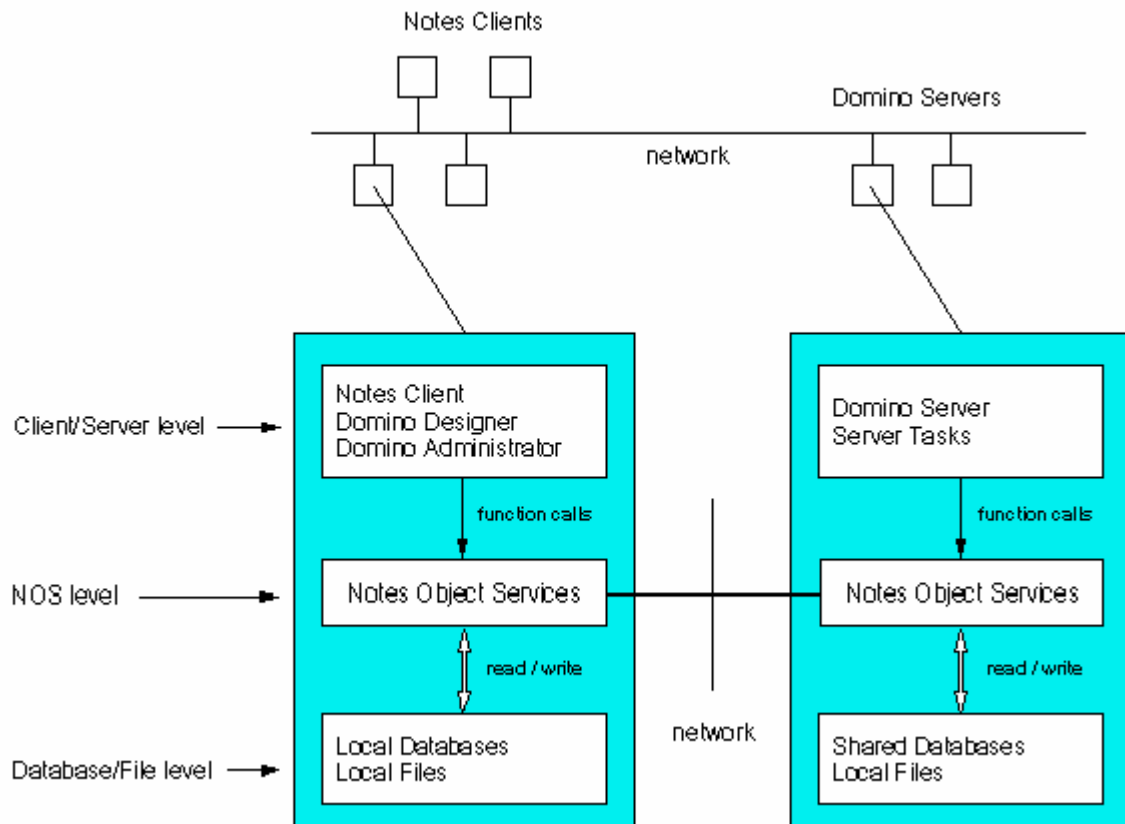


1.1. 1.1. Архитектура и компоненты Notes/Domino



1.2. Рис. 11.1. Функциональность сервера Domino

- • «Несет» базы и предоставляет их в совместное использование клиентам
- • Выполняет агентов
- • Выполняет репликации баз между серверами
- • Занимается передачей почты по протоколам Notes RPC и SMTP
- • «Несет» HTTP Server, что позволяет пользователям работать с базами броузером (включая iNotes, именуемый Domino Web Access с версии 6.5)
- • Поддерживает протоколы POP3, IMAP, LDAP...
- • Поддерживает протокол IIOP (CORBA), что позволяет Java-приложениям удаленно работать с объектами на сервере Domino
- • Позволяет обмениваться информацией между базами Notes и реляционными базами (DECS)
- • Реализует функции обеспечения безопасности (идентификация, авторизация, доступ...)

1.3. 1.1. Платформы для серверов и клиентов, требования к платформам

В дистрибутиве каждой версии имеется база help/readme.nsf с названием наподобие «Lotus Notes/Domino 6.5 Release Notes» или соответствующий файл readme.pdf. Там всегда содержится документ с соответствующей информацией, а так же многочисленные уточнения и дополнения.

Для Notes and Domino 6.5 platforms and system requirements следующие.

1.3.1. 1.1.1. Notes Client

Platform	Windows 95/98	Windows 2000/ Windows XP	Macintosh	Windows NT
Supported operating system versions	Windows 95 (2nd edition installer minimum); Windows 98 (see the "Windows service pack requirements" Release Note for Service Pack information)	Windows 2000 Professional; Windows XP Professional (see the "Windows service pack requirements" Release Note for Service Pack information)	Macintosh OS 10.1.x; Macintosh OS 10.2.x	Windows NT4 (see the "Windows service pack requirements" Release Note for Service Pack information)
Processors supported	Intel Pentium	Intel Pentium	Power PC	Intel Pentium
RAM	64 MB minimum 128 MB or more recommended	128 MB minimum 256 MB or more recommended	128 MB minimum 256 MB or more recommended	64 MB minimum 128 MB or more recommended
Disk space (The minimum amounts are the disk space required for installing default files. More disk space is required if databases are replicated locally or copied locally)	275 MB required	275 MB required	(OS 10) 250 MB required	275 MB required
Monitors supported	Color monitor required	Color monitor required	Color monitor required, 256 colors or greater.	Color monitor required
Protocols supported				
NetBEUI/NetBIOS ⁽¹⁾	Yes	Yes (Windows 2000) No NetBEUI (Windows XP)	No	Yes
NetBIOS over IP ⁽²⁾	Yes	Yes	No	Yes
NetBIOS over IPX	Yes ⁽³⁾	Yes ⁽³⁾	No	Yes
SPX	Yes	Yes	No	Yes
SPX II	No	No	No	Yes ⁽⁴⁾
TCP/IP	Yes	Yes	Yes	Yes
X.PC	Yes	Yes	Yes	Yes

1.3.2. 1.1.2. Domino Administrator Client

Platform	Windows 98	Windows 2000/ Windows XP	Windows NT
Supported operating system versions	Windows 98 (see the "Windows service pack requirements" Release Note for Service Pack information)	Windows 2000 Professional; Windows XP Professional (see the "Windows service pack requirements" Release Note for Service Pack information)	Windows NT4 (see the "Windows service pack requirements" Release Note for Service Pack information)
Processors supported	Intel Pentium	Intel Pentium	Intel Pentium
RAM	64 MB minimum 256 MB or more recommended	128 MB minimum 256 MB or more recommended	64 MB minimum 256 MB or more recommended
Disk space (The minimum amounts are the disk space required for installing default files. More disk space is required if databases are replicated locally or copied locally)	275 MB required	275 MB required	275 MB required
Monitors supported	Color monitor required	Color monitor required	Color monitor required
Protocols supported			
NetBEUI/NetBIOS ⁽¹⁾	Yes	Yes (Windows 2000) No NetBEUI (Windows XP)	Yes
NetBIOS over IP ⁽²⁾	Yes	Yes	Yes
NetBIOS over IPX	Yes ⁽³⁾	Yes ⁽³⁾	Yes
SPX	Yes	Yes	Yes
SPX II	No	No	Yes ⁽⁴⁾
TCP/IP	Yes	Yes	Yes
X.PC	Yes	Yes	Yes

1.3.3. 1.1.3. Domino Designer

Platform	Windows 98	Windows 2000/ Windows XP	Windows NT
Supported operating system versions	Windows 98	Windows 2000 Professional; Windows XP Professional	Windows NT4
Processors supported	Intel Pentium	Intel Pentium	Intel Pentium
RAM	64 MB minimum 128 MB or more recommended	128 MB minimum 256 MB or more recommended	64 MB minimum 128 MB or more recommended
Disk space	275 MB required	275 MB required	275 MB required

(The minimum amounts are the disk space required for installing default files. More disk space is required if databases are replicated locally or copied locally)			
Protocols supported			
NetBEUI/NetBIOS ⁽¹⁾	Yes	Yes (Windows 2000) No (Windows XP)	Yes
NetBIOS over IP ⁽²⁾	Yes	Yes	Yes
NetBIOS over IPX	Yes ⁽³⁾	Yes ⁽³⁾	Yes
SPX	Yes	Yes	Yes
SPX II	No	No	Yes ⁽⁴⁾
TCP/IP	Yes	Yes	Yes
X.PC	Yes	Yes	Yes

Footnotes

¹ Only Microsoft NetBEUI is supported.

² Only Microsoft TCP/IP is supported.

³ Both Novell NetBIOS and Microsoft NetBIOS over IPX are supported.

⁴ Using Microsoft's NWLink IPX/SPX stack.

1.3.4. 1.1.4. Domino Server – таблица 1

Platform	Windows 2000	Windows NT	Windows 2003
Supported operating system versions	Windows 2000 Server; Windows 2000 Advanced Server (see the "Windows service pack requirements" Release Note for Service Pack information)	Windows NT4 Intel ⁽¹⁾ (see the "Windows service pack requirements" Release Note for Service Pack information)	Windows 2003 Server; Windows 2003 Enterprise Edition (see the "Windows service pack requirements" Release Note for Service Pack information)
Processors supported	Intel Pentium	Intel Pentium	Intel Pentium
RAM	128 MB minimum 192 MB or more recommended	128 MB minimum 192 MB or more recommended	128 MB minimum 192 MB or more recommended
Disk space	1 GB minimum 1.5 GB or more recommended	1 GB minimum 1.5 GB or more recommended	1 GB minimum 1.5 GB or more recommended
Disk swap space	128 MB minimum	128 MB minimum	128 MB minimum
Monitors supported	Color monitor required	Color monitor required	Color monitor required
Protocols supported			
NetBEUI/NetBIOS ⁽²⁾	Yes	Yes	Yes
NetBIOS over IP ⁽³⁾	Yes	Yes	Yes
NetBIOS over IPX	Yes	Yes	Yes
SPX ⁽⁴⁾	Yes	Yes	Yes

SPX II	Yes ⁽⁵⁾	Yes ⁽⁵⁾	Yes ⁽⁵⁾
TCP/IP	Yes	Yes	Yes
X.PC	Yes	Yes	Yes

1.3.5. 1.1.5. Domino server – таблица 2

Platform	AIX	Linux	Solaris
Supported operating system versions	AIX 5.1; AIX 5.2 (see the "AIX - IOCP and patch requirements" Release Note for Service Pack information)	Red Hat 7.2; Red Hat Enterprise Linux AS 2.1 (Uni-processor only); SuSE 8.0 (Server and Enterprise); UnitedLinux 1.0; Powered by UnitedLinux 1.0 (see the "Linux patch requirements" Release Notes for more information)	Solaris 8 Solaris 9 (see "Solaris patch requirements" Release Note for patch information)
Processors supported	PowerPC, POWER, POWER2, POWER3 RS64	Intel x86	UltraSPARC and newer
RAM	192 MB minimum; 256 MB or more recommended	128 MB minimum; 192 MB or more recommended	192 MB minimum 256 MB or more recommended
Disk space	1 GB minimum 1.5 GB or more recommended	1 GB minimum 1.5 GB or more recommended	1 GB minimum 1.5 GB or more recommended
Disk swap space	3 times the physical RAM installed	3 times the physical RAM installed	3 times the physical RAM recommended
Monitors supported	Color monitor required	Color monitor required	Color monitor required
Protocols supported			
NetBEUI/NetBIOS ⁽²⁾	No	No	No
NetBIOS over IP ⁽³⁾	No	No	No
NetBIOS over IPX	No	No	No
SPX ⁽⁴⁾	No	No	No
SPX II	No	No	No
TCP/IP	Yes	Yes	Yes
X.PC	Yes	Yes	Yes

1.3.6. 1.1.6. Domino server – таблица 3

Platform	iSeries	z/OS	Linux on zSeries
Supported operating system versions	OS/400 Version 5, Release 1 or later (see the "Domino for iSeries" chapter of these Release Notes for more information)	z/OS Version 1, Release 2 or later - or - z/OSe Version 1, Release 3 or later (see the "Domino for z/OS" chapter of these Release Notes for more information)	UnitedLinux 1.0 for IBM S/390 (see the "Domino for Linux on zSeries service pack requirements" Release Note for service pack information)
Processors	PowerPC (RISC)	Any that supports	S/390 G5/G6;

supported		your release level of z/OS	zSeries (z800, z900, z990)
RAM	288 MB minimum; 512 MB or more recommended	1 MB minimum; 2 MB or more recommended	1 MB minimum 2 MB or more recommended
Disk space	1 GB minimum 1.5 GB or more recommended	3 3390-3 volumes minimum	2.5 GB minimum 2.5 GB or more recommended
Disk swap space	N/A	N/A	N/A
Monitors supported	Color monitor required	Color monitor required	Color monitor required
Protocols supported			
NetBEUI/NetBIOS ⁽²⁾	No	No	No
NetBIOS over IP ⁽³⁾	No	No	No
NetBIOS over IPX	No	No	No
SPX ⁽⁴⁾	No	No	No
SPX II	No	No	No
TCP/IP	Yes	Yes	Yes
X.PC	No	No	No

Citrix support information

The Notes client is supported on Citrix Metaframe XPe FR3 on Windows 2000 and Windows 2003 server using NT and MAC ICA clients. For additional information, please see the "Citrix support statement" release note in this chapter.

Footnotes

¹ Do not install a Domino server on a Domain Controller. The processing of NT domain logons by Domain Controllers can consume large amounts of processing resources, especially for larger domains, and thus can affect Domino server performance. If the Domino server is to be within an NT domain, the server should be a member server within the domain.

² Only Microsoft NetBEUI is supported.

³ Only Microsoft TCP/IP is supported.

⁴ Domino clusters and partitioned server configurations do not support the IPX/SPX protocol. At this time, Lotus does not plan to provide IPX/SPX network support for future releases of these features.

⁵ Using Microsoft's NWLink IPX/SPX stack

1.4. 1.1. Типы лицензий серверов и клиентов в R6

Типы лицензий серверов R6

- • **Domino Utility Server** - provides application services only, with support for Domino clusters. The Domino Utility Server is a new installation type for Lotus Domino 6 that removes client access license requirements. Note that it does NOT include support for messaging services.
- • **Domino Messaging Server** - provides messaging services. Note that it does NOT include support for application services or Domino clusters.
- • **Domino Enterprise Server** - provides both messaging and application services, with support for Domino clusters.

Note All three types of installations support Domino partitioned servers. Only the Domino Enterprise Server supports a service provider (xSP) environment.

Типы лицензий клиентов R6

- • **Notes Client** - Standard Notes client without Design features
- • **Domino Designer** - Design environment for building custom applications. Includes the Notes client
- • **Domino Administrator** - System administration environment for performing administrative tasks. Includes the Notes client

1.5. 1.1. Каталог Domino (Domino Directory)

База **NAMES.NSF** - Каталог Domino (старое название «Общая адресная книга») - содержит основную конфигурационную информацию для всех серверов домена.

- • Person – документы с информацией о пользователях
- • Group – документы, определяющие группы
- • Connection – документы, описывающие соединения между серверами для репликаций и передачи почты
- • Server – конфигурационные документы серверов
- • Configuration – конфигурационные документы, относящиеся к конкретному серверу, группе серверов или всем серверам домена
- • И другие...

Каждый сервер использует информацию из своей локальной реплики NAMES.NSF. Синхронность информации в репликах NAMES.NSF на разных серверах обеспечивается репликациями.

База NAMES.NSF доступна по протоколам Notes и может быть доступна по протоколам LDAP и HTTP.

1.6. 1.1. ID-файлы сертификатов, серверов и пользователей

Каждый сервер Domino или пользователь Notes имеет свой ID-файл («файл идентификационных данных») - ассоциированный с этим сервером или пользователем уникальный двоичный файл, обычно имеющий расширение .ID. Этот файл идентифицирует своего владельца в контактах с серверами, используется в операциях шифрования, создания и проверки «электронной подписи» и т.п..

ID-файл пользователя или сервера создается сертификатом (certifier). Сертификатор - лицо (обычно, администратор), имеющее специальный ID-файл - ID сертификатора. ID-файл сертификатора используется при создании, сертификации и ресертификации ID-файлов пользователей и серверов.

Логически информация в ID-файле включает две «области» – область открытой информации (ничем не защищена) и область секретной информации (зашифрована по алгоритму шифрования с одним ключом, в качестве ключа используется пароль ID-файла). Пароль необходим для предотвращения возможности использования ID-файла без ведома владельца. Когда клиент Notes открывает ID-файл, он запрашивает у пользователя пароль и дешифрует на нем информацию из области секретной информации ID-файла.

Область открытой информации	Иерархический сертификат, состоящий из набора сертификатов-компонент
	Маловероятно, несколько неиерархических (простых) сертификатов (анахронизм версий 1 и 2)
	Возможно, несколько сертификатов X.509
Область секретной информации	Параметры ID-файла
	Секретный ключ Notes (private key)
	Ранее использовавшиеся секретные ключи Notes
	Набор ключей шифрования (алгоритм с одним ключом)
	Секретные ключи, связанные с сертификатами X.509

Иерархический сертификат. Состоит из набора сертификатов-компонент. Используется при аутентификации пользователя или сервера в первой фазе их контакта с сервером и при проверке «электронной подписи». Сертификат-компонента содержит:

- **Имя владельца сертификата**, например Nikolay N. Iontsev/InterTrustCorp/SU.
- **Имя создавшего сертификат**, например /InterTrustCorp/SU.
- **Тип сертификата** (Notes international encryption, Notes multi-purpose, Notes certificate authority).
- **Срок истечения сертификата.**
- **Открытый ключ (public key).** Открытый ключ используется при шифровании почты и локальных баз данных, а также в процессе проверки «электронной подписи». Его копия также заносится в Каталог Domino и становится доступной другим пользователям домена. Копия открытого ключа может передаваться пользователям из других доменов. Небольшая тонкость: информация, которая хранится в поле с меткой Certified Public Key документа из Каталога Domino, содержит открытый ключ, но не является в точности открытым ключом – скорее всего это иерархический сертификат целиком.
- **Подпись создавшего сертификат.** Значение функции хеширования по информации из сертификата, зашифрованное по алгоритму RSA на секретном ключе создавшего сертификат.

Параметры ID-файла содержат различную информацию об ID-файле. В частности, в их число входят **номер лицензии** (permanent license number), **вид лицензии** (International или North American, определяет длину используемых в алгоритмах

шифрования ключей) и **тип** (Hierarchical Certifier, Hierarchical User or Server, Flat User or Server, Flat Certifier).

Секретный ключ Notes (private key). Имеется только в ID-файле и нигде более. Используется для шифрования почты и локальных баз данных, а также в процессе создания «электронной подписи». Пара «секретный-открытый ключ» может быть изменена владельцем ID-файла, при этом новый открытый ключ должен быть передан сертификатору для ресертификации ID-файла владельца (замены в нем сертификатов) и помещения в Каталог Domino.

Ключи шифрования (encryption key's). Ключи шифрования используются для шифрования документов в базах данных. Они создаются пользователями и передаются другим пользователям, которые должны иметь доступ к документам, зашифрованным этими ключами.

ID-файл сервера идентифицирует сервер в контактах «сервер-сервер» и «сервер-станция». Он создается при установке первого сервера или при регистрации очередного сервера. Содержит те же компоненты (обычно, кроме пароля), что и ID-файл пользователя. Различие лишь в том, что при создании ID-файла сервера информация о нем была занесена в документ Server в Каталоге Domino, а не в документ Person, как при регистрации нового пользователя.

ID-файл сертификатора (CERT.ID) идентифицирует сертификатора организации. Создается в процессе установки первого сервера в организации. Впоследствии может быть создан и другой ID-файл сертификатора организации. Сертификатор (обычно, администратор) использует ID-файл сертификатора при регистрации новых пользователей и серверов (добавление сертификата в их ID-файлы), ресертификации пользователей и серверов (замена сертификатов в их ID-файлах) и выпуске взаимных сертификатов. Кроме того, ID-файл сертификатора также используется при создании набора ID-файлов для сертификаторов оргединиц первого уровня в организации. Несмотря на то, что ID-файл сертификатора имеет в основном те же компоненты, что и ID-файлы пользователя и сервера, имеются и отличия. В частности, сертификатор не может работать под ID-файлом сертификатора с иерархическим именем как пользователь Notes - для этого у сертификатора имеется «обыкновенный пользовательский» ID-файл.

1.7. 1.1. Дерево имен организации

/Acme Corp., Inc./US – сертификат 0	«Самосоздано» при установке первого сервера организации
Jon Jones/Acme Corp., Inc./US – пользователь 1 Alice Brow/Acme Corp., Inc./US – пользователь 2 Server11/Acme Corp., Inc./US – сервер 1 Server12/Acme Corp., Inc./US – сервер 2 /Marketing/Acme Corp., Inc./US – сертификат 1	Создано сертификатом 0
Jon Jones/Marketing/Acme Corp., Inc./US – пользователь 3 Server13/Marketing/Acme Corp., Inc./US – сервер 3	Создано сертификатом 1

CN/OU4/OU3/OU2/OU1/O/C – общая структура имени

1.7.1. 1.1.1. Пример дерева имен организации

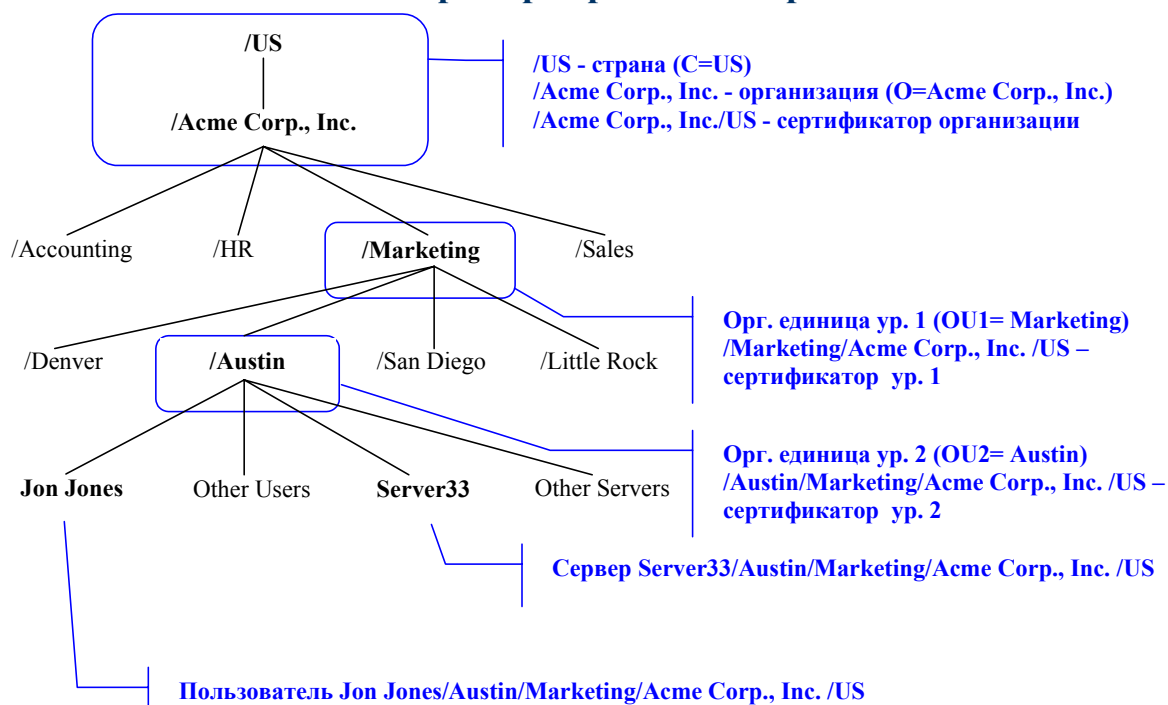


Рис. 2 Узел в дереве = ID сертификата, лист в дереве (под любым узлом) = ID сервера или пользователя

Jon Jones/Austin/Marketing/Acme Corp., Inc./US – пользователь
Server33/Austin/Marketing/Acme Corp., Inc./US – сервер
/Austin/Marketing/Acme Corp., Inc./US – сертификат ур. 2
/Marketing/Acme Corp., Inc./US – сертификат ур. 1
/Acme Corp., Inc./US – сертификат организации

Abbreviate: Jon Jones/Austin/Marketing/Acme Corp., Inc./US
Canonicalize: CN=Jon Jones/OU2=Austin/OU1=Marketing/O=Acme Corp., Inc./C=US

1.7.2. 1.1.2. Пример процесса создания дерева имен

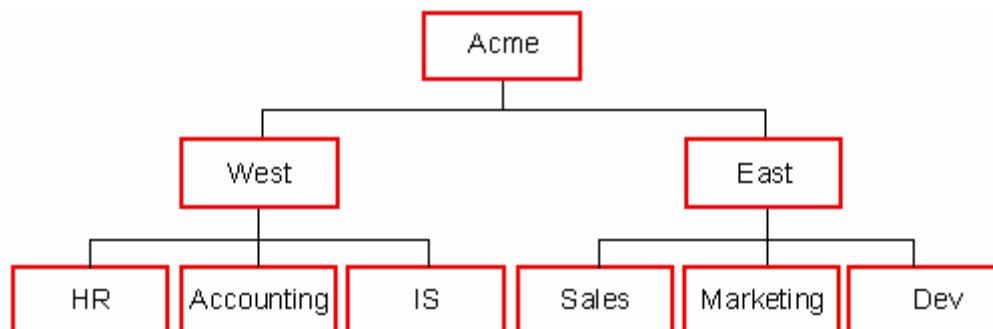


Рис. 3 OU1 + OU2 – регистрация сертификатов

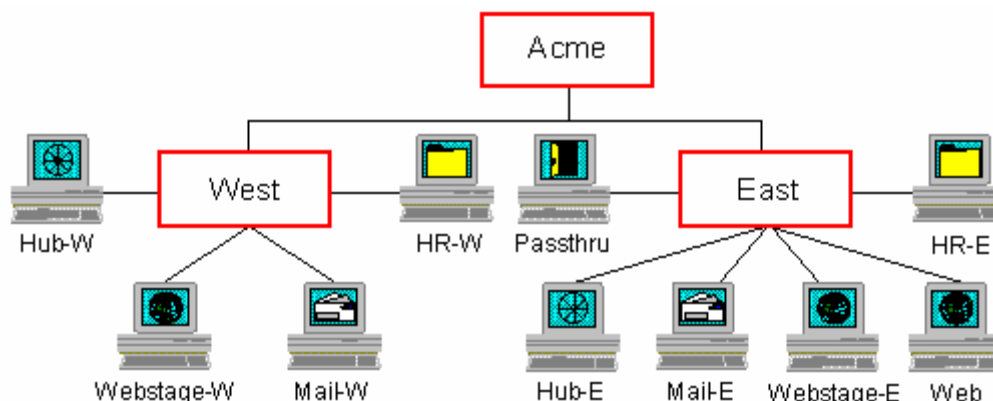


Рис. 4 Регистрация и установка серверов

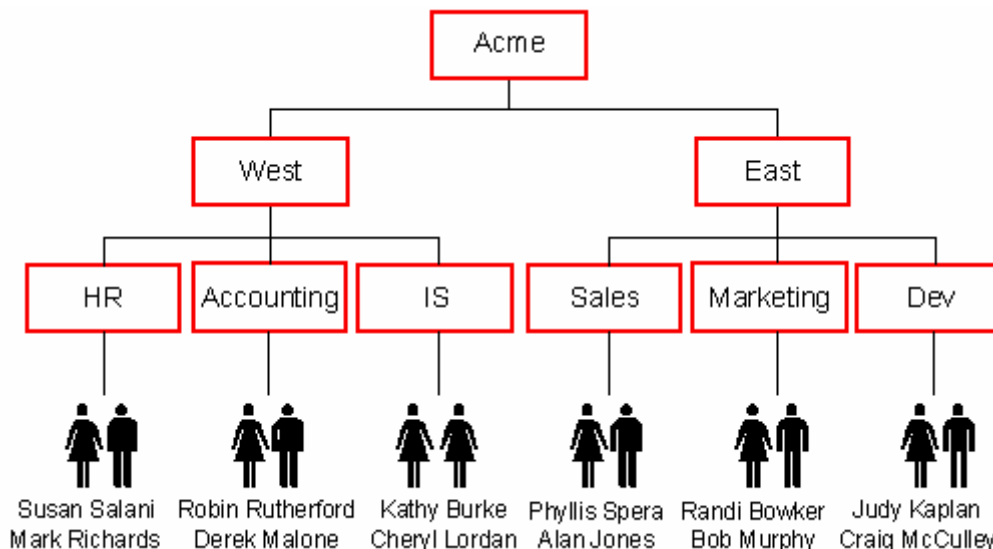


Рис. 5 Регистрация пользователей

1.7.3. 1.1.3. Альтернативные имена (были введены в R5)

Пользователь в ID-файле может иметь два имени (но не более двух!) - основное (обычно, «английское») и альтернативное (например, «русское»).

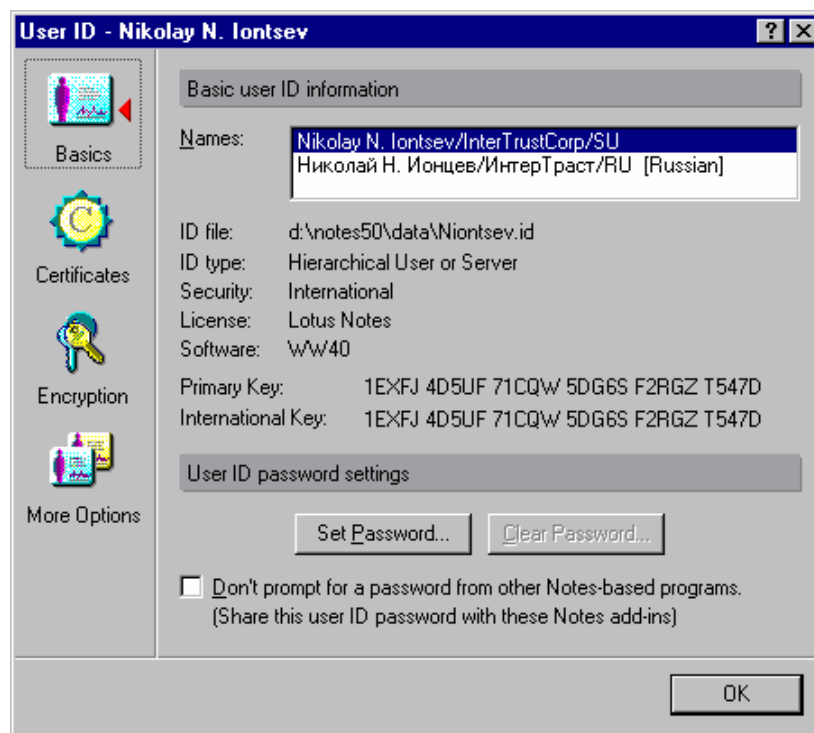


Рис. 6 Пользователь имеет два имени - основное и альтернативное («русское»)

Назначение альтернативных имен выполняется при регистрации новых пользователей или ресертификации существующих. Для этого ID-файл сертификатора уже должен иметь альтернативные имена. ID-файл сертификатора может иметь более двух имен, причем «по мере спуска по дереву имен наблюдается вложенность».

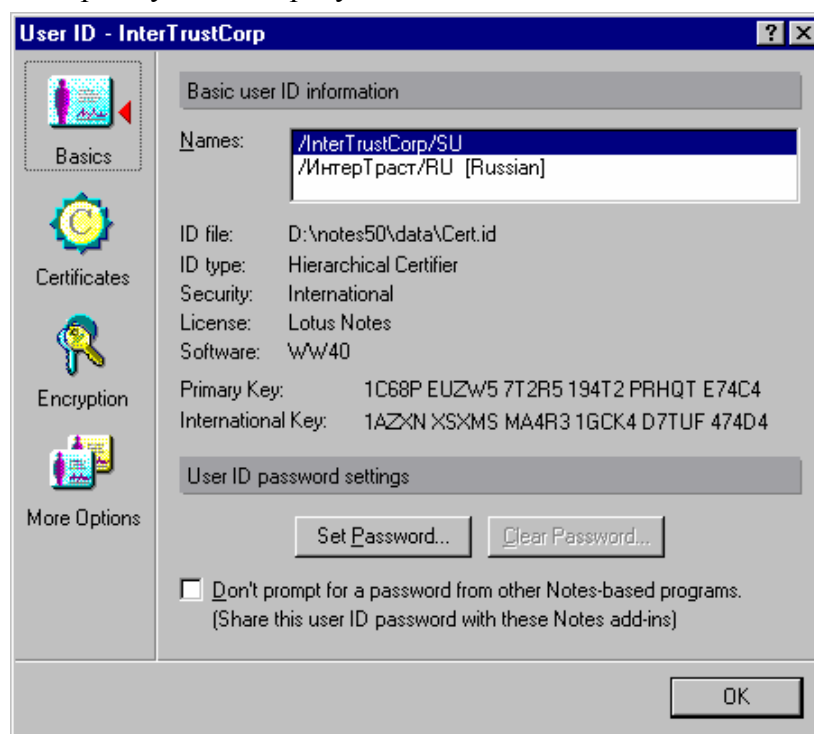


Рис. 7 Сертификатор имеет два имени - основное и альтернативное («русское»), но может иметь много альтернативных имен

Например, ID-файл сертификатора организации /Acme имеет поддержку имен на английском, французском, немецком, шведском и русском. Дерево имен «ветвится» на /America/Acme и /Europa/Acme. ID-файл сертификатора /America/Acme имеет поддержку имен на английском и французском. ID-файл сертификатора /Europa/Acme имеет

поддержку имен на английском, французском, немецком, шведском и русском. Пользователь User1/America/Acme имеет английское имя и может иметь альтернативное французское имя. Пользователь User1/Europa/Acme имеет английское имя и может иметь еще одно альтернативное имя: на французском, немецком, шведском или русском.

Серверы альтернативных имен иметь не должны. Принудительное назначение серверу альтернативного имени повлечет неработоспособность сервера.

ID-файл с альтернативным именем не работает на клиенте R4.

Процесс назначения альтернативных имен должен идти по дереву имен сверху вниз - от сертификатора верхнего уровня к сертификаторам подчиненных уровней и далее к пользователям.

1.7.4. 1.1.4. Длины имен и набор допустимых символов

Приведенная ниже таблица соответствует R5. В R6 допустимо «длинное отчество», однако прочие подробности в документации отсутствуют. Хотя по непроверенным сведениям для хранения имен в R6 применяется кодировка UNICODE, зафиксированные в форумах многочисленные проблемы с «не-английскими» основными именами в разных подсистемах указывают на то, что этим лучше не пользоваться.

Name	Maximum Length	Valid Character
Organization Certifier Name	3 to 64 Characters (recommended to limit to 32 characters if possible)	A - Z, 0 - 9, -, _ ' (dash, period, space, underscore, and apostrophe) Note: See Supporting Information field below.
Organization Unit Certifier Name	64 Characters	A - Z, 0 - 9, -, _ ' (dash, period, space, underscore, and apostrophe) Note: See Supporting Information field below.
Country Code	0 or 2 Characters	A - Z
Password - Organization - OU - Server/User	-32 Characters -at least 12 (recommended) to 32 chars. -63 Characters	A - Z, 0 - 9, & -, _ ' (ampersand, dash, period, space, underscore, and apostrophe)
Server Name	79 Characters	A - Z, 0 - 9, & -, _ ' (ampersand, dash, period, space, underscore, and apostrophe) Space is not recommended. If you use Space, you must enter the Server name in quotes (" ") when you are entering a command set at the Server Console. Periods (.) are not recommended.
Notes Name Network	31 Characters	A - Z, 0 - 9, -, _
Notes Port Name	31 Characters	A - Z, 0 - 9, -, _
User First Name + User Last Name	Must not be greater than 80 Characters	A - Z, 0 - 9, & -, _ ' (ampersand, dash, period, space, underscore, and apostrophe)
User Middle Initial	2 Characters	A - Z, 0 - 9, & -, _ ' (ampersand, dash, period, space, underscore, and apostrophe)
Notes Domain Name	31 Characters (minimum of 3 characters)	A - Z, 0 - 9, & -, _ ' (ampersand, dash, period, space, underscore, and apostrophe) Do not use periods (.) in a domain name as they are reserved characters.

1.8. 1.1. Шифрование и электронная подпись

1.8.1. 1.1.1. Введение в систему шифрования RSA

Encryption for Privacy

► Secret Key Encryption



► Public Key Encryption

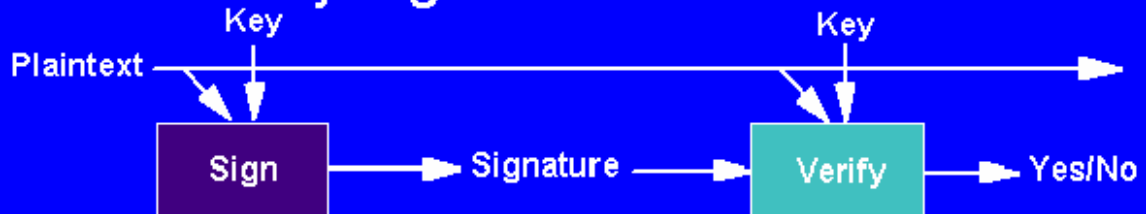


Рис. 8 Симметричный - Secret Key Encryption, RSA (два ключа) – Public Key Encryption

1.8.2. 1.1.2. Введение в электронную подпись

Encryption for Integrity

► Secret Key Signatures



► Public Key Signatures



Рис. 9 Симметричный - Secret Key Signatures, RSA (два ключа) – Public Key Signatures

1.8.3. 1.1.3. Простой пример на принцип работы алгоритма RSA

I. Generating the encryption keys

The public key :

1. choose an odd number E : $E = 5$
2. Choose 2 prime-numbers, p and q with p not q, and make sure that it is possible to divide $(p-1)(q-1)-1$ with E
 $p = 7, q = 17$
3. Multiply p with q and get N
 $N = p * q = 7 * 17 = 119$
4. The numbers N and E are now the public key
 $(N, E) = (119, 5)$

The private key :

1. Subtract 1 from p,q and e, multiply the result and add 1
 $(p-1) (q-1) (E-1) + 1 = 6 * 16 * 4 + 1 = 385$
2. Divide the result with E and get D: $D = 385 / 5 = 77$
3. The numbers N and D are now the private key
 $(N, D) = (119, 77)$

II. How to encrypt using the keys

Encrypt the message using the public key:

1. Translate the text-strings into a

collection of numbers, like appropriate number of the char in the alphabetical order; by example char "s" is now 19

Original Char = 19

2. The algorithm :

a) get the Power of the text-chars with E

$$19^5 = 2476099$$

b) divide with N and get the remainder

$$2476099 / 119 = 20807 + 66$$

3. The remainder is the encrypted Char "s"

Encrypted Char = 66

Decrypt the message using the private key:

1. The algorithm:

a) get the Power of the encrypted Text with D

$$66^{77} = (1,27,\dots)^{140}$$

b) divide with N

$$(1,27,\dots)^{140} / 119 = (1,069,\dots)^{138} + 19 / 119$$

2. The rest of that is the decrypted Char

Decrypted Char = 19

To send an encrypted message, you have to get the public key of the receiving person from a directory (in a Notes-system from the N&A-Book). Using this key you will encrypt the message. Because only the receiving person knows his own (required) private key, only he can decrypt the message. The encrypted message contains parameter "N", which makes it impossible to calculate the parameter "D" only with that information. To break the code, you have to split the "N"-parameter back to Prime-Numbers. If the Number "N" would be a Number with 170 digits, even a supercomputer would take more than 10000 years to rebuild it.

1.9. 1.1. Сертификаты и аутентификация

1.9.1. 1.1.1. Сертификат Notes

Простой сертификат, взаимный сертификат или сертификат-компоненту из иерархического сертификата можно представлять себе в виде «бумажного документа» примерно следующего содержания.

СЕРТИФИКАТ

Я, сертифициатор (пользователь, сервер) [*/InterTrustCorp/SU*] ,

утверждаю, что

пользователь (сервер, сертифициатор) [*Nikolay N. Iontsev/InterTrustCorp/SU*]

имеет открытый ключ [*7777777777*].

Тип сертификата [*Notes multi-purpose*].

Срок действия сертификата до [*01.08.2005*].

Подпись сертифициатора

Рис. 10 Интерпретация содержания сертификата

При применении иерархических и взаимных сертификатов используются следующие **правила доверия открытым ключам**.

1. 1. Доверять любому открытому ключу, полученному из сертификатов-компонент иерархического сертификата, имеющегося в своем ID-файле.
2. 2. Доверять любому открытому ключу, полученному из имеющего силу (т.е. уже прошедшего проверку) сертификата-компоненты.

1.9.2. 1.1.2. Процедура аутентификации между субъектами из одной организации

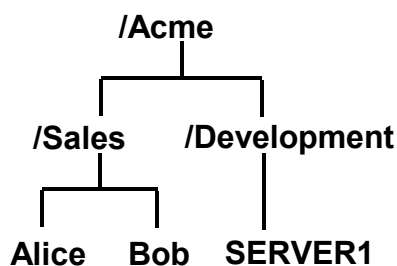


Рис. 11 Дерево имен компании Асте

Server1/Development/Acme		Имя сервера	
/Acme -> /Acme	Сертификат-компонента	ID-файл сервера	
/Acme -> /Development/Acme	Сертификат-компонента		
/Development/Acme -> Server1/Development/Acme	Сертификат-компонента		
Alice/Sales/Acme		Имя клиента	
/Acme -> /Acme	Сертификат-компонента	ID-файл клиента	
/Acme -> /Sales/Acme	Сертификат-компонента		
/Sales/Acme -> Alice/Sales/Acme	Сертификат-компонента		

Шаг 1

- • Клиент Alice/Sales/Acme пытается получить доступ к серверу SERVER1/Development/Acme. Клиент передает серверу все сертификаты-компоненты из своего ID-файла. Сервер начинает процесс аутентификации (определения имени и открытого ключа) клиента.
- • Сравнением своего имени с именем клиента сервер выявляет наличие общего предка. Общий предок всегда существует, когда клиент и сервер из одного дерева имен. В нашем случае этот общий предок - /Acme. Сервер читает открытый ключ /Acme из сертификата-компоненты в своем ID-файле. Согласно правилу 1 сервер «уверенно знает» имя и открытый ключ /Acme.
- • Сервер проверяет сертификат-компоненту, которую /Acme создал для /Sales/Acme, используя открытый ключ /Acme. Если проверка успешна, согласно правилу 2 сервер «уверенно знает» имя и открытый ключ /Sales/Acme.
- • Сервер проверяет сертификат-компоненту, которую /Sales/Acme создал для Alice/Sales/Acme, используя открытый ключ /Sales/Acme. Если сертификат имеет силу, согласно правилу 2 сервер «уверенно знает» имя и открытый ключ Alice/Sales/Acme.

Шаг 2

- • Сервер проверяет, «знает ли» клиент свой секретный ключ:
- • сервер генерирует случайное число и посылает его клиенту
- • клиент шифрует это число по RSA своим секретным ключом и возвращает полученный код серверу
- • сервер использует открытый ключ клиента для декодирования по RSA присланного клиентом кода. Если только декодированное число совпадает с оригиналом, сервер предполагает, что клиент подлинный.

Шаг 3

- • Сервер передает клиенту все сертификаты-компоненты из своего ID-файла. Клиент начинает процесс аутентификации (определения имени и открытого ключа) сервера.
- • Сравнением своего имени с именем сервера клиент выявляет наличие общего предка. Общий предок всегда существует, когда клиент и сервер из одного дерева имен. В нашем случае этот общий предок - /Acme. Клиент читает открытый ключ /Acme из сертификата-компоненты в своем ID-файле. Согласно правилу 1 клиент «уверенно знает» имя и открытый ключ /Acme.
- • Клиент проверяет сертификат-компоненту, которую /Acme создал для /Development/Acme, используя открытый ключ /Acme. Если проверка успешна, согласно правилу 2 клиент «уверенно знает» имя и открытый ключ /Development/Acme.
- • Клиент проверяет сертификат-компоненту, которую /Development/Acme создал для Server1/Development/Acme, используя открытый ключ /Development/Acme. Если сертификат имеет силу, согласно правилу 2 клиент «уверенно знает» имя и открытый ключ Server1/Development/Acme.

Шаг 4

- • Клиент проверяет, «знает ли» сервер свой секретный ключ:
- • клиент генерирует случайное число и посылает его серверу
- • сервер шифрует это число по RSA своим секретным ключом и возвращает полученный код клиенту
- • клиент использует открытый ключ сервера для декодирования по RSA присланного сервером кода. Если только декодированное число совпадает с оригиналом, клиент предполагает, что сервер подлинный.

Процедура аутентификации закончена – стороны уверенно знают имена и открытые ключи друг друга. С этого момента может решаться вопрос о дополнительных проверках при аутентификации (документ Server), шифровании трафика по порту и

предоставлении клиенту доступа к серверу (сравнение имени «как строки» явно или вхождением в группу).

