой ID файл, или забывает пароль, пользователь может работать с администраторами и восстановить ID файл из резервного.

Запрос резервной копии файла ID

Пользователь делает следующие шаги.

*2539 Если Вы подозреваете, что ID файл поврежден, запросите зашифрованный резервный ID у своего администратора.

*2540 Выбирайте Файл – Сервис – Восстановить учетную запись.

*2541 Выбирайте ID файл, который Вы хотите восстановить.

*2542 Войдите в контакт с первым администратором, внесенным в список, в окна диалога и запросите первый пароль для восстановления ID.

*2543 Введите пароль, полученный от администратора, и затем нажимайте Enter.

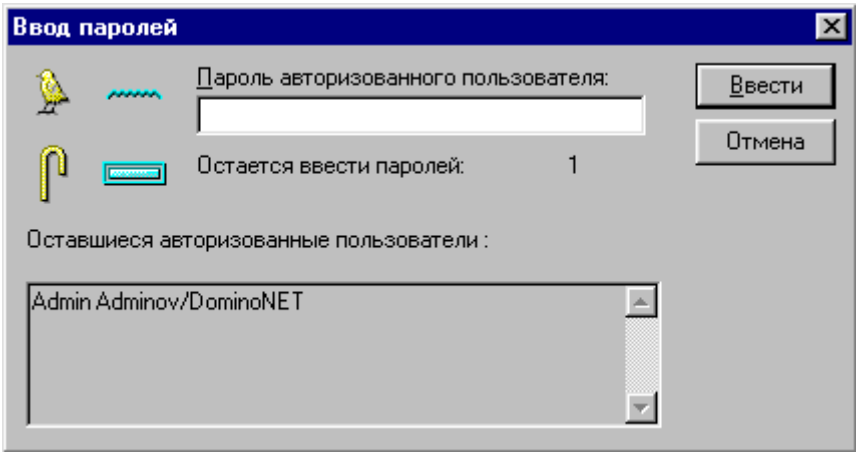


Рис. 101 Диалоговое окно ввода пароля для восстановления пароля ID файла.

*2544 Шаги описанные выше повторите для всех администраторов, пока Вы не получаете число паролей, требуемых, чтобы отпереть файл.

*2545 Введите новый пароль, и затем повторите ввод пароля снова, чтобы подтвердить изменения.

*2546 Если Вы имеете, несколько ID файлов, удалите их и использует копию восстановленного ID файла.

Получение пароля восстановления для ID файла.

Из соображения безопасности, администраторы должны выполнять эти шаги с их собственных рабочих местах. Использование отдельного рабочего места предотвращают от использования программ перехвата. Если неправомочный пользователь получает ID файл администратора и пароль, неправомочный пользователь может получить пароль восстановления администратора для всех ID файлов. Поэтому Вы должны защитить ID файл администратора.

*2547 Отсоедините на локальный диск, зашифрованный резервный ID файл пользователя из почтовой базы или Mail-In базы данных.

*2548 Если ID файл пользователя поврежден, пошлите копию ID файла из централизованной почтовой базы или из Mail-In базы данных пользователю.

*2549 Из клиента Domino Administrator, выбирайте закладку Настройка – Сервис – Заверения – Пароль восстановления.

*2550 Введите пароль ID файла администратора.

*2551 Определите ID файл, который Вы хотите восстановить. Укажите файл, который вы отсоединили.

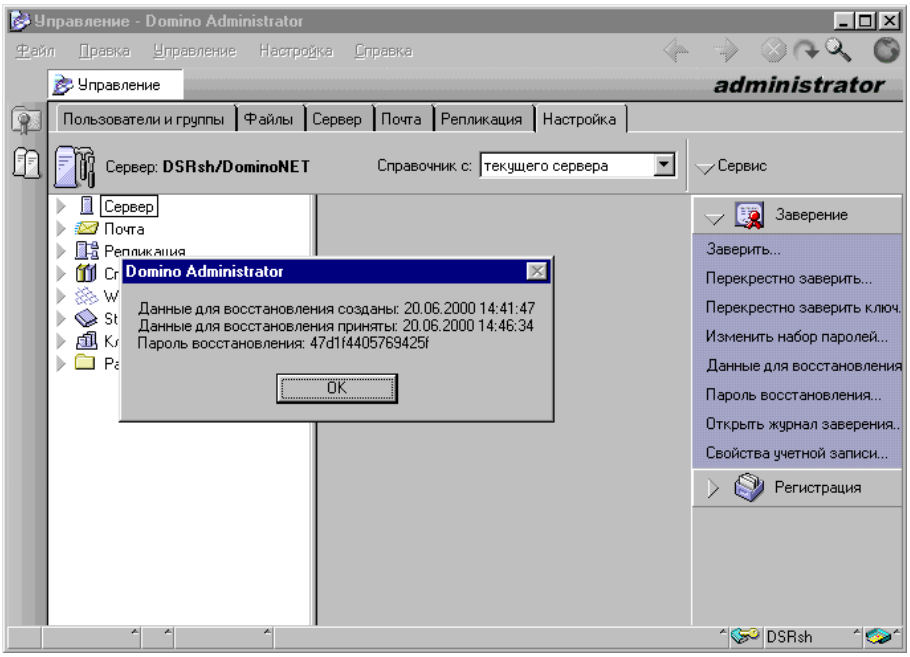


Рис. 102 Информационное окно с паролем восстановления ID файла.

*2552 Администратор дает пользователю пароль администрирования, который будет показан.

6.1.6.5 Изменение информации об администраторах, для восстановления ID файла.

Если администратор оставляет Вашу организацию, Вы должны модернизировать информацию восстановления, используемую пользователем при восстановлении ID файлов и затем посылать новую информацию пользователям, чтобы добавить ее в их ID файлы.

Добавление или удаление имен администраторов.

Администратор с доступом к ID сертификатора заканчивает эти шаги:

*2553 Из Domino Administrator, выбирайте закладку Настройка, затем из панели инструментов справа - Заверение.

*2554 Выбирайте – Данные для восстановления.

*2555 Выбирайте ID файл сертификатора и введите пароль.

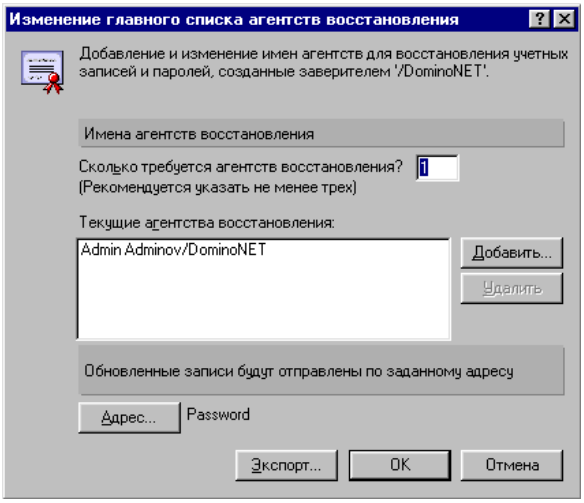


Рис. 103 Диалоговое окно ввода или замены имен администраторов восстановления пароля ID файла.

*2556 Делайте следующее:

- Чтобы удалить администратора, выбирайте его имя и затем нажмите кнопку Удалить.
- Чтобы добавить новых администраторов выбирайте кнопку Добавить, затем выбирайте имена администраторов, которые будут уполномочены восстанавливать ID файлы.

*2557 (Необязательно) Измените число администраторов требуемых для разблокирования ID.

*2558 Когда Вы заканчиваете добавлять или удалять имена, выбирайте – OK.

*2559 Выполните процедуру подготовки к восстановлению ID файлов.

6.1.7 Безопасность публичного ключа.

Каждый ID пользователя Notes и ID Domino сервера имеет уникальный публичный ключ для сертификата Notes. Публичный ключ сохраняется в ID файле и в Person документе или

Server документе для этого ID в Domino Directory. Notes и Domino использует публичный ключ, чтобы идентифицировать пользователей и серверов, проверять цифровые подписи, шифровать сообщения и базы данных.

ID пользователь Notes может также иметь уникальный публичный ключ для интернет сертификата.

Создание новых публичных ключей для Notes сертификатов.

Если Вы подозреваете, что ID был украден или потерян, либо скопирован без разрешения, Вы можете создавать новый публичный ключ для ID. Создание нового публичного ключа позволяет, Вам, продолжать использовать другие части ID - например, ключи шифрования. Это лучше, чем создавать полностью новый ID.

Пользователи Notes могут создавать новый публичный ключ для сертификата Notes. Новый публичный ключ должен быть сертифицирован прежде, чем его можно использоваться Notes.

После сертификации нового публичного ключа, Вы должны настроить сервер, чтобы проверял публичные ключи. Проверка публичных ключей использует соответствие публичному ключу, сохраненному в Domino Directory, с публичным ключом в ID файле. При проверке публичного ключа неправомочный пользователь, со старым публичным ключом, не получит доступ на сервер

Добавление существующего публичного ключа в Domino Directory.

Когда Вы регистрируете пользователя или сервер, Domino автоматически добавляет публичные ключи Notes в Person документу или Server документу. Domino также автоматически добавляет интернета публичный ключ к Person документу, когда Вы выпускаете интернет сертификат, для пользователей. Однако Вы можете вручную добавить публичный ключ ID сервера или пользователя в Domino Directory в этих ситуациях:

*2560 Пользователь хочет послать шифрованную почту пользователю Notes в другом домене или пользователю, который использует S/MIME приложение, для отправки почты. Чтобы посылать S/MIME или Notes шифрованную почту, Domino должен иметь доступ к интернет сертификату получателя или публичному ключ Notes. Если получатель находится в другом домене и Domino Directory для этого домена, сохранен на сервере в домене отправителя, то Domino не может получить доступ к публичному ключу получателя для шифрования. Отправитель должен получить публичный ключ получателя и добавлять его в персональную адресную книгу или в Domino Directory.

*2561 Пользовательский или публичный ключ сервера в Domino Directory становится известен или случайно удален, и администратор должен заменить его.

6.1.7.1 Создание нового публичного ключа Notes и добавление его в Domino Directory.

Создание и сертификация нового публичного ключа требует следующих процедур, которые описаны ниже:

*2562 Пользователь создает новый публичный ключ и представляет его для сертификации.

*2563 Администратор Сертификатор - сертифицирует публичный ключ пользователя и добавляет его в Domino Directory.

*2564 Пользователь сливает новый сертификат в ID файл пользователя.

Создание нового публичного ключа Notes.

Владелец ID исполняет эти шаги.

*2565 Выбирайте Файл – Сервис – Учетная запись.

*2566 Ведите пароль (если требуется).

*2567 Выбирайте – Дополнительно – Создать общий ключ.

*2568 Когда Вы видите, предупреждение, что на создание ключа потребуется время, нажимайте – OK, чтобы продолжить.

*2569 Выбирайте адрес администратора или сертификатора для сертификации или адресуйте записку напрямую сертификатору - например /East/Acme. Domino отправляет запрос человеку, обозначенному в секции администрирования, соответствующего документа сертификата в виде Сертификаты из Domino Directory.

*2570 Выбирайте – Отправить.

Ресертификация ID и добавление публичного ключа в Domino Directory.

Администратор - Сертификатор исполняет эти шаги.

*2571 Открывает почтовый запрос сертификации.

*2572 Выбирайте – Действие – Заверить вложенную учетную запись.

*2573 Выбирайте ID сертификатора для использования и нажимайте – OK.

*2574 Введите пароль для ID и нажимайте – OK.

*2575 Выбирайте – Заверить.

*2576 (Необязательно) Выбирайте - Сервер, для выбора сервера и нажимайте – OK, чтобы изменить сервер регистрации. Регистрационный сервер - сервер, чей Domino Directory будет обновлен.

*2577 (Необязательно) Измените дату истечения сертификата.

*2578 (Необязательно) Определяйте минимальную длину пароля.

*2579 Выбирайте – Заверить. Имя ID владельца появляется в поле Кому:, объяснительный текст появляется в поле Тема: окна сертификации, для отправки заверенной учетной записи.

*2580 (Необязательно) Выбирайте – Подписать, чтобы доказать, что Вы - отправитель ID.

*2581 Выбирайте – Отправить.

Принятие нового сертификата в ID файл.

ID владелец исполняет эти шаги.

*2582 Открывает почтовый запрос сертификации.

*2583 Выбирайте – Действие – Принять сертификат. В окне будет показана информация о новом ключе и сертификаторе, который заверил ID

Проверка публичного ключа Notes.

Проверка публичных ключей Notes сохраненных в Domino Directory помогает предотвращать неправомочного пользователя или сервер от вызова другого сервера.

*2584 Из клиента Domino Administrator, выбирайте закладку Настройка, откройте Server документ для сервера.

*2585 Выбирайте закладку Security.

*2586 В секции Security Sittings, выбирайте – Yes, в поле Compare Notes public keys against those stored in Directory.

*2587 Сохраните документ.

*2588 Перезапустите сервер, чтобы изменения вступили в силу.

6.1.7.2 Добавление публичного ключа Notes в Domino Directory.

Вы можете копировать публичный ключ Notes в файл или отправлять его пользователю или администратору, который вставит публичный ключ в персональную адресную книгу или в Domino Directory. Это позволяет пользователям шифровать почту, посланную пользователю в другую организацию.

Как послать публичный ключ по почте.

*2589 Выбирайте Файл – Сервис – Учетная запись.

*2590 Ведите пароль (если требуется).

*2591 Выбирайте кнопку Дополнительно – Отправить общий ключ.

*2592 Адресуйте письмо человеку, который будет вставлять ключ в Domino Directory или в персональную адресную книгу.

*2593 (Необязательно) В поле Копия:, введите имена любых других людей, которых Вы хотите уведомить относительно запроса.

*2594 (Необязательно) Выбирайте - Подписать или Шифровать, чтобы доказать, что Вы - отправитель ID.

*2595 Выбирайте – Отправить.

Копирование публичного ключа в файл.

*2596 Выбирайте Файл – Сервис – Учетная запись.

*2597 Ведите пароль (если требуется).

*2598 Выбирайте кнопку Дополнительно и выбирайте – Копировать общий ключ.

*2599 Спасите содержание буфера обмена в файле.

*2600 Передайте файл тому, кто будет вставлять его в Domino Directory или в персональную адресную книгу.

Вставка публичного ключа в персональную адресную книгу.

*2601 В Вашей персональной адресной книге, создайте документ Контакта для владельца общественного ключа.

*2602 Выбирайте закладку Дополнительно, откройте файл или почтовое сообщение, которое содержит публичный ключ.

*2603 Скопируйте публичный ключ в буфер обмена и вставьте его в поле Заверенный общий ключ, документа Контакта.

*2604 Сохраните документ.

Вставка публичного ключа в Domino Directory.

*2605 Из клиента Domino Administrator, делайте одно из следующего:

- Выбирайте закладку Пользователи и группы, затем – Edit Person.
- Выбирайте закладку Настройка, затем – Edit Server.

*2606 Выбирайте – Certificates – Notes Certificates – Notes certified public keys, в Person документе, или закладка Administration – Certified public keys, Server документа.

*2607 Открывайте файл или почтовое сообщение, который содержит публичный ключ.

*2608 Скопируйте публичный ключ в буфер обмена и вставьте его в одно из полей:

- Поле Public certified key, для иерархических сертификатов Domino.
- Поле Flat name key, для Person документа, неиерархических сертификатов Domino.

Примечание. Вы не может вставлять сертификат интернета в Person документ или Server документ.

*2609 Сохраните Person документ или Server документ.

6.1.7.3 Использование взаимных сертификатов серверов и рассылки подписанных S/MIME сообщений.

Domino использует два типа взаимных сертификатов: Notes и интернет сертификатов. Взаимные сертификаты Notes позволяют пользователям в различных иерархически сертифицированных организациях доступ на сервера, и получать подписанные сообщения почты. Взаимные сертификаты интернет позволяют пользователям получать подписанные и шифрованные почтовые сообщения и посылать зашифрованные почтовые сообщения.

В иерархических именах Notes, Вы неявно доверяете сертификатам, выпущенным любым из Ваших предков. Например, John/Sales/NYC/Acme может доверять NYC/Acme, чтобы выпустить сертификаты для Services/NYC/Acme или Sally/Accounting/NYC/Acme. Но если Вы не имеете общего предка с пользователем или сервером, Вы нуждаетесь во взаимном сертификате, чтобы доверять пользователю или серверу. Когда Вы или один из Ваших предков создаете взаимный сертификат, Вы доверяете общественному ключу, указанному в том сертификате.

Например. Взаимный сертификат Fred/Sales/ABC, в действительности говорит следующее – I trust that Fred has a trustworthy public key - я полагаю, что можно доверять общественному ключу Фреда.

Если Вы выпускаете взаимный сертификат Authority Certificate интернета, Вы доверяете CA, чтобы выпустить сертификаты пользователям и серверов, ниже в дереве имен.

Например. Взаимный сертификат Sales/ABC означают, что Вы доверяете Sales/ABC, чтобы выпустить сертификат для Fred/Sales/ABC.

Взаимные сертификаты Notes.

Чтобы позволить пользователям и серверам из различных иерархически сертифицированных организаций доступ на сервера в другой организации, Вы используете взаимные сертификаты. Каждая организация выпускает взаимный сертификат для ID из другой организации, затем хранит взаимный сертификат, который он выпускает в персональной адресной книге или в Domino Directory.

Например, если Alan Jones/Sales/East/Acme хочет получить доступу к серверу Support/Seascape, он нуждается во взаимном сертификате от /Seascape, а сервер Support/Seascape нуждается во взаимном сертификате для /Sales/East/Acme. Когда Alan Jones/Sales/East/Acme пробует получить доступ на сервер, он (сервер) проверяет взаимные сертификаты. Если сервер находит сертификат, он проверяет, позволяется ли Alan Jones/Sales/East/Acme доступ на сервер.

Вы также используете взаимные сертификаты, чтобы проверить цифровую подпись пользователя из другой организации. Обратите внимание, чтобы проверить подпись, взаимный сертификат необходим только в одном направлении, проверяющий нуждается во взаимном сертификате для подписывающего лица.

Взаимные сертификаты могут создаваться в различных уровнях организации. Например, чтобы позволить каждому пользователю в пределах одной организации, регистрироваться на сервере в другой организации, каждая организация имеет взаимный сертификат для сертификата другой организации в Domino Directory. Взаимные сертификаты могут также выпускаться на уровне индивидуальных пользователей или ID серверов.

Пример. Чтобы позволить единственному пользователю регистрироваться на любом сервере в другой орг. единице организации, или проверить цифровой подпись пользователя в этой орг. единице, ID пользователя нуждается во взаимном сертификате для орг. единицы. Организация в свою очередь нуждается во взаимном сертификате этого пользователя.

Два взаимных сертификата не обязательно должны быть симметричными.

Пример. Одна организация может иметь взаимный сертификат для орг. единицы, а другая организация может иметь взаимный сертификат для сертификата организации.

Если Вы имеете взаимные сертификаты для организации, или сертификат орг. единицы, настройте сервер для ограничения доступа, на определенные сервера, которые хранят конфиденциальную информацию. Позвольте серверам Вашей организации доступ на сервера другой организации, но запретите серверам этой организации доступ, на Ваши сервера. Обменяйтесь взаимными сертификатами, как требуется, но настройте на серверах списки доступа, чтобы запретить доступ серверов из других организаций.

Сервера хранят взаимные сертификаты в Domino Directory. Для доступа на сервера, пользователи хранят копии взаимных сертификатов в своих персональных адресных книгах. Взаимные сертификаты, сохраненные в персональных адресных книгах пользователя, используются только этим пользователем - то есть только пользователем, который имеет взаимный сертификат, может использовать его.

Взаимный сертификат интернет.

Взаимный сертификат интернета - сертификат для интернет клиента, который утверждает идентичность пользователя или сервера и утверждает идентичность Authority Certificate (CA), который сертифицировал пользователя или сервер. Взаимный сертификат интернет гарантирует получателю шифрованного сообщения S/MIME, что сертификату отправителя можно доверять и что сертификат имеет силу, для подписанного сообщения S/MIME. Он также подтверждает идентичность сервера, когда клиент Notes использует SSL, для доступа на интернет сервер.

Взаимные сертификат интернета сохраняются в документах “Контакта” в персональных адресных книгах и могут использоваться только пользователем, для которого они были выпущены.

Взаимный сертификат интернета может быть помечен специальной опцией доверия, доверять сертификату или не доверять. Отмечая взаимный сертификат опцией - не доверять, пользователи могут запретить посылать или получать зашифрованную или подписанную почту, без удаления взаимного сертификата из персональной адресной книги. Сертификаты интернет автоматически добавляются к персональной адресной книге и автоматически получают статус - доверия.

6.1.8 Примеры применения взаимных сертификатов.

Идентификация всех серверов и пользователей в разных организациях.

Этот пример описывает шаги, которые проделывают две компании Acme и ABC, чтобы позволить всем пользователям и серверам, в обеих организациях, опознавать друг друга.

*2610 Сертификатор организации Acme, сертификат /Acme, получает взаимный сертификат для сертификатора организации ABC и сохраняет его в Domino Directory для компании Acme.

*2611 Сертификатор организации ABC, сертификат /ABC, получает взаимный сертификат для сертификатора организации Acme и сохраняет его в Domino Directory для компании ABC.

Идентификация только избранных серверов и пользователей в разных организациях.

Компания Acme хочет позволить пользователям из компании Seascape, у кого имеется иерархический сертификат /AppDevelopment/Seascape, доступ клиентов на сервер с именем CSSUPPORT/East/Acme, компании Acme.

*2612 Сертификатор орг. единицы /East/Acme, компании Acme, имеет взаимный сертификат для орг. единицы /AppDevelopment/Seascape компании Seascape и хранит его в Domino Directory, компании Acme.

*2613 Сертификатор орг. единицы /AppDevelopment/Seascape, компании Seascape, имеет взаимный сертификат для орг. единицы /East/Acme компании Acme и хранит его в Domino Directory, компании Seascape.

Эти взаимные сертификаты позволяют пользователям Kelly Jones/AppDevelopment/Seascape и Jonathan Moutal/AppDevelopment/Seascape получить доступ на сервер CSSUPPORT/East/Acme. Однако они не позволяют пользователям получить доступ на сервер Acme Mail-W/West/Acme.

Рассылка шифрованной почты S/MIME.

Alan Jones имеет интернет сертификат, выпущенный от имени CA Acme. Dave Lawson имеет интернет сертификат, выпущенный от имени CA ABC. Если Alan Jones и Dave Lawson хотят обмениваться шифрованными сообщениями S/MIME, они должны иметь:

*2614 Alan Jones - в своей персональной адресной книге должен иметь, взаимный сертификат для ABC, которому доверяют.

*2615 Dave Lawson - в своей персональной адресной книге должен иметь, взаимный сертификат для Acme, которому доверяют.

В этом случае Alan Jones и Dave Lawson смогут посылать шифрованные сообщения S/MIME друг другу.

6.1.8.1 Как добавить, затребованный взаимный сертификат интернет или Notes?

Когда пользователи получают доступ на сервер или получают подписанное сообщение, они могут принимать взаимные сертификаты Notes или интернета, от другой организации. Domino добавляет взаимный сертификат в персональную адресную книгу. При этом в следующий раз, когда пользователь затребует доступ к серверу, или попытается подписать почтовое сообщение, сервер может идентифицировать пользователя или проверять подпись.

Вы можете также добавить взаимный сертификат в Notes Domino Directory, так чтобы все пользователи могли использовать его. Однако пользователи должны всегда добавлять взаимные интернет сертификаты в их персональные адресные книги.

Как добавить взаимный сертификат Notes в Domino Directory?

При использовании рабочей станции Notes, Вы делаете попытку доступа на сервер в организации, с которой пользователи не имеют взаимного сертификата.

*2616 Когда Domino показывает сообщение с предупреждением, выберите кнопку – Advanced Options:

Ваш локальный Domino Directory не содержит взаимного сертификата для организации обозначенной ниже. Поэтому Вы не можете убедиться, что документы, подписанные членами этой организации подлинны, или, что Вы фактически общаетесь с тем сервером, за который он (сервер) себя выдает, потому что Вы не можете проверять, что ключ приведенный ниже правилен.

Вы хотите, не показывать это предупреждение в будущем, создавая взаимный сертификат для этой организации?

*2617 Чтобы избежать возможности, сертифицировать самозванца, обратитесь к кому-либо, кто заслуживающего доверия, из названной организации и запросите его, чтобы он сообщил Вам общественный ключ организации. Сравните его с ключом, показанным в окне Advanced Options. Если сравнение ключей проходит, заполните эти поля:

Поле	**Значение**
Certifier	Имя ID файла сертификатора Вашей организации

Server	Место положение Domino Directory, куда будет помещен взаимный сертификат
Subject name	Организация или орг. единица, для которой Вы хотите выпустить взаимный сертификат Например – /Acme
Subject alternate name list	Дополнительное имя, как правило, имя на родном языке, если такое.
Expiration date	Дата истечения взаимного сертификата

*2618 Выбирайте – Заверить. Domino размещает взаимный сертификат в представлении - Server – Certificates Domino Directory, на сервере, который Вы определили.

6.1.8.2 Как добавить взаимный сертификат Domino по телефону?

Две организации могут добавлять взаимные сертификаты пользователю, серверу или сертификатору, имея имя и общественный ключ ID, чтобы бы получить сертификат по телефону. Для получения взаимного сертификата, эти шаги должны быть выполнены с каждой из требующей взаимные сертификаты организации, поочередно.

Вы не можете использовать эту процедуру, для создания взаимного сертификата интернет.

Запрос взаимного сертификата для ID пользователя, сервера или сертификатора.

Используйте эти шаги, чтобы добавить взаимный сертификат для пользователя сервера или сертификатора, орг. единицы, когда Вы имеете доступ к ID пользователя, сервера или сертификатора.

*2619 Из клиента Domino Administrator, выбирайте закладку Настройка.

*2620 Выбирайте из панели инструментов Сервис – Заверение – Свойство учетной записи.

*2621 Выбирает ID файл пользователя, сервера или сертификатора и нажимайте – Открыть.

*2622 Введите пароль (если требуется).

*2623 С закладки Общие, запишите полное имя. Например, Alan Jones/Sales/East/Acme, Mail-E/East/Acme, или /Acme.

*2624 Запишите значение основного ключа, точно так, как он отображается, включая пробелы в поле Основной ключ. Не путайте с полем Общий ключ, на закладке - Сертификаты.

*2625 Позвоните в организацию, которая добавит взаимный сертификат, и сообщите имя пользователя и ключ, точно так, как Вы записали их.

Запрос взаимного сертификата для предка сертификата ID.

Используйте эти шаги, чтобы добавить взаимный сертификат для организации или орг. единицы, когда Вы имеете доступ к ID пользователя или сервера.

*2626 Из клиента Domino Administrator, выбирайте закладку Настройка.

*2627 Выбирайте из панели инструментов Сервис – Заверение – Свойство учетной записи.

*2628 Выбирает ID файл пользователя, сервера или сертификатора и нажимайте – Открыть.

*2629 Введите пароль (если требуется).

*2630 Выбирайте закладку Сертификаты, в поле Сертификат выдан от имени, выбирайте сертификат, для которого Вы хотите получить взаимный сертификат.

*2631 Запишите точное имя сертификата.

*2632 Запишите значение общего ключа точно, как оно отображается в информационном поле Общий ключ, включая пробелы.

*2633 Звоните в организацию, которая добавит взаимный сертификат, и передайте имя и общий ключ, точно так, как Вы записали их.

Как добавить взаимный сертификат в Domino Directory или Personal Address Book?

После того, как кто-то из другой организации передал Вам имя и публичный (общий) ключ по телефону, используйте этими шаги, чтобы добавить взаимный сертификат для ID.

*2634 Из клиента Domino Administrator, выбирайте закладку Настройка.

*2635 Выбирайте из панели инструментов Сервис – Заверение – Перекрестно заверить ключ.

*2636 Выбирайте файл сертификатора и затем выбирайте – OK.

*2637 Введите пароль для сертификатора.

*2638 В поле Имя, введите полное иерархическое имя для ID, полученного Вами для создания взаимного сертификата.

*2639 Введите общий ключ для ID, который Вы получили по телефону, включая пробелы.

*2640 (Необязательно) Измените дату истечения сертификата. По умолчанию - 10 лет.

*2641 (Необязательно) Нажмите кнопку Заверитель, чтобы выбрать нужного сертификатора, от имени которого будет выпущен взаимный сертификат.

*2642 (Необязательно) Нажмите кнопку Сервер, выбирайте регистрационный сервер, чей Domino Directory будет хранить взаимный сертификат. Чтобы сохранить сертификат в персональной адресной книге пользователя, выберите Локальный компьютер. Нажимайте клавишу OK.

*2643 Нажимайте кнопку Заверить. Domino размещает взаимный сертификат в представлении - Server – Certificates, Domino Directory выбранного регистрационного сервера.

6.1.8.3 Как добавить взаимный сертификат Domino для ID файлов, используя для этого почту?

Организации, которые не могут связываться через почту Notes, могут использовать эти шаги, чтобы добавить взаимный сертификат Domino для пользователя, сервера и ID

сертификатора. Для взаимного сертифицирования, Вы должны выполнить эту процедуру дважды, с каждой стороны поочередно.

Вы не можете использовать эту процедуру, чтобы создать взаимные сертификаты интернет.

Создание безопасной копии ID файла.

Используйте эти шаги, чтобы создать безопасную копию пользователя, сервера или ID сертификатора, чтобы сертифицировать ее.

*2644 Из клиента Domino Administrator, выбирайте закладку - Настройка.

*2645 Выбирайте из панели инструментов – Сервис – Заверение – Свойство учетной записи.

*2646 Выбирает ID файл пользователя, сервера или сертификатора и нажимайте – Открыть.

*2647 Введите пароль (если требуется).

*2648 На закладке Дополнительно, выбирайте – Создать защищенную копию.

*2649 Выбирайте путь и название для файла безопасной копии, и затем – OK. Имя по умолчанию для файла - SAFE.ID.

*2650 Скопируйте файл на дискету.

*2651 Использует почту, чтобы послать дискету администратору в другую организацию.

Как добавить взаимный сертификат, используя безопасную копию ID файла?

Используйте эти шаги, чтобы добавить взаимный сертификат в Domino Directory.

*2652 Из клиента Domino Administrator, выбирайте закладку - Настройка.

*2653 Выбирайте из панели инструментов – Сервис – Заверение – Перекрестно заверить.

*2654 Выбирает файл сертификатора, который выпустит взаимный сертификат и затем – OK.

*2655 Введите пароль для сертификатора.

*2656 Выбирайте ID файл безопасной копии, для заверения и затем – OK.

*2657 Заполните одно или большее количество этих полей:

Поле	**Значение**
Subject name	Имя организации или орг. единица, для взаимного сертифицирования. Например, /Acme
Subject alternate name list	Альтернативное имя
Expiration date	Дата истечения взаимного сертификата
Certifier	Полное имя сертификатора Вашей организации
Server	Сервер, в Domino Directory которого будет хранится копия взаимного сертификата

*2658 Нажмите – Заверить. Domino создаст взаимный сертификат.

6.1.8.4 Как добавить взаимный сертификат Domino для ID, используя почту Notes?

Если Вы можете передавать почту в организацию, которая будет взаимно сертифицировать пользователя, сервер, или ID сертификатора, Вы можете использовать почту Notes, чтобы добавить взаимный сертификат Domino. Для взаимного сертифицирования, эти шаги должны быть выполнены дважды, с каждой стороны в организациях поочередно.

Вы не можете использовать эту процедуру, для создания сертификатов интернета.

Отправка ID для взаимного сертифицирования.

*2659 Выбирайте из меню Файл – Сервис – Учетная запись и вводите пароль.

*2660 На закладке Сертификаты, нажмите кнопку - Запросить перекрестный.

*2661 Выбирает пользователя, сервер, или ID сертификатора, для кого Вы хотите создать взаимный сертификат, и затем выбирайте – OK.

*2662 Введите пароль (если требуется).

*2663 Адресуйте запрос на взаимный сертификат администратору или сертификатору другой организации, и затем нажимайте – Отправить.

Выпуск взаимного сертификата для ID.

*2664 Открывайте запрос, на взаимный сертификат, полученный по почте.

*2665 Выбирайте из меню Действия – Заверить перекрестно вложенную учетную запись.

*2666 Выбирайте файл сертификатора, который выпустит взаимный сертификат, затем – OK.

*2667 Введите пароль для сертификатора.

*2668 Заполните одно или большее количество этих полей:

Поле	**Значение**
Subject name	Имя организации или орг. единица, для взаимного сертифицирования. Например, /Acme
Subject alternate name list	Альтернативное имя
Expiration date	Дата истечения взаимного сертификата
Certifier	Полное имя сертификатора Вашей организации
Server	Сервер в Domino Directory которого будет хранится копия взаимного сертификата

*2669 Нажмите – Заверить. Domino создаст взаимный сертификат.

6.1.8.5 Как добавить взаимный сертификат интернета от интернет сервера?

Пользователи могут получить взаимные сертификаты интернет непосредственно от интернет сервера. Этот метод может быть самый быстрый способ получить взаимный сертификат интернета. Чтобы сделать это, инструктируйте Ваших пользователей сделать следующее:

*2670 Удостоверится, что Вы имеете доступ к серверу, на котором сертификат сохранен, и что Вы знаете адрес интернета сервера.

*2671 Если Вы используете Proxy сервер для доступа в интернет, удостоверьтесь, что настроили секцию Proxy в документе места вызова.

*2672 Выбирайте из меню Файл – Сервис – Добавить перекрестный сертификат интернета.

*2673 В поле Имя сервера, введите адрес интернета сервера, на котором сертификат хранится, и нажимайте кнопку Связь.

*2674 (Необязательно), если сервер не отвечает по порту HTTP, выберите другой протокол, для соединения с интернет сервером. Notes использует SSL связь с сервером, чтобы добавить сертификат.

*2675 Выбирайте сертификат, для которого Вы хотите добавить взаимный сертификат.

*2676 Выбирайте – Заверитель. Это - ID, которым сертификат будет сертифицирован. Выберите ID, затем введите пароль, если необходимо.

*2677 Выбирайте – Сервер. Это сервер, Domino Directory которого будет хранить взаимный сертификат. По умолчанию, это - персональная адресная книга, в локальном каталоге данных.

*2678 Выбирайте – Заверить.

6.1.8.6 Создание взаимного сертификата для пользователя из Person документа.

Вы можете создавать взаимные сертификаты Notes и или интернет, из сертификатов, сохраненных в документе Person пользователя.

*2679 Делает одно из следующего:

- Из клиента Domino Administrator, выбирайте закладку - Пользователи и группы и откройте Person документ для пользователя, которому вы хотите создать взаимный сертификат.
- В персональной адресной книге, откройте документ – Контакт, для пользователя, которому хотите создать сертификат

*2680 Выбирайте - Действия – Create Cross Certificate (Создать взаимный сертификат).

*2681 Выбирает сертификат, для взаимного сертификата.

*2682 Заполните эти поля и затем нажимайте – Заверить:

Поле	**Значение**

Certifier	Имя сертификатора ID. По умолчанию, Ваш сертификатор ID. Если Вы имеете доступ, Вы можете выбирать и другой ID выше Вашего в Вашей иерархии организации.
Server	Регистрационный сервер, который проводит взаимное сертифицирование. По умолчанию, сертификат сохраняется локально, в Вашей персональной адресной книге. Вы можете выбирать другой сервер для сохранения взаимного сертификата.
Subject name	Имя, кто будет сертифицирован.
Subject alternate name list	Альтернативное имя
Public Key	Публичный ключ
Expiration date	Дата истечения взаимного сертификата

*2683 Повторите эти шаги для каждого пользователя, для которого Вы хотите создать взаимные сертификаты.

6.1.9 Просмотр взаимных сертификатов.

Просмотреть взаимные сертификаты можно из клиента Domino Administrator. Выбирайте закладку Настройка, представление Разное – Сертификаты. Сертификаты показываются в представлении по категориям, согласно типу:

*2684 Internet cross-certificates

*2685 Notes cross-certificates

*2686 Internet certifiers

*2687 Notes certifiers

Сертификаты, чей тип не может быть определен, внесен в список как - Unknown.

6.2 Шифрование и электронная подпись

Глава описывает, как использовать шифрование, подписывать сообщения и как использовать цифровую подпись, чтобы проверить автора сообщения.

6.2.1 Шифрование

Шифрование защищает данные от неправомочного доступа. Используя Notes и Domino, Вы может шифровать:

*2688 Сообщения, посланные другим пользователям. При этом неправомочный пользователь не сможет прочитать сообщение, в то время как оно находится в процессе доставки. Вы можете также зашифровать уже сохраненные и поступающие сообщения.

*2689 Сетевые порты. Когда Вы шифруете информацию, посланную между рабочей станцией Notes и Domino сервером или между двумя Domino серверами, неправомочный пользователь не сможет читать данные, в то время как они находится в процессе передачи.

*2690 Когда Вы используете SSL, чтобы шифровать информацию, посланную между клиентом интернета и Domino сервером или рабочей станцией Notes и интернет сервером, неправомочный пользователь не может считать данные, в то время как они находится в процессе доставки.

*2691 Поля, документы и базы данных. Разработчики могут шифровать поля в документе, полный текст документа или локальные базы данных. Тогда только указанные пользователи смогут читать эту информацию.

6.2.1.1 Публичные и личные ключи шифрования.

Для всех типов шифрования, кроме шифрования сетевых портов, Domino использует публичные и личные ключи так, чтобы данные, зашифрованные одним из ключей, могли быть расшифрованы только другой стороной другим ключом.

Публичные и личные ключи математически связаны и уникально идентифицируют пользователя. Публичные и личные ключи сохраняются в ID файле. Публичный ключ также сохраняется в Domino Directory, где он доступен другим пользователям, и в некоторых случаях в персональных адресных книгах некоторых пользователей.

Domino использует два набора публичных и личных ключей - Notes и интернет. Вы используете Notes публичные и личные ключи, чтобы шифровать поля, документы, базы данных и сообщения, посланные другим пользователям Notes. Вы используете интернет публичные и личные ключи, чтобы посылать и получить шифрованный сообщения S/MIME и шифровать сессии SSL между рабочими станциями Notes и интернет серверами.

Когда Вы регистрируете пользователей, Domino автоматически создает публичные и личные ключи для пользователя, добавляет их к ID файлу, добавляет публичный ключ в Domino Directory. Вы можете также создавать для интернет, публичные и личные ключи после регистрации пользователя. Domino добавляет интернет личные ключи к ID файлу. Domino хранит сертификаты интернета (которые содержат публичные ключи) в ID файле, а также в Domino Directory.

Чтобы создавать публичные и личные ключи, Domino использует Dual-key RSA Cryptosystem и RC2 и RC4 алгоритмы для шифрования. Чтобы создавать интернет, публичные и личные ключи, Domino используют X.509 формат сертификатов, который является промышленным форматом стандарта, который используют многие приложения, включая Domino.

Размер публичных ключей зависит от того, имеет ли пользователь Северо-Американскую или Международную лицензию Notes.

6.2.2 Шифрование почты.

Шифрование почты защищает сообщения от неправомочного доступа. Только тело почтового сообщения шифруется, информация заголовка - например, Кому:, От Кого:, поля Тема: - нет.

Пользователи Notes могут шифровать почту, посланную другим пользователям Notes или пользователям приложений почты, которые поддерживают S/MIME - например, IE и Netscape.

Пользователи могут шифровать почту, посланную другим пользователям Notes, полученную от других пользователей Notes, или шифровать все документы, сохраненные в почтовой базе данных. Notes использует публичный ключ получателя, который сохранен в персональной адресной книге или в Domino Directory, чтобы шифровать уходящую и сохраненную почту.

Вообще, почта, посланная пользователям в другой, не-Notes домен, не может быть шифрована. Однако если получатель почты использует Notes, и отправитель имеет доступ к публичному ключу получателя, отправитель может шифровать почтовое сообщение. Публичный ключ получателя может быть сохранен или в Domino Directory, к которому отправитель имеет доступ, или в персональной адресной книге отправителя.

Когда пользователи Notes посылают почту получателям, которые используют почтовые приложения, поддерживающие S/MIME, пользователи Notes могут использовать S/MIME, чтобы шифровать сообщения. Отправители должны иметь публичный ключ получателя, чтобы шифровать сообщение. Публичный ключ получателя сохраняется в X.509 сертификате, персональной адресной книге отправителя, или в Domino Directory.

Шифрование сообщений не затрагивает скорость, с которой сообщение будет идти от отправителя получателю. Однако шифрование увеличивает время, требуемое, чтобы послать и открыть сообщение. Дополнительное время требуется на шифрование в начале передачи и на дешифрование, каждый раз, когда получатель открывает сообщение. Время, требуемое для послания и открытие сообщения, зависит от размера сообщения и количества графики, объектов и приложений к сообщению. В большинстве случаев, задержка не значительная.

6.2.2.1 Как работает шифрование исходящей почты Notes?

*2692 Отправитель посылает сообщение и выбирает опцию шифрования.

*2693 Notes производит случайный ключ шифрования и шифрует сообщение им.

*2694 Notes шифрует случайный ключ шифрования с использованием публичного ключа получателя, который он получает из Domino Directory или персональной адресной книги и добавляет в конец сообщения новый ключ. Публичный ключ получателя должен быть сохранен или в Domino Directory, указанном в установке имени в файле NOTES.INI или в персональной адресной книге отправителя.

*2695 Если зашифрованное сообщение адресовано нескольким получателям, сообщение шифруется только один раз с одним случайным ключом, но случайный ключ шифруется с использованием публичного ключа, каждого получателя.

*2696 Когда получатель пытается открыть, шифрованное сообщение, почтовое приложение пользователя делает попытку де шифрования случайного ключа, используя личный ключ получателя. Если это удается, случайный ключ дешифрует сообщение.

*2697 Если расшифровка успешна, получатель может читать сообщение. Если расшифровка неудачна, пользователь получает сообщение, указывающее, что расшифровка потерпела неудачу, и почтовая служба не позволяет пользователю доступ к сообщению.

6.2.2.2 Как работает шифрование исходящей почты S/MIME?

*2698 Отправитель посылает сообщение и выбирает опцию шифрования сообщения. Точный набор команд зависит от почтового приложения пользователя.

*2699 Почтовое приложение отправителя Notes или другая почтовая программа S/MIME, производит случайный ключ шифрования и шифрует им сообщение.

*2700 Почтовое приложение отправителя шифрует случайный ключ шифрования с использованием публичного ключа получателя, и добавляет в конец сообщения, зашифрованный ключ шифрования. Для почты S/MIME, посланной из клиента Notes, сертификат X.509 получателя, должен быть сохранен в персональной адресной книге отправителя, или Domino Directory. Если он найден, Notes использует публичный ключ получателя, найденный в сертификате, чтобы шифровать сообщения. Если никакой сертификат для получателя не найден, отправитель получает предупреждение, что шифрование не возможно, для этого получателя. Отправителю тогда предоставляется выбор, не посылать сообщения, или посылать его незашифрованное.

*2701 Если зашифрованное сообщение адресовано нескольким получателям, сообщение шифруется только однажды, одним случайным ключом, но случайный ключ шифруется, используя публичный ключ каждого получателя.

*2702 Когда получатель пытается открыть, зашифрованное сообщение, почтовое приложение пользователя делает попытку дешифровать случайный ключ, используя личный ключ получателя. Если это удается, случайный ключ дешифрует сообщение, показывая его пользователю.

*2703 Если дешифрование не удалось, получатель не получает доступ к сообщению. Пользователь получает сообщение, указывающее, что дешифрование потерпело неудачу, и почтовое приложение не позволяет пользователю доступ сообщению.

6.2.3 Шифрование почтовых сообщений.

Шифруйте исходящую, поступающую и сохраненную почту, чтобы защитить свои сообщения, во время доставки сообщений, и сохраненных в почтовых базах данных на сервере. Вы можете шифровать исходящие почтовые сообщения, посланные пользователям Notes, или с S/MIME пользователям. Вы можете шифровать приходящую и сохраненную и сохраненную в почтовой базе данных почту только, если Вы используете почтового клиента Notes.

Шифрование исходящей почты.

Шифрование исходящей почты гарантирует отправителю, что только получатель сообщения сможет прочитать эту почту.