1.9.3. 1.1.3. Процедура аутентификации между субъектами из разных организаций

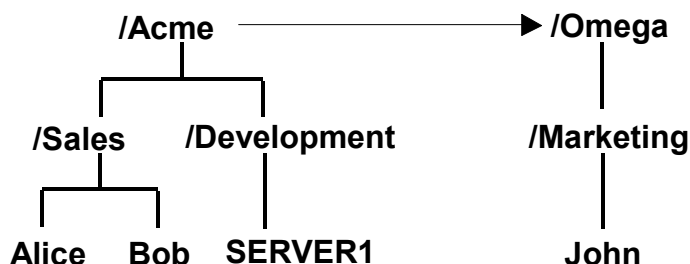


Рис. 12 Деревья имен компаний Асме и Омега

Server1/Development/Acme	Имя сервера	
/Acme -> /Acme	Сертификат-компонента	ID-файл сервера
/Acme -> /Development/Acme	Сертификат-компонента	
/Development/Acme -> Server1/Development/Acme	Сертификат-компонента	
+ /Acme -> /Omega	Взаимный сертификат	NAMES.NSF сервера
John/Marketing/Omega	Имя клиента	
/Omega -> /Omega	Сертификат-компонента	ID-файл клиента
/Omega -> /Marketing/Omega	Сертификат-компонента	
/Marketing/Omega -> John/Marketing/Omega	Сертификат-компонента	
+ (или) /Omega -> /Acme	Взаимный сертификат	NAMES.NSF клиента
+ (или) John/Marketing/Omega -> /Acme	Взаимный сертификат	

В этом случае приходится использовать как иерархические сертификаты из ID-файлов, так взаимные сертификаты из «адресных книг» NAMES.NSF. Предполагаем, что сертифициатор /Acme создал взаимный сертификат для сертифициатора /Omega. Этот взаимный сертификат хранится в Каталоге Domino (локальной адресной книге) сервера SERVER1/Development/Acme. Предполагаем, что пользователь John/Marketing/Omega создал взаимный сертификат для сертифициатора /Acme. Этот взаимный сертификат хранится в локальной адресной книге на станции пользователя.

Шаг 1

- Клиент John/Marketing/Omega пытается получить доступ к серверу SERVER1/Development/Acme. Клиент передает серверу все сертификаты-компоненты из своего ID-файла. Сервер начинает процесс аутентификации (определения имени и открытого ключа) клиента.
- Поскольку общих предков у John/Marketing/Omega и SERVER1/Development/Acme нет, сервер вынужден обратиться к своей базе NAMES.NSF в поисках взаимного сертификата. Этот взаимный сертификат должен быть выпущен от имени сервера SERVER1/Development/Acme или одного из его предков для пользователя John/Marketing/Omega или одного из его предков. По условию /Acme, предок SERVER1/Development/Acme, создал взаимный сертификат для /Omega, предка John/Marketing/Omega. Сервер извлекает из своей локальной адресной книги этот взаимный сертификат.
- Найденный взаимный сертификат подписан сертифициатором /Acme. Сервер читает открытый ключ /Acme из сертификата-компоненты в своем ID-файле. Согласно правилу 1 сервер «уверенно знает» имя и открытый ключ /Acme.

- • Сервер проверяет взаимный сертификат, используя открытый ключ /Acme. Если проверка успешна, согласно правилу 2 сервер «уверенно знает» открытый ключ /Omega.
- • Сервер проверяет сертификат-компоненту, которую /Omega создал для /Marketing/Omega, используя открытый ключ /Omega. Если проверка успешна, согласно правилу 2 сервер «уверенно знает» имя и открытый ключ /Marketing/Omega.
- • Сервер проверяет сертификат-компоненту, которую /Marketing/Omega создал для John/Marketing/Omega, используя открытый ключ /Marketing/Omega. Если сертификат имеет силу, согласно правилу 2 сервер «уверенно знает» имя и открытый ключ John/Marketing/Omega.

Шаг 2

- • Сервер проверяет, «знает ли» клиент свой секретный ключ:
 - • сервер генерирует случайное число и посылает его клиенту
 - • клиент шифрует это число по RSA своим секретным ключом и возвращает полученный код серверу
 - • сервер использует открытый ключ клиента для декодирования по RSA присланного клиентом кода. Если только декодированное число совпадает с оригиналом, сервер предполагает, что клиент подлинный.

Шаг 3

- • Сервер передает клиенту все сертификаты-компоненты из своего ID-файла. Клиент начинает процесс аутентификации (определения имени и открытого ключа) сервера.
- • Поскольку общих предков у John/Marketing/Omega и SERVER1/Development/Acme нет, клиент вынужден обратиться к своей базе NAMES.NSF в поисках взаимного сертификата. Этот взаимный сертификат должен быть выпущен от имени пользователя John/Marketing/Omega или одного из его предков для сервера SERVER1/Development/Acme или одного из его предков. По условию сам John/Marketing/Omega создал взаимный сертификат для /Acme, предка SERVER1/Development/Acme. Клиент извлекает из своей локальной адресной книги этот взаимный сертификат.
- • Найденный взаимный сертификат подписан John/Marketing/Omega. Клиент читает открытый ключ John/Marketing/Omega из сертификата-компоненты в своем ID-файле. Согласно правилу 1 клиент «уверенно знает» имя и открытый ключ John/Marketing/Omega.
- • Клиент проверяет взаимный сертификат, которую John/Marketing/Omega создал для /Acme, используя открытый ключ John/Marketing/Omega. Если проверка успешна, согласно правилу 2 клиент «уверенно знает» имя и открытый ключ /Acme.
- • Клиент проверяет сертификат-компоненту, которую /Acme создал для /Development/Acme, используя открытый ключ /Acme. Если проверка успешна, согласно правилу 2 клиент «уверенно знает» имя и открытый ключ /Development/Acme.
- • Клиент проверяет сертификат-компоненту, которую /Development/Acme создал для Server1/Development/Acme, используя открытый ключ /Development/Acme. Если проверка успешна, согласно правилу 2 клиент «уверенно знает» имя и открытый ключ Server1/Development/Acme.

Шаг 4

- • Клиент проверяет, «знает ли» сервер свой секретный ключ:
 - • клиент генерирует случайное число и посылает его серверу
 - • сервер шифрует это число по RSA своим секретным ключом и возвращает полученный код клиенту
 - • клиент использует открытый ключ сервера для декодирования по RSA присланного сервером кода. Если только декодированное число совпадает с оригиналом, клиент предполагает, что сервер подлинный.

Процедура аутентификации закончена – стороны уверенно знают имена и открытые ключи друг друга. С этого момента может решаться вопрос о дополнительных проверках при аутентификации, шифровании трафика по порту и предоставлении клиенту доступа к серверу (сравнение имени «как строки» явно или вхождением в группу).

1.10. 1.1. Понятие репликаций

Для обозначения совокупности расположенных на разных серверах Domino реплик одной и той же базы можно использовать термин «распределенная база данных Notes».

При этом термин «реплика базы»:

- предполагает, что существует (или будет существовать) по крайней мере еще одна база, имеющая тот же самый идентификатор реплики (Replica ID), что и данная.

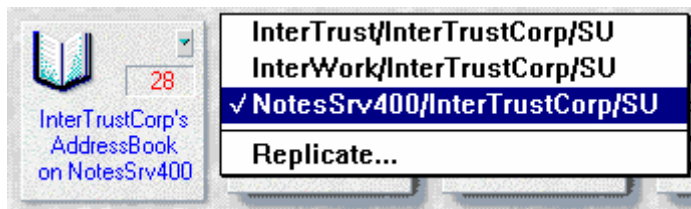


Рис. 13 Пиктограммы реплик базы «стекированы» - расположены одна за другой

«Увидеть» идентификатор реплики можно на панели свойств базы.

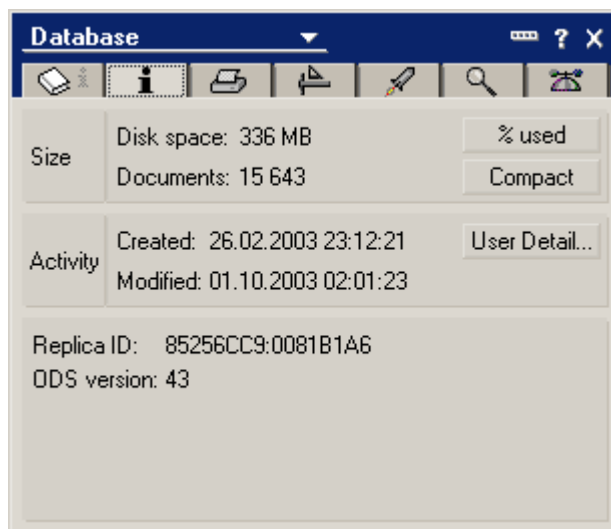


Рис. 14 Эта база имеет идентификатор реплики 85256CC9:0081B1A6

Идентификатор реплики (**Replica ID**) - уникальный идентификатор, позволяющий отличать реплики базы данных на различных серверах и станциях от обычных копий. Различные реплики одной и той же базы на различных серверах и станциях могут иметь разные названия и имена файлов, но у них одинаковый идентификатор реплики. Копия же базы, выполненная средствами Notes, гарантированно будет иметь другой идентификатор реплики, чем оригинал. Однако копия базы, выполненная средствами операционной системы, будет иметь тот же идентификатор реплики, что и оригинал (поскольку само значение идентификатора реплики хранится в файле базы)

- предполагает, что за собственно созданием реплики последуют настроенные администратором и выполняемые автоматически по расписанию или по явному указанию администратора сервера или пользователя станции процессы репликации - обмена изменениями между репликами
- не означает, что содержание двух или более реплик базы будет совершенно одинаковым. Вообще говоря, это не так и во времени, и по наличию содержащихся в репликах документов.

Суть процесса репликации состоит в следующем. Реплики одной и той же распределенной базы находятся на разных серверах. Пользователи, имеющие доступ к репликам, изменяют их содержимое (изменяют документы, создают новые документы, удаляют существующие документы) параллельно и независимо друг от друга. В

результате содержимое реплик становится неодинаковым. В определенное расписанием время на одном из серверов серверная программа Replicator («репликатор») вызывает другой сервер. Если соединение состоялось, репликатор в первую очередь составляет списки баз, реплики которых присутствуют на обоих серверах.

Далее репликатор для каждой реплики сравнивает списки документов. Новые, модифицированные или удаленные в реплике на вызванном сервере документы принимаются в реплику на вызывавшем сервере. Затем репликатор, если осуществляется репликация по схеме Pull-Push, принимает в свою реплику новые, модифицированные или удаленные документы из реплики на вызванном сервере. Кроме того, в репликациях обычно участвуют элементы дизайна и список управления доступом базы. По завершении этого процесса содержимое всех реплик баз на обоих серверах приходит в некоторое «установившееся» состояние. Однако это «установившееся» состояние, вообще говоря, не означает, что содержимое обеих реплик станет совершенно одинаковым. В частности, «неодинаковость» может создаваться за счет разных прав доступа серверов к репликам на других серверах или запланированного использования специальных формул, описывающих множество реплицируемых документов (селективные репликации).

1.11. 1.1. Домен

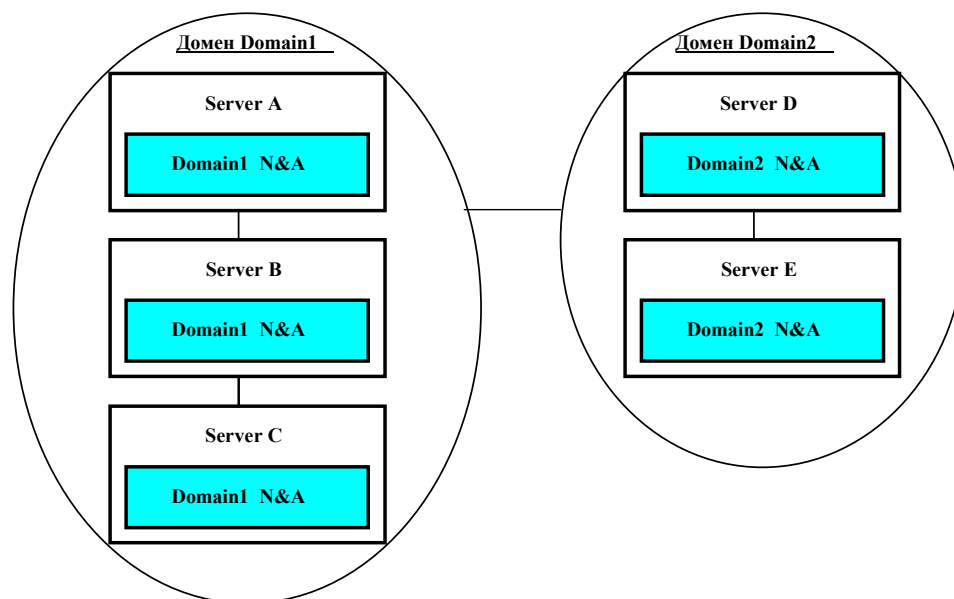


Рис. 15 Два домена, в каждом домене база NAMES.NSF (N&A) имеет одинаковый идентификатор реплики, но идентификаторы реплик баз NAMES.NSF из разных доменов различны

Домен - группа серверов, совместно использующих одну и ту же по содержанию базу данных Каталог Domino (старое название «Общая адресная книга») - NAMES.NSF. В действительности каждый сервер пользуется «своей локальной» репликой NAMES.NSF, а одинаковое состояние реплик поддерживается на основе репликаций. Репликация - обмен изменениями между двумя копиями базы с одинаковым Replica ID, расположенными на разных серверах.

Каталог Domino создается на первом сервере домена при установке сервера и реплицируется с него на другие серверы домена. Изменения, вносимые в Каталог Domino на одном из серверов домена, при репликациях автоматически (но не «мгновенно», а в соответствии с составленным администратором расписанием репликаций) распространяются в Каталоги Domino других серверов домена.

В Каталоге Domino содержится информация обо всех пользователях и серверах данного домена, всех возможных соединениях между серверами этого домена для выполнения репликаций и передачи почты, возможных соединениях серверов данного домена с некоторыми серверами из других доменов, и т.п. Иногда говорят, что «информация из Каталога Domino полностью задает конфигурацию домена», а «каждый из серверов домена полностью знает конфигурацию своего домена, но не знает конфигурации других доменов».

Домен никак не лимитируется физическим расположением серверов. Можно иметь один домен в одной организации, даже если ее многочисленные офисы разбросаны по всему миру. Напротив, можно иметь много доменов в одной крупной и расположенной территориально в одном месте организации.

Обычно в домене используют один ID сертификата организации - одно дерево имен. Но в то же время в одном домене можно иметь и несколько деревьев имен - использовать несколько ID сертификатов организации.

1.12. 1.1. Поименованная сеть Domino

Поименованная сеть Domino (Domino Named Network, DNN) - группа серверов Domino из одного домена, использующих для «общения» между собой один и тот же сетевой протокол на постоянной основе (постоянное соединение). Серверы из одной поименованной сети Domino «могут в любое время напрямую» соединяться между собой по этому протоколу.

При присвоении имен сетей Domino должно быть учтено следующее:

- серверы Domino, использующие один и тот же сетевой протокол и расположенные физически в одной и той же локальной сети, должны иметь одно и то же имя сети Domino
- серверы Domino, использующие разные сетевые протоколы, не могут принадлежать к одним и тем же сетям Domino
- серверы Domino, использующие один и тот же сетевой протокол, но расположенные физически в разных локальных сетях, должны принадлежать к разным сетям Domino. Серверы Domino, использующие один и тот же сетевой протокол, расположенные в разных локальных сетях и устанавливающие соединение между собой по модему (X.PC) или посредством Network Dialup с активизацией его из Domino, должны принадлежать к разным сетям Domino. Только в случае, если между этими двумя локальными сетями существует постоянно действующий мост (реализуемый сетевыми программными или аппаратными средствами, а не средствами Domino), по соображениям нагрузки на мост возможно помещение серверов из этих разных локальных сетей как в одну сеть Domino, так и в разные сети Domino
- серверы Domino, использующие два или более сетевых протокола, должны принадлежать к нескольким сетям Domino, по одной на каждый протокол.

Понятие «поименованная сеть Domino» существенно используется при передаче почты между серверами. Считается, что серверы, находящиеся в одной и той же поименованной сети Domino, всегда могут напрямую соединиться друг с другом для передачи почты. Поэтому сервер, обнаружив почту, которую необходимо передать на другой сервер в той же самой поименованной сети, передает ее «автоматически» - связывается с сервером назначения по общему протоколу и передает, игнорируя при этом приоритеты писем и не используя информации из документов Connection о расписании передачи почты. Если бы понятие «поименованная сеть Domino» не использовалось, то для того, чтобы «описать» все возможные варианты передачи почты между N серверами, администратору потребовалось бы создать в Каталоге Domino $N*(N-1)$ документов Connection типа Network (если $N=10$, то $N*(N-1) = 90$).

1.12.1. 1.1.1. Простой пример

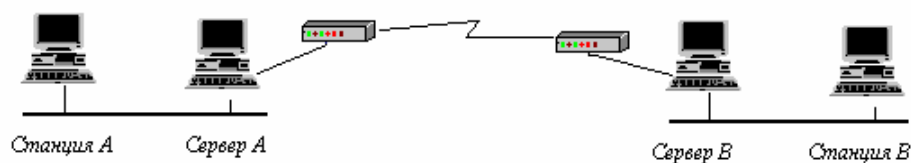


Рис. 16 Поименованные сети не определены по модемному соединению. Поэтому сервера А и В должны находиться в разных поименованных сетях Domino

1.12.2. 1.1.2. Продвинутый пример

1.12.2.1. 1.1.2.1. Без учета репликаций Каталога Domino

A,D,I	NETBIOS
H,E	TCP/IP
B,C,F,G	Novell SPX

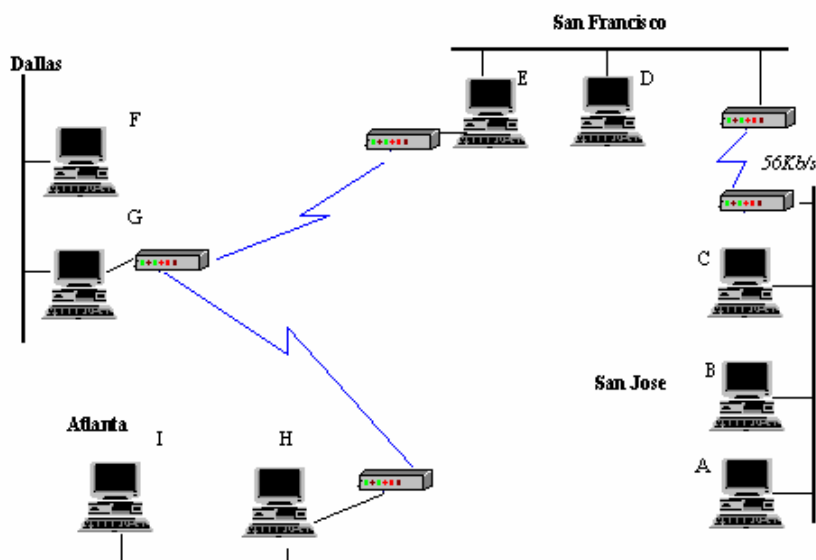


Рис. 17 Пример домена

В Атланте: "AtlantaNetBIOSLAN"
 "AtlantaTCPIPLAN"
 В Далласе: "DallasNovellSPX"
 В Сан-Франциско: "SanFranciscoTCPIPLAN"
 "SanFranciscoSanJoseNetBIOSLAN"
 В Сан-Хосе: "SanJoseNovellSPX"
 "SanFranciscoSanJoseNetBIOSLAN"

1.12.2.2. 1.1.2.2. С учетом репликаций Каталога Domino

A,D,E,I,H	NETBIOS
H,E	TCP/IP
A,B,C,F,G	Novell SPX

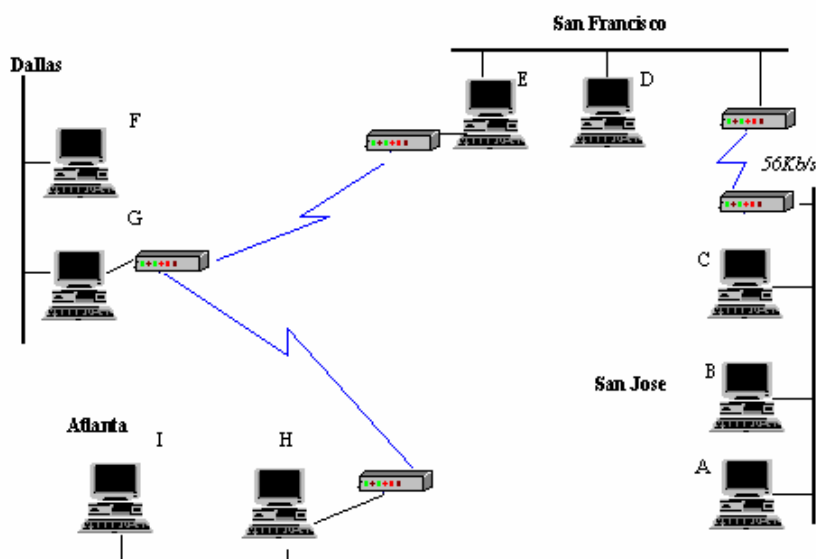


Рис. 18 Пример домена

В Атланте: "AtlantaNetBIOSLAN" (I, H)
 "AtlantaTCPIPLAN" (H)
 В Далласе: "DallasNovellSPX" (G, F)
 В Сан-Франциско: "SanFranciscoTCPIPLAN" (E)

"SanFranciscoSanJoseNetBIOSLAN" (A, D, E)

B Can-Xoce: **"SanJoseNovellSPX"** (A, B, C)

"SanFranciscoSanJoseNetBIOSLAN" (A, D, E)

1.13. 1.1. План развертывания полигона в учебном классе

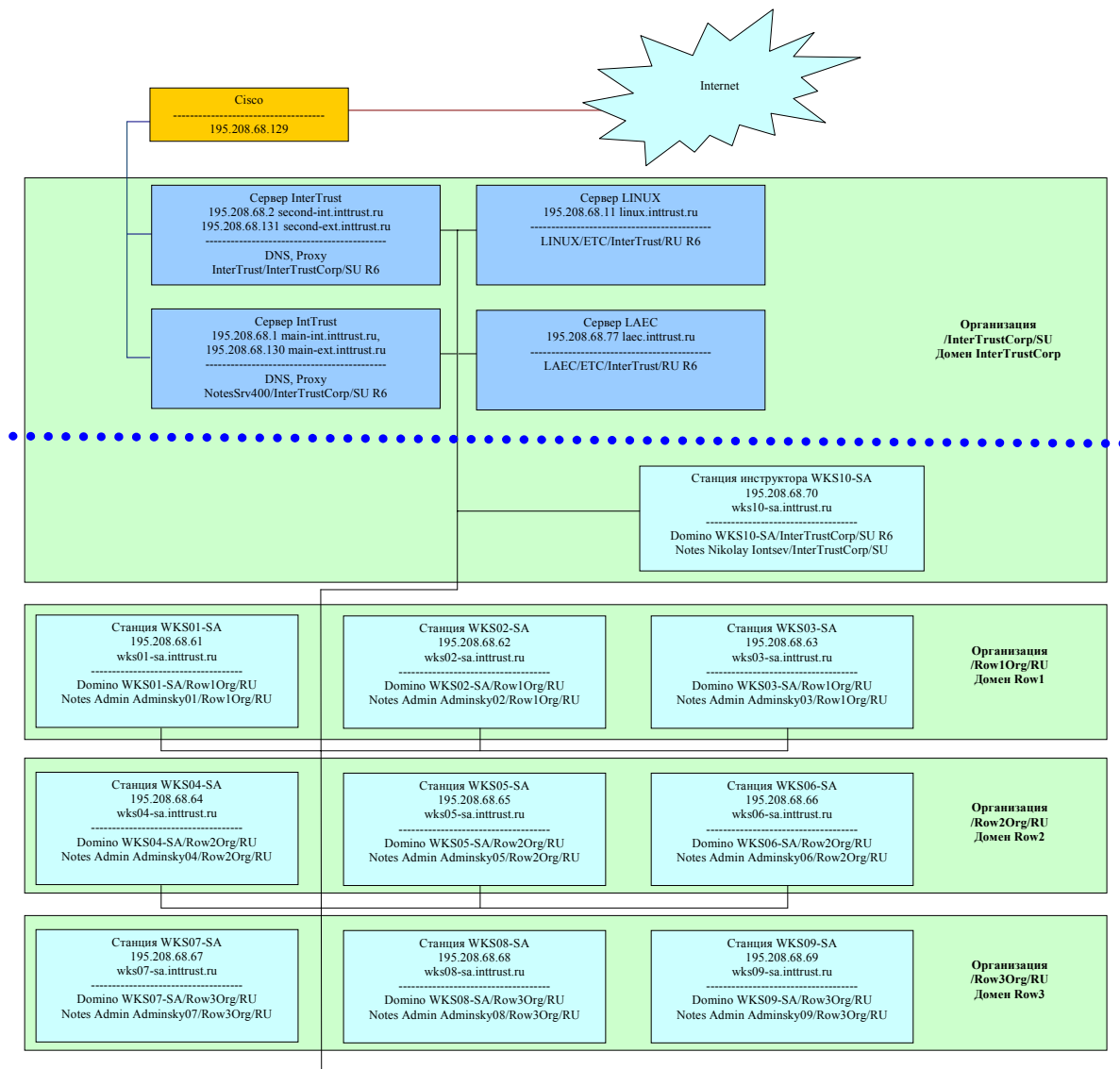
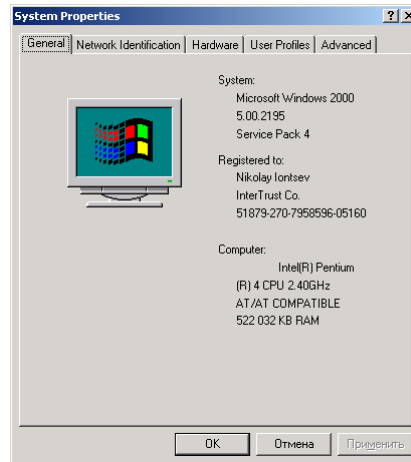


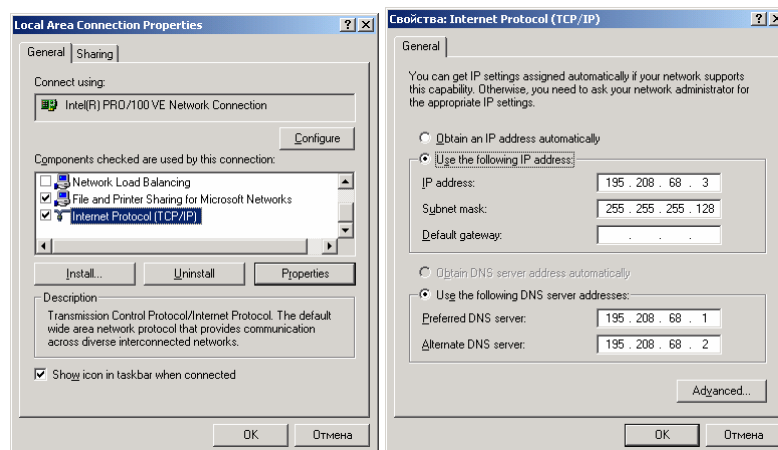
Рис. 19 В каждой организации один домен

1.14. 1.1. Подготовительные действия на компьютере для установки сервера Domino и клиентов

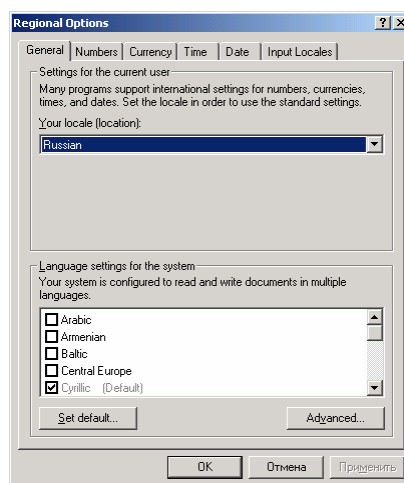
- • Установлены ли необходимые Fix или SP



- • Установлена ли поддержка необходимых сетевых протоколов



- • Имеет ли экаунт, под которым будет выполняться установка, необходимые права (запись в реестр и каталоги)
- • Выбрано ли под экаунтом «русское locale»



1.15. 1.1. Установка первого сервера в организации

1.15.1. 1.1.1. Первая фаза установки

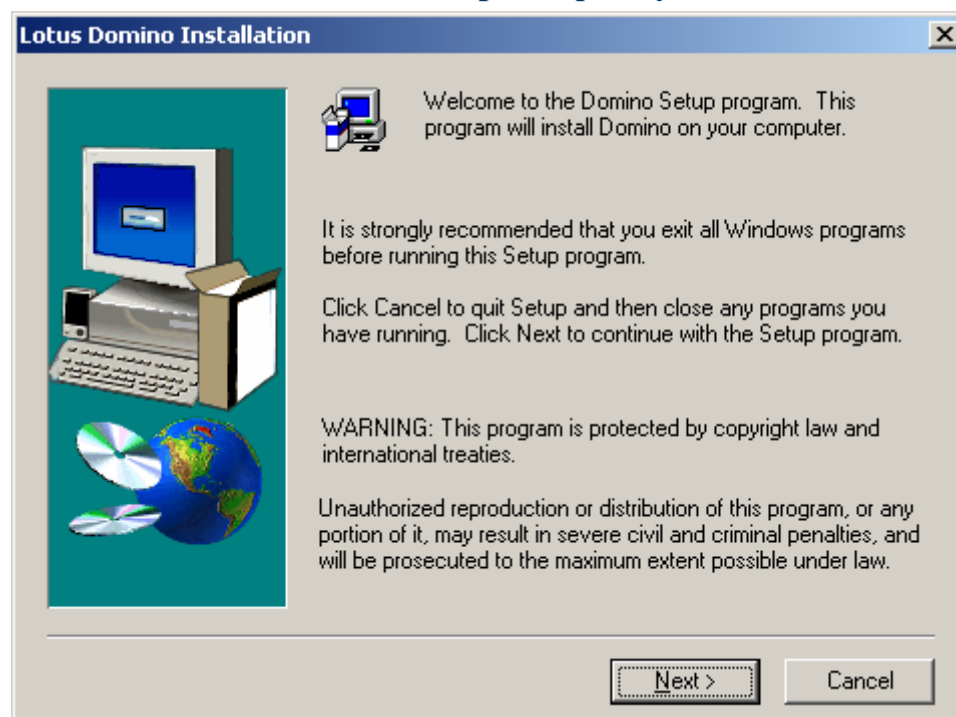


Рис. 20 Без комментариев...

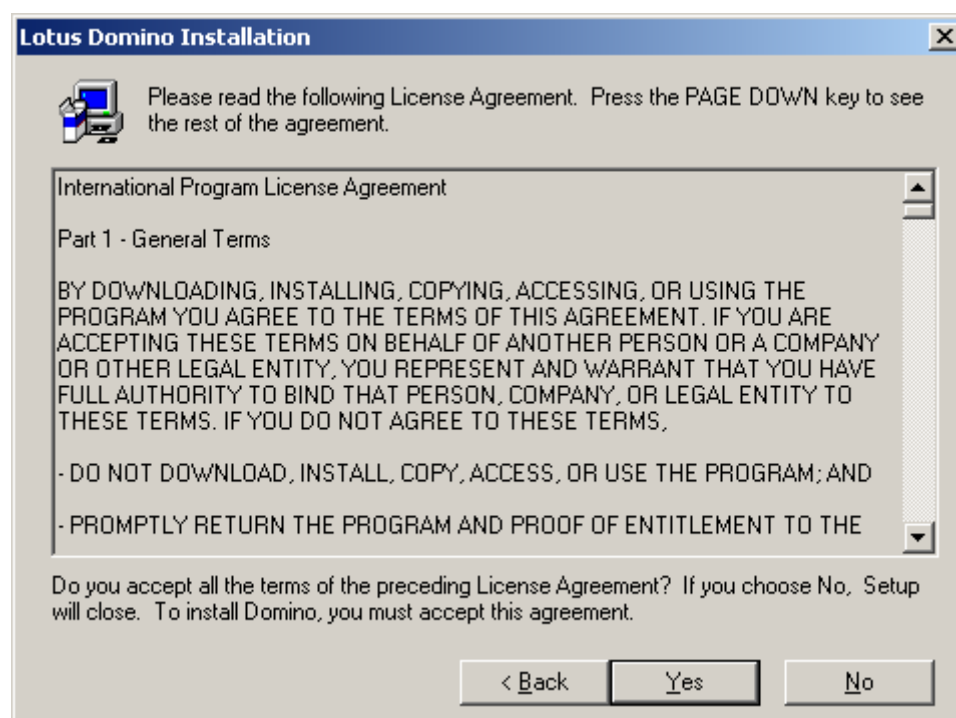


Рис. 21 С лицензионным соглашением всегда согласен...

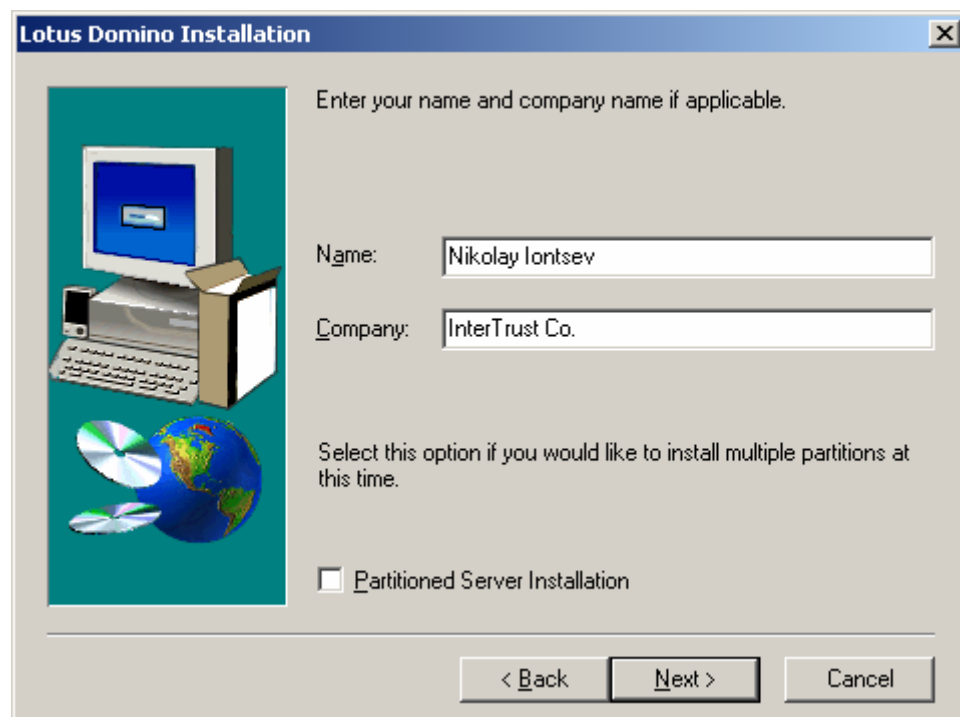


Рис. 22 Выбрана обычная установка (не Partition...)

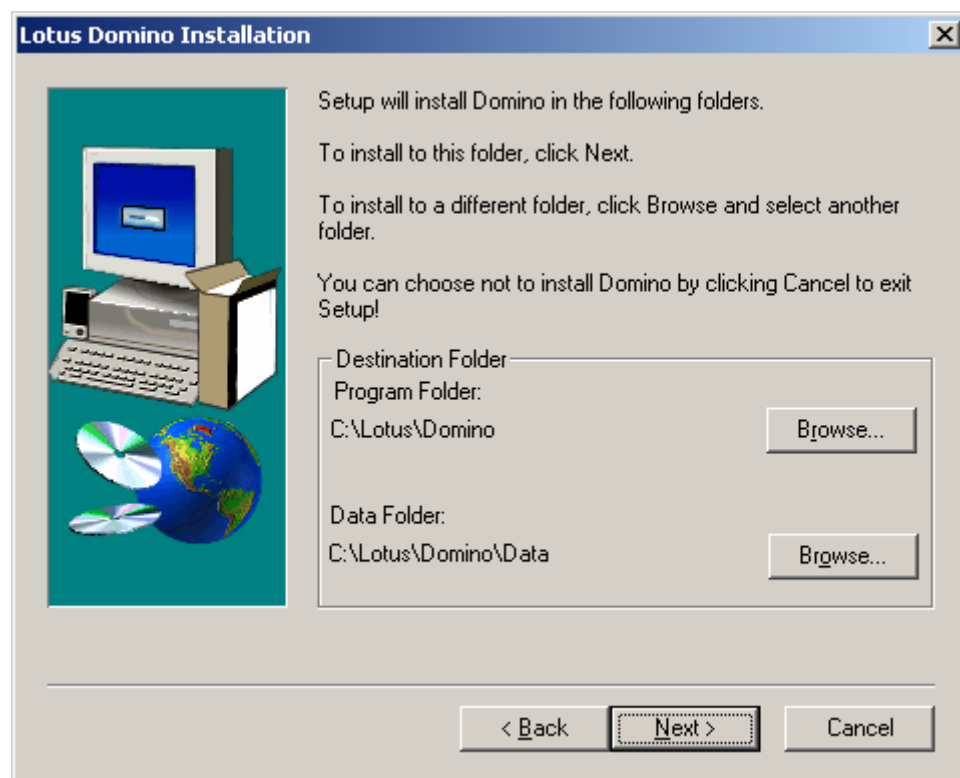


Рис. 23 Выбраны каталоги программ и данных

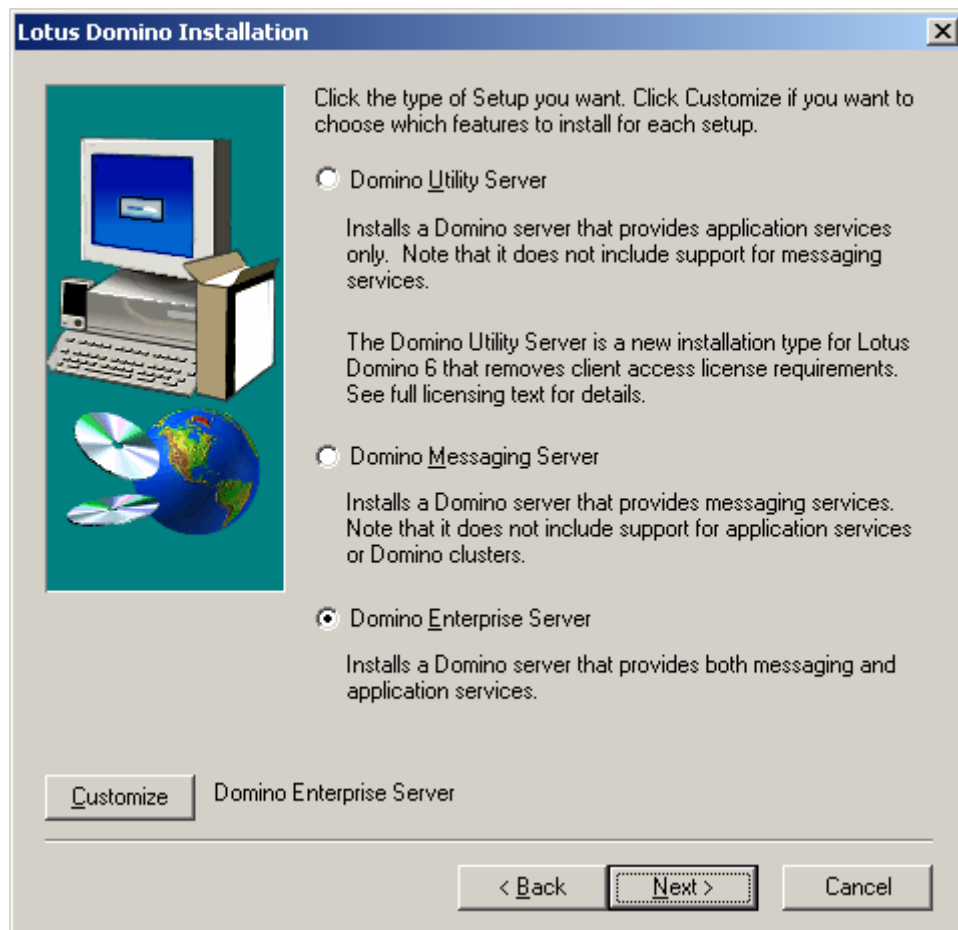


Рис. 24 Выбран тип устанавливаемого сервера и уточнения по кнопке *Customize*

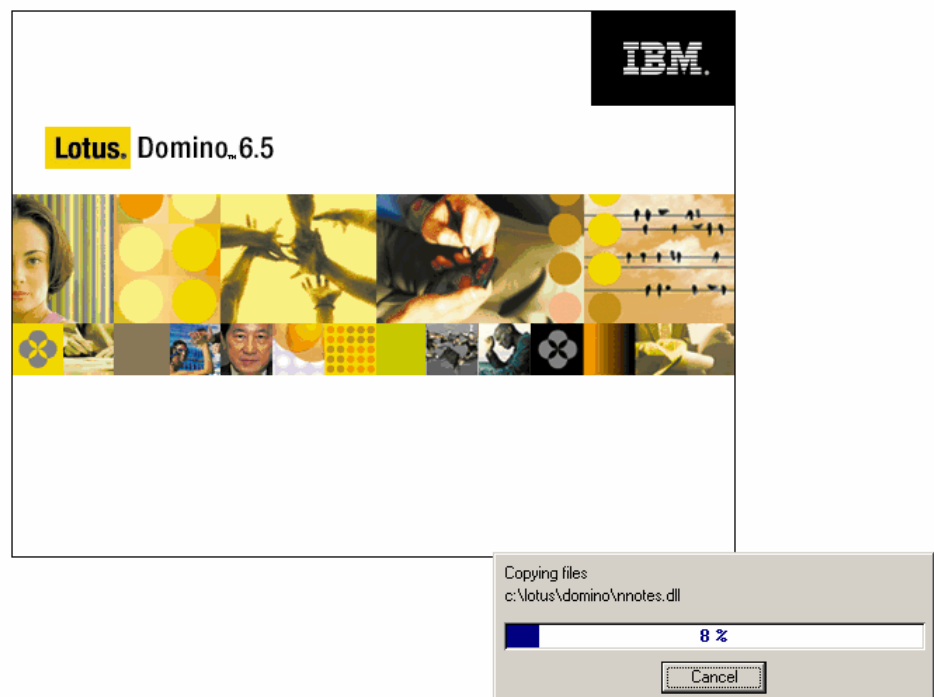


Рис. 25 Выполняется копирование файлов

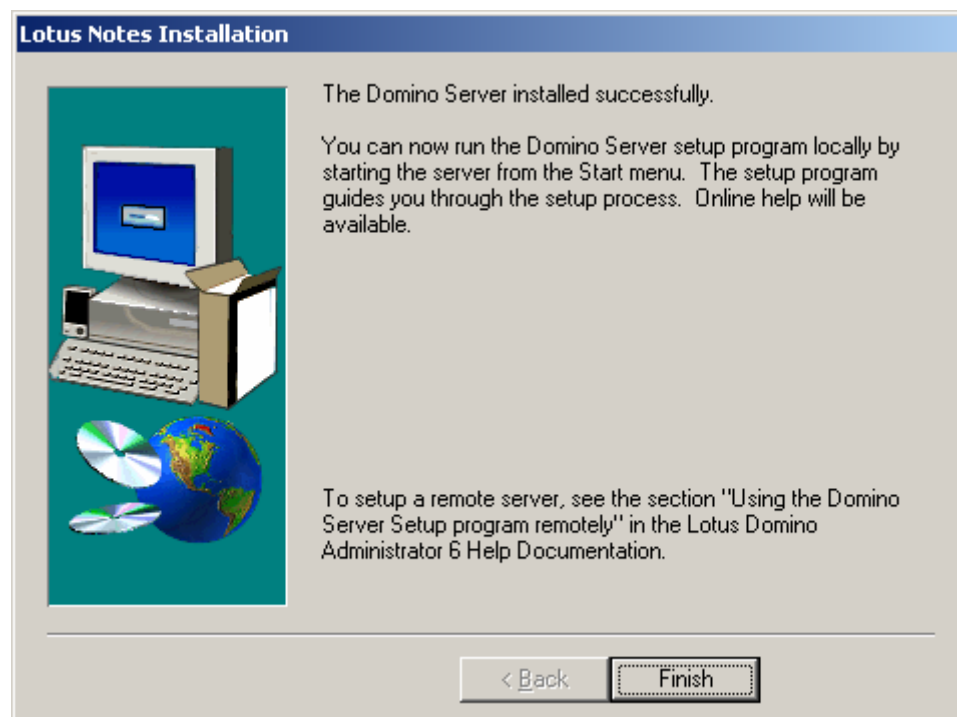


Рис. 26 Конец первой фазы

1.15.1.1. 1.1.1.1. Partition Server Installation

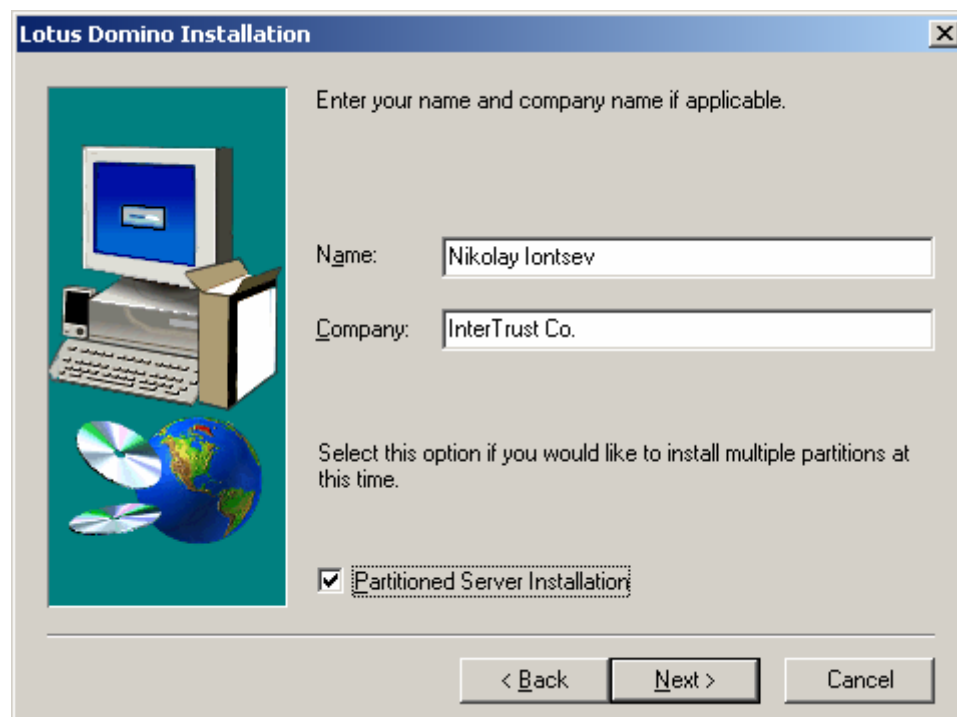


Рис. 27 Выбрана установка нескольких серверов на один компьютер

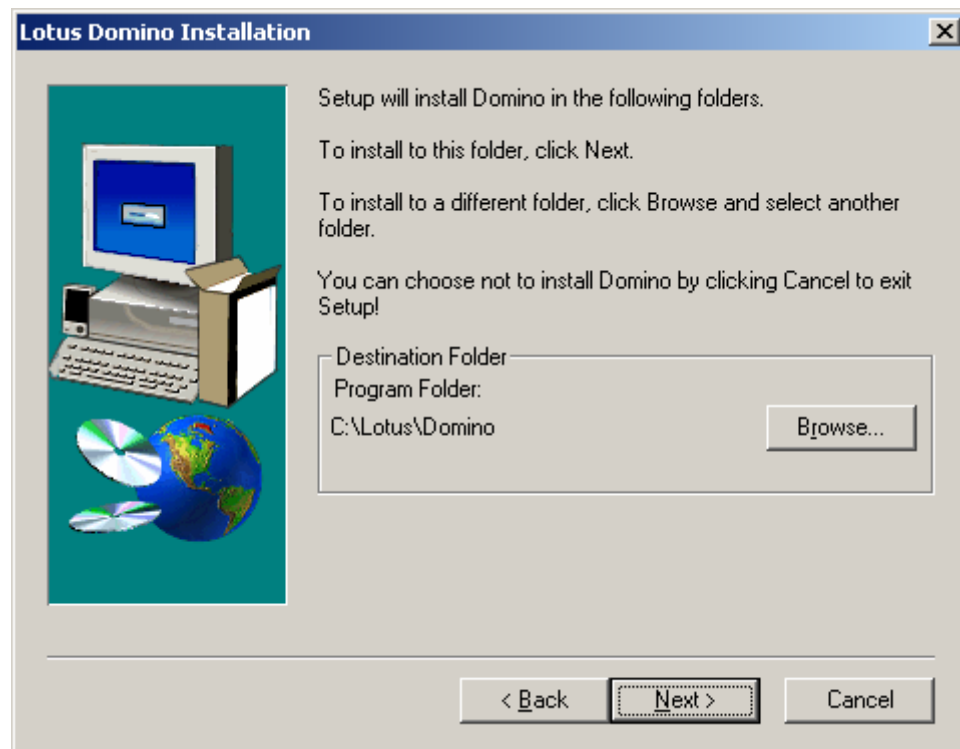


Рис. 28 Каталог программ общий для всех серверов

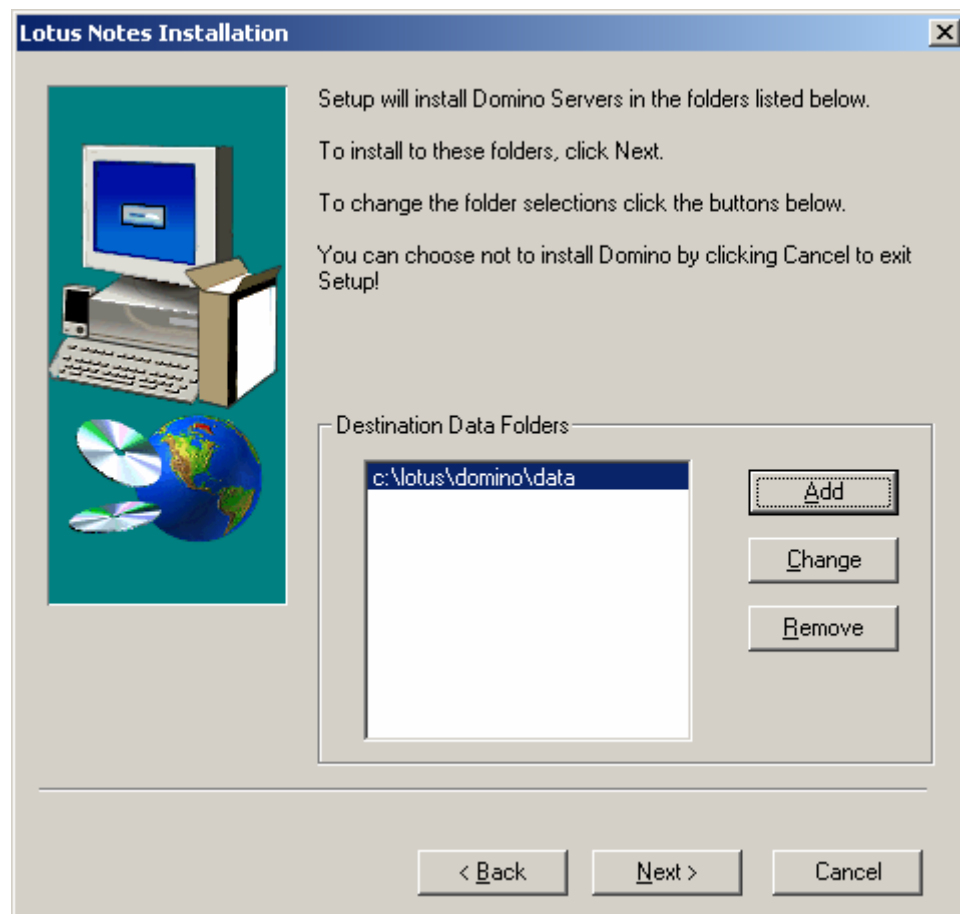


Рис. 29 А каталоги данных разные – у каждого Partition-сервера свой

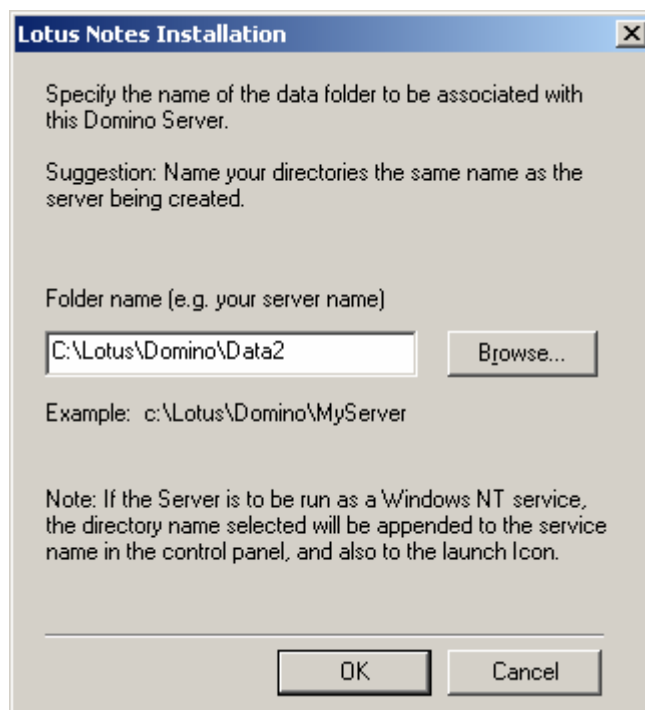


Рис. 30 Добавляем второй Partition-сервер

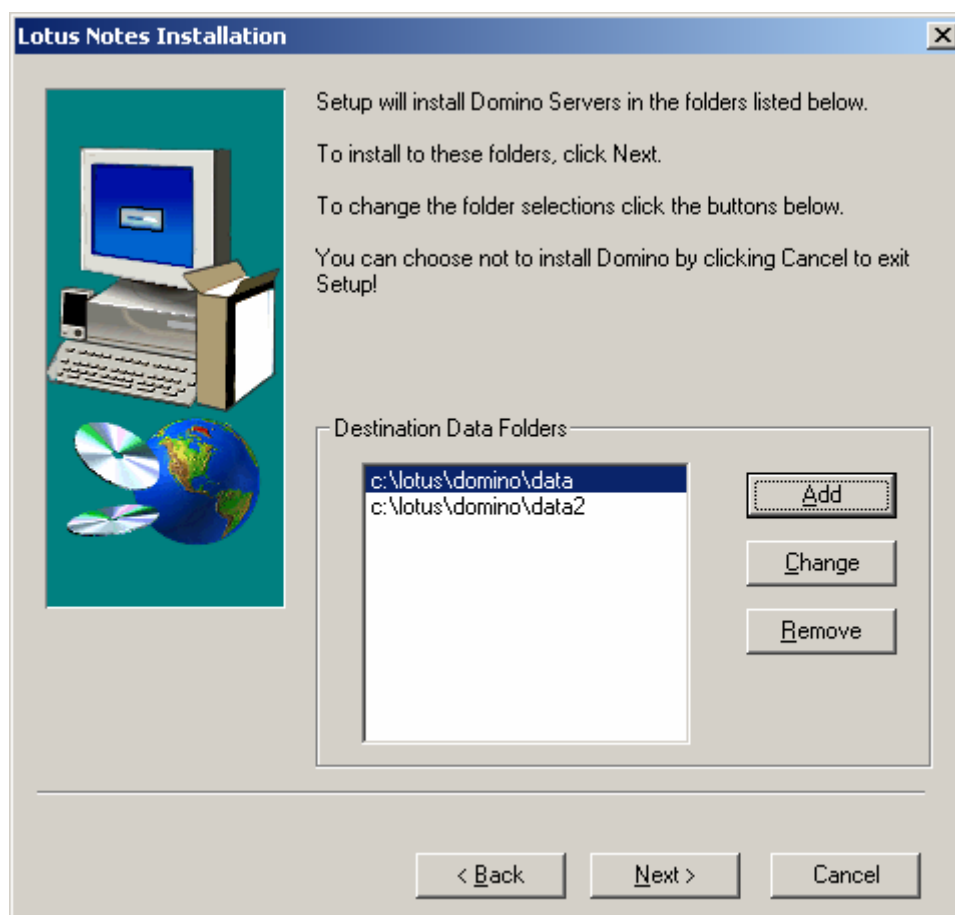


Рис. 31 Так можно сколько угодно раз, вопрос лишь в наличии ресурсов...

Учтите, что Partition-серверы затем потребуют дополнительных настроек, прежде всего касающихся привязки служб к IP-адресам и портам. Наиболее распространенный вариант, когда каждый Partition-сервер имеет свой IP-адрес. Но и в этом случае Вас ждет несложная, но дополнительная работа. Поэтому без четко осознаваемой необходимости устанавливать Partition-серверы вместо обычных не стоит...

1.15.2. 1.1.2. Вторая фаза установки

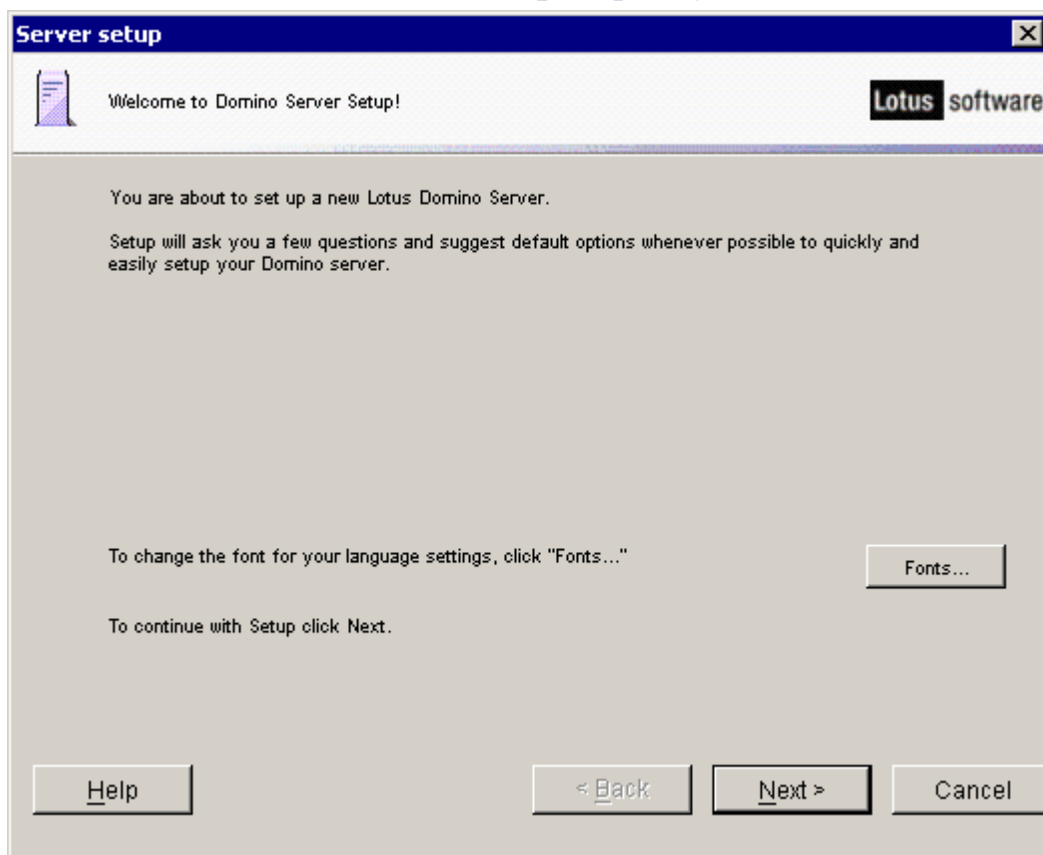


Рис. 32 Можно изменить шрифты

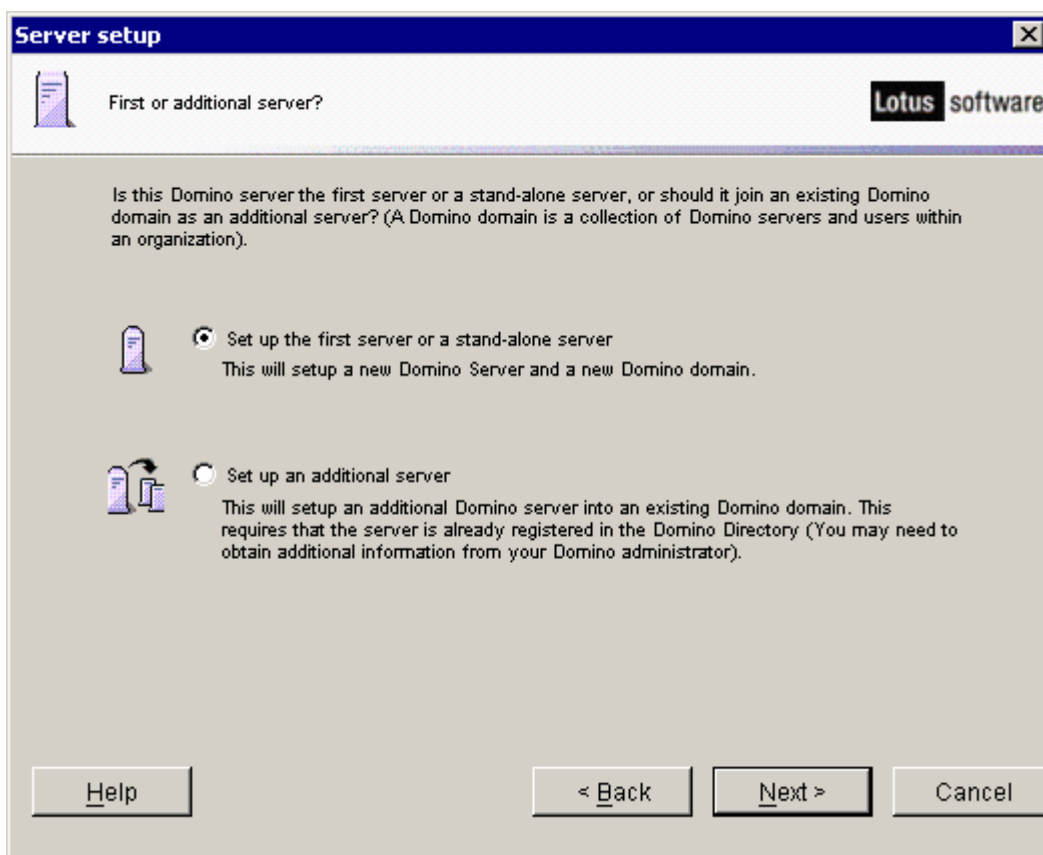


Рис. 33 Выбрана установка первого сервера в новом домене - влечет создание нового каталога Domino (names.nsf)

Server setup [X]

 Provide a server name and title **Lotus software**

You must provide a unique name for your new Domino server. Carefully choose the server name; you cannot easily change it later. By default, Setup recommends that you use the computer's host name as the server name.

 Server name:
For example: Sales1

Optional: Provide a short title which describes the purpose or function of this server. (You can always change this information later in the Domino Directory)

 Server title:
For example: Corporate Sales Server 1

 ☐ I want to use an existing server ID file:
C:\Lotus\Domino\Data\server.id

Рис. 34 Задано имя сервера – wks10-sa

Рекомендации по выбору имен серверов:

- Все серверы в домене Domino должны иметь уникальные CN. Например, два сервера с именами Server/MSK/Company и Server/SPB/Company имеют одинаковое CN Server.
- CN сервера, работающего по протоколу TCP/IP, должно совпадать с именем хоста или FQDN. Например, wks10-sa/WWCorp, если этот сервер и все его клиенты согласно настройкам протокола TCP/IP (домен по умолчанию) находятся в одном домене Internet intrust.ru, или wks10-sa.intrust.ru/WWCorp, если сервер должен быть доступен клиентам и серверам из других доменов Internet.

Рис. 35 Заданы имя сертификатора организации - /WWWCorp – и пароль для ID-файла сертификатора

Следующее окно получают при нажатии кнопки Customize... в предыдущем.

Рис. 36 В окне, получаемом по кнопке Customize..., можно выбрать код страны, например, RU, что повлекло бы изменение имени сертификатора организации на /WWWCorp/RU, а так же решить проблему предыдущих версий – установку первого сервера сразу в подразделении первого уровня (OUI). Для этого задают название подразделения первого уровня, например, Sales (тогда имя сертификатора подразделения будет /Sales/WWWCorp/RU), и пароль для ID-файла сертификатора этого подразделения.

Server setup [X]

Choose the Domino domain name Lotus software

As part of setting up the first Domino server, Setup creates a new Domino domain, which is a collection of Domino servers and users that share the same Domino Directory.

The Domino domain name can be the same as the organization name. Choose a short domain name.

Domino domain name: For example: Acme

Рис. 37 Задано название домена – *WWCorp* – в данном случае оно совпадает с именем организации

Server setup [X]

Specify an Administrator name and password Lotus software

To create the Administrator's ID, you must provide the administrator's name and password. You can use the name of a specific person, or a last name only to create a generic Administrator ID that can be used by several people.

First name: Middle: Last name (or generic account name):

Administrator password: Confirm password:

Minimum of 5 characters

The Administrator ID file will be stored inside the server's Domino Directory.

☒ Also save a local copy of the ID file:

C:\Lotus\Domino\Data\admin.id

☐ I want to use an existing Administrator ID file:

C:\Lotus\Domino\Data\admin.id

Рис. 38 Заданы имя администратора и пароль для его ID-файла. ID-файл сохраняется в каталоге Domino и, дополнительно (такая возможность отсутствовала в предшествующих версиях) в файле

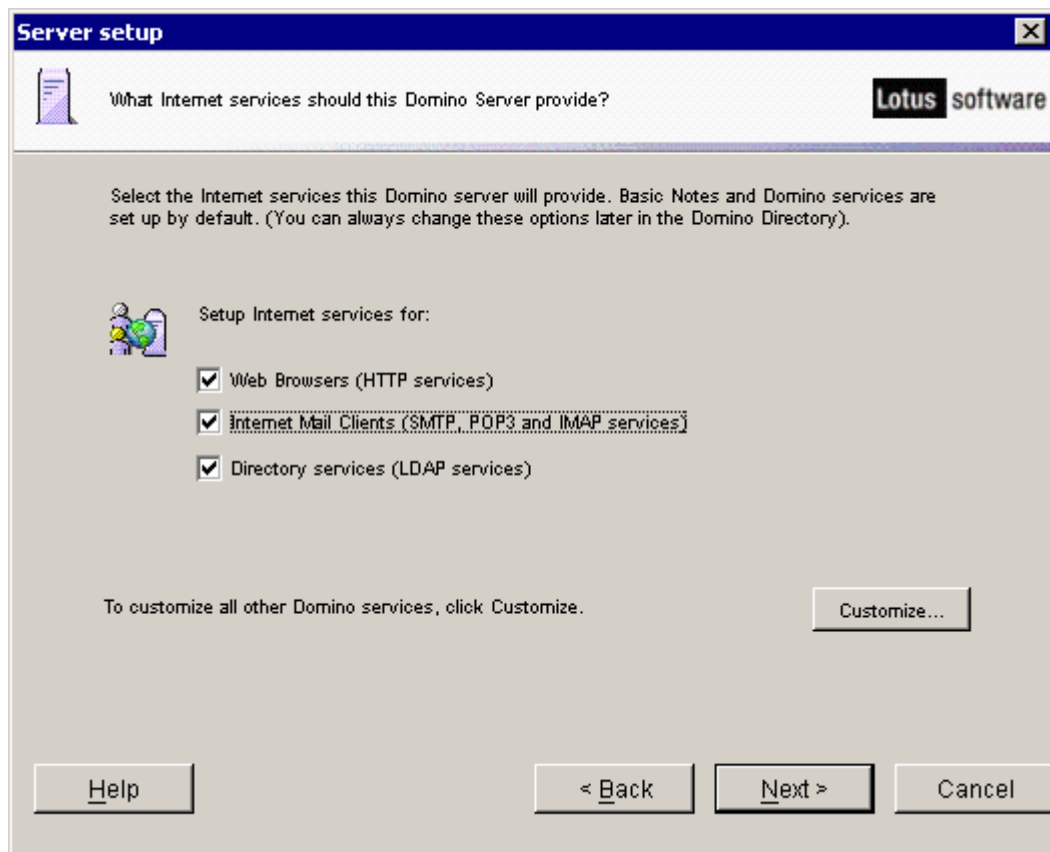


Рис. 39 Выбор списка задач, запускаемых при старте сервера. Делать это желательно в окне, открываемом по кнопке *Customize...*

Следующее окно получают при нажатии кнопки *Customize...* в предыдущем.

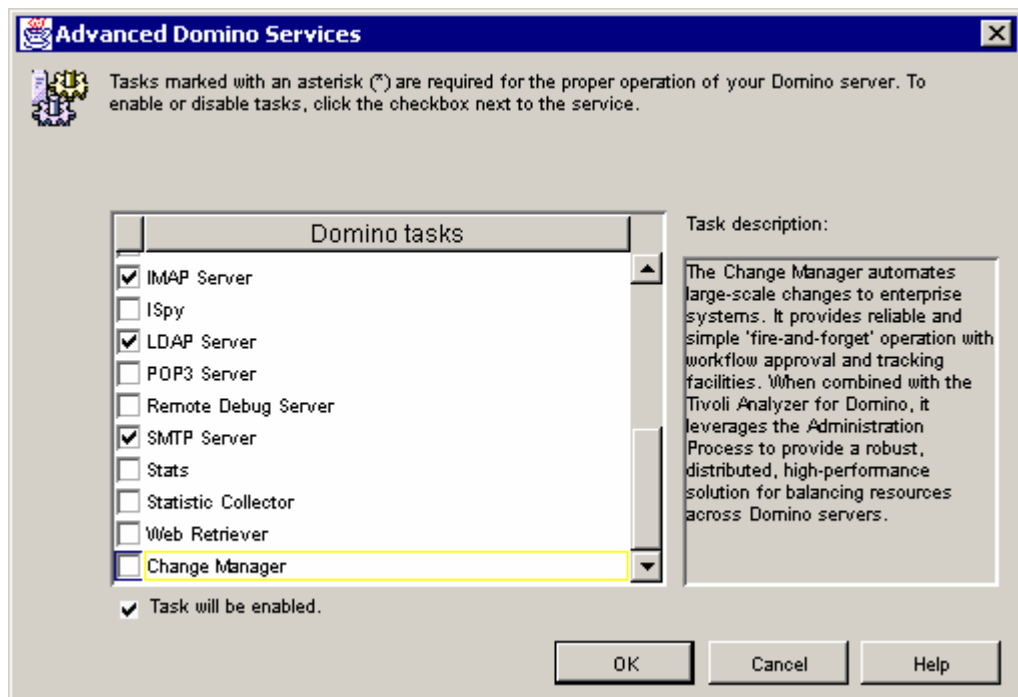


Рис. 40 Выбран список задач, запускаемых при старте сервера

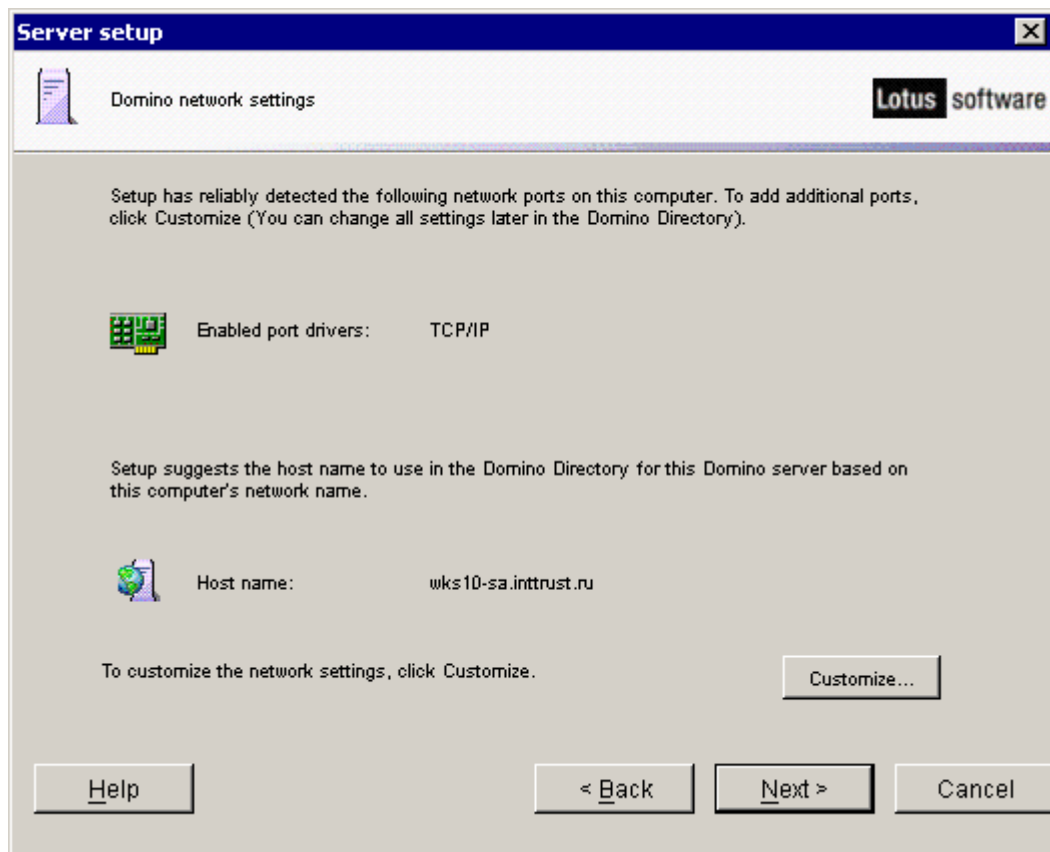


Рис. 41 Конфигурирование портов – подробности доступны в окне по кнопке Customize...

Следующее окно получают при нажатии кнопки Customize... в предыдущем.

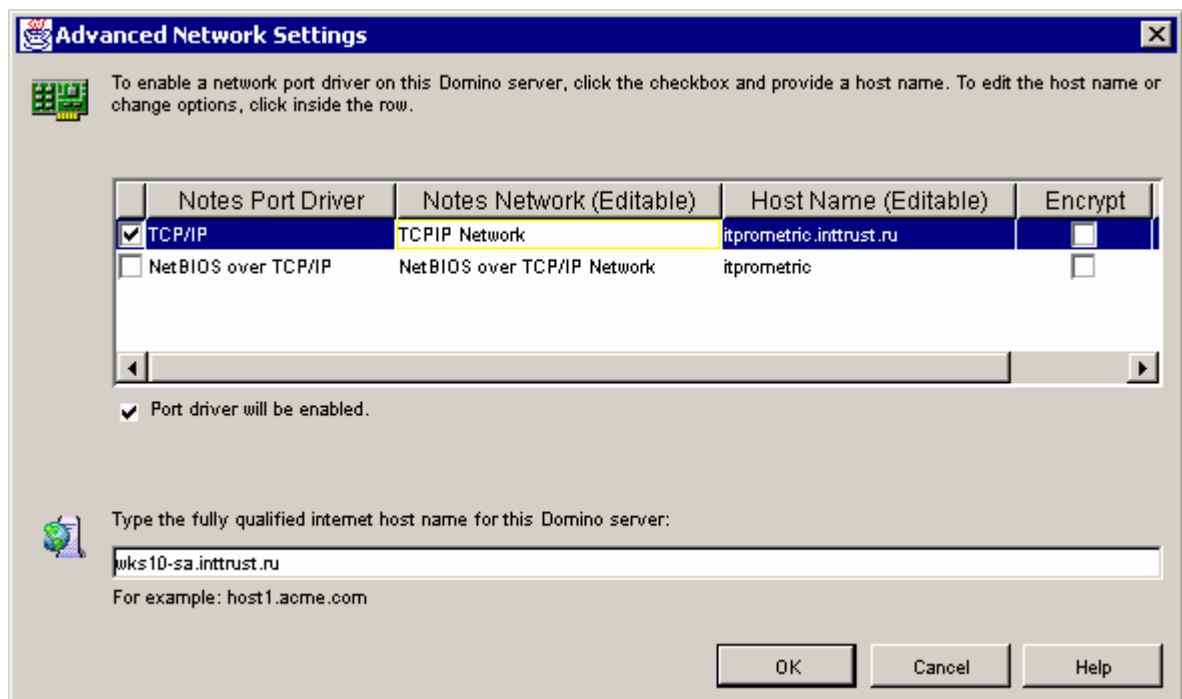


Рис. 42 Конфигурирование портов – выбор нужных портов, названий поименованных сетей, имен хостов, шифрования на порту и...

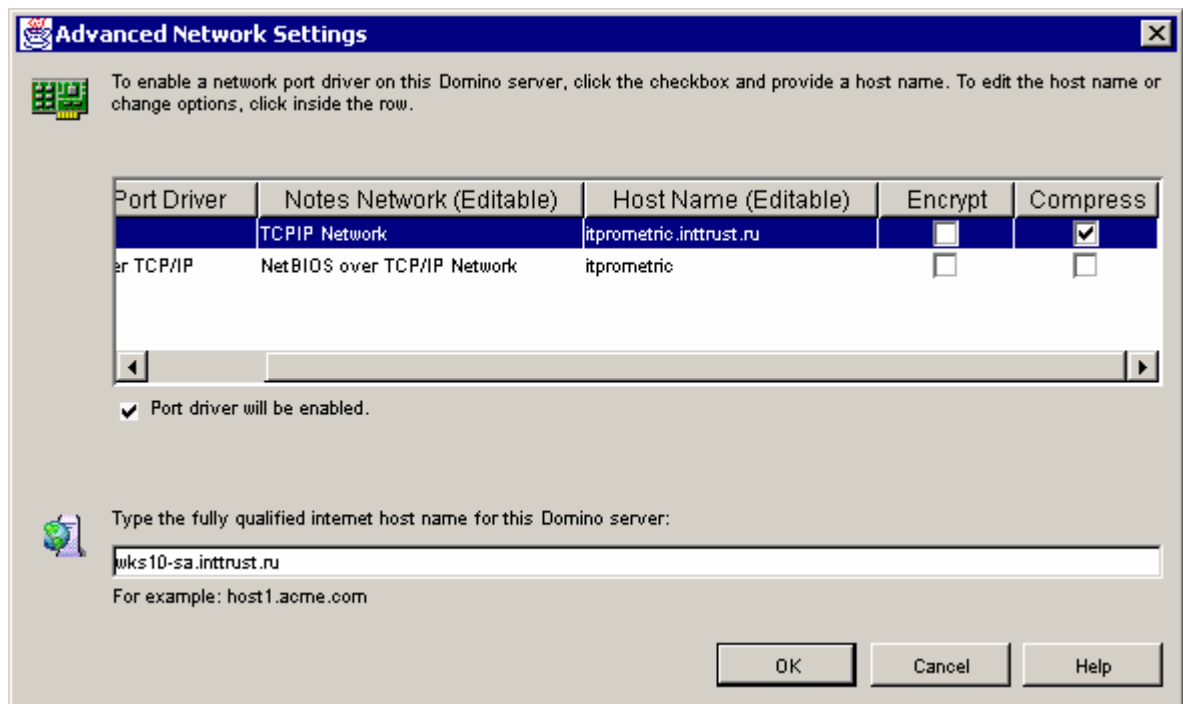


Рис. 43 ...новой возможности – компрессии сетевого трафика по порту.

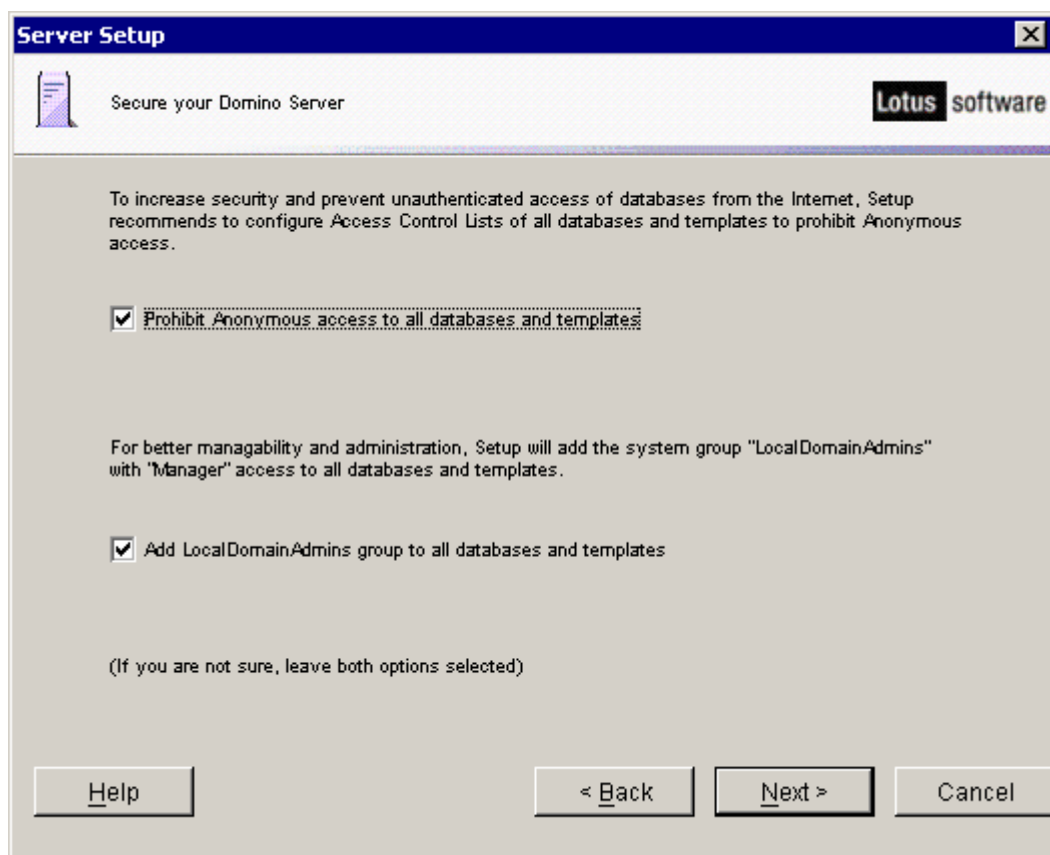


Рис. 44 Добавить во все базы и шаблона группу LocalDomainAdmins (в предшествующих версиях использовалась группа Administrators) с уровнем доступа Manager и Анонимус с уровнем доступа No Access

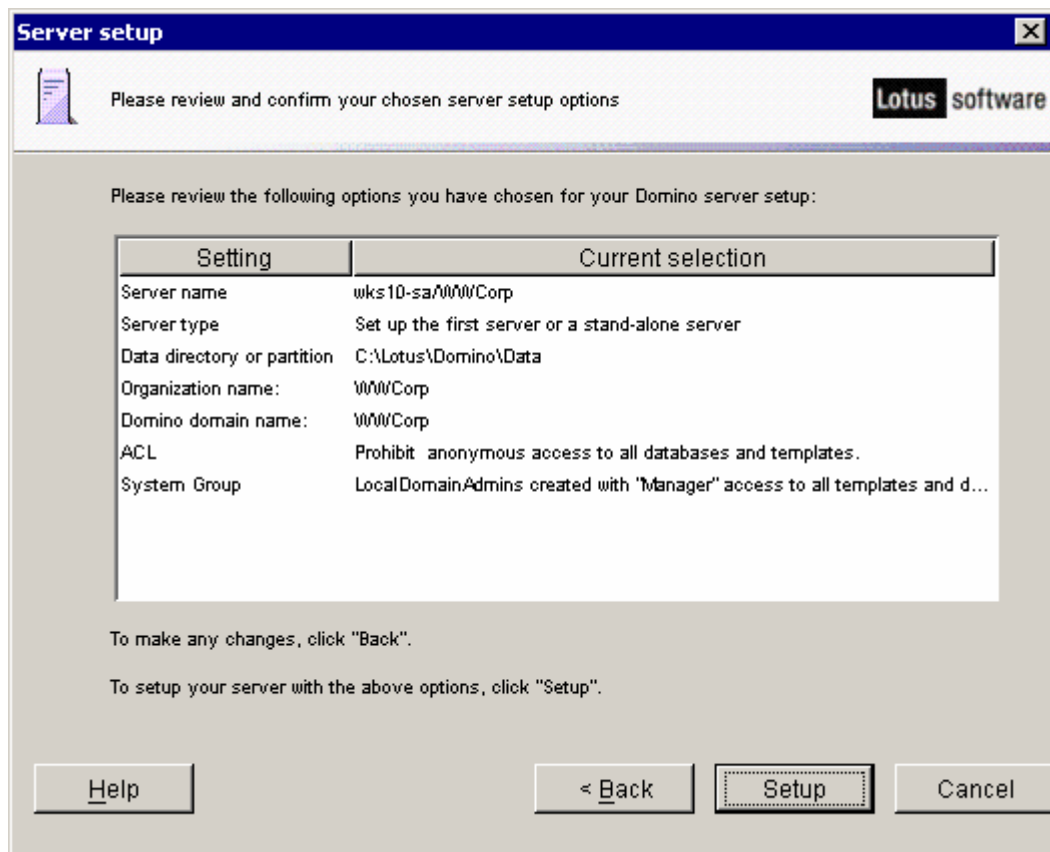


Рис. 45 Основные из выбранных параметров

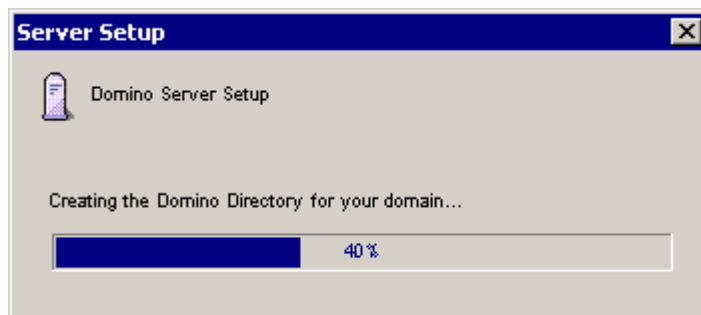


Рис. 46 Идет процесс установки

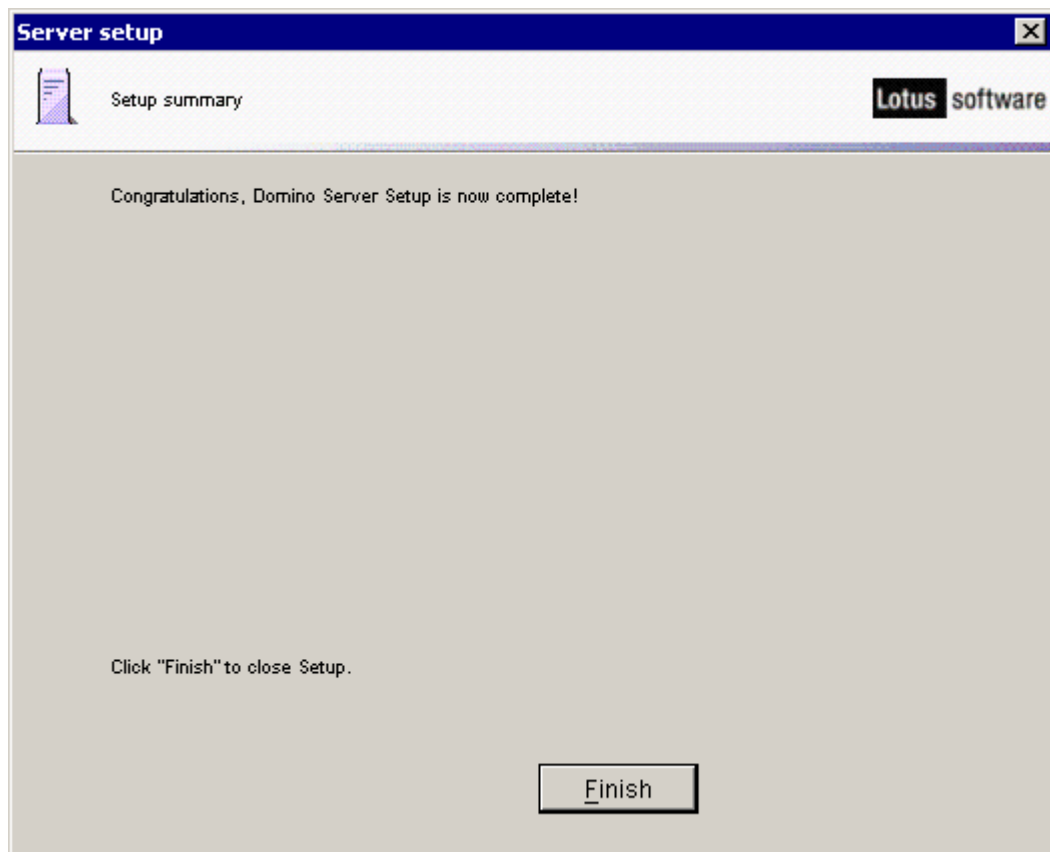


Рис. 47 Установка завершена

1.15.3. 1.1.3. Запуск сервера

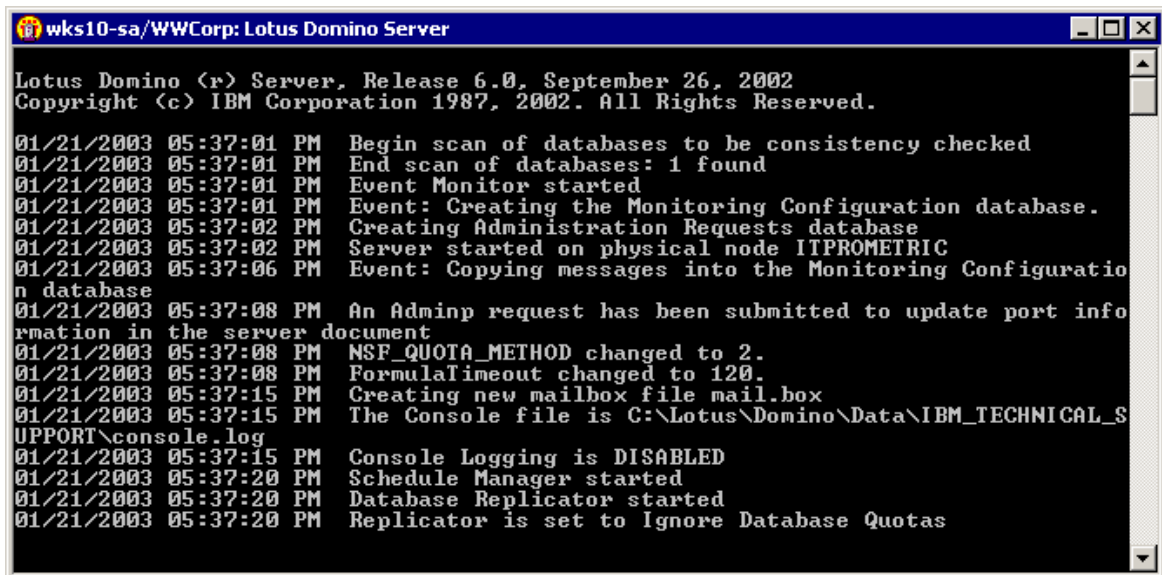


Рис. 48 Первый реальный запуск сервера, формат времени указывает на то, что на компьютере было неправильно выставлено Locale