Пользователи могут выбирать, будут ли они использовать тип шифрования Domino или S/MIME, для шифрования исходящих почтовых сообщений. Notes использует шифрование S/MIME для исходящей почты в следующих ситуациях:

*2704 Пользователь выбирает значение - Прямо через интернет, в поле Отправка исходящей почты:, на закладке текущего документа Место вызова. Почта, посланная с использованием этого документа - Место вызова, будут использовать формат MIME.

*2705 Пользователь выбирает формат MIME, в поле Формат сообщений, отправляемых на адреса интернета, на закладке – Почта, текущего местоположения. Почтовые сообщения, посланные из этого местоположения для адресатов интернета, которые не могут быть найдены в локальной адресной книге или Domino Directory, будут использовать формат MIME.

*2706 Пользователь выбирает - Prefers MIME, в поле Format preferences for incoming mail, на закладке Mail, Person документа. Почта, посланная этому пользователю, будет использовать формат - MIME.

*2707 Пользователь создает сообщение, используя форму, в свойствах полей которой включена опция - Store contents as HTML and MIME. Если получатель может принимать сообщения Notes или формат MIME, или если Notes не может найти Person документ для получателя, сообщение будет использовать формат MIME.

Каждый получатель шифрованной почты S/MIME, должны иметь публичный ключ интернета, доступный отправителю. Этот ключ может быть сохранен или в Domino Directory, который является доступным отправителю, или в персональной адресной книге отправителя. Если получатель Notes не имеет публичного ключа интернета, доступного отправителю, Notes пытается использовать публичный ключ Notes получателя, если он доступен, чтобы зашифровать сообщение.

Шифрование входящей почты в почтовом файле.

Если пользователи имеют доступ редактора к своим Person документам, в Domino Directory, они могут установить опцию шифрования сами, для почты, которую они получают. Иначе, Вы должны закончить эту процедуру для них.

*2708 Открыть Person документ для пользователя в Domino Directory.

*2709 Выбирайте закладку Mail и установите значение Yes, в поле Incrypt incoming mail:.

*2710 Сохраните документ.

Шифрование сохраненной почты в почтовом файле пользователя.

Пользователи могут шифровать черновики не отосланных сообщений и сообщения, которые они сохраняют после отправки их адресату. Для не отосланной почты, сообщение шифруются только публичным ключом отправителя. Для отосланной почты, сообщение шифруется с применением ключа отправителя и публичного ключа получателя.

Только сообщения, сохраненные после установки этой опции, будут шифроваться. Чтобы зашифровать старые сообщения, пользователи должны открыть их и повторно сохранить сообщения. Шифровка почты сохраненной в почтовом ящике, предотвращает неправомочный доступ к сообщениям администраторов или пользователей с неправомочным доступом к почтовым файлам на сервере.

6.2.4 Шифрование данных при передаче по порту сервера.

Вы можете шифровать данные в сети, при использовании определенных портов, чтобы предотвратить прослушивание данных по сети, с возможным анализатором протоколов сети. Шифрование сети происходит в слое передачи сети выбранного протокола и независимо от других форм шифрования. Данные сети шифруются только, во время, когда они находится на пути следования. Как только данные получены и сохранены, шифрование в сети больше не действует.

Шифрование данных сети происходит, если Вы позволяете шифрование данных сети с обеих сторон сети. Например, если Вы разрешаете шифрование по порту TCP/IP на сервера, Вы не должны позволить шифрование на портах TCP/IP, на рабочих станциях или серверах, которые соединяются с сервером.

Шифрование связей сервера могут замедлить выполнение работ сервером. Шифрование данных в сети имеет небольшое влияния на работу клиента. Кроме того, шифрованные данные сети не могут быть сжаты. Поэтому, если Вы шифруете данные сетевого порта, который использует сжатие данных, типа модема, Вы не получаете выгоды производительности от модема.

Шифрование данных сетевого порта сервера.

*2711 Из клиента Domino Administrator, выбирайте сервер, для которого Вы хотите шифровать данные в сети.

*2712 Выбирайте закладку Сервер, из панели инструментов - Сервис – Сервер – Настройка портов.

*2713 В окне настройки портов, выбирайте опцию - Шифровать данные передающиеся по сети и затем – ОК.

6.2.5 Электронная подпись.

Шифрование и электронная подпись связаны между собой. Электронная подпись подтверждает, что человек, который создал сообщение, является автором этого сообщения, и что никто не вмешивался в данные. Эта опция добавляет электронную подпись в отправляемое сообщение и поля или секции документов. Дизайнер базы данных определяет, являются или нет поля и секции базы данных подписываемыми, а пользователи могут выбирать, подписывать сообщения или нет.

Пользователи могут подписывать почтовые сообщения, посланные другим пользователям Notes или пользователям других почтовых приложений, которые поддерживают протокол S/MIME - например, IE и Netscape. Domino использует публичные и личные ключи Notes или интернет, для электронных подписей. Те же самые ключи, используются для шифрования.

6.2.5.1 Как работает электронная подпись?

Электронная подпись Notes.

Когда Вы подписываете сообщение, с использованием подписи Notes, все поля сообщения подписываются.

*2714 Notes, на основании данных генерирует некоторое число, которое представляет данные и затем зашифрует его личным ключом автора данных, формируя электронную подпись.

*2715 Notes прилагает подпись и публичный ключ подписывающего лица, и сертификат подписывающего лица к данным.

*2716 Когда кто-то получает доступ к подписанным данным, Notes проверяют, что подписавшее лицо, имеет общий сертификат или общего предка сертификата с читателем данных, при этом он доверяет его сертификату. Если так, Notes делает попытку де шифрования подписи, используя публичный ключ, который соответствует частному ключу лица, которое подписало данные.

*2717 Если дешифрование успешно, Notes указывает, кто подписал сообщение. Если дешифрование не успешно, Notes указывает, что он не мог проверять подпись. Неудачный дешифрование может указывать, что в данные вмешались, или что отправитель не имеет сертификата, которому доверяет читатель. Это могло бы случаться, например, когда

пользователь получает почту от пользователя в другой компании, и этот пользователь не имеет взаимного сертификата.

Электронная подпись S/MIME.

Когда Вы подписываете сообщение подписью S/MIME, только тело сообщения и приложения к нему подписываются.

*2718 Notes генерирует некоторое число, с использованием подписываемых данных, и затем зашифрует его с использованием частного ключа автора данных, формируя подпись.

*2719 Notes прилагает цепь подписей, то есть все сертификаты для подписи и подписи данных.

*2720 Когда кто-то получает доступ к подписанным данным, Notes или почтовое приложение, делают попытку расшифровки подписи, используя публичный ключ. Если действия успешны, Notes или почтовое приложение подтверждает, что подписывающее лицо имеет общее сертификаты или общего предка сертификатора, которому читатель доверяет.

Обратите внимание. Типично, пользователь Notes сертификатор организации выпускает взаимные сертификаты CA. Доверие может также быть установлено, если пользователь Notes выпускает взаимный сертификат непосредственно сертификатору подписывающего лица.

*2721 Notes или почтовое приложение сравнивает дешифрованное число, полученное с использованием данных, с числом которое вычисляется после передачи сообщения.

*2722 Если сравнение происходит удачно, это означает, что подпись имеет силу и данные небыли изменены, Notes или S/MIME отправляет предупреждение, указывает, кто подписал сообщение.

*2723 Если дешифрование неуспешно, Вы получаете сообщение, указывающее, что проверить подпись невозможно. Неудачное дешифрование может указывать, что в данные вмешались, или что отправитель не имеет сертификата, которому доверяет читатель. Это могло бы случится, когда пользователь получает почту от пользователя в другой компании, и этот пользователь не имеет взаимного сертификата.

Подписанная отправляемая почта.

Пользователи могут управлять опцией, будет ли почта, которую они посылают подписана. Пользователи могут подписывать отдельные почтовые сообщения, или подписывать все почтовые сообщения, которые они посылают.

При посылке подписанных сообщений пользователям, использующим почтовые приложения S/MIME, пользователи Notes должны иметь дополнительный набор публичных и личных ключей интернета, и должны редактировать их Person документы, чтобы позволить S/MIME для подписи сообщений.

6.3 Установка серверов Firewalls.

Эта глава описывает Firewall, чтобы предотвратить нападения на Вашу систему пользователями из интернета.

6.3.1 Firewalls.

Безопасность важнейшая из проблем, чтобы рассмотреть ее, когда Вы устанавливаете Domino для интернет. Например, когда пользователи отправляет почту в интернет или имеют доступ на Web сервера, внешние пользователи так же могут иметь доступ к Вашему серверу. Ваше планирование должно включить стратегию для защиты Domino системы от прямых и косвенных нападений из интернета.

Firewall - система, которая разработана и предназначена для управления доступом к сетевым приложениям. Типично, Firewall управляет доступом к частным сетям из интернета. Firewall особенно важен, когда Вы хотите позволить некоторой информации проходить между частной сетью и интернетом, но Вы не хотите дать неправомочным пользователям полный доступ частной сети.

Вы можете использовать Firewalls, чтобы обезопасить себя от двух типов нападений на Вашу систему - прямое нападения или косвенные нападения. Прямые нападения пробуют уязвимость транспортного набора протоколов и программ. Чтобы принимать меры против прямых нападений, установите твердую конфигурацию Router / Firewall и бдительно управляйте системой. Прямые нападения типично нацелены на хосты UNIX. Чтобы сорвать такие нападения, используйте программы типа SATAN (System Administrator Tool for Analyzing Networks), чтобы проверить систему, безопасности и выявить уязвимость системы.

Косвенные нападения типа распространения вирусов, используют более высокий уровень. Вирусы часто копируются, и этим причиняется немало проблем - например, заполняя жесткий диск, или останавливают сервер - или уничтожают данные. Косвенные нападения очень трудны в обнаружении. Чтобы принимать меры против них, обучите пользователей, и бдительно управляйте системой, налагая строгие ограничения на тип данных, которые могут проходить через барьерный сервер во внутреннюю сеть.

Вы можете установить Firewalls трех типов. Основанных на фильтровании пакетов, управлении доступом на уровне сетей, на уровне приложений и уровне Proxy, которые управляют доступом на прикладном уровне.

Вообще, Proxy система может понимать данные, связываться от имени пользователя и возвращает информацию назад пользователю. Proxy может обеспечивать Вас детальной информацией относительно действий клиента, затребованной информацией и информации, которая была передана. Эта информация может также и кэшироваться, так что пользователь может получать ответ очень быстро.

Если Вы уже имеете Firewall сервер в Вашей организации, Вы можете сконфигурировать Notes и Domino, чтобы работать через Firewall сервер. Если Вы не имеете Firewall сервер, обратитесь Вашему администратору сети, чтобы выяснить, необходимость применения этого устройства.

После того, как Вы установите Firewall сервер, Вы настраиваете рабочие станции Notes и Domino сервера, чтобы соединиться с использованием этих серверов. После того, как Вы настраиваете рабочие станции или сервера для связи через Firewall сервер, использование сервера Firewall прозрачно для пользователя.

Хотя мы не требуем, чтобы Вы использовали и Proxy или фильтр пакетов, чтобы управлять доступом в уровнях сетей и приложений. Например, Вы можете сконфигурировать Router, чтобы позволять движение в Domino сети только через Firewall, а затем сконфигурировать Domino Passthru сервер позволять пропускать только пользователей Вашей организации.

Используя и Proxy и фильтр пакетов, Вы обеспечиваете отдельные пункты контроля управления доступом и для сети и безопасности приложений.

Типы серверов Firewalls:

Фильтры пакетов. Firewall работающий на фильтровании пакетов исследует предназначение и содержание каждого пакета, который является частью информации, переданной по сети. Он проверяет, позволяется ли в сеть передача пакетов этому адресату, и позволяется ли этот тип информации передавать или принимать в Вашу сеть.

Proxy приложения. Proxy Firewall сервер - программа, которая понимает тип информации, которую Вы передаете, например, Notes и Domino удаленный запрос процедур (RPC) или информация HTTP формата. Вы можете управлять потоком информации между внутренними и внешними клиентами и серверами. Proxy сервера работают таким же самым образом, как и фильтрация пакетов, кроме доставки пакетов предназначению. Вы можете настроить Passthru Domino сервер как Proxy приложение, для Notes и Domino RPCS, или Вы можете использовать HTTP Proxy, чтобы использовать HTTP протоколы интернета, использующие опции SSL, для Notes и Domino RPCS.

Circuit-Level Proxy. Circuit-Level Proxy подобен Proxy приложению, за исключением того, что не требуется разделять тип информации, которую Вы передаете. Например, SOCKS сервер может действовать как Circuit-Level Proxy. Вы можете использовать Circuit-Level Proxy, чтобы использовать протоколы интернета с TCP/IP - то есть IMAP, LDAP, POP3, NTTP, SMTP, IIOP и HTTP. Вы не можете использовать Circuit-Level Proxy для Notes и Domino RPCS, или протоколов интернета, вместе с SSL.

6.3.2 Использование Domino сервера в качестве сервера Firewall.

Используйте Domino Passthru сервер как Proxy приложение для Notes и Domino RPCS. Passthru сервер обеспечивает все уровни безопасности для Notes и Domino. При определении для клиентов, использовать единственный Domino сервер для связи с внешним миром. Вы можете запретить использование других протоколов интернета, например HTTP, IMAP и LDAP.

Когда Вы настраиваете Proxy приложение, удостоверитесь, что следующие службы имен (DNS) - правильно сконфигурированы:

*2724 db.DOMAIN и db.ADDR, которые являются базами данных DNS, используют правильно определения имен, хостов IP к адресам. Базы DNS должны содержать правильные имена хостов и их адреса.

*2725 Файлы HOSTS должны содержать полные интернет имена серверов с доменов.

*2726 Если Вы используете службу NIS, Вы должны использовать полные имена доменов и хостов в доменах. Удостоверьтесь, что служба NIS может сосуществовать с DNS.

Чтобы установить Passthru Domino сервер как Proxy приложение, Вы должны сначала соединить сервер с интернетом и затем настаивать рабочие станции Notes и Domino сервера, чтобы использовать Passthru сервер как Proxy при вызове услуг вне Вашей сети. Чтобы использовать рабочую станцию или сервер, для использования Passthru сервера, Вы должны определить Passthru сервер в документе Место вызова для рабочего места и в Server документе для сервера.

Рисунок ниже показывает, как добавляется Domino Passthru сервер к Firewall с фильтрованием пакетов. В этом примере Passthru сервер добавит выгоду от Proxy для

нескольких Notes и Domino клиентов. Определяя единственный пункт входа для Notes и Domino движения на фильтр пакетов, Вы можете централизовать администрирование Proxy приложения.

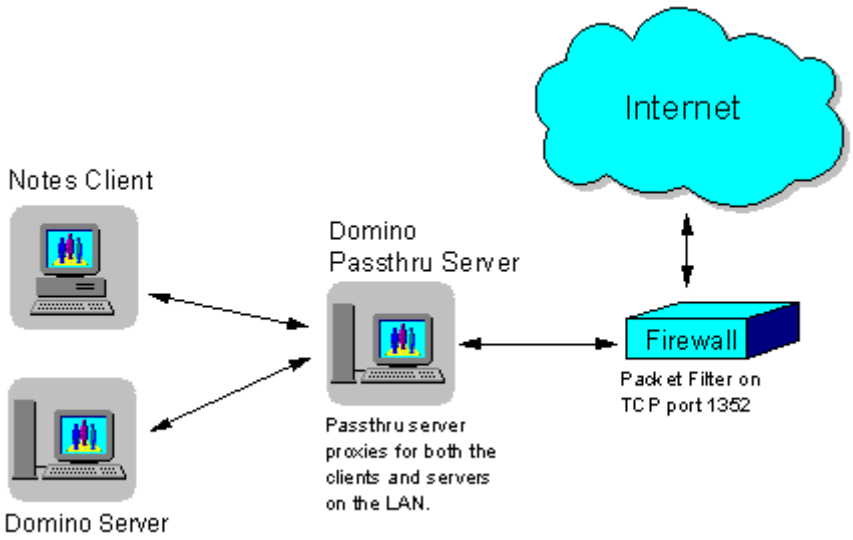


Рис. 104 Пример использования Domino сервера в качестве Firewall.

6.3.2.1 Использование двух сетевых адаптеров для Domino Passthru сервера.

Вы можете сконфигурировать Domino Passthru сервер, чтобы предотвращать неправомочное движение с сети LAN. Чтобы сделать это, Вы устанавливаете два сетевых адаптера сети на Domino сервере, один связанный будет связан с интернетом, и сконфигурирован для TCP/IP, а другого связан с сетью организации, и сконфигурирован для другого сетевого протокола, типа NetBIOS или SPX. Позволяя связь между сервером и интернетом по TCP/IP и связь для организации, по другому протоколу, Вы гарантируете Вашей системе безопасность от нападений.

Если необходимо, Вы можете использовать TCP/IP с двух сторон на сервере, однако Вы должны выключить TCP/IP маршрутизацию между адаптерами. Запретите любые дополнительные задачи TCP, типа FTP, SendMail, NFS и так далее.

Domino Passthru сервер может обеспечивать Вам доступ в реальном режиме времени к серверам назначения интернет, если администратор разрешает эту функцию.

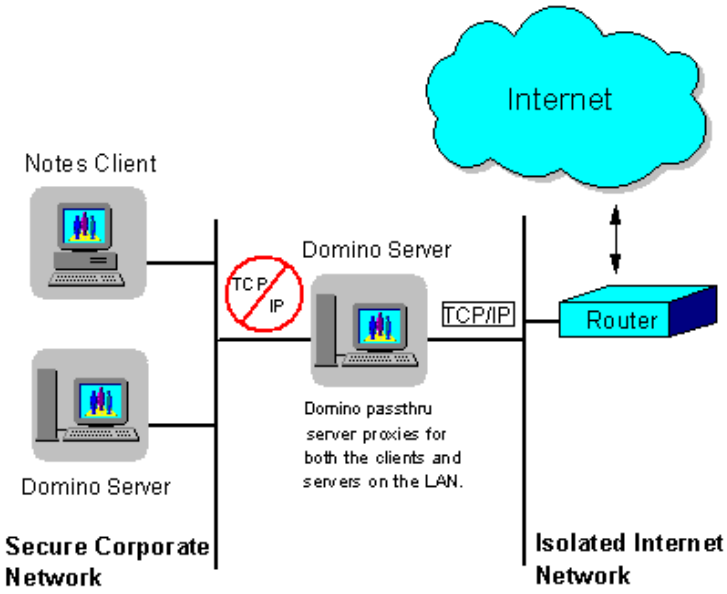


Рис. 105 Пример использования для Domino сервера двух сетевых карт.

Чтобы усилить систему защиты, поместите Router между Domino Passthru сервером и общей сетью LAN и позволите движение по сети только на Passthru сервер. Если Вы используете двойные сетевые адаптеры, конфигурируйте сеть, для использования Router и держите синхронизированными часы в системе.

6.3.3 Использование Proxy HTTP как Proxy приложение Firewall.

Вы можете использовать HTTP Proxy сервер, чтобы использовать HTTP протокол или SSL - например, IMAP, LDAP или NNTP. Вы можете также использовать HTTP Proxy сервер, чтобы использовать Notes и Domino RPCS.

Одно преимущество в использовании Proxy сервера состоит в том, что он является единственным источником для Web сессий Вашей компании. Это минимизирует потенциальные цели для нападающего. Web Proxy также позволяет кэширование часто посещаемых страниц. Это может улучшать выполнение работ.

Протокол сети имел обыкновение связываться между пользователем на частной сети и HTTP Proxy сервером - всегда HTTP. HTTP Proxy сервер может использовать родной протокол сети серверов - типа FTP, Gopher и WAIS - чтобы связаться с интернет серверами минуя Firewall. Так, если пользователь делает, запрос через HTTP Proxy для страницы на Gopher сервере интернет, HTTP Proxy сервер использует Gopher, чтобы получить страницу и затем использует HTTP, чтобы послать страницу пользователю.

SSL - протокол безопасности, который обеспечивает секретность коммуникаций по интернету. Вы можете сконфигурировать HTTP Proxy сервер, чтобы позволять SSL клиенту открывать безопасный туннельный переход через Proxy. Когда этот безопасный туннель создан, HTTP Proxy сервер не читает или интерпретирует данные, которые пропускают между пользователем и интернетом сервером, он просто пропускает информацию безопасным способом. SSL использует соединяющийся метод, чтобы расширить возможности HTTP Proxy и открыть безопасный туннельный канал. Вы можете использовать этот метод с SSL, чтобы использовать LDAP, IMAP, POP3, SMTP, IIOP и NTTP.

Если HTTP Proxy сервер поддерживает CONNECT метод, Вы можете настроить HTTP Proxy сервер, для Notes и Domino RPCS. Когда Вы настраиваете HTTP Proxy сервер, сконфигурируйте CONNECT метод для порта 1352, чтобы позволить Notes и Domino RPCS использовать Proxy.

Вы должны настроить рабочие станции Notes и Domino сервера для доступа на HTTP Proxy сервер. Чтобы настроить рабочую станцию, Вы вводите информацию о Proxy сервере в документ Место вызова для рабочей станции. Чтобы настроить сервер, для использования HTTP Proxy сервера, Вы определяете эту информацию Proxy в Server документе для сервера.

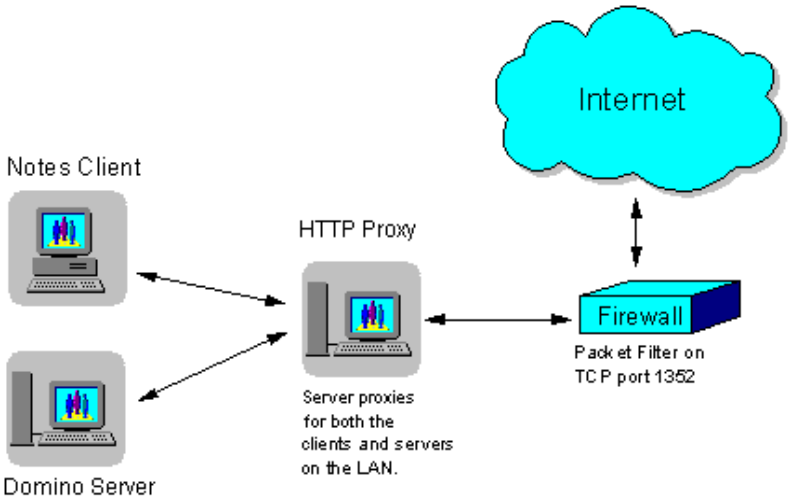


Рис. 106 Пример использования Domino сервера в качестве HTTP Proxy.

6.3.4 Использование SMTP Router и SMTP Listener как Proxy приложение Firewall.

Вы можете использовать SMTP Router и SMTP Listener как Proxy приложение Firewall. В этом случае, один сервер в Вашем домене, обозначена как Firewall машина и настроена как единственный контактный компьютер, с внешними клиентами и серверами. Этот Firewall сервер Вы конфигурируете как:

*2727 The SMTP server, using SMTP foreign domain and connection documents

*2728 The Relay Host for SMTP systems within the firewall

В пределах Вашей компании, имена интернета решают записи MX обозначение Firewall машины. Firewall сервер может тогда применять опции безопасности SMTP, чтобы управлять доступом клиентов и серверов.

6.3.5 Circuit-Level Proxy Firewalls.

Circuit-Level Proxy Firewalls, определены как SOCKS сервера, и они работают вне прикладных слоев протокола. Эти сервера позволяют клиентам проходить через центральную службу и соединяться с TCP/IP портом, который клиенты определяют. SOCKS сервера могут идентифицировать исходный адрес запросов и блокировать неправомочных клиентов от соединения с интернетом. Для увеличения уровня безопасности, добавьте к фильтрованию пакетов, Firewall с определенными портам SOCKS. Для большего количества информации по SOCKS, смотрите Web страницу http://www.socks.nec.com/

Domino имеет встроенную поддержку для SOCKS версии 4.2. Большинство SOCKS версий серверов обратно совместимы. Используя встроенную поддержку SOCKS, Вы используете централизованные услуги SOCKS, которые могут существовать в общей сети. Вы можете конфигурировать рабочие станции Notes и Domino сервера, чтобы не использовать SOCKS сервер.

Рабочие места Notes и Domino сервера должны знать, как получить доступ на SOCKS сервер, чтобы использовать его. Чтобы настроить рабочую станцию или сервер, Вы должны определить информацию Proxy в документе Место вызова для рабочей станции или в Server документе для сервера.

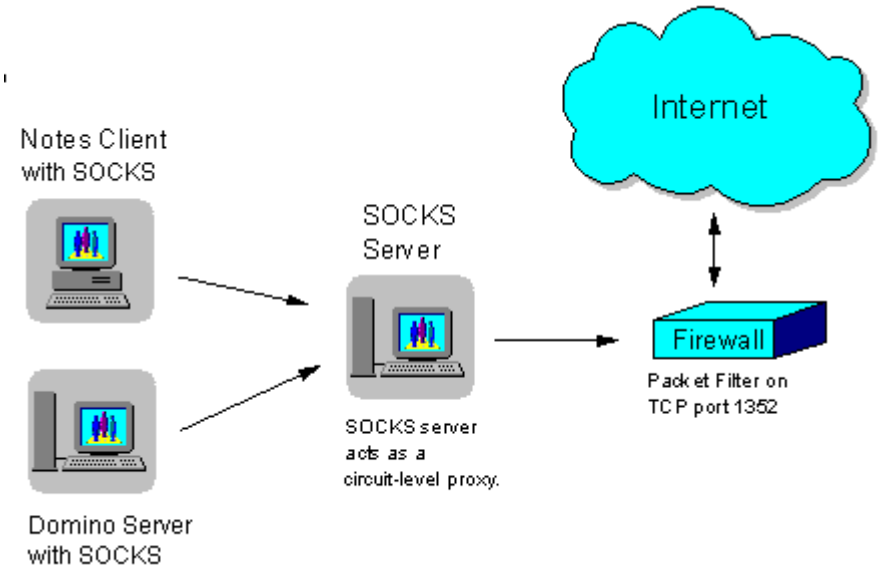


Рис. 107 Пример использования Domino сервера в качестве SOCKS сервера.

Следующий рисунок показывает рабочую станцию Notes и Domino сервер, с использованием встроенной поддержки SOCKS для доступа в интернет, через Domino Passthru сервер, через SOCKS сервер, и наконец через фильтрующий пакеты Firewall.

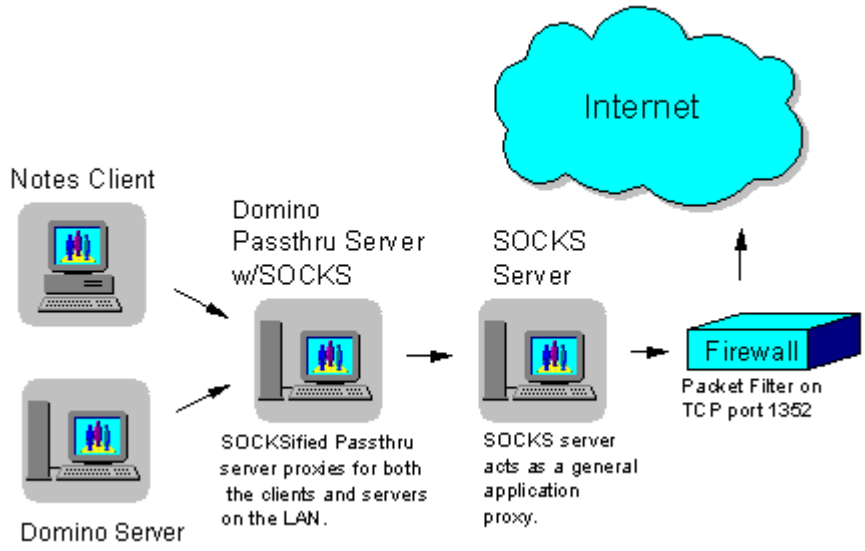


Рис. 108 Пример защиты рабочих станций Notes, Domino серверами и серверами Firewall.

6.3.5.1 Конфигурирование рабочей станции Notes и Domino сервера для соединения с интернет.

Позвольте SOCKS доступ на хост независимо от источника Socket. Чтобы сделать это, фильтр исходного адреса SOCKS сервера, должен позволять любой Socket.

Фильтр адреса назначения требует 1352 Socket.

Для Notes и Domino, не позволите передачу пакетов для любого хоста, определите только SOCKS сервер при использовании адреса назначения, который включает порт 1352.

db.DOMAIN и db.ADDR, баз данных DNS используйте привязку имен хостов к IP адресам. Записи должны содержать правильные имена хостов и адреса.

DNS файлы, должен содержать полное имя домена и SOCKS сервера.

Если Вы используете NIS, Вы должны использовать полное имя домена. Удостоверьтесь, что NIS может сосуществовать с DNS.

SOCKS версия 4.2 решает IP адреса в локальном масштабе. Удостоверитесь, что внутренний DNS установлен, чтобы решать адреса.

Конфигурирование соединения интернет с Domino серверами

Так как SOCKS не использует связей, исходящих из интернет, и тех, чей исходный адрес находится в локальной сети, Вы можете устанавливать связи, непосредственно с целевым сервером, или с Domino Passthru сервером.

Если Вы используете Domino Passthru сервер как Proxy приложение, позволяете только пакеты, которые имеют адрес назначения Domino Proxy сервер, с использованием 1352 порта.

Если Вы не используете Domino Proxy Passthru сервер, то позволяете назначения адресования, для любого хоста, по умолчанию, порт 1352.

(Необязательно) Позволяют только связи от доверенных хостов, для этого порта с использованием значения - 1352.

6.4 Установки Domino Certificate Authority.

Глава описывает, как установить Domino Certificate Authority (CA), чтобы выпустить сертификаты для сервера и клиентов.

6.4.1 Domino Certificate Authority.

Authority Certificate (CA) сертификат, позволяет серверам и клиентам использовать SSL или S/MIME для обмена почтой. CA - ручается за идентичность сервера и клиента, выпуская сертификаты интернета, в которые впечатана с цифровая подпись CA. Цифровая подпись гарантирует клиенту и серверу, что сертификату клиента или сервера можно доверять. Если клиент и сервер идентифицирует, то есть идентифицирует цифровую подпись в сертификате, они могут устанавливать безопасную сессию SSL или обмениваться безопасными сообщениями S/MIME. Если клиент и сервер не может идентифицировать друг друга, они не могут устанавливать безопасные сессии или обменивать безопасными сообщениями.

Вы можете использовать, коммерческий сертификатор, производителей третьих фирм, типа VeriSign. Вы можете также использовать шаблон базы данных Application Authority Certificate (CCA50.NTF) чтобы установить свой Domino CA. Использование Domino CA, избавит Вас от лишних расходов. Кроме того, многие из администраторов уже знакомы с Domino, поэтому не будет требоваться дополнительное обучения.

Таблица администраторских задач Domino CA.

Domino администратор CA ответственен за эти задачи:

Задача	**Цель**
Подписывать сертификаты для серверов и клиентов	Создаются, имеющие силу сертификаты, для сервера и клиента, которые включают цифровую подпись CA.
Создавать Person документы для клиентов в Domino Directory	Person документ хранит сертификат клиента, который используется для идентифицикации клиента. Поэтому, Person документ должен существовать для клиента прежде, чем запрос может быть одобрен.
Добавлять сертификаты клиентам, использующим сертификаты Third-Party CA в Domino Directory	В течение идентифицикации клиента и шифрования S/MIME, Domino проверяет Person документ на наличие публичного ключа клиента.
Ресертифицировать клиентам, просроченные сертификаты.	Это гарантирует, что сервера и клиенты могут продолжать использовать сертификат.

6.4.2 Настройка сервера Domino CA.

Domino CA сервер – это хост Domino Application Authority Certificate. Пользователи, сервера, администраторы и Domino CA используют приложение, чтобы управлять сертификатами клиентов и серверов. Большинство организаций нуждается только в единственном сервере Domino CA.

Чтобы установить сервер Domino CA, Вы должны выполнить эти задачи:

*2729 Настроить сервер как Domino Web сервер.

*2730 Создать базу данных Domino Application Authority Certificate, с использованием шаблона Domino CA - CCA50.NTF.

*2731 Создать Key Ring файл и CA сертификат.

*2732 Сконфигурировать CA профиль для Key Ring и установки почтовой системы.

*2733 Настроить SSL на сервере CA.

6.4.2.1 Создание приложения Domino Certificate Authority.

*2734 Удостоверьтесь, что Вы уже установили сервер как Domino Web сервер.

*2735 Используя клиента Domino Designer, создайте базу данных Domino Application Authority Certificate на сервере, с использованием шаблона Authority Certificate - CCA50.NTF. Чтобы найти файл шаблона, выбирайте опцию - Показать дополнительные шаблоны.

*2736 Редактируйте ACL базы данных Domino R5 Authority Certificate, следующим образом:

- Добавьте в ACL имена администраторов, которые будут выпускать, и управлять сертификатами интернета. Назначите им доступ редактора с правом удаления документов и роль [CAPrivlegedUser].

- Установите доступ по умолчанию – автор, с созданием документов.

Примечание, чтобы скрыть базу Domino Application Authority Certificate, из окна просмотра баз данных, когда пользователи выбирают меню Файл – База данных – Открыть, или когда Web клиенты, просматривает список базы данных, отмените опцию - Отображать в окне Открытие баз данных, в свойствах Базы данных.

6.4.2.2 Создание файла Key Ring и сертификата CA.

Вы используете сертификат CA, чтобы подписать сертификаты для сервера и клиентов и добавлять цифровую подпись CA к сертификатам клиента и сервера. Сертификат CA хранится в файле Key Ring, который является двоичным файлом, который защищен паролем.

Когда Вы используете клиента Domino Administrator, чтобы создать файл Key Ring, он по умолчанию сохраняется в каталоге данных клиента. Если Вы будете использовать других клиентов, чтобы одобрять и подписывать запросы клиентов, рассмотрите перемещение файла Key Ring на сетевой диск или дискету. Это гарантирует, что он будет доступен для других клиентов.

Удостоверитесь, однако, что Вы держите файл Key Ring в безопасном месте. Чтобы предотвратить неправомочный доступ. Только администраторы, которых Вы определяете, должны иметь доступ файлу Key Ring и его паролю.

Создание файла Key Ring и сертификата CA.

*2737 Удостоверьтесь, что Вы установили Domino Application Authority Certificate.

*2738 Из клиента Domino Adminstrator, выбирайте закладку Файлы, откройте базу данных Domino Application Authority Certificate.

*2739 Выбирайте опцию – Create Certificate Authority Key Ring & Certificate.

*2740 Заполните эти поля:

Поля	**Значения**
Key ring file name	Имя файла. По умолчанию - CAKEY.KYR сохраняется в каталоге данных клиента Domino Administrator.
Key ring password	Пароль - 12 символов рекомендуется.
Password verify	Повторный ввод пароля, для проверки.

Key Size	Размер пары публичного и личного ключа. Чем больше размер, тем более сильное шифрование. Если Вы используете международную версию Domino, только размер - 512 бит доступен.
Common name	Наглядное имя, которое идентифицирует сертификат CA Пример, Acme SSLCA.
Organization	Имя Организации владельца сертификата. Используйте имя компании.
Organizational Unit	(Выборочно) Имя отдела владельца сертификата.
City or Locality	(Выборочно) Город.
State or Province	Штат, край, область.
Country	Страна.

Обратите внимание, на общее имя организации, орг. единицы, город, государство или область и страну, при составлении CA сертификата. Выбирайте имя CA тщательно. Это - дорогостоящий процесс, чтобы переиздавать сертификаты, если Вы изменяете имя.

*2741 Нажмите на кнопку – Create Certificate Authority Key Ring.

*2742 После того, как Вы прочитаете, информация относительно файла Key Ring и имени CA, выбирайте – OK.

*2743 Сделайте резервную копию файла Key Ring и храните его в безопасном месте.

Примечание, чтобы управлять приложением Domino Application Authority Certificate с рабочей станции, создайте копию файла Key Ring, и распределите его по рабочим станциям. Рассмотрите вопрос размещения файла Key Ring на сетевом диске, на который могут получить доступ только администраторы. Вы должны определить местоположение файла Key Ring в Domino профиле Application Authority Certificate по умолчанию.

Изменение пароля для файла Key Ring.

Чтобы использовать длительное время сертификат из соображений безопасности файла Key Ring, периодически изменяйте для него пароль.

*2744 Из клиента Domino Adminstrator, выбирайте закладку Файлы и откройте базу данных Domino Application Authority Certificate.

*2745 Выбирайте представление - View Certificate Authority Key Ring, потом нажимайте – Change CA Key Ring Password

*2746 Введите старый пароль, и затем выбирайте – OK.

*2747 Введите новый пароль, по крайней мере, 12 символьный, и затем – OK.

6.4.2.3 Конфигурирование профиля приложения Domino Certificate Authority.

Профиль Application Authority Certificate опознает Key Ring файл CA и определяет имя CA сервера. Domino добавляет связь с сервером CA, когда Вы посылаете сообщение клиентам и администратору сервера, который запрашивает сертификат. Клиенты и администраторы серверов используют эту информацию, чтобы определить, где приобрести сертификаты.

*2748 Удостоверьтесь, что Вы создали файл Key Ring и сертификат CA.

*2749 Из клиента Domino Adminstrator, выбирайте закладку Файлы и откройте базу данных Domino Application Authority Certificate.

*2750 Выбирайте – Configure Certificate Authority Profile.

*2751 Если необходимо, введите полный путь к CA файлу Key Ring и введите имя файла в поле File CA key ring. По умолчанию, Notes ищет файл Key Ring на локальном диске. Вы можете также определить его на сетевой диск, для доступа других администраторов.

*2752 Введите в поле TCP/IP DNS name server полное имя сервера, на который запущено приложение CA. Domino использует это имя, чтобы указать, где приобрести подписанные сертификаты, в сообщениях посланных администраторам и клиентам.

Следующие четыре поля устанавливают значения по умолчанию для экрана сертификата клиента. Вы можете изменять их.

Поле	**Значение**
Use SSL for certificate transactions?	*2753 Yes - (по умолчанию) использовать SSL *2754 No - не использовать SSL.
Certificate Server port number	TCP/IP порт номер. Domino использует этот порт при посылке уведомления электронной почты клиентам, чтобы приобрести сертификат. По умолчанию - 80.
Mail confirmation of signed certificate to requestor?	*2755 Yes - генерировать подтверждающее письмо для подписанного сертификата; *2756 No (по умолчанию) - не посылать подтверждение.
Submit signed certificates to AdminP for addition to the Directory?	*2757 Yes (по умолчанию) – подтверждать запрос подписанного сертификата процессом администрирования, который будет сохранять этот сертификат в Domino Directory. *2758 No - не подтверждать.
Default validity period	Число лет, которое, подписанный сертификат имеет силу. По умолчанию - 2 года.

*2759 Сохраните и закройте документ.

6.4.2.4 Настройка SSL для сервера CA.

Так как администраторы серверов и клиенты используют браузер для доступа на сервер CA, чтобы запрашивать и приобретать сертификаты, используют SSL, чтобы защитить сервер CA. Когда Вы устанавливаете CA сервер для использования SSL, Вы создаете файл сервера Key Ring и запрашиваете сертификат сервера. Domino автоматически одобряет сертификат сервера и сливает сертификат CA, как Trusted Root.

*2760 Удостоверьтесь, что Вы сконфигурировали профиль для Domino Application Authority Certificate.

*2761 Из клиента Domino Adminstrator, выбирайте закладку Файлы и откройте базу данных Domino Application Authority Certificate.

*2762 Выбирайте опцию – Create Server Key Ring & Certificate.

*2763 Заполните эти поля:

Поле	**Значение**
Key ring file name	Имя для файла. По умолчанию - CAKEY.KYR сохраняется в каталоге данных Domino Administrator.
Key ring password	Пароль - 12 символов рекомендуется.
Password verify	Повторный ввод пароля, для проверки.
Key Size	Размер публичного и личного ключа. Чем больший размер, тем более сильное шифрование. Если Вы используете международную версию Domino, только размер - 512 бит доступен.
Common name	Полное имя TCP/IP хоста, включая имя домена – например, www.lotus.com
Organization	Имя организации владельца сертификата. Используйте имя компании.
Organizational Unit	(Optional) Имя отдела владельца сертификата.
City or Locality	(Optional) Город.
State or Province	Штат, край, область.
Country	Страна.

*2764 Выбирайте – Create Server Key Ring.

*2765 Введите пароль для файла сервера Key Ring и затем – OK.

*2766 Копирует файл сервера Key Ring (keyfile.key и keyfile.sth) в Domino каталог данных на сервере. Domino Application Authority Certificate создает файл на локальном диске, однако, сервер нуждается в файле сервера Key Ring, чтобы использовать SSL.

*2767 Сконфигурируйте SSL порт. Позволите установление подлинности сервера только на сервере.

*2768 Если клиенты используют, Netscape, делает следующее:

- Из клиента Domino Adminstrator, выбирайте закладку Файлы, откройте базу данных Domino Application Authority Certificate, откройте – Свойства базы данных.
- На закладке Basics, выберите Web: Требовать наличия SSL-подключения, чтобы вынудить браузер использовать SSL, для соединения с этой базой данных.

Обратите внимание, если вы используете клиента IE Microsoft, не делайте этого шага, который вынуждает пользователей использовать SSL для доступа к приложению. Клиенты, которые используют IE, должны использовать TCP/IP, для доступу к Domino Application Authority Certificate и сливать сертификат как Trusted Root. IE не позволяет клиентам принимать сертификат для сервера, для которого они не имеют сертификата Trusted Root.

6.4.3 Просмотр файла Key Ring

*2769 Из клиента Domino Adminstrator, выбирайте закладку Файлы, откройте Domino Application Authority Certificate.

*2770 Выбирайте представление View Key Ring Authority Certificate.

*2771 Выбирайте Display CA Key Ring.

*2772 Введите пароль.

*2773 Двойной щелчок на документе ключа CA, открывает документ, который Вы хотите открыть и просмотреть.

*2774 Для выхода из документа, выбирайте кнопку Close.

6.4.4 Экспорт файла CA Key Ring

Экспортируйте CA Key Ring в текстовый файл при проблемах с сервером CA и сравните файл Key Ring.

*2775 Из клиента Domino Adminstrator, выбирайте закладку Файлы, откройте Domino Application Authority Certificate.

*2776 Выбирайте представление View Key Ring Authority Certificate.

*2777 Нажимайте – Dump CA Key Ring to Text.

*2778 Введите пароль.

*2779 Введите имя файла, в который Вы хотите экспортировать Key Ring файл. Notes создает этот текстовый файл и сохранит его в каталоге данных.

*2780 Чтобы просмотреть текстовый фай, откройте его редактором текста.

6.5 Определение доступа на Domino сервер с использованием имени и пароля, анонимный доступ.

Глава описывает, как настроить сервер для доступа клиентов с использованием имени и пароля клиента. Описывается так же предоставление анонимного доступа для клиентов интернет / интранет.

6.5.1 Идентификация для пользователей интернет / интранет, с использованием имени и пароля

Идентификация с использованием имени и пароля, также известной как базовая система идентификации, использует базовый протокол - вызов / ответ, чтобы вынудить пользователей ввести их имя и пароль. После чего, сервер проверяет пароль из Person документа в Domino Directory. Domino сервер запросит имя и пароль только, когда интернет / интранет клиент пробует получить доступ к базе данных на сервере. Доступ для интернет / интранет отличается от доступа клиентов Notes и Domino серверов только этим. Domino сервер просит всегда клиента Notes или Domino сервер ввести имя и пароль, когда клиент или сервер делает попытку доступа на сервер.

Если Вы хотите назначить соответствующий доступ к базам данных для интернет / интранет клиента, основанного на безопасности ACL Domino, Вы должны создать Person документ для этого клиента в Domino Directory. Клиенты, которые не имеют Person документов, рассматриваются, как Anonymous и могут получить доступ на сервер с этими правами.

Идентификация с использованием проверки имени и пароля, позволяет Domino иметь Person документ для клиента, обращающегося к серверу. Domino использует Person документ, чтобы идентифицировать клиента. После того, как клиент идентифицирован, доступ к базам данных может быть определен.

Пример. Если Вы хотите, чтобы Алан Джонес имел доступ редактора к базе данных, но по умолчанию предоставлять доступ автора, Вы должны создать Person документ для Алана Джонес. Вы должны настроить ACL базы данных, чтобы включить Алана Джонес с доступом редактора и включить пользователя Anonymous как автора.

Вы можете использовать имя и пароль для идентификации с использованием TCP/IP или SSL на любых серверах, которые работают по протоколам интернета, а именно NNTP, LDAP, POP3, HTTP, SMTP, IIOP или IMAP. Для каждого протокола интернета позволенного на сервере, Вы можете определить свой метод безопасности.

Пример. Вы можете позволить SSL для HTTP связей, но требовать ввода имени и пароля для NNTP связей с использованием TCP/IP. Вы могли бы использовать ввод имени и пароля с анонимным доступом и с SSL идентификацией клиента. Позвольте пользователям с сертификатами SSL, идентифицироваться с использованием SSL, позвольте другим пользователям вводить имя и пароль, если не имеется сертификата SSL.

Обратите внимание, что идентификация с использованием имени и пароля, не поддерживается, когда Domino сервер действует как SMTP клиент. Например, когда Domino сервер соединяется с SMTP сервером для передачи почты. Безопасность, с использованием имени и пароля, поддерживается только, когда Domino сервер действует, как SMTP сервер - то есть когда осуществляется SMTP доступ клиентов на Domino сервер.

Идентификация с использованием имени и пароля по TCP/IP.

Используйте идентификацию с использованием имени и пароля по TCP/IP, чтобы идентифицировать пользователей, если не требуется доступа к конфиденциальным данным на сервере. Например, Вы можете показывать различную информацию пользователям, запрашивая их имена и пароли, для предоставления информации в базах данных, которая не является конфиденциальной. Никакая информация, включая имя и пароль, посланный между пользователем и сервером, не шифруется. Идентификация по TCP/IP, с использованием имени и пароля, не защищена от прослушивания.

Идентификация с использованием SSL, имени и пароля.

Если Вы используете SSL вся информация, включая имя и пароль, будет использовать шифрование. SSL обеспечивает целостность данных для пользователей и серверов при использовании имени и пароля. Требование имени и пароля в дополнение к безопасности SSL, обеспечивает наиболее сильную безопасность для пользователей, которые используют эту особенность.

6.5.1.1 Идентификация Web клиентов, с использованием имени и пароля, основанное на сессиях клиентов

Чтобы разрешить опцию безопасности идентифицикации для Web клиентов, Вы может использовать один из двух методов. Первый это базовая идентификация, с использованием имени и пароля. Второй способ основан на сессиях пользователей, с использованием имени и пароля.

Особенности идентификации пользователей, с использованием имени и пароля, базирующихся на сессиях клиентов.

Сессия, это время, в течение которого Web клиент активно зарегистрирован на сервере. Сессий основанная безопасность, с использованием имени и пароля, включают в себя дополнительные возможности, которые не доступны в базовой системе безопасности. Вы используете Server документ из Domino Directory, чтобы определить идентификацию основанную на сессиях клиентов.

Настройка форм HTML для регистрации пользователей.

HTML форма для регистрации пользователей, позволяет пользователям вводить имена и пароли и затем использовать имя и пароль для всей сессии пользователя. Браузер посылает имя и пароль на сервер, используя набор знаков сервера, поэтому пользователи могут вводить имя и пароль, используя знаки второй половины ASCII или Latin-1.

Domino использует по умолчанию HTML форму, которая создана и сконфигурирована в базе данных Configuration (DOMCFG.NSF). Вы можете настраивать форму, чтобы добавить дополнительную информацию.

Период времени для окончания регистрации, установленное по умолчанию.

Вы можете определить период времени для разрегистрации Web клиента на сервере, после указанного периода бездеятельности. Пользователи могут также добавить в конец команды значение - ?Logout, в конец URL, чтобы выйти из сессий. Например:

```
http:\\acmeserver\sessions.nsf\?Logout.
```

Определение максимального числа сессий клиентов.

Вы можете определить максимальное число сессий пользователей, позволенных на сервере в одно и то же время. Если сервер работает медленно, Вы можете уменьшать число активных сессий пользователей.

Чтобы использовать сессия основанную идентификацию, Web клиенты должны использовать браузер, который поддерживает Cookies. Domino использует Cookies для отслеживания сессий пользователей.

6.5.1.1.1 Настройка сессий основанной идентификации с использованием имени и пароля.

Чтобы настроить сессий основанную идентификацию для Web клиентов, с использованием имени и пароля, Вы должны редактировать Server документ в Domino Directory. Вы должны также создать Person документ для каждого Web клиента, который будет использовать сессий основанную идентификацию с использованием имени и пароля.

Хотя Web клиенты требуют Person документов, они не нуждаются в лицензиях Notes, так как они не используют программное обеспечение рабочего места Notes для доступа к серверу.

*2781 Из клиента Domino Administrator, выбирайте закладку Настройка, откройте Server документ.

*2782 Выбирайте закладку Internet Protocols – Domino Web Engine

*2783 Заполните эти поля, затем спасите документ:

Поле	**Значение**
Session authentication	*2784 Enable – разрешение сессий основанной функции идентификации клиентов, с использованием имени и пароля *2785 Disabled- по умолчанию, не разрешено.
Idle session timeout	Значение задержки для, разрегистрации Web клиента, если клиент ничего не делает По умолчанию - 30 минут.
Maximum active sessions	Максимальное число активных одновременных сессий клиентов По умолчанию - 1000.

Создание Person документов для Web пользователей.

*2786 В Domino Directory, создайте Person документ для каждого Web пользователя, который нуждается в доступе на сервер. Вы можете также редактировать Person документ существующего пользователя.

*2787 В каждом Person документе, заполните эти поля и затем сохраните документ:

Поле	**Значение**
First name, Middle initial, Last name	Имя инициалы фамилия

User name	Полное имя пользователя. Это имя, пользователь вводит при попытке доступа на сервер. Это поле может содержать несколько имена. Однако Domino использует первое имя этого поля, чтобы проверить пользователя в ACL баз данных и в списках доступа для проектов. Например, это поле может содержать эти имена: *2788 Alan Jones *2789 Al Jones *2790 AJ Когда сервер запросит имя и пароль, пользователь может ввести Al Jones. Однако Domino использует имя Alan Jones, чтобы определить его в ACL баз данных и списках доступа к проектам. Поэтому, имя Alan Jones должно быть то, которое появляется в ACL и списках доступа для проектов.
Internet password	Пароль

После того, как Вы установили сервер и создали Person документы, редактируете ACL баз данных для каждой базы данных на сервере, к которым Вы хотите дать доступ.

Настройка HTML форм для регистрации Web пользователей.

Domino снабжает Вас HTML Log-In формой по умолчанию, чтобы позволить пользователям вводить их имена и пароли и затем использовать имя и пароль для сессий пользователя. Эта форма создана и сконфигурирована в базе данных Configuration (DOMCFG.NSF). Вы можете настраивать форму, чтобы ввести дополнительную информацию. Чтобы сделать это, Ваш Domino Web сервер должен быть установлен.

Создайте Domino базу данных Configuration. Если Вы не создаете базу данных, Domino используйте свою форму Log-In.

Создание формы для регистрации.

Определите форму для регистрации пользователей. Если база данных Configuration существует на Web сервере, но Вы не создали, или не определили формы для регистрации, Domino использует форму $$LoginUserForm, как форму для регистрации пользователей.

Самый простой способ создавать традиционную Log-In форму, состоит в том, чтобы изменить копию формы $$LoginUserForm.

Пример. Log-In форма, поставляемая с Domino, в базе данных Configuration. Вы можете также создавать новую форму Log-In from scratch. Вы должны иметь клиента Domino Designer, чтобы редактировать или создать формы.

*2791 Запустите клиента Domino Designer и откройте базу данных Configuration (DOMCFG.NSF).

*2792 Чтобы создать Вашу форму, использующую имя $$LoginUserForm, сделайте копию $$LoginUserForm, затем двойным щелком открывайте ее. Вы можете переименовывать

копию, если необходимо, например в CustomLoginForm. Чтобы создать новую форму, выбирайте кнопку – Новая Форма.

*2793 Когда Вы заканчиваете проектирование формы, сохраните ее.

Определение формы для регистрации пользователей.

*2794 Из клиента Notes и открывает Domino базу данных Configuration (DOMCFG.NSF).

*2795 Выбирайте Создать – Mapping a Login Form.

*2796 Выбирайте тип сервера, соответствующий Вашему Web серверу.

*2797 (Необязательно) Введите комментарии.

*2798 Введите имя файла базы данных, которая содержит форму. Это должно быть имя Domcfg.nsf, если Вы не храните форму в различных базах данных.

*2799 Введите имя форма, например - LoginUserForm.

*2800 Сохраните и закрывайте документ.

6.5.1.2 Настройка базовой идентификации Web клиентов, с использованием имени и пароля.

Чтобы настроить базовую идентификацию для Web интернет / интранет клиентов, Вы создаете Person документ для каждого пользователя в Domino Directory, назначаете пароль интернета для каждого пользователя. В Server документе, Вы должны определить, протоколы интернета для ведения имени и пароля. Для разрешения доступа пользователей к базам данных, Вы должны включить их имена в ACL баз данных.

Редактирование Server документа для настройки базовой идентификации Web клиентов.

*2801 Из клиента Domino Administrator, выбирайте закладку Настройка и откройте Server документ.

*2802 Выбирайте закладку Ports – Internet Ports. Закладка имеет пять дополнительных закладок: Web, Directory, News, Mail и IIOP. Каждая закладка содержит список протоколов и соответствующие имени - например, закладка Web содержит список для HTTP/HTTPS, закладка News содержит список для NNTP, закладка Mail имеет настройки для IMAP, POP SMTP и так далее.

*2803 Выбирайте закладку, для которой Вы хотите определить идентификацию Web клиентов, с использованием имени и пароля. Для каждого из протоколов, делайте следующее:

- Если Вы хотите, чтобы клиенты использовали базовую идентификацию, когда они соединяются с использованием TCP/IP, выберите значение – Yes в поле Name & password, TCP/IP секции.
- Если Вы устанавливаете SSL на сервер, и Вы хотите, чтобы клиенты использовали базовую идентификацию, когда они соединяются с использованием SSL, выберите значение – Yes, в поле Name & password в секции SSL.

*2804 Сохраните документ.

Обратите внимание. Если Вы хотите разрешить доступ LDAP клиентов, использующих Netscape 4.5 для доступа на сервер, с использованием базовой идентификации, Вы должны также позволить анонимный доступ на сервер. Netscape 4.5 LDAP клиенты возвращают адрес электронной почты для идентификации и опознания клиентского адреса, анонимно прежде, чем Domino может подтверждать подлинность пользователя.

*2805 После того, как Вы настроили сервер и внесли изменения в Person документы, редактируете ACL для каждой базы данных на сервере, к которым Вы хотите дать доступ пользователям.

6.5.1.3 Контроль уровня доступа для Web клиентов.

Вы можете выбирать уровень доступа Domino при идентификации Web клиентов, для Domino каталогов и LDAP Directory.

*2806 Из клиента Domino Administrator, выбирайте закладку Настройка и откройте Server документ.

*2807 Выбирайте закладку Security.

*2808 Из секции Web Server Access, выберите одно из следующего значений:

More name variations with lower security - более низкий уровень безопасности. Domino пробует идентифицировать пользователей, основываясь на их имени и пароле. Этот метод, может быть уязвим, когда злоумышленник делают попытку для доступа на сервер, используя законный экаунт пользователя. Этот выбор установлен по умолчанию. Этот выбор позволяет пользователям вводить любое из следующих имен в окно диалога Web браузера:

Идентификация для Domino Directory	**Идентификация для LDAP Directory**
Last name	Surname
First name	Givenname
Common name	Common name (CN)
Full hierarchical name (канонический формат)	DN
Full hierarchical name (абривеатура)	DN
Short name	UID
Alias name (имя, внесенное в список поля User Name, Person документа, исключая первое значения списка)	
Soundex number	

Fewer name variations with higher security - более высокий уровень безопасности. Эта техника поиска менее уязвима при нападениях, потому что предпринимается единственная попытка, уменьшая вероятность подбора пароля. Этот выбор рекомендуется для более

сильной системы безопасности. Этот выбор требует, чтобы пользователи вводили только следующие имена в окно диалога из Web браузера:

Идентификация для Domino Directory	**Идентификация для LDAP Directory**
Full hierarchical name	DN
Common name или Common name, с CN=префиксом	CN
	UID or UID with UID= prefix
Alias name (имя, внесенное в список поля User Name, Person документа, исключая первое значения списка)	

*2809 Сохраните и закройте документ.

6.5.1.4 Примеры использования имен для идентификации Web клиентов, с использованием ограничений

More name variations with lower security. При использовании этого слабого уровня безопасности, пользователь Alan Jones/Sales/East/Acme может вводить в следующие имена при идентификации для Domino Directory, используя Web браузер:

Пример	**Описание**
Alan Jones	Общее имя
Alan	Имя
Jones	Фамилия
Ajones	Короткое имя
Alan Jones/Sales/East/Acme/US	Полное иерархическое имя (абривеатура)
cn=Alan Jones/ou=East/ou=Sales/o=Acme/c=us	Полное иерархическое имя (канонический формат)

Если Вы хотите идентифицировать Alan Jones/Sales/East/Acme/US в LDAP Directory, он может вводить следующие имена, используя Web браузер:

Пример	**Описание**
Alan Jones	Общее имя
Alan	Имя
Jones	Фамилия
Ajones	Короткое имя

cn=Alan Jones, cn=recipients, ou=Sales, ou=East, o=Acme, c=us (имеет силу для сервера Microsoft Exchange)	Полное иерархическое имя (канонический формат)
uid=ajones, ou=Sales, ou=East, o=Acme, c=us (имеет силу для сервера Netscape Directory)	Полное иерархическое имя (канонический формат)
Alan Jones/Sales/East/Acme/US	Полное иерархическое имя (абривеатура)

Fewer name variations with higher security. При использовании ограничений на уровень идентификации имен пользователей, пользователь Alan Jones/Sales/East/Acme может вводить только в следующие имена, при идентификации для Domino Directory, с использованием Web браузера:

Пример	**Описание**
Alan Jones/Sales/East/Acme	Полное иерархическое имя (абривеатура)
CN=Alan Jones	Общее имя с CN= префиксом
Alan Jones	Общее имя
cn=Alan Jones/ou=East/ou=Sales/o=Acme/c=us	Полное иерархическое имя (канонический формат)

Если Вы хотите идентифицировать пользователя Alan Jones/Sales/East/Acme в LDAP Directory, пользователь может вводить следующие имена, используя Web браузер:

Пример	**Описание**
Ajones	UID
Alan Jones	CN
cn=Alan Jones, cn=recipients, ou=Sales, ou=East, o=Acme, c=us (имеет силу для сервера Microsoft Exchange)	DN
uid=ajones, ou=Sales, ou=East, o=Acme, c=us (имеет силу для сервера Netscape Directory)	DN
uid=Ajones (имеет силу для сервера Netscape Directory)	UID с UID=префиксом

6.5.2 Идентификация Web клиентов, с использованием имени и пароля, во вторичных Domino Directory и LDAP Directory.

Когда Web клиент идентифицирует на сервере, по умолчанию сервер проверяет только первичный Domino Directory, чтобы определить, существует ли имя и пароль в Person документе. Если Ваша организация использует вторичные Domino Directory и или LDAP Directory, чтобы идентифицировать Web клиентов, Вы можете настроить Domino, чтобы он проверял дополнительный каталоги.

Когда Вы отмечаете правило домена, опцией – Trusted, Domino ищет имя и пароль сначала в первичном Domino Directory, если не находит проверяет вторичные Domino Directory и LDAP Directory. Вы настраиваете Directory Assistance, определяя порядок, в котором Domino будет просматривать вторичные каталоги.

Иерархическое имя, введенное пользователем, будет проверено правилами, базы данных Directory Assistance, для проверки соответствия имени организации и орг. единицы, указанным в этих правилах.

Например, если введено имя пользователя - Dave Lawson/Lotus, в базе данных Directory Assistance, должен быть документ правила для организации - */Lotus.

Поиск имен и паролей пользователей, для идентификации Web клиентов, с использованием вторичных каталогов, может использовать - SSL.

6.5.3 Обеспечение дополнительной безопасности для пароля интернета.

Когда Вы вводите пароль интернета и сохраняете Person документ, Domino автоматически шифрует поле пароля интернета. Чтобы улучшать безопасность пароля, используйте более безопасный формат для хранения пароля интернета. Используйте опцию более безопасного хранения пароля только, если доступ пользователей выполняется на сервера Domino 4.6 или позже.

Вы можете модернизировать формат пароля для Person документов, которые уже существуют или автоматически использовать более безопасный формат пароля для всех Person документов, которые Вы создаете.

Для существующих Person документов, проделайте следующее:

*2810 Из клиента Domino Administrator, выбирайте закладку Пользователи и группы. Выбирайте Person документы, в которых Вы хотите модернизировать формат пароля в более безопасный формат.

*2811 Выбирайте – Действия – Upgrade to More Secure Internet Password Format.

*2812 Нажмите – OK.

Для применения опций защиты к новым Person документам делайте следующее:

*2813 Из клиента Domino Administrator, выбирайте закладку Настройка, затем вымирайте представление Сервер – Все документы на сервере – Server документ.

*2814 Выбирайте – Действия – Edit Directory Profile

*2815 В поле Use more secure Internet passwords, выбирайте значение – Yes.

*2816 Сохраните и закройте документ профиля.

6.5.4 Анонимный доступ для пользователей интернет / интранет.

Когда Вы устанавливаете анонимный доступ, клиенты интернет / интранет могут получить доступ на сервера без идентификации. Domino не делает запись деятельности в базах данных для этих клиентов - например, в файле LOG.NSF и в окне диалога деятельности пользователя.

При использовании анонимного доступа, Вы никогда не знаете, кто обращается к базам данных на сервере. Поэтому, Вы не можете использовать идентификацию клиента - то есть имя клиента и пароль, чтобы управлять доступом к базам данных и модулям приложений. Используйте анонимный доступ только тогда, когда Вы не должны знать, кто обращается к базе данных, и или когда Вы не должны управлять доступом, основанным на идентичности клиента.

Вы можете использовать анонимный доступ с TCP/IP и или с SSL на любом сервере, где работают задачи NNTP, LDAP, HTTP, SMTP, IIOP. Для каждого протокола интернета позволенного на сервере, Вы можете определить метод безопасности.

Например, Вы можете позволять SSL для HTTP доступа, но требовать введений имен и паролей для NNTP доступа, то TCP/IP.

В дополнение к использованию анонимного доступа, Вы можете использовать и установление подлинности, с использованием имени и пароля по SSL. Тогда пользователи могут использовать любой из этих методов для соединений с сервером.

Например, если пользователь имеет сертификат SSL, пользователь может получить доступ на сервер с использованием SSL, кто не имеет сертификата SSL, получает доступ на сервер анонимно.

6.5.4.1 Настройка анонимного доступа для клиентов интернет / интранет.

Чтобы настроить анонимный доступ для клиентов интернет / интранет, Вы настраиваете сервер для анонимного доступа и затем настраиваете ACL баз данных, чтобы включить пользователя Anonymous.

Установки из Server документа перекрывают ACL для анонимных пользователей.

Например, если ACL базы данных содержит запись Anonymous, но установка в Server документе, не позволяет анонимный доступ на сервер, клиенты не получат анонимного доступа к базе данных. Если Вы не позволяете анонимный доступ, но клиенты пробуют доступ на сервер анонимно, клиенты получают отказ в доступе.

*2817 Из клиента Domino Administrator, выбирайте закладку Настройка, откройте Server документ.

*2818 Выбирайте закладку Ports – Internet Ports. Закладка содержит пять дополнительных закладок: Web, Directory, News, Mail IIOP. Каждая закладка содержит список протоколов, соответствующих названиям протоколов. Например, закладка Web содержит список HTTP/HTTPS, Закладка News - NNTP, закладка Mail – IMAP, POP, SMTP и так далее.

*2819 Выбирайте закладку и протокол, для которого Вы хотите позволить анонимный доступ, и для каждого протокола, делайте следующее:

- Если Вы хотите позволить клиентам анонимный доступ, когда они соединяют использование TCP/IP, выбирайте значение – Yes, в поле Anonymous, TCP/IP секции.

- Если Вы устанавливаете SSL на сервер, и Вы хотите позволить клиентам анонимный доступ, когда они соединяются с использованием SSL, выбирайте значение - Yes, в поле Anonymous, SSL секции.

*2820 Сохраните документ.

*2821 В ACL каждой базы данных на сервере, сделайте следующее:

- Создайте запись для имени Anonymous. Если Вы не добавляете эту запись в ACL, пользователи и сервера, кто получит доступ анонимно, получают доступ к данным по умолчанию.

- Назначите соответствующий уровень доступа - типично доступ читатель.

*2822 Перезапустите сервер, чтобы изменения вступили в силу.

6.5.5 Скрытие списка баз данных сервера для Web клиентов.

Вы можете определить, могут ли Web клиенты просматривать список баз данных сервера используя команду - ?Open. По умолчанию, пользователи не могут просматривать список баз данных, даже если они имеют доступ на сервер. Если Вы скрываете список баз данных от Web пользователей, они могут все еще открыть индивидуальные базы данных, для которых они имеют доступ.

Скрытие списка баз данных полезно, если Вы имеете виртуальные сервера на одном компьютере, или если некоторые базы данных не предназначены для использования Web. Виртуальные сервера используют один и тот же каталог данных Domino, и поэтому клиенты могут просматривать базы данных, предназначенные для другого виртуального сервера.

*2823 Из клиента Domino Administrator, выбирайте закладку Настройка, откройте Server документ.

*2824 Выбирайте закладку Internet Protocols – HTTP.

*2825 В поле Allow HTTP clients to browse databases, выбирайте значение – No

*2826 Сохраните документ.

6.5.6 Validation и Authentication, для интернет / интранет клиентов.

После того, как Вы устанавливаете доступ клиентам, с использованием проверки их имени и пароля, создаете Person документы, для пользователей интернет / интранет, Domino идентифицирует пользователей когда:

*2827 Они пытаются делать кое-что, для чего доступ ограничен.

*2828 Установление подлинности для сессии разрешено.

*2829 Анонимный доступ не позволяется на сервер.

Например, когда пользователь пробует открыть базу данных, которая имеет ACL без доступа назначенного по умолчанию. Domino проверяет пользователя по имени пользователя и паролю. Идентификация завершается правильно, если пользователь вводит имя и пароль, который соответствует имени и паролю, сохраненному в Person документе

пользователя. Если ACL базы данных позволяет доступ этому пользователю, пользователь получает доступ к базе.

Этот метод, Domino использует для идентификации LDAP клиентов и зависит от того, установлена ли переменная LDAP_STRICT_RFC_ADHERENCE в файле NOTES.INI.

Как работает Validation и Authentication?

Этот пример описывает, как клиент Andrew использует TCP/IP, для соединения с сервером Mail-E.

*2830 Andrew пробует получить доступ к базе данных на сервере Mail-E.

*2831 Сервер проверяет Server документ, чтобы определить, позволяется ли анонимный доступ для TCP/IP. Если это так, то:

- Сервер проверяет ACL базы данных на наличие записи Anonymous.
- Если ACL не содержит записи Anonymous, сервер проверяет доступ по умолчанию, в ACL базе данных.
- Если по умолчанию, доступ читатель или выше, Andrew получает доступ к базе данных

*2832 Если анонимный доступ запрещен для этого протокола, или если ACL базы данных не позволяет анонимный доступ, то сервер проверяет Server документ, чтобы определить, позволяется ли доступ для TCP/IP, с использованием имени и пароля. Если доступ с использованием имени и пароля позволяется, то:

- Сервер вынуждает пользователя Andrew ввести имя пользователя и пароль.
- Если Andrew использует Web клиента, сервер проверяет что введенное имя пользователя соответствует уровню требуемого для идентификации - More name variations with lower security или Fewer name variations with higher security.
- Сервер проверяет имя пользователя в поле User Name, в Person документе для пользователя и проверяет пароль в поле Internet Password, из Person документа.
- Сервер проверяет первичный Domino Directory для Person документа. Сервер также проверяет вторичные Domino Directory и LDAP Directory, если пользователь - Web клиент, и Domino сконфигурирован, для поиска имени во вторичных Domino Directory и LDAP Directory.
- Если пароль введен правильно, сервер проверяют ACL базы данных для введенного имени, которое внесено в список имен поля первым, в Person документе.
- Если первая запись поля, соответствует записи в ACL, Andrew получает доступ к базе данных, используя уровень доступа, указанный для этой записи в ACL.

6.6 Настройка SSL на сервере Domino.

Глава описывает, как настроить SSL на сервере Domino, чтобы разрешить безопасный доступ интернет и интранет доступ в Вашей организации.

6.6.1 SSL безопасность.

Secure Sockets Layer (SSL) - протокол безопасности, который обеспечивает безопасность соединений и установление подлинности для Domino серверов и задач, которые работают по TCP/IP.

SSL предлагает следующие опции безопасности:

*2833 Данные передаваемые от клиентов шифруются в течении всей сессии клиентов.

*2834 Кодируется просмотр сообщения, присоединенных данных, и обнаруживается любое вмешательство в сообщения.

*2835 Сертификат сервера сопровождающий данные утверждает, что сервер тот за кого он себя выдает.

*2836 Сертификат клиента сопровождающий данные утверждает, что клиент тот за кого он себя выдает. Установление подлинности для клиента необязательно.

интернет протоколы поддерживающиеся Domino и SSL.

Вы должны установить Domino сервер и затем настроить SSL. Вы можете использовать безопасность SSL для клиентов интернета, которые используют один из протоколов интернет, чтобы соединиться с Domino сервером:

*2837 Web сервер и Web Navigator (HTTP)

*2838 Network News Transfer Protocol (NNTP)

*2839 Post Office Protocol 3 (POP3)

*2840 Internet Message Access Protocol (IMAP)

*2841 Lightweight Directory Access Protocol (LDAP)

*2842 Simple Mail Transport Protocol (SMTP)

*2843 Internet Inter-ORB Protocol (IIOP)

*2844 The Java applet that uses this protocol must be set up to use SSL.

*2845 Simple Authentication and Security Layer (SASL)

Domino использует SASL автоматически, если SSL настроен для идентификации клиента на сервере и если LDAP клиент поддерживает этот протокол. Никакая дополнительная конфигурация не требуется.

6.6.2 Настройка SSL на сервере Domino.

Установите SSL на сервере Domino так, чтобы клиенты и сервера, которые соединяются с сервером, использовали SSL, для гарантирования секретности и идентификации в сети. Вы настраиваете SSL на основании протокола, который собираетесь использовать.

Например, Вы можете использовать SSL для почтовых протоколов IMAP, POP3 и SMTP - но не для других протоколов.

Вы должны закончить процесс установки, независимо от того, запрашивает ли Ваш сервер сертификаты от Domino, или от сертификатора других производителей CA.

Чтобы настроить Domino сервер для использования SSL, Вы и CA исполняете эти шаги:

*2846 Устанавливаете приложение Server Certificate Admin (CERTSRV.NSF), которое Domino создает автоматически в течение установки сервера.

*2847 Создайте файл сервера Key Ring, чтобы хранить сертификат сервера.

*2848 Запрашивайте SSL сертификат сервера от CA.

*2849 Сливайте сертификат CA как Trusted Root в файл сервера Key Ring.

*2850 CA одобряет просьбу о сертификате сервера и посылает Вам уведомление, что Вы можете приобрести сертификат.

*2851 Сливает одобренный сертификат сервера в файл Key Ring.

*2852 Конфигурируйте порт для использования SSL.

*2853 Если Вы используете идентификацию клиентов, добавьте имена клиентов в ACL баз данных, для доступа к элементам дизайна базы данных.

6.6.2.1 Установка приложения Server Certificate Admin.

Domino автоматически создает базу данных Server Certificate Admin в течение процесса установки сервера. Если Server Certificate Admin не доступен после того, как Вы запускаете Domino сервер, используете шаблон Certificate Admin (CSRV50.NTF), чтобы создать базу данных. Используйте Server Certificate Admin (CERTSRV.NSF) для:

*2854 Запроса сертификата сервера от Domino, или CA независимого производителя

*2855 Добавьте сертификата CA как Trusted Root

*2856 Управления сертификатом сервера в файле Key Ring, и создания само заверенного сертификата для испытательных целей.

Установка приложения Server Certificate Admin.

*2857 Удостоверьтесь, что Вы установили сервер как Domino Web сервер.

*2858 Редактирует ACL базы данных Server Certificate Admin, следующим образом:

- Добавьте имена администраторов серверов, кто будет иметь доступ к этой базе данных из клиента Domino Administrator. Назначите им доступ менеджера.
- Назначьте доступ по умолчанию - нет доступа, чтобы запретить другим пользователям, использовать базу данных.
- Установите в поле Предельный уровень доступа через интернет – Нет доступа.

Примечание Вы не должны добавлять имена администраторов сервера в локальном режиме доступ к базе данных.

*2859 Закончите процедуру Create server key ring file.

Предупреждение, чтобы скрыть базу данных Server Certificate Admin, когда пользователи выбирают из меню Файл – База данных – Открыть, или когда Web клиенты просматривают список баз данных сервера, уберите отметку опции, в свойствах базы данных – Отображать в окне Открытия базы данных.

6.6.2.2 Создание файла сервера Key Ring.

Прежде, чем Вы запросите сертификат от CA, Вы должны создать файл сервера Key Ring, чтобы хранить сертификат. Key Ring файл - двоичный файл, который защищен паролем. Он сохраняется на жестком диске сервера. Когда Вы создаете файл сервера Key Ring, Domino производит сертификат сервера, без отметки сертификатора. Сертификат сервера без отметки сертификатора не имеет силу, пока CA не подпишет его.

Каждый сертификат сервера SSL имеет уникальное имя, оно используется для SSL связей. Когда Вы создаете файл сервера Key Ring, Вы определяете это имя. Хотя некоторые компоненты имени необязательные, чем большее количество компонентов Вы включаете в него, тем меньшее вероятность, что Вы столкнетесь с идентичным именем в другом месте в интернете.

*2860 Удостоверится, что Вы создали базу данных Server Certificate Admin.

*2861 Из клиента Domino Administrator, выбирайте закладку Файлы, откройте базу данных Server Certificate Admin.

*2862 Выбирайте – Create Key Ring.

*2863 Заполните эти поля:

Поле	**Значение**
Key Ring File Name	Имя файла По умолчанию KEYFILE.KYR. **Примечание.** Название Key Ring файла появится на закладке Ports – Internet Ports, Server документа. Если вы изменяете имя по умолчанию, Вы должны редактировать Server документ.
Key Ring Password	Пароль - 12 символов
Key Size	Размер 512-бит
Common name	Полное имя TCP/IP хоста, включая домен Пример: www.lotus.com
Organization	Название Организации - Acme.
Organizational Unit	(Optional) Отдел в организации.
City or Locality	(Optional) Город
State or Province	Штат, провинция
Country	Страна

*2864 Выбирайте – Create Key Ring.

*2865 После того, как Вы прочитаете, информация относительно файла Key Ring и увидите его имя, выбирайте – OK. Notes создает файл Key Ring и разместит, его в каталоге данных Notes на локальном компьютере клиента.

*2866 Скопируйте файл Key Ring в каталог данных на сервер.

6.6.2.3 Запрос SSL сертификата сервера.

Вы можете запрашивать и получать сертификат сервера или от CA производителей третьих фирм или от Domino. Сертификат сервера - двоичный файл, который уникально опознает сервер. Сертификат сервера содержит публичный ключ, имя, дату истечения и цифровую подпись, он сохраняется на жестком диске сервера.

Когда Вы запрашиваете сертификат сервера SSL, Вы используете стандартный Public-Key Cryptography Standards (PKCS) формат, этот промышленный формат используют многие производители CA, включая Domino. Прежде, чем Вы запрашиваете сертификат от производителя CA третьих фирм, убедитесь, что производитель CA использует формат PKCS, или не некоторый другой формат, типа Privacy-Enhanced Mail (PEM). Если Вы не уверены в этом, требуйте от производителя, проверить CA.

Получение сертификата от Domino CA.

*2867 Удостоверится, что Вы уже создали Key Ring файл сервера и имеете к нему доступ.

*2868 Из клиента Domino Administrator, выбирайте закладку Файлы и откройте базу данных Server Certificate Admin.

*2869 Выбирайте – Create Certificate Request.

*2870 Заполните эти поля:

Поле	**Значение**
Key Ring File Name	Имя файла Key Ring, включая путь к нему
Log Certificate Request	Выбирайте одно из двух: *2871 Yes - (по умолчанию) протоколировать запрос Server Certificate Admin application *2872 No – не протоколировать
Method	Метод получения сертификата: *2873 Paste – вставить из буфера обмена *2874 Form on CA's site – обратится на сервер поставщика CA

*2875 Нажмите - Create Certificate Request.

*2876 Введите пароль для файла сервера Key Ring.

*2877 Скопируйте сертификат в буфер обмена, включая специальные строки начала сертификата и его конца, потом – OK.

*2878 На сервере, используйте один из этих методов для просмотра Domino Authority Certificate или участке Web CA:

- Если Вы используете IE Microsoft, используете TCP/IP, чтобы соединиться с приложением. Вы должны иметь Trusted root certificate сервера, чтобы использовать SSL для доступа на сервер. Если Вы не имеете этого сертификата, Вы должны соединиться с сервером с использованием TCP/IP. Сертификат CA сервера - сертификат, который Вы можете использовать вместо Trusted root certificate, который Вы получаете для каждого сайта. Сертификат сайта позволяет Вам доступ только на определенный сервер.

- Если Вы используете Netscape и, используете SSL, чтобы соединиться с приложением. Используйте инструкции для браузера, чтобы принять сертификат сайта.

*2879 Выбирайте – Request Server Certificate.

*2880 Введите Ваше имя, адрес электронной почты, телефонный номер и любые комментарии для CA.

*2881 Вставьте сертификат в окно диалога и затем выбирайте - Submit Certificate Request.

Получение сертификата от производителя CA.

*2882 Удостоверится, что Вы уже создали Key Ring файл сервера и имеете к нему доступ.

*2883 Из клиента Domino Administrator, выбирайте закладку Файлы и откройте базу данных Server Certificate Admin.

*2884 Выбирайте – Create Certificate Request.

*2885 Заполните эти поля:

Поле	**Значение**
Key Ring File Name	Имя файла Key Ring, включая путь к нему
Log Certificate Request	Выбирайте одно из двух: *2886 Yes - (по умолчанию) протоколировать запрос Server Certificate Admin application *2887 No – не протоколировать
Method	Метод получения сертификата: *2888 Paste into form on CA's site (рекомендуется) *2889 Send to CA by e-mail **Примечание.** Вы должны выбрать опцию Paste into form on CA's site, если запрашиваете сертификат VeriSign, этот производитель не поддерживает PKCS формат, для запросов по E-Mail. Если Вы выбрали Send to CA by email, введите CA E-Mail адрес, и свой E-Mail адрес, номер телефона и адрес.

*2890 Нажимайте Create Certificate Request.

*2891 Вводите пароль для Key Ring сервера.

*2892 Если Вы выбрали опцию Paste into form on CA's site, сделайте следующее:

- Скопируйте сертификат в буфер обмена.
- Используйте браузер, чтобы посетить сервер CA, и затем следовать за инструкциями, для запроса сертификата.

6.6.2.4 Как получить сертификат CA, слить его в Key Ring файл как Trusted Root сертификат.

Сертификат сервера должен содержать сертификат CA как Trusted Root. Trusted Root позволяет серверам и клиентам, которые имеют общий сертификат CA, связываться. Прежде, чем Вы сливаете сертификат сервера, подписанный CA, сливаете сертификат CA в Ваш файл Key Ring как Trusted Root.

Domino CA сертификат.

*2893 Удостоверьтесь, что Вы уже создали Key Ring файл сервера и имеете к нему доступ.

*2894 Просмотрите Domino Application Authority Certificate через Web сервер CA:

- Если Вы используете IE Microsoft, используете TCP/IP, чтобы соединиться с приложением. IE не позволяет Вам принимать сертификат, в Ваш браузер.
- Если Вы используете Netscape, используете SSL, чтобы соединиться с приложением. Используйте инструкции, по браузеру, чтобы принять сертификат сайта.

*2895 Выбирайте – Accept This Authority in Your Server.

*2896 Скопируйте сертификат в буфер обмена.

*2897 Из клиента Domino Administrator, выбирайте закладку Файлы и откройте Server Certificate Admin.

*2898 Выбирайте - Install Trusted Root Certificate into Key Ring.

*2899 Введите имя файла Key Ring, который будет хранить этот сертификат. Вы определили это имя, когда Вы создавали запрос на сертификат сервера.

*2900 Введите имя, которое файл Key Ring будет использовать, чтобы идентифицировать этот сертификат. Если Вы оставляете это поле незаполненной, Domino использует имя сертификата по умолчанию.

*2901 В поле Certificate Source, вставьте содержание буфера обмена.

*2902 Нажмите Merge Trusted Root Certificate into Key Ring.

*2903 Введите пароль для файла Key Ring, и затем – OK.

Сертификат производителей CA третьих фирм.

Просмотрите имеющиеся по умолчанию Trusted Root сертификаты в Вашем файле Key Ring, чтобы удостовериться, что сертификат производителя CA, уже не включен в файл. Если сертификат уже имеется, Вы не должны завершать эти шаги.

*2904 Удостоверится, что Вы уже создали Key Ring файл сервера и имеете к нему доступ.

*2905 Рассмотрите Web сайт CA и получите сертификат Trusted Root с сервера CA. В большинстве случаев сертификат Trusted Root находится в присоединенном файле, или доступен Вам, чтобы скопировать его в буфер обмена.

*2906 Из клиента Domino Administrator, выбирайте закладку Файлы, откройте Server Certificate Admin.

*2907 Выбирайте Install Trusted Root Certificate into Key Ring.

*2908 Введите имя файла Key Ring, который будет хранить этот сертификат. Вы определили это имя, когда Вы создавали запрос на сертификат сервера.

*2909 Введите имя, которое файл Key Ring будет использовать, чтобы идентифицировать этот сертификат. Если Вы оставляете это поле незаполненной, Domino использует имя сертификата по умолчанию.

*2910 Делайте одно из следующего:

- Если Вы скопировали содержание сертификата CA в буфер обмена, выбирайте опцию Clipboard в поле Source Certificate. Вставьте содержание буфера обмена в поле.
- Если Вы получили файл, который содержит сертификат CA, выбирайте опцию File в поле Source Certificate. Введите имя файла в поле названия файла.

*2911 Выбирайте - Merge Trusted Root Certificate into Key Ring

*2912 Введите пароль для файла Key Ring, и затем – OK.

6.6.2.5 Сертификаты Domino SSL trusted roots, установленные по умолчанию.

Domino содержит несколько сертификатов Trusted Root по умолчанию, когда Вы создаете Key Ring файл для сервера. Вам не нужно сливать сертификаты производителей CA, как Trusted Root, так как эти сертификаты существует в Key Ring файле по умолчанию.

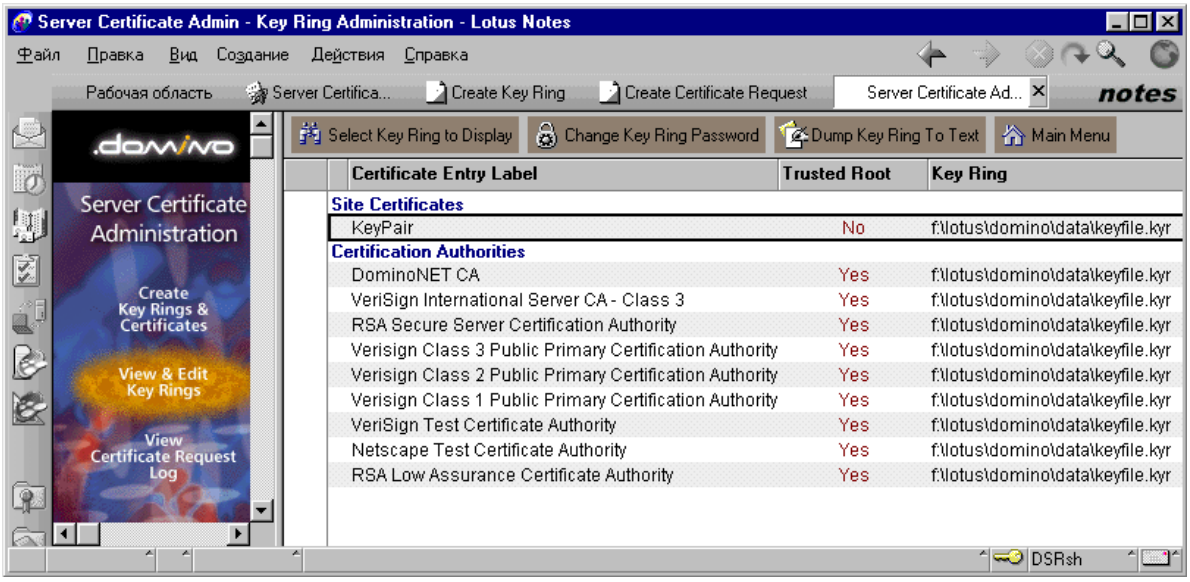


Рис. 109 Просмотр имеющихся в Domino CA сертификатов.

Trusted root certificate name	Organization	Organizational Unit	Country
VeriSign Class 4 Public Primary Certification Authority	VeriSign, Inc.	Class 4 Public Primary Certification Authority	US
VeriSign Class 3 Public Primary Certification Authority	VeriSign, Inc.	Class 3 Public Primary Certification Authority	US
VeriSign Class 2 Public Primary Certification Authority	VeriSign, Inc.	Class 2 Public Primary Certification Authority	US
VeriSign Class 1 Public Primary Certification Authority	VeriSign, Inc.	Class 1 Public Primary Certification Authority	US
RSA Secure Server Certificate Authority	RSA Data Security, Inc.	Secure Server Certification Authority	US
Netscape Test Certificate Authority	Netscape Communications Corp.	Test CA	US
RSA Low Assurance Certificate Authority	RSA Data Security, Inc.	Low Assurance Certification Authority	US
VeriSign Persona Certificate Authority	RSA Data Security, Inc	Persona Certificate	US

6.6.2.6 Подпись сертификата сервера.

CA подписывает сертификат сервера, чтобы добавить цифровую подпись CA в сертификат.

Метод подписи сертификата сервера, зависит от того, был ли сертификат выпущен от имени производителя CA или получен с использованием Domino.

Получение подписи сертификата от Domino CA.

Запрос о сертификате появляется в представлении Request Server Certificate в базе данных Application Authority Certificate. Когда CA подписывает сертификат, CA может автоматически посылать электронную почту администратору сервера. Эта электронная почта описывает, где можно забрать сертификат и содержит Pickup ID, чтобы идентифицировать сертификат в течение процесса Pickup. Domino автоматически производит Pickup ID.

Обратите внимание, что эти шаги относятся к подписанию сертификата сервера, который был выпущены Domino CA.

*2913 Удостоверьтесь, что администратор сервера слил сертификат CA как Trusted Root.

*2914 Удостоверьтесь, что Вы понимаете политику Вашей организации по подписанию сертификатов. Подпишите сертификат только, если запрос на сертификат удовлетворяет политике безопасности Вашей организации.

*2915 Из клиента Domino Administrator, выбирайте закладку Файлы, откройте Domino Application Authority Certificate.

*2916 Выбирайте Server Certificate Requests.

*2917 Открывайте запрос.

*2918 Рассматривайте информацию пользователя и имя. Удостоверьтесь, что информация, предоставленная Вам, удовлетворяет политике безопасности Вашей организации.

*2919 Далее следуют шаги, которые Вы выполняете, в зависимости от того, хотите ли Вы отвергнуть или одобрить запрос о предоставлении сертификата.

*2920 Чтобы отвергнуть запрос, делайте следующее:

- Введите причину для отклоненного запроса.
- Если Вы не хотите посылать письмо администраторы, отмените опцию - Send a notification уведомление email to the requester. Иначе, Domino посылает администратору письмо, указывающее на отказ запроса и причину отказа.
- Нажимайте - Deny.