1.16. 1.1. Установка клиентов Notes, Designer и Administrator

1.16.1. 1.1.1. Первая фаза установки - Install

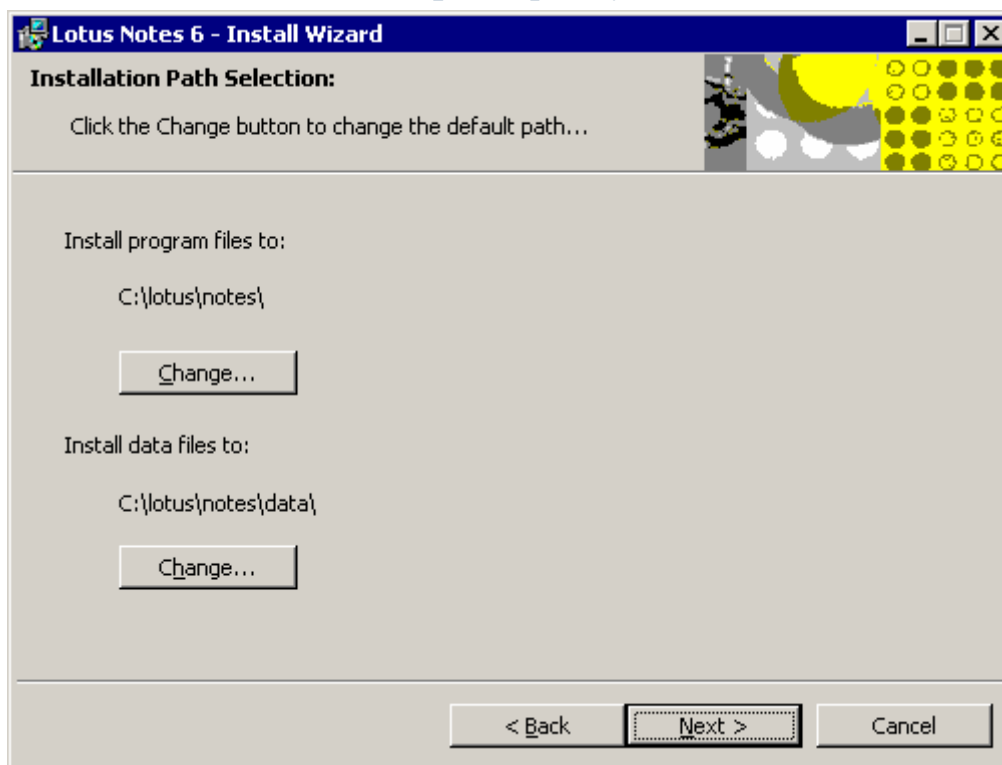


Рис. 49 Выбираем каталог программ и данных. Такая установка не бывает в варианте «Multiple Users»

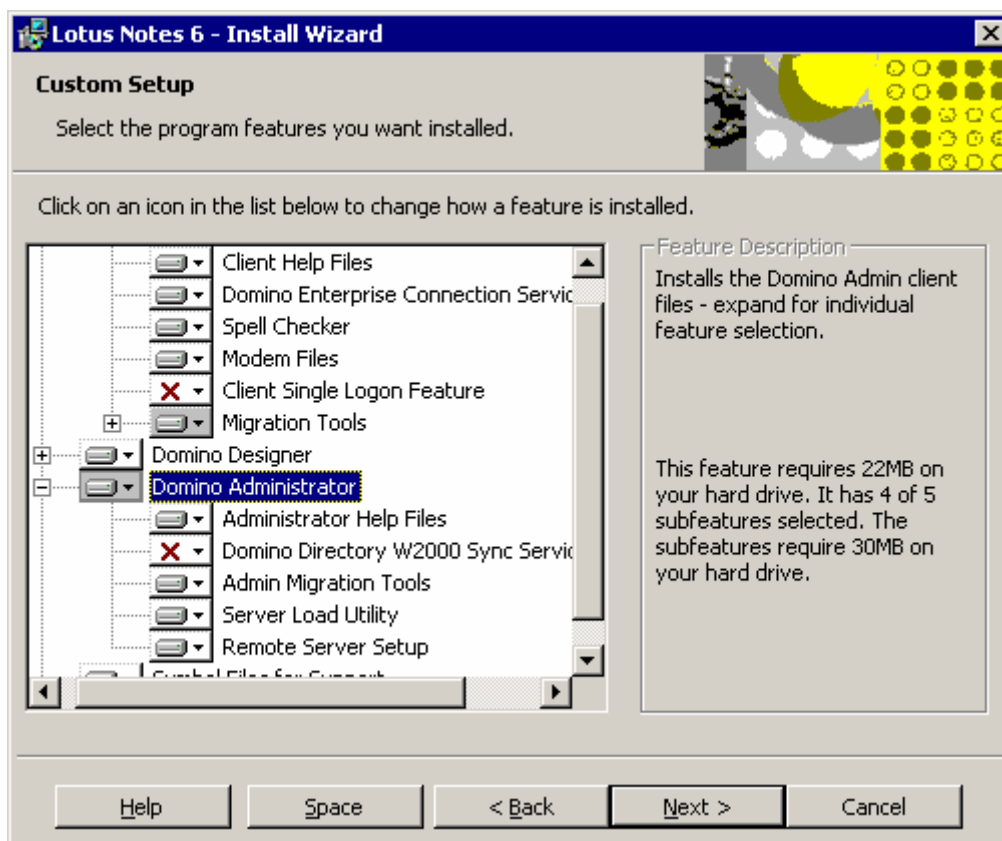


Рис. 50 Выбираем устанавливаемые компоненты – практически все. Обратите внимание, что многие компоненты Администратора по умолчанию не выбраны

1.16.2. 1.1.2. Вторая фаза - Setup

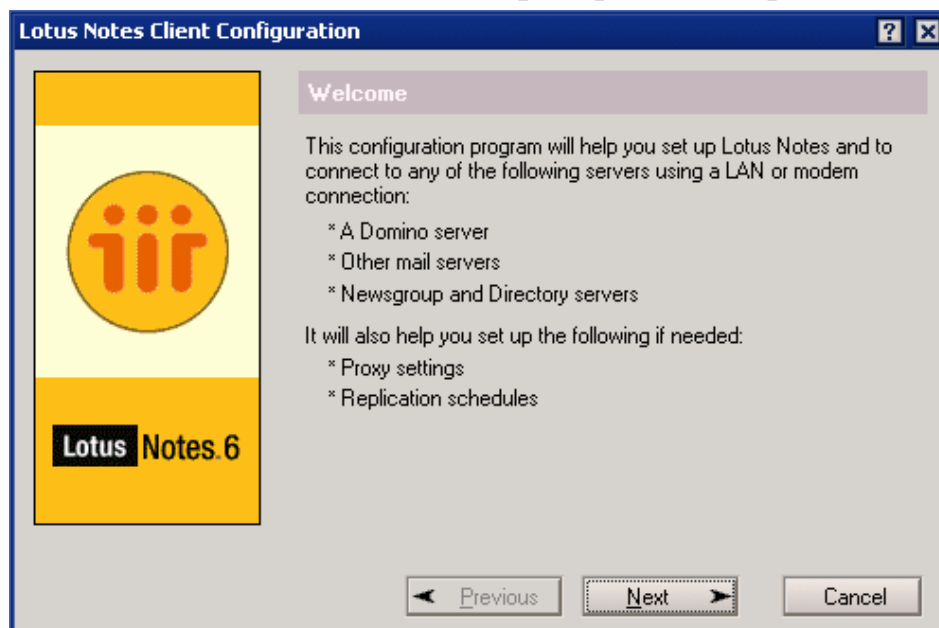


Рис. 51 Очевидно Next...

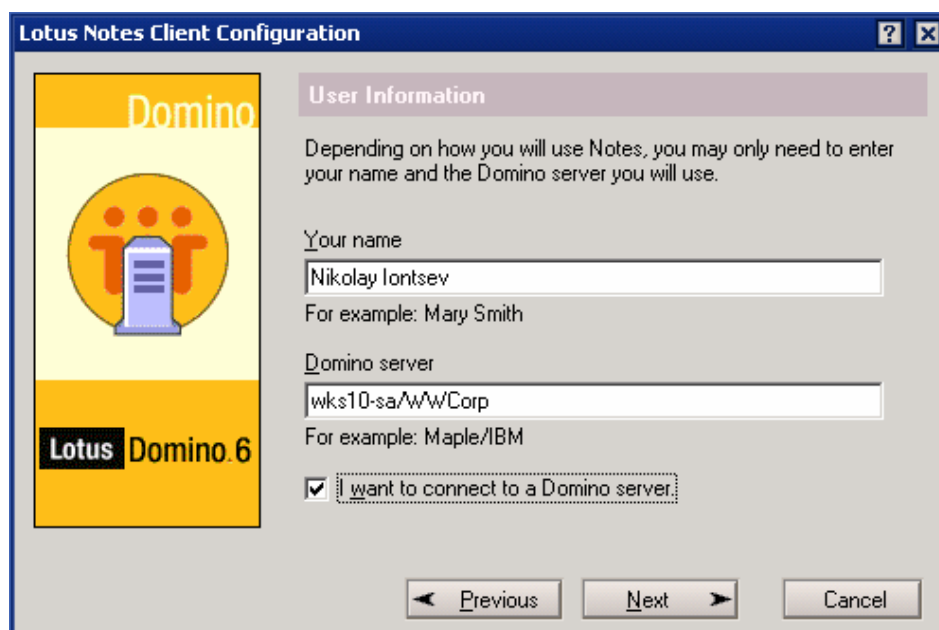


Рис. 52 Имя пользователя, сервер Domino (обычно тот, на котором находится почтовый файл пользователя) и «галка» I want to connect to a Domino server (иначе будет установка «автономного» клиента)

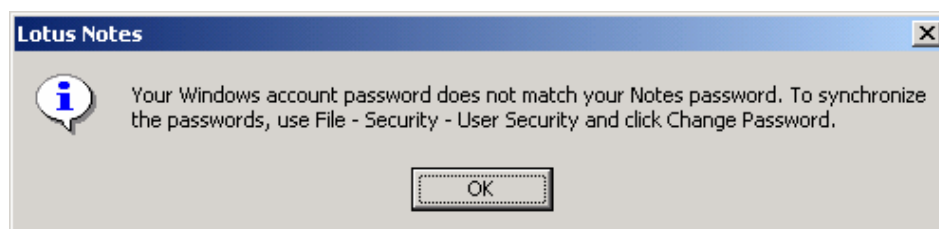


Рис. 53

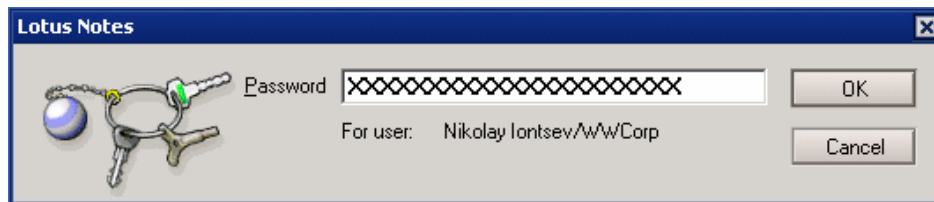


Рис. 54 К моменту появления этого окна клиент Notes уже установил соединение с сервером wks10-sa/WWCorp, «нашел» в каталоге Domino по имени Nikolay Iontsev соответствующий документ Person, а в нем присоединенный ID-файл. После ввода пароля ID-файл будет скопирован на станцию пользователя и удален из документа Person на сервере

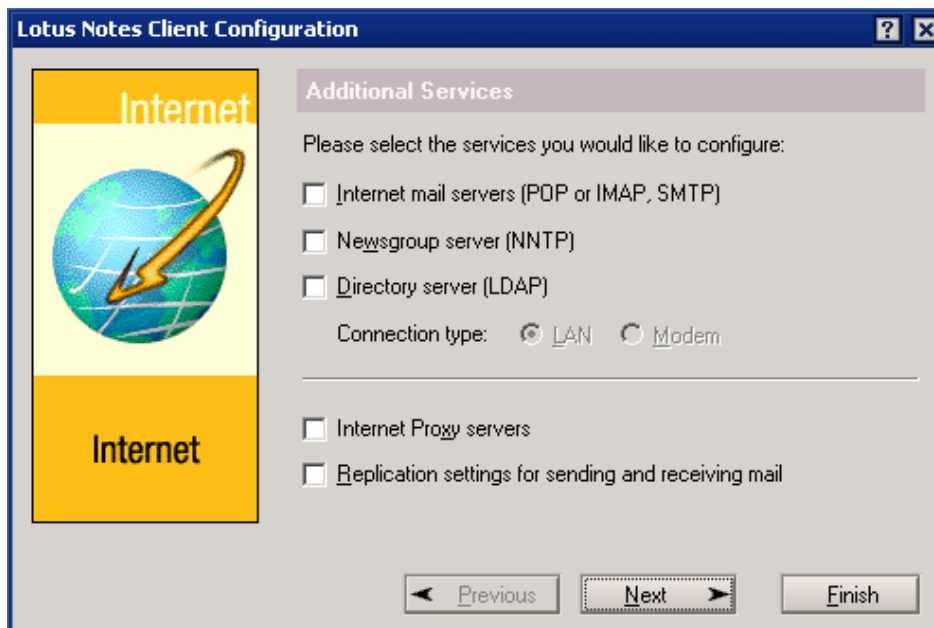


Рис. 55 Создание экаунтов, настройка используемого проху-сервера и выбор параметров репликации для почтового файла сведен в одно окно – поэтому от всего этого легко отказаться...

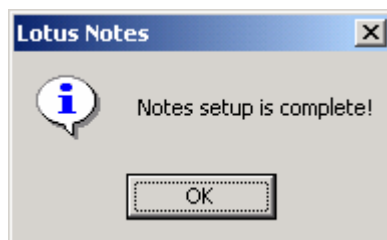


Рис. 56 Установка завершена

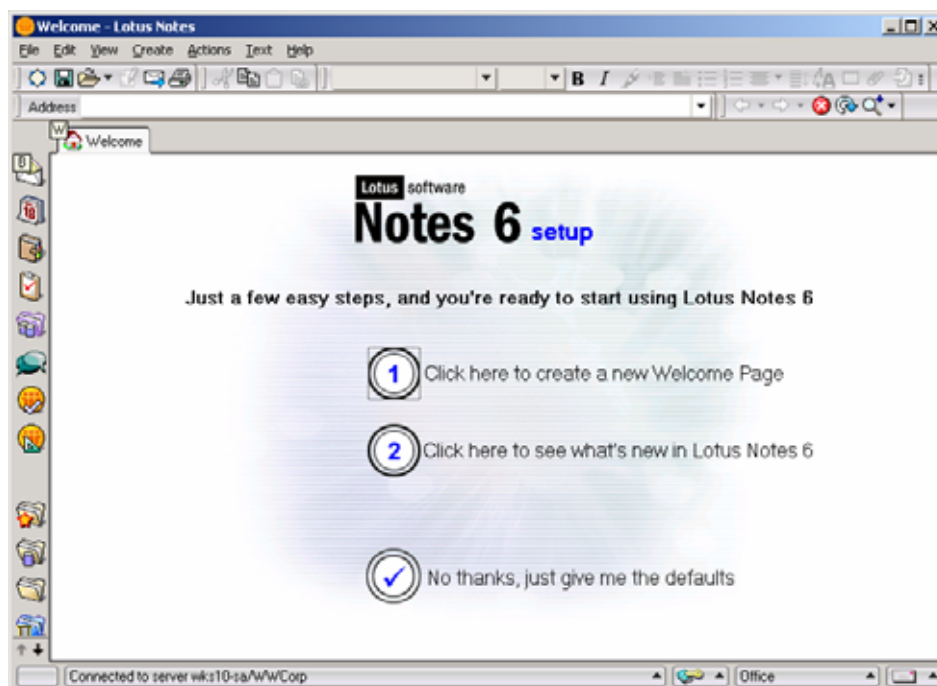


Рис. 57 Первый запуск клиента Notes

1.16.3. 1.1.3. Запуск клиента Администратора

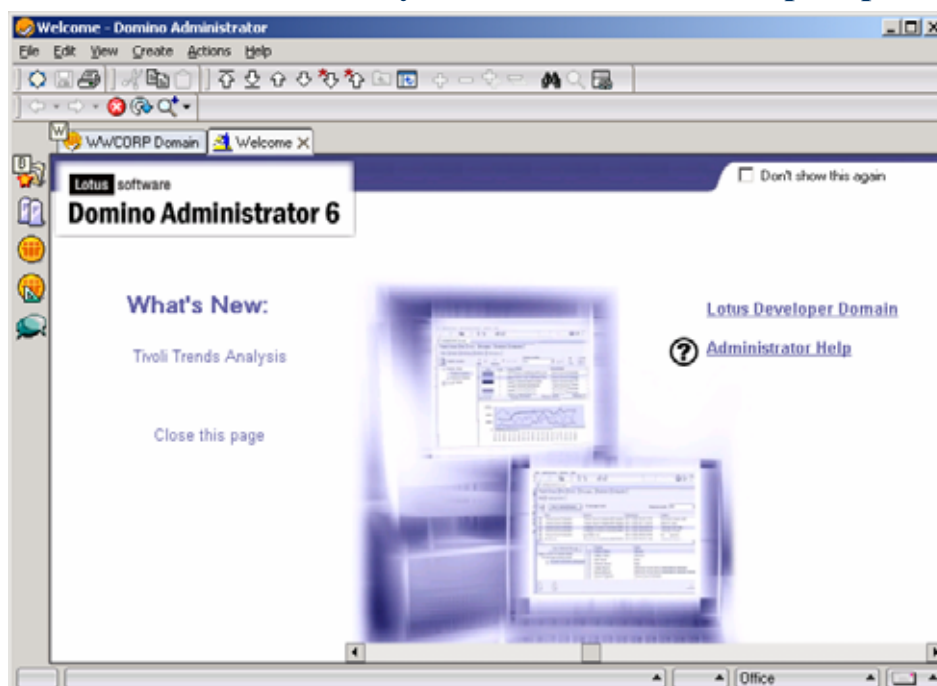


Рис. 58 По традиции непосредственно из клиента...

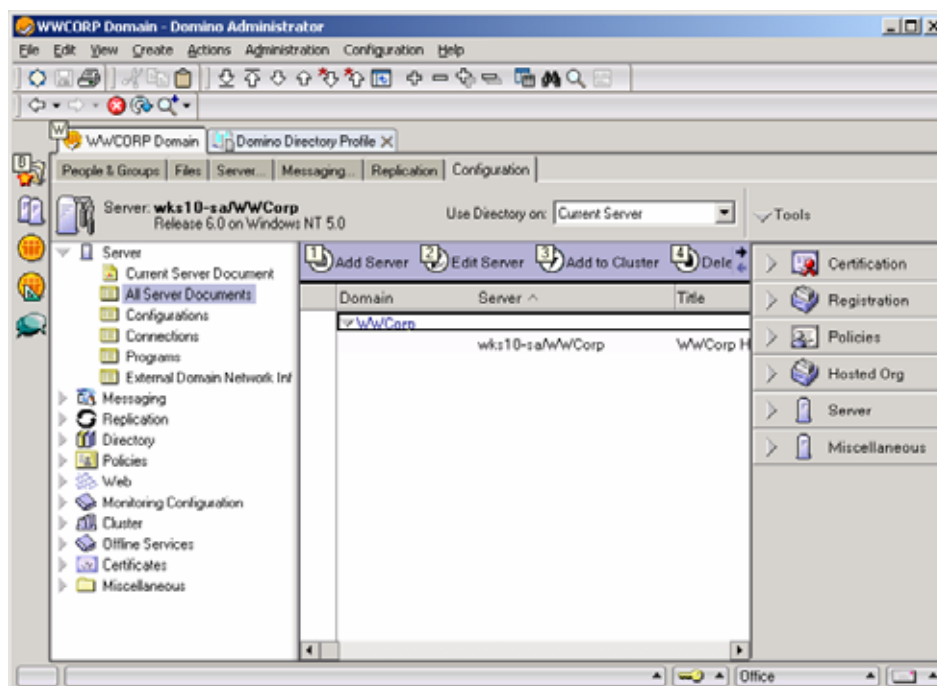


Рис. 59 6 закладок

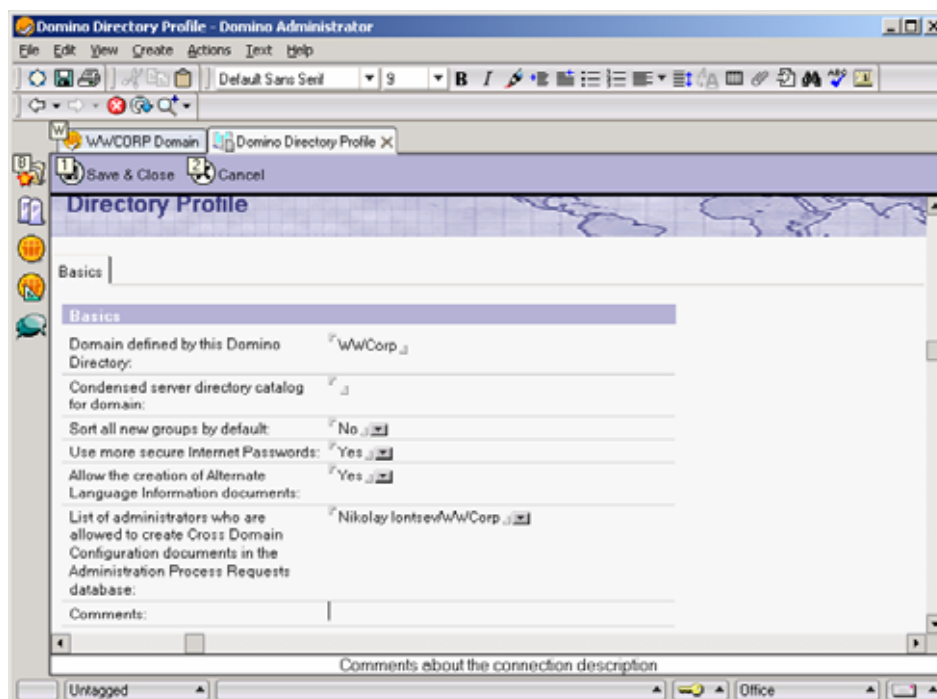


Рис. 60 При первом открытии каталога Domino на первом сервере предлагается заполнить профильный документ каталога

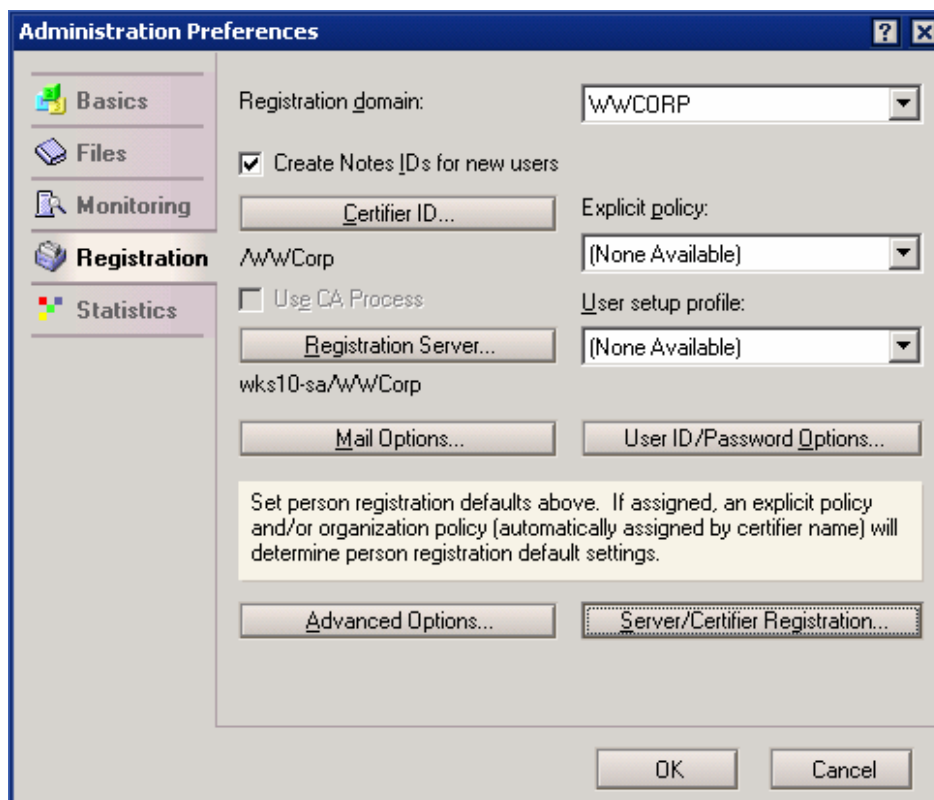


Рис. 61 Далее полезно задать параметры клиента администратора. Обратите внимание на новую закладку Statistics...



Рис. 62 При выборе в предшествующем окне местоположения ID-файла сертификатора организации появляется сообщение об отсутствии в нем Recovery Information

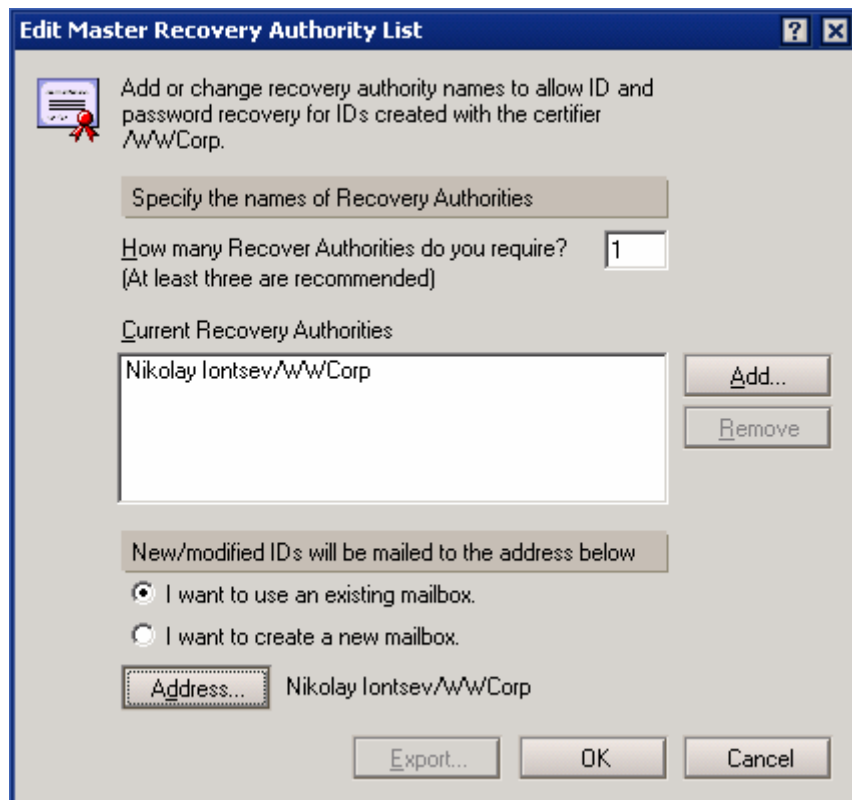


Рис. 63 В «реальной жизни» лучше как можно раньше добавить Recovery Information в ID-файл сертификатора организации... Только не так «примитивно», как проделано в этом окне... Однако в учебном классе мы сделаем это позже, при подробном рассмотрении темы Recovery Information

1.16.4. 1.1.4. Регистрация дополнительных серверов

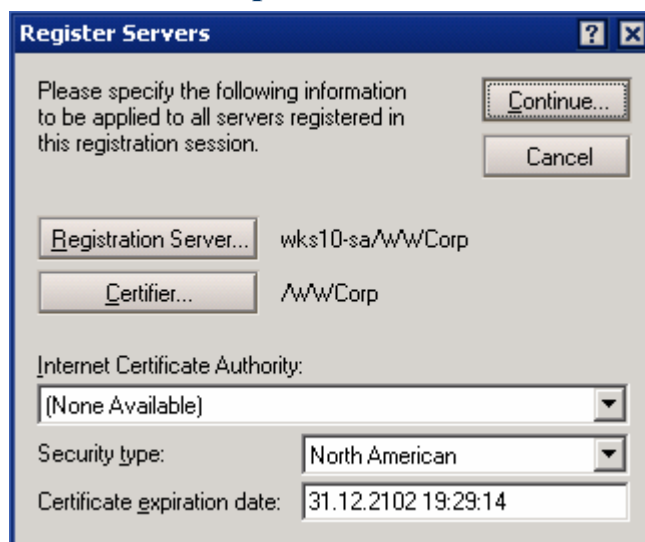


Рис. 64 Единственное отличие от R5 – поле Internet Certificate Authority

Register New Server(s)

Basics

Registration Server: wks10-sa/WWCorp

Certifier: /WWCorp

Advanced

Server name: wks01-sa

Server title:

Domino domain name: WWCORP

Server administrator name: LocalDomainAdmins

ID file password:

Weak Password quality scale: Strong

Password is optional (0)

Location for storing server ID:

☐ In Domino Directory

☒ In file: Set ID File... C:\lotus\notes\...\ids\servers\wks01sa.id

New Server

Server Name ^	Registration Status ^	Date ^
wks01-sa	Ready for registration	24.01.2003

Register All Register Remove Done

Рис. 65 Первый дополнительный сервер...

Register New Server(s)

Basics

Registration Server: wks10-sa/WWCorp

Certifier: /WWCorp

Advanced

Server name: wks11-sa

Server title:

Domino domain name: /WWCORP

Server administrator name: LocalDomainAdmins

ID file password:

Weak Password quality scale: Strong

Password is optional (0)

Location for storing server ID:

☐ In Domino Directory

☒ In file: Set ID File... C:\lotus\notes\...\ids\servers\wks11sa.id

New Server

Server Name ^	Registration Status ^	Date ^
wks07-sa	Ready for registration	24.01.2003
wks08-sa	Ready for registration	24.01.2003
wks09-sa	Ready for registration	24.01.2003
wks11-sa	Ready for registration	24.01.2003

Register All Register Remove Done

Рис. 66 ... и остальные по его образу и подобию, затем Register All

1.16.5. 1.1.5. Регистрация пользователей – администраторов дополнительных серверов

Register Person -- New Entry

Provide name, password and other basic information for the new person. To view/edit additional registration settings, check the 'Advanced' checkbox below.

Registration Server... wks10-sa/WwCorp

First name: Admin Middle name: Last name: WKS05SA Short name: AWKS05SA

Password: 11111111 Mail system: Lotus Notes Explicit policy: (None Available)

Password Options... No organization policy assigned to this person

Policy Synopsis...

☒ Create a Notes ID for this person

☒ Advanced New Person Migrate People... Import Text File... [OK] [Cancel]

Registration Queue (local):

User Name	Registration Status	Date
WKS01SA, Admin	Ready for registration	24
WKS02SA, Admin	Ready for registration	24
WKS03SA, Admin	Ready for registration	24
WKS04SA, Admin	Ready for registration	24

Register All Register Delete Options... Views... Done

Рис. 67 Закладка Basics – из нового ПОЛИТИКИ

Register Person -- New Entry

Mail system: Lotus Notes Mail Server... wks10-sa/WwCorp

Mail file name: mail\awks05sa Mail file template: Lotus SmartSuite Library (6) Mail (R6) Microsoft Office Library (6) Personal Address Book Personal Journal (R6) TeamRoom (6)

☒ Create file now ☐ Create file in background

Mail File Replicas... About... mail6.ntf

Mail file owner access: Manager

☐ Create full text index ☐ Set database quota 0 MB ☐ Set warning threshold 0 MB

☒ Advanced New Person Migrate People... Import Text File... [OK] [Cancel]

Registration Queue (local):

User Name	Registration Status	Date
WKS01SA, Admin	Ready for registration	24
WKS02SA, Admin	Ready for registration	24
WKS03SA, Admin	Ready for registration	24
WKS04SA, Admin	Ready for registration	24

Register All Register Delete Options... Views... Done

Рис. 68 Закладка Mail – из нового создание реплик на другие сервера через ADMINP

Register Person -- New Entry

Basics

Mail

Address

ID Info

Groups

Other

Mail Internet Address Information

Internet address: AwKS05SA@intrust.ru

Internet Domain: intrust.ru

Address name format: FI LastName

Separator: None

Supply internet address format settings for the selected people or person. The Internet address is created using the person's name, the internet domain and internet address format components. It must be unique in the address book.

☒ Advanced

New Person

Migrate People...

Import Text File...

Registration Queue (local):

User Name	Registration Status	Date
WKS01SA, Admin	Ready for registration	24
WKS02SA, Admin	Ready for registration	24
WKS03SA, Admin	Ready for registration	24
WKS04SA, Admin	Ready for registration	24

Register All

Register

Delete

Options...

Views...

Done

Рис. 69 Закладка Address – ничего нового

Register Person -- New Entry

Basics

Mail

Address

ID Info

Groups

Other

☒ Create a Notes ID for this person

Certifier ID Information

☐ Use CA process

Certifier ID... /WWCorp

Security type: North American

Certificate expiration date: 23.01.2005 20:06:45

Location for storing user ID

☒ In Domino directory

☒ In file: Set ID File... C:\lotus\notes\data\ids\people\awks05sa.id

☐ In mail file

☒ Advanced

New Person

Migrate People...

Import Text File...

Registration Queue (local):

User Name	Registration Status	Date
WKS01SA, Admin	Ready for registration	24
WKS02SA, Admin	Ready for registration	24
WKS03SA, Admin	Ready for registration	24
WKS04SA, Admin	Ready for registration	24

Register All

Register

Delete

Options...

Views...

Done

Рис. 70 Закладка ID Info – из нового выпуск сертификата с использованием задачи CA

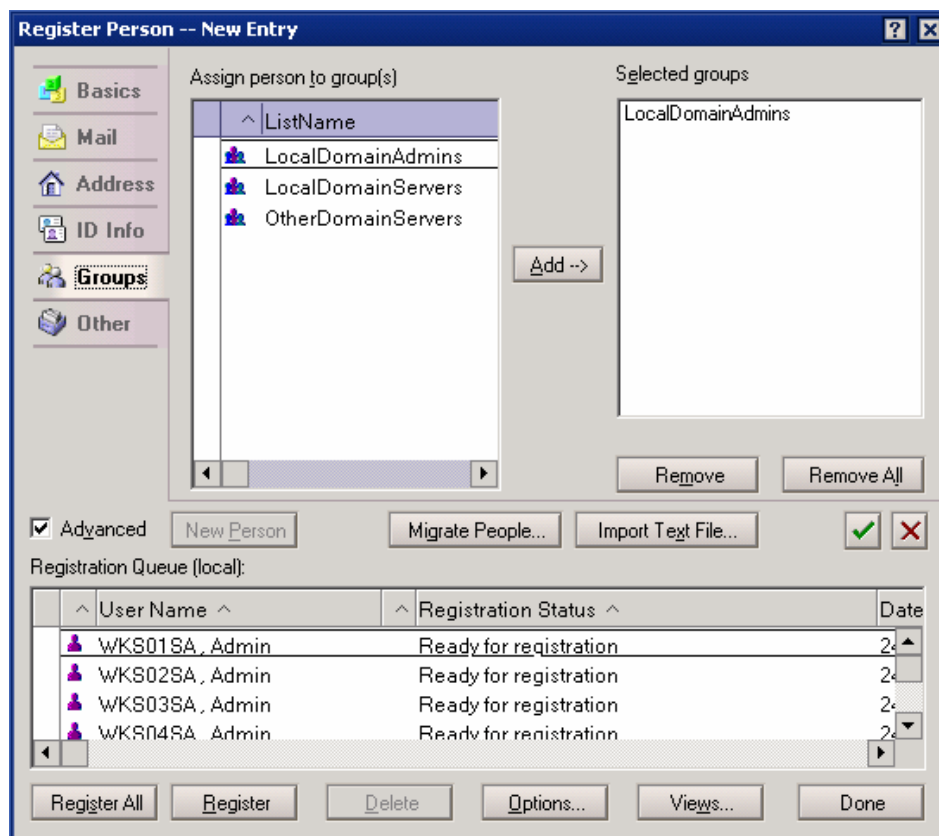


Рис. 71 Закладка Groups – ничего нового

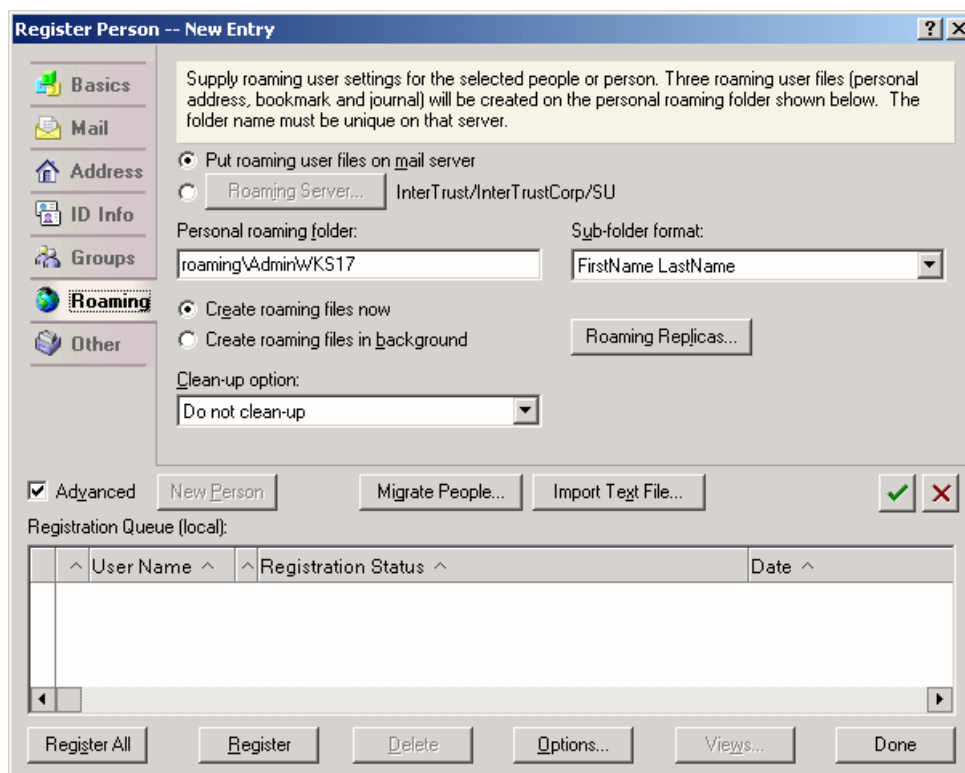


Рис. 72 А вот закладки Roaming в 6.0 нет...Она появляется с 6.0.1...

Register Person -- New Entry

☒ Basics
☐ Mail
☐ Address
☐ ID Info
☐ Groups
☐ Roaming
☒ **Other**

Setup profile: IntTrust Office
 Unique org unit:
 Location:
 Local administrator:
 Comment:
 Choose an alternate name language to enable alternate name and org unit
 Alternate name language: (None) Alternate name: Alternate org unit:
 Preferred language: (None)
 Windows User Options...

☒ Advanced

Registration Queue (local):

^	User Name ^	Registration Status ^	Date ^

Рис. 73 Закладка Other

Add Person to Windows 2000

☒ Add this person to Windows 2000
 Add person to Active Directory container
 intrust.ru/Компания ИНТЕРТРАСТ/Отдел разработок
 Windows 2000 full name: Admin WKS17
 User logon name: AWKS17
 Pre-Windows 2000 name: AWKS17
 Add person to Windows 2000 groups
 intrust.ru/Users/SMS Admins
 intrust.ru/Users/SMS Reporting Users
 intrust.ru/Users/TWGAdmins
 intrust.ru/Users/TWGSuperAdmins
 intrust.ru/Users/webProxyUsers
 intrust.ru/Users/WinSockProxyUsers
 You can add the currently selected people/person to Windows 2000 and optionally assign the people/person to groups. For a single person, supply the unique logon name and full name (the Notes shortname and fullname are the defaults).

Рис. 74 Окно Windows User Options

1.17. 1.1. Configuration Directory

- • Это селективная реплика обыкновенной (исходной) Domino Directory, содержащая только документы, связанные с конфигурированием и администрированием сервера, но не содержащая документов, относящихся к пользователям, группам, почтовым базам и т.п.
- • Configuration Directory получается значительно меньше по размеру, чем исходная - Primary Domino Directory
- • Логика работы:
 - • Для конфигурирования и основной работы сервера имеющихся документов обычно и так достаточно
 - • В процессах же аутентификации, проверки вхождения в группы, поиска адресов и др., требующих дополнительных документов, этот сервер обращается к «ближайшему» серверу с Primary Domino Directory

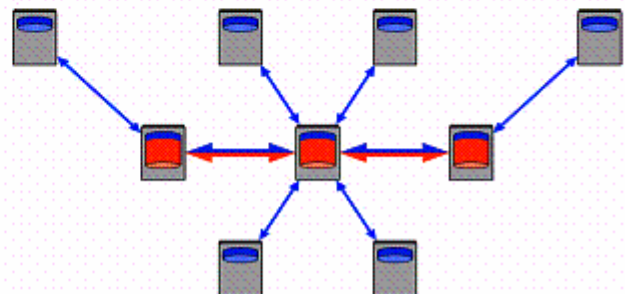
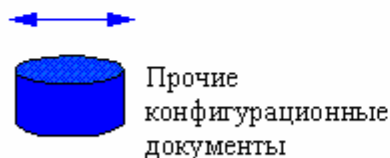
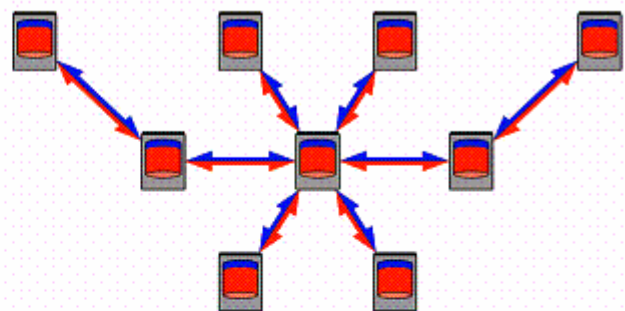
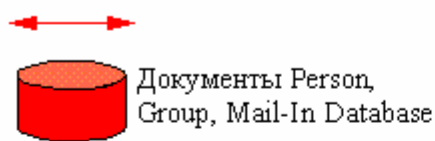


Рис. 75

- • Выбрать эту возможность можно в процессе установки очередного сервера в домене (на первом сервере домена, естественно, создается Primary Domino Directory)
- • Можно «доустановить» эту возможность и потом. Для этого в репликационных установках Domino Directory нужно выбрать Configuration Documents Only. Затем командой консоли Replicate провести репликацию базы NAMES.NSF с другим сервером, имеющим Primary Domino Directory. После этого сервер перезапустить. Остальное «доделает» задача Administration Process (она должна обработать два запроса: Set Directory Filename и Store Directory type in Server Record)

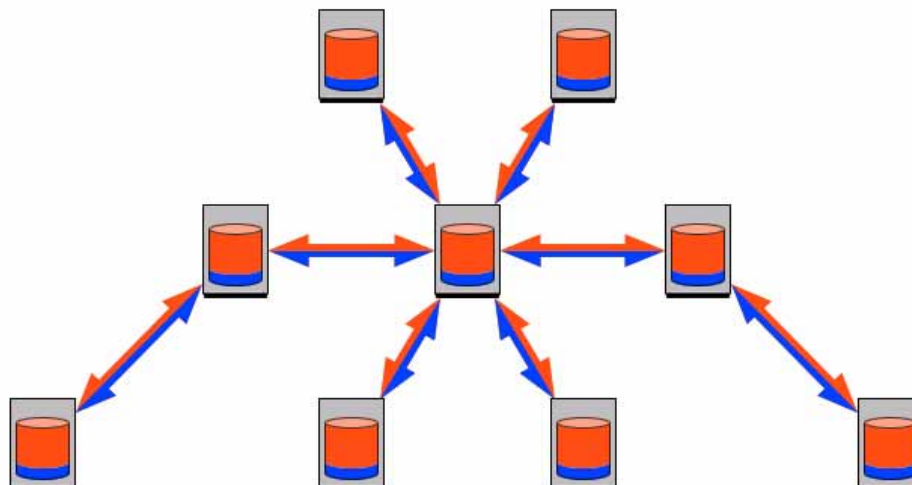


Рис. 76. Traditional Directory Structure

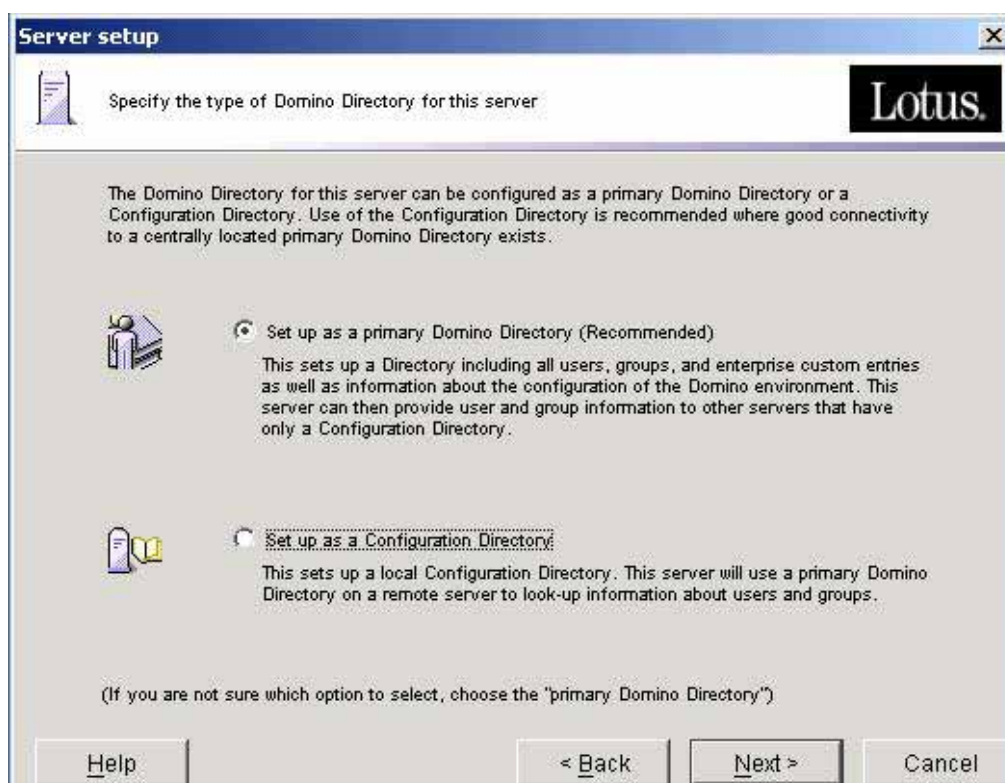


Рис. 77. Выбор типа каталога

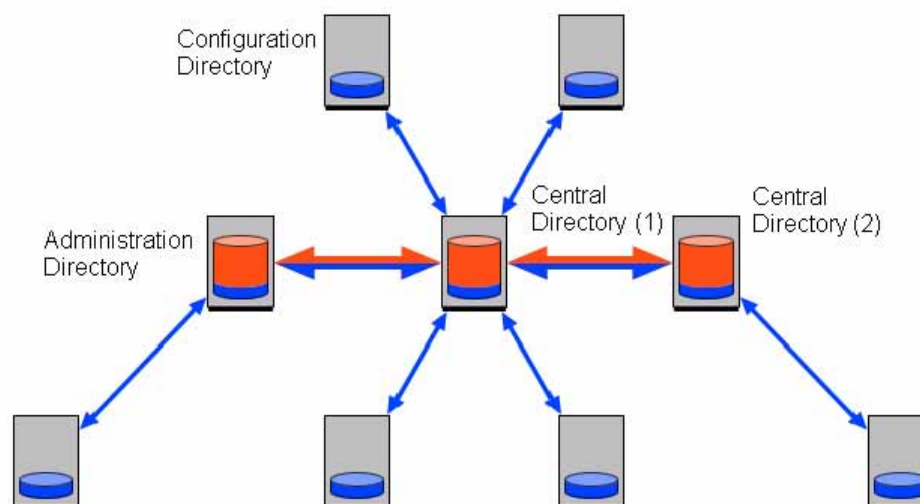


Рис. 78. Central Directory Structure

1.17.1. 1.1.1. No Configuration Directory - не просто селективные репликации...