*2921 Чтобы одобрить запрос, сделайте следующее:

- Введите период действия сертификата. Для краткосрочных проектов, 90 дней; для продолжающихся проектов, Вы можете ввести несколько лет.
- Если Вы не хотите посылать сообщение по почте администратору, что он может теперь забрать свой сертификат, отмените опцию - Send a notification уведомление email to the requester. Иначе, Domino посылает электронную почту администратору с URL местоположения сертификата.
- Нажмите – Approve.
- Введите пароль для Key Ring файла CA, затем – OK.

Получение подписи сертификата от производителя CA.

Производители фирм разработчиков CA решают сами, как подписать сертификат сервера. Для большего количества информации обратитесь к производителю CA.

6.6.2.7 Как слить подписанный сертификат сервера в файл Key Ring.

После того, как Вы слили сертификат CA как Trusted Root, и администратор CA одобряет Ваш запрос сертификации сервера, слейте подписанный сертификат в Key Ring файл сервера.

Domino CA.

*2922 Удостоверьтесь, что администратор CA подписал сертификат и Вам доступен сетевой диск, на котором хранится Key Ring сервера.

*2923 Если администратор CA дал Вам, URL, чтобы забрать сертификат из Domino базы данных Authority Certificate, обратитесь по URL и заберите сертификат.

*2924 Если необходимо получите Pickup ID от CA, сделайте следующее:

- Откройте Domino Application Authority Certificate, браузером.
- Выбирайте опцию - Pick Up Server Certificate.
- Введите полученный Pickup ID и выбирайте опцию - Pick Up Signed Certificate.

*2925 Скопируйте сертификат в буфер обмена.

*2926 Из клиента Domino Administrator, выбирайте закладку Файлы и откройте Server Application Certificate Admin.

*2927 Выбирайте - Install Certificate into Key Ring.

*2928 Введите имя файла Key Ring, который будет хранить этот сертификат. Вы определяли этот файл Key Ring, когда Вы создавали запрос на сертификат сервера.

*2929 В поле Source Certificate, выберите – Clipboard. Вставьте содержание буфера обмена в следующее поле.

*2930 Выбирайте – Megre Certificate into Key Ring.

*2931 Введите пароль для файла Key Ring, затем – OK.

Third-party CA.

*2932 Удостоверьтесь, что представитель CA подписал сертификат, и Вы имеете доступ к каталогу, который содержит файл сервера Key Ring.

*2933 Используйте инструкции, полученные от CA, чтобы приобрести сертификат. В большинстве случаев, CA отправляет сертификат, как присоединенный файл, или дает Вам URL, для посещения сайта производителя, чтобы копировать и вставить сертификат в буфер обмена.

*2934 Из клиента Domino Administrator, выбирайте закладку Файлы и откройте Server Application Certificate Admin.

*2935 Выбирайте - Install Certificate into Key Ring.

*2936 Введите имя файла Key Ring, который будет хранить этот сертификат. Вы определили этот файл Key Ring, когда Вы создавали запрос на сертификат сервера.

*2937 В поле Source Certificate, выберите – Clipboard. Вставьте содержание буфера обмена в следующее поле.

*2938 Выбирайте – Megre Certificate into Key Ring.

*2939 Введите пароль для файла Key Ring, и затем – OK.

6.6.2.8 Конфигурирование порта SSL.

Вы можете сконфигурировать SSL порт на сервере, чтобы использовать один из двух опознавательных методов: идентификация только для сервера, или идентификация для

сервера и клиента. Вы должны установить идентификацию на базе протокола. Некоторые протоколы не поддерживают идентификацию для клиентов.

Настраивая порт для SSL, Вы:

*2940 Конфигурируете порт

*2941 Определите, требуете ли Вы от пользователей для доступа на сервере использовать только SSL, или и SSL и TCP/IP

Использование идентификации только сервером.

Установление подлинности для сервера, шифрует транзакции, подтверждает данные, идентифицирует сервера. Используйте только для сервера установление подлинности, если доступ клиентов на сервер должен быть анонимный. Для управления доступом к базам данных на сервере, установите проверку имени и пароля. Разрешите SSL только для сервера:

*2942 Сервер должен иметь сертификат от CA третьей фирмы или Domino.

*2943 Клиенты должны иметь сертификат CA сервера, отмеченные как Trusted Root.

*2944 Если Вы используете клиента Notes, клиент Notes должен иметь взаимный сертификат для сервера CA.

Использование идентификации сервером и клиентом.

В дополнение к безопасности сервера, установите опцию, идентификации клиентом. Используя идентификацию для сервера и клиента, Вы может управлять доступом к базам данных, определяя индивидуальные имена пользователей в ACL баз данных. Позвольте идентификацию SSL для клиента и сервера. Закончите вышеупомянутые процедуры идентификации для сервера.

*2945 Клиенты должны иметь сертификаты от CA независимых разработчиков или от Domino.

*2946 Server должен иметь сертификат CA клиента, отмеченный как Trusted Root.

*2947 Каждый клиент должен иметь Person документ в Domino Directory, который содержит SSL публичный ключ сертификата клиента.

6.6.2.8.1 Конфигурирование порта для использования SSL.

Вы можете сконфигурировать порт, чтобы использовать идентификацию только для сервера, или использовать идентификацию для клиента и сервера.

*2948 Откройте Server документ.

*2949 Выбирайте закладку Ports – Internet Ports.

*2950 Заполните эти поля:

Поле	**Значение**

SSL key file	Имя файла Key Ring сервера, который используется сервером. Если файл Key Ring находится не в каталоге данных сервера, введите полный путь к файлу. **Примечание.** Domino не использует это поле для IIOP, который использует другой файл Key Ring. Вы не можете изменять имя файла Key Ring для IIOP.
SSL protocol version	Выбирайте одно: *2951 V2.0 only – позволяется только SSL версии 2.0 соединения *2952 V3.0 Handshake – делается попытка соединения с использованием SSL версии 3.0. Если попытка неудачна, но обнаружено SSL версии 2.0, предпринимается попытка соединения с использованием SSL версии 2.0. *2953 V3.0 Only – позволяется только SSL версии 3.0 соединения *2954 V3.0 And V2.0 Handshake – предпринимается попытка соединения с использованием SSL версии 2.0, если попытка неудачна и получено сообщение об ошибке, предпринимается попытка соединения по SSL 3.0, если это возможно. *2955 Negotiated - (по умолчанию) делается попытка соединения с использованием SSL версии 3.0. Если попытка неудачна, используется SSL версии 2.0. Используйте эту установку, если Вы не имеете проблем с использованием протоколов. **Примечание.** Domino не использует это поле для HTTP.
Accept SSL site certificates	Выбирайте одно: *2956 Yes - чтобы позволять этому серверу принимать сертификаты сайтов и использовать SSL для доступа интернет сервера, даже если сервер не имеет общего сертификата с интернет сервером. *2957 No - не позволять принимать сертификаты
Accept expired SSL certificates	Выбирайте одно: *2958 Yes - позволять клиентам доступу на сервер, даже если сертификат клиента просрочен. *2959 No - не позволять клиентам доступ на сервер, срок действия сертификатов, которых истек.

*2960 Выбирайте закладку для протокола, который Вы хотите сконфигурировать и затем, заполняйте эти поля:

Поле	**Значение**
SSL port number	Введите номер порта, на котором Domino слушает запросы для SSL. **Обратите внимание**, если Вы изменяете номер порта по умолчанию, клиенты должны изменить их конфигурации также. Номер порта по умолчанию обычно изменяется только, если сервер Firewall или Proxy использует это значение порта.
SSL port status	Выбирайте значение Enabled, чтобы позволить соединения SSL по порту. **Примечание.** Domino сервер может работать как SMTP сервер или как SMTP клиент. Поэтому у вас имеется две настройки SSL порта. Для разрешения использования Domino сервера с SSL выбирайте – Enabled в поле SMTP Inbound.
Client certificate	Выбирайте одно: *2961 No - не использовать идентификацию клиентов. *2962 Yes - использовать. **Примечание.** SMTP и IIOP не поддерживают эту функцию.
Name & password	Выбирайте одно: *2963 No – не использовать идентификацию с использованием имени и пароля пользователя. *2964 Yes - использовать идентификацию с использованием имени и пароля пользователя.
Anonymous	Выбирайте одно: *2965 Yes - все используют анонимный доступ. *2966 No - запретить анонимный доступ. **Обратите внимание**, если Вы выбрали значение – Yes для пользователя Anonymous и для доступа Client certificate, Domino сначала пробует идентифицировать клиента. Если идентификация терпит неудачу, Domino пробует соединять пользователя анонимно. Если Вы выбираете – Yes для доступа Anonymous и для доступа Client certificate, и для Name & password, Domino сначала пробует идентифицировать клиента с использованием сертификата клиента. Если это не удается, Domino пробует использовать имя и пароль, для идентификации. Если и это не удается, Domino пробует соединить пользователя анонимно.

6.6.3 Требование установки SSL связи, с сервером.

После того, как Вы установили SSL на сервере, Вы можете требовать SSL соединений. Например, Вы можете вынуждать клиентов и сервера использовать SSL, чтобы соединиться с определенным портом сервера или, не разрешать доступ клиентам и серверам, которые используют TCP/IP, чтобы соединиться с этим портом. Требуйте SSL связей, когда Вы хотите удостовериться, что клиенты используют безопасные соединения для доступа к базам данных на сервере. Если Вы не требуете SSL соединений, клиенты могут использовать или SSL, или TCP/IP, чтобы соединиться с сервером.

Вы можете требовать SSL соединений для всех баз данных на сервере или только для некоторых баз данных.

Требование соединений по SSL, для всех баз данных на сервере.

*2967 Из клиента Domino Administrator, выбирайте закладку Настройка, откройте Server документ.

*2968 Выбирайте закладку Ports – Intrnet Ports.

*2969 Выбирайте закладку нужного протокола.

*2970 В поле TCP/IP port status, выберите значение – Redirect to SSL. Обратите внимание NNTP, POP3 и SMTP не поддерживают Redirect to SSL установку.

Требование соединения SSL, для выбранной базы данных.

*2971 Запустите клиента Notes.

*2972 Выбрать базу данных, для которой Вы хотите вынудить клиентов использовать SSL.

*2973 Откройте свойства базы данных.

*2974 На закладке Basics, выберите - Web: Требовать наличия SSL-подключения.

6.6.4 Настройка доступа к базам данных для SSL клиентов.

После того, как Вы установили SSL на Domino сервере, Вы должны дать доступ клиентам к базам данных на сервере.

Доступ для анонимных пользователей.

Если Вы настраиваете клиента для идентификации только сервером, Вы не можете вводить имя в ACL базах данных, так как клиент не использует имя пользователя для доступа на сервер. Вместо этого, Вы добавляете имя Anonymous в ACL баз данных и списков доступа к модулям приложений. Если Вы не определяете Anonymous доступ, Domino дает всем анонимным пользователям доступ - по умолчанию.

Доступ для идентифицированных клиентов.

Если Вы устанавливаете идентификацию клиентов и сервера, Вы можете управлять доступом клиентов к базам данных, добавляя их имена в ACL баз данных и спискам доступа. Вы должны использовать первое имя, внесенное в список имен пользователя, из Person документа для идентификации клиента.

6.6.5 Управление сертификатами сервера и запросами на выдачу сертификатов.

Вы можете делать следующие, чтобы управлять Вашими сертификатами сервера и запросами на сертификацию:

*2975 Просмотрите сертификаты сервера SSL

*2976 Работа с просроченными сертификатами

*2977 Просмотр запросов сертификатов

*2978 Изменение значения “доверия”, для CA сертификатов, определенных как Trusted Root

*2979 Изменение пароля для файла сервера Key Ring

6.6.5.1 Просмотр SSL сертификатов сервера.

Каждый SSL сертификат сервера содержит информацию:

*2980 Дата истечения. По умолчанию Trusted Root сертификаты, которые поставляются с Domino, не имеют дат истечения сертификатов.

*2981 Название сервера назначения, который затребовал сертификат.

*2982 Название сервера назначения, который подписал сертификат.

*2983 Размер публичного ключа. Размер определяет степень шифрования публичного ключа.

Просмотр SSL сертификатов сервера.

*2984 Спланируйте драйв в каталог, который содержит файл Key Ring.

*2985 Из клиента Domino Administrator, выбирайте закладку Файлы, откройте базу данных Server Certificate Admin.

*2986 Выбирайте представление View & Edit Key Ring.

*2987 (Необязательно) Для просмотра сертификатов другого файла, делайте следующее:

- Выбирайте - Select Key Ring file to Display
- Введите путь и имя файла Key Ring, который содержит сертификаты, которые Вы хотите просмотреть.
- Введите пароль для файла Key Ring.

*2988 Делайте одно из следующего:

- Чтобы просмотреть сертификат сервера, выберите документ в категории Site Certificates.
- Чтобы просмотреть Trusted Root Certificate, выберите документ из категории Certification Authorities.

6.6.5.2 Работа с просроченными сертификатами.

После того, как истекает срок действия сертификата, Вы больше не можете использовать его, чтобы связаться с серверами и клиентами.

*2989 Создайте новый Key Ring файл и запросите новый сертификат от Certification Authority (CA).

*2990 Слейте сертификат CA как Trusted Root в файл Key Ring.

*2991 Слейте подписанный сертификат сервера в Key Ring файл.

6.6.5.3 Просмотр запросов для сертификатов.

Администраторы сервера могут просматривать информацию о запрошенных CA сертификатах и отслеживать запросы. Документ запроса содержит информацию о сертификате, дату и время запроса, файл Key Ring для сертификации, и если используется электронная почта, адрес администратора, который послал запрос.

Для Domino CA можно также просматривать информацию относительно запросов сертификации сервера или клиента, по ожидающим одобрение, одобренным запросам, ожидающим одобрения и отвергнутым запросам.

База данных Server Certificate Admin.

*2992 Из клиента Domino Administrator, выбирайте закладку Файлы, откройте базу данных Server Certificate Admin.

*2993 Выбирайте представление View Certificate Request Log.

*2994 Открывайте документ запроса.

Domino CAs.

*2995 Из клиента Domino Administrator, выбирайте закладку Файлы, откройте базу данных Domino Certificate Authority.

*2996 Выбирайте представление Server Certificate Requests или Client Certificate Requests.

*2997 Используйте меню Действия, чтобы показать запросы, ожидающие одобрение, одобренные запросы, и отклоненные запросы.

6.6.5.4 Как установить или отменить доверие CA сертификату Trusted Root.

Удалите сертификат CA Trusted Root из сертификата сервера, когда Вы больше не хотите связаться с серверами и клиентами, которые используют сертификаты, подписанные этим CA.

*2998 Убедитесь, что вы имеете доступ к файлу Key Ring.

*2999 Из клиента Domino Administrator, выбирайте закладку Файлы и откройте базу данных Server Certificate Admin.

*3000 Выбирайте представление View & Edit Key Rings.

*3001 Из категории Certification Authorities, откройте документ, который содержит сертификат, и который Вы хотите редактировать.

*3002 Нажмите кнопку Do Not Trust Certificate, чтобы отменить доверие этому сертификату, как Trusted Root. Domino помечает сертификат опцией недоверия, но не удаляет его из базы данных. Чтобы удалять сертификат из файла Key Ring, нажмите кнопку Delete Certificate. После того, как Вы удаляете сертификат, Вы не сможете его восстановить. Вместо этого, Вы должны будете слить сертификат как Trusted Root заново.

*3003 Введите пароль для файла Key Ring.

6.6.5.5 Изменение пароля файла Key Ring сервера.

*3004 Убедитесь, что вы имеете доступ к файлу Key Ring.

*3005 Из клиента Domino Administrator, выбирайте закладку Файлы, откройте базу данных Server Certificate Admin.

*3006 Выбирайте представление View & Edit Key Rings.

*3007 Нажмите на кнопку Change Key Ring password.

*3008 Введите имя Key Ring файла и затем – ОК.

*3009 Введите текущий пароль – ОК.

*3010 Введите новый пароль, по крайней мере, 12 знаков и затем – ОК.

6.6.6 Создание безопасного сертификата для тестирования SSL сертификации.

Вы можете создавать Self-Certified Certificate (безопасный тестовый сертификат), чтобы проверить процедуру сертификации в Вашей организации. Потому что этот сертификат не заверен CA, используйте его только для испытательных целей.

*3011 Из клиента Domino Administrator, выбирайте закладку Файлы, откройте базу данных Server Certificate Admin, затем выбирайте – Create Key Rings & Certificates.

*3012 Выбирайте - Create Key Ring with Self-Certified Certificate.

*3013 Заполните эти поля, затем выбирайте – Create Key Ring with Self-Certified Certificate:

Поле	**Значение**
Key Ring File Name	Имя файла По умолчанию KEYFILE.KYR. **Примечание.** Название Key Ring файла появится на закладке Ports – Internet Ports, Server документа. Если вы изменяете имя по умолчанию, Вы должны редактировать Server документ.
Key Ring Password	Пароль - 12 символов
Key Size	Размер 512-бит
Common name	Полное имя TCP/IP хоста, включая домен Пример: www.lotus.com
Organization	Название Организации - Acme.

Organizational Unit	(Optional) Отдел в организации.
City or Locality	(Optional) Город
State or Province	Штат, провинция
Country	Страна

*3014 Скопируйте файл Key Ring в каталог данных на сервере.

6.6.7 SSL в международных организациях.

SSL использует публичные и личные ключи для сессий, которые имеют различные степени шифрования. Лицензия, используемая для сервера, с использованием которой создается сертификат SSL - определяет силу шифрования. Сервер, который использует Северо-Американскую лицензию, имеет более сильное шифрование, чем сервер, использующий международную лицензию.

Публичные и личные ключи.

Каждый сертификат SSL имеет публичный и личный ключ. Эти ключи, которые создаются при создании сертификата SSL, позволяют владельцам сертификата идентифицировать себя по сети и использовать S/MIME, чтобы шифровать и подписывать сообщения.

Сила шифрования, используемого для ключевой пары, зависит от лицензии сервера, или браузера, с использованием которого создавался SSL сертификат. Если сервер или браузер имеет Северо-Американскую лицензию, ключевые пары создаются с использованием шифрования - 1024 бит. Если сервер или браузер имеет международную лицензию, то пары ключей создаются с использованием шифрования - 512 бит. Начиная с версии 5.0.4, Domino поставляется с Global лицензией, которая использует – 1024 битные ключи шифрования.

Negotiated session keys (cipher specification).

Ключ для сессии Negotiated создается в начале SSL рукопожатия. Это рукопожатие определяет ключ, используемый при шифровке информации для соединения. Ключ сессии Negotiated изменяется каждый раз при запуске новой сессии.

Если сервер имеет Северо-Американскую лицензию, то ключ сессии - 128 бит. Если сервер имеет международную лицензию, ключ сессии - 40 бит. Если Вы поддерживаете связь между Северо-Американскими странами и другими странами, применяется более низкий уровень шифрования. Например, пользователь в Париже (Франция), устанавливает сессию с сервером в Вашингтоне, сервер генерирует ключ шифрования - 40 бит.

Одно исключение к этому правилу - если сервер использует Global Server ID, выпущенный от имени VeriSign. VeriSign Global Server ID позволяет Американским серверам и международным банкам генерировать ключ в 128 бит, при связи с международным браузерами и серверами по HTTP, NNTP, LDAP, IMAP и POP3. Если Ваш браузер поддерживает Global Server ID, то Domino автоматически использует ключ в 128 бит для сессии. Для информации относительно VeriSign Global Server IDS, посетите Web сервер http://www.verisign.com/

Вы можете изменять спецификацию ключа, чтобы управлять размером ключа для сессий Negotiated, для требуемого сервера.

6.6.8 Изменение спецификации шифра SSL.

Вы можете определить один или большее количество SSL спецификации шифра для службы HTTP. Вы можете определить шифр - 128 бит для службы HTTP.

Изменение шифра.

*3015 Из клиента Domino Administrator, выбирайте закладку Настройка, откройте Server документ из Domino Directory.

*3016 Выбирайте закладку Ports – Internet Ports – Web.

*3017 Нажмите кнопку Modify для поля SSL Chipher. Вы получите список доступных SSL спецификаций шифров.

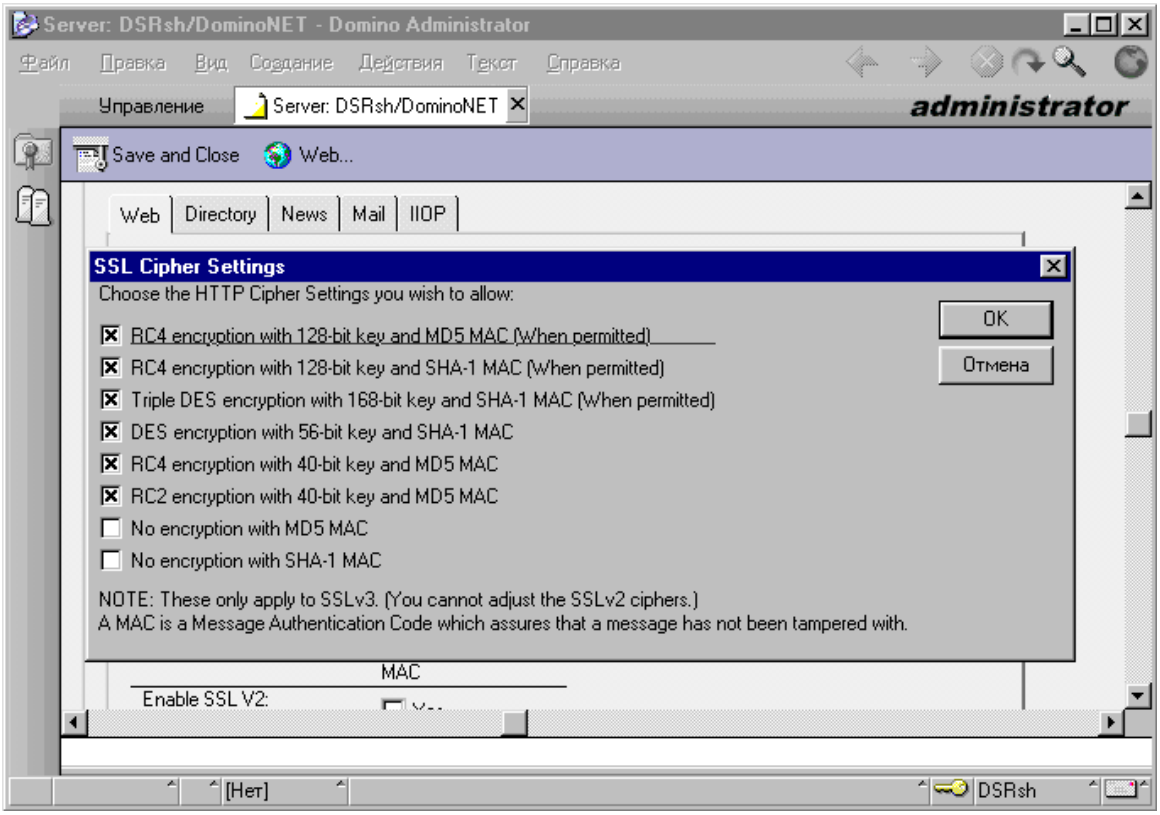


Рис. 110 Диалоговое окно определения шифров, используемых SSL.

*3018 Выбирайте нужную спецификацию шифра, затем – OK.

*3019 Сохраните и закройте документ.

Вы можете также использовать переменную SSLCIPHERSPEC в файле NOTES.INI, чтобы определить SSL спецификацию шифра, для задач LDAP, IMAP, POP3, NNTP и HTTP. Вы можете выбирать несколько шифров только для HTTP. Для всех других задач, Вы можете определить только один шифр.

6.6.9 Установление подлинности и идентификация для SSL.

SSL клиенты проверяются только тогда, когда они пытаются получить доступ к ограниченным ресурсам. Например, когда пользователи пробуют открыть базу данных, у которой доступ по умолчанию закрыт, при этом требуется использовать SSL, чтобы

идентифицировать. Сервер определяет, есть ли у клиента сертификат, имеется ли анонимный доступ, или клиент должен ввести имя и пароль.

Метод использования, подтверждения подлинность LDAP клиентов зависит от того, установленной переменной LDAP_STRICT_RFC_ADHERENCE в файле NOTES.INI.

Правило доверия SSL публичным ключам.

Доверенный сертификат CA подписывает ключевые пары, публичного и личного ключей, и надежно передает их клиенту.

Вы можете доверять любому серверу или клиенту, которые имеют цифровую подпись или для которого Вы имеете сертификат CA, помеченный как Trusted Root.

Пример применения доверия.

Следующий пример описывает, как клиент Hugo использует SSL, чтобы соединиться с сервером Mail-E:

*3020 Hugo пробует доступ к базе данных на сервере Mail-E.

*3021 Mail-E проверяет Server документ, чтобы видеть, позволяется ли SSL для протокола. Если SSL позволяется, установление подлинности продолжается. Иначе, Hugo лишается доступа на сервер с использованием SSL.

*3022 Hugo посылает запрос, Mail-E определяет информацию относительно SSL соединения, типа поддерживаемых алгоритмов шифрования и даты истечения сертификата.

*3023 Mail-E посылает сертификат Hugo, который содержит публичный ключ Mail-E. Hugo проверяет цифровую подпись CA на сертификате Mail-E, чтобы идентифицировать сервера Mail-E. Если Hugo имеет сертификат CA сервер Mail-E, отмеченный как Trusted Root, в своем сертификате, или если Hugo использует клиента Notes, Hugo имеет взаимный сертификат для CA, то Hugo знает, что сертификат сервера Mail-E имеет силу, и опознавательный процесс, продолжается. В противном случае, опознавательный процесс завершается.

*3024 Если Hugo доверяет сертификату CA Mail-E, Hugo использует алгоритм, чтобы создать ключ сессии. Он использует публичный ключ, сохраненный в сертификате Mail-E, чтобы зашифровать ключ сессии, и посылает его Mail-E. Ключ для сессии, из соображений безопасности генерируется для каждой сессии.

*3025 Mail-E использует личный ключ Mail-E, для де шифрования ключа сессии и использует ключ сессии, чтобы шифровать данные между Hugo и Mail-E.

*3026 Если установление подлинности клиента позволяется, следующее происходит:

- Mail-E запрашивает сертификат Hugo.
- Hugo посылает Mail-E свой сертификат.
- Mail-E проверяет цифровую подпись CA на сертификате Hugo, чтобы проверить идентичность Hugo. Если Mail-E имеет сертификат CA Hugo, отмеченным как Trusted Root в сертификате сервера, то Mail-E знает, что сертификат Hugo имеет силу.
- Mail-E проверяет имя пользователя, в Person документе и имя в сертификате Hugo и подтверждает, что публичный ключ в сертификате Hugo, соответствует публичному

ключу в его Person документе. Mail-E проверяет сначала Person документы в первичном Domino Directory. Mail-E также проверяет вторичные Domino Directory и LDAP Directory, если пользователь - Web клиент, а Domino сконфигурирован для поиска во вторичных Domino Directory и LDAP Directory.

*3027 Если Mail-E не может идентифицировать Hugo, Mail-E проверяет, позволяется ли анонимный доступ на сервер для протокола. Если позволено, следующее происходит:

- Сервер проверяет, имеется ли запись имени Anonymous в ACL базы данных.
- Если не имеется, сервер проверяет доступ по умолчанию.
- Если доступ по умолчанию читатель и выше, то Hugo позволяется анонимный доступ к базе данных, используя уровень доступов - по умолчанию.

*3028 Если анонимный доступ не разрешается, или если в ACL базы данных не позволяет анонимный доступ, сервер проверяет, позволяется ли идентификация, с использованием имени и пароля, на сервере, для протокола. Если доступ по имени и пароля позволяется, следующее происходит:

- Сервер просит, чтобы Hugo ввел свое имя пользователя и пароль.
- Сервер проверяет имя в Person документах для пользователя Hugo и пароль, который Hugo ввел. Сервер также проверяет вторичные Domino Directory и LDAP Directory, если пользователь - Web клиент, а Domino сконфигурирован для поиска во вторичных Domino Directory и LDAP Directory..
- Если пароль верен, сервер проверяют ACL базы данных для первой записи, из списка имен Person документа для Hugo.

*3029 Если первая запись в поле имени, соответствует записи в ACL, Hugo получает доступ к базе данных, используя уровень доступа, указанный для этой записи.

6.7 Настройка клиентов для использования S/MIME и SSL.

Глава описывает, как настроить клиента Notes, чтобы использовать SSL и посылать безопасные S/MIME сообщения. Она также описывает, как настроить клиента интернет, для использования SSL, чтобы соединиться с Domino сервером.

6.7.1 SSL и S/MIME для клиентов.

Клиенты могут использовать Domino Certificate Authority (CA) или CA других производителей, чтобы получить сертификат SSL. Метод, который Вы будете использовать, чтобы настроить клиента, зависит от следующего:

*3030 Тип Клиента - или Notes или другой клиент интернет

*3031 Тип сертификата CA - Domino CA или другой производитель CA, типа VeriSign

*3032 Требования безопасности для клиента: серверное SSL установление подлинности, SSL установление подлинности клиента, или S/MIME безопасность для сообщений.

Идентификация с использованием SSL клиентом и сервером.

SSL - протокол, используемый Notes и другими клиентами интернета, который шифрует соединения, подтверждает данные и подлинность серверов, идентичность клиента, когда

Notes или другой клиент интернет соединяется с интернетом сервером - например, Web сервером или LDAP сервером.

На сервере с настроенным SSL протоколом, Вы можете выбирать разрешение SSL на всех протоколов, или позволять SSL только на некоторых протоколах. Например, Вы можете позволить SSL на протоколах почты IMAP, POP3, SMTP, но запретить его для NNTP.

Вы можете настроить клиента для идентификации сервером, или и установление подлинности клиентом и сервером. Как Вы настроите клиента, зависит от того, требует ли сервер устанавливать подлинности, или установление подлинности будут осуществлять клиент и сервер.

Установление подлинности сервером позволяет клиентам проверять идентичность сервера, чтобы удостовериться, что другой сервер не выдает себя за сервер, к которому Вы хотите получить доступу.

Установление подлинности клиентом, позволяет администраторам серверов идентифицировать клиента, обращающегося на сервер и управлять доступом к базам данных, основанным на идентичности клиента. Например, если Вы хотите, чтобы Alan Jones имел доступ редактора к базе данных, но все другие обращающийся к базе данных, имели доступ автора, Вы можете настроить ACL базы данных, чтобы включить имя Alan Jones как редактор, но предоставить пользователю Anonymous доступ автора.

Вы должны тщательно рассмотреть, хотите ли Вы требовать идентификации клиента. Если Вы не должны идентифицировать пользователей интернета, кто имеет доступ на сервер, Вы не должны настаивать установление подлинности клиента. Фактически, в некоторых случаях, требуя интернет сертификат, Вы может запретить пользователям вызов сервера. Если Вы требуете интернет сертификат, пользователь должен исполнить дополнительные шаги, чтобы настроить установление подлинности клиента.

Notes и клиенты интернет, которые используют установление подлинности клиента, имеет интернет сертификаты, которые содержат публичные и личные ключи, имя, дату истечения, и цифровую подпись сертификата. Клиенты Notes хранят интернет сертификаты в Notes ID файле, клиенты интернет хранят интернет сертификаты в локальном файле. Публичный ключ клиента также сохраняется в Domino Directory, так что другие могут получить к нему доступ.

интернет и клиенты Notes могут получить интернет сертификаты или от Domino CA или независимых производителей CA.

Шифрование сообщений с использованием S/MIME.

S/MIME - протокол, используемый клиентами, чтобы подписать сообщения почты и посылать шифрованные почтовые сообщения пользователям почтовых программ, которые также поддерживают S/MIME протокол. IE и Netscape Коммуникатор поддерживают эти функции. Клиент Notes использует интернет сертификат, тот же самый сертификат, используемый для SSL - в Notes ID файле и публичный ключ, сохраненный в Domino Directory, чтобы шифровать и подписывать сообщения.

Клиент Notes должен также иметь публичный ключ каждого получателя в Domino Directory, чтобы послать шифрованные сообщения другим пользователям.

6.7.2 Установки Notes и интернет клиентов, для SSL идентификации сервером.

Вы можете настроить Notes или другого клиента интернета для идентифицикации, чтобы шифровать сессии, заверять данные и подтверждать подлинность сервера при соединении с интернет сервером. Вы не нуждаетесь в интернет сертификате, если Вы настраиваете клиента только для серверной установке подлинности.

Вы можете выбирать разрешение SSL на всех протоколов, или позволять SSL только на некоторых протоколах. Вы должны также позволить анонимный доступ к порту, иначе Domino будет требовать интернет сертификата или имя и пароль, от клиента.

Для доступа к интернет серверу и использования установление подлинности сервером, клиенты должны иметь:

*3033 Программное обеспечение, типа Web браузера или клиента Notes, который поддерживает SSL.

*3034 Trusted Root сертификат Domino CA или независимого производителя CA.

*3035 (Только для Notes клиента) взаимный сертификат, созданный с использованием Trusted Root сертификата Domino CA независимого производителя CA.

Используйте соответствующий синтаксис для установления безопасного соединения. Пример соответствующего синтаксиса, для установления безопасного соединения, когда браузер пользователи определяет URL для сервера следующий:

```
Https://
```

6.7.2.1 Получение Trusted Root сертификата для SSL идентифицикации сервером.

Копия сертификата CA называется Trusted Root сертификатом. После получения сертификата Trusted Root, клиент доверяет CA и любым сертификатам, выпущенным этим CA. Если Вы устанавливаете сервер установление подлинности для клиентов интернета, Вы добавляете этот сертификат Trusted Root в локальный файл. Если Вы настраиваете установление подлинности сервером для клиентов Notes, Вы добавить этот Trusted Root сертификат в Domino Directory, что пользователи могли получить доступ к нему, чтобы произвести взаимный сертификат в их персональных адресных книгах.

Клиенты Notes могут также использовать персональный Web Navigator, чтобы получить сертификат Trusted Root и взаимные сертификаты, чтобы получить доступ к серверу. Однако при добавлении сертификата Trusted Root в Domino Directory упрощает процесс идентифицикации сервером, для пользователей.

Если клиент Notes хочет установить доверие только с одним сервером, вместо всех серверов, которые имеют сертификат, выпущенный от определенного CA, клиент может создать взаимный сертификат только для этого сервера.

Получение сертификата Trusted Root для Notes клиента.

*3036 Если сертификат Trusted Root является для Domino CA, делает следующее:

- Из клиента Domino Administrator, выбирайте закладку Настройка, выбирайте из панели инструментов Сервис – Регистрация – Заверитель для интернета.
- Выберите CA key ring файл и введите пароль для него.

- Если необходимо, измените регистрационный сервер, сервер который первым будет хранить сертификат Trusted Root в Domino Directory. После этого, Domino Directory реплицирует Trusted Root сертификат на другие сервера.

- Нажмите – Регистрация.

- Выбирайте закладку Настройка, представление Разное – Сертификаты и просмотрите созданный сертификат в категории Internet Certifiers.

*3037 Если сертификат Trusted Root, является сертификатом производителя CA, клиент Notes, делает следующее:

- Используйте персональный Web Navigator, чтобы просмотреть сайт производителя CA.

- Следуйте инструкциями сайта CA, чтобы слить сертификат CA как Trusted Root. Domino автоматически добавит Trusted Root сертификат и создаст взаимный сертификат для CA в персональной адресной книге пользователя.

Получение Trusted Root сертификата для клиента интернета.

Вы можете также использовать следующие шаги, чтобы получить сертификат Trusted Root для клиента Notes, использующего персональный Web Navigator.

*3038 Если Trusted Root сертификат является сертификатом Domino CA, клиент интернета, делает следующее:

- Обратитесь через Web к приложению Domino Certificate Authority.

Если Вы используете IE, используете TCP/IP соединение, чтобы просматривать приложение. Вы должны иметь общий сертификат с сервером, чтобы получить доступ к нему, используя SSL. Однако IE не позволяет Вам принимать сертификат сайта в Ваш браузер. Сертификат сайта, является сертификатом полученным для пользователя сайта, который позволяет Вам доступ только определенному сайту.

Если Вы используете Netscape, используете SSL соединение, чтобы просмотреть приложение. Сервер показывает окно диалога и спрашивает Вас, хотите ли Вы принять сертификат сайта. Проверьте CA сертификат, перед принятием его как Trusted Root.

- Выбирайте опцию – Accept This Authority In Your Browser.

*3039 Если Trusted Root сертификат является сертификатором производителя CA, для клиента интернет, следуйте установленным порядком CA, чтобы слить Trusted Root сертификат для CA. Если и клиент и сервер имеют сертификаты, выпущенные от CA, или уже имеют общий CA, то этот шаг не нужен.

6.7.2.2 Создание взаимных сертификатов интернет для CA.

Прежде чем клиент Notes может подтверждать подлинность серверов или посылать шифрованные сообщения S/MIME, клиент должен сначала создать взаимный сертификат для сервера CA и хранить его в персональной адресной книге. Это позволяет клиенту Notes доверять серверам, которые имеют сертификаты, выпущенные этими CA. SSL установление подлинности сервера для клиентов интернет, не требует взаимного сертификата.

Клиент Notes может также создавать взаимный сертификат для сервера, однако, это позволяет клиенту доверять только этому серверу. Если клиент Notes создает взаимный сертификат для сервера, клиент Notes не должен получать Trusted Root сертификат для CA.

Создание взаимного сертификата интернет.

*3040 Удостоверитесь, что CA создал Trusted Root сертификат в Domino Directory.

*3041 Из клиента Notes, откройте документ сертификата в Domino Directory и выберите – Действие – Create Cross Certificate.

*3042 Выбирайте сертификат, для которого Вы собираетесь создать взаимный сертификат.

*3043 Удостоверитесь, что выбрали Локальный компьютер, выбирайте – Заверить.

Просмотр взаимного сертификата интернет.

*3044 Из клиента Notes, откройте персональную адресную книгу.

*3045 Выбирайте представление Параметры – Сертификаты.

*3046 Просмотрите категорию Перекрестные сертификаты интернета.

6.7.3 Установка клиентов Notes для S/MIME.

Вы можете настроить клиента Notes, чтобы использовать шифрование и электронную подпись S/MIME, при рассылке почты другим пользователям, использующим программы почты с поддержкой S/MIME.

Для шифрования, использования цифровых подписей S/MIME, клиент Notes должен иметь:

*3047 Взаимные сертификаты Domino CA, или производителей третьих фирм CA, созданные с использованием сертификата Trusted Root

*3048 интернет сертификат, выпущенный от Domino CA или производителя третьих фирм CA

*3049 Доступ и доверие публичному ключу получателя почты, чтобы посылать шифрованную почту.

*3050 MIME формат, выбранный для документов, зашифрованного или подписанного

Публичные и личные ключи для интернет сертификата, могут быть произведены, используя публичные и личные ключи, которые уже существуют в Notes ID файл. Вы можете произвести новые ключи, использующие больший размер ключа. Хотя производство новых ключей более безопасно, чем использование существующих ключей, используя существующие ключи более легкий способ.

Настройка Notes клиентов с сертификатом от Domino CA.

Производитель CA и клиент заканчивают эти шаги, чтобы добавить интернет сертификат к Notes ID файлу.

*3051 CA добавляет Trusted Root сертификат в Domino Directory, чтобы клиент мог получить доступ к нему.

- Клиент может также добавлять Trusted Root сертификат в персональную адресную книгу. Однако при добавлении Trusted Root сертификата в Domino Directory упрощается процесс настройки клиентов Notes, для S/MIME.

*3052 Клиент создает взаимный сертификат, используя Trusted Root сертификат для CA, сохраняет его в персональной адресной книге.

*3053 Чтобы создать сертификат, использующий существующие публичный и личный ключи, из Notes ID файла, сделайте следующее:

- (Шаг CA) Добавляет интернет сертификат в Person документ.
- (Шаг клиента) Идентифицирует на домашнем сервере. Notes автоматически добавляет интернет сертификат к ID файлу.

*3054 Чтобы создать интернет сертификат, используя новые публичный и личный ключи, сделайте следующее:

- Клиент запрашивает интернет сертификат от CA.
- CA одобряет запрос, и Domino автоматически добавляет публичный ключ клиента к пользовательскому Person документу.
- Клиент Notes сливает сертификат в ID файл.

Настройка Notes клиентов с сертификатом от производителя третьих фирм CA.

Производитель CA и клиент заканчивает эти шаги, чтобы добавить сертификат CA в Notes ID файл.

*3055 Используйте персональный Web Navigator, чтобы просмотреть сайт CA. Например, чтобы получить интернет сертификат VeriSign, посетите http://digitalid.verisign.com, и следуйте инструкциям.

*3056 Клиент следует инструкциям CA, для требования и слияния интернет сертификата.

*3057 Клиент следует порядком CA, чтобы слить CA сертификат для сервера, к которому клиент хочет получить доступ.

- Если и клиент и сервер имеют сертификаты, выпущенные от CA, или уже имеются общие CA сертификаты, то этот шаг не нужен. Notes автоматически создает взаимный сертификат CA и добавляет его к персональной адресной книге, когда Вы получаете Trusted Root сертификат.

*3058 CA добавляет публичный ключ клиента к Person документу.

6.7.4 Настройка Notes и интернет клиентов для SSL идентификации клиентов.

Вы можете настроить Notes или клиента интернета для идентифицикации клиента с сервером. Вы не можете использовать установление подлинности клиента для SMTP и IIOP связей. Для SSL идентифицикации клиента, Notes или клиент интернета должен иметь:

*3059 интернет сертификат выпущенного от Domino CA или производителя CA

*3060 Trusted Root сертификат для Domino CA или производителя CA

*3061 (Только для клиентов Notes) взаимный сертификат для Domino CA или производителя CA, созданный от Trusted Root сертификата

*3062 Программное обеспечение, типа Web браузера, или рабочего места Notes, которое поддерживает использование SSL

Используйте соответствующий синтаксис для безопасного соединения. Например, соответствующий синтаксис для безопасного соединения, когда браузер пользователи определяет URL для сервера - следующий:

```
Https://
```

Если LDAP клиент поддерживает простое установление подлинности и безопасный протокол слоя (SASL), Domino автоматически использует этот протокол, когда клиент соединяет с сервером с использованием SSL установление подлинности клиента. SASL не поддерживается для TCP/IP связей или SSL связей только с установлением подлинности сервером.

Публичные и личные ключи для интернет сертификата, могут быть произведены, используя публичные и личные ключи, которые уже существуют в Notes ID файл. Вы можете произвести новые ключи, использующие больший размер ключа. Хотя производство новых ключей более безопасно, чем использование существующих ключей, используя существующие ключи более легкий способ.

Настройка Notes и интернет клиентов с сертификатом, полученным от производителя CA.

Производитель CA и клиенты заканчивает эти шаги.

*3063 (Только клиенты интернета) создайте Person документы для клиентов интернет.

*3064 Клиент следует порядку CA для требований и слития интернета сертификата. Клиент Notes использует персональный Web Navigator, чтобы просматривать Web сайт CA. Клиент интернета может использовать любой доступный браузер. Например, чтобы получить интернет сертификат от VeriSign, посетите сайт http://digitalid.verisign.com, и следуйте инструкциям.

*3065 Клиент следует порядку CA, чтобы слить Trusted Root сертификат для CA. Если и клиент и сервер имеют сертификаты, выпущенные от CA, или уже имеют CA, то этот шаг не нужен. Если Вы используете персональный Web Navigator, Notes автоматически создает взаимный сертификат CA сервера и добавит его к персональной адресной книге, когда Вы получаете Trusted Root сертификат.

*3066 CA добавляет публичный ключ клиента к Person документу пользователя.

6.7.4.1 Как добавить интернет сертификат в Person документ.

Если Вы должны выпустить интернет сертификаты для клиентов Notes, и Вы не хотите требовать, чтобы каждый пользователь обращался в интернет и запрашивал сертификат и сливал его в ID файл, Вы можете выпускать интернет сертификат из Domino Directory и добавить его к Person документу пользователя. При издании интернет сертификатов, с использованием Domino Directory, упрощает процесс распределения интернет сертификатов пользователям.

Сервер, на котором Вы выпускаете интернет сертификаты, должен быть настроен для процесса администрирования и пользователи должны иметь интернет адрес в Person документе.

*3067 Удостоверитесь, что Вы имеете процесс администрирования, запущенный на сервере.

*3068 Из клиента Domino Administrator, выбирайте закладку Пользователи и группы.

*3069 Выбирайте имена пользователей, которые нуждаются в интернет сертификатах.

*3070 Выбирайте из меню Действия – Add Internet Cert to Selected People.

*3071 Выбирайте Key Ring файл CA и введите пароль.

*3072 Введите дату истечения сертификата, и затем выбирайте – Заверить.

Эти шаги происходят автоматически:

*3073 Для каждого выбранного пользователя, Domino создает сертификат и хранит, его в базе данных Administration Requests, в поле Add Internet Certificate to Person Record.

*3074 Когда база данных Administration Requests копируется на сервер администрирования в Domino Directory, процесс администрирования размещает сертификат в Person документе пользователя.

*3075 После того, как Domino Directory реплицируется на почтовый сервер пользователя и пользователь впоследствии пытается получить доступ на почтовый сервер, Notes признает, что имеется сертификат в Domino Directory, которого нет в ID файле пользователя. Notes автоматически помещает интернет сертификат в ID файл пользователя.

6.7.4.2 Создание Person документа, для клиентов интернет, с использованием SSL идентификации клиента.

В Domino Directory на Вашем Domino сервере, создайте Person документы для клиентов интернета, использующих идентификацию SSL, чтобы соединиться с Domino сервером. Person документ для клиента хранит публичный ключ клиента, который используется, чтобы проверить идентичность клиента интернет. Person документ также содержит список имен, который Domino сервер может использовать, чтобы идентифицировать клиента интернета. Когда клиент интернета пробует соединяться с сервером, Domino ищет имя, интернет сертификат в поле Person документа клиента. Domino сравнивает публичный ключ, представленный ему, с сохраненным в Person документе. Сравнение публичного ключа позволяет Domino подтверждать подлинность пользователя, даже если имеются несколько пользователей с тем же самым именем, так как каждый публичный ключ уникален. Если Domino находит совпадение и публичный ключ имеет силу, то первое имя, внесенное в список имени пользователя, используется, чтобы проверить ACL баз данных и списки доступа к модулям.

Например. Если Person документ пользователь в поле имени, содержит эти имена: Alan Jones, Ajones, Alan, Al Jones, а клиент использует имя Al Jones для доступа на сервер, Domino идентифицирует пользователя, проверяет публичный ключ представленный ему, с использованием публичного ключа из Person документа. Domino использует имя Alan Jones, чтобы проверить ACL баз данных и списки доступа к модулям.

Настройка Person документа.

*3076 Создайте новый Person документ в Domino Directory.

*3077 Введите в Ф. И. О. в соответствующие поля.

*3078 Введите в поле User Name имя пользователя, так как оно определено в сертификате.

*3079 (Необязательно) Вводят дополнительную информацию относительно клиента на закладках Work/Home

*3080 Сохраните документ.

Примечание, если клиент хочет использовать сертификат на Domino сервере в другом домене, Вы должны добавить Person документ в Domino Directory для этого домена. Убедитесь, что Вы создали и настроили базу данных Master Address Book (Directory Assistance), так что Domino может находить клиента в Domino Directory для этого домена.

6.7.4.3 Запрос интернет сертификата для SSL и S/MIME.

Прежде, чем интернет и клиенты Notes смогут использовать установление подлинности клиента или смогут посылать шифрованные сообщения или подписанную почту, используя при этом S/MIME, они должны иметь интернет сертификаты. Вы должны закончить эти шаги для интернет и клиентов Notes, чтобы создать новые публичный и личный ключи для интернет сертификата. Вы не должны делать этого, если Вы используете клиента Notes и сертификат CA в Person документе в Domino Directory. Notes автоматически добавляет интернет сертификаты, сохраняя в Person документе и Notes ID файле, когда пользователь идентифицирует с сервером.

Вы следуете этими шагами, чтобы запросить интернет сертификат.

Domino CA.

Вы используете Domino приложение Certificate Authority, чтобы получить интернет сертификат от Domino CA.

Если Вы требуете интернет сертификат для клиента интернет, Вы должны использовать или Netscape Navigator или IE Microsoft, чтобы получить сертификат от Domino Certificate Authority. Приложение автоматически обнаруживает, какой браузер Вы используете, и показывает соответствующие шаги.

1. Если Вы требуете интернет сертификат для клиента Notes, Вы должны использовать персональный Web Navigator.

2. Если Вы используете IE Microsoft, используете TCP/IP, чтобы соединить с Domino Certificate Authority. IE не позволяет Вам принимать сертификат сайта в Ваш браузер.

3. Если Вы используете Netscape, используете SSL, чтобы соединить с Domino Certificate Authority. Когда браузер спрашивает, хотите ли Вы принять сертификат сайта как Trusted Root, следуйте за предлагаемыми шагами, чтобы принять сертификат.

*3081 Рассмотрите приложение Domino Certificate Authority.

*3082 Выбирайте из левой панели Request Client Certificate.

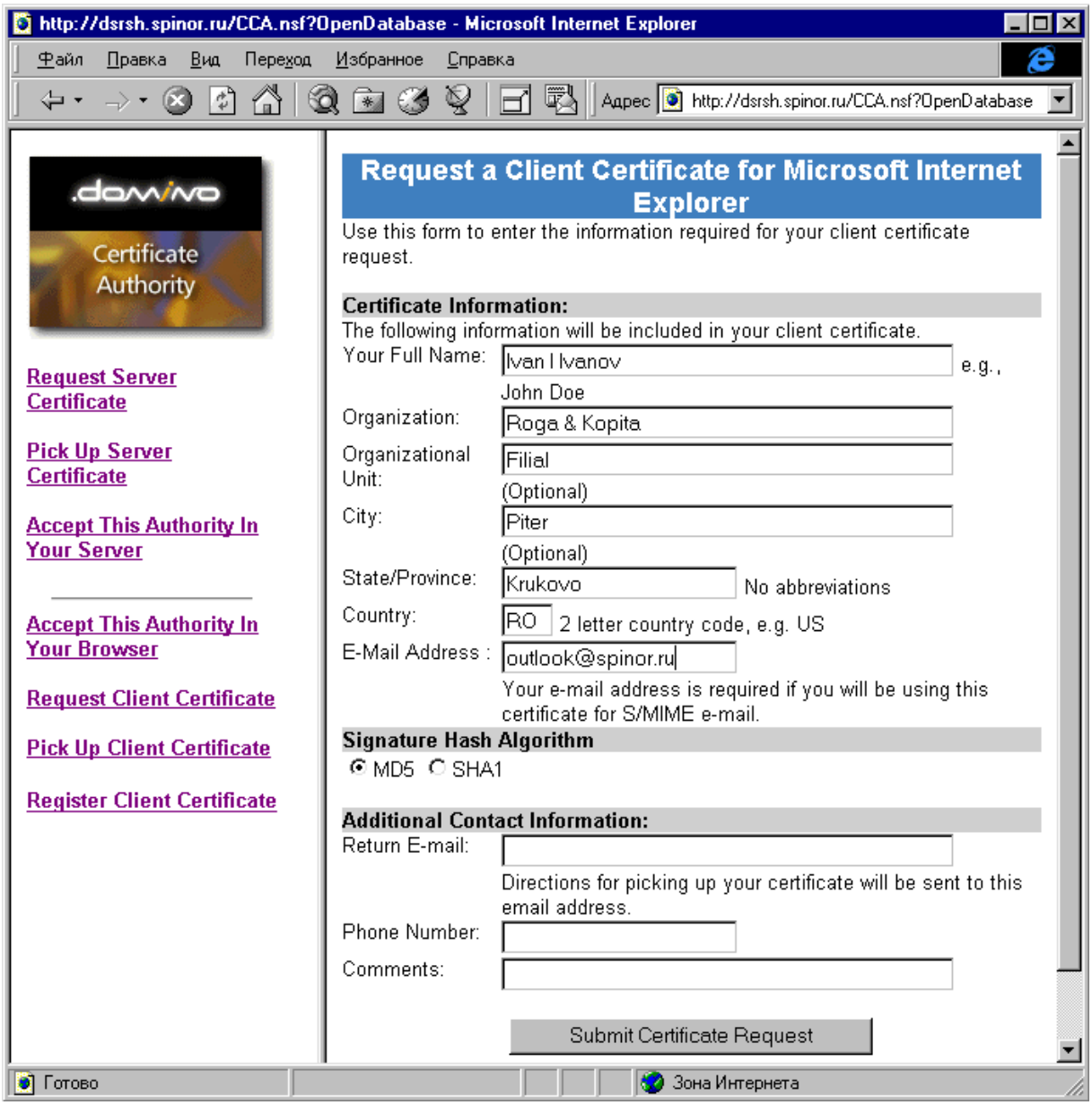


Рис. 111 Пример запроса сертификата от Domino CA.

*3083 Введите Ваше имя и информацию о Вашей организации. Эта информация будет отображаться в Вашем интернет сертификате.

*3084 Введите любую дополнительную информацию для контакта с Вами, которую Вы хотите послать CA.

*3085 Если Вы используете Netscape, введите размер для публичного и личного ключа. Чем больше число, тем более сильное шифрование.

*3086 Когда Вы заполните форму Submit Certificate Request, чтобы отослать запрос CA.

Производители CA третьих фирм.

Производители CA, на своих Web сайтах, как правило определяют как Вы должны запрашивать интернет сертификаты. Обратитесь на Web сервер производителя CA и введите запрос сертификата.

6.7.4.4 Подпись интернет сертификата и добавление сертификата в Domino Directory.

Когда CA подписывает интернет сертификат, CA добавляет цифровую подпись в сертификат, если Вы используете Domino CA, добавляет публичный ключ в Domino Directory. Если Вы используете производителя CA третьих фирм, Вы должны закончить дополнительные шаги, чтобы добавить публичный ключ в Domino Directory.

Вы не должны заканчивать эти шаги, если Вы используете клиента Notes и сертификат CA в Person документе, в Domino Directory. Notes автоматически добавляет интернет сертификат, сохраненный в Person документе в Notes ID файл, когда пользователь идентифицирует с сервером.

Вы следуете этими шагами, чтобы подписывать и добавить интернет сертификат в Domino Directory. Эти шаги различны и зависят от того, кем выпущен сертификат, от имени Domino CA или производителя CA третьих фирм.

Domino CA.

Запрос интернет сертификата появляется в представлении Client Certificate Requests, базы данных Domino Certificate Authority. Когда CA подписывает сертификат, CA может автоматически посылать электронную почту клиенту. Это почтовое сообщение описывает, где можно забрать сертификат, и включает в себя Pickup ID, который клиент должен использовать, чтобы идентифицировать сертификат в течение процесса Pickup. Domino автоматически генерирует – Pickup ID.

Обратите внимание, что шаги ниже предназначены для клиента, который подписывает сертификат, выпущенный - Domino CA. Эти шаги нужно выполнять администраторам Domino CA.

*3087 Удостоверитесь, что Вы как администратор, понимаете политику Вашей организации по выпуску и подписанию сертификатов. Вы должны подписывать сертификаты для клиентов только, если запросы на сертификат соответствуют политике безопасности Вашей организации.

*3088 Удостоверитесь, что Вы запустили процесс администрирования на сервере. Если Вы подписываете сертификат для клиента интернета, удостоверитесь, что Вы создали Person документ для него.

*3089 Из клиента Domino Administrator, выбирайте закладку Файлы, откройте приложение Domino Certificate Authority.

*3090 Выбирайте представление Client Certificate Requests.

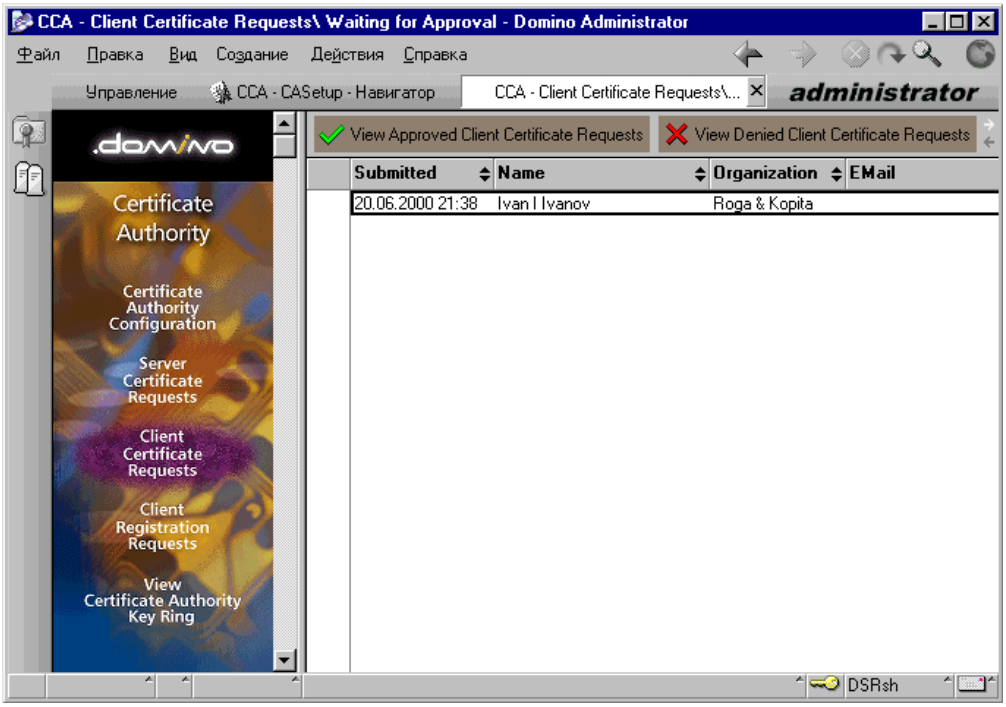


Рис. 112 Представление Domino CA приложения, для работы с запросами пользователей, на получение сертификата от Domino CA.

*3091 Открывайте запрос, который Вы хотите подписать.

*3092 Внимательно рассмотрите информацию пользователя и его имя. Удостоверитесь, что представленная информация, не противоречит политике безопасности Вашей организации.

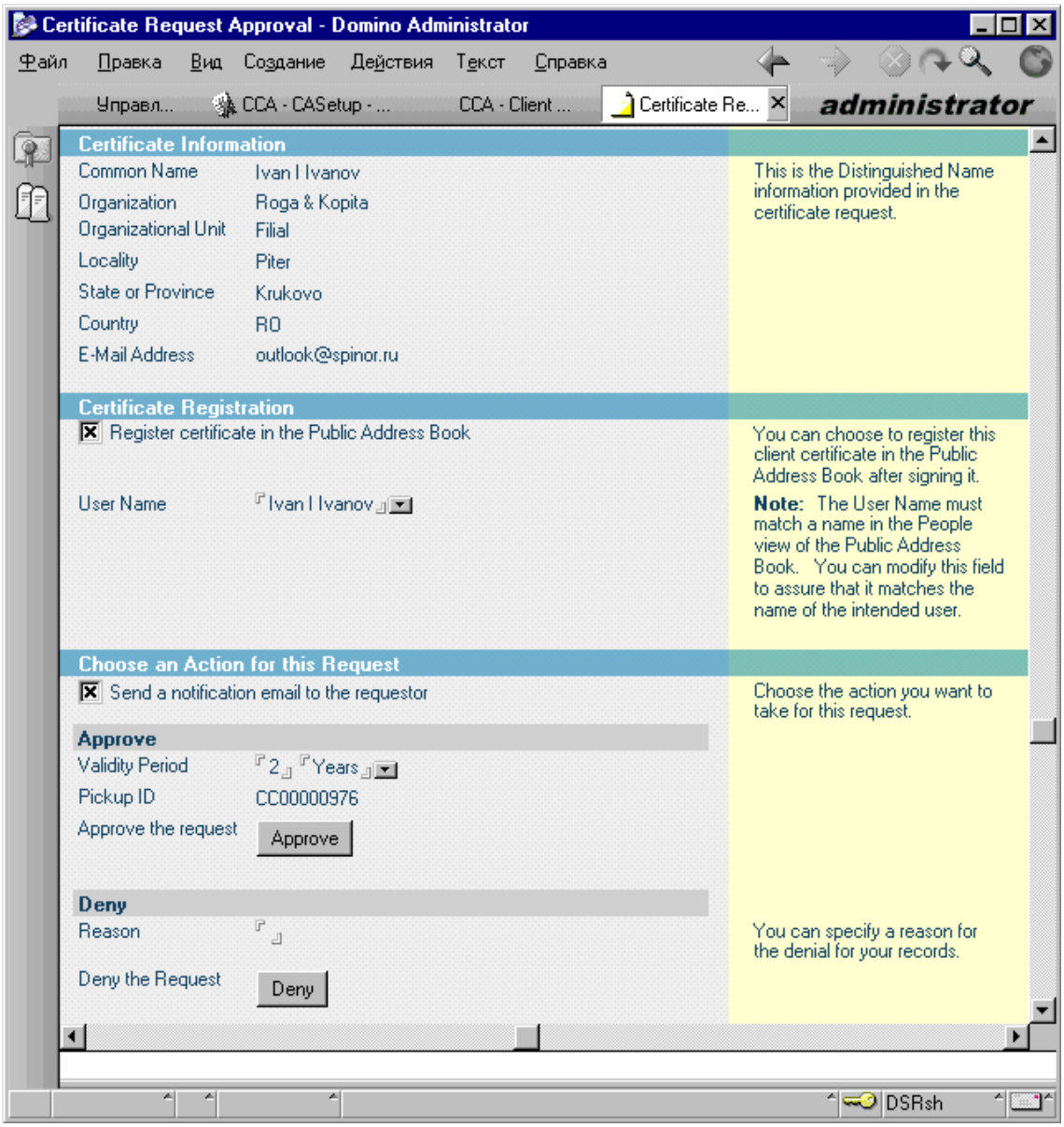


Рис. 113 Пример документа запроса сертификата.

*3093 Выбирайте опцию Register certificate in the Public Address Book, чтобы добавить публичный ключ клиента автоматически к Person документу.

*3094 Выполняйте следующие шаги, в зависимости от того, хотите ли Вы одобрять или отвергнуть запрос.

*3095 Запрос отвергается:

- Введите причину для отклоненного запроса.
- Если Вы не хотите послать электронную почту автору запроса, уберите пометку опции Send notification email to the requestor, иначе, пользователю посылается уведомление, что Вы отвергли запрос, который содержит причину отклонения запроса.
- Нажимайте кнопку Deny.

*3096 Чтобы одобрить запрос:

- Введите период действия сертификата. Для краткосрочных проектов - 90 дней, для продолжительных проектов Вы можете вводить несколько лет.

- Если Вы не хотите послать электронную почту автору запроса, уберите пометку опции Send notification email to the requestor, иначе, пользователю посылается уведомление, что Вы одобрили запрос. Письмо будет содержать URL, с указанием местоположения Вашего сертификата.

- Нажимайте клавишу Approve, вводите пароль для CA Key Ring. При выполнении этого действия, в базе данных Administration Requests будет размещен соответствующий запрос. Когда процесс администрирования будет запущен, и он обработает запрос, сертификат будет добавлен к Person документу клиента в Domino Directory.

Клиент не сможет использовать сертификат, для подтверждения подлинности в ACL базах данных, пока процесс администрирования не заканчивает свою работу.

Производитель CA третьих фирм.

После того, как пользователи получают интернет сертификат от производителя CA, они должны зарегистрировать сертификат в Domino CA. Клиент Notes должен использовать персональный Web Navigator, чтобы выполнить эти шаги.

*3097 Чтобы представить интернет сертификат в Domino CA, клиент заканчивает следующие шаги:

- При использовании SSL соединения, используйте браузер, чтобы открыть Domino приложение Certificate Authority.

- Выбирайте Register Client Certificate.

- Введите Ваше имя, адрес электронной почты, телефонный номер и любые комментарии. Эта информация появится в запросе, введенном в Domino приложении Certificate Authority.

- Нажмите кнопку Submit Certificate.

*3098 Чтобы добавить сертификат в Person документ, Domino CA администратор заканчивает следующие шаги:

- Из клиента Domino Administrator, выбирайте закладку Файлы, откройте приложение Domino Certificate Authority.

- Выбирайте представление Client Registration Requests

- Откройте документ запроса.

- Если Вы не хотите послать электронную почту клиенту, указав, что Вы отвергли или принимать запрос и причину, по которой Вы сделали это, уберите пометку опции - Send notification email to the requestor.

- Если Вы не хотите одобрять запрос, выбирайте – Reject, для отклонения запроса. Иначе, выбирайте Accept – OK. При выполнении этого действия, в базе данных Administration Requests будет размещен соответствующий запрос на сервере Domino CA. Когда процесс администрирования будет запущен, и он обработает запрос, сертификат будет добавлен к Person документу клиента в Domino Directory.

6.7.4.5 Как слить интернет сертификат.

Когда CA администратор одобряет запрос пользователя, пользователь сливает подписанный сертификат или в локальный файл, или в ID файл, если клиент - клиент Notes. Вы следуете этими шагами, чтобы слить интернет сертификат.

Вы не должны заканчивать эти шаги, если Вы используете клиента Notes и выпущенный CA сертификат в Person документе в Domino Directory. Notes автоматически добавляет интернет сертификат, сохраненный в Person документе в Notes ID файл, когда пользователь идентифицирует с сервером.

Клиент Notes должен использовать персональный Web Navigator, чтобы слить интернет сертификат в ID файл. Клиент интернета может использовать любой доступный браузер.

Domino CA.

*3099 Если CA выдал Вам URL, чтобы использовать его для приобретения сертификата в Domino приложении Certificate Authority, открывайте его в том же самом браузере, в котором Вы запрашивали сертификат. Просмотрите URL страницу.

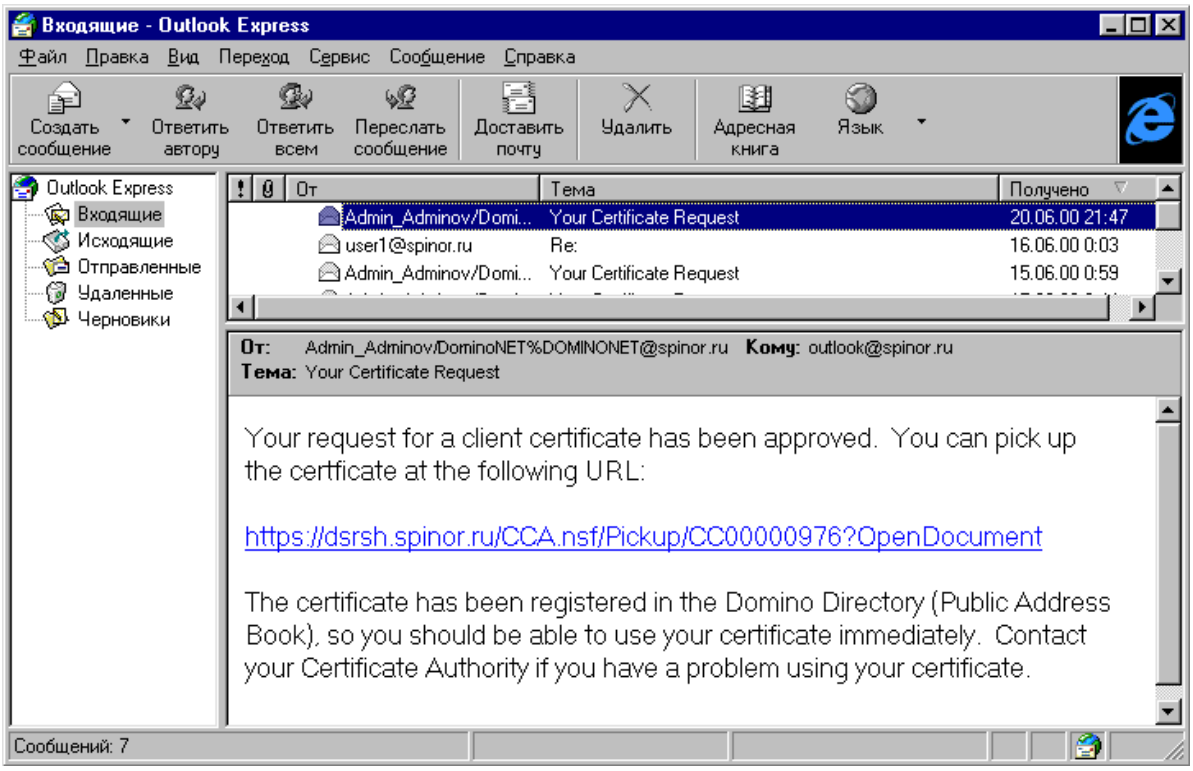


Рис. 114 Пример уведомления о выдаче сертификата полученного по почте, с указанием места нахождения (URL) сертификата.

*3100 Если необходимо, получите Pickup ID от производителя CA, и делайте следующее:

- Выбирайте Pick Up Client Certificate.
- Введите в значение Pickup ID, в поле и нажмите Pick Up Signed Certificate

*3101 Просмотрите информацию о Вашем сертификате и нажмите, Accept Certificate. Следуйте указаниям программного обеспечения Вашего браузера.

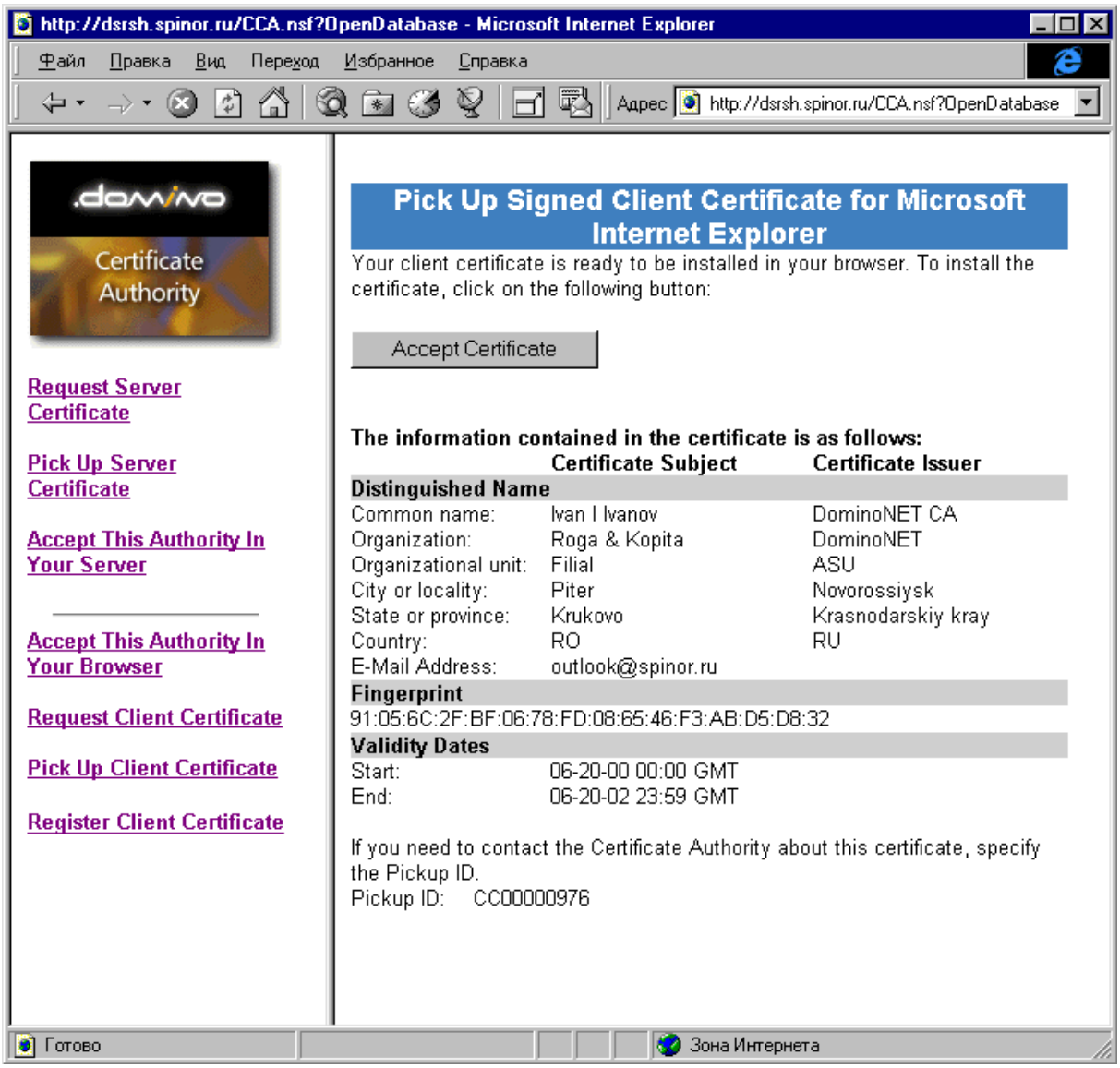


Рис. 115 Просмотр и принятие сертификата от Domino CA.

Независимые производители CA.

Производитель CA определяет сам, как Вы должны слить интернет сертификат. Просматривайте сайт производителя CA, и следуйте за инструкциями, предусмотренными, слива интернет сертификата.

6.7.5 Установка SSL для Notes или Domino с использованием SMTP.

Клиент Notes или Domino сервер может действовать как SMTP клиент, когда он отправляет почту на SMTP сервер. Клиент Notes или Domino сервер может использовать SSL, чтобы соединить с Domino сервером, со службой SMTP, или другим типом SMTP сервера. Вы не можете настраивать клиента Notes или Domino сервер, для SSL идентификации клиента, при соединении с использованием SMTP.

Если Вы не имеете сертификата CA сервера, отмеченного как Trusted Root в файле сервера Key Ring, для Вашего Domino сервера, Domino автоматически добавляет сертификат и регистрирует это в файле LOG.NSF. Другие протоколы интернета не позволяют пользователям доступ, если они не имеют сертификата CA сервера, отмеченного как

Trusted Root. Однако Вы должны помечать сертификаты CA как Trusted Root вручную, чтобы гарантировать, что добавленные сертификаты Trusted Root, имеет силу.

Установки SSL для Domino сервера, маршрутизирующего почту на SMTP сервера.

*3102 Из клиента Domino Administrator, выбирайте закладку Настройка, откройте Server документ.

*3103 Выбирайте Ports – Internet Ports – Mail.

*3104 В секции - SMTP Outbound, выбирайте значение - Disabled, в поле TCP/IP port status.

Обратите внимание. Если Вы не выбираете значение Disabled, в поле TCP/IP port status, Domino всегда будет соединяется с серверами SMTP, без использования SSL.

*3105 В секции SMTP Outbound, выбирайте значение – Enabled, в поле SSL port status

*3106 Сохраните и закройте документ.

*3107 Добавляйте сертификаты CA Trusted Root, для SMTP серверов.

6.7.6 Использование SSL с Directory Assistance, для LDAP Directory.

Directory Assistance позволяет Вам расширить поиск пользователей в Вашей системе. Вы можете включить в поиск, не только пользователей из первичного Domino Directory, но и пользователей, которые размещены во вторичных Domino Directory и LDAP Directory. Чтобы установить Directory Assistance, Вы создаете базу данных из шаблона DA50.NTF. Эта база данных позволяет Вам создавать документы, которые определяют каталоги пользователей для Вашего домена.

При использовании Directory Assistance для LDAP Directory, Вы можете указать серверу - использовать SSL, при соединении с LDAP серверами. Это позволит защитить коммуникации между Вашим сервером и другим LDAP сервером. Мы рекомендуем, использовать SSL, если Ваша LDAP служба, идентифицирует Web браузеров клиентов.

Когда Domino сервер соединяется с неизвестным LDAP сервером с использованием SSL, оба сервера должны иметь взаимные сертификаты, которым сервера доверяют. Если дело обстоит не так, Вы должны добавить Trusted Root сертификат Key Ring в файл сервера прежде, чем Ваш сервер сможет соединяться с LDAP сервером.

6.7.7 Просмотр и удаление интернет сертификатов.

Когда Вы больше не хотите давать интернет пользователям доступ к Domino серверу с использованием SSL установление подлинности сервера или клиент Notes, чтобы послать S/MIME шифрованную почту, указанному получателю, удаляете публичный ключ сертификата из клиентских интернет сертификатов, Person документов в Domino Directory. Клиент все еще будет иметь интернет сертификат, но без публичного ключа в Person документе, клиент не может использовать установление подлинности для доступа на Domino сервер. Клиент Notes не может посылать S/MIME шифрованную почту указанному получателю. Клиенты интернета могут все еще получить доступ на Domino сервер - анонимно, если Вы имеете анонимный доступ на сервере. Клиент Notes сможет посылать не шифрованные сообщения пользователям.

Вы можете также просматривать информацию о интернет сертификате из Domino Directory.

*3108 Из клиента Domino Administrator, выбирайте закладку Пользователи и группы, затем Person документ для просмотра интернет сертификата, который Вы хотите просмотреть или удалить.

*3109 Выбирайте из панели акций, открытого для редактирования документа, кнопку Examine интернет Certificate(s).

*3110 Если Вы хотите удалить интернет сертификат, выберите сертификат и нажмите – Delete.

7 Проблемы ошибки, возникающие при работе Domino систем, их решения.

Даже при осторожном обслуживании серверов, Вы можете иногда сталкиваться с неожиданными проблемами в системе. Эта глава описывает методы поиска неисправностей и предлагает способы решений общих (обычных) проблем. Вы можете использовать для поиска общих неисправностей. Lotus имеет Web сервер Customer Support, который может помочь Вам в поиске неисправностей.

```
http://www.lotus.support.com
```

7.1.1 Инструменты для диагностики и решения проблем.

Domino обеспечивает Вас несколькими инструментами, чтобы помочь Вам в решении проблем. Большинство инструментов доступно из клиента Domino Administrator. Таблица ниже суммирует доступные инструменты и указывает когда каждый из них полезен.

Если Вы не решили возникшую проблему после просмотра данной секции, попытайтесь найти решение на Lotus Web Customer Support сервере.

Инструмент	**Проблемы, при которых можно использовать этот инструмент**	**Как получить доступ к инструменту**
LOG.NSF – файл протокола сервера	Все проблемы	С закладки Сервер – Анализ, из Domino Administrator
Файл протокола Web сервера Domino (DOMLOG.NSF)	Проблемы с Web сервером	С закладки Сервер – Анализ, из Domino Administrator
Серверная база данных MAIL.BOX	Проблемы с маршрутизацией почты	С закладки Почта - Почта, из Domino Administrator
Трассировка почты	Проблемы с маршрутизацией почты	С закладки Почта - Почта, из Domino Administrator
Ispy	Незначительные проблемы с передачей почты. Проблемы с сервером	Конфигурируется из баз данных Statistics and Events, с закладки Настройка, из Domino Administrator
Отчеты о почте	Проблемы с активностью пользователей	С закладки Почта - Почта, из Domino Administrator
Отслеживание сообщений	Потерянная почта	С закладки Почта – Трассировка, из Domino Administrator
Статус маршрутизации почты	Не доставленная почта	С закладки Почта - Почта, из Domino Administrator

Карта топологии маршрутизации почты	Проблемы с маршрутизацией почты между серверами	С закладки Почта - Почта, из Domino Administrator
События Mail routing events из файла протоколов (LOG.NSF)	Не доставленная почта	С закладки Почта - Почта, из Domino Administrator
События “Shared Mail” из файла протоколов (LOG.NSF)	Использование дискового пространства	С закладки Почта - Почта, из Domino Administrator
Трассировка сети	Проблемы с подключениями	Установки пользователя. Выбирайте из меню Файл – Параметры – Параметры настройки – Порты – Трассировка
События репликаций в файле протоколов (LOG.NSF)	Проблемы с репликациями для Particular серверов	С закладки Репликация, из Domino Administrator
История репликации	Проблемы с репликациями для некоторых баз данных	Свойства базы данных. Выбирайте из меню Файл – База данных – Свойства, или выбирайте Файл – Репликация – Журнал
Расписание репликаций	Проблемы с репликациями для Particular серверов	С закладки Репликация, из Domino Administrator
Карта топологий репликаций	Проблемы с репликациями между серверами	С закладки Репликация, из Domino Administrator
Статистика и события	Статистика и события сервера	Конфигурируется с закладки Настройка, из Domino Administrator. Представление Анализ с закладки Сервер – Анализ, из Domino Administrator
База данных Analysis	Проблемы с базами данных	С закладки Файлы, из Domino Administrator
База данных Administration Requests	Ошибки Administration Process	С закладки Сервер – Анализ, из Domino Administrator
Команды сервера	…	С закладки Сервер – Статус, из Domino Administrator

7.1.2 Использование русских букв в Notes.

7.1.2.1 Использование в Lotus Notes однобайтовой и двухбайтовой кодировок.

В Lotus Notes может храниться любая информация полях типа RichText. При использовании текстовой информации используется кодировка LMBCS. При этом один символ кодируется несколькими байтами: английские буквы - одним байтом, русские - двумя, китайские, японские, корейские - тремя... Внутри базы допускаются тексты, в которых рядом находятся и английская буква, и русская буква, и японский иероглиф. При выводе текстовой информации из баз на экран происходит перекодирование ее из LMBCS в кодировку, поддерживаемую машиной (native). Перекодировка ведется по таблицам .cls. При этом не на всех платформах такое преобразование может работать. Если какой-то символ из текста в базе по текущей таблице перекодировки не может быть сопоставлен символу в кодировке машины, он будет виден на экране на Windows-платформах как что-то среднее между мягким знаком и буквой Б, а в OS/2 - в виде полностью закрашенного квадрата.

Notes использует в качестве таблиц перекодировки файлы l_cpdos.cls, l_cpwin.cls - только Windows-подобные платформы, для сортировки - collstd.cls.

Lotus приняла соглашение о двухбайтовой кодировке русских букв только после того, как Notes стали применять в России. При установке английского клиента или сервера, символы с кодами от 128 до 255 по умолчанию соответствуют греческим буквам (такими их считает Notes), и Notes сортирует их по-гречески, но за счет русификатора и фонтов рисуются на экране как русские буквы.

В то время и другого то варианта не было, как установить продукт и выполнить копирование следующих файлов кодировки и сортировки. Файлы последней строки используется для правильного экспорта из Notes:

copy l_cp437.cls l_cpdos.cls

copy l_cp1252.cls l_cpwin.cls

copy collus.cls collstd.cls

copy l_cp1251.cls в l_cp1252.cls

При установке русского клиента копирование этих файлов происходит автоматически и Вам не нужно выполнять эту процедуру.

“В природе” известны также Киевские кодировки. При их использовании русские буквы в двухбайтовой кодировке и русские буквы в однобайтовой кодировке рустуются на экране нормально, но новая информация в базу пишется в двухбайтовой кодировке.

7.1.2.2 Русские буквы на консоли Domino Administrator.

Для правильного отображения русских букв на консоли Domino Administrator, на Windows платформе, помогает изменение строк в секции [FONTS] из WIN.INI:

```
Terminal,0=MS Sans Serif,204

Terminal=MS Sans Serif,204
```

7.1.3 Проблемы с процессом администрирования.

*3111 Как искать проблемы связанные с процессом администрирования. Эти шаги предназначены для поиска неисправностей процесса администрирования, когда он запущен.

*3112 Проблемы и сообщения об ошибках. Сообщения, которые появляются в протоколе сертификации Certification Log, или на консоли сервера.

7.1.3.1 Как искать проблемы связанные с процессом администрирования.

Разнообразные условия и ошибки могут мешать процессу администрирования функционировать должным образом. Например, ошибки могут происходить, когда имеется недостаточное количество памяти, или когда Вы переименовываете, удаляете, или повторно сертифицируете пользователя, перемещаете пользователя в различные иерархические организации. Используйте эти шаги для разрешения проблем с процессом администрирования.

*3113 Процесс администрирования запускается на сервере, который нет реплики Domino Directory

*3114 Удостоверьтесь, что процесс администрирования правильно установлен.

*3115 Если процесс администрирования работал ранее успешно, но не работает, как ожидается теперь, попытайтесь выявить, что могло быт, изменено в системе.

*3116 Проверьте эти условия и исправьте их если необходимо:

- Процесс администрирования, задача Adminp должна быть запущена на всех серверах. Чтобы проверять это, введите команду Sh Ta на консоли сервера.
- Сервер администрирования должен быть определен для Domino Directory. Чтобы сделать это, выберите из меню Файл – База данных – Управление доступом – Дополнительно.
- Удостоверитесь, что Вы определили сервер администрирования для всех баз данных. Каждая база данных должна иметь сервер администрирования прежде, чем запрос может быть сделан в процессе администрирования.
- Domino Directory (NAMES.NSF) и база данных запросов администрирования (ADMIN4.NSF) должна реплицироваться должным образом между серверами.
- Каждый запрос в базе запросов администрирования, должен содержать соответствующий документ ответа, который показывает, что процесс администрирования обработал запрос. Исправьте любые ошибки, обозначенные в документе ответа.
- Документы сертификатов должны иметь правильный публичный ключ; публичный ключ должен соответствовать ключу в каждом CERT.ID.

7.1.3.2 Process Administration – проблемы и сообщения об ошибках.

Эти ошибки могут появиться в базе Certification Log, или на консоли сервера. Некоторые из этих сообщений требуют, чтобы Вы исправили некоторое состояние, в то время как другие - только статусные сообщения.

Administration Process: retrying a request that could not be performed previously because another process was modifying the document. Сообщение указывает, что в процессе обработки отдельных запросов, две нити процесса администрирования одновременно попытались изменять документ в Domino Directory. В результате, процесс администрирования повторяет один из запросов. Это статусное сообщение и никаких действий не требуется.

Administration Process: Unable to access transfer context information. Сообщение указывает, что процесс администрирования не может получить доступ к глобальной информация, которая требуется для выполнения определенной задачи. Повторно запустите процесс администрирования, или если необходимо перезапустите сервер.

Administration Process: Unable to create entry thread. Сообщение появляется, когда процесс администрирования не может создать нить, для использования и управления задачами процесса администрирования. Повторно запустите процесс администрирования, или если необходимо перезапустите сервер.

Insufficient memory - Admin's request queue pool is full. Сообщение указывает, что не хватает памяти для процесса администрирования. Повторно перезапустите сервер.

No Address book is present on this server; the Admin Process cannot continue without one. Сообщение появляется, когда Вы запускаете процесс администрирования на сервере, который не имеет реплики Domino Directory. Создайте реплику Domino Directory на сервере и затем перезапустите процесс администрирования.

Removing *viewname* view notes in the Address Book. Сообщение появляется, когда процесс администрирования удаляет Obsolete Statistics и Events Monitoring документы из Domino Directory. Это статусное сообщение, и никаких действий не требуется.

Reporter: Could not locate view *viewname*. Сообщение появляется, когда процесс администрирования не может найти документы Obsolete Statistics и Events Monitoring в Domino Directory. Это – статусное сообщение и никакое действие не требуется.

The Administration Process cannot delete the database *databasename* at this time because it is in use by someone else; will try again at *time*. Сообщение появляется как результат удаляющего несвязанного запроса для почтового файла. Сообщение указывает, что процесс администрирования повторяет запрос, чтобы удалить почтовый файл, который был первоначально недоступен, потому что кто-то обращался к нему. Это статусное сообщение и никакое действие не требуется.

The Administration Process could not change or delete the name from the document because another process was modifying it. Сообщение указывает на то, что при обработке удаляющего или переименовывающего запроса, две нити процесса администрирования попытались изменять тот же самый документ в базе данных. В результате, только один запрос был обработан и процесс администрирования повторяет запрос. Это статусное сообщение и никакого действия не требуется.

The Administration Process does not have enough memory to compute the formulas required for request processing. Сообщение указывает на то, что недостаточно памяти для процесса администрирования. Чтобы исправлять это, повторно запустите сервер.

The Administration Process is retrying a name change or deletion from the document. Сообщение появляется как результат переименовывающего или удаляющего запроса. Это указывает, что процесс администрирования повторяет запрос, чтобы переименовывать или удалить имя из документа, который был первоначально, недоступен, потому, что, кто-то обращался к документу. Это статусное сообщение и никакого действия не требуется.

The certificate contained in the note was not issued by the selected certifier. Сообщение появляется, если требуется Ваше подтверждение действия. Выбирайте - Действия – Recertify Select People, или Действия - Recertify Select Server, но Вы не выбираете первоначальный сертификат. Если Вы не определяете первоначальный сертификат, когда выбираете это действие, Вы можете выполнить запрос, но он не будет отправлен по почте в базу данных процесса администрирования. Чтобы исправить это, выбирайте это действие снова и выбирайте первоначальный сертификат.