- При отсутствии необходимых документов сервер с Configuration Directory обращается к «ближайшим» серверам с Primary Domino Directory
- Выбор «ближайшего» сервера управляем - на сервере с Primary Domino Directory можно задавать список серверов с Configuration Directory, которым разрешено обращаться к данному
- Для поиска документов Person, Group, Mail-in Database сервером с Configuration Directory может использоваться Directory Assistance, «перенаправляющий» запрос в Extended Directory Catalog или на сервер LDAP
- Для сокращения сетевого трафика сервер с Configuration Directory кэширует результаты запросов

1.17.2. 1.1.2. Configuration Directory - окно Replication Settings

В учебном классе вы можете выбрать при установке дополнительного сервера любой вариант. При выборе Configuration Directory вас могут ожидать проблемы, когда первый сервер домена и остальные серверы с Primary Domino Directory остановлены. В дальнейшем вы, вероятно, откажитесь от Configuration Directory. Как это сделать, показано в окнах на Рис. 81 и Рис. 82, однако это требует владения понятием «селективные репликации», что подробно рассматривается в курсе позже, в теме «репликации между серверами». После внесения изменений в репликационные установки нужно командой консоли Replicate провести репликацию базы NAMES.NSF с другим сервером, имеющим Primary Domino Directory, и перезапустить сервер.

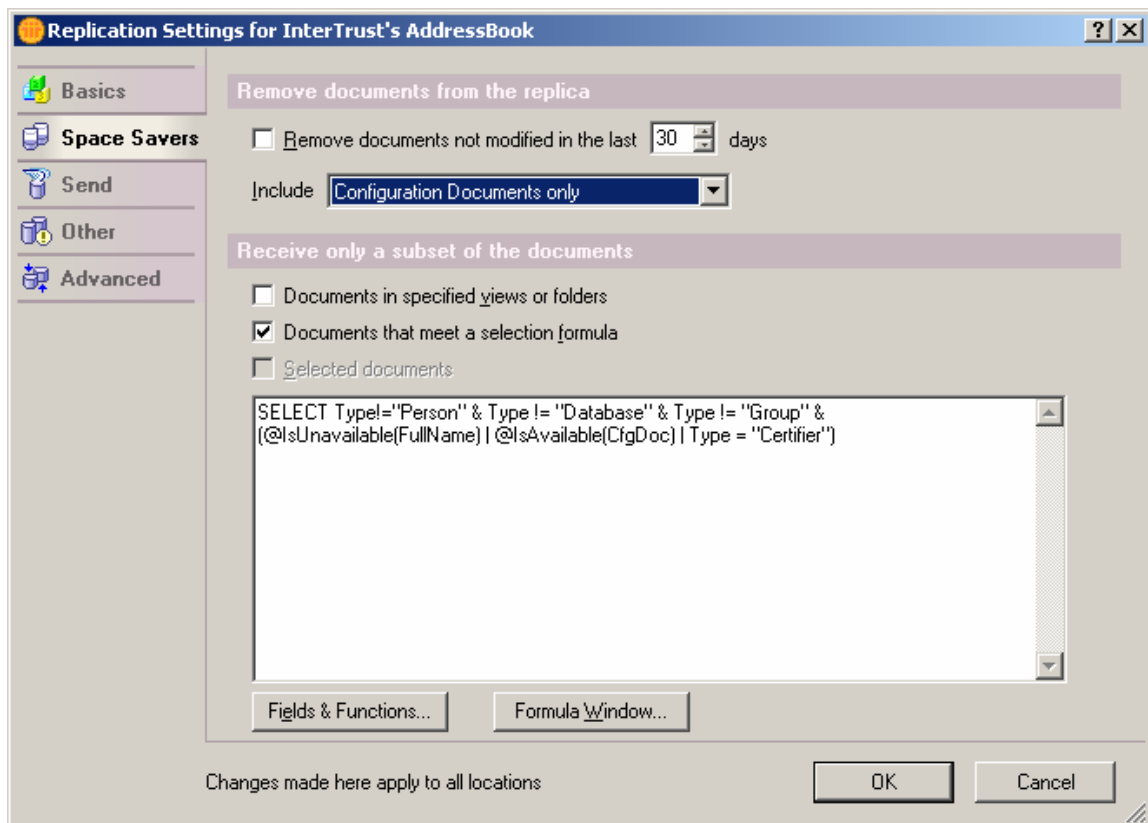


Рис. 79 Окно репликационных установок на закладке Space Savers для Configuration Directory

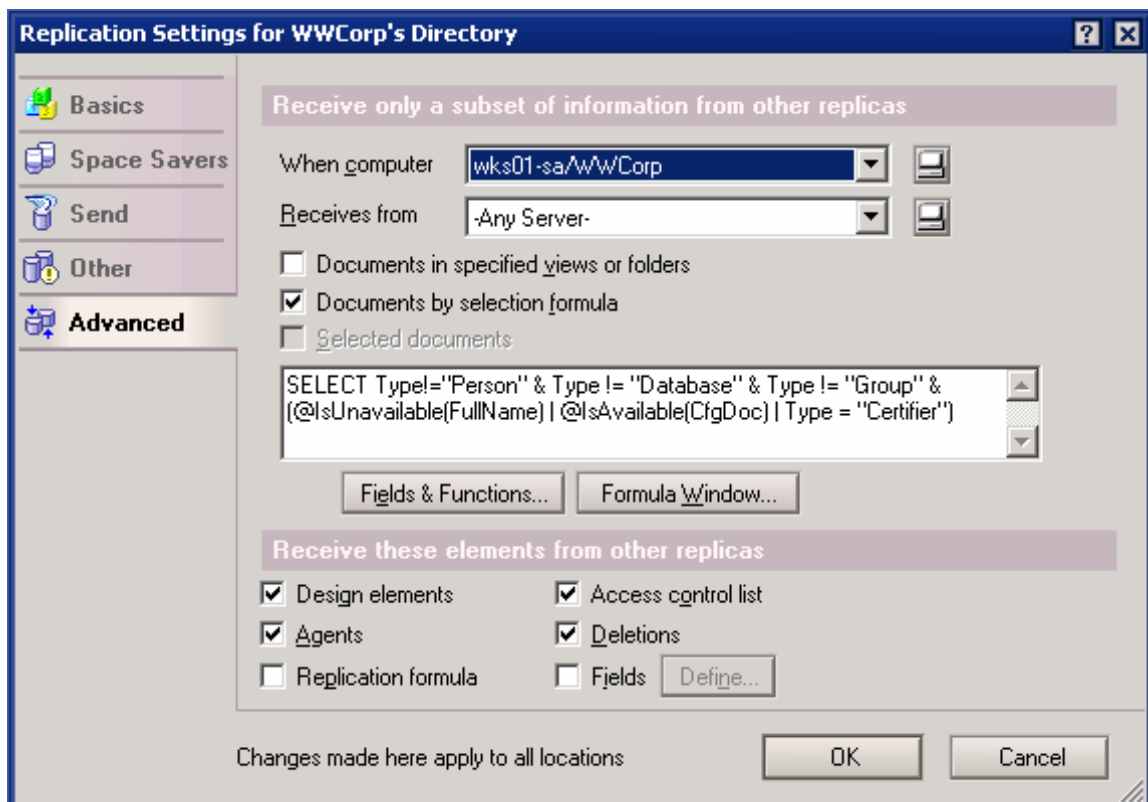


Рис. 80 Окно репликационных установок на закладке Advanced для Configuration Directory

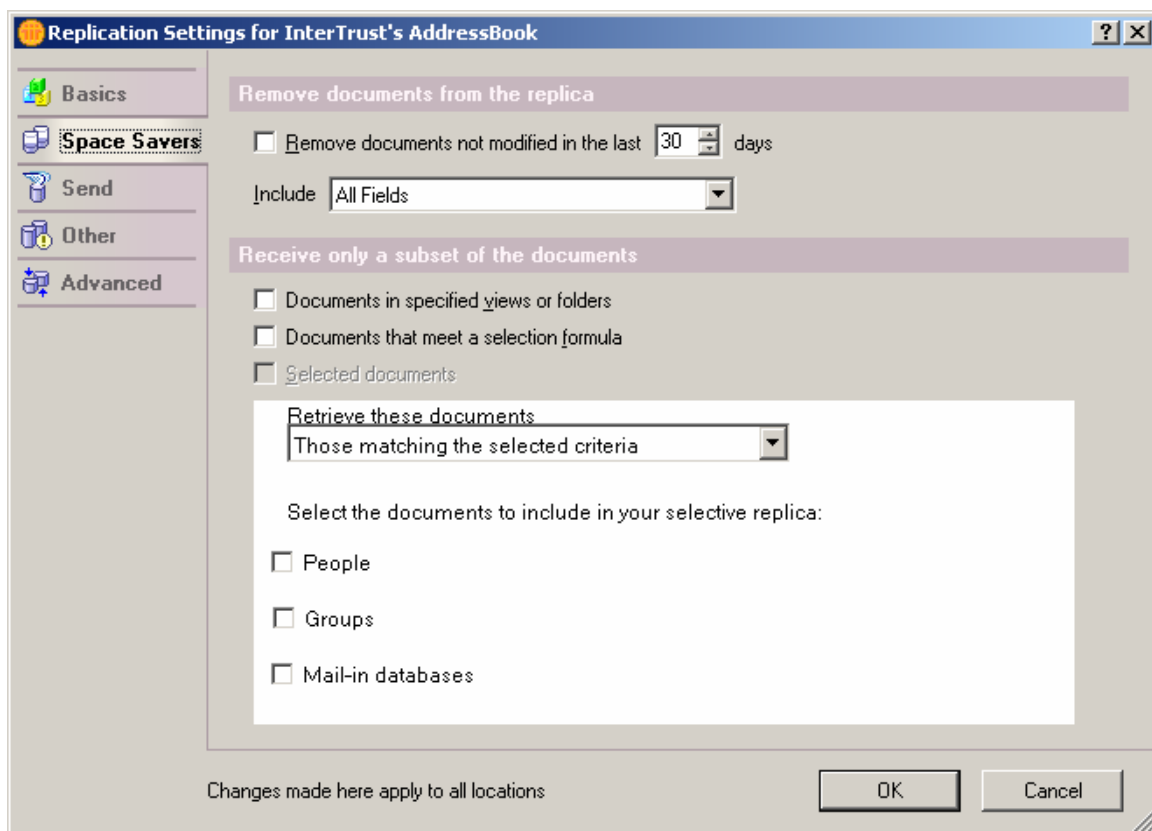


Рис. 81 Окно репликационных установок на закладке Space Savers для Primary Domino Directory

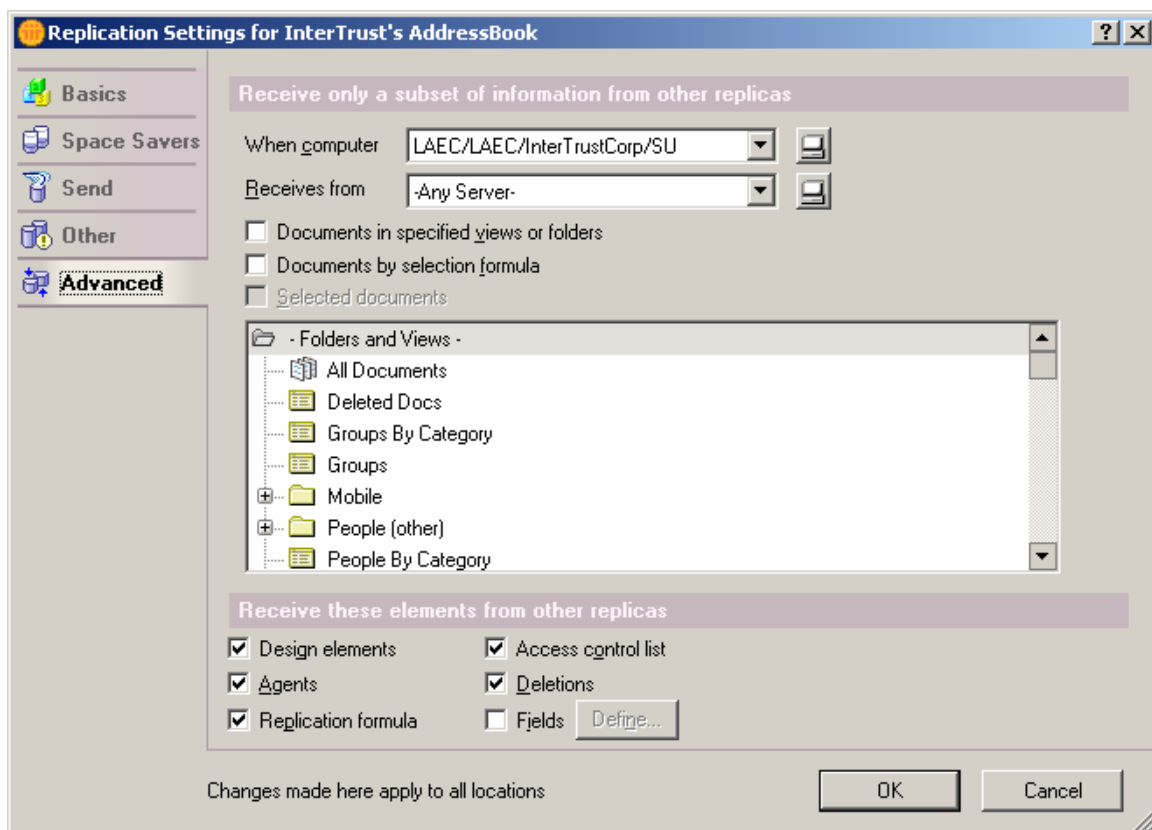


Рис. 82 Окно репликационных установок на закладке Space Savers для Primary Domino Directory

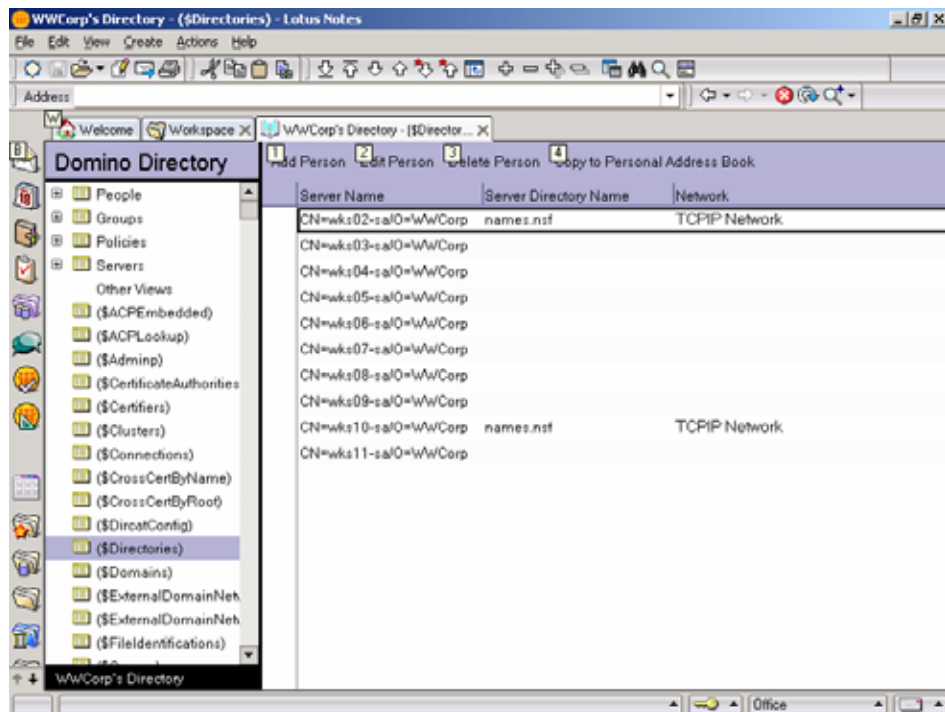


Рис. 83 К вопросу поиска сервером с Configuration Directory (wks01-sa/WWCorp) сервера с Primary Domino Directory – скрытый вид (\$Directories)

1.18. 1.1. Установка дополнительного сервера в существующем домене организации

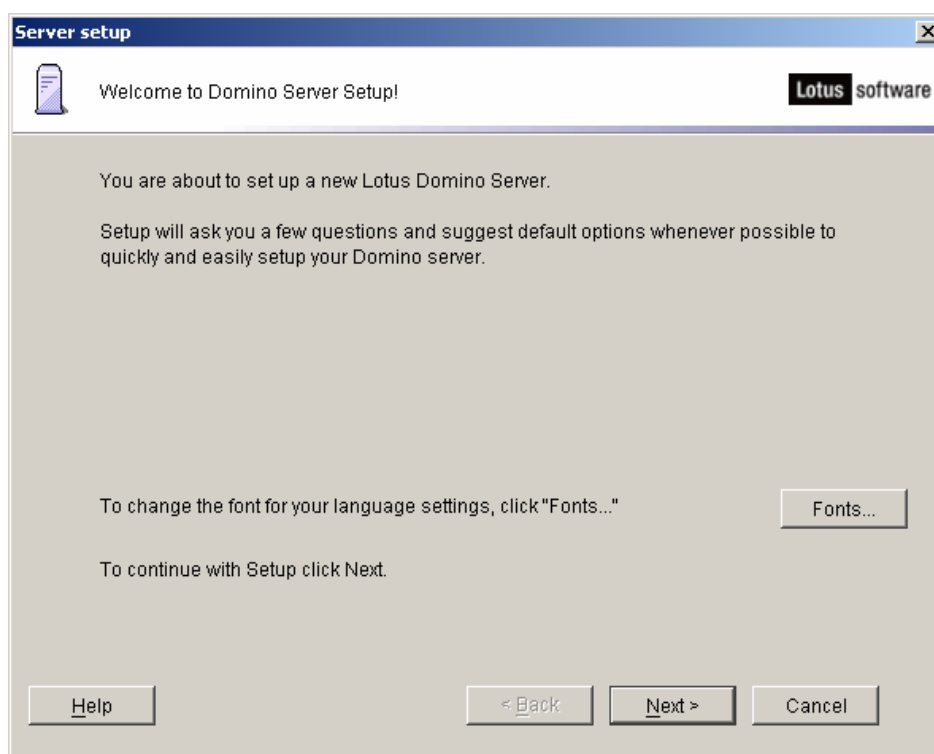


Рис. 84 Можно изменить шрифты

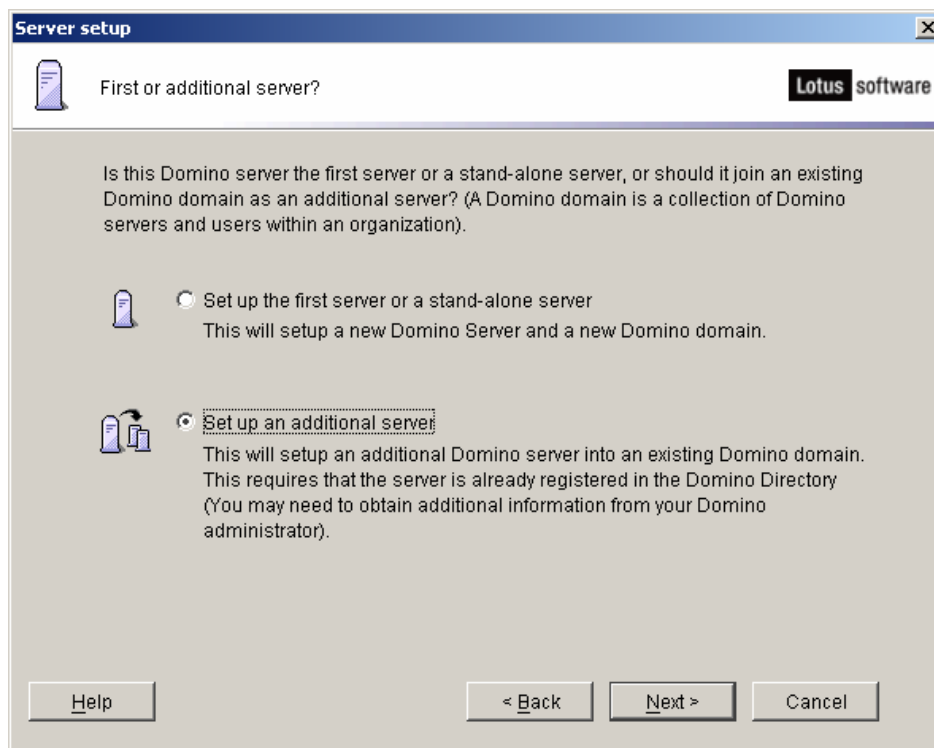


Рис. 85 Выбрана установка дополнительного сервера в существующем домене - влечет создание реплики каталога Domino (names.nsf)

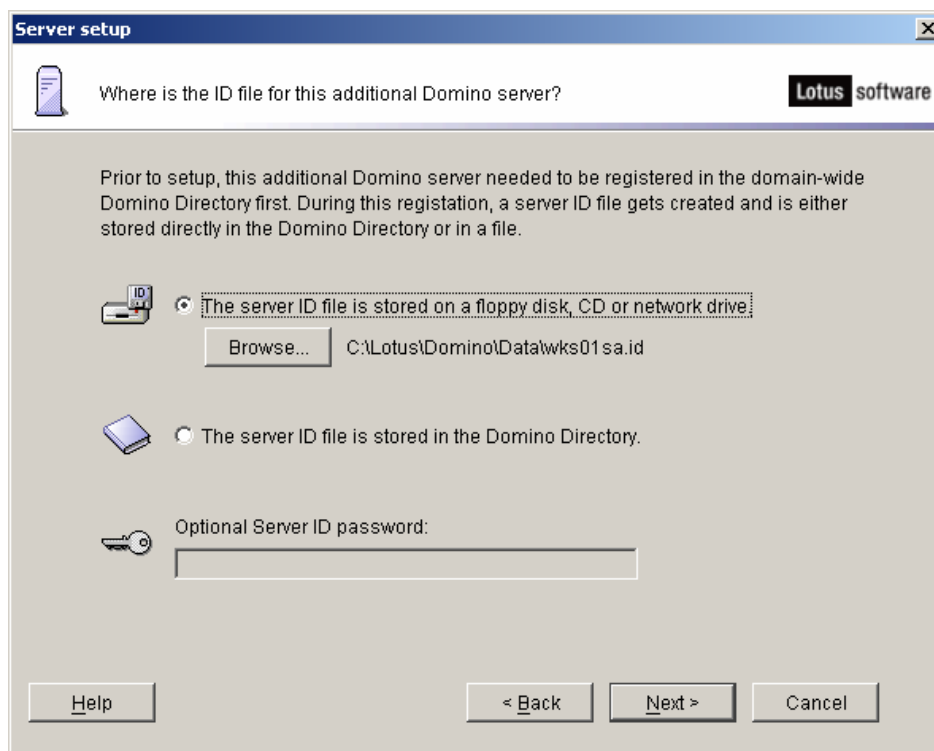


Рис. 86 Дополнительный сервер к этому моменту должен быть зарегистрирован, т.е. для него должен быть создан ID-файл и документ Server в каталоге Domino существующего сервера. В данном окне выбирается способ получения ID-файла устанавливаемого сервера. Либо ID-файл передан как файл на компьютер, где устанавливается сервер (что и выбрано в окне), либо при регистрации ID-файл был защищен паролем и сохранен как присоединенный файл в документе Server в каталоге Domino существующего сервера (делается второй выбор и вводится пароль, ID-файл копируется в каталог устанавливаемого сервера и удаляется из документа Server)

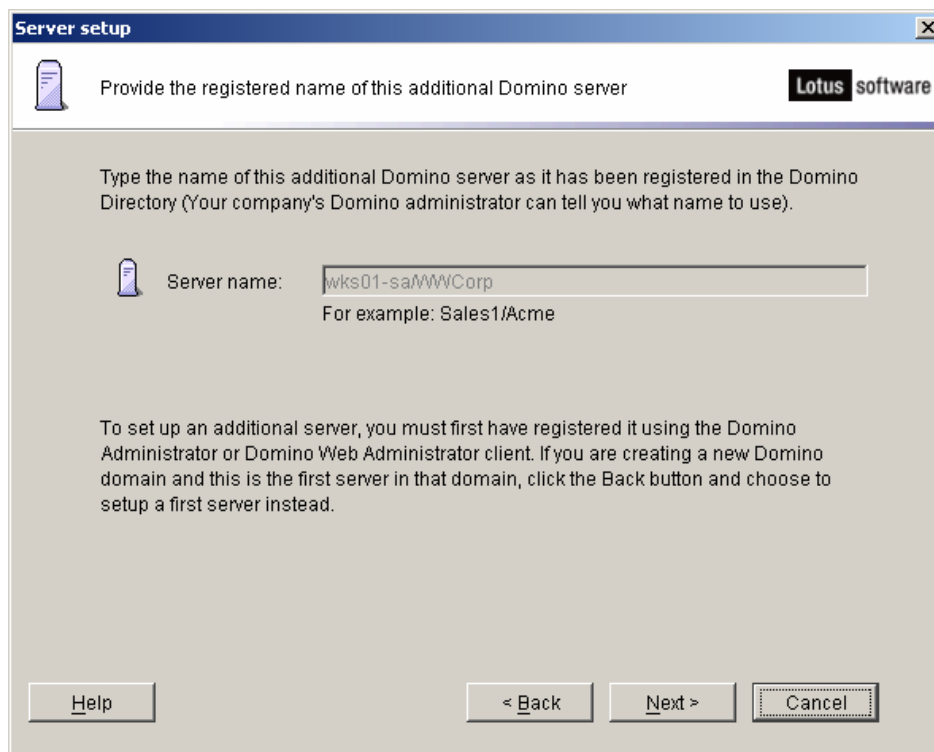


Рис. 87 Имя сервера извлекается из ID-файла

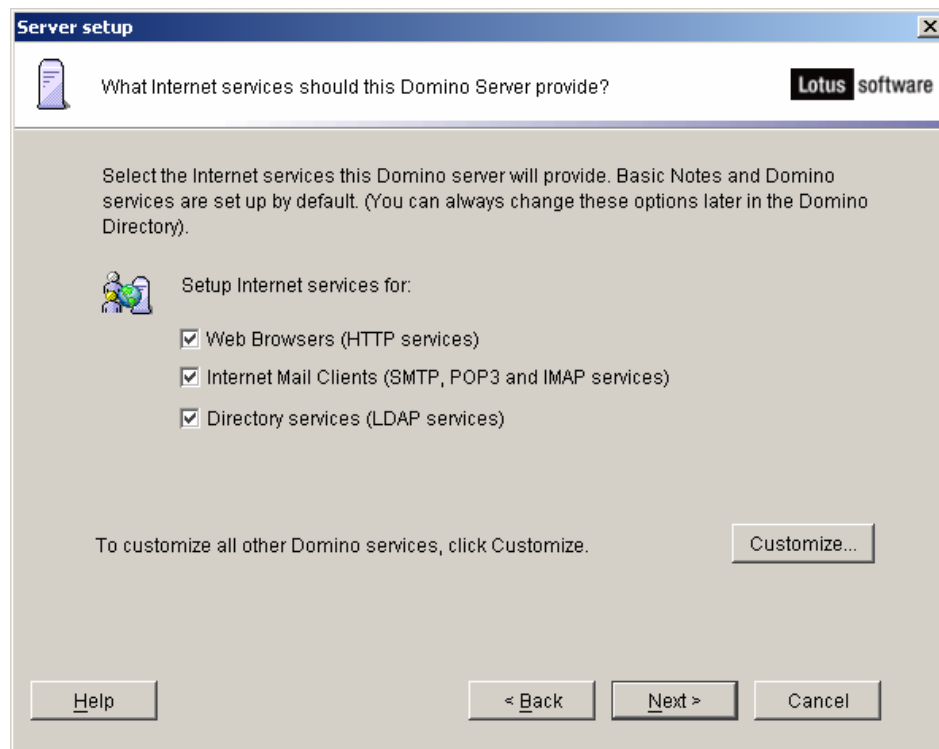


Рис. 88 Выбор списка задач, запускаемых при старте сервера. Делать это желательно в окне, открываемом по кнопке Customize...

Следующее окно получают при нажатии кнопки Customize... в предыдущем.

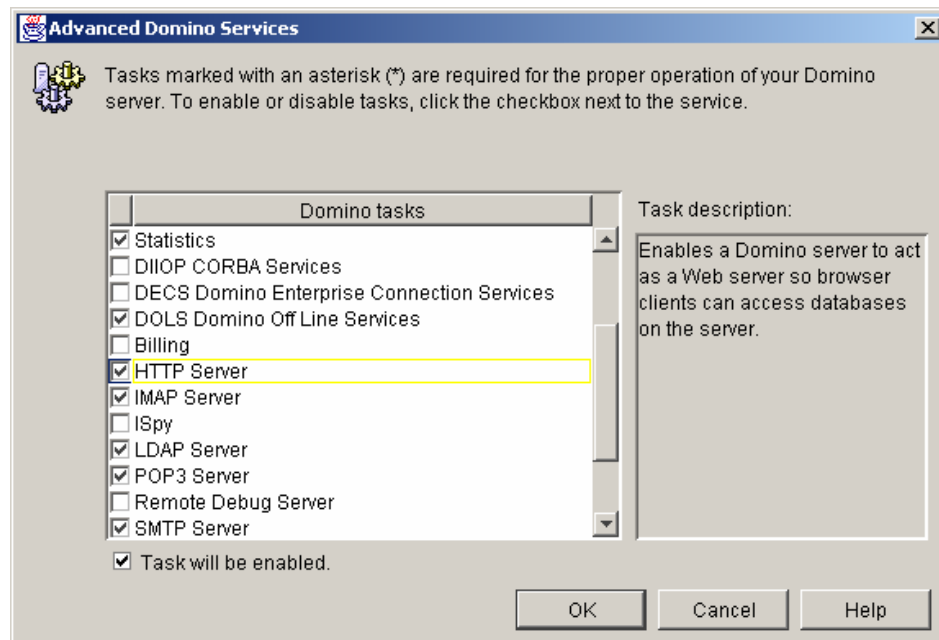


Рис. 89 Выбран список задач, запускаемых при старте сервера

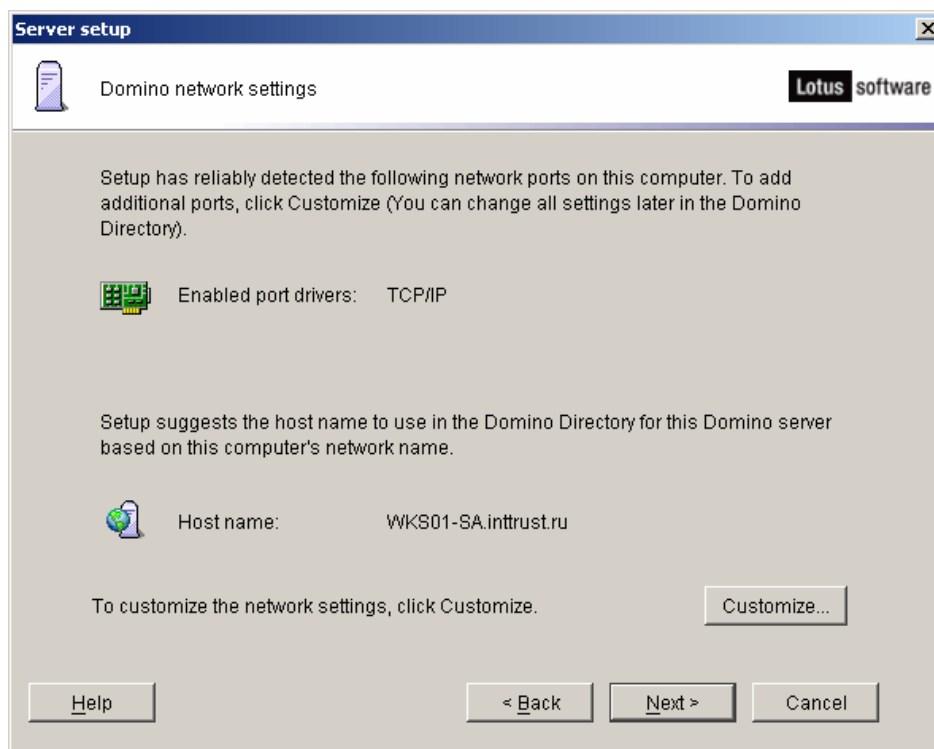


Рис. 90 Конфигурирование портов – подробности доступны в окне по кнопке Customize...

Следующее окно получают при нажатии кнопки Customize... в предыдущем.

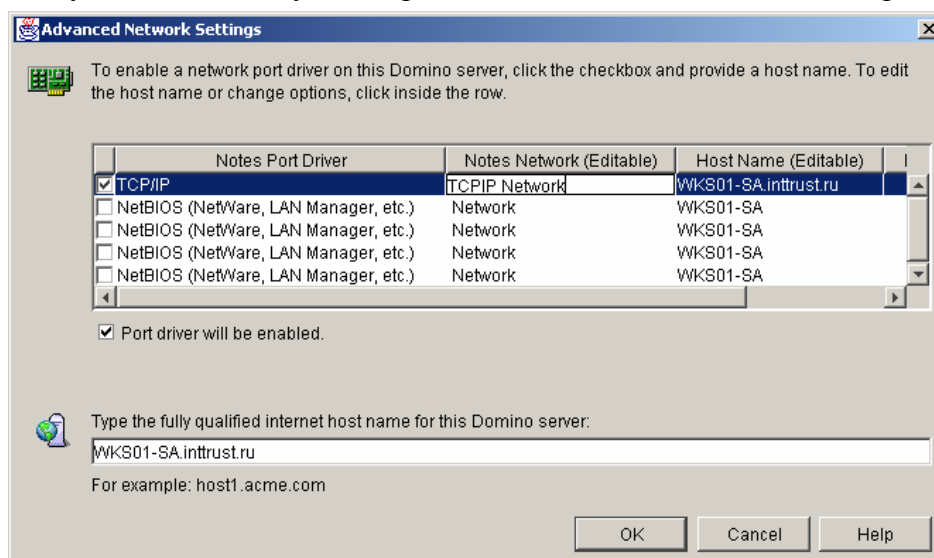


Рис. 91 Конфигурирование портов – выбор нужных портов, названий поименованных сетей, имен хостов, шифрования на порту и...

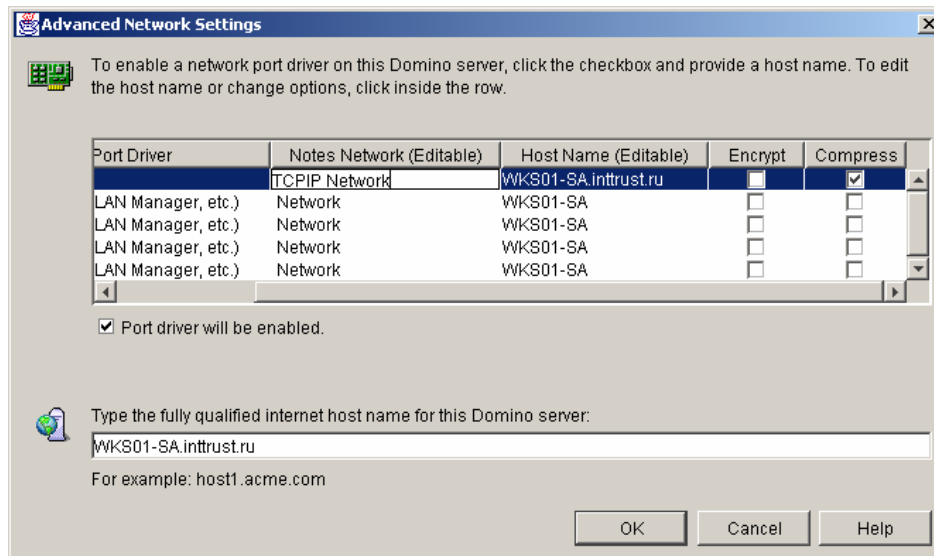


Рис. 92 ...новой возможности – компрессии сетевого трафика по порту.

Кстати про компрессию сетевого трафика... Она включается в настройках порта и, чтобы работала, должна быть выбрана **на обеих сторонах R6**.

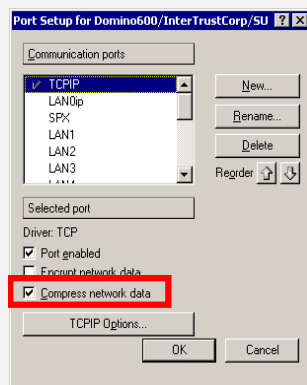


Рис. 93 Выбор компрессии сетевого трафика по порту на клиенте и сервере

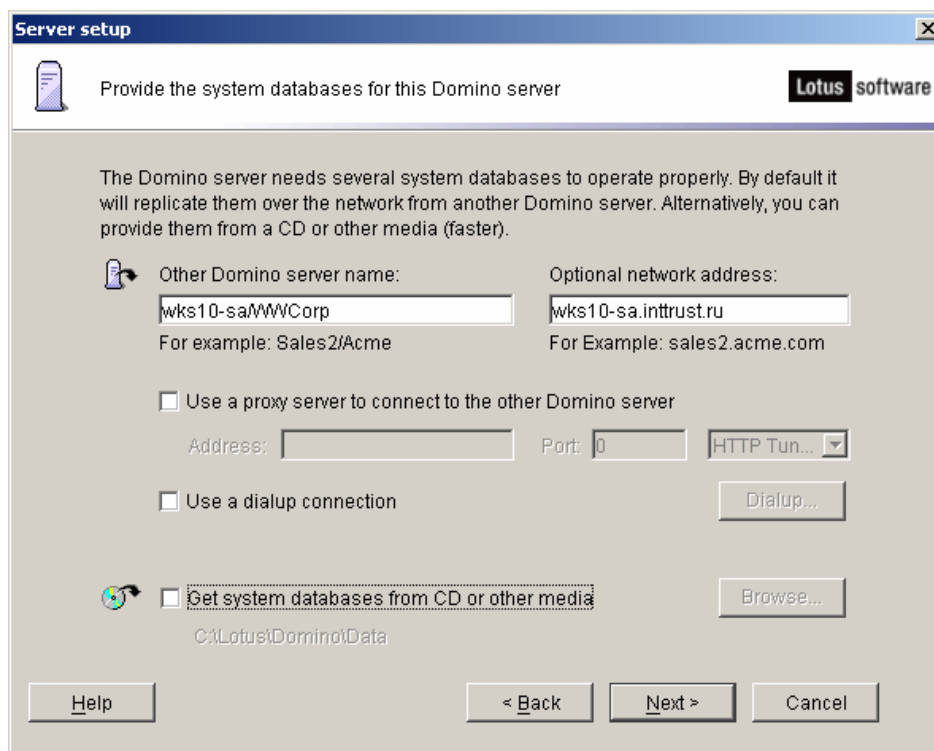


Рис. 94 Определяется способ получения реплики каталога Domino и других системных баз с существующего сервера. В окне выбран стандартный способ – по локальной сети с существующего сервера wks10-sa/WWCorp с сетевым адресом wks10-sa.intrust.ru. Возможно подключение к существующему серверу через прокси-сервер (либо HTTP-туннель, либо SOCKs) или по модемному соединению (XPC). Появился новый вариант – реплику «большого» каталога Domino взять с указанного местоположения, а только затем «дореплицировать» с существующим сервером.