The replica of the *database* moved by the Administration Process has not been initialized by the replicator. Сообщение появляется как результат мониторинга, перемещения запроса реплики. Это указывает, что процесс администрирования ожидает, пока Replicator не инициализировал реплику на новом сервере или местоположении прежде, чем будет удален оригинал базы. Это статусное сообщение и никакое действие не требуется.

The selected certifier isn't an ancestor of the entity to be updated. Сообщение появляется, когда Вы пытаетесь выбирать - Действия – Request Move to new Certifier, чтобы переместить пользователя в другую иерархию, но Вы не выбрали первоначальный сертификат. Если Вы не определяете первоначальный сертификат, Вы можете генерировать запрос, но он не будет отправлен по почте в базу данных администрирования. Чтобы исправлять это, выбирайте повторно действие Request Move to New Certifier и определите сертификат.

The selected certifier isn't the target certifier in the move request. Сообщение появляется, когда Вы выбираете - Действия – Complete move for selected entries, чтобы сделать попытку перемещения имен пользователей в различные иерархии и выбран не тот сертификат, что Вы определяли. Если сертификат, который Вы определили при завершении перемещения неправильный, выбирайте имя пользователя в представлении запросов администрирования и выбирайте - Действия – Complete move for selected entries снова, при этом определите правильный сертификат.

7.2 Проблемы с агентами и Agent Manager.

*3117 Инструменты, применяемые при проблемах с агентами и Agent Manager. Описываются инструменты, которые Вы можете использовать для локализации проблем с менеджером агентов и агентами.

*3118 Agent manager и агенты. Описывает проблемы, которые могут происходить, когда менеджер агентов или агент не работает, как Вы ожидаете.

7.2.1 Инструменты, применяемые при проблемах с агентами и Agent Manager.

Всякий раз, когда агент не будет запускаться, проверьте Agent Log, чтобы просмотреть, когда агент последний раз запускался и завершился ли он. Для дополнительной информации, проверьте консоль сервера или строки Miscellaneous events, в файле протоколов LOG.NSF, на наличие сообщений от менеджера агента.

Команды сервера.

Используйте эти команды сервера при проблемах с агентами:

```
Tell amgr schedule

Tell amgr status

Tell amgr debug
```

Файл протокола (Log file).

Чтобы позволять протоколирование агентов в файл протоколов LOG.NSF, отредактируйте NOTES.INI файл, чтобы включить переменную в него переменную Log_AgentManager. Перемененная определяет, будет ли регистрироваться или нет начало выполнения агентов в файле протоколов и будет ли показывается на консоли сервера, события выполнения агентов.

Протоколы агентов (Agent Log).

Agent Log - представление в базах данных, которая показывает последний запуск агента и описывает, выполнился ли агент или нет.

*3119 В базе данных, выбирайте представление Агенты.

*3120 В представлении, которое содержит список всех агентов, выбирают нужного агента.

*3121 Выбирайте опцию - Агент – Журнал.

7.2.2 Agent manager и агенты – проблемы и сообщения об ошибках.

Эти темы содержат предложения для поиска неисправностей, если возникают проблемы с менеджером агентов и или агентами:

*3122 Agent Manager не работает, как ожидалось

*3123 Агент не запускается, как ожидалось

*3124 Агент запускается, но не завершает свою работу

*3125 Агент не запускается в назначенное время

*3126 Escrow agent не работает

*3127 Пользователь не может создать агента

7.2.2.1 Agent Manager не работает, как ожидалось.

Менеджер агентов не может работать эффективно.

*3128 Менеджер агентов не может быть намечен для запуска. Если менеджер агентов не запустится, проверьте поле Start time/End time в секции Server Task – Agent Manager, Server документа. Если время не указанно в этом поле – менеджер агентов трактует его как время простоя. Если необходимо, откорректируйте время.

*3129 Требования системных ресурсов для менеджера агентов может быть слишком высоко. Если менеджер агентов работает слишком долго, чтобы управлять агентами, перенесите запуск агентов на ночь, когда требование к системным ресурсам, обычно низкое.

Если Ваш Сервер Domino 4.6 или ранее, Вы можете увеличивать значение поля Max % busy before delay в Server документе. Domino R5 не поддерживает это поле.

Примечание. Обратите внимание, если Вы выделяете большое количество ресурсов менеджеру агентов, количество ресурсов доступное другими задачам сервера уменьшается.

7.2.2.2 Агент не запускается, как ожидалось.

Если имеются ошибки в коде агента, агент может не работать должным образом. Агент может не иметь достаточного доступа, или потому что агент не настроен для запуска на данном Сервере.

*3130 Недостаточный доступ в базе данных ACL может нарушить работу агента должным образом. Например, пользователь может создать агента, который копирует выбранные документы из базы данных. Если пользователь и агент - не имеет доступ автора в ACL базы данных, агент запустится, но не будет копировать документы. Чтобы определять, существует ли проблема, просмотрите в журнале ошибки доступа, после запуска агента.

*3131 Если агент не будет запускаться на выбранном сервере, проверьте ограничения агента на закладке безопасности, Server документа. Эта секция содержит поля Run personal agents, Run restricted LotusScript/Java agents, Run unrestricted LotusScript/Java agents, которые определяют, кто имеет доступ для запуска агентов на сервере. Хотя пользователь и имеет соответствующий доступ в базе данных ACL, он может быть не способен создавать агентов на сервере, без соответствующего доступа в Server документе.

Вы должны также проверить секцию доступа сервера, на закладке безопасности Server документа. Эта секция содержит поля Only allow server access to users listed in this Directory, Access server, Not access server, которые разрешают или запрещают доступ к серверу. Агент наследует привилегии доступа пользователя, который создает агента и не может запускаться на сервере, для которого создатель не имеет доступа.

*3132 Конфликты по времени могут останавливать агента. В Server документе щелкните на закладке Server Tasks – Agent Manager и проверьте поля Daytime Parameters Start time/End time и Nighttime Parameters Start time/End time. Если не указанно время в этих полях – сервер трактует это как время простоя. Если пользователь создает агента и определяет, что он должен запускаться во время простоя менеджера агентов, агент не будет запущен. Сравните поля в Server документа и время, на которое агент намечен для запуска. Если конфликт существует, измените, график менеджера агентов на сервере, или просите пользователя перенести время выполнения агента.

*3133 Если LotusScript или агент Java не завершается нормально, проверьте поле Max LotusScript/Java execution time в Server документе. Если сложный агент требует большего количества времени, чем было намечено, менеджер агентов завершает агента перед завершением.

Просите пользователя перенести агента на ночь, когда период времени боле длителен, или увеличьте значение поля Max LotusScript/Java execution time в Server документе. Если ни одно из этих решений не приемлемо, просите пользователя, чтобы он заменил один агент несколькими, но менее длинными по времени выполнения.

7.2.2.3 Агент запускается, но не завершает свою работу.

Когда агент запускается, но не завершает свою работу, проверьте проток сервера (LOG.NSF), консоль сервера и журнал агента, для поиска сообщений ошибок.

*3134 Если агент запускается вручную, но не запускается, когда Вы пытаетесь его запустить в фоновом режиме, проверьте код агента. Агент может содержать команды – LotusScript, методы интерфейса пользователя, которые не предназначены для запуска в фоновом режиме.

*3135 Поле Max LotusScript/Java execution time, Server документа определите время, за которое агент LotusScript/Java должно закончить свое выполнение. Если агент превышает

этот максимум, агент не завершает свою работу и делает запись в журнале агента. Просмотрите код агента, чтобы удостовериться, что он функционирует правильно. Пример. Удостоверьтесь, что код не содержит бесконечной петли. Если код правилен, просмотрите время работы агента в Server документе.

7.2.2.4 Агент не запускается в назначенное время.

Если агент запускается, но не в то время, на которое Вы его определили, возможно, что сервер может быть занят другими задачами. Чтобы собраться, информация относительно того, когда агент последний раз запустился, проверьте журнал агента. После чего проверьте эти условия состояния и исправьте их, если необходимо.

*3136 Конфликты по времени запуска могут повлиять на запуск агента. В Server документе, щелкните на закладке Server Tasks – Agent Manager и проверьте поля Nighttime Parameters Start time/End time и Daytime Parameters Start time/End time. Если значения этих полей не содержать период Вашего рабочего дня, менеджер агентов не будет запускаться в течение этого периода. Например, если дневные параметры - 8 AM и 5 PM, и ночные параметры - 8 PM и 8 AM, менеджер агентов не будет запускать никакие агенты между 5 PM и 8 PM.

*3137 Назначения могут быть неправильны в файле NOTES.INI. Проверьте значения переменных менеджера агента в NOTES.INI файле:

- Amgr_DocUpdateAgentMinInterval
- Amgr_DocUpdateEventDelay
- Amgr_NewMailAgentMinInterval
- Amgr_NewMailEventDelay

*3138 Редактируйте файл NOTES.INI, чтобы включить переменную Log_AgentManager=1. Вы можете также позволять это установку в документе конфигурации для серверов из Domino Directory.

Для серверов под управлением Domino 4.6 или ранее, установка Max % busy before delay, возможно превышена. Установка Max % busy before delay управляет максимальным процентом от времени менеджер агентов, затраченного на управление агентами. Если процент от времени превышен, задержка происходит прежде, чем менеджер агентов запускает следующий агент. После падения процента ниже порога, менеджер агентов возобновляет запуск агентов.

7.2.2.5 Escrow агент не работает.

Escrow агент не будет работать если:

*3139 Не имеется никакого Person документа, содержащего фразы Escrow агента в поле User Name.

*3140 Больше чем один Person документ содержат фразы Escrow Agent в поле User Name.

*3141 Escrow агент пытается посылать зашифрованную почту получателю, чей Person документ не содержит публичный ключ.

7.2.2.6 Пользователь не может создать агента.

Если пользователь не может создавать агентов, в некоторой базе данных, проверьте ACL базы данных, чтобы убедиться имеет ли пользователь, требуемый уровень доступа на создание агентов в этой базе данных. Чтобы создавать персональных агентов, пользователь должен иметь, по крайней мере, доступ читателя к базе данных, в которой агент будет создан. Чтобы создавать общие агенты, пользователь должен иметь, по крайней мере, доступ дизайнера.

7.3 Продлеммы с Domino Directories, Directory Catalog, Directory Assistance.

Эти темы описывают, как локализовать проблемам, связанным с использованием Directory Catalog, Directory Assistance и службы LDAP. Вы можете также искать решения общих проблем на Customer Support Lotus Web сервере.

7.3.1 Directory Assistance – проблемы и сообщения об ошибках.

Searches in a secondary Domino Directory configured in directory assistance fail. Удостоверитесь, что поле Domain Name, документа Directory Assistance для вторичного Domino Directory, отличается от первичного Domino Directory, или любых других Domino Directory, сконфигурированных в Directory Assistance. Если поле Domain Name, указанный для вторичного Domino Directory не будет уникально, поиск во вторичном Domino Directory закончится неудачей и Вы получите сообщение - User *xxx* not found in any Name and Address Book. Если вторичный каталог не связан с Notes доменом, убедитесь что ввели уникальное имя домена, которое отличается от первичного домена сервера, на котором хранится вторичный каталог.

Directory assistance could not access Public Address Book on Server x, error is Server Not Responding. Когда Вы повторно запускаете сервер, который использует Directory Assistance, сервер делает попытку доступа к репликам вторичных Domino Directory, которые указаны как связи (links) с базами данных в Directory Assistance, чтобы можно их загружать в память. Если сервер не может достигнуть реплик, это сообщение появляется на консоли сервера. Чтобы избегать этой проблемы, в документах Directory Assistance, вводите в имена серверов и название файлов для реплик. Избегайте указания связей (links) с базами данных реплик. Это сообщение может появиться, когда сервер использующий Directory Assistance, пытается посмотреть имя во вторичном Domino Directory, на недоступном в данный момент сервере. Как механизм борьбы, Вы можете определить больше чем одну реплику вторичного Directory для Directory Assistance.

7.3.2 Directory catalog – проблемы и сообщения об ошибках.

Эти темы описывают проблемы, с которыми Вы можете сталкиваться при работе с Directory catalog

Имя отсутствует в Directory catalog.

Если окажется, что имена отсутствуют в Directory catalog, удостоверьтесь, что задача DirCat строит Directories, как ей было назначено.

*3142 Откройте исходный Directory catalog.

*3143 Выбирайте документ Configuration, затем - Файл – Свойства Документа.

*3144 Щелкает на закладке Поля, вторая закладка свойств.

*3145 Выбирайте поле Directories. Проверите, что задача DirCat может иметь доступ ко всем Directories, указанным в окне. Типично, это означает что сервер, который хранит исходный Directory catalog также, хранит реплики всех Directories.

*3146 Выбирайте поле Since, чтобы видеть дату и время когда задача DirCat последний раз запускалась на всех Directories, указанных в поле Directories. Если любое из следующего имеет место, запустите Dircat задачу снова:

- Если имеется меньшее количество отметок время/дата чем фактических Directories - например, если имеется четыре Directories в поле Directories, но только две отметки время/дата имеются – для задачи DirCat и она попыталось получить доступ к исходному Directory catalog, но потерпела неудачу.

- Если отметки время/дата старше, чем ожидается - задача DirCat возможно еще не завершилась для модернизации исходного Directory catalog.

*3147 Если вышеупомянутые шаги не решают, проблему, редактируйте файл NOTES.INI, чтобы включить установку Log_Dircat=1, которая будет протоколировать информацию задачи DirCat в файл LOG.NSF. Вы можете использовать эту информацию для решения проблемы.

Domino не может найти реплику Directory catalog на сервере.

Чтобы искать информацию в Directory catalog, сервер должен хранить реплику Directory catalog. Кроме того, Public Directory Profile в первичном Domino Directory сервера должен определять имя файла для Directory catalog. Все реплики Directory catalog на серверах в одном домене должны использовать то же самое имя файла.

Исходный Directory catalog больше по размеру, чем его реплики.

Когда задача DirCat запущенна по исходному Directory catalog, она строит дополнительное скрытое представление, которое содержит информацию Identifying, относительно конфигурации Directories в каталоге. Когда Вы создаете реплику исходного Directory catalog на сервере или когда пользователь создает локальную реплику исходного Directory catalog, реплика не содержит это дополнительное представления, поэтому реплики всегда меньше чем исходный Directory catalog.

7.3.3 LDAP service – проблемы и сообщения об ошибках.

Эти темы описывают проблемы, с которыми Вы можете сталкиваться с LDAP службой:

Слишком медленный поиск LDAP.

Если поиск LDAP медлен, сделайте следующее для первичной реплики Domino Directory. Если Вы осуществляете поиск LDAP во вторичных Domino Directories, сделайте следующее на каждой реплике вторичного Domino Directory.

*3148 Создает полнотекстовый индекс для Domino Directory.

*3149 Выбирайте LDAP выбор конфигурации Optimize LDAP queries в документе Configuration Settings, чтобы создать представления, которые улучшают выполнение поиска.

*3150 После того как Вы заканчиваете шаги, перечисленные выше, просмотрите значения LDAP полей конфигурации:

- **Maximum number of entries returned** - ограничивает число записей, которые LDAP сервер может возвращать. По умолчанию не имеется никакого предела, но Вы могли бы установить предел 100 записей, например.

- **Timeout** - ограничивает количество времени, которое LDAP поиск может занимать. По умолчанию предел не установлен, но Вы могли бы установить предел в 60 секунд, например.

- **Minimum characters for wildcard search** - увеличить число знаков, которые пользователи должны вводить перед вводом в первого поиска по знакам в запросе поиска. По умолчанию 1. Не определите 0 (ноль), если Directory не маленький. Установка значения 0 (ноль) может закончиться медленным поиском, потому что установка Optimize LDAP queries не применяется, когда никакие знаки не введены.

Сервер Domino не возвращает всю ожидаемую информацию.

По умолчанию, Domino сервер только возвращает некоторые значения полей, анонимным LDAP клиентам. Однако Вы можете сконфигурировать LDAP, чтобы возвращать дополнительные значения полей.

7.4 Проблемы с маршрутизацией почты.

Разнообразные ошибки могут заставить Domino не нормально рассылать почту. Эти темы описывают решения общих проблем с почтой и обеспечивают Вас детальной информацией относительно решения проблем передачи почты и поиска неисправностей.

7.4.1 Инструменты для решения проблем с маршрутизацией почты.

Сообщение о недоставке почты.

Пользователи должны всегда пробовать повторно, отослать почту, для которой они получили сообщения о неудачной доставке. Чтобы помочь пользователям в решении проблем неудачной доставки, попросите их выполнить шаги указанные ниже. Попросите, чтобы они использовали первые три шага, чтобы послать Вам копию их базы данных почты. При отправке Вам копии их почтовой базы данных сохраняет поле свойств сообщений, которые Вы анализируете как средства поиска неисправностей.

*3151 Пользователь создает новую почтовую базу данных для рабочей станции, из меню Файл – База данных – Создать. Убедитесь, что использовали шаблон MAIL50.NTF.

*3152 Пользователь копирует любые сообщения неудачной доставки из оригинальной почтовой базы и вставляет эти сообщения в новую базу данных.

*3153 Пользователь присоединяет новую почтовую базу данных к почтовому сообщению и посылает ее Вам.

Вы открываете базу данных почты, запускаете присоединенную почтовую базу и просматриваете сообщения неудачи доставки.

Сообщение неудачной доставки содержит причину, по которой доставка потерпела неудачу и путь, по которому сообщение было послано. Используйте эту информацию, чтобы далее исследовать проблему.

Трассировка сообщения.

Для локализации проблем с маршрутизацией почты, Вы отслеживаете доставку почты, чтобы проверить, может ли сообщение доставлено, без фактической рассылки сообщения.

*3154 Из клиента Domino Administrator, выбирайте закладку Почта – Почта.

*3155 Из панели инструментов выбирайте - Сервис – Трассировка доставки…

*3156 Заполните эти поля, и затем щелкают – Отправить.

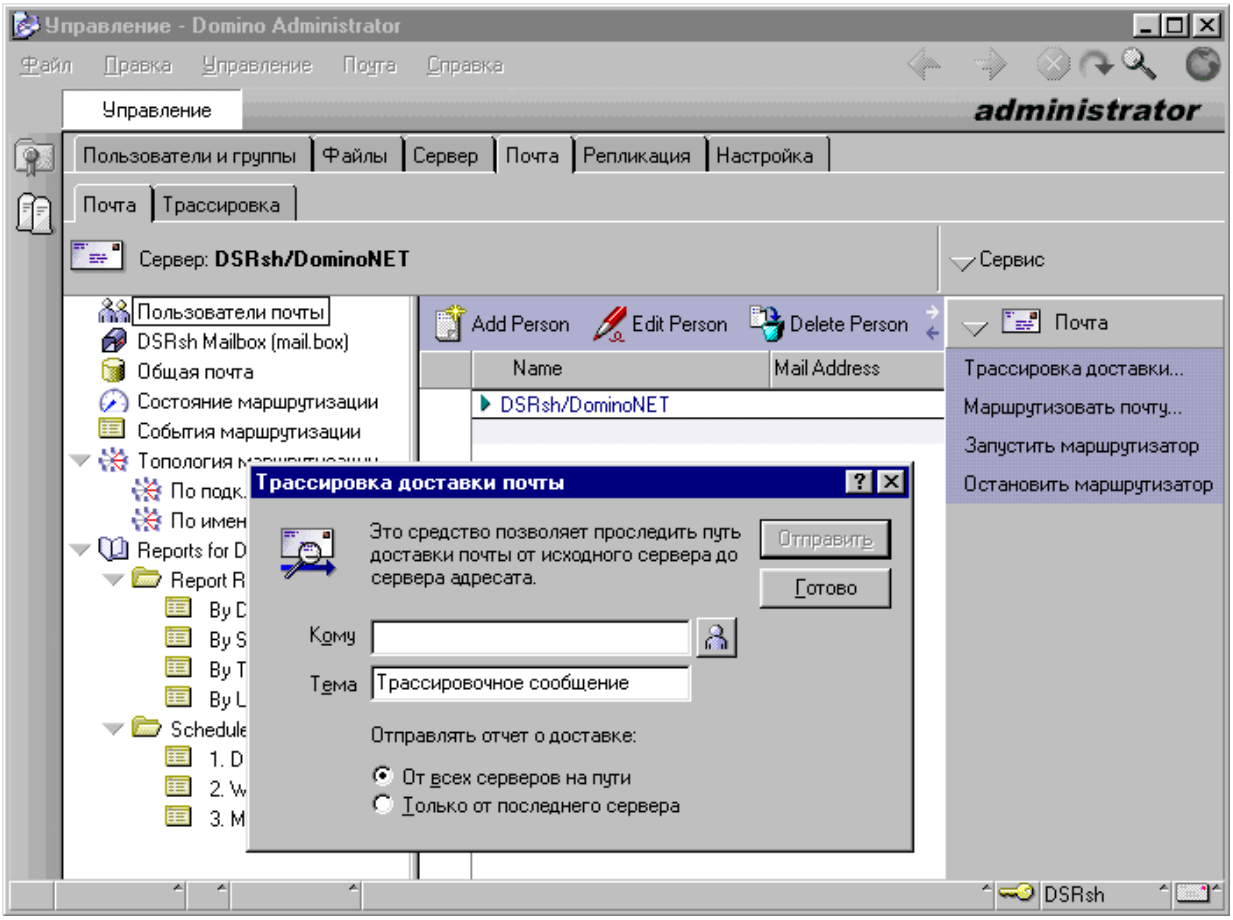


Рис. 116 Диалоговое окно настройки трассировки сообщений.

Карты топологии маршрутизации почты.

Карты топологии маршрутизации почты полезны для решения проблем с передачей почты между серверами.

*3157 Из клиента Domino Administrator, выбирайте закладку Почта – Почта.

*3158 Выбирайте одно из представлений – Топология маршрутизации:

- По подключениям
- По поименованным сетям

Из клиента Domino Administrator, выбирайте закладку Почта – Почта, затем выберите представление Состояние маршрутизации. Вы можете также просматривать представление для почтовых протоколов, из файла LOG.NSF.

Проба почты.

При использовании Mail Probe, Вы можете проверять и собирать статистику по передаче почты.

7.4.2 Проблемы с маршрутизацией почты и сообщения об ошибках.

Эти темы описывают общие проблемы и ошибки, связанные с рассылкой и или получением почты:

7.4.2.1 Пользователь не может получать любую почту, включая почту, посланную пользователями, чьи почтовые файлы находятся на том же самом сервере.

Если пользователь не может получать любую почту, включая почту, посланную другими пользователями, чьи почтовые файлы находятся на той же самой почтовом сервере, проверьте представление Mail Routing Events, файла протоколов, рабочей станции. Также, проверьте файл MAIL.BOX, рабочей станции пользователя, чтобы определить, накапливается ли почта. Измените установку переменной Log_MailRouting в файле NOTES.INI, чтобы увидеть более детальную информацию о маршрутизации почты.

7.4.2.2 Пользователи получают сообщение – File is in use by another process.

Если почтовый файл получателя или файл MAIL.BOX, при посылке или получения почты файл заблокирован, например, занят процессом BackUp, Domino генерирует сообщение File is in use by another process. Ждите, пока процесс закончится, и затем повторно пошлите сообщение.

7.4.2.3 Пользователи получают сообщение, при попытке отослать почту, на том же самом почтовом сервере - NAMES.NSF does not contain a required view.

Если все пользователи на одном почтовом сервере не могут посылать или получать почту, и они получают сообщение NAMES.NSF does not contain a required view, Вы должны модернизировать дизайн Domino Directory. Выберите - Файл – База данных – Заменить структуру. Когда Вы заменяете или настраиваете дизайн Domino Directory, дизайн должен быть однороден во всех репликах базах данных.

Обратите внимание, что имеются два шаблона для адресных книг. PUBNAMES.NTF для Domino Directory и PERNAMES.NTF для персональных адресных книг. Убедитесь, что Вы используете шаблон PUBNAMES.NTF, при работе с Domino Directory.

7.4.2.4 Пользователи получают сообщение – No route found to Domain x from Server y.

Если пользователи не могут посылать почту в другой домен и получают сообщение типа No route found to Domain x from Server y, удостоверьтесь, что Domino Directory каждого домена имеют документ подключения с одного из серверов, к серверу в другом домене. Если документ подключения не существует, создайте его. Если имеется документ подключения, удостоверитесь что информация, содержащаяся в нем правильна.

7.4.2.5 На консоли сервера появляется сообщение – Router: Possibly no DOMAIN set.

Если это сообщение появляется на консоли и затем задача Router останавливается, если Server документ содержит ошибки. В Server документе, проверите поле ими почтового

домена. Убедитесь, что домен указан правильно, и что поля ServerKeyFileName, или KeyFileName оба содержат правильное имя ID сервера, для этого сервера. Если необходимо, сделайте исправления в Server документе. Также проверьте, чтобы документ подключения, который вы используете, обращался к правильному ID сервера. Если необходимо, редактируйте документ подключения.

7.4.2.6 Пользователи получают сообщение – Server Error: File Does Not Exist.

Это сообщение происходит, когда пользователь пробует читать сообщение, которое связано с активным файлом Shared Mail, который был ненадлежащим образом перемещен в другой каталог, или жесткий диск.

7.4.2.7 Пользователи получают сообщение – User name is not unique.

Проверьте Domino Directory на предмет дублирование имен получателей. Могут иметься больше чем один Person документ, для пользователя. Пользователь и группа могут иметь то же самое имя и так далее.

7.4.2.8 Пользователи получают сообщение – User not listed in the Public Address Book.

Если имя получателя введено с орфографической ошибкой, письмо возвратится отправителю, с сообщением - User not listed in the Public Address Book. Если имя домена внесено с орфографической ошибкой, письмо будет возвращено с сообщением No route found to domain name from server name. Проверьте Domino Directory на предмет правильного введения записи имени и повторно отошлите документ.

7.4.2.9 Если приходится добавлять к адресу получателя - @domainname, для нормальной доставки сообщений пользователям другого домена.

Если пользователи сообщают, что они не могут посылать почту в другой домен, если они не включают в адрес @domainname, сконфигурируйте Directory Assistance и Directory catalog, чтобы включить имена каталогов пользователей, из других доменов.

7.4.3 Как локализовать проблемы с маршрутизацией почты.

Когда у Вас имеется “мертвая” или ожидающая доставки почта, это указывает на проблему с маршрутизацией передачи почты. Если пользователи имеют проблемы с рассылкой или получением почты, используйте эти пункты, чтобы собрать информацию и идентифицировать проблему, затем исправьте ее.

*3159 Проанализируйте отчет о недоставке сообщения.

*3160 Вы можете использовать трассировку доставки почты.

*3161 Проверьте Domino Directory на предмет ошибок.

*3162 Проверьте рабочие станции отправителя и или получателя на предмет ошибок настройки почты.

*3163 Проверьте сервер на предмет наличия ошибок работы с почтой.

*3164 Проверьте настройки Shared Mail, если Вы используете эту функцию.

7.4.3.1 Проверка Domino Directory на наличие ошибок в настройках почты.

Domino Directory - источник многих неприятностей, которые влияют на передачу почты должным образом. Проверьте эти условия и исправьте их, если необходимо.

*3165 Проверить историю репликаций Domino Directory, чтобы убедится, что все изменения реплицируются должным образом. Удостоверьтесь, что ACL Domino Directory позволяет серверам, по крайней мере, доступ редактора. Проверьте сообщения в базе данных процесса администрирования, удостоверьтесь, что процесс администрирования был правильно установлен и работает должным образом.

Проблемы с почтой происходят, если репликации Domino Directory во всем домене не происходят правильно.

Например, если Вы перемещаете почтовый файл пользователя, и изменения в Person документе не реплицируются между двумя серверами, сообщение направленные этому пользователю будут возвращаться отправителю.

*3166 Ищите и исправляйте любую из этих проблем в Person документах.

- Не имеется никакого Person документа для получателя в Domino Directory. Если необходимо, регистрируйте получателя, чтобы создать документ.
- Имя получателя почты на сервере отправителе указано неправильно. Исправьте его, если необходимо.
- Имеются несколько имен получателя в Domino Directory. Могут иметься больше чем один Person документ, пользователь или группа имеет того же самое имя и так далее.
- Получатель получает почту через шлюз. Удостоверитесь, что Person документ получателя содержит адрес отправителя.

*3167 Проверьте Server документы, сервера отправителя почты и получателя. Удостоверитесь, что имена серверов, доменов и поименованных сетей Notes, записаны правильно.

*3168 Проверить документы подключений, для передачи почты. Если два сервера находятся в различных поименованных сетях, или доменах, то Вы должны создать пары документов подключений, чтобы позволить почте маршрутизироваться между этими серверами. Для серверов в одной поименованной сети, почта, перемещается автоматический, так что Вы не нуждаетесь в документах подключения.

Чтобы проверять маршрутизацию почты, из клиента Domino Administrator, выбирайте закладки - Почта – Почта. Вы можете просмотреть почтовую топологию двумя способами: топологию по подключениям и топологию по поименованным сетям. Ищите сервера на которые не может передаваться почта. Проверьте Domino Directory, редактируйте или создайте документы по мере необходимости:

- Отсутствуют документы подключения
- Удостоверитесь, что Domino Directory каждого домена имеет документ подключения от одного из серверов, к серверу в другом домене.
- Поименованная сеть Notes записана с орфографической ошибкой, или домен в документе подключения содержит ошибку.

- Неправильно указан телефонный номер в документе подключения.
- Отсутствует значение Mail Routing, в поле Routing Tasks, документа подключения.

*3169 Если почта, передается с использованием документов Non-Adjacent Domain или Foreign Domain, проверьте, чтобы Domino Directory содержит правильно созданные документы Non-Adjacent Domain или Foreign Domain документы. Для Non-Adjacent Domain, проверите, что существует документ подключения, для промежуточного сервера.

*3170 Если Ваша организация использует несколько адресных книг, убедитесь что в NOTES.INI файле содержатся правильные имена этих адресных книг.

7.4.3.2 Проверка рабочих станций отправителя и или получателя на предмет ошибок настройки почты.

Проверьте эти условия и исправьте их, если необходимо:

*3171 Проверьте настройки рабочей станции - Файл – Параметры - Параметры настройки. Проверьте установки для почты в поле Почтовая программа. Если не выбрана ни какая из доступных установок, почта для пользователя работать не будет. Проверьте назначения для портов.

*3172 Проверьте персональную адресную книгу пользователя на отсутствие представлений. Если какие либо представления отсутствует, замените дизайн персональной адресной книги. Выбирайте - Файл – База данных – Заменить дизайн, определяйте шаблон персональной адресной книги - PERNAMES.NTF. Убедитесь, что вы НЕ указали шаблон PUBNAMES.NTF, который используется для Domino Directory. Замена дизайна удаляет любые частные представления, но не затрагивают данные.

*3173 Проверить, использует ли пользователь, соответствующий документ Место вызова.

Пример. Пользователь, который часто работает в дороге, когда работает в офисе, может пытаться использовать документ Место вызова, который используется только для работы из дома. Другая проблема, возможно, состоит в том, что документ Место вызова может содержать неправильную информацию. Чтобы проверить документ Место вызова, для рабочего места пользователя, выбирайте – Файл – Подключение – Изменить параметры.

*3174 Проверьте рабочее место отправителя на предмет заполнения поля Главный/почтовый сервер и поле Почтовый файл.

7.4.3.3 Проверка сервера на предмет наличия ошибок работы с почтой.

Проверьте эти условия, исправьте их, если необходимо:

*3175 Проверьте, что посылающий и получающий сервера имеют взаимные сертификаты. Из клиента Domino Administrator, выбирайте закладку Настройка. Из панели инструментов, выбирайте – Сервис – Заверение – Свойства учетной записи. Выберите соответствующий ID файл сервера и нажмите – Открыть. Выбирайте закладку Сертификаты, чтобы просмотреть сертификаты сервера. Повторите операцию для другого сервера. Повторно сертифицируйте один или оба ID сервера, по мере необходимости.

*3176 Удостоверитесь, что имеются достаточно памяти и места на диске на почтовом сервере получателя. Добавьте память сервера, и или увеличьте значение Swapping. Добавьте диск на сервер.

*3177 Проверьте почтовый файл пользователя. В редких случаях почтовый файл получателя может быть разрушен. Сделайте одно из ниже перечисленного:

- Запустите задачу Fixup. Используйте эту процедуру, если база данных находится в формате R5. Не делайте этого, если Вы не используете Transaction logging, или если база данных находится в формате R4.x.

- Запустите Fixup с параметром (-J). Как только Fixup завершится, выполните полное резервное копирование базы данных.

*3178 Проверьте установки Domain и переменные в файле NOTES.INI. Если при запуске сервера, Router посылает сообщение на консоль или в файл LOG.NSF – Mail Router started for domain x. Чтобы увидеть, настройки доменов из NOTES.INI, введите эту команду на консоли сервера:

```
Show Configuration Domain
```

Проверите, что имя домена правильно введено. Добавьте переменную домена или исправьте запись имени домена, вводя эту команду с консоли сервера:

```
Set Configuration Domain = DomainName
```

Где DomainName - имя почтового сервера домена Notes.

*3179 Проверить базу MAIL.BOX на сервере:

- Запустите задачу Fixup. Используйте эту процедуру, если база данных находится в формате R5. Не делайте этого, если Вы не используете Transaction logging, или если база данных находится в формате R4.x.

- Запустите Fixup с параметром (-J). Как только Fixup завершится, выполните полное резервное копирование базы данных.

Если исправить базу не удалось, закройте сервер и переименуйте MAIL.BOX

Например, переименуйте базу данных в BADMAIL.BOX.

Запустите повторно сервер, при этом будет создан новый файл MAIL.BOX. После этого копируйте любые, не разрушенные документы из базы данных BADMAIL.BOX, в базу данных MAIL.BOX.

7.4.3.4 Проверка настройки Shared Mail.

Проверьте эти условия, исправьте их, если необходимо.

*3180 Удостоверьтесь, что почта Shared Mail разрешена. Чтобы определять, используется ли общий файл почты или индивидуальные почтовые файлы, введите эту команду на консоли сервера:

```
Load Object Info USERMAIL.NSF
```

Где USERMAIL.NSF - имя файла почты пользователя или имя каталога, который содержит почтовые файлы.

Если Вы входите, имя каталога, информация, которая появляется, описывает каждый файл почты в каталоге.

*3181 Проверьте файл Shared Mail на предмет разрушения, если Вы подозреваете, что файл Shared Mail испорчен, Вы можете восстановить файл.

*3182 Проверить, что имеются достаточно места на диске для файла Shared Mail. Если места мало, Вы можете произвести чистку устаревших сообщений из файла Shared Mail.

*3183 Удостоверитесь, что почтовый файл пользователя не был несвязан с файлом Shared Mail. Если необходимо, обновите связь почтового файла пользователя с файлом Shared Mail.

7.5 Проблемы с планированием встреч и резервированием ресурсов.

Темы описывают, как локализовать проблемы с планированием встреч и резервированием ресурсов.

7.5.1 Информация о свободном времени пользователя недоступна.

Если, при планировании встречи пользователь не может посмотреть свободное время выбранного им пользователя, потому что в окне свободного времени не содержится никакой информации, или пользователь получает сообщение - Нет информации планирования, для выбранных пользователей, то следующие пункты помогут Вам локализовать эту проблему.

*3184 Убедитесь, что имя Вашего коллеги, приглашаемого на встречу, написано правильно. Если Вы с коллегой принадлежите различным доменам Notes, убедитесь, что определили полное иерархическое имя, включая имя домена.

*3185 Убедитесь, что версия Вашего сервера - 4.5 или выше.

*3186 Убедитесь, что почтовый сервер запущен. Поиск свободного времени терпит неудачу, если Domino не может получить доступ к базе данных свободного времени на почтовом сервере Вашего партнера, потому что сервер в данное время не работает. Если сервер не запущен, пользователь может все еще закончить обработку приглашения, включая посылку и получение назначений на встречу. Также, поиски для других людей, приглашения с поисками свободного времени на других серверах, все еще будет работать.

*3187 Убедитесь, что задача Schedule Manager запущенна на почтовом сервере.

*3188 Убедитесь, что приглашенный имеет профиль календаря, после модернизации дизайна в Domino 4.5 или выше.

*3189 Убедитесь, что пользователь включен в список пользователей, которые могут читать информацию о свободном времени пользователя, в профиле календаря.

*3190 Убедитесь, что поиск свободного времени находит информацию о графике свободного времени для пользователей, чьи почтовые сервера находятся в смежных и других не Notes доменах. Если Вы не в состоянии это сделать, удостоверитесь, что имеются соответствующие документы доменов. Кроме того, проверьте поле Calendar server name в Domain документе, чтобы удостовериться, что сервер календаря был определен для домена.

*3191 Проверьте, что почтовый сервер работает по тому же самому протоколу. Протоколы портов для серверов должны совпадать.

7.5.2 Пользователь получает сообщение - Can't Find User in Name and Address Book.

Ситуация типично возникает, когда пользователь оставляет компанию и больше не существует для него Person документ в Domino Directory. Чтобы решать эту проблему, найдите документ, связанный с Note.ID и удалите документ.

7.5.3 Пользователь получает сообщение – Cannot perform this action locally.

Это сообщение появляется, когда Вы пробуете создать документ Site Profile в базе данных Resource Reservation, используя при этом локальном режиме работы с базой на сервере. Чтобы избежать этого сообщения, откройте базу данных Resource Reservation с использованием сети.

7.5.4 Пользователь получает сообщение – No resource/room found for time and/or capacity requirements.

Сообщение No resource/room found for time and/or capacity requirements, может появится, когда пользователь создает резервирование в базе данных Resource Reservation. Это сообщение указывает, что в имени Site Profile, для которого создается ресурс включена запятая - например, Acme, East. Измените имя Site Profile, например на Acme East.

7.6 Проблемы с модемом и удаленными соединениями.

Разнообразные условия могут влиять на поведение модема, при использовании удаленного соединения с сервером. Эти темы описывают общие проблемы и ошибки, предоставляют Вам информацию для поиска модемных неисправностей.

7.6.1 Инструменты для диагностики и решения проблем с модемом и удаленными соединениями.

Протоколирование операций ввода - вывода модема.

Чтобы делать записи, о движении данных с использованием модема, в файл LOG.NSF, Вы должны разрешить протоколирование событий модема. Протоколирование событий модема полезна, когда Вы имеете проблемы со связью по модему.

*3192 Выбирайте - Файл – Параметры – Параметры настройки – Порты – Параметры COMx – Записывать ввод/вывод модема.

*3193 Нажимайте ОК, дважды.

Данные командные строки модема.

Когда Вы настраиваете модем и командный файл модема, Вы можете включать в него длинные строки инициализации модема. Если эти установки содержат ошибку, может быть трудно, определить, какие команды, или параметр вызывает проблему.

Чтобы выявить проблемную команду или параметр, разделите командную строку на пополам и введите новую команду сразу после первой половины строки. Попытайтесь установить связь снова и затем проверьте протокол, чтобы определить, какая из половин строки дает ошибку. Продолжайте делить строку установок, пока Вы не выявите команду или параметр, который вызывает проблему.

7.6.2 Как локализовать проблему с модемом или удаленным соединением?

Если сервер или рабочая станция, не может соединиться через модем, могут иметь место проблемы с передачей информации. Например, почта не передается между двумя серверами, связанными модемами. Используйте эти пункты для локализации проблем с обеих сторон для связи:

*3194 Выключите и повторно включите модем на сервере или рабочей станции. Выполнение этого обычно помогает, когда модем ведет себя некорректно. Например, если модем набирает номер несуществующего телефона, отказывается от посланных в него команд, свечение LED индикаторов, в ненормальной комбинации, или при другом необычном его поведении.

*3195 Удостоверьтесь, что выбран правильный тип модема и модель, в настройках сервера или рабочего места. Если Вы подозреваете, что аппаратные средства неправильно работает или повреждены, замените поврежденные компоненты.

*3196 Проверьте конфигурацию модема. Проверьте положение выключателей - DIP, телефонную линию и кнопки на модеме.

*3197 Проверьте, что вы набираете правильный номер. Если вы набираете номер из офиса, убедитесь, что набираете префикс выхода на линию, обычно 9 с запятой.

*3198 Запретите ожидание гудка АТС и установите правильно способ набора номера.

P - для способа набора номера в пульсе.

T - для способа набора номера в тоне.

*3199 Не включайте другие телефонные аппараты, параллельно Вашему модему. Вы будете получать разрыв соединения, если кто-то пытается использовать дополнительный параллельный телефон на этой линии.

*3200 Удостоверится, что вы используете аналоговую линию. Если телефонная система - цифровая, а Ваш модем аналоговый, Вы не будете получать тон АТС. Обратитесь с Вашу телефонную компанию для получения аналоговой линии.

*3201 Проверьте COM порт, скорость порта и назначения контроля управления потоком аппаратных средств, они должны быть одинаковы для модемов, которые пробуют соединяться.

*3202 Проверьте командный файл модема. Удостоверитесь, что он правильно выбран для Вашего модема. Удостоверитесь, что он использует правильный синтаксис и не содержит ошибок записи, параметров команд.

*3203 Проверяет документ подключения, в Domino Directory. Удостоверитесь, что поля в документе подключения содержат правильную информацию для набора номера модемов.

*3204 Проверьте представление Miscellaneous Events, файла LOG.NSF. Иногда модемы, которые используют те же самые стандарты модема, не могут соединяться друг с другом из-за протокола модема. Обратитесь к изготовителю модема, чтобы решить проблему.

*3205 Проверьте представление Phone Calls, файла LOG.NSF. Numerous CRC или ошибки передачи указывает, что один или оба модема обнаруживают ошибки передачи. Поврежденный RJ-11 кабель или неудовлетворительное качество телефонной линии, может вызывать ошибки. Замените шнур и попросите телефонную компанию проверить телефонную линию.

*© **InterTrust Co.** Тел. 956-7928*

7.6.3 Проблемы и сообщения об ошибках, при использовании модемов и удаленных соединений.

7.6.3.1 Данные не передаются между двумя серверами, соединенными Null-Modem кабелем.

Если Вы соединяете два сервера Null-Modem кабелем, и сервера устанавливают связь, но данные не передаются между ними, пробуют эти шаги, чтобы решить проблему:

*3206 Замените кабель модема или смените порт, который Вы уверено, знаете, что он работает правильно.

*3207 Измените скорость порта. Выбирайте скорость порта, которая соответствует скорости порта, которая установлена с другой стороны.

7.6.3.2 Dial-Up сервер не может инициализировать модем, или синхронизировать его с удаленным модемом.

Если LOG.NSF указывает, что сервер не может инициализировать модем, или синхронизироваться его с удаленным модемом. Пробуйте эти пункты, чтобы решить проблему:

*3208 Поверьте, модем, или повторно установить это, с использованием операционной системы.

*3209 Проверьте кабель между сервером и модемом. Удостоверитесь, что кабель исправен и присоединен к правильному порту и не поврежден.

*3210 Удостоверитесь, что порт правильно сконфигурирован.

*3211 Определите более низкую скорость порта.

*3212 Замените модем или RS-232 карту интерфейса, на заведомо рабочую карту.

7.6.3.3 Игнорирование значений команд в командном файле модема.

Вы можете заметить эту проблему, если Вы проверяете файл протокола и не найдете ответов OK, после ввода одной или более команд. Пробуйте эти пункты, чтобы решить проблему:

*3213 Удостоверитесь, что AT-команды, в файле команд модема, набраны все в верхнем, или все в нижнем регистре. Многие модемы не признают смешивания регистров.

*3214 Удостоверитесь, что количество знаков в командной строке, не превышает установки для модема. Используйте SETUP=AT, в начале каждой линии, чтобы разбить команды на несколько частей.

7.7 Проблемы с соединениями - Network Dial-Up.

Тема описывает, как устранить проблемы связи с использованием Network Dial-Up.

Если пользователь создает документ подключения, выбирайте тип документа Network Dial-Up, но не может соединяться с сервером, проверьте эти условия и исправлять их, если необходимо.