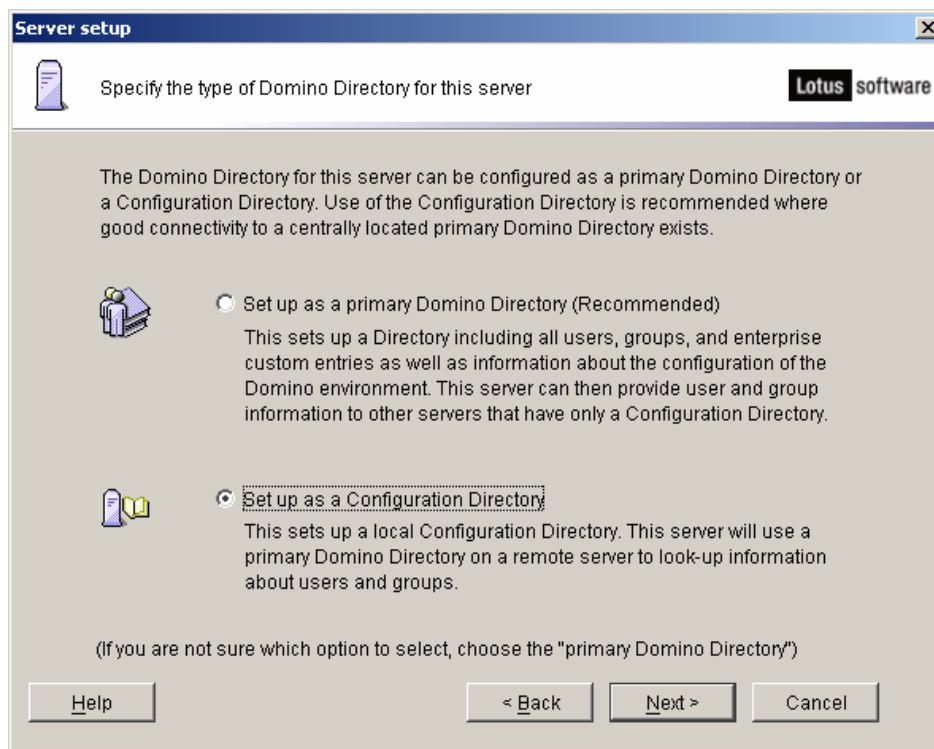


Рис. 95 Выбирается тип каталога Domino на устанавливаемом сервере – «полный» или Configuration Directory

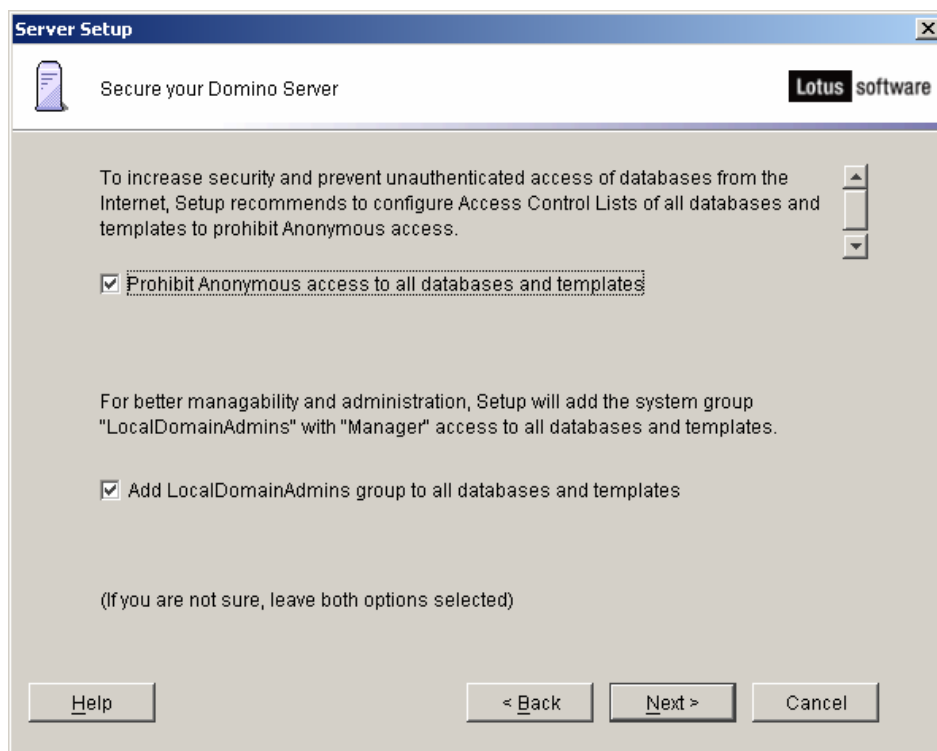


Рис. 96 Добавить во все базы и шаблона группу LocalDomainAdmins (в предшествующих версиях использовалась группа Administrators) с уровнем доступа Manager и Anonymous с уровнем доступа No Access

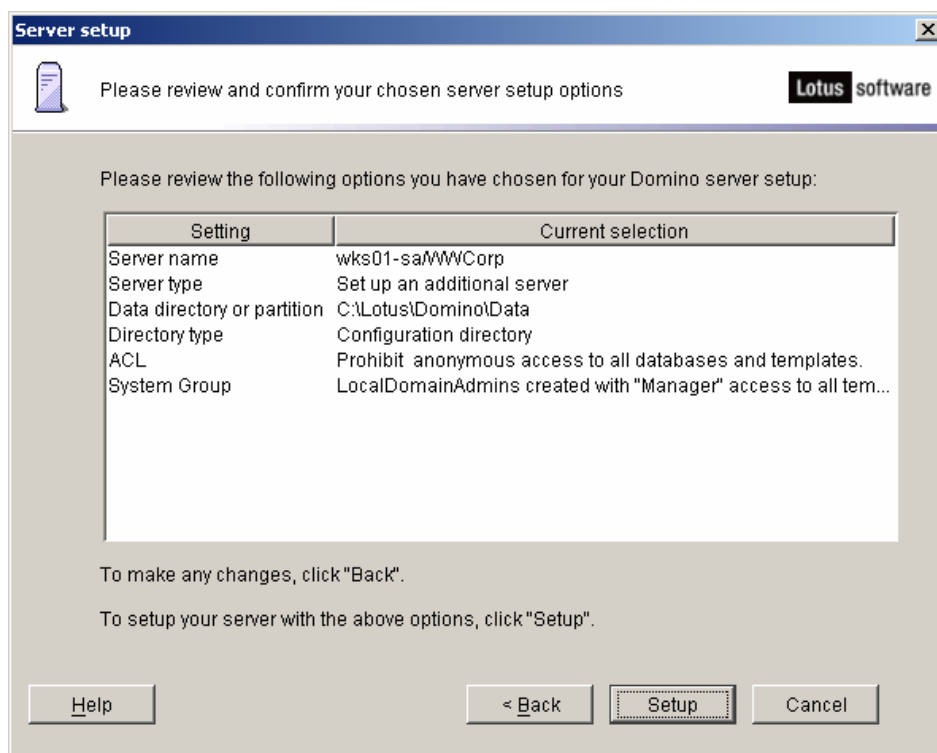


Рис. 97 Основные из выбранных параметров

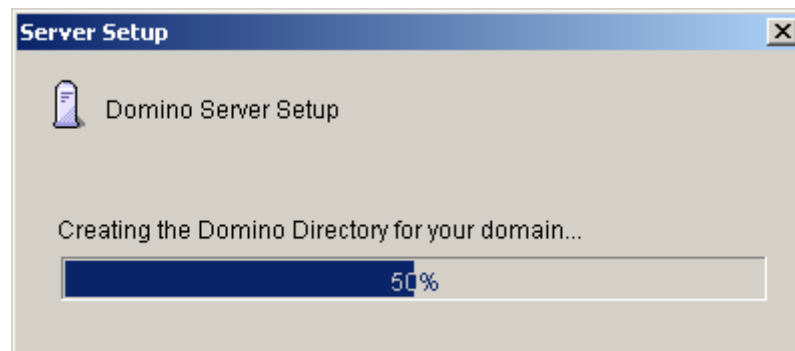


Рис. 98 Идет процесс установки

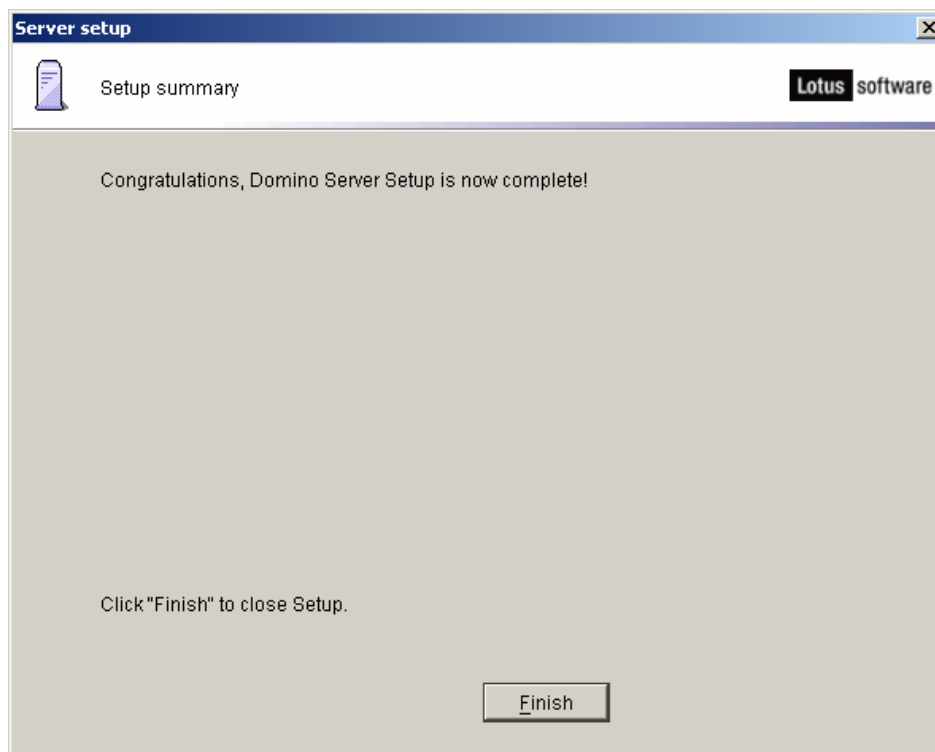


Рис. 99 Установка завершена

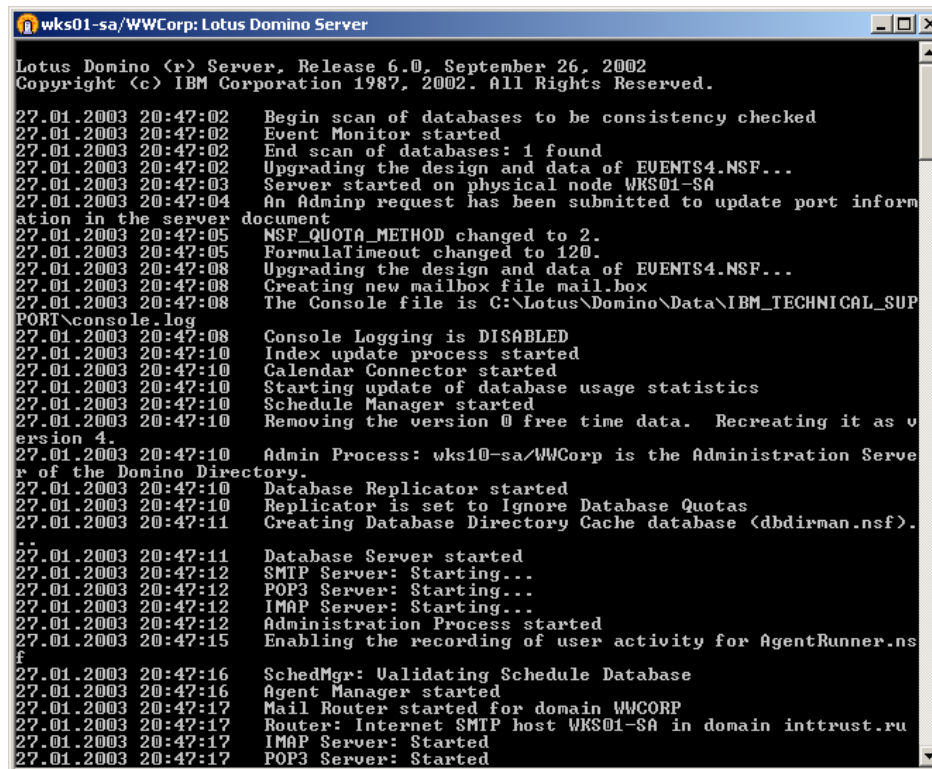
A screenshot of a Lotus Domino Server console window. The title bar reads 'wks01-sa/WWCorp: Lotus Domino Server'. The window contains a log of server startup events. The text is as follows:
Lotus Domino (r) Server, Release 6.0, September 26, 2002
Copyright (c) IBM Corporation 1987, 2002. All Rights Reserved.
27.01.2003 20:47:02 Begin scan of databases to be consistency checked
27.01.2003 20:47:02 Event Monitor started
27.01.2003 20:47:02 End scan of databases: 1 found
27.01.2003 20:47:02 Upgrading the design and data of EVENTS4.NSF...
27.01.2003 20:47:03 Server started on physical node WKS01-SA
27.01.2003 20:47:04 An Adminp request has been submitted to update port information in the server document
27.01.2003 20:47:05 NSF_QUOTA_METHOD changed to 2.
27.01.2003 20:47:05 FormulaTimeout changed to 120.
27.01.2003 20:47:08 Upgrading the design and data of EVENTS4.NSF...
27.01.2003 20:47:08 Creating new mailbox file mail.box
27.01.2003 20:47:08 The Console file is C:\Lotus\Domino\Data\IBM_TECHNICAL_SUPPORT\console.log
27.01.2003 20:47:08 Console Logging is DISABLED
27.01.2003 20:47:10 Index update process started
27.01.2003 20:47:10 Calendar Connector started
27.01.2003 20:47:10 Starting update of database usage statistics
27.01.2003 20:47:10 Schedule Manager started
27.01.2003 20:47:10 Removing the version 0 free time data. Recreating it as version 4.
27.01.2003 20:47:10 Admin Process: wks01-sa/WWCorp is the Administration Server of the Domino Directory.
27.01.2003 20:47:10 Database Replicator started
27.01.2003 20:47:10 Replicator is set to Ignore Database Quotas
27.01.2003 20:47:11 Creating Database Directory Cache database (dbdirman.nsf).
..
27.01.2003 20:47:11 Database Server started
27.01.2003 20:47:12 SMTP Server: Starting...
27.01.2003 20:47:12 POP3 Server: Starting...
27.01.2003 20:47:12 IMAP Server: Starting...
27.01.2003 20:47:12 Administration Process started
27.01.2003 20:47:15 Enabling the recording of user activity for AgentRunner.nsf
27.01.2003 20:47:16 SchedMgr: Validating Schedule Database
27.01.2003 20:47:16 Agent Manager started
27.01.2003 20:47:17 Mail Router started for domain WWCORP
27.01.2003 20:47:17 Router: Internet SMTP host WKS01-SA in domain intrust.ru
27.01.2003 20:47:17 IMAP Server: Started
27.01.2003 20:47:17 POP3 Server: Started

Рис. 100 Первый реальный запуск сервера

После установки дополнительных серверов и клиентов необходимо «проверить и доделать» следующее:

- Проверить в ACL NAMES.NSF, назначена ли группа LocalDomainAdmins на те же роли, что и администратор первого сервера. Обычно не назначена – требуется назначить, чтобы не получать отказов при попытках выполнять отдельные операции...
- Наладить репликации по расписанию между серверами. Для этого открыть в NAMES.NSF дополнительные серверов документы Connection, «разрешить их», задать частоту репликаций около 10 минут, запретить использование этих документов для передачи почты и сохранить. Почта будет передаваться и без документов Connection, поскольку через пару часов все серверы домена окажутся в одной поименованной сети TCPIP Network (благодаря работе программы Administration Process и репликациям по расписанию).

1.19. 1.1. Удаленная установка дополнительного сервера в существующем домене организации

На устанавливаемом сервере должна быть уже выполнена первая фаза установки сервера – Install – «копирование файлов». Удаленно можно выполнять только вторую фазу установки – Setup.

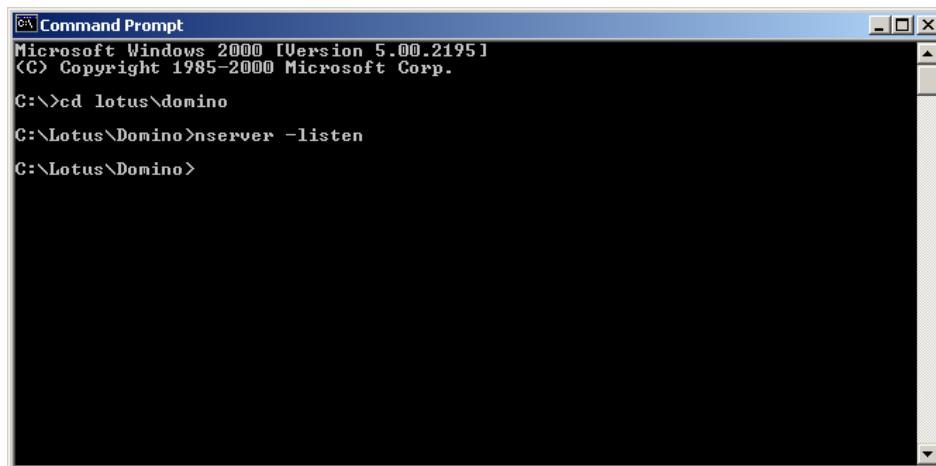


Рис. 101 На устанавливаемом удаленно сервере выдается команда `nserver -listen`

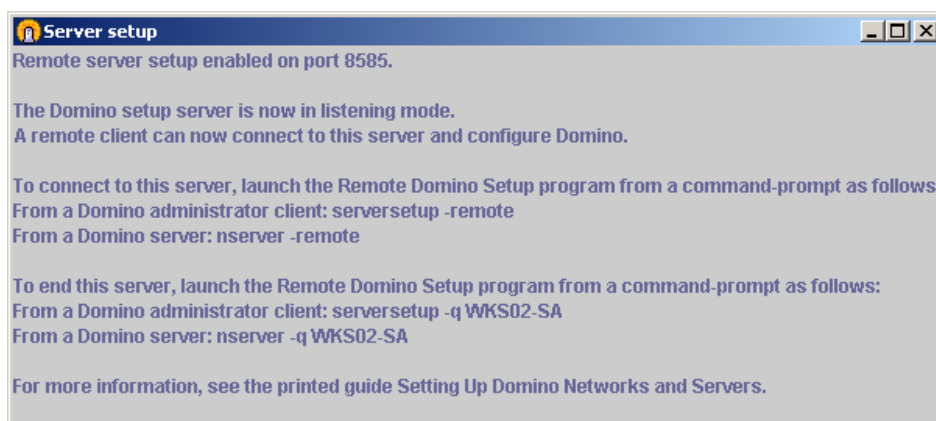


Рис. 102 Окно, появившееся на устанавливаемом удаленно сервере, подтверждает, что на порту 8585 запущен листенер программы удаленной установки. Дальнейшая установка продолжается на компьютере, на котором установлен клиент администратора с программой удаленной установки.

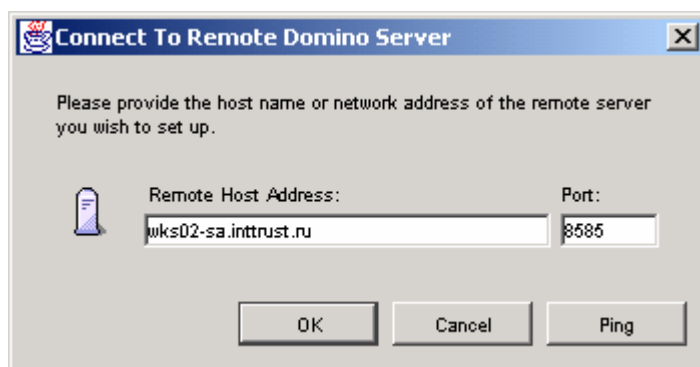


Рис. 103 В данном случае программа удаленной установки запускалась простейшим способом – «щелчком по пиктограмме». В появившемся окне запрашивается имя хоста и порт листенера сервера.

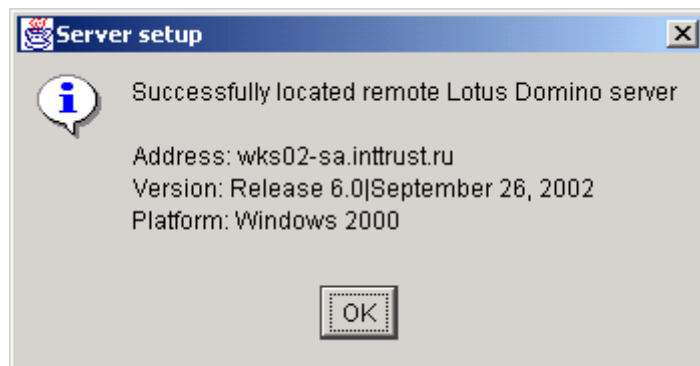


Рис. 104 Соединение программы удаленной установки с листенером прошло успешно

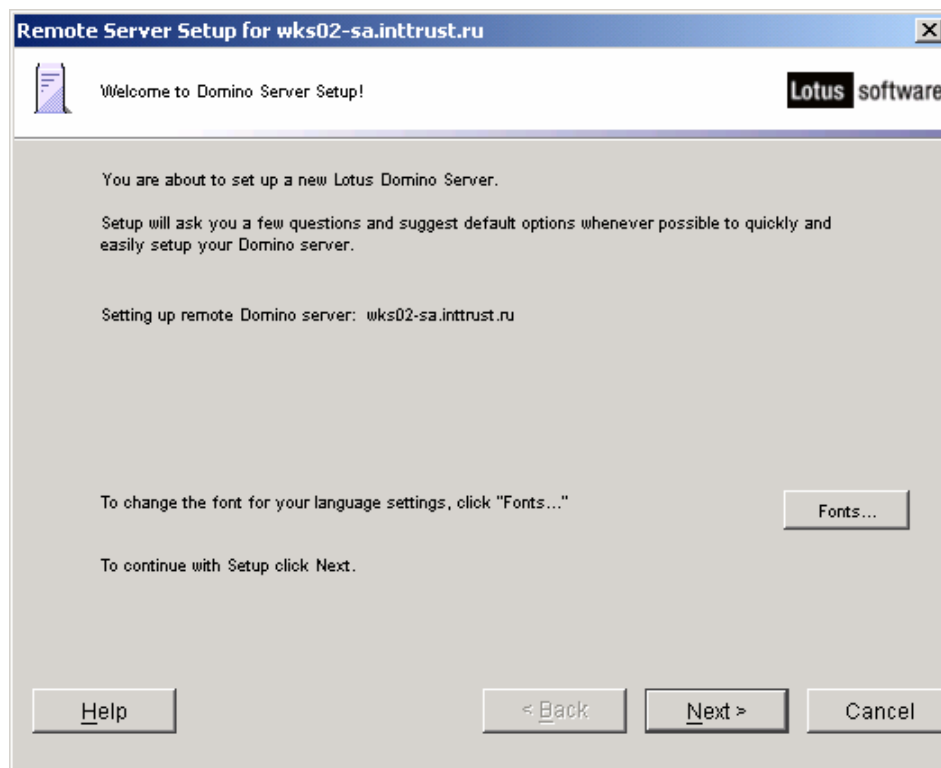


Рис. 105 Появляется первое окно программы установки. Можно изменить шрифты

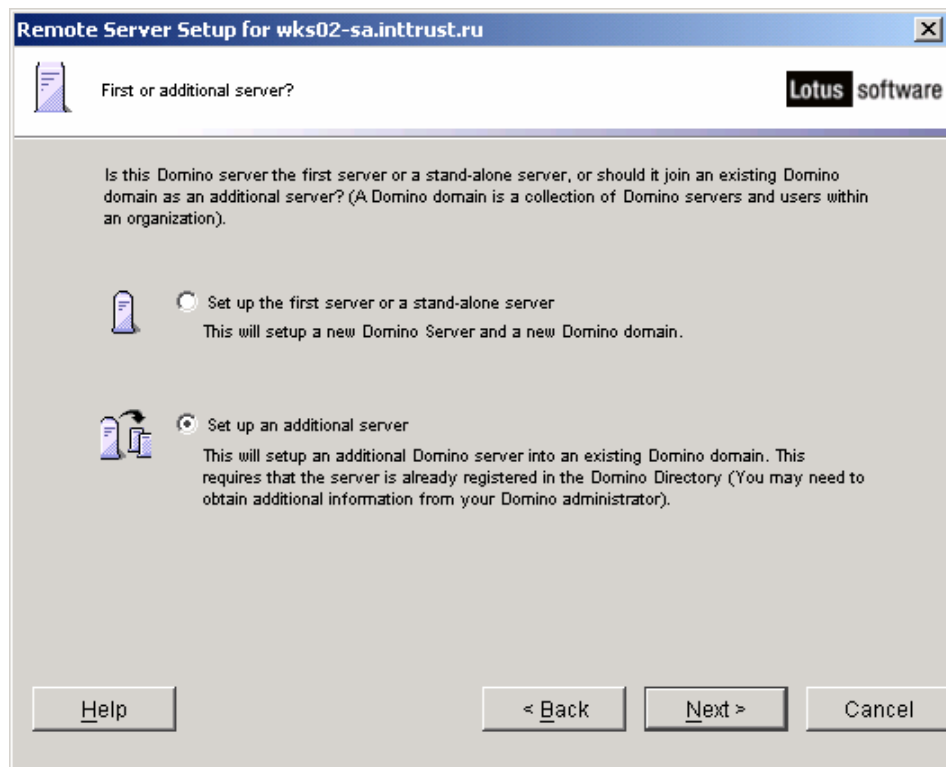


Рис. 106 Выбрана установка дополнительного сервера в существующем домене - влечет создание реплики каталога Domino (names.nsf)

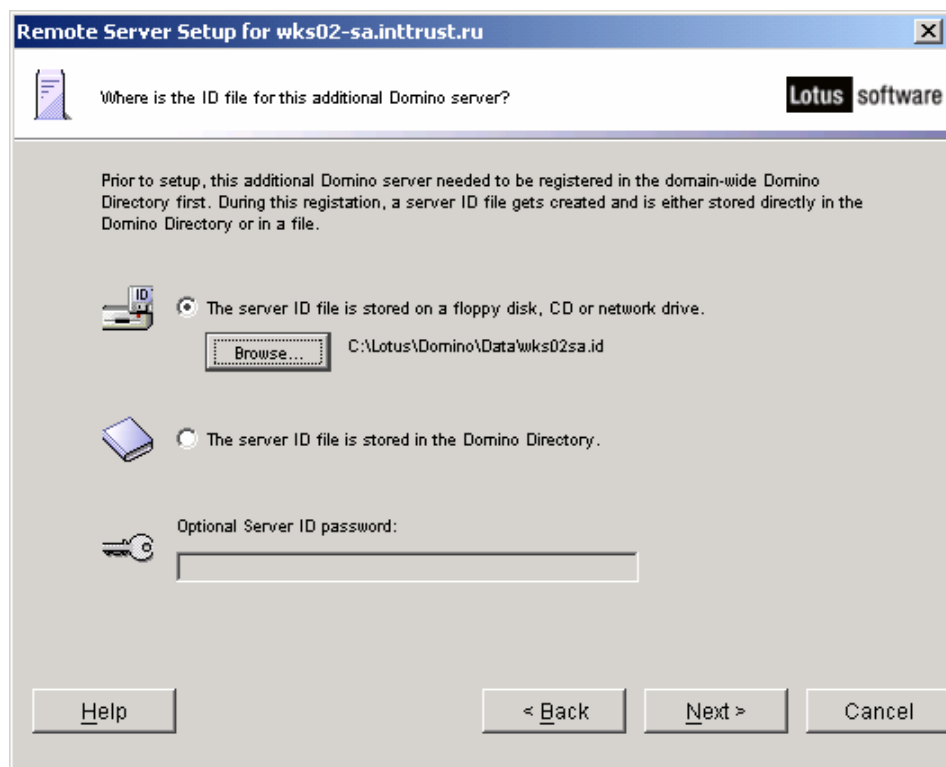


Рис. 107 Дополнительный сервер к этому моменту должен быть зарегистрирован, т.е. для него должен быть создан ID-файл и документ Server в каталоге Domino существующего сервера. В данном окне выбирается способ получения ID-файла устанавливаемого сервера. Либо ID-файл передан как файл на компьютер, где устанавливается сервер (что и выбрано в окне, C:\Lotus\Domino\Data – каталог на удаленном сервере, ID-файл был помещен туда до начала установки), либо при регистрации ID-файл был защищен паролем и сохранен как присоединенный файл в документе Server в каталоге Domino существующего сервера (делается второй выбор и вводится пароль, ID-файл копируется в каталог устанавливаемого сервера и удаляется из документа Server)

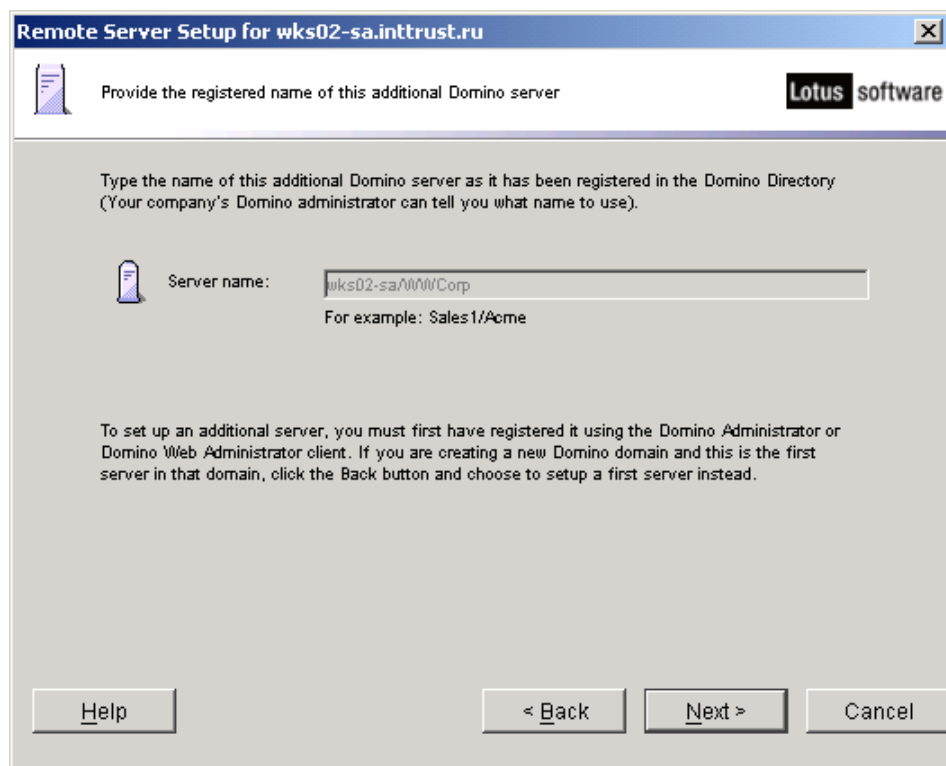


Рис. 108 Имя сервера извлекается из ID-файла

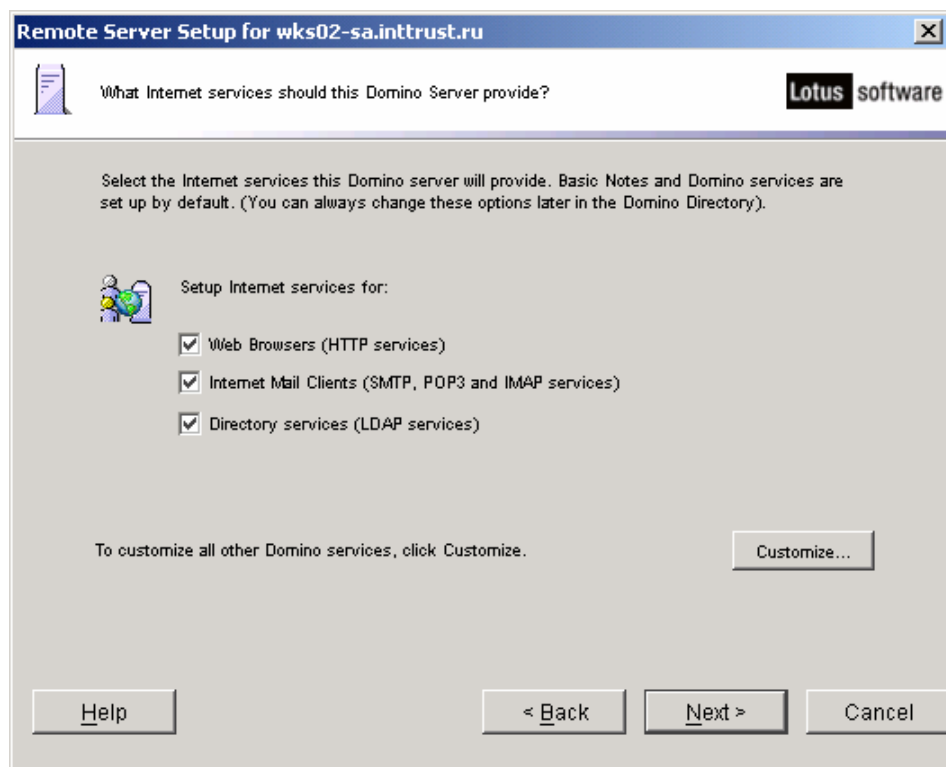


Рис. 109 Выбор списка задач, запускаемых при старте сервера. Делать это желательно в окне, открываемом по кнопке Customize...

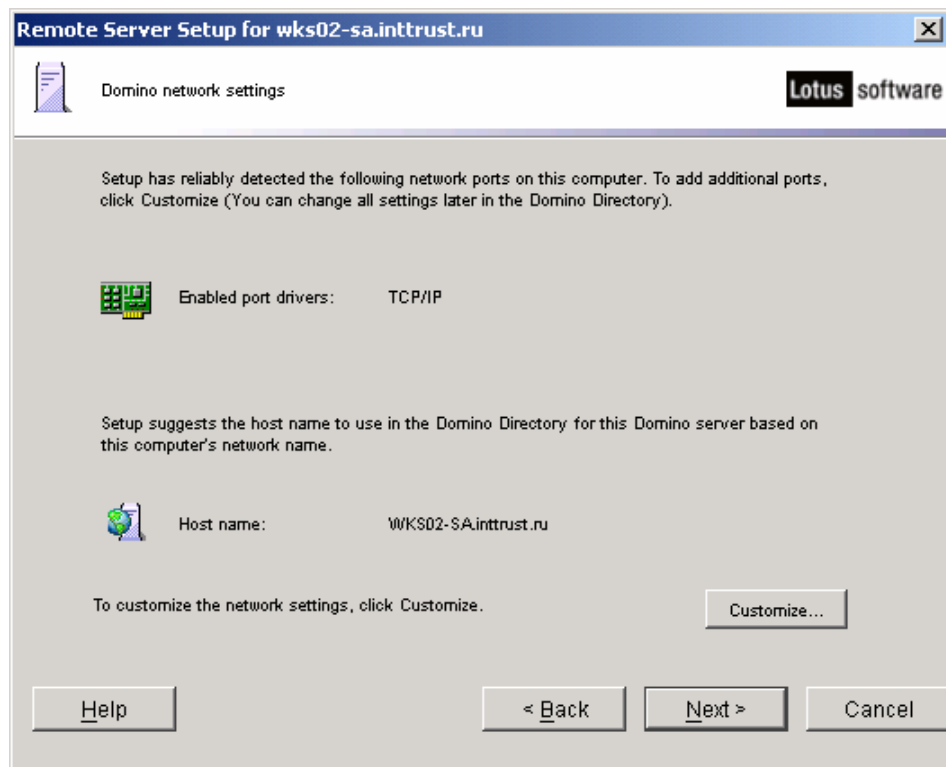


Рис. 110 Конфигурирование портов – подробности доступны в окне по кнопке *Customize...*

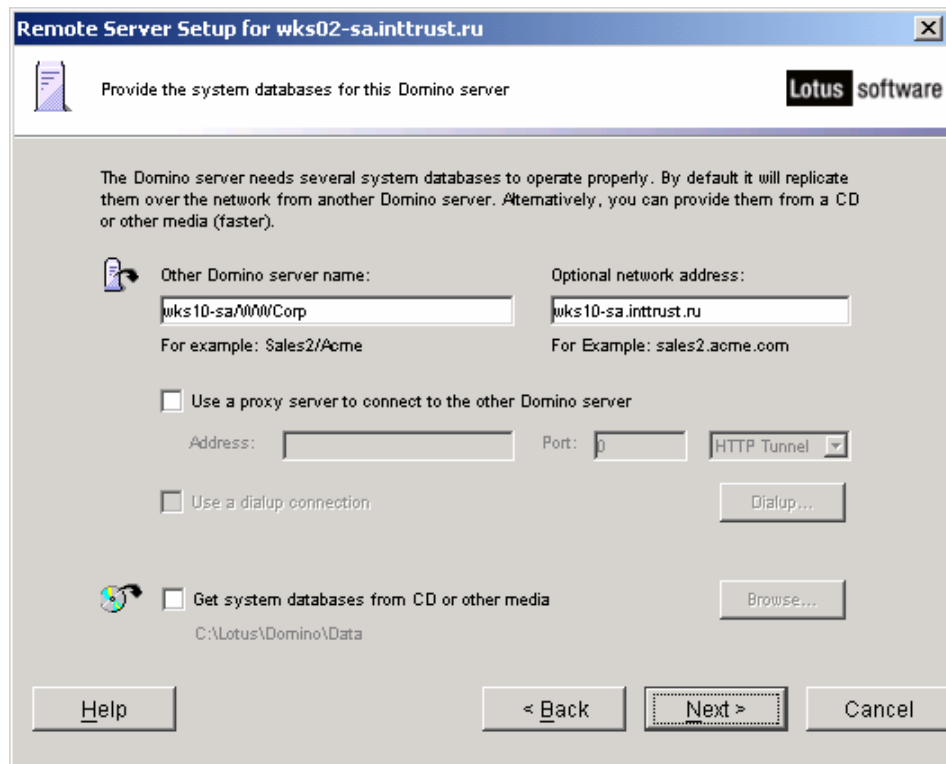


Рис. 111 Определяется способ получения реплики каталога Domino и других системных баз с существующего сервера. В окне выбран стандартный способ – по локальной сети с существующего сервера *wks10-sa/WWCorp* с сетевым адресом *wks10-sa.intrust.ru*. Возможно подключение к существующему серверу через прокси-сервер (либо HTTP-туннель, либо SOCKs) или по модемному соединению (XPC). Появился новый вариант – реплику «большого» каталога Domino взять с указанного местоположения, а только затем «дореплицировать» с существующим сервером.

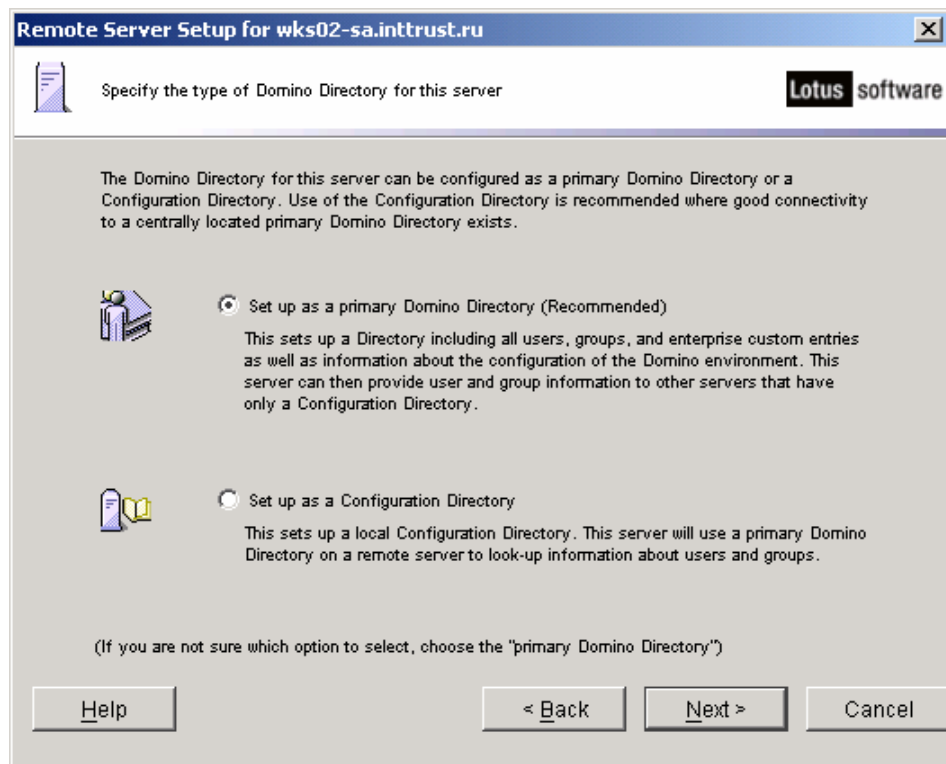


Рис. 112 Выбирается тип каталога Domino на устанавливаемом сервере – «полный» или Configuration Directory

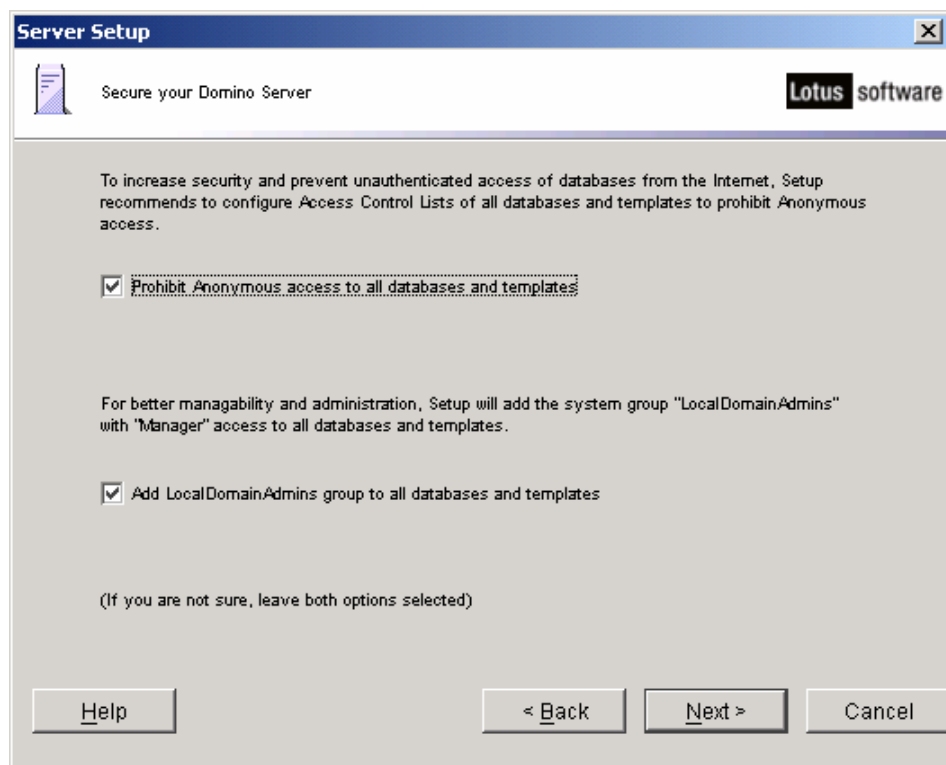


Рис. 113 Добавить во все базы и шаблона группу LocalDomainAdmins (в предшествующих версиях использовалась группа Administrators) с уровнем доступа Manager и Anonymous с уровнем доступа No Access

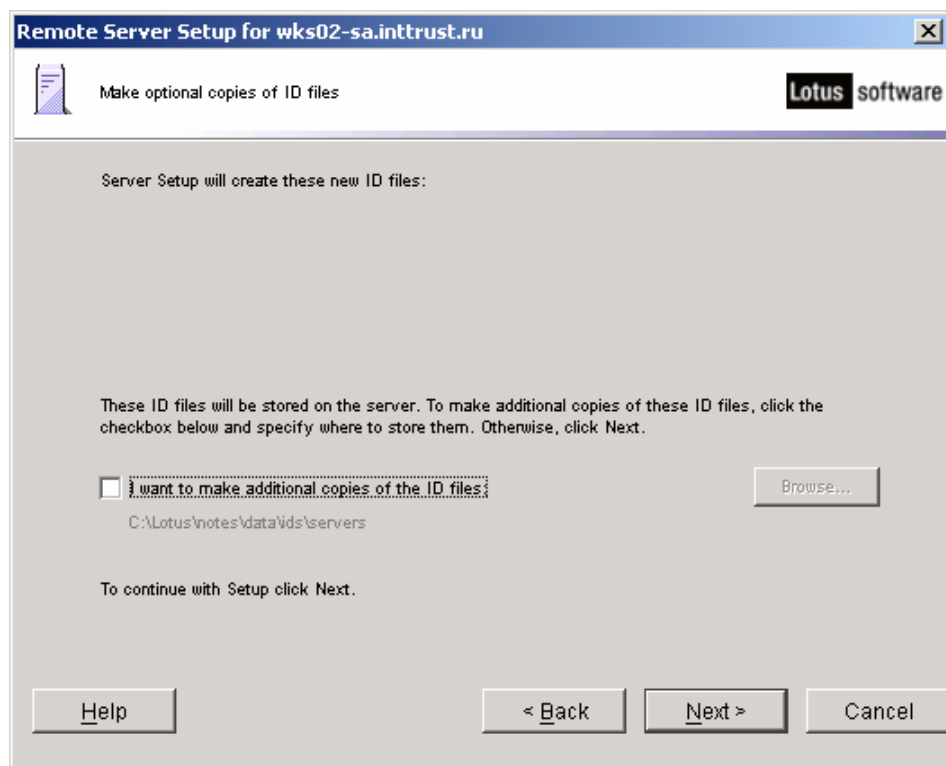


Рис. 114 Если бы на устанавливаемом удаленно сервере создавались бы ID-файлы (была бы выбрана установка первого сервера), их можно было бы скопировать на станцию администратора