*3215 Удостоверитесь, на рабочую станцию и или сервер было установлено программное обеспечение Remote access client - Dial up Networking for Windows95/NT или Apple Remote Access, для MacIntosh. Если программное обеспечение не было установлено, пользователи получат сообщение Error initializing remote LAN service. Установите программное обеспечение клиента Dial-Up или сервера и затем пробуйте соединиться.

*3216 Удостоверитесь, что удаленный сервер доступен. Если модем занят или сервер недоступен, то сервер не может отвечать на Ваши запросы.

*3217 Удостоверитесь, что пользователь имеет необходимую привилегию использовать связь Dial-Up, чтобы звонить на сервер. Если необходимо, измените привилегии пользователя. Также, удостоверитесь, что пользователь использует правильный ID пароль.

*3218 Используйте Trace the connection to the server, для проверки документов подключений.

Обратите внимание, что информация о трассировке сохраняется в представлении Miscellaneous Events, файла протоколов. Вы можете изменять уровень детализации протоколов, в поле Log Trace Connections - Log Options. Для отображения максимального количества информации, выберите значение Full Trace Information.

*3219 Используйте ручной метод связи с сервером, с использованием операционной системы, если связь установлена, попробуйте соединить рабочую станцию или сервер, используя сеть LAN. Если это не удается, проверьте конфигурацию сети и проверьте модем.

*3220 Удостоверитесь, что вы используете правильный документ подключения.

7.8 Проблемы с Partitioned серверами.

Темы описывают решения общих проблем и ошибок, которые могут происходить с Partitioned серверами.

7.8.1 Крушение Partitioned серверов.

Все процессы, связанные с Partitioned сервером, имеют то же самое названия для семафоров памяти. Если Partitioned сервер аварийно останавливается, остановите все процессы, связанные с этим сервером, так как старые процессы не освобождают память.

Убедитесь, что установка KillProcess=1 имеется в NOTES.INI файле, ДО запуска Partitioned сервера. Эта установка позволяет автоматическую уборку всех процессов, в случае незапланированного закрытия сервера.

7.8.2 Пользователь получает сообщение – Server exiting: partition number xx is already in use.

Сообщение появляется, когда Вы пробуете запускать больше чем один Partition сервер, или когда клиент Domino Administrator все еще запущен от предыдущего сервера в том же самом Partition. Чтобы исправить это, остановите все процессы, связанные с Partition. Если это не помогает, перезапустите систему.

7.8.3 Пользователь получает сообщение – Server not responding connecting to a partitioned server.

Это сообщение может появиться, если Partitioned сервер не использует TCP/IP Port Mapping.

*3221 Если сервер назначения имеет одну сетевую карту интерфейса с установленным Port Mapping сервером, убедитесь, что сервер Port Mapping запущен. Domino не может устанавливать связь с сервером и делить адреса IP, если сервер Port Mapping не может переадресовывать запросы к соответствующему порту, сервера назначения.

*3222 Удостоверьтесь, что информация о Port Mapping в файле NOTES.INI имеет правильный порядок. В файле NOTES.INI имеются записи, которые ссылаются на все другие Partitioned сервера как на компьютер. Если записи, содержащие информацию, находятся не по возрастанию, Domino выдает сообщение Server not responding или Server's name changed. Редактируйте Port Mapping в файле NOTES.INI, удостоверьтесь, что Partitioned сервера внесены в список, в определенном порядке, как в этом примере:

```
TCPIP_PORTMAPPING00=

TCPIP_PORTMAPPING01=

TCPIP_PORTMAPPING02=

TCPIP_PORTMAPPING03=
```

После изменения файла NOTES.INI остановите и перезапустите сервер, чтобы изменения вступили в силу.

*3223 Удостоверитесь, что номер порта, добавленный в конец записей, к адресу IP сервера назначения, соответствует номеру порта в файле NOTES.INI для сервера назначения. Также, проверите, что имя сервера занесено правильно.

Пример, это установка в Port Mapping сервера файл NOTES.INI, назначает IP адрес сервера и номер порта:

TCPIP_PORTMAPPING00=CN=Server1/O=Org1,198.114.89.123:13520

Файл сервера NOTES.INI содержит запись:

TCPIP_TCPIPADDRESS = 0,198.114.89.123:13520

7.9 Проблемы с Passthru соединениями.

Если соединение через Passthru не работает, как ожидается, проверьте эти условия и исправьте их, если необходимо.

Совет. Чтобы сделать записи о проблемах связи в файле протоколов, установите в поле Log Options, значение - Trace Full Information. Вы можете также отслеживать связи для Passthru сервера.

*3224 Проверьте, что Passthru сервер запущен на Domino сервере R4.x или выше. Сервер назначения может быть и Notes R3, или Domino Release 4. x или выше.

*3225 Проверьте Server документ, чтобы убедится, что Passthru позволяется. Поле Route through field на закладке Security, Server документа, введено ограничивает, кто может использовать сервер как Passthru сервер. По умолчанию это поле не заполнено и поэтому

никто не может использовать сервер как Passthru сервер. Вы можете также создавать новый документ подключения типа Passthru, который будет содержать имена различных серверов, которым позволяется доступ через Passthru на сервер назначения.

Вы можете также использовать поле Access this server, Server документа, чтобы ограничить, кто может использовать Passthru, для доступа к серверу. Если это поле не заполнено на сервере назначения, сервер не позволяет Passthru сессии. Только пользователи группы и сервера, явно указанные в этом поле, получат доступ на сервер с использованием Passthru.

Обратите внимание, что это поле не ограничивает общий доступ на сервер.

*3226 Удостоверьтесь, что документ подключения должным образом сконфигурирован. Проверьте файл протокола, на наличие сообщения Unable to find any path to ServerName, которое указывает на то, что не иметься достаточно информации в Domino Directory, чтобы определить путь на сервер назначения, или что информация в Domino Directory является неправильной. Например, имя сервера содержит орфографическую ошибку.

7.10 Проблемы с репликациями.

Эти темы описывают, как устранить проблемы с репликациями.

7.10.1 Инструменты для локализации проблем с репликациями.

Проблемы с ACL базам данных, аварии сервера, проблемы протокола и неправильно конфигурированные документы подключения – общие причины ошибок репликаций. Используйте эти инструменты для устранения проблем с репликациями.

Файл протоколов Log.nsf.

Для доступа к протоколам, из клиента Domino Administrator, выбирайте закладки Сервер – Анализ, выбирайте файл LOG.NSF сервера, который Вы хотите проверить. Проверьте наличие проблем в этих представлениях:

*3227 Miscellaneous events

*3228 Phone calls

*3229 Replication events

Примечание. Вы может также проверять информацию о репликациях на закладке Репликации, в клиенте Domino Administrator.

Редактируйте файл NOTES.INI, чтобы включить переменную Log_Replication, которая позволяет Вам показывать детальную информацию о Ваших репликациях в LOG.NSF файле.

Statistics And Events.

База данных статистики STATREP5.NSF, содержит записи статистики. Она создается, когда Вы загружаете задачу Collect, если она еще не существует. Вы можете устанавливать оповещение, для некоторых данных этой статистики. Например, Вы могли бы заставлять генерировать сообщение, для оповещения о неудачных попытках репликаций. Вы можете также выводить статистику в любую базу данных, предназначенную для этой цели, хотя типично статистика хранится в базе данных STATREP5.NSF.

Обратите внимание, что Вы можете редактировать файл NOTES.INI, чтобы включить в него переменную Repl_Error_Tolerance, которая увеличивает число идентичных ошибок репликаций между двумя базами данных, которые сервер пропускает прежде, чем он заканчивает репликацию. По умолчанию - 2 ошибки. Чем выше это значение, тем более часто появляется сообщения типа - Out of disk space.

Если Вы запускаете задачу Event на сервере, Вы можете создавать документы Event Monitor, чтобы сообщать о проблемах с репликациями. Вы можете также создавать документ Monitor Replication, которые будут уведомляет Вас, если определенная база данных не в состоянии реплицироваться в течение некоторого времени. Чтобы просматривать эти события из клиента Domino Administrator, выбирайте закладку Сервер – Анализ – Statistics – Events. Вы можете использовать информацию о репликациях с закладки клиента Domino Administrator, для этого выбирайте любое из доступных представлений.

7.10.2 Проблемы с репликациями и сообщения об ошибках.

Темы описывают, как устранять некоторые проблемы с репликациями баз данных.

7.10.2.1 Два сервера не могут реплицировать любые базы данных.

Когда два сервера не могут реплицировать любую из баз, данных между собой, эти сообщения могут появляться в протоколах:

- Unable to replicate with server *x*: Server Not Responding.
- Unable to replicate with server *x*: The Notes server is not a known TCP/IP Host.
- Unable to replicate with server *x*: Your address book does not contain any cross certificates capable of authenticating the server.
- Unable to replicate with server *x*: The server's address book does not contain any cross certificates capable of authenticating you.
- Unable to replicate with server *x*: You are not authorized to use the server or remote server.

Проверьте следующие условия и исправьте их, если необходимо:

*3230 Создайте документы подключения, для репликаций. Если Вы не позволяете одновременный запуск нескольких репликаторов на сервере, удостоверитесь, что графики репликаций не накладываются друг на друга.

*3231 Убедитесь, что сервера имеют общий или взаимный сертификат.

*3232 Удостоверьтесь, что сервера доступны. Проверьте протоколы на наличие записи Unable to replicate with server *x*: Server not responding - указывает, что один сервер не может соединяться с другим сервером для репликаций, или сервер X - недоступен.

*3233 Проверьте представление Miscellaneous Events log, есть ли сообщение ошибок сети, когда сервер попытался соединяться с другим сервером.

*3234 Проверьте представление Phone Calls log, чтобы видеть, способны ли два сервера использовать эту связь.

7.10.2.2 Намеченные репликации не происходят между двумя серверами.

*3235 Проверьте имена серверов в документах подключения.

*3236 Удостоверится, что не имеет пересекающихся расписаний для репликаций. Если документы подключения имеют накладывающиеся графики репликаций, исправьте графики, или запустите на сервере несколько репликаторов.

*3237 Если сервер имеет много подключенных пользователей или серверов, или если сервер исполняет много задач, это может занять более длинный промежуток времени, чтобы строить список баз данных, которые сервера будут реплицировать. Если создание списка занимает много время, намеченные репликации могут быть отсрочены. Проверьте статистику загрузки сервера и если необходимо, реплицируйте только определенные базы данных. Удалите устаревшие базы данных с серверов и или переместите некоторые базы данных на другие сервера. Вы можете также уменьшать число пользователей, которые должны иметь доступ на сервер или уменьшать число задач, исполняемых на сервере.

*3238 Удостоверьтесь, что сервер имеет достаточно места на диске. В противном случае, удалите устаревшие базы данных и или переместите некоторые базы данных на другой сервер.

7.10.2.3 Одна из баз данных не реплицируется между двумя серверами.

Когда репликации происходят правильно между двумя серверами, но одна база данных не реплицируется:

*3239 Сообщение Unable to replicate *xxx*.nsf появляется в протоколах.

*3240 Пользователи сообщают, что документы различны в каждой реплике базы данных.

Чтобы исправить проблему, проверьте эти пункты:

*3241 Удостоверьтесь, что ACL установлен правильно. Сообщение Access control is set to not allow replication в протоколах указывает, что сервера не имеют достаточного доступа, чтобы выполнить репликацию. Дайте серверам нужный доступ к базе данных в ACL, чтобы копировать изменения. Сервер должен иметь:

- Доступ редактора, чтобы копировать изменения документов
- Доступ дизайнера, чтобы копировать изменения представлений и форм
- Доступ менеджера, чтобы копировать изменения ACL

Если репликатор происходит через Passthru сервер, Passthru сервер должен также иметь необходимый доступ, чтобы передать изменения и замены.

*3242 Проверьте протоколы для поиска записи Unable to copy document, или подобное сообщение. Это сообщение указывает на то, что база данных разрушена. Чтобы исправлять проблему, делайте один из следующего:

- Запустите задачу Fixup. Используйте эту процедуру, если база данных находится в формате R5. Не делайте этого, если Вы не используете Transaction logging, или если база данных находится в формате R4.x.
- Запустите Fixup с параметром (-J). Как только Fixup завершится, выполните полное резервное копирование базы данных.

*3243 Проверяет протоколы, для поиска записи Replication is disabled, сообщение указывает, что базе данных не позволяется реплицироваться. Чтобы позволить реплицирование исходной базы данных, выбирайте – Файл – Репликация – Настройка, в окне Параметры репликации, на закладке Прочее, уберите флажок с опции Временное отключить репликацию.

*3244 Проверьте, установлена ли опция Использовать единую таблицу управления доступа для всех реплик, на закладке настройки ACL для базы данных. Иногда репликация не может происходить, потому что этот выбор был установлен, и сервер, хранящий реплики, не имеет соответствующего доступа, чтобы копировать ACL. Если дело обстоит так, дайте серверу доступ менеджера в базе данных ACL.

7.11 Проблемы с доступом на сервер.

Темы описывают, как устранить проблемы с доступом на сервер и возникающие при этом ошибки:

7.11.1 Администратор не может ввести команды на консоли сервера.

Если администратор не имеет доступа к программе рабочей станции на сервере, используйте серверные программы Load, Tell, или Set Configuration, для защиты консоли сервера паролем.

Используйте команду Set Secure на консоли, или используйте клиента Domino Administrator, чтобы удалить пароль консоли.

7.11.2 Пользователи не могут видеть новые сервера и просматривать списки серверов.

Если пользователи не могут видеть новый сервер, когда они пробуют добавлять, создавать, или копировать базу данных, удостоверитесь, что Domino Directory содержит Server документ для нового сервера и, что информация в документе является точной и правильно записанной.

Если никакой Server документ не существует, создайте его и затем удостоверитесь, что новый Server документ копируется по всему Вашему домену серверов. Если Server документ существует и содержит точную информацию для нового сервера, проверьте файл протокола на домашнем сервере пользователя, чтобы видеть, имеются ли проблемы с сетью.

7.11.3 Сообщение – Server not responding.

Сообщение Server not responding может появляться, когда Вы устанавливаете клиента или пробуете открыть любую базу данных на каком то из серверов.

*3245 Проверьте установки сети, в которой установлен Domino сервер.

*3246 Убедитесь, что сервер не был переименован или повторно сертифицирован. Когда пользователь пробует открыть базу данных, но сервер был повторно сертифицирован или переименован, пользователь получит сообщение Server not responding. Пользователи должны использовать новое название сервера, чтобы открыть базу данных.

*3247 Проверьте Server документ на предмет несуществующего имени хоста в поле Notes RPC proxy. Из клиента Domino Administrator, выбирайте закладку Настройка, откройте

соответствующий Server документ. Выбирайте закладку Ports – Proxies. Domino сервер, использующий TCP/IP, не может передавать почту или начинать репликацию с другими серверами в локальном домене, если значение имени хоста недействительно или не существует. В дополнение к сообщению Server not responding вы можете получить следующие сообщения No Path Found to Server, Proxy Reports that the Connection Request Failed.

Domino сервер сконфигурирован так, чтобы использовать Notes RPC proxy, для всех исходящих соединений через внесенный в список Proxy сервер, существует он или нет. Поэтому, большинство Domino системы не использует - RPC proxy, это поле должно быть пустым.

Обратите внимание, разрешена ли опция - Full trace logging, в файле NOTES.INI. Если да, то Вы получите в файле протоколов детальную информацию о неудавшихся попытках соединения с удаленным сервером. PassThru_LogLevel типично устанавливается в 0, чтобы минимизировать ненужное протоколирование.

*3248 Если вы используете протокол NetBIOS, удостоверятся, что он сконфигурирован должным образом и что он запущен на рабочей станции или сервере. Рабочая станция и сервер должны использовать ту же самую версию NetBIOS.

Сетевые фильтры могут запрещать движение протоколов в сети, от Notes до моста, или маршрутизатора. Мосты и маршрутизаторы часто сконфигурированы, чтобы подавлять движение в сети с использованием протокола NetBIOS.

7.11.4 Пользователь или сервер получают сообщение – You are not authorized to access the server или подобные сообщения.

Когда пользователи или сервера получают сообщение - Not authorized to access the server, проверьте эти пункты, чтобы идентифицировать и затем устранить проблему.

*3249 Проверьте Domino Directory

*3250 Проверьте ID сервера.

*3251 Убедитесь, что пользователь имеет надлежащий сертификат для доступа к серверу.

*3252 Проверьте сеть и аппаратные средства компьютера.

7.11.5 Проверка Domino Directory при проблемах с доступом на сервер.

Многие условия могут влиять на надлежащий доступ к серверам и могут быть отслежены в Domino Directory.

*3253 Проверьте, что эти поля в Server документе содержат правильную информацию. После каждого изменения, которые Вы делаете, убедитесь, что сохранили Server документ перед попыткой доступа на сервер снова.

Поля	**Проверьте значения**
Server name	Имя сервера
Domain name	Имя домена Notes
Port	Порты сервера

Notes Network	Имя Notes сети

Поля с закладки Restrictions	**Проверьте значения**
Access server	Удалите содержимое этого поля, если оно содержит любую информацию. Только эти имена пользователей или групп, внесенные в список в это поле получат доступу на этот сервер.
Not access server	Удалите содержимое этого поля, если оно содержит любую информацию. Пользователям или группам, внесенным в список в это поле, не позволяется доступ к серверу.

*3254 Удостоверится, что сервер документ не испорчен. Чтобы определять, является ли он испорченным, создайте новый Server документ и используйте его вместо старого. Если новый Server документ решает проблему, вероятно, что оригинальный документ сервера, является испорченным. Убедитесь, что вы сохранили оригинал документа Server документ, или скопируйте и вставьте его в другую базу данных.

Когда Вы создаете новый Server документ, убедитесь, что скопировали публичный ключ в новый Server документ.

*3255 Проверьте, что заверенный публичный ключ в файле ID сервера соответствует публичному ключу. Чтобы сделать это, скопируйте заверенный публичный ключ и вставьте его в текстовый файл, а затем сравните два его значения, которые должны быть одинаковыми. Если значение отличаются от ID сервера, вероятно, что он был создан другим сертификатором ID. Перед изменением ключа, создайте резервную копию ключа из Domino Directory.

*3256 Проверьте Group документы в Domino Directory для правильного указания пользователей и имен серверов. В частности проверьте документы групп, внесенных в поля Access server и Not access server в Server документе. Кроме того, убедитесь, что проверили установку типа групп для этих документов групп. Тип группы, назначенный для группы, может затрагивать доступ на сервер.

*3257 Разрешайте любые конфликты репликаций, сохраненные как конфликты для Person или Group документов.

*3258 Удостоверьтесь, что все представления в Domino Directory обновлены или не разрушены. Чтобы восстановить все представления в этой базе данных, запускайте команду на консоли сервера:

```
Load updall names.nsf -r
```

Если Вы подозреваете, что база данных Domino Directory - разрушена, сделайте одно из следующего:

- Запустите задачу Fixup. Используйте эту процедуру, если база данных находится в формате R5. Не делайте этого, если Вы не используете Transaction logging, или если база данных находится в формате R4.x.

- Запустите Fixup с параметром (-J). Как только Fixup завершится, выполните полное резервное копирование базы данных.

Кроме того, если Вы подозреваете, что Domino Directory разрушен, пробуете использовать резервную копию Domino Directory, или создавать новую реплику Domino Directory.

*3259 Замените дизайн для Domino Directory из меню Файл – База данных – Заменить дизайн. Это гарантирует, что Domino Directory использует правильный шаблон - PUBNAMES.NTF.

*3260 Проверьте форму для Server документа Domino Directory.

*3261 Удостоверьтесь, что Passthru должным образом сконфигурирован в Server документе.

7.11.6 Проверка ID сервера, при проблемах с доступом на сервер.

Когда Вы получаете сообщение You are not authorized to access that server, проблема может быть связано с ID сервера.

*3262 Проверьте ID сервера. Если ID сервера поврежден, Domino сервер может запускаться, но пользователи не будут способны получить доступу к нему. Вы можете так же получить сообщение Server Error: Damaged ID, при запуске Domino сервера.

Если server ID был недавно повторно сертифицирован, возможно, он был поврежден, если Domino сервер не был закрыт прежде, чем ID сервера был повторно заверен или слит.

Если Вы подозреваете, что ID сервера поврежден, Вы можете заменить ID, новым ID сервера.

*3263 Проверить, что сервер имеет все требуемые сертификаты.

*3264 Проверьте, что публичный ключ, сохраненный в Server документе, соответствует ключу, сохраненному в ID сервера. Чтобы сделать это, скопируйте публичный ключ ID в буфере обмена и затем вставьте его в текстовый файл, чтобы Вы могли сравнивать этот ключ, с публичным ключом в Server документе.

7.11.7 Замена ID сервера.

Если Вы подозреваете, что ID сервера поврежден, замените это резервным ID. Если Вы не имеете резервного ID сервера, создайте новый ID. Убедитесь, что использовали то же самое имя для нового ID файла, которое использовалось старым ID файлом.

*3265 Закройте Domino сервер.

*3266 Переименуйте старый ID файла, например в Server.OLD. Вы должны переименовать ID, чтобы вынудить запросить путь к новому ID файлу на жестком диске.

*3267 Скопируйте резервный, или новый, ID файл сервера в каталог на жестком диске. ID файлы типично располагаются в каталоге - c:\Notes\data.

*3268 Повторно запустите сервер.

7.11.8 Копирование публичного ключа.

*3269 Из клиента Domino Administrator, выбирайте закладку Настройка.

*3270 Из панели инструментов справа, выбирайте - Сервис – Заверение – Свойства учетной записи.

*3271 Выбирайте ID файл сервера, нажимайте – Открыть.

*3272 С закладки Дополнительно, нажмите кнопку Копировать общий ключ, чтобы скопировать публичный ключ в буфер обмена.

*3273 Вставьте публичный ключ в поле Certified public key, Server документ.

7.12 Проблемы, вызывающие крушение сервера.

Когда сервер терпит аварию, самое простое решение перезапустить его. Однако Вы могли бы захотеть выяснить, почему сервер потерпел крах, чтобы избегать в будущем аварий. Эти темы описывают Ваши действия при крушении сервера.

7.12.1 Что делать при крушении сервера.

Наиболее общие причины аварий сервера - следующее:

*3274 Мало системных ресурсов выделенных серверу

*3275 Высокая загрузка сервера

*3276 Проблемы с программным обеспечением

*3277 Проблемы с сетью

*3278 Изменение окружающей среды сети или операционной системы

*3279 Изменение конфигурации компьютера сервера, например замена сетевой карты или программного обеспечения для нее.

Используйте эти шаги для анализа крушения сервера. Если, после завершения этих шагов, Вы не решили проблему, консультируйтесь с Вашим техническим представителем поддержки.

*3280 Соберите информацию о Вашей системе:

- Версия Domino сервера
- Версия операционной системы.
- Тип сети и версии сетевых протоколов
- Версии сервисных пакетов установленных для операционной системы
- Конфигурация компьютера сервера
- Имена API программ и задач, работавших на сервере.

*3281 Обратить внимание на любые изменения для элементов Domino или окружающей среды. Если возможно, возвратитесь к предыдущей конфигурации, чтобы определить, происходит ли проблема.

*3282 Если последнее сообщение на консоли сервера начиналось словом Panic, ... запишите, полное сообщение.

*3283 Если возможно, захватите изображение последнего экрана, который был, показал на консоли.

*3284 Остановите все задачи, запущенные на Domino сервере и затем остановите Domino сервер.

*3285 Если NOTES.RIP или UNIX файл CORE был создан, проверите время и дату файла, который должен совпасть со временем и датой крушения. Переименуйте, и сохраните файл NOTES.RIP, или UNIX файл CORE так, чтобы Domino не перезаписал его в течение будущего крушения. Если необходимо, Lotus Customer Support будет использовать этот файл, чтобы выделить, где произошло крушение.

Обратите внимание, если крушение не производит NOTES.RIP или UNIX файл CORE, сервер, может быть, не имеет достаточного места на диске или ему не хватает памяти.

*3286 Повторно запустите сервер.

*3287 Проверьте представление Miscellaneous Events на наличие ошибок протоколов. Сделайте запись всех записей, которые произошли перед крушением сервера и после. Чтобы делать это, двойным - щелчком запустите соответствующую запись, чтобы открыть ее. В частности ищите *.NSF файл в записях, который может указывать, где крушение произошло. Если специфическая база данных, найдена, которая вызывает крушение, проверьте историю репликации этой базы данных для просмотра дополнительной информации.

*3288 Соберите эти файлы конфигурации:

- CONFIG.SYS - для OS/2
- NOTES.INI - все платформы
- STARTUP.CMD - для OS/2
- PROTOCOL.INI - для OS/2
- NET.CFG - для OS/2 и сетевого обеспечения
- AUTOEXEC.NCF - для сетевого обеспечения
- STARTUP.NCF - для сетевого обеспечения
- Файл диагностики Windows - WindowsNT

7.12.2 Крушение сервера – проблемы и сообщения об ошибках.

Темы описывают проблемы и ошибки, которые могут вызвать крушение сервера:

7.12.2.1 Разрушение базы данных вызывает крушение сервера.

Если Unable to copy database, Unable to copy document, или подобное сообщение появляется в представлении Miscellaneous Events файла протоколов, значит база данных разрушена. Делайте одно из следующего, чтобы исправить проблему:

*3289 Запустите задачу Fixup. Используйте эту процедуру, если база данных находится в формате R5. Не делайте этого, если Вы не используете Transaction logging, или если база данных находится в формате R4.x.

*3290 Запустите Fixup с параметром (-J). Как только Fixup завершится, выполните полное резервное копирование базы данных.

Обратите внимание, что задача Fixup может занять существенное количество времени, чтобы обработать большое количество баз данных или всего сервера.

7.12.2.2 Разрушение представления вызывает крушение сервера.

Если крушение сервера, кажется связанно с разрушением представления базы данных, запустите задачу Updall на базе данных с ключом (-r):

```
Load updall databasename -r
```

Обратите внимание, что запуск задачи Updall может занять существенное количество времени, чтобы обработать большую базу данных. Будет также требоваться существенное количество времени, если Вы запускаете Updall без определения имени базы данных, задача будет обрабатывать все базы данных на сервере.

7.12.2.3 Обновление индекса базы данных вызывает крушение сервера.

Если авария сервера возникает при обновлении индекса базы данных, делайте следующее:

*3291 Запустите задачу Updall на базах данных с ключом (-r), чтобы установить поврежденный индекс базы данных:

```
Load updall databasename -r
```

*3292 Если задача Updall не устраняет проблему, используйте эту процедуру:

- Сделайте реплику разрушенной базы данных. Убедитесь, что дали реплике новое имя файла.
- Удалите оригинал база данных.
- Используйте первоначальное имя файла базы данных, чтобы переименовать новую точную копию.
- Повторно запустите сервер.

7.12.2.4 Задача Router вызывает крушение сервера.

Во многих случаях, крушение происходит, в то время когда специфическая задача запущенна. Вы можете часто определить задачу с экрана сервера после крушения, или из файла NOTES.RIP, для UNIX файла CORE. Если крушение связано с задачей Router, замените базу данных MAIL.BOX.

*3293 Переименуйте базу данных MAIL.BOX.

*3294 Повторно запустите сервер. Сервер автоматически создаст новую базу MAIL.BOX.

*3295 Копируйте и вставьте сообщения из старой базы MAIL.BOX, в новую базу MAIL.BOX.

7.12.3 Файлы NOTES.RIP и UNIX CORE.

Используйте NOTES.RIP файлы и UNIX файлы CORE, чтобы определить причину крушения рабочей станции или сервера. Программа с именем QNC.EXE создает эти файлы в каталоге данных Domino. Файлы содержат информацию относительно задач, запущенных на сервере, когда сервер потерпел крах. Каждая задача - например, Replicator, Router, или Update - обозначена отдельной записью QNC. Если одна из этих задач терпит аварию, QNC программа для задачи производит NOTES.RIP или UNIX файл CORE.

7.13 Проблемы с Transaction logging.

Эти темы описывают общие проблемы с Transaction logging. Вы можете также искать решения общих проблем на сервере - www.support.lotus.com.

Неверный путь к файлам Transaction log.

Если Domino не может получить доступ к файлам Transaction log и сообщения об ошибке показывается на консоли сервера.

*3296 Проверьте путь к файлам протоколов, чтобы удостовериться, что он существует.

*3297 Проверьте, какие права имеет сервер, на запись к каталогу с файлами протоколов.

*3298 Если путь правилен и устройство в норме, перезапустите сервер. Проблема должна быть устранена, и Вы не должны будете приступать к следующим шагам.

*3299 Если путь правилен, но устройство хранения данных разрушено, замените устройство, или отредактируйте переменную TRANSLOG_PATH из файла NOTES.INI, чтобы указать на другой путь к файлам.

Обратите внимание, если Вы редактируете переменную TRANSLOG_PATH, убедитесь, что Вы ввели тот же самое значение в поле Log path в Server документе до перегрузки сервера, в противном случае Domino будет обращаться к старому пути.

*3300 Повторно перезапустите сервер. Domino создает новые файлы Log и Control и назначит новые идентификаторы DBIID на все R5 базы данных.

*3301 Если значение поля Automatic fixup of corrupt databases установлено значение - Yes, в Server документе, задача Fixup запускается на базах данных, которые требуют восстановления информации. Иначе, Вы должны запускать Fixup вручную.

*3302 Исполните полное резервное копирование всех баз данных.

Разрушение Transaction log.

Если Transaction log окажется поврежденным или разрушенным, сообщения об ошибке будет показано на консоли сервера, указывающие, что Log поврежден.

Ошибка может происходить из-за неудавшегося чтения или записи в Transaction log.

*3303 Повторно перезапустите сервер, чтобы исправить ошибку. Если ошибка Log не появляется снова, Log - не поврежден.

*3304 Останавливайте сервер снова, так что бы он чисто закрылся (без ошибок).

*3305 Исполните полное резервное копирование баз данных.

*3306 Повторно запустите сервер.

Если Вы продолжаете получать ошибку, что Transaction log поврежден или испорчен.

*3307 Удалите файлы Transaction log и файлы Control.

*3308 Повторно запустите сервер. Domino создает новый файл Log и Control, назначает новые DBIID, для всех R5 баз данных.

*3309 Если значение поля Automatic fixup of corrupt databases установлено значение - Yes, в Server документе, задача Fixup запускается на базах данных, которые требуют восстановления информации. Иначе, Вы должны запускать Fixup вручную.

*3310 Исполните полное резервное копирование всех баз данных.

Если ошибка произошла в течение восстановления информации, архивированный файл Log может быть испорчен.

*3311 Повторно перезапустите сервер, чтобы исправить проблему, затем остановите сервер, так что бы он закрылся чисто (без ошибок).

*3312 Во время того, как сервер остановлен, используйте утилиту резервного копирования, чтобы исполнить восстановление информации. Если архивный Log, все еще не может использоваться, восстановите базу данных без транзакций в испорченном Log.

*3313 Исполните полное резервное копирование всех баз данных.

*3314 Повторно запустите сервер.

7.14 Web сервер – проблемы и сообщения об ошибках.

Эти темы описывают, как избавится от некоторых общих проблем и ошибок Web сервера Domino:

7.14.1 IIS останавливается при старте Domino.

Если Вы настроили Domino, как ISAPI расширение Microsoft Internet Information Server (IIS), но сервер останавливается, когда Вы запускаете Domino, повторно запустите IIS сервер. Удостоверитесь, что ID файл сервера Domino не защищен паролем. Вы не можете использовать защищенный паролем ID файл сервера вместе с IIS.

Чтобы проверить, защищен ли ID файл паролем, из клиента Domino Administrator, выбирайте из меню Файл – Сервис – Учетная запись. Удостоверитесь, что Вы выбрали ID файл сервера и нажмите кнопку Очистить пароль. Если вы будете запрошены ввести пароль, то ID файл защищен паролем. Введите пароль и затем – ОК, чтобы очистить пароль

7.14.2 Многократный ввод имени и пароля, для доступа пользователей на Web сервер.

Вы можете сконфигурировать Domino Web сервер так, чтобы Domino запрашивал имя и пароль Web пользователей только однажды, когда они получают доступ в различные каталоги сервера через Web. Подобно другим Web серверам, Domino твердо поддерживает модель HTTP идентификации.

Например, если имя сервера - www.acme.com, то www.acme.com – является каталогом высшего уровня, а www.acme.com/doc, www.acme.com/hr - подкаталогами сервера. Если

пользователь подтвердил свою подлинность на сервере, при вызове домашней страницы с www.acme.com, то пользователь будет получать доступ во все подкаталоги сервера www.acme.com. Однако если пользователь открывает страницу с www.acme.com/doc, вводит имя и пароль, но затем пытается получить доступ на www.acme.com/hr, Domino попросит пользователя снова ввести свои данные.

Чтобы пользователь, многократно не запрашивался вводить имя и пароль, направляйте его, для подтверждения его подлинности к самым высшим уровням каталога сервера. При таком планировании пути, Domino запрашивает пользователей ввести имя и пароль только однажды в течение сессии браузера.

Если Web сервер включает связи с другими серверами, и эти сервера требует установления подлинности пользователей, пользователь будет ввести свое имя и пароль для этих серверов.

7.14.3 Пользователи не могут получить доступ к Domino Web серверу с использованием интернета.

Firewall сервер, часто не пускает пользователей к Domino Web серверу через интернет. Если Вы имеете прямую связь с интернетом, Вы можете использовать утилиту PING, для проверки доступа к Domino серверу. Если Вы можете “пинговать” сервер, но не может получить доступ на него, воспользуйтесь утилитой Telnet и проверьте запрос к серверу по порту - 1352. Если соединение по Telnet, терпит неудачу, то Ваш Firewall сервер блокирует TCP порт.

7.14.4 Пользователи не могут просматривать список баз данных на Web сервере или не могут получить доступ к базе данных.

Если пользователи пробуют использовать команду - ?OpenServer, чтобы показать список файлов на сервере, но Web сервер выдает сообщение Database browsing not allowed, проверьте, позволен ли выбор Allow HTTP clients to browser databases, в Server документе для этого сервера.

Если пользователи пробуют доступ к базам данных и получают сообщение Unauthorized exception, удостоверитесь, что пользователи имеют соответствующий доступ к базе данных в ACL.

7.14.5 Пользователь получает сообщение – Error 403 - Directory Browsing error - Access forbidden.

Проверьте Server документ, поле Home URL и Default Home page. Поле отвечает за домашнюю страницу Web сервера, одно из этих полей должно содержать запись.

7.15 Web Administrator – проблемы и сообщения об ошибках.

Темы описывают общие проблемы с Web Administrator и ошибки:

7.15.1 Использование Web Administrator с браузером Netscape.

Если вы используете Web Administrator с браузером Netscape, и Вы изменяете, размер окна браузера, апплет может заново инициализироваться. Чтобы избежать этого, устанавливайте размер окна перед использованием Web Administrator, чтобы запустить апплет.

7.15.2 Пользователь получает сообщение – A Java or script error, при старте Web Administrator.

Web Administrator требует, чтобы браузер поддерживал Java, Javascript или ActiveX Script. В некоторых случаях, эти особенности могут быть выключены в Вашем браузере. Удостоверитесь, что Вы разрешили Java и Javascript или ActiveX Script в Вашем браузере.

Если Ваш браузер не поддерживает эти особенности, Вы должны модернизировать Ваш браузер, чтобы Вы могли использовать Web Administrator.

7.15.3 Web Administrator не показывает корректно Web страницы.

Если Вы используете Netscape, когда Вы изменяете, установки для Web Administrator или размер окна браузера, в некоторых случаях страница может показываться не правильно. Чтобы исправлять это, делайте один из следующего:

Повторно запустите браузер, когда Вы изменяете установки или размер окна.

Редактируйте NOTES.INI файл, чтобы включить переменную WebAdmin_Expire_Cache равную единице.

7.15.4 Пользователь не может получить доступ к базе данных Web Administrator.

Удостоверитесь, что Вы имеете надлежащий уровень доступа и роль в ACL базы данных Web Administrator. Ваше имя должно также быть внесено в список Administer the server from a browser и Run restricted LotusScript/Java agents, Server документа.

Когда Вы запускаете Web Administrator, Domino спрашивает Вас имя и пароля, которые сохранены в Вашем Person документа. Вы должны ввести имя и пароль для доступа к этой базе данных.

Создание новой базы данных Web Administrator.

Domino создает базу данных Web Administrator, когда задача HTTP запускается первый раз на сервере. Имейте в виду, что удаление базы данных удаляет существующие настройки.

*3315 Введите эту команду на консоли сервера:

```
tell http quit
```

*3316 Удалите базу данных WEBADMIN.NSF.

*3317 Введите эту команду на консоли сервера:

```
load http
```

7.15.5 Некоторые команды Web Administrator недоступны.

Если некоторые команды недоступны, когда Вы запускаете Web Administrator, проверьте следующее:

*3318 Удостоверитесь, что Вы имеете соответствующую роль, в ACL базы данных Web Administrator (WEBADMIN.NSF). Роли определяют, какие команды будут доступны Вам.

*3319 Удостоверитесь, что сервер имеет базы данных, связанные с командами Web Administrator, он использует эти базы данных:

- Administration Requests (ADMIN4.NSF)
- Database Catalog (CATALOG5.NSF)
- Domino Directory (NAMES.NSF) specified on the Preferences page
- Log (LOG.NSF)
- Notes Administration Help (HELP5_ADMIN.NSF) in the Doc subdirectory on the server
- Statistics (STATREP5.NSF)
- Statistics & Events (EVENTS5.NSF)
- Web server log (DOMLOG.NSF)

1Инсталляция, обновление программного обеспечения R5. 5

1.1Какой тип инсталляции программного обеспечения сервера выбрать и чем они отличаются? 5

1.2Какие новые возможности появились в версии R5? 6

1.3Какие существуют общие принципы для обновления серверов до версии R5? 8

1.3.1Что нужно учесть при модернизации системы до R5? 8

1.3.2Какой должен быть порядок действий администраторов, при модернизации системы? 9

1.3.3Нужно ли “проигрывать” проект модернизации? 11

1.3.4Как можно протестировать приложения перед их модернизацией в новый формат? 11

1.4Как модернизировать почтовый интернет сервер R4 до версии R5? 12

1.4.1Как модернизировать сервер, использующий SMTP/MIME Message Transfer Agent (MTA) до версии R5? 13

1.4.1.1Сохранение важных файлов Domino сервера. 13

1.4.1.2Запрещение функции Housekeeping для SMTP/MIME MTA. 13

1.4.1.3Остановка задачи Router. 13

1.4.1.4Остановка подзадачи Inbound. 14

1.4.1.5Обработки сообщений в базе данных SMTP.BOX. 14

1.4.1.6Очистка очереди сообщений на прием (Inbound Work Queue). 14

1.4.1.7Остановка SMTP/MIME MTA и сервера Domino. 15

1.4.1.8Проверка файла NOTES.INI для почтового интернет сервера. 15

1.4.1.9Инсталляция программного обеспечение сервера Domino R5, на сервере MTA. 15

1.4.1.10Замена дизайна базы данных Public Address Book для почтового интернет сервера. 16

1.4.1.11Уплотнение базы данных Domino Directory после замены дизайна. 16

1.4.1.12Восстановление представлений в Domino Directory. 16

1.4.1.13Восстановление представлений в базах данных на модернизированном Domino сервере. 16

1.4.1.14Репликация нового дизайна Domino Directory на другие сервера. 17

1.4.1.15Настройка конфигурации почтового интернет сервера. 17

1.4.1.16Редактирование Server документ для почтового интернет сервера. 18

1.4.2Модернизация базы Administration Requests для MTA сервера. 18

1.4.3Что нового в Domino Directory R5? 19

1.4.3.1Использование профиля настройки для Domino Directory. 19

1.4.3.2Новые и удаленные представления в Domino Directory. 19

1.4.3.3Новые формы в Domino Directory R5. 20

1.4.4Где находятся элементы конфигурирования серверов R4 и их аналоги в R5? 20

1.5Как обновить программного обеспечения рабочей станции Notes R4 до версии R5? 24

1.5.1Что нужно сделать перед модернизацией клиентов Notes R4? 25

1.5.2Как инсталлировать программного обеспечения Notes R5? 25

1.5.3Что происходит с рабочим пространством R4, при обновлении рабочей станции до R5? 26

1.5.4Какие изменения происходят в персональной адресной книге пользователя? 27

1.5.5Что происходит с базой данных Portfolio в Notes R5? 28

1.5.6Можно ли модернизировать мой почтовый файл в формат R5, сразу после установки программного обеспечения Notes R5? 28

1.5.7Что происходит с записями для интернет почты? 28

1.5.8Меняются ли установки защиты рабочей станции, установленные по умолчанию? 28

1.5.9Как происходит синхронизация часового пояса и установка перехода на летнее время в Notes R5? 28

1.5.10Возможно ли использование функций календаря и планирования для интернет почты в Notes R5? 29

1.6Могут ли существовать рабочие станции R4 и R5 на одном компьютере клиента? 29

1.7Как в Notes R5, сделать так, чтобы при старте появлялось рабочая область, а не стартовая страница R5? 30

1.8Что такое QMRs/QMUs? 30

1.8.1После установки QMR или QMU в каталогах сервера и рабочей станции появились файлы с расширением *.IIB. Что это за файлы? 31

1.8.2Что делать, если при установке QMR или QMU возникают ошибки, и процесс обновления останавливается? 31

1.9Как модернизировать базы данных и приложения в новый формат R5? 33

1.9.1Общие принципы модернизации баз данных в новый формат. 34

1.9.2Модернизация баз данных в формат R5. 34

1.9.3Модернизация почтовых файлов пользователей. 34

1.9.4Замена шаблонов на новые версии R5. 37

1.9.5Модернизация приложений для Web. 37

1.9.6Использование шаблонов для Web со старыми браузерами. 38

1.9.7Замена дизайна базы данных Библиотека документов. 38

1.9.8Сохранение баз данных в формате R4. 38

1.9.9Использование функции Transaction logging в Domino R5. 39

2Администрирование серверов Lotus Domino. 41

2.1Какие существуют особенности в администрировании смешанной среды серверов Lotus Domino? 41

2.1.1Особенности маршрутизации интернет почты в смешанной среде серверов. 41

2.1.1.1Конвертирование интернет почты в смешанных средах серверов. 41

2.1.2Шифрованные сообщения в смешанных средах серверов. 44

2.1.3Использование функции Message Tracking в смешанных средах серверов. 44

2.1.4Использование шаблона Domino Directory R5 в смешанной среде серверов. 44

2.1.5Работа сервиса LDAP в смешанных средах серверов. 45

2.1.6Особенности использования кластера серверов в смешанных средах. 45

2.1.7Идентификация пользователей Web сервером в смешанных средах серверов. 45

2.2Какие существуют конфигураций систем, построенные на основе Lotus Domino серверов? 46

2.2.1Что такое иерархическая схема имен организации и для чего она нужна? 46

2.2.1.1Примеры имен серверов и пользователей....46
2.2.2Типы Domino серверов, которые будут использоваться в построении системы. 48
2.2.2.1Использование Hub серверов....48
2.2.2.2Использование почтовых серверов и серверов каталогов....49
2.2.2.3Использование серверов приложений....50
2.2.2.4Использования Passthru сервера. 51
2.2.2.5Законченная конфигурация серверов для организации....51
2.3Как добавить дополнительный Domino сервер в домен?....52
2.3.1Установка и конфигурирование дополнительного Domino сервера....52
2.3.1.1Создание схемы иерархических имен серверов и пользователей....52
2.3.1.2Создание базы данных Certification Log. 55
2.3.2ID Сертификатора....55
2.3.2.1Создание ID сертификатора для Организации. 57
2.3.2.2Создание ID сертификатора для Орг. единицы....58
2.3.3Общий подход к назначению паролей в Domino системе. 59
2.3.4Регистрация и установка дополнительных серверов. 60
2.3.4.1Регистрация дополнительного сервера. 60
2.3.4.2Установка дополнительных портов сервера....62
2.3.5Настройка глобальных параметров администрирования. Установки по умолчанию. 63
2.4Как сконфигурировать Domino сервер, для использования удаленного доступа?....64
2.4.1Типы удаленных соединений 64
2.4.2Соединение с использованием типа соединения Notes Direct Dial-Up. 66
2.4.2.1Планирование топологии с удаленными серверами. 66
2.4.2.2Настройка топологии для использования удаленных серверов. 66
2.4.2.3Пример топологии Acme's для использования удаленных серверов. 67
2.4.2.4Определение количества модемов для удаленного сервера. 68
2.4.2.5Пример топологии компании Acme's для удаленного сервера с использованием модемов. 69
2.4.2.6Настройка портов сервера. 70
2.4.2.7Опции настроек порта. 71
2.4.2.8Командные файлы для модемов. 73
2.4.3Настройка сервера использующего удаленный доступ к сети. 74
2.4.4Passthru сервера и Hunt группы. 75
2.4.4.1Настройки сервера для использования Passthru. 75
2.4.4.2Создание топологии Passthru серверов. 76
2.4.4.3Пример топологии Passthru серверов для компании Acme's. 76
2.4.4.4Настройка Passthru сервера. 78
2.4.4.5Настройка серверов назначений, к которым можно получить доступ с использованием Passthru серверов. 78
2.4.5Настройки сервера для доступа к нему через интернет 79
2.4.5.1Internet Service Providers и соединений по интернет. 79
2.4.5.2Установка программного обеспечения для связи с интернет. 80
2.4.5.3Установка Proxy сервера для соединения с интернет. 80
2.4.5.4Тестирование подключение сети с использованием утилиты PING. 81
2.5Как настроить соединения Domino серверов?....81