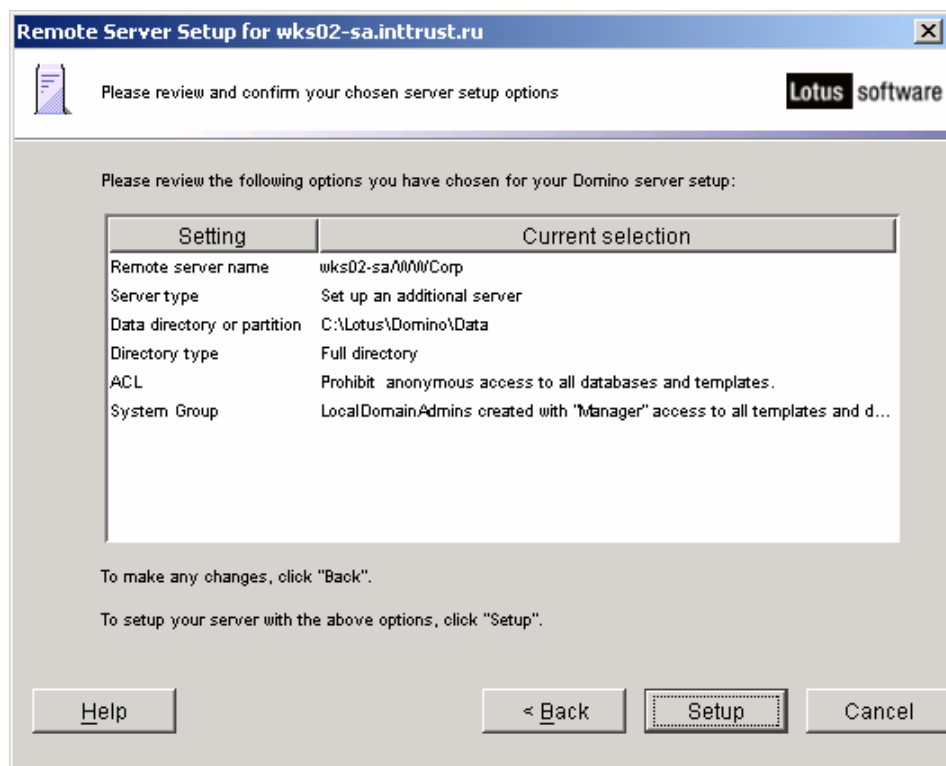


Рис. 115 Основные из выбранных параметров

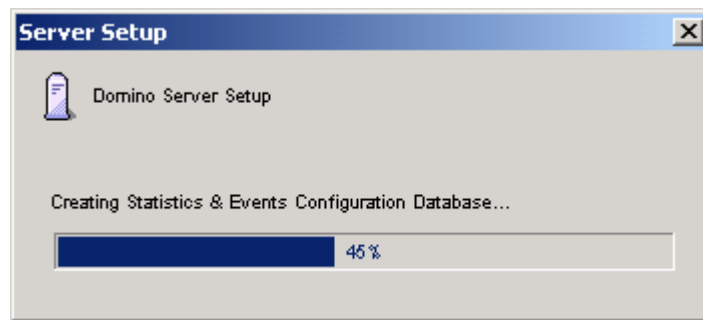


Рис. 116 Идет процесс установки

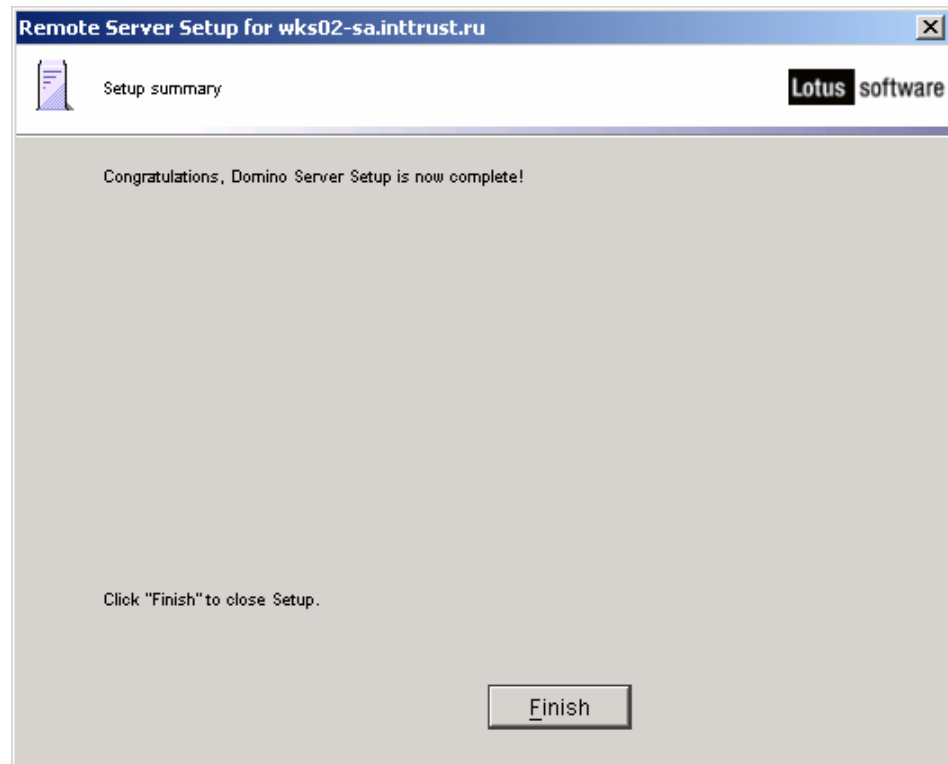


Рис. 117 Установка завершена

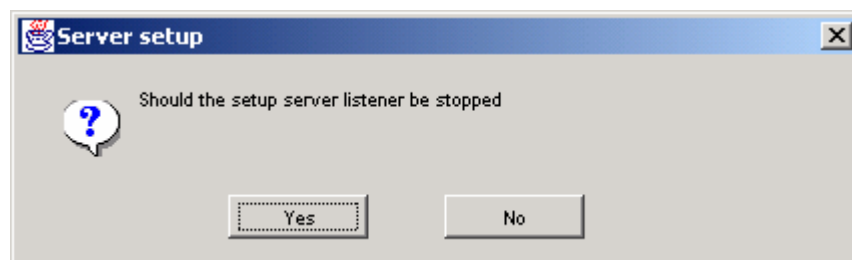
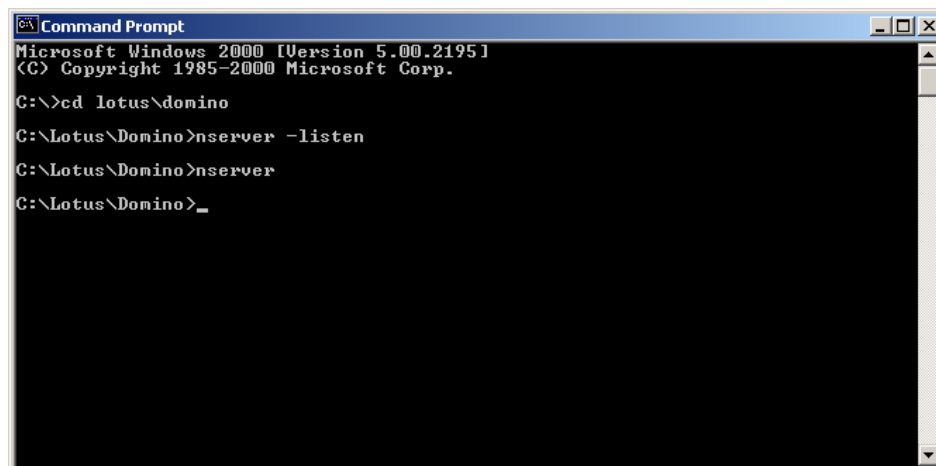


Рис. 118 Программа удаленной установки предлагает завершить листенер на устанавливаемом сервере, что и было сделано



```
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

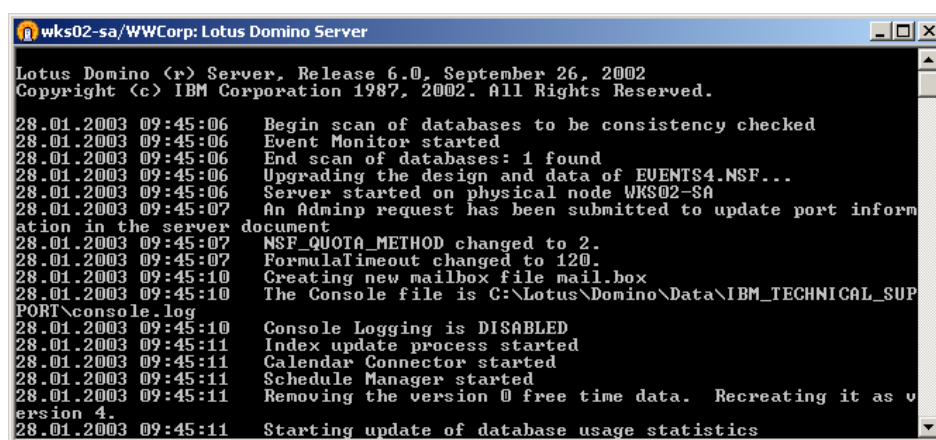
C:\>cd lotus\domino

C:\Lotus\Domino>nserver -listen

C:\Lotus\Domino>nserver

C:\Lotus\Domino>_
```

Рис. 119 Теперь, уже на компьютере установленного сервера, обычным образом запускается сервер

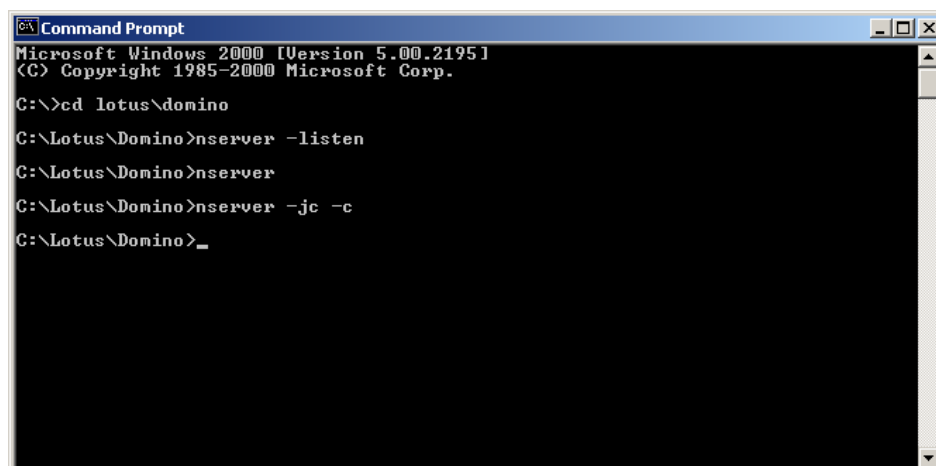


```
wks02-sa/WWCorp: Lotus Domino Server

Lotus Domino (r) Server, Release 6.0, September 26, 2002
Copyright (c) IBM Corporation 1987, 2002. All Rights Reserved.

28.01.2003 09:45:06   Begin scan of databases to be consistency checked
28.01.2003 09:45:06   Event Monitor started
28.01.2003 09:45:06   End scan of databases: 1 found
28.01.2003 09:45:06   Upgrading the design and data of EVENTS4.NSF...
28.01.2003 09:45:06   Server started on physical node WKS02-SA
28.01.2003 09:45:07   An Adminp request has been submitted to update port inform
28.01.2003 09:45:07   ation in the server document
28.01.2003 09:45:07   NSF_QUOTA_METHOD changed to 2.
28.01.2003 09:45:07   FormulaTimeout changed to 120.
28.01.2003 09:45:10   Creating new mailbox file mail.box
28.01.2003 09:45:10   The Console file is C:\Lotus\Domino\Data\IBM_TECHNICAL_SUP
28.01.2003 09:45:10   PORT\console.log
28.01.2003 09:45:10   Console Logging is DISABLED
28.01.2003 09:45:11   Index update process started
28.01.2003 09:45:11   Calendar Connector started
28.01.2003 09:45:11   Schedule Manager started
28.01.2003 09:45:11   Removing the version 0 free time data.  Recreating it as v
28.01.2003 09:45:11   ersion 4.
28.01.2003 09:45:11   Starting update of database usage statistics
```

Рис. 120 Первый реальный запуск сервера



```
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>cd lotus\domino

C:\Lotus\Domino>nserver -listen

C:\Lotus\Domino>nserver

C:\Lotus\Domino>nserver -jc -c

C:\Lotus\Domino>_
```

Рис. 121 Затем, остановив сервер, можно запустить на компьютере сервера Controller и сервер Domino, но без консоли

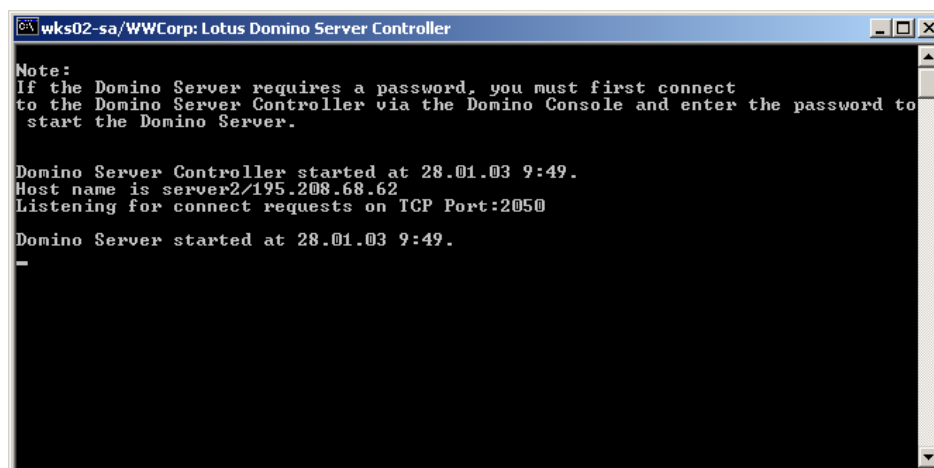


Рис. 122 Окно контроллера сервера Domino. Он «слушает» на порту 2050

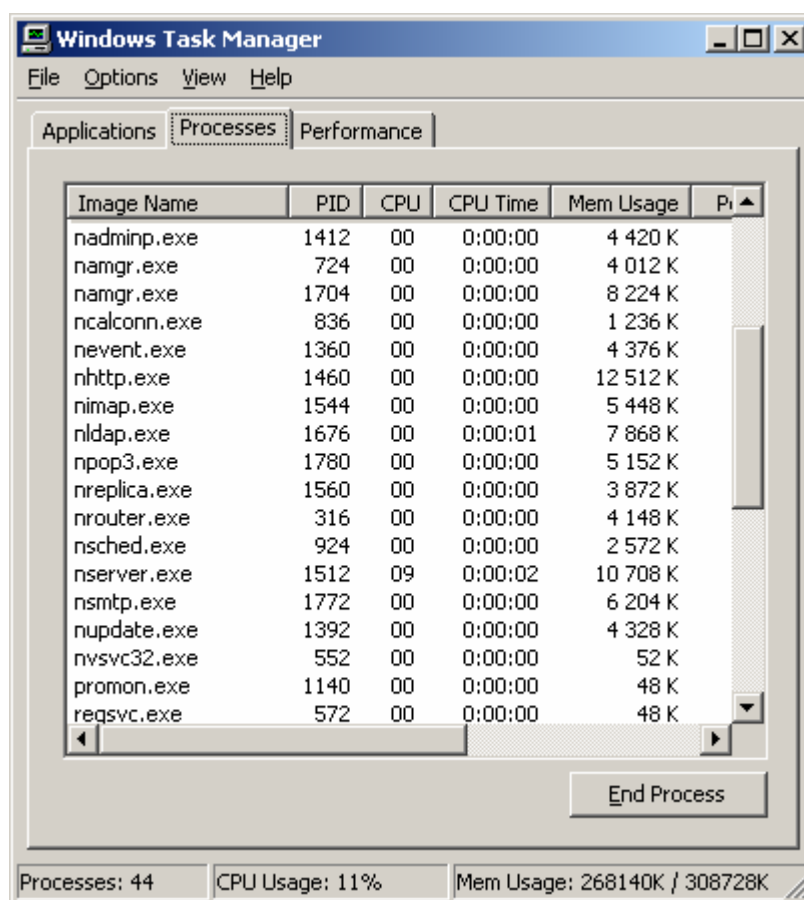


Рис. 123 Тот факт, что при этом запустился и сам сервер, виден из списка задач. Дальнейшая работа продолжается на компьютере администратора

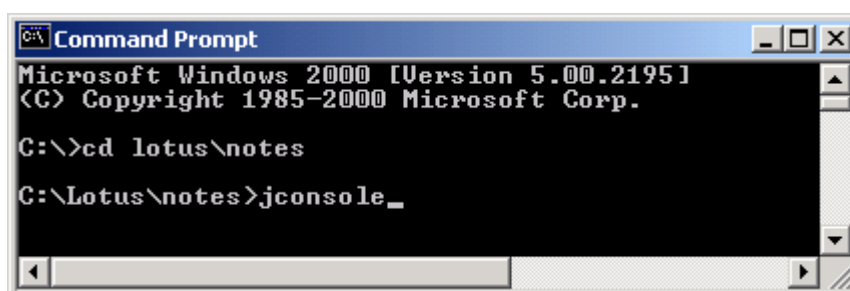


Рис. 124 Из каталога клиента администратора запускается Jconsole – Java-консоль

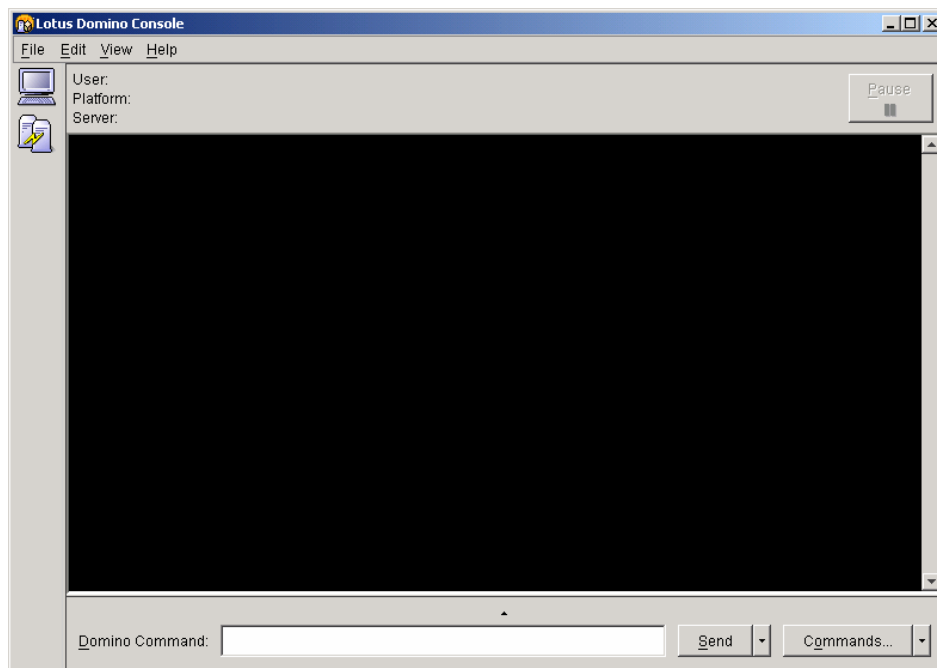


Рис. 125 Окно только что стартовавшей Java-консоли

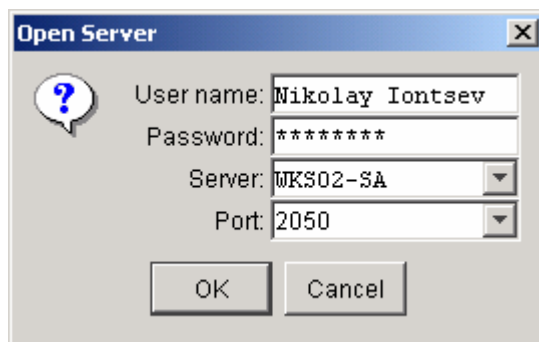


Рис. 126 Устанавливаем соединение с контроллером сервера

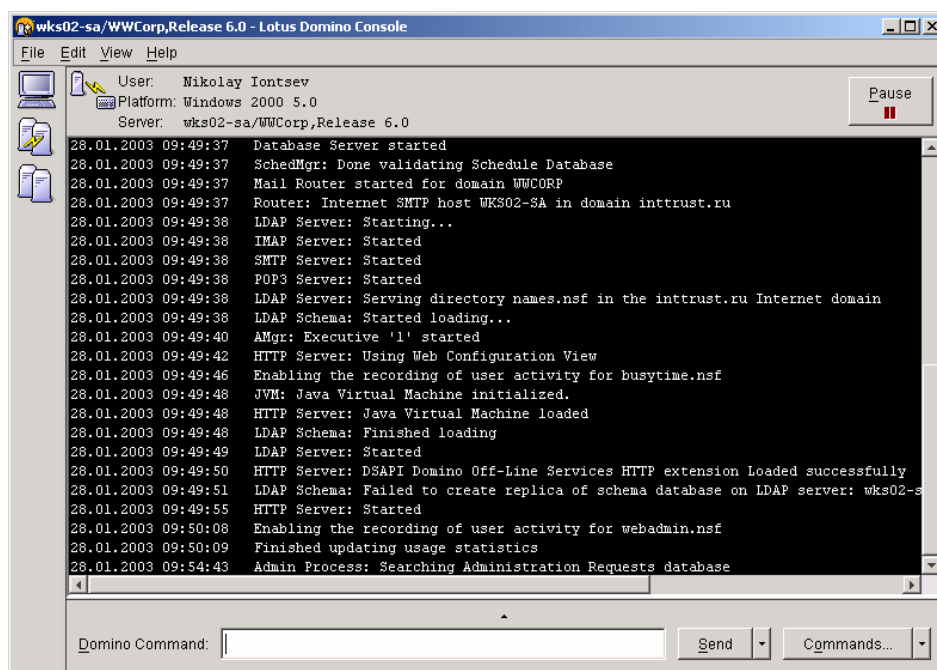


Рис. 127 Получаем консоль сервера

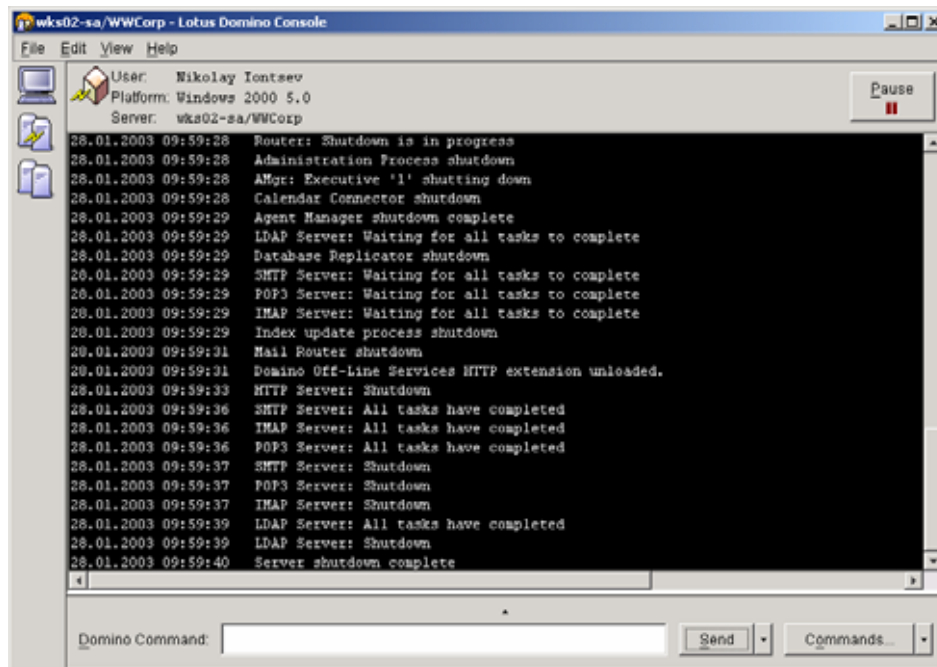


Рис. 128 Пока контроллер сервера работает, можем удаленно останавливать, «убивать зависший» и вновь запускать сервер, а так же использовать команды операционной системы

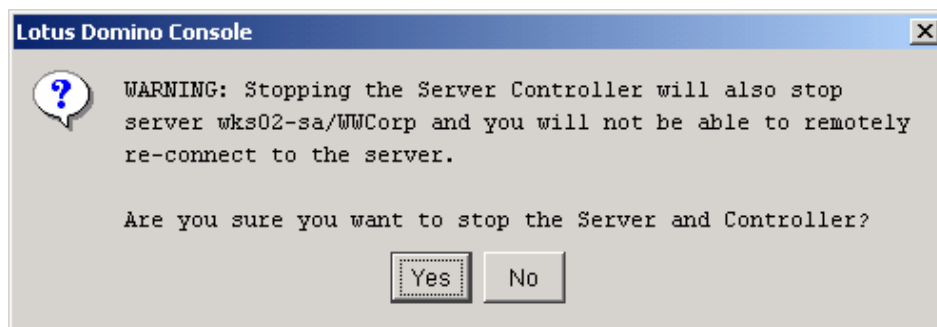


Рис. 129 Но если удаленно остановим контроллер, сервер и контроллер завершатся, и нам придется снова подойти на компьютер сервера для запуска сервера Domino и (или) контроллера

1.20. 1.1. xSP Server Setup (поддержка Hosted Organization)

Все сервера в домене ставятся в этой моде – и первый, и дополнительные. Нельзя поставить сервер в такой моде в существующий не-xSP-домен. Нельзя перевести существующий не-xSP-домен в эту моду.

1.20.1. 1.1.1. Что такое Hosted Organization Support (xSP)

- • Позволяют провайдером услуг Domino (ASP) удобно и безопасно хостировать приложения и службы (HTTP, POP3, IMAP...) многих организаций на одном кластере из серверов Domino
- • Хостируемые серверы Domino «виртуальны» на одном экземпляре реального сервера Domino
- • Кластеры добавляют к этому только надежность и балансировку нагрузки
- • Virtual Directory - многие независимые организации (деревья имен) в одной Domino Directory
- • Каждая хостируемая организация имеет свой ID-файл сертификата организации
- • Хостируемые организации логически изолированы
 - • Используется Extended ACL (xACL) в NAMES.NSF и ADMIN4.NSF
 - • Используются Directory ACL для каталогов с базами
 - • Используются Internet Sites

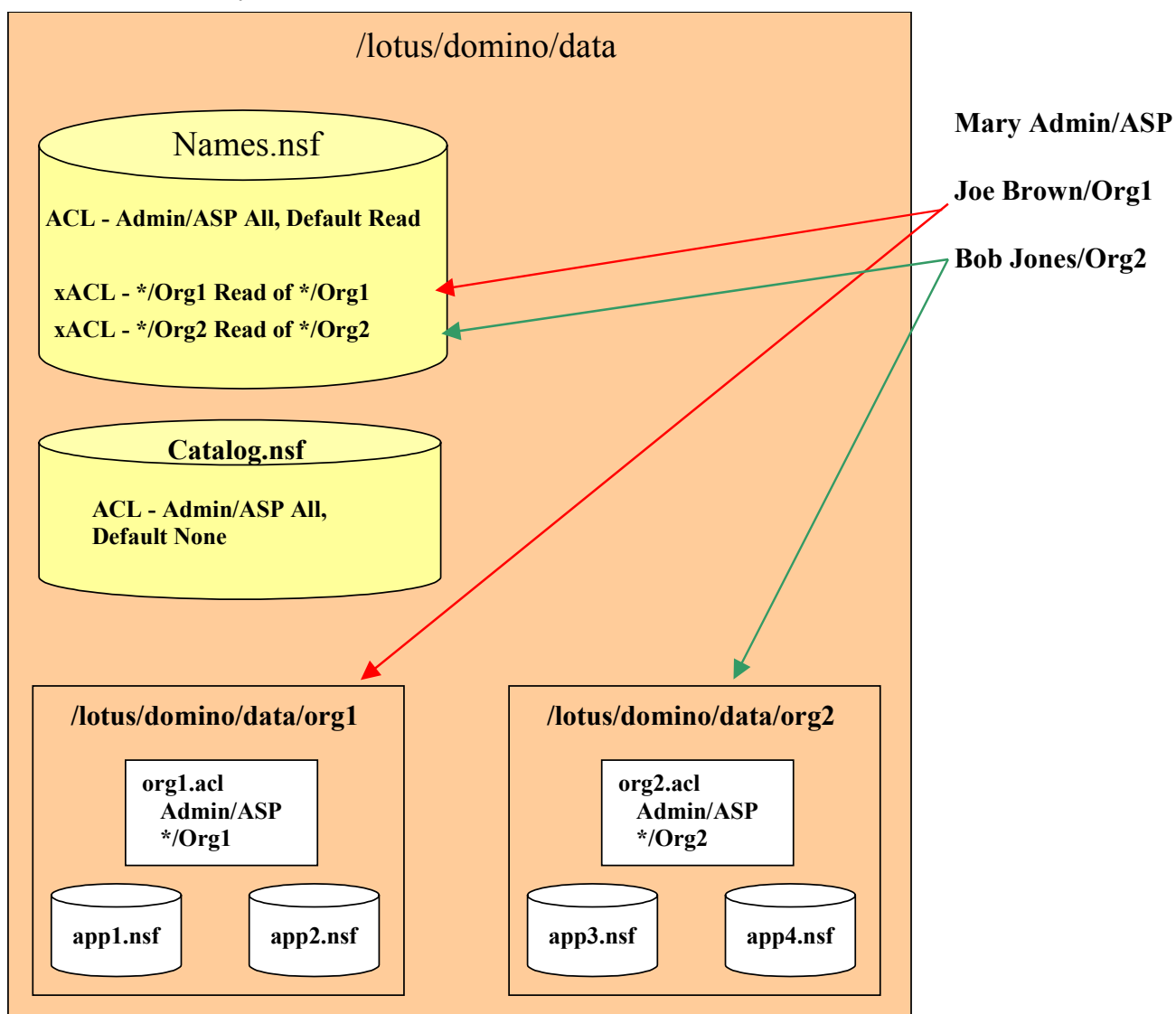


Рис. 130 Domino Data и «виртуальные» каталоги»

1.20.2. 1.1.2. Первая фаза установки сервера Domino R6

Запускаем `setup.exe -asp`.

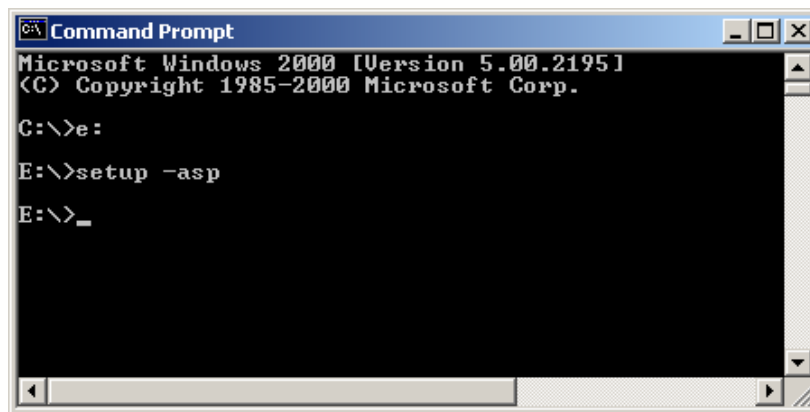


Рис. 131

Далее никаких видимых отличий от обычной установки.

1.20.3. 1.1.3. Вторая фаза установка сервера Domino R6

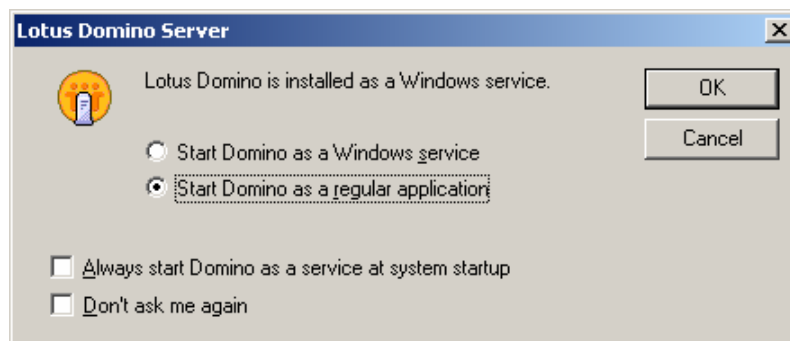


Рис. 132 Это обычный «пускач», появившийся с 6.02

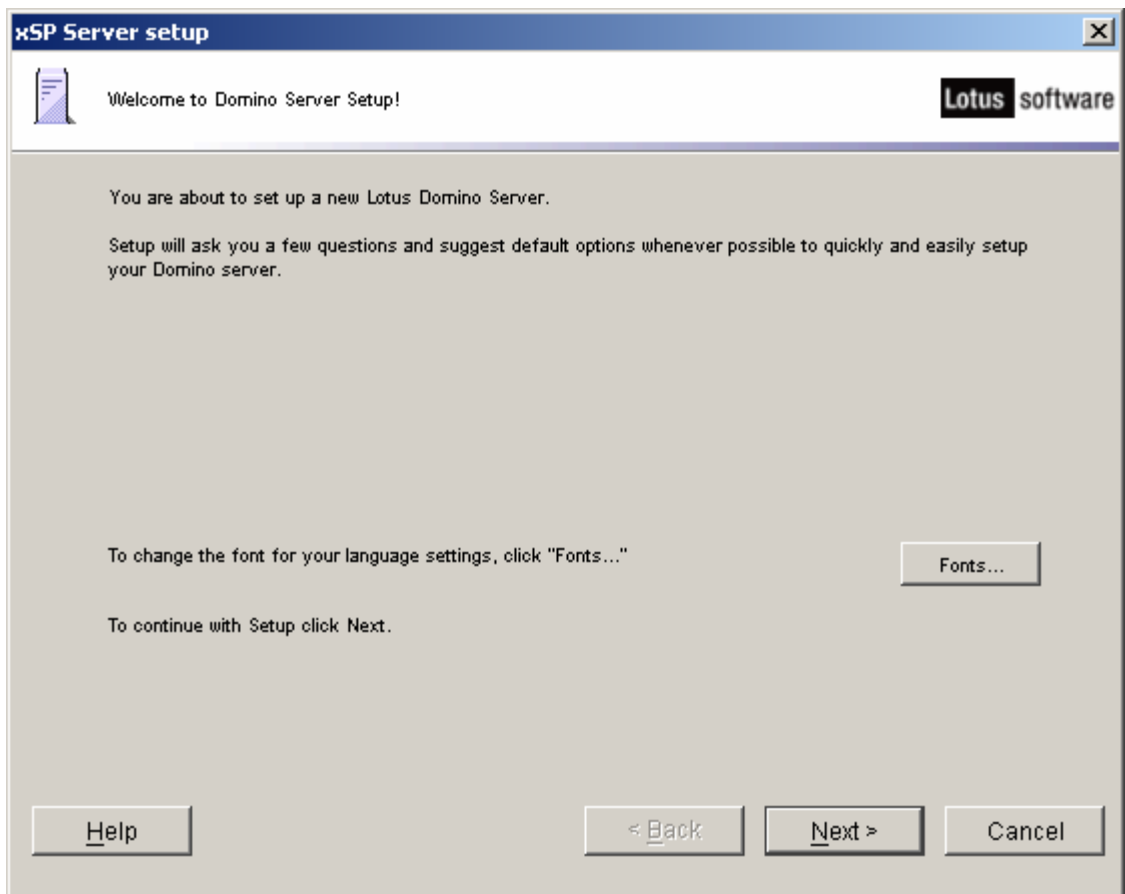


Рис. 133 Пока все обычно, кроме заголовка

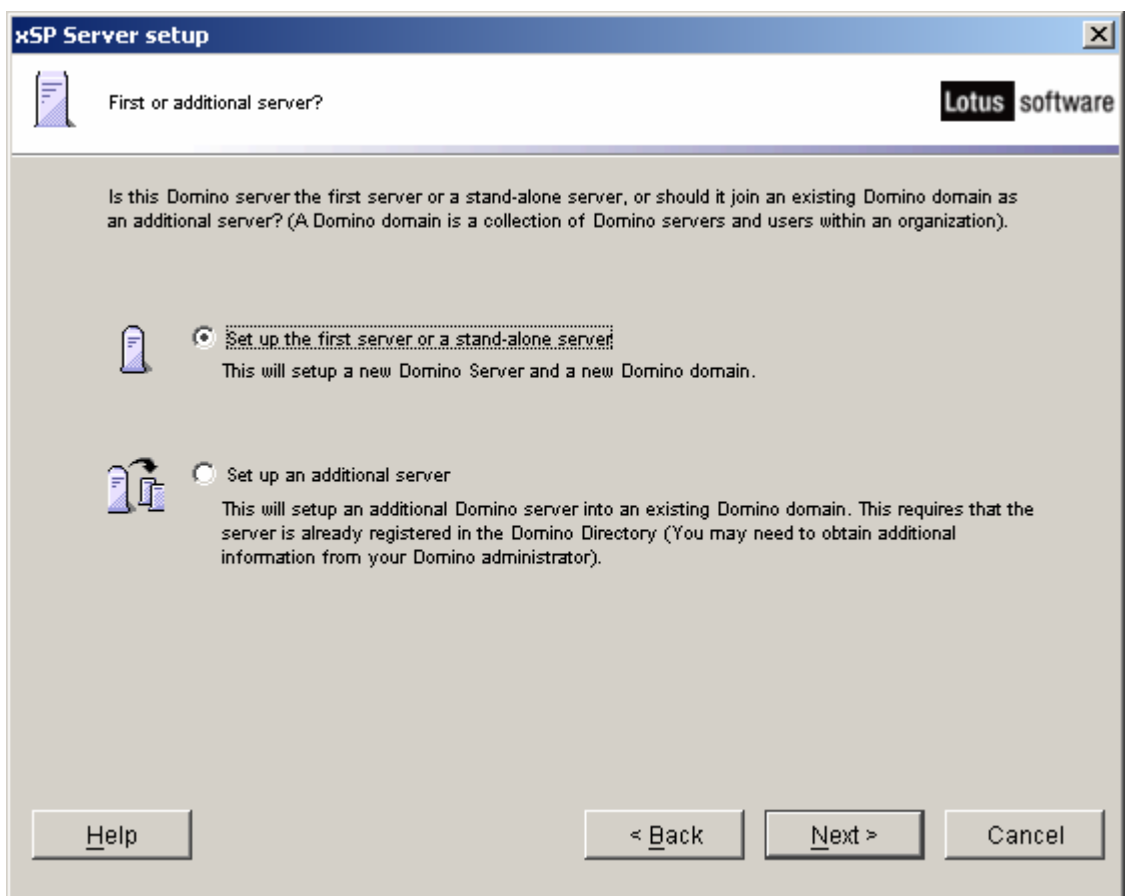


Рис. 134 Первый сервер

xSP Server setup 

 Provide a server name and title 

You must provide a unique name for your new Domino server. Carefully choose the server name; you cannot easily change it later. By default, Setup recommends that you use the computer's host name as the server name.

 Server name:
For example: Sales1

Optional: Provide a short title which describes the purpose or function of this server. (You can always change this information later in the Domino Directory)

 Server title:
For example: Corporate Sales Server 1

 ☐ I want to use an existing server ID file:
C:\Lotus\Domino\Data\server.id 

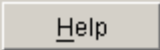
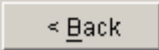
   

Рис. 135 Имя сервера

xSP Server setup Lotus software

Choose your organization name

The organization name is usually your company name. It becomes part of each server and user name. Do not choose a long organization name. For example, instead of Acme Corporation, use Acme.

Organization name:
Minimum of 3 characters

This server's final name will be: xSPServer1/IntTrustxSP
Atypical user name will be: Nikolay Iontsev/IntTrustxSP

Organization Certifier password:
Minimum of 5 characters

Confirm password:

☐ I want to use an existing certifier ID file:
C:\Lotus\Domino\Data\cert.id

To specify additional organization settings click Customize.

Рис. 136 Имя организации и пароль для ID сертификатора

xSP Server setup Lotus software

Choose the Domino domain name

As part of setting up the first Domino server, Setup creates a new Domino domain, which is a collection of Domino servers and users that share the same Domino Directory.

The Domino domain name can be the same as the organization name. Choose a short domain name.

Domino domain name:
For example: Acme

Рис. 137 Домен совпадает с именем организации и его нельзя изменить – специфика!

xSP Server setup Lotus software

Specify an Administrator name and password

To create the Administrator's ID, you must provide the administrator's name and password. You can use the name of a specific person, or a last name only to create a generic Administrator ID that can be used by several people.


 First name:
 Middle:
 Last name (or generic account name):


 Administrator password:
 Confirm password:

Minimum of 5 characters

The Administrator ID file will be stored inside the server's Domino Directory.

☒ Also save a local copy of the ID file:
 C:\Lotus\Domino\Data\admin.id Browse...


☐ I want to use an existing Administrator ID file:
 C:\Lotus\Domino\Data\admin.id Browse...

Help
< Back
Next >
Cancel

Рис. 138 Имя и пароль xSP-админа

xSP Server setup Lotus software

What Internet services should this Domino Server provide?

Select the Internet services this Domino server will provide. Basic Notes and Domino services are set up by default. (You can always change these options later in the Domino Directory).


 Setup Internet services for:

- ☒ Web Browsers (HTTP services)
- ☒ Internet Mail Clients (SMTP, POP3 and IMAP services)
- ☒ Directory services (LDAP services)

To customize all other Domino services, click Customize. Customize...

Help
< Back
Next >
Cancel

Рис. 139

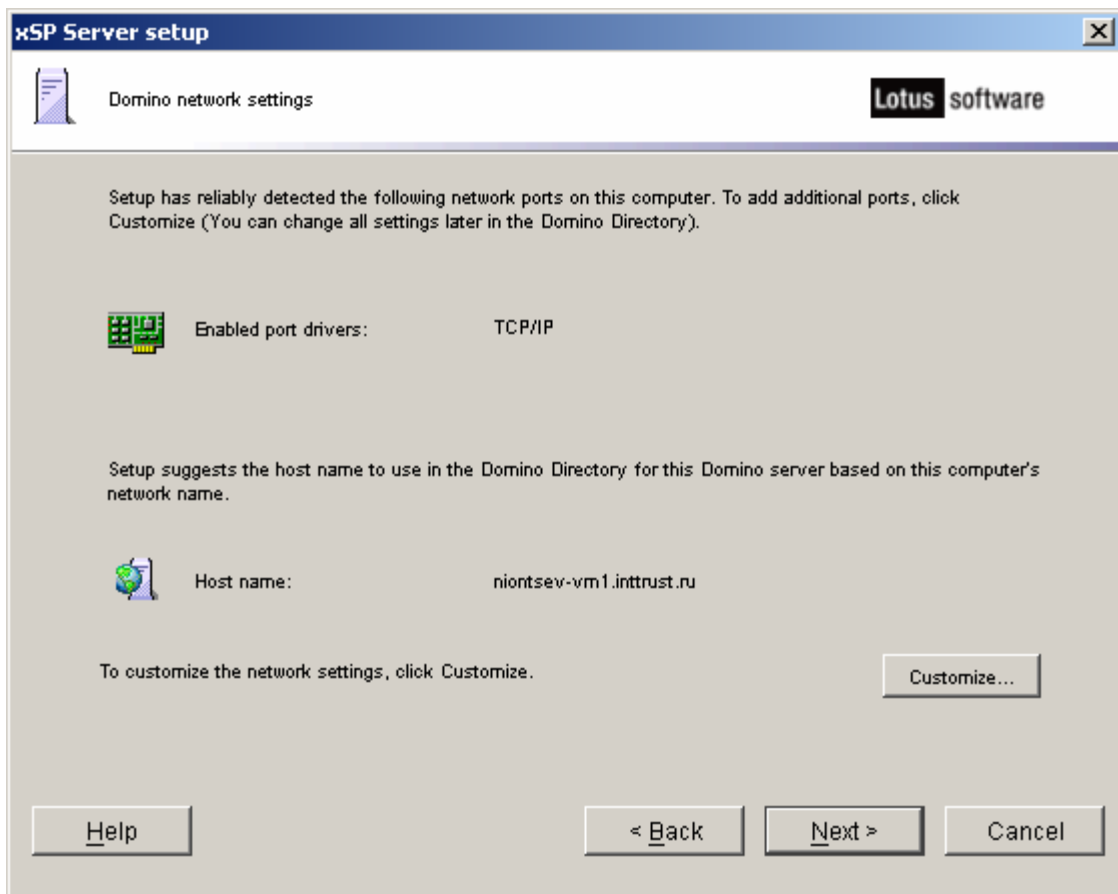


Рис. 140

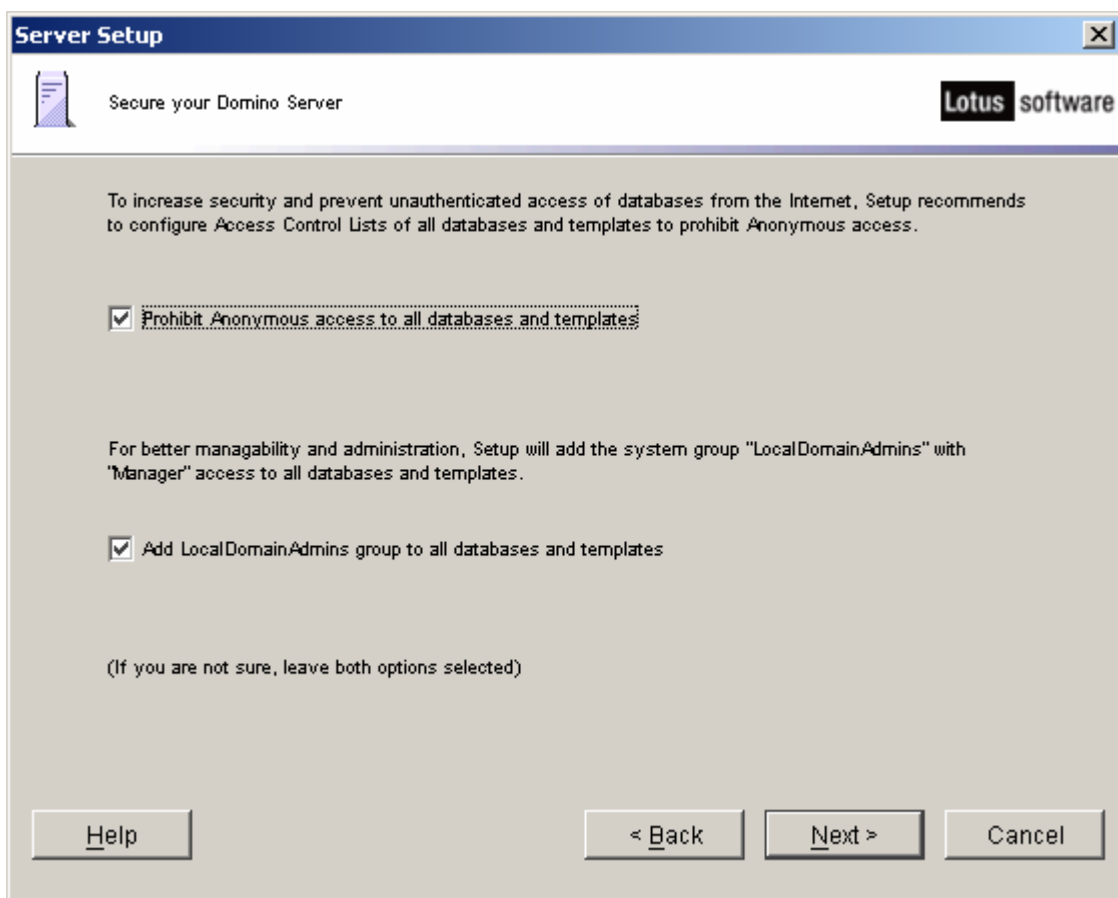
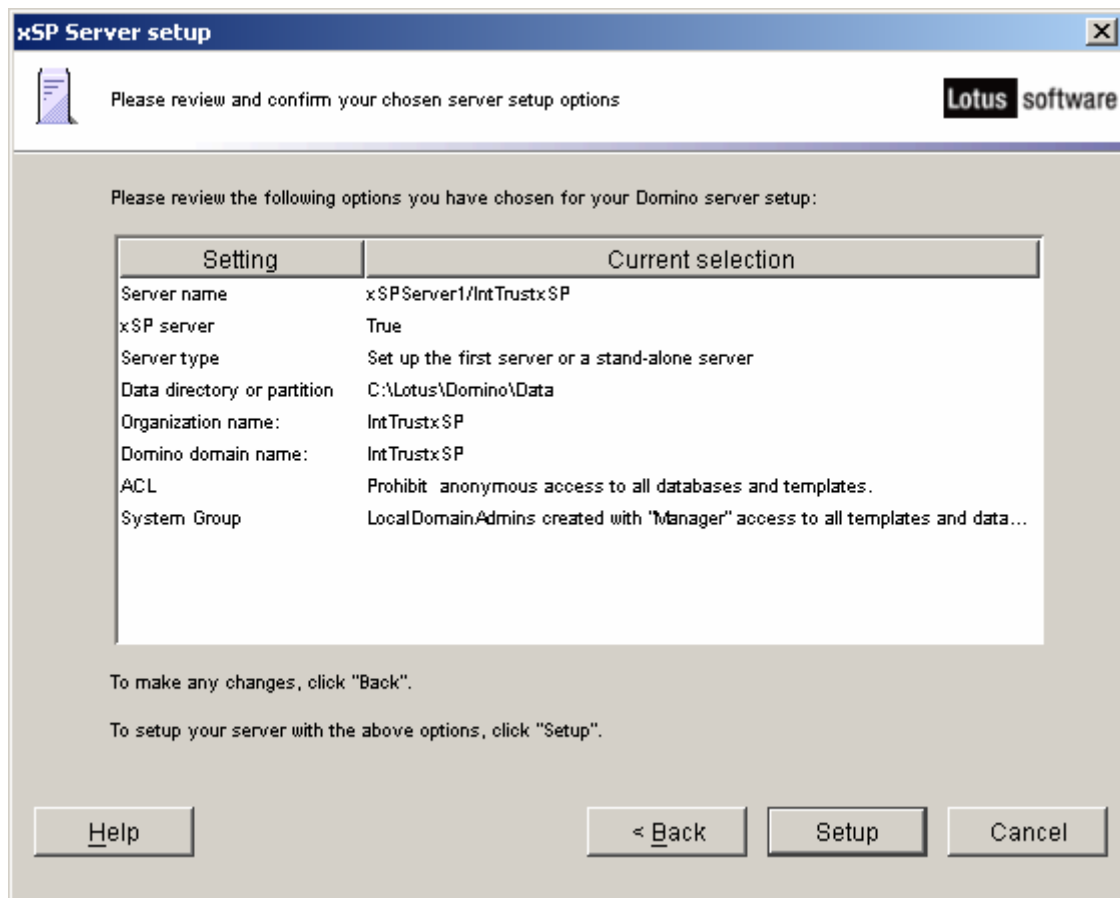
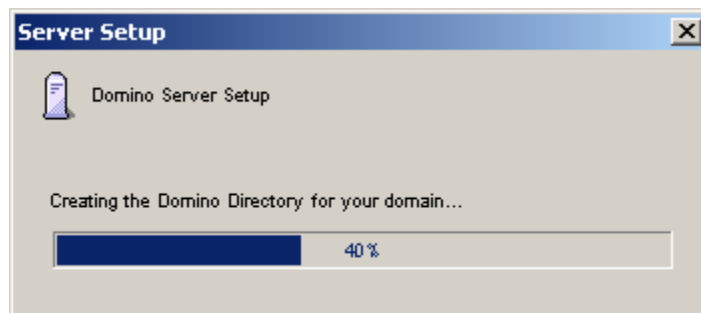