2.5.1Как спланировать топологию для серверных подключений? 82
2.5.1.1Использование топологии Hub-and-Spoke. 82
2.5.1.2Использование топологии Peer-to-Peer. 83
2.5.2Процесс соединения сервера с сервером партнером. 84
2.5.3Как создать подключения для сервера? 85
2.5.3.1Подключение для двух серверов с использованием сети LAN. 85
2.5.3.2Подключение для сервера с использованием Direct Dial-Up (Dial-Up Modem). 86
2.5.3.3Подключение для сервера с использованием Network Dial-Up. 87
2.5.3.4Шифрование документа подключения Network Dial-Up. 89
2.5.3.5Подключение для сервера с использованием Passthru. 90
2.5.4Какой приоритет использует Domino, при выборе использования документов подключений? 90
2.5.4.1Соединение Сервер – Сервер, с использованием интернета. 91
2.5.4.2Создание документа подключения для соединения серверов через интернет. 91
2.5.4.3Создание документа подключения для двух серверов, через интернет, с использованием Proxy сервера. 92
2.5.5Как выполнить трассировку сетевого соединения между серверами? 93
2.5.6Для чего используется документ EDNI? 93
2.6Как планировать репликации баз данных? 94
2.6.1Когда именно нужно создавать реплики баз данных? 95
2.6.2Как происходит процесс репликаций между двумя серверами? 95
2.6.2.1Что происходит при репликации между двумя серверами? 96
2.6.3Топология системы репликаций. 97
2.6.3.1Использование топологии репликаций Hub-and-Spoke. 97
2.6.3.2Использование топологии репликаций Peer-to-Peer. 99
2.6.4Документы подключений для репликаций. 99
2.6.4.1Выбор типа направления репликаций. 101
2.6.4.2Расписание репликаций. 102
2.6.4.3Репликация только выбранных баз данных. 104
2.6.4.4Репликации баз данных согласно их приоритетов. 104
2.6.4.5Ограничение времени репликаций. 104
2.6.4.6Использование нескольких репликаторов одновременно 104
2.6.4.7Отклонение запросов на репликации с сервера. 105
2.6.4.8Запрещение репликаций. 106
2.6.4.9Форсирование намеченных репликаций. 106
2.6.5Просмотр расписания репликаций и карты топологии репликаций 106
2.6.6Тестирование репликаций. 108
2.7Настойка функции поиска Domain Search. 108
2.7.1Поиск в домене Domino серверов. 108
2.7.2Разрешение использования функций поиска Domain Search. 110
2.7.3Поиск в системных файлах. 111
2.7.3.1Настройка поиска в системных файлах. 112
2.7.4Включение баз данных в Domain Index. 112
2.7.5Конфигурирование Domain Index. 113

2.7.6Настройка клиентов Notes для использования Domain Search. 113
2.7.7Использование документа - Content Categories. 114
2.7.8Безопасность в Domain Search. 116
2.8Настройка календаря и планирования 117
2.8.1Событие календаря и расписание. 117
2.8.2Настройки календаря 118
2.8.3Создание базы данных ресурсов - Resource Reservations 120
2.8.4Создание документов Site Profile и Resource документы в базе планирования ресурсов 120
2.8.4.1Редактирование и удаление документов ресурсов 122
2.8.5Создание документа Holiday. 123
2.9Конфигурирование Partitioned серверов. 125
2.9.1Partitioned сервера 125
2.9.2Установка и настройка Partitioned серверов. 126
2.9.3Конфигурирование Partitioned серверов. 126
2.9.3.1Назначение отдельных IP адресов Partitioned серверам. 128
2.9.3.2Назначение нескольких IP адресов на один сетевой интерфейс NIC. 129
2.9.3.3Использование одного IP адреса и Port Mapping на Partitioned сервере 129
2.9.3.4Конфигурирование Port Mapping для использования с одним IP адресом. 130
2.9.3.5Пример конфигурации с одним IP адресом и Port Mapping. 131
2.9.4Использование Partitioned серверов в кластере серверов Domino. 131
2.9.5Удаление Partition сервера с компьютера. 133
2.10Настройка процесса администрирования - Administration Process 133
2.10.1Задача Administration Process 134
2.10.2Выбор сервера администрирования для Domino Directory 135
2.10.3Настройка Administration Process 135
2.10.4Выбор сервера администрирования для баз данных 136
2.10.4.1Процесс Administration Requests в различных доменах. 137
2.10.4.2Создание конфигурации Cross-Domain и необходимых для этого документов. 137
2.10.4.3Проверка работы Administration Process. 140
2.10.4.4Настройка ACL для Administration Process. 140
2.10.5База данных Administration Requests. 141
2.10.6Обслуживание запросов администрирования. 142
2.10.6.1Расписание выполнение запросов Administration Request. 143
2.10.6.2Изменение значения нитей для Administration Process. 144
2.10.6.3Создание представления $AdminP. 145
2.11Установка и настройка Web Administrator. 145
2.11.1Web Administrator 145
2.11.2Настройка Web Administrator. 145
2.11.3Установка доступа к базе данных Web Administrator 146

2.11.3.1Дополнительные настройки для доступа к Web Administrator. 147
2.11.4Запуск и настройка Web Administrator 148
2.11.5Использование Web Administrator 149
2.12Установка Domino Web сервера 150
2.12.1Web сервер Domino 150
2.12.1.1Как работает Domino Web сервер? 152
2.12.2Установка Domino Web сервера. 153
2.12.2.1Настройка параметров Domino Web сервера. 153
2.12.3Настройка Web сервера 154
2.12.4Запуск и остановка Domino Web сервера. 156
2.12.5Поддержка нескольких Web серверов. 156
2.12.5.1Настройка поддержки нескольких Web серверов на одном сервере. 157
2.12.5.2Настройка безопасности для виртуальных Web серверов. 159
2.12.6Использование псевдонима для Web сервера. 160
2.12.6.1Настройка безопасности для псевдонимов Web сервера. 161
2.12.7Поддержка Java аппретов. 162
2.12.8Управление Java сервелетами на Web сервере 164
2.12.9Увеличение производительности Web сервера. 166
2.12.9.1Управление Кеш памятью Web сервера. 166
2.12.9.2Настройка сетевого Time-Out для Web сервера. 167
2.12.9.3Установка числа нитей, используемых Domino Web сервером 168
2.12.9.4Оптимизация загрузки файлов Web клиентами. 169
2.12.10 Поиск ссылок для команд Redirect URL. 170
2.12.11 Ограничение данных пользователя, которые посылаются на сервер. 170
2.12.12 Отображение информации Web сервером. 171
2.12.12.1Выбор домашней страницы по умолчанию для Web сервера. 171
2.12.12.2Пример использования домашней страницы по умолчанию. 172
2.12.12.3Выбор формата изображений *.GIF или *.JPEG 173
2.12.12.4Выбор числа строк для отображения представлений на сервере. 174
2.12.13 Настройка сообщений Web сервера. 174
2.12.14 Создание базы данных Domino Configuration. 175
2.12.15 Создание и настройка сообщений Web сервера. 175
2.12.15.1Пример настройки сообщений Web сервера. 176
2.12.16 Выбор набора интернациональных символов для затребованных страниц. 176
2.12.17 Максимально число документов, возвращаемое поиском. 179
2.12.18 Изменение запросов Web URLs, при изменении местоположения, каталогов и файлов Web сервера. 179
2.12.18.1Перенаправление запросов URL для каталогов. 179
2.12.18.1.1Примеры для перенаправления URLs и каталогов 181
2.12.18.2Изменение места хранения файлов HTML, CGI, Icon. 182
2.13Установка и настройка Domino для использования с Microsoft Internet Information Server 183

2.13.1Domino и Microsoft IIS. 183
2.13.2Настройка Domino для использования Microsoft IIS. 184
2.13.2.1Базовые требования для Domino и Microsoft IIS. 184
2.13.2.2Конфигурирование Domino для Microsoft IIS. 184
2.13.2.3Установка опций безопасности Domino для Microsoft IIS. 186
2.14Установка сервиса NNTP. 186
2.14.1Сервис NNTP 186
2.14.2Настройка Domino сервера и сервиса NNTP. 187
2.14.2.1Настройка Server документа, для использования сервиса NNTP. 188
2.14.2.2Контроль доступа на Domino сервер со службой NNTP. 189
2.14.2.3Создание документа подключения для сервера Domino, сервисом NNTP. 189
2.14.2.4Настройка портов по умолчанию для сервера, на котором запущен сервис NNTP. 192
2.14.3Настройка групп новостей. 193
2.14.4Группы новостей. 195
2.14.5Создание и поддержка групп новостей. 195
2.14.5.1Поддержка групп новостей. 195
2.14.5.2Создание групп новостей. 196
2.14.5.3Использование контрольных сообщений для администрирования групп новостей. 197
2.14.5.4Архивирование и удаление статей из групп новостей. 198
2.15Transaction Logging. 199
2.15.1Как работает Transaction logging? 200
2.15.2Установка и настройка Transaction logging. 201
2.15.3Запрещение Transaction logging для некоторых баз данных. 204
2.15.4Расписание резервного копирования для Transaction Login. 205
2.15.5Использование Transaction logging для восстановления. 206
2.16Кластер серверов Lotus Domino. 206
2.16.1Что такое кластер серверов Domino? 206
2.16.1.1Какие выгоды Вы получите от использования кластера серверов? 206
2.16.2Системные требования к кластеру. 207
2.16.3Как работает кластер Domino? 208
2.16.3.1Как работает переадресация запросов в кластере? 208
2.16.3.2Когда происходит переадресация в кластере? 209
2.16.3.3Когда не происходит переадресации в кластере? 211
2.16.3.4Как Domino находит нужную реплику при переадресации? 211
2.16.3.5Как работает балансировка нагрузки в кластере? 212
2.16.4Компоненты кластера. 213
2.16.4.1Cluster Manager. 213
2.16.4.2Cluster Database Directory. 214
2.16.4.3Cluster Database Directory Manager. 214
2.16.5Как работает кластерный репликатор? 215
2.16.6Перенаправление почты в кластере. 216

2.16.7Как работает календарное планирование в кластере? 217
2.16.8Выделенная сеть для кластера, нужно ли это? 217
2.16.9Создание кластера серверов Domino 218
2.16.10 Как убедиться, что кластер создан и работает корректно? 219
2.16.11 Запуск инструмента анализа кластера. 219
2.16.12 Управление доступом пользователей к базам данных. 220
2.16.12.1Поддержка ACL баз данных в кластере. 220
2.16.12.2Управление другими назначениями, которые ограничивают доступ к базам данных. 221
2.16.13 Настройка почты в кластере. 221
2.16.13.1Изменение маршрутизации почты при отказе одного из серверов. 222
2.16.13.2Использование Shared Mail в кластере. 223
2.16.14 Использование стандартного репликатора в кластере. 223
2.16.14.1Реплики по расписанию в кластере 223
2.16.14.2Запрещение кластерных репликаций. 224
2.16.14.3Разрешение протоколирования, для кластерных репликаций. 225
2.16.15 Установка выделенной сети LAN для Вашего кластера 226
2.16.16 Балансировка рабочей нагрузки на кластер 227
2.16.17 Ограничение рабочей нагрузки сервера 228
2.16.18 Индекс готовности сервера 228
2.16.18.1Выбор порога готовности сервера 229
2.16.18.2Настройка порога готовности сервера. 230
2.16.19 Настройка максимального числа пользователей на сервере. 231
2.16.20 Управление состоянием Failover в кластере 231
2.16.21 Управление доступностью баз данных в кластере. 233
2.16.21.1Установка атрибута - Out of Service, для баз данных 233
2.16.21.2Установка атрибута - In Service, для баз данных. 234
2.16.22 Использование кластера Domino серверов в интернете. 234
2.16.22.1Как работает Internet Cluster Manager? 234
2.16.22.2Генерирование URLs, при использовании ICM. 236
2.16.22.3Конфигурирование ICM 236
2.16.22.3.1Определение выделенного IP адреса для ICM 238
2.16.22.3.2Запуск ICM 239
2.16.22.4Failover и балансирование рабочей нагрузки на сервера. 240
2.16.22.5Безопасность. 241
2.16.22.6Управление и контроль ICM. 241
2.16.22.7Совместимость с предыдущими версиями серверов Domino. 241
2.17Команды Domino сервера. 242
2.17.1Ввод команд сервера 242
2.17.1.1Ввод команды с консоли сервера. 242
2.17.1.2Ввод команд сервера с использованием Domino Administrator. 243
2.17.1.3Запуск Batch-файла на консоли сервера. 243
2.17.1.4Вывод ответа команды сервера в файл. 243

2.17.2Команды Domino сервера. 244
2.17.2.1Broadcast 244
2.17.2.2Dbcache Flush 244
2.17.2.3Drop 244
2.17.2.4Exit 244
2.17.2.5Help 244
2.17.2.6Load 244
2.17.2.7Pull 244
2.17.2.8Push 245
2.17.2.9Quit 245
2.17.2.10Replicate 245
2.17.2.11Restart 246
2.17.2.12Route 246
2.17.2.13Set Configuration 246
2.17.2.14Set Secure 246
2.17.2.15Show Allports 247
2.17.2.16Show Cluster 247
2.17.2.17Show Configuration 247
2.17.2.18Show Directory 247
2.17.2.19Show Diskspace 247
2.17.2.20Show Memory 247
2.17.2.21Show Port 247
2.17.2.22Show Schedule 248
2.17.2.23Show Server 248
2.17.2.24Show Stat 248
2.17.2.25Show Tasks 248
2.17.2.26Show Users 248
2.17.2.27Start Port 248
2.17.2.28Stop Port 248
2.17.2.29Tell 249
2.17.2.30Trace 255
2.18Задачи сервера. 255

3Администрирование пользователей и групп. 257

3.1Пользователи Notes. 257
3.1.1Определение установок по умолчанию для пользователей. 257
3.1.2Что такое - профиль установки пользователя? 258
3.1.3Что такое ECL рабочей станции? 259
3.1.3.1Пример ECL. 259
3.1.3.2Создание ECL для рабочей станции. 260
3.1.4Процесс регистрации пользователей. 261
3.1.5Методы регистрации пользователей. 263
3.1.5.1Использование Базовой регистрации пользователей. 264
3.1.5.2Использование выборочной регистрации пользователей. 265
3.1.5.3Регистрация пользователей из текстового файла. 271

3.1.6Для чего используются группы? 273
3.1.6.1Создание и модификация групп 274
3.1.7Как добавить альтернативный язык и альтернативное имя пользователю? 274
3.1.7.1Как добавить альтернативное имя – ID сертификатору? 275
3.1.7.2Как добавить Альтернативное имя конечному пользователю? 276
3.1.7.3Как добавить альтернативное имя при регистрации нового пользователя? 278
3.2Как выполнить миграцию пользователей из WindowsNT домена в Notes? 278
3.2.1Выбор WindowsNT домена, для импорта пользователей в Notes 278
3.2.2Импортирование пользователей WindowsNT для регистрации в Notes 279
3.2.3Настройка опций миграции для пользователей WindowsNT 280
3.2.4Выбор способа конвертирования поля Full Names пользователя WindowsNT в Notes имя пользователя 280
3.2.5Создание короткого имени Notes (Short Names) для пользователей WindowsNT. 282
3.2.6Регистрация пользователей и завершение миграции из WindowsNT. 282
3.3Как использовать WindowsNT User Manager для управления пользователями Domino сервера? 283
3.3.0.1Синхронизация пользователей и групп Domino и WindowsNT 284
3.3.0.2Разрешение операции синхронизации Notes и WindowsNT User Manager. 284
3.3.1Синхронизация пользователей WindowsNT и Notes пользователей. 285
3.3.2Использование WindowsNT User Manager, для домена Domino. 286
3.3.3Изменение установок регистрации Notes для WindowsNT пользователей. 287
3.3.4Использование WindowsNT для создания экаунта пользователя и регистрация Notes пользователя. 292
3.3.5Регистрация существующих экаунтов пользователей WindowsNT в Notes. 294
3.3.6Добавление WindowsNT групп в Notes 294
3.3.7Использование WindowsNT User Manager для удаления групп пользователей 295
3.4Управление пользователями, серверами и группами. 296
3.4.1Управление пользователями. 296
3.4.1.1Изменение имени Notes пользователя с использованием Administration Process. 297
3.4.1.2Как изменить общее имя пользователя? 297
3.4.1.3Как переместить имя пользователя в иерархии имен? 298
3.4.1.4Как преобразовать простые имена пользователей - в иерархические? 298
3.4.1.5Как удалить имя пользователей из Domino системы? 299
3.4.1.6Ресертификация ID пользователя. 301
3.4.1.7Как перенести почтовый файла пользователя на другой сервер, или в другой каталог? 301
3.4.2Управление серверами. 302
3.4.2.1Как изменить имя администратора сервера? 302
3.4.2.2Сравнивание серверов (Decommissioning a server) 303
3.4.2.3Как удалить имя сервера из Domino системы? 308
3.4.2.4Ресертификация ID файла сервера. 309
3.4.2.5Преобразование простого имени (Flat Name) сервера - в иерархическое 310
3.4.3Использование инструмента управления группами. 310

4Почтовая система Domino сервера. 312

4.1Обзор возможностей. 312

4.1.1Передача сообщений и протоколы доступа к почте. 313

4.1.2Как передаются сообщения в системе Domino? 314

4.1.3Domino Directory и маршрутизация почты. 315

4.1.4Domain Name Service (DNS) и маршрутизация почты. 316

4.1.4.1Примеры использования нескольких записей MX records. 317

4.2Почтовая адресация в версии R5. 318

4.2.1Поля Address Internet в Person документах. 318

4.2.1.1Как форматируется Адрес интернета? 319

4.2.2Выбор формата интернет адреса для Вашей организации 320

4.2.3Формирование нестандартного интернет адреса. 321

4.2.4Проверка интернет адреса на уникальность. 322

4.3Какой тип маршрутизации почты выбрать и как ее настроить? 323

4.3.1Планирование топологии почтовой маршрутизации. 323

4.3.1.1Какие типы почтовых клиентов поддерживает сервер Domino? 323

4.3.1.2Маршрутизация внутренней почты. 324

4.3.1.3Маршрутизация внешней почты. 325

4.3.2Какие конфигурации можно использовать для маршрутизации почты? 326

4.3.2.1Использование одного сервера для всех рассылки и получения почтовых сообщений интернета. 326

4.3.2.2Использование одного сервера для отправки и одного сервера для принятия интернет сообщений. 327

4.3.2.3Использование двух серверов для сбалансирования нагрузки интернет почты. 328

4.3.2.4Маршрутизация почты в локальном интернет домене. 330

4.3.2.5Маршрутизация почты с использованием Third-Party сервера и внутреннего интернет домена серверов Domino. 331

4.3.2.6Использование Smart Host. 332

4.3.2.7Использование всеми серверами маршрутизации исходящей интернет почты. 333

4.3.3Для чего используется документ Configuration Settings? 334

4.3.4Настройка Notes маршрутизации. 335

4.3.4.1Создание документа Adjacent Domain. 337

4.3.4.2Создание документа Non-Adjacent Domain. 337

4.3.4.3Создание документа Foreign domain. 338

4.3.4.4Создание документа Foreign SMTP domain. 339

4.3.4.5Создание документа SMTP Connection. 340

4.3.5Настройка SMTP маршрутизации. 340

4.3.5.1Настройка получения и отправки интернет почты 340

4.3.5.2Настройка SMTP маршрутизации во внешние интернет домены из локального интернет домена. 341

4.3.5.3Настройка SMTP маршрутизации в пределах локального интернет домена. 341

4.3.5.4Настройка серверов для получения почты посланной с использованием SMTP маршрутизации. 342

4.3.6Настройка решения адресов. 343

4.3.6.1Настройка опции Forwarding Address. 343

4.3.6.2Настройка опции Smart Host. 343

4.3.6.3Использование нескольких имен интернет доменов в одной организации. 344
4.3.6.4Способы поиска адреса в Person документах пользователей 345
4.3.6.5Настройка Router, для разрешения IP адреса SMTP сервера назначения. 346
4.3.7Настройки Relay Host или Firewall. 347
4.3.8Настройка передачи сообщений с использованием Dial-Up connection. 347
4.4Настройка почтовой системы Domino. 349
4.4.1Настройка почты. 349
4.4.2Требование для работы почтовой системы. 349
4.4.3Настройка системы передачи сообщений 350
4.4.3.1Оптимизация настроек Вашей почтовой системы. 351
4.4.3.1.1Создать несколько баз данных MAIL.BOX. 351
4.4.3.1.2Запрещение автоматического поиска адреса, основанного на вводе нескольких символов адреса. 352
4.4.4Запись дополнительной информации относительно передачи почты в файл LOG.NSF 352
4.4.5Временное запрещение маршрутизации почты. 353
4.4.6Настройка маршрутизации Notes почты. 353
4.4.6.1Расписание маршрутизации почты Notes. 354
4.4.6.2Изменение стоимости маршрутизации подключений между Domino серверами. 355
4.4.6.3Маршрутизация сообщений согласно приоритета. 357
4.4.7Контроль передачи сообщений. 357
4.4.7.1Ограничения размера почтовых сообщений пользователей. 357
4.4.7.2Настройка контроля передачи сообщений. 358
4.4.7.3Настройка дополнительных параметров передачи сообщений. 359
4.4.7.4Настройка текстовых сообщений при сбое в доставки почты. 361
4.4.8Ограничения маршрутизации входящей почты. 363
4.4.8.1Ограничения для входящих SMTP соединений. 364
4.4.8.2Настройка ограничения для Вашего сервера, при передаче почты через него (ограничение использования Relay). 365
4.4.8.3Ограничения базовой маршрутизации почты Notes доменов для организации и Орг. Единиц. 367
4.4.8.4Ограничения по отправителям интернет почты, для Ваших пользователей. 369
4.4.8.5Ограничение на то, кто может получать почту из интернета из Вашей Организации. 370
4.4.8.6Поддержка расширений SMTP для входящих сессий. 371
4.4.9Ограничения для исходящих сообщений сервера. 373
4.4.9.1Ограничения на рассылку почты в интернет. 373
4.4.9.2Поддержка исходящих SMTP расширений. 374
4.4.10 Конфигурирование опций доставки сообщений. 375
4.4.10.1Настройка опций доставки сообщений. 375
4.4.10.2Ограничения маршрутизации почты базирующейся на квотах баз данных. 376
4.5Использование Shared Mail. 377
4.5.1Как работает Shared Mail? 378
4.5.2Как установить Shared Mail? 378
4.5.2.1Создание и активация базы данных Shared Mail. 378
4.5.2.2Создание и разрешение использования дополнительной базы данных Shared Mail. 379
4.5.3Управление базой данных Shared Mail. 379

4.5.3.1Связывание (Linking) почтовых файлов с базой данных Shared Mail. 379
4.5.3.2Включение или исключение почтового файла в базу данных Shared Mail. 380
4.5.3.3Очистка устаревших сообщений в базе данных Shared Mail. 381
4.5.3.4Восстановление базы данных Shared Mail. 382
4.5.3.5Удаление базы данных Shared Mail. 382
4.6Использование сервиса POP3 на Domino сервере. 383
4.6.1Установка сервиса POP3 на Domino сервере. 383
4.6.1.1Запуск и остановка сервиса POP3. 384
4.6.1.2Изменение значения порта, для задачи POP3. 384
4.6.2Настройки для пользователей POP3. 385
4.6.2.1Установки в Person документах, для POP3 пользователей 385
4.6.2.2Создание почтового файла для пользователя POP3. 386
4.6.2.3Конфигурирование программного обеспечения клиента POP3. 387
4.7Установка сервиса IMAP. 387
4.7.1Сервис IMAP. 387
4.7.2Установки сервиса IMAP. 388
4.7.2.1Запуск и остановка задачи IMAP. 388
4.7.2.2Изменение значения порта по умолчанию, для задачи IMAP. 389
4.7.3Настройки для пользователей IMAP. 389
4.7.3.1Настройки Person документов, для пользователей IMAP. 389
4.7.3.2Создание почтового файла для пользователя IMAP вручную. 390
4.7.3.3Конвертирование почтового файла IMAP. 391
5Каталог Domino сервера. База данных Domino Directory. 393
5.1Domino Directory. 393
5.1.1Настройки Domino Directory для домена Notes. 394
5.1.1.1Настройка ACL для Domino Directory. 394
5.1.1.2Расписание репликаций для базы данных Domino Directory. 396
5.1.1.3Использование профиля для Domino Directory. 396
5.1.2Оптимизация производительности Domino Directory. 397
5.2Использование нескольких Domino Directories. 398
5.2.0.1Как планировать использование нескольких Domino Directory. 398
5.2.0.2Как Domino просматривает Domino Directories при поиске. 400
5.3Directory Catalogs. 401
5.3.0.1Mobile Directory Catalog. 402
5.3.0.1.1Пример использования Mobile Directory Catalog. 403
5.3.0.2Server Directory Catalog. 403
5.3.0.3Настройка Directory Catalog. 404
5.3.0.3.1Подготовка сервера к построению первичного Directory Catalogs. 404
5.3.0.3.2Настройки первичного Directory Catalog. 405
5.3.0.3.3Построение и модернизация первичного Directory Catalogs. 408
5.3.0.4Настройка использования Directory Catalog на серверах. 409
5.3.0.5Настройки Mobile Directory Catalog. 410

5.3.0.5.1Настройка расписания для запуска задачи обновления Directory Catalogs. 411
5.3.0.5.2Добавление и удаление полей из Directory Catalog. 411
5.3.0.5.3Оптимизация производительности Directory Catalog. 412
5.3.0.6Мониторинг Directory Catalogs. 413
5.4Настройка сервиса LDAP. 414
5.4.1Как сервис LDAP обрабатывает запросы поиска интернет адреса. 415
5.4.2Установка сервиса LDAP. 415
5.4.2.1Запуск и остановка сервиса LDAP. 416
5.4.2.2Настройка пользователей для использования сервиса LDAP. 416
5.4.3Оптимизирование настроек сервиса LDAP. 417
5.4.3.1Конфигурирование полей для анонимного доступа LDAP сервиса. 418
5.4.3.2Оптимизация поиска LDAP. 420
5.4.3.3Как можно изменять и настраивать процесс поиска LDAP сервиса. 421
5.4.3.4Настройка действий LDAP сервиса, при нахождении имен дубликатов в документах и в правилах обработки имен из Directory Assistance. 422
5.4.3.5Разрешение поиска с использованием Alternate Language. 422
5.4.3.6Изменение значения порта сервиса LDAP и его конфигурирование. 424
5.4.4Мониторинг сервиса LDAP. 425
5.5Directory Assistance. 426
5.5.1Вторичные Domino Directories и Directory Assistance. 426
5.5.1.1Сервер Directory Catalog и Directory Assistance. 426
5.5.1.2Идентификация Web клиентов во вторичных Domino Directory. 427
5.5.1.2.1Пример. Как сервер просматривает пароль Web клиента, с использованием Directory Catalog. 427
5.5.1.2.2Пример просмотра сертификата Web клиента, во вторичном Domino Directory. 429
5.5.1.3Поиск LDAP, во вторичных Domino Directory. 430
5.5.1.3.1Пример расширенного поиска LDAP во вторичных Domino Directory. 430
5.5.1.4Проверка адреса Notes во вторичных Domino Directory. 431
5.5.2Разрешение поиска в LDAP Directories из Directory Assistance. 432
5.5.2.1Идентификация Web клиентов из LDAP Directory. 432
5.5.2.1.1Пример использования LDAP Directory для идентификации Web клиентов 432
5.5.2.2Использование групп пользователей с LDAP Directory. 433
5.5.3Правила обработки имен в Directory Assistance. 434
5.5.4Порядок поиска в Directory Assistance. 435
5.5.5Создание базы данных Directory Assistance. 436
5.5.5.1Идентификация базы данных Directory Assistance на серверах. 436
5.5.6 Настройка Directory Assistance, для использования вторичных Domino Directory. 437
5.5.6.1Планирование места хранения реплик вторичных Domino Directory. 437
5.5.6.2Разрешение доступа к Domino Directory. 437
5.5.6.3Создание документа Directory Assistance для вторичного Domino Directory. 438
5.5.7 Настройка Directory Assistance для LDAP Directory. 440
5.5.7.1Идентификация Web клиентов с использованием LDAP Directory. 440
5.5.7.2Идентификация пользователей в группах из LDAP Directory. 442
5.5.7.3Использование SSL в установках Directory assistance для LDAP Directory. 442
5.5.8 Каскадные Domino Directory. 444

5.5.9 Сервер Каталогов ... 446

5.5.9.1Конфигурируйте сервер каталога для Notes пользователей. ... 446

6Безопасность и контроль доступа на Domino сервера. ... 447

6.1Защита ID файлов и работа с ними. ... 447

6.1.1Сертификаты. ... 447

6.1.2Просмотр сертификатов ID файла. ... 448

6.1.3Защита ID файлов Notes и Domino серверов паролем. ... 449

6.1.3.1Особенности защиты паролем. ... 449

6.1.4Проверка пароля пользователя при идентификации пользователя. ... 451

6.1.4.1Установка проверки пароля. ... 452

6.1.5Назначение нескольких паролей для ID сервера или сертификатора. ... 454

6.1.6Восстановление пароля ID файла. ... 455

6.1.6.1Как работает функция восстановления ID файла? ... 456

6.1.6.2Настройки необходимые для восстановления пароля ID файлов. ... 457

6.1.6.3Подготовка к восстановлению ID файлов ... 458

6.1.6.4Восстановление пароля для ID файла. ... 460

6.1.6.5Изменение информации об администраторах, для восстановления ID файла ... 462

6.1.7Безопасность публичного ключа. ... 463

6.1.7.1Создание нового публичного ключа Notes и добавление его в Domino Directory. ... 464

6.1.7.2Добавление публичного ключа Notes в Domino Directory ... 465

6.1.7.3Использование взаимных сертификатов серверов и рассылки подписанных S/MIME сообщений. ... 466

6.1.8Примеры применения взаимных сертификатов ... 468

6.1.8.1Как добавить, затребованный взаимный сертификат интернет или Notes? ... 469

6.1.8.2Как добавить взаимный сертификат Domino по телефону? ... 470

6.1.8.3Как добавить взаимный сертификат Domino для ID файлов, используя для этого почту? ... 472

6.1.8.4Как добавить взаимный сертификат Domino для ID, используя почту Notes? ... 473

6.1.8.5Как добавить взаимный сертификат интернета от интернет сервера? ... 473

6.1.8.6Создание взаимного сертификата для пользователя из Person документа. ... 474

6.1.9 Просмотр взаимных сертификатов. ... 475

6.2Шифрование и электронная подпись ... 475

6.2.1Шифрование. ... 475

6.2.1.1Публичные и личные ключи шифрования. ... 476

6.2.2Шифрование почты. ... 476

6.2.2.1Как работает шифрование исходящей почты Notes? ... 477

6.2.2.2Как работает шифрование исходящей почты S/MIME? ... 477

6.2.3Шифрование почтовых сообщений. ... 478

6.2.4Шифрование данных при передаче по порту сервера. ... 479

6.2.5Электронная подпись. ... 480

6.2.5.1Как работает электронная подпись? ... 480

6.3Установка серверов Firewalls. ... 481

6.3.1Firewalls. ... 481

6.3.2Использование Domino сервера в качестве сервера Firewall. 483
6.3.2.1Использование двух сетевых адаптеров для Domino Passthru сервера. 484
6.3.3Использование Proxy HTTP как Proxy приложение Firewall. 485
6.3.4Использование SMTP Router и SMTP Listener как Proxy приложение Firewall. 486
6.3.5Circuit-Level Proxy Firewalls 486
6.3.5.1Конфигурирование рабочей станции Notes и Domino сервера для соединения с интернет. 487
6.4Установки Domino Certificate Authority. 488
6.4.1Domino Certificate Authority. 488
6.4.2Настройка сервера Domino CA. 489
6.4.2.1Создание приложения Domino Certificate Authority. 489
6.4.2.2Создание файла Key Ring и сертификата CA 490
6.4.2.3Конфигурирование профиля приложения Domino Certificate Authority. 491
6.4.2.4Настройка SSL для сервера CA. 492
6.4.3Просмотр файла Key Ring 493
6.4.4Экспорт файла CA Key Ring 494
6.5Определение доступа на Domino сервер с использованием имени и пароля, анонимный доступ. 494
6.5.1Идентификация для пользователей интернет / интранет, с использованием имени и пароля 494
6.5.1.1Идентификация Web клиентов, с использованием имени и пароля, основанное на сессиях клиентов 495
6.5.1.1.1Настройка сессий основанной идентификации с использованием имени и пароля. 496
6.5.1.2Настройка базовой идентификации Web клиентов, с использованием имени и пароля. 498
6.5.1.3Контроль уровня доступа для Web клиентов. 499
6.5.1.4Примеры использования имен для идентификации Web клиентов, с использованием ограничений 500
6.5.2Идентификация Web клиентов, с использованием имени и пароля, во вторичных Domino Directory и LDAP Directory. 502
6.5.3Обеспечение дополнительной безопасности для пароля интернета. 502
6.5.4Анонимный доступ для пользователей интернет / интранет. 503
6.5.4.1Настройка анонимного доступа для клиентов интернет / интранет. 503
6.5.5Скрытие списка баз данных сервера для Web клиентов. 504
6.5.6Validation и Authentication, для интернет / интранет клиентов. 504
6.6Настройка SSL на сервере Domino. 505
6.6.1SSL безопасность. 505
6.6.2Настройка SSL на сервере Domino. 506
6.6.2.1Установка приложения Server Certificate Admin. 507
6.6.2.2Создание файла сервера Key Ring. 507
6.6.2.3Запрос SSL сертификата сервера. 508
6.6.2.4Как получить сертификат CA, слить его в Key Ring файл как Trusted Root сертификат. 510
6.6.2.5Сертификаты Domino SSL trusted roots, установленные по умолчанию. 512
6.6.2.6Подпись сертификата сервера. 513
6.6.2.7Как слить подписанный сертификат сервера в файл Key Ring. 514
6.6.2.8Конфигурирование порта SSL 515
6.6.2.8.1Конфигурирование порта для использования SSL. 516

6.6.3Требование установки SSL связи, с сервером. 518
6.6.4Настройка доступа к базам данных для SSL клиентов. 519
6.6.5Управление сертификатами сервера и запросами на выдачу сертификатов. 519
6.6.5.1Просмотр SSL сертификатов сервера. 519
6.6.5.2Работа с просроченными сертификатами. 520
6.6.5.3Просмотр запросов для сертификатов. 520
6.6.5.4Как установить или отменить доверие CA сертификату Trusted Root. 520
6.6.5.5Изменение пароля файла Key Ring сервера. 521
6.6.6Создание безопасного сертификата для тестирования SSL сертификации. 521
6.6.7SSL в международных организациях. 522
6.6.8Изменение спецификации шифра SSL. 523
6.6.9Установление подлинности и идентификация для SSL. 524
6.7Настройка клиентов для использования S/MIME и SSL. 525
6.7.1SSL и S/MIME для клиентов. 525
6.7.2Установки Notes и интернет клиентов, для SSL идентификации сервером. 527
6.7.2.1Получение Trusted Root сертификата для SSL идентифицикации сервером. 527
6.7.2.2Создание взаимных сертификатов интернет для CA. 528
6.7.3Установка клиентов Notes для S/MIME. 529
6.7.4Настройка Notes и интернет клиентов для SSL идентификации клиентов. 530
6.7.4.1Как добавить интернет сертификат в Person документ. 531
6.7.4.2Создание Person документа, для клиентов интернет, с использованием SSL идентификации клиента. 532
6.7.4.3Запрос интернет сертификата для SSL и S/MIME. 533
6.7.4.4Подпись интернет сертификата и добавление сертификата в Domino Directory. 535
6.7.4.5Как слить интернет сертификат. 539
6.7.5Установка SSL для Notes или Domino с использованием SMTP. 540
6.7.6Использование SSL с Directory Assistance, для LDAP Directory. 541
6.7.7Просмотр и удаление интернет сертификатов. 541
7Проблемы ошибки, возникающие при работе Domino систем, их решения. 543
7.0.1Инструменты для диагностики и решения проблем. 543
7.0.2Использование русских букв в Notes. 545
7.0.2.1Использование в Lotus Notes однобайтовой и двухбайтовой кодировок. 545
7.0.2.2Русские буквы на консоли Domino Administrator. 545
7.0.3Проблемы с процессом администрирования. 546
7.0.3.1Как искать проблемы связанные с процессом администрирования. 546
7.0.3.2Process Administration – проблемы и сообщения об ошибках. 546
7.1Проблемы с агентами и Agent Manager. 548
7.1.1Инструменты, применяемые при проблемах с агентами и Agent Manager. 548
7.1.2Agent manager и агенты – проблемы и сообщения об ошибках. 549
7.1.2.1Agent Manager не работает, как ожидалось. 549
7.1.2.2Агент не запускается, как ожидалось. 550

7.1.2.3Агент запускается, но не завершает свою работу. 550
7.1.2.4Агент не запускается в назначенное время. 551
7.1.2.5Escrow агент не работает. 551
7.1.2.6Пользователь не может создать агента. 552
7.2Продлеммы с Domino Directories, Directory Catalog, Directory Assistance. 552
7.2.1Directory Assistance – проблемы и сообщения об ошибках. 552
7.2.2Directory catalog – проблемы и сообщения об ошибках. 552
7.2.3LDAP service – проблемы и сообщения об ошибках. 553
7.3Проблемы с маршрутизацией почты. 554
7.3.1Инструменты для решения проблем с маршрутизацией почты. 554
7.3.2Проблемы с маршрутизацией почты и сообщения об ошибках. 556
7.3.2.1Пользователь не может получать любую почту, включая почту, посланную пользователями, чьи почтовые файлы находятся на том же самом сервере. 556
7.3.2.2Пользователи получают сообщение – File is in use by another process. 556
7.3.2.3Пользователи получают сообщение, при попытке отослать почту, на том же самом почтовом сервере - NAMES.NSF does not contain a required view. 556
7.3.2.4Пользователи получают сообщение – No route found to Domain x from Server y. 556
7.3.2.5На консоли сервера появляется сообщение – Router: Possibly no DOMAIN set. 556
7.3.2.6Пользователи получают сообщение – Server Error: File Does Not Exist. 557
7.3.2.7Пользователи получают сообщение – User name is not unique. 557
7.3.2.8Пользователи получают сообщение – User not listed in the Public Address Book. 557
7.3.2.9Если приходится добавлять к адресу получателя - @domainname, для нормальной доставки сообщений пользователям другого домена. 557
7.3.3Как локализовать проблемы с маршрутизацией почты. 557
7.3.3.1Проверка Domino Directory на наличие ошибок в настройках почты. 558
7.3.3.2Проверка рабочих станций отправителя и или получателя на предмет ошибок настройки почты. 559
7.3.3.3Проверка сервера на предмет наличия ошибок работы с почтой. 559
7.3.3.4Проверка настройки Shared Mail. 560
7.4Проблемы с планированием встреч и резервированием ресурсов. 561
7.4.1Информация о свободном времени пользователя недоступна. 561
7.4.2Пользователь получает сообщение - Can't Find User in Name and Address Book. 561
7.4.3Пользователь получает сообщение – Cannot perform this action locally. 562
7.4.4Пользователь получает сообщение – No resource/room found for time and/or capacity requirements. 562
7.5Проблемы с модемом и удаленными соединениями. 562
7.5.1Инструменты для диагностики и решения проблем с модемом и удаленными соединениями. 562
7.5.2Как локализовать проблему с модемом или удаленным соединением? 562
7.5.3Проблемы и сообщения об ошибках, при использовании модемов и удаленных соединений. 564
7.5.3.1Данные не передаются между двумя серверами, соединенными Null-Modem кабелем. 564
7.5.3.2Dial-Up сервер не может инициализировать модем, или синхронизировать его с удаленным модемом. 564
7.5.3.3Игнорирование значений команд в командном файле модема. 564
7.6Проблемы с соединениями - Network Dial-Up. 564
7.7Проблемы с Partitioned серверами. 565

7.7.1Крушение Partitioned серверов. ... 565
7.7.2Пользователь получает сообщение – Server exiting: partition number xx is already in use. ... 565
7.7.3Пользователь получает сообщение – Server not responding connecting to a partitioned server. ... 565
7.8Проблемы с Passthru соединениями. ... 566
7.9Проблемы с репликациями. ... 567
7.9.1Инструменты для локализации проблем с репликациями. ... 567
7.9.2Проблемы с репликациями и сообщения об ошибках. ... 568
7.9.2.1Два сервера не могут реплицировать любые базы данных. ... 568
7.9.2.2Намеченные репликации не происходят между двумя серверами. ... 568
7.9.2.3Одна из баз данных не реплицируется между двумя серверами. ... 569
7.10Проблемы с доступом на сервер. ... 570
7.10.1Администратор не может ввести команды на консоли сервера. ... 570
7.10.2Пользователи не могут видеть новые сервера и просматривать списки серверов. ... 570
7.10.3Сообщение – Server not responding. ... 570
7.10.4Пользователь или сервер получают сообщение – You are not authorized to access the server или подобные сообщения. ... 571
7.10.5Проверка Domino Directory при проблемах с доступом на сервер. ... 571
7.10.6Проверка ID сервера, при проблемах с доступом на сервер. ... 573
7.10.7Замена ID сервера. ... 573
7.10.8Копирование публичного ключа. ... 573
7.11Проблемы, вызывающие крушение сервера. ... 573
7.11.1Что делать при крушении сервера. ... 574
7.11.2Крушение сервера – проблемы и сообщения об ошибках. ... 575
7.11.2.1Разрушение базы данных вызывает крушение сервера. ... 575
7.11.2.2Разрушение представления вызывает крушение сервера. ... 575
7.11.2.3Обновление индекса базы данных вызывает крушение сервера. ... 575
7.11.2.4Задача Router вызывает крушение сервера. ... 576
7.11.3Файлы NOTES.RIP и UNIX CORE. ... 576
7.12Проблемы с Transaction logging. ... 576
7.13Web сервер – проблемы и сообщения об ошибках. ... 577
7.13.1IIS останавливается при старте Domino. ... 578
7.13.2Многократный ввод имени и пароля, для доступа пользователей на Web сервер. ... 578
7.13.3Пользователи не могут получить доступ к Domino Web серверу с использованием интернета. ... 578
7.13.4Пользователи не могут просматривать список баз данных на Web сервере или не могут получить доступ к базе данных. ... 578
7.13.5Пользователь получает сообщение – Error 403 - Directory Browsing error - Access forbidden. ... 579
7.14Web Administrator – проблемы и сообщения об ошибках. ... 579
7.14.1Использование Web Administrator с браузером Netscape ... 579

7.14.2Пользователь получает сообщение – A Java or script error, при старте Web Administrator. 579
7.14.3Web Administrator не показывает корректно Web страницы. 579
7.14.4Пользователь не может получить доступ к базе данных Web Administrator. 579
7.14.5Некоторые команды Web Administrator недоступны. 580