Рис. 141



Puc. 142



Puc. 143

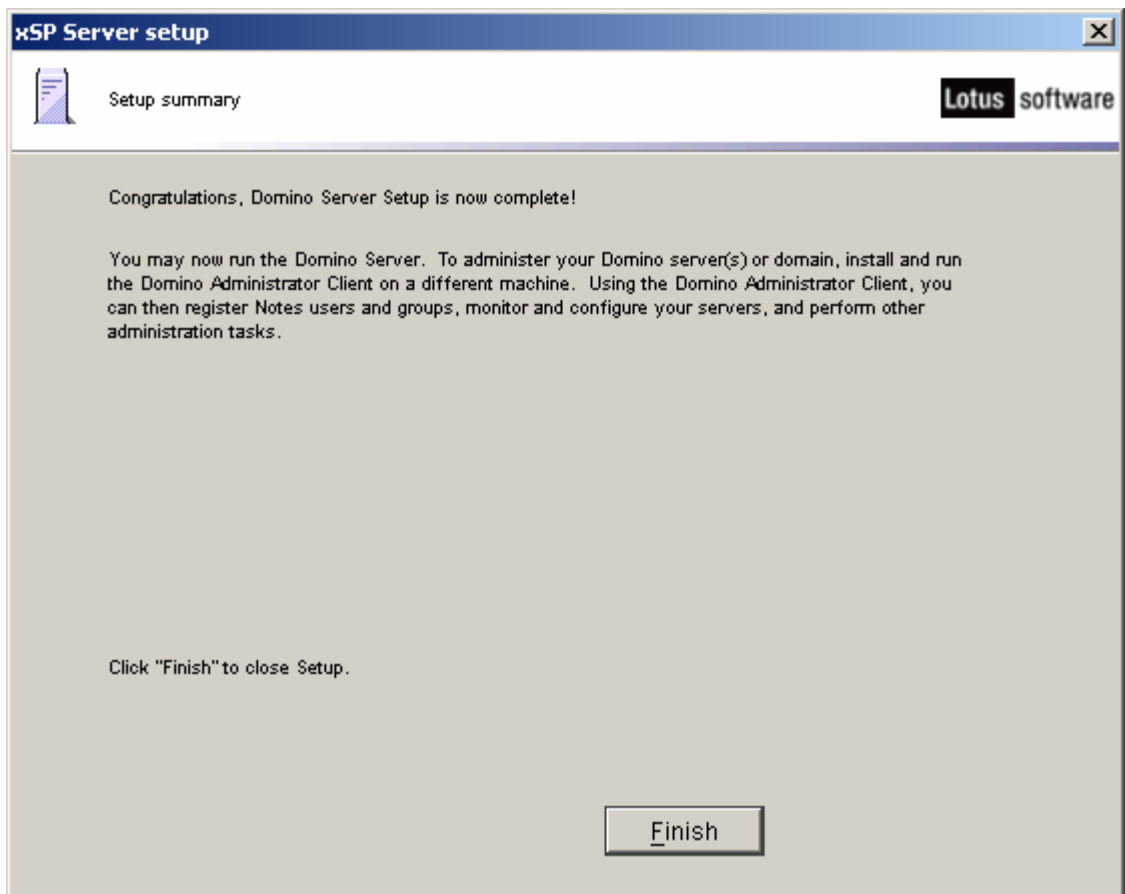


Рис. 144

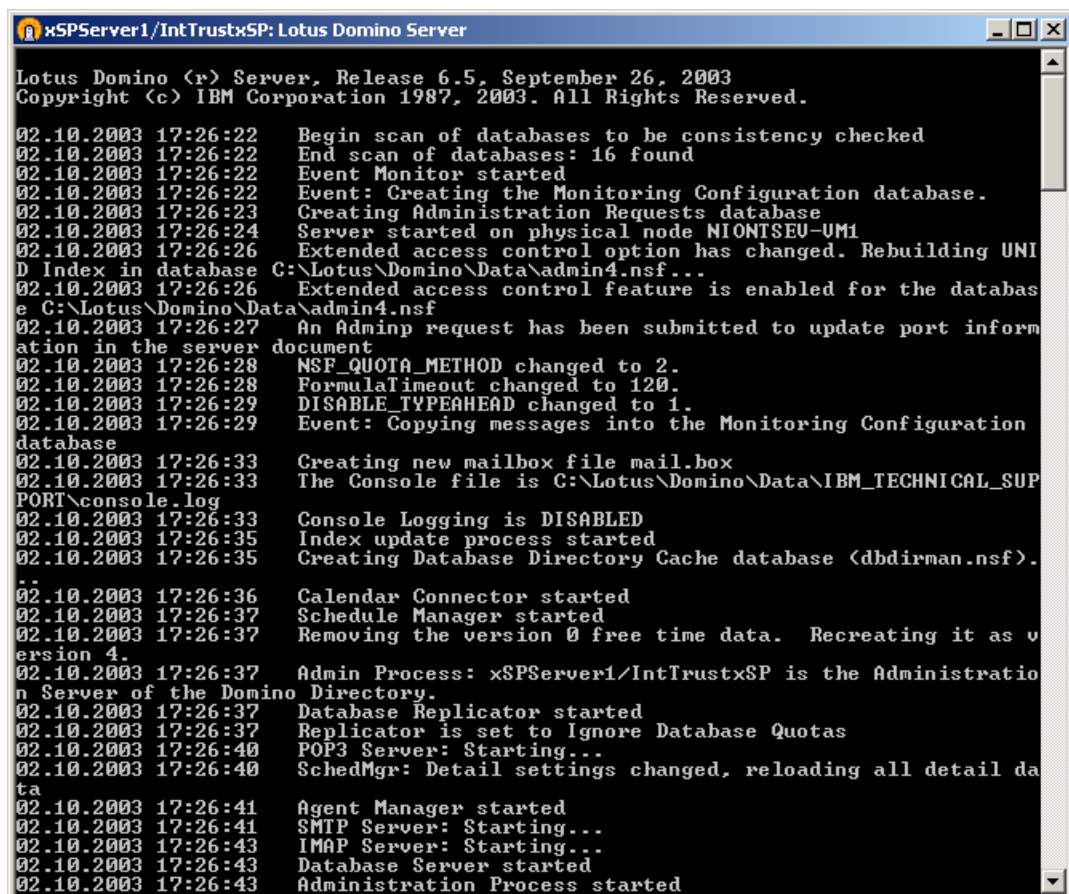


Рис. 145 Тот факт, что это xSP-сервер, уже заметен по сообщениям «Extended access control ... changed/enabled ... admin4.nsf»...

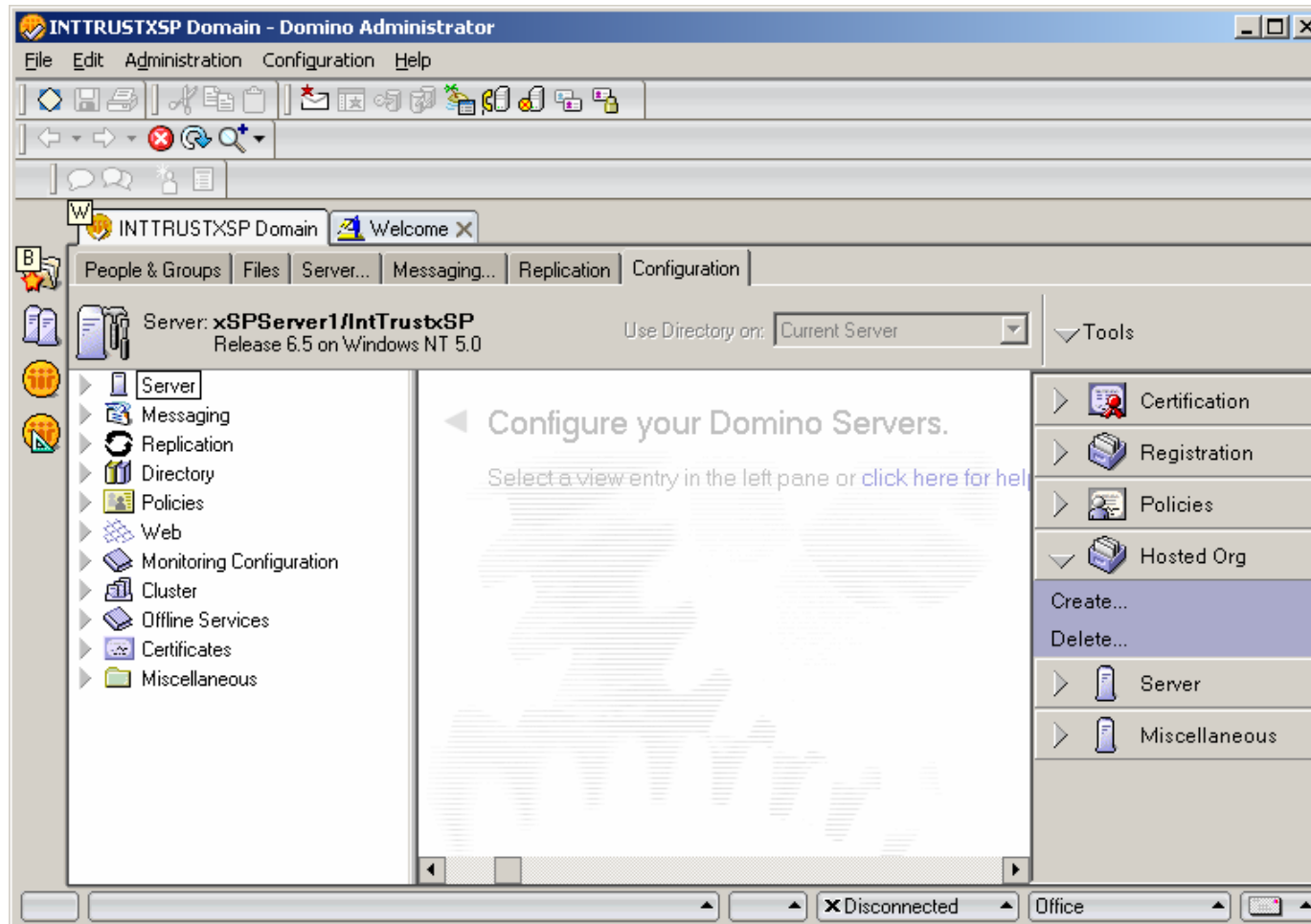


Рис. 146 После установки клиента Администратора видим, что операции Hosted Org-Create и Delete стали доступны...

1.21. 1.1. Дополнительные заметки

1.21.1. 1.1.1. Сервер и клиенты на одном компьютере

Нерекомендуемая в рабочей среде, но типичная для учебных центров конфигурация.

Lotus	\Domino		Каталог программ сервера: nServer.exe - ядро сервера, n***.exe - серверные задачи, nlNotes.exe — клиент в каталоге сервера	*.exe, *.dll Файл NOTES.INI для сервера (KitType=2)
		\data	Каталог данных сервера	*.id, names.nsf, log.nsf, mail[n].box ...
	\Notes		Каталог программ клиентов: Notes, Designer, Administrator	*.exe, *.dll Файл NOTES.INI для всех клиентов (KitType=1)
		\data	Каталог данных клиентов	*.id, *.dsk, names.nsf, bookmark.nsf, log.nsf, mail.box ...

1.21.2. 1.1.2. Удаление сервера и клиентов

1) Из Control Panel - Add/Remove Program выполнить UnInstall для сервера и клиентов.

2) Каталог Lotus со всем оставшимся его содержимым удалить - иначе при новой установке будут использоваться старые базы, ID-файлы и NOTES.INI, в результате чего могут быть проблемы.

3) На всякий случай можно заглянуть в реестр и, если вдруг это необходимо (обычно UnInstall R5/6 корректно «вычищает» реестр), вручную «вычистить» реестр от «ссылок на предыдущую установку» сервера или клиентов:

```
HKEY_LOCAL_MACHINE\
    SOFTWARE\Lotus\Domino - сервер
    SOFTWARE\Lotus\Notes - клиенты
    SYSTEM\CurrentControlSet\Services\LotusDominoServer - сервер как сервис
NT/2000/2003
    SYSTEM\CurrentControlSet\Services\LotusNotesSingleLogon - сервис
SingleLogon для клиентов
    SYSTEM\CurrentControlSet\Services\notestat\Performaice - dll для
«наблюдения» за сервером из Performaice Monitor
```

1.21.3. 1.1.3. Чтобы при запуске сервера Domino как сервиса на его консоли даты отображались в «русском» формате

Чтобы при запуске сервера Domino как сервиса на его консоли и в LOG.NSF даты были в «русском» формате, нужно исправить в реестре настройки для Default:

REGEDIT4

```
[HKEY_USERS\DEFAULT\Control Panel\International]
"Locale"="00000419"
```

```
"sLanguage"="RUS"
"sCountry"="Russia"
"iCountry"="7"
"sList"=";"
"iMeasure"="0"
"sDecimal"=","
"sThousand"=" "
"iDigits"="2"
"iLZero"="1"
"sCurrency"="p."
"iCurrDigits"="0"
"iCurrency"="1"
"iNegCurr"="5"
"sDate"="."
"sTime"=":"
"sShortDate"="dd.MM.yy"
"sLongDate"="d MMMM yyyy 'r.'"
"iDate"="1"
"iTime"="1"
"iTLZero"="0"
"s1159"=""
"s2359=""
```

```
[HKEY_USERS\DEFAULT\Control Panel\International\Sorting Order]
```



date.reg

1.22. 1.1. Использование Domino Administrator

1.22.1. 1.1.1. Навигация в клиенте администратора

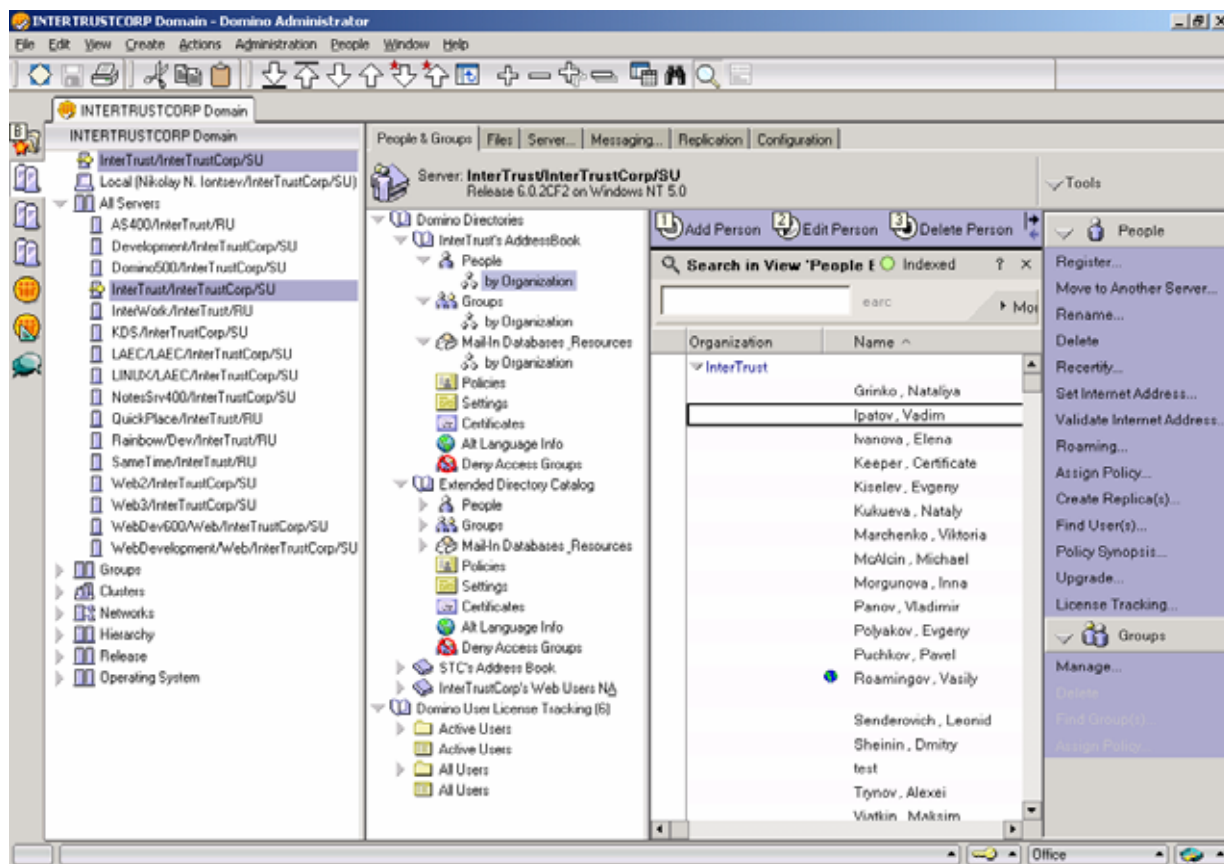


Рис. 147 People & Groups – операции с пользователями и группами

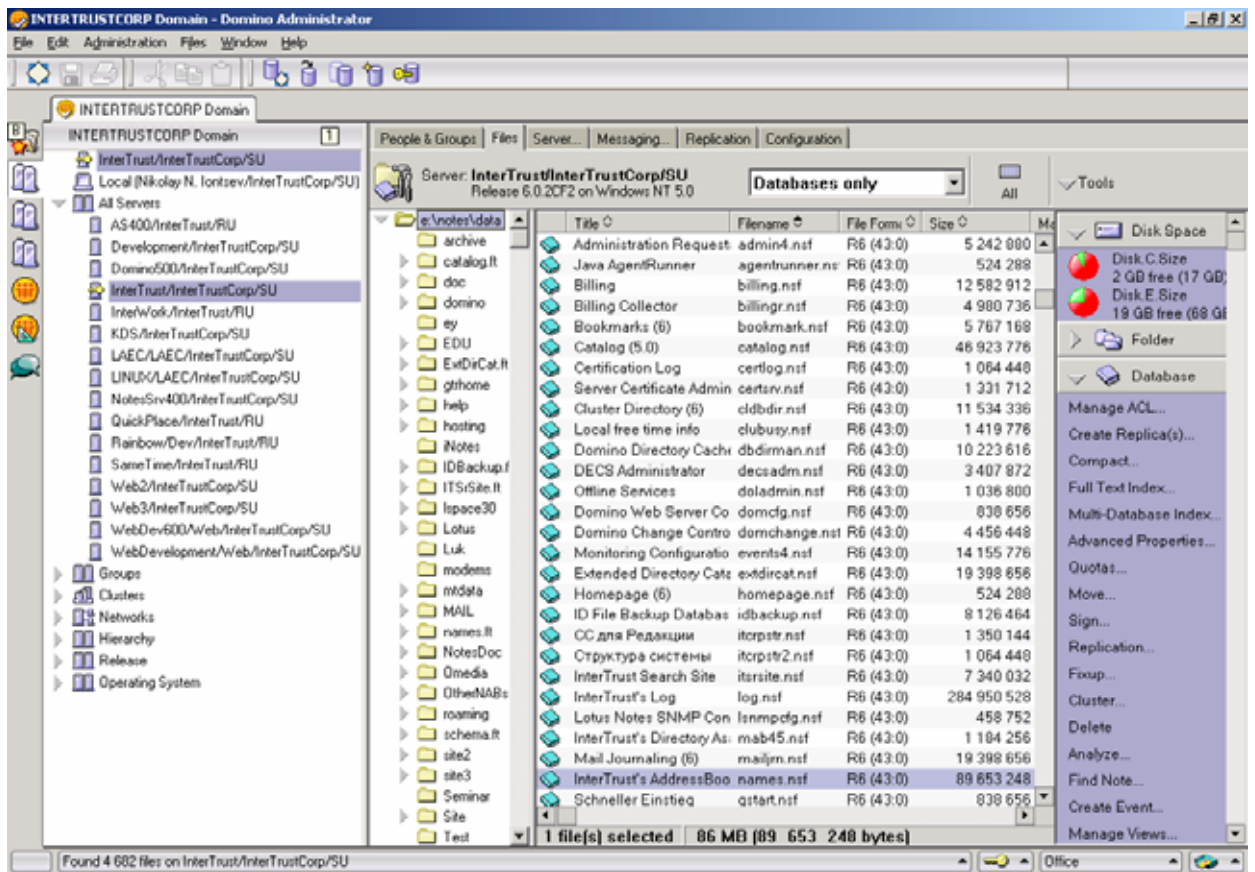


Рис. 148 Files – операции с базами, шаблонами, каталогами...

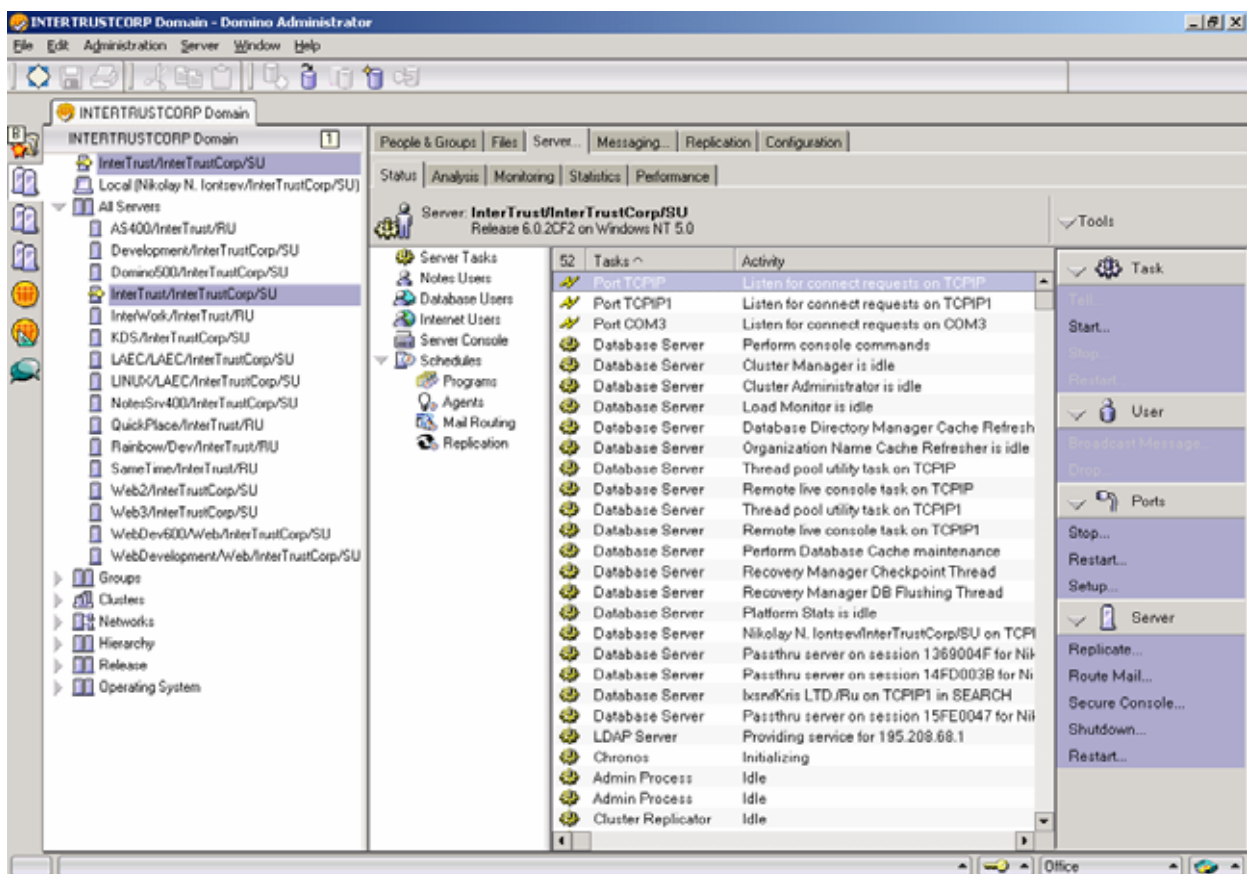


Рис. 149 Server – управление и контроль работы сервера

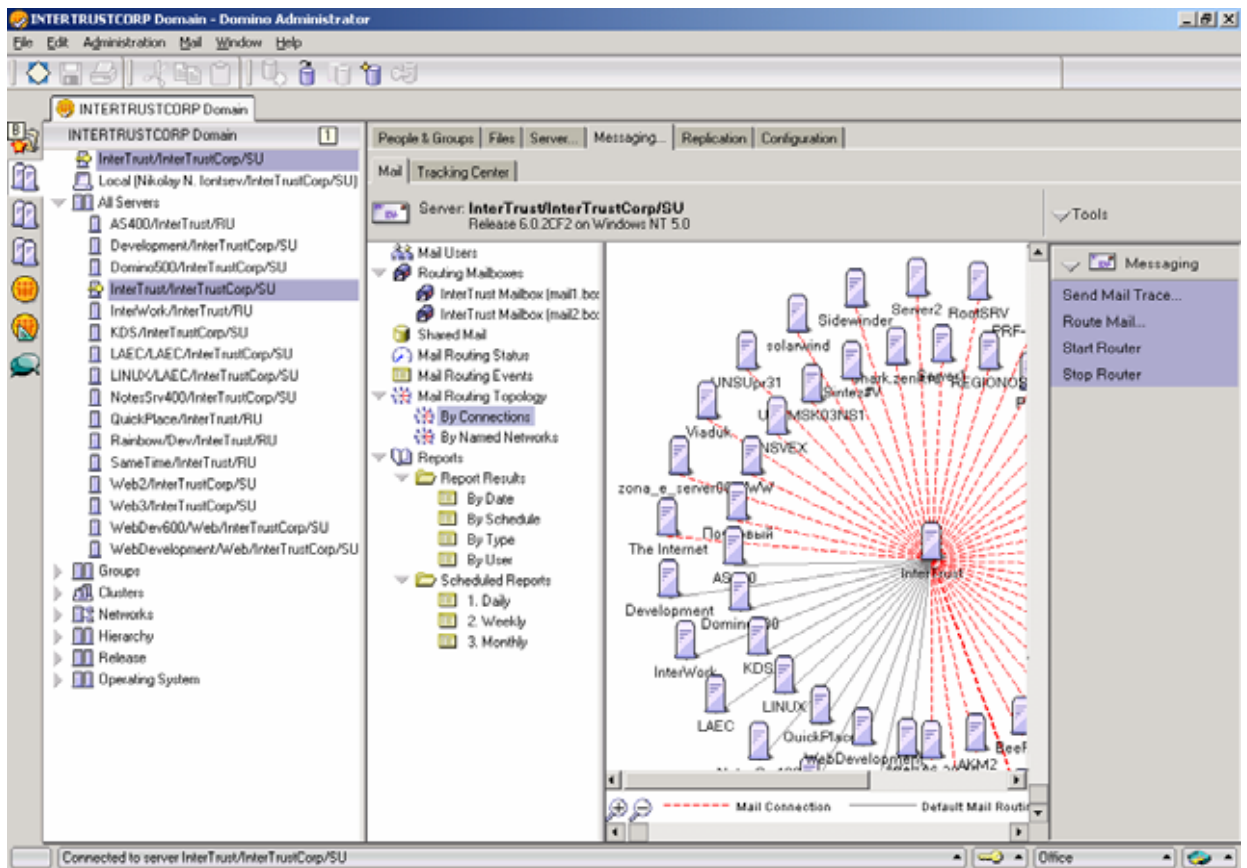


Рис. 150 Mail – контроль работы почтовой системы

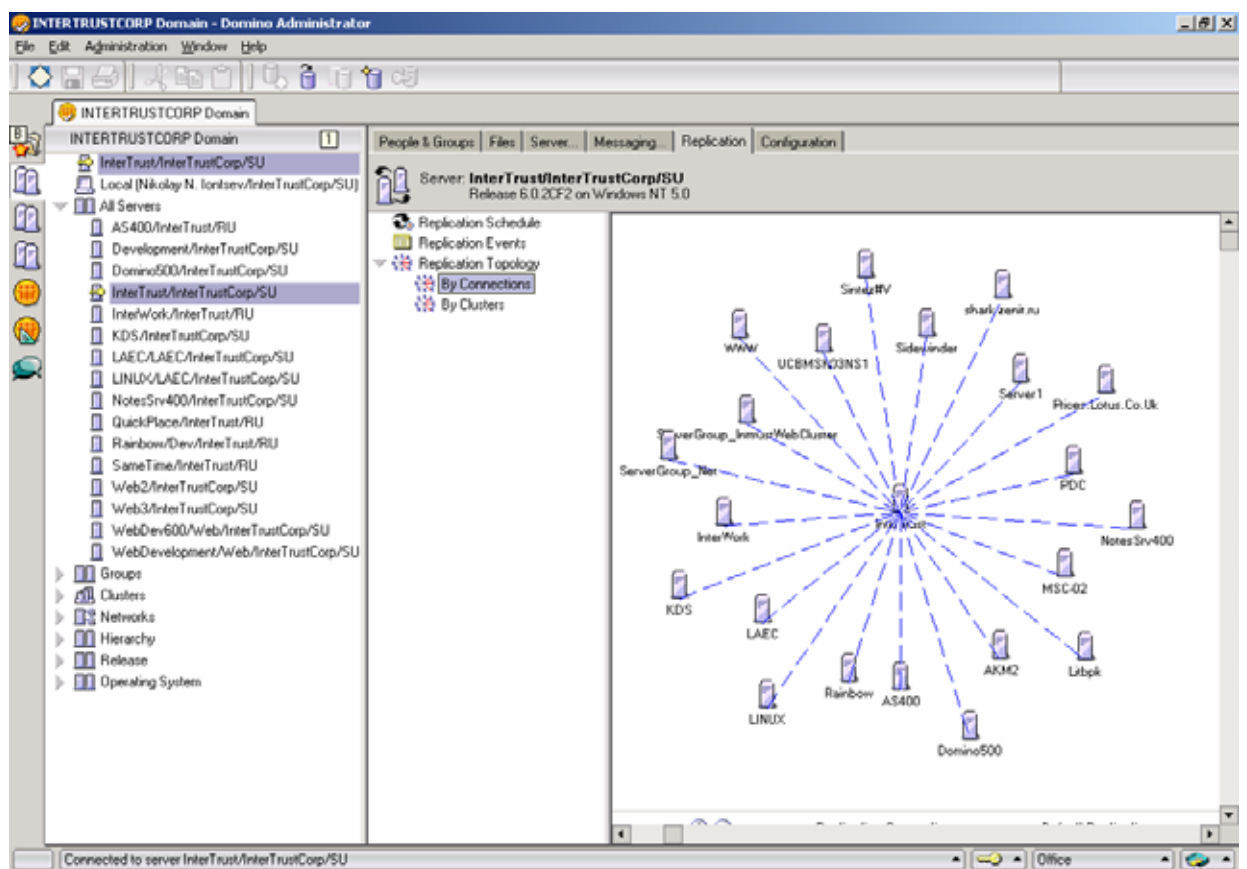


Рис. 151 Replication – контроль репликаций между серверами

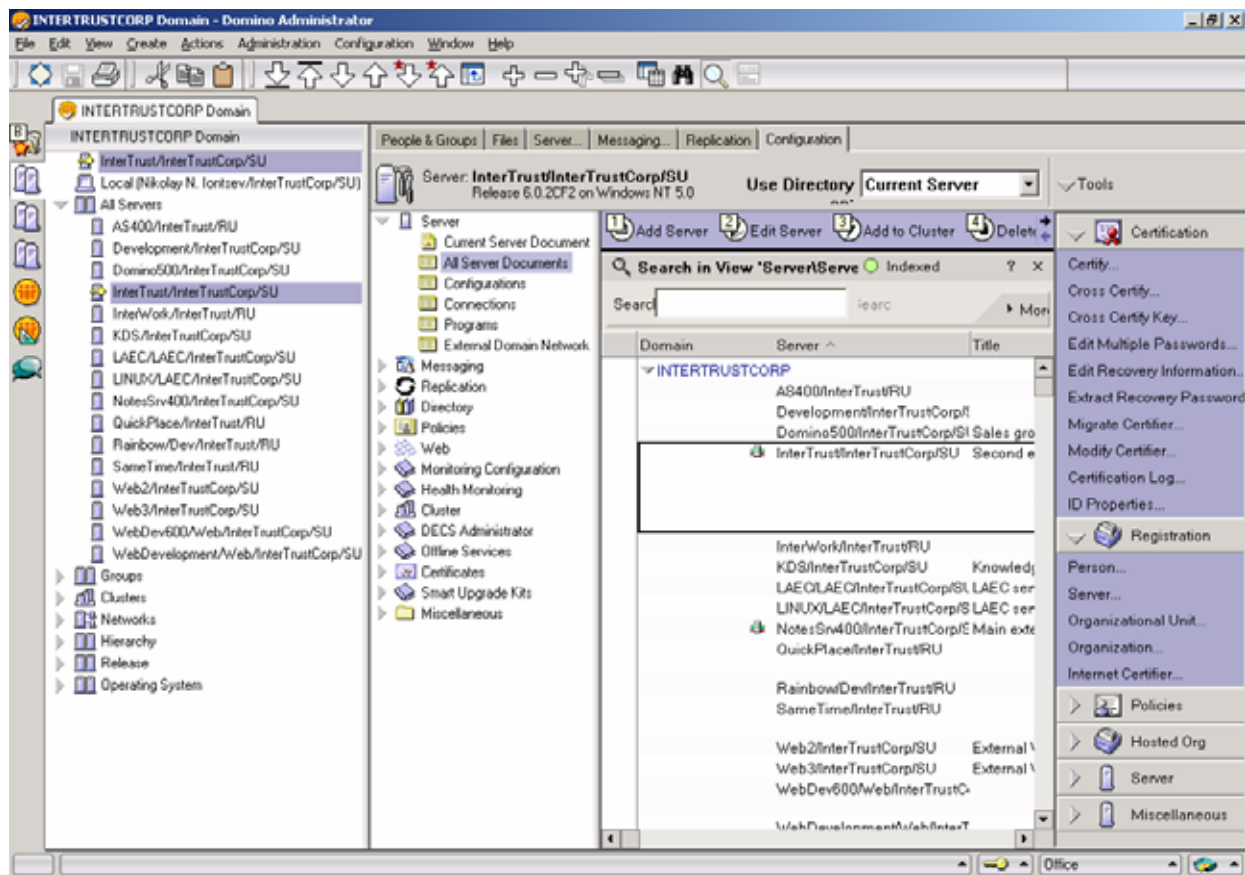


Рис. 152 Configuration – операции по конфигурированию серверов домена

1.22.2. 1.1.2. Свойства (Preferences) клиента администратора

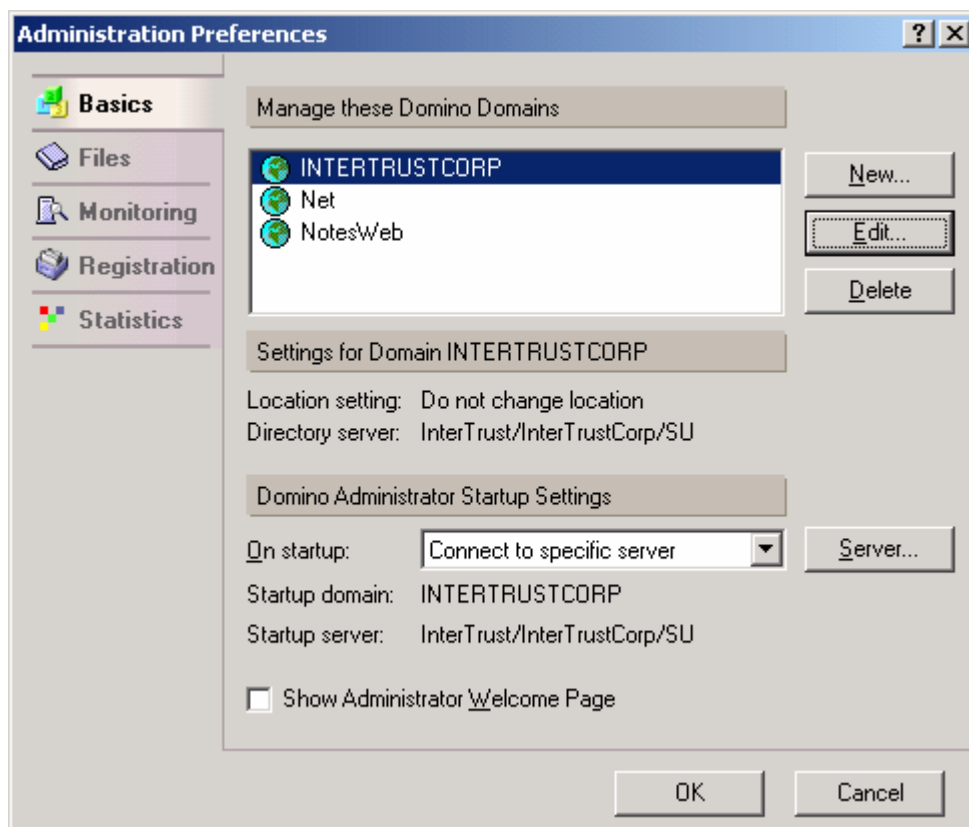


Рис. 153 Edit – сервер, с которого клиент администратора получает информацию о домене

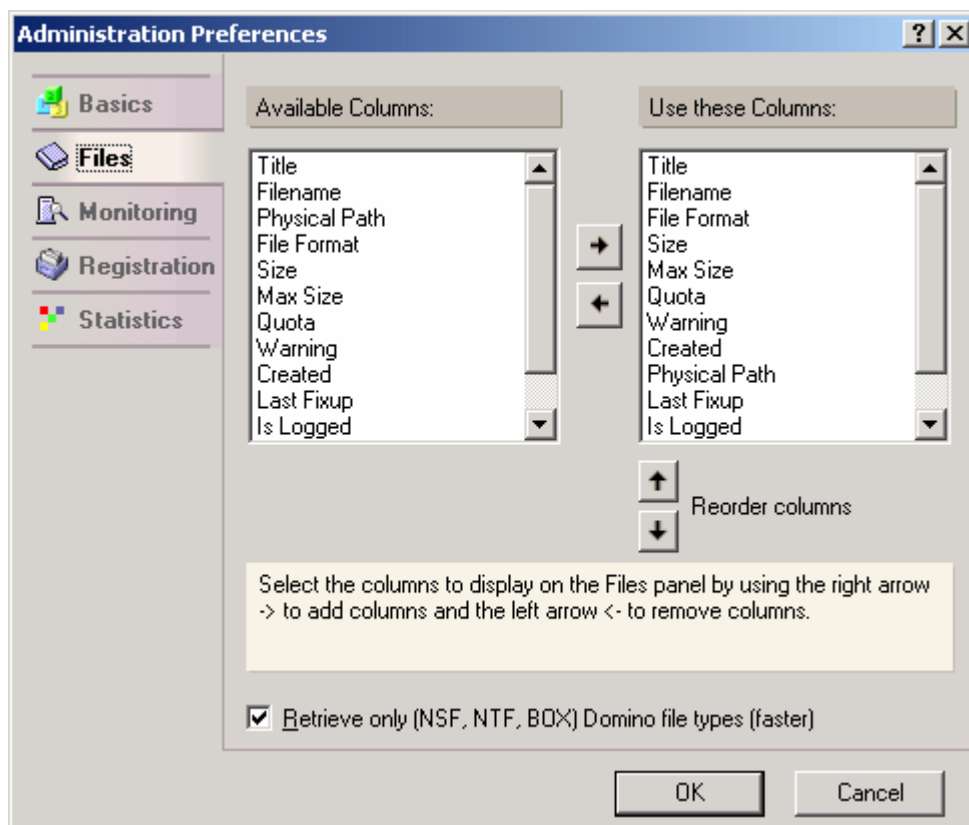


Рис. 154 Набор и порядок следования колонок на закладке Files

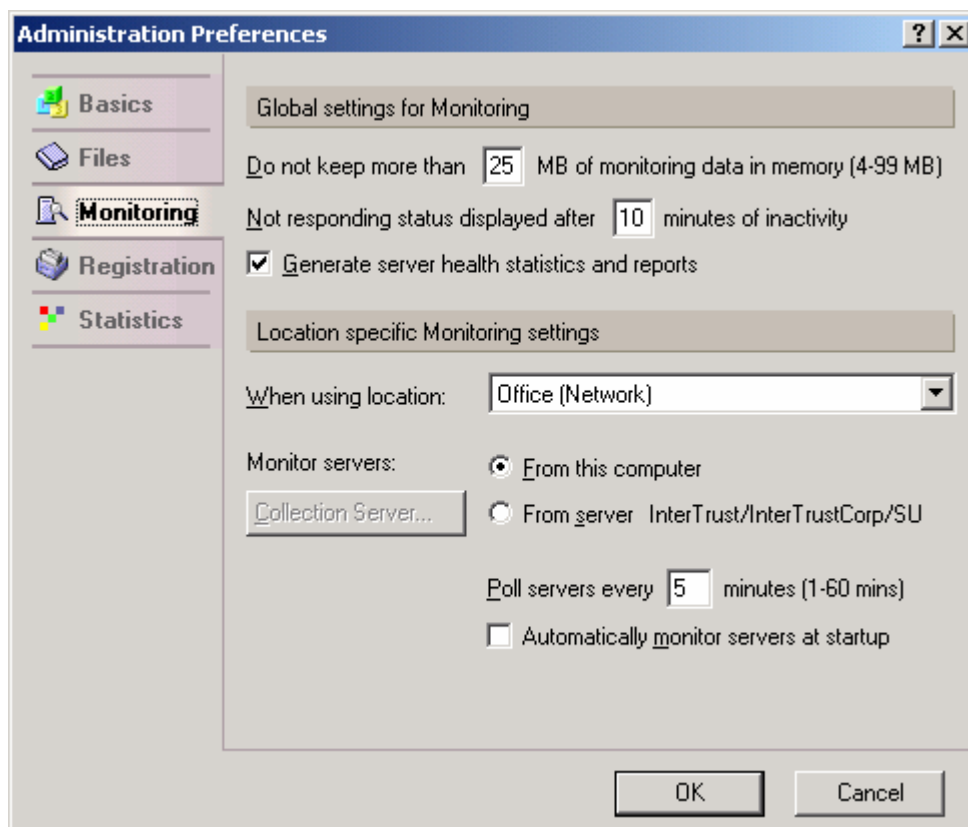


Рис. 155 Выберите флаг *Generate server health statistics and reports* – клиент будет вычислять «показатели здоровья» серверов. Частота опроса в поле *Pull servers every* в 1 минуту «очень жесткая» - клиент может не успевать «опросить» несколько серверов за минуту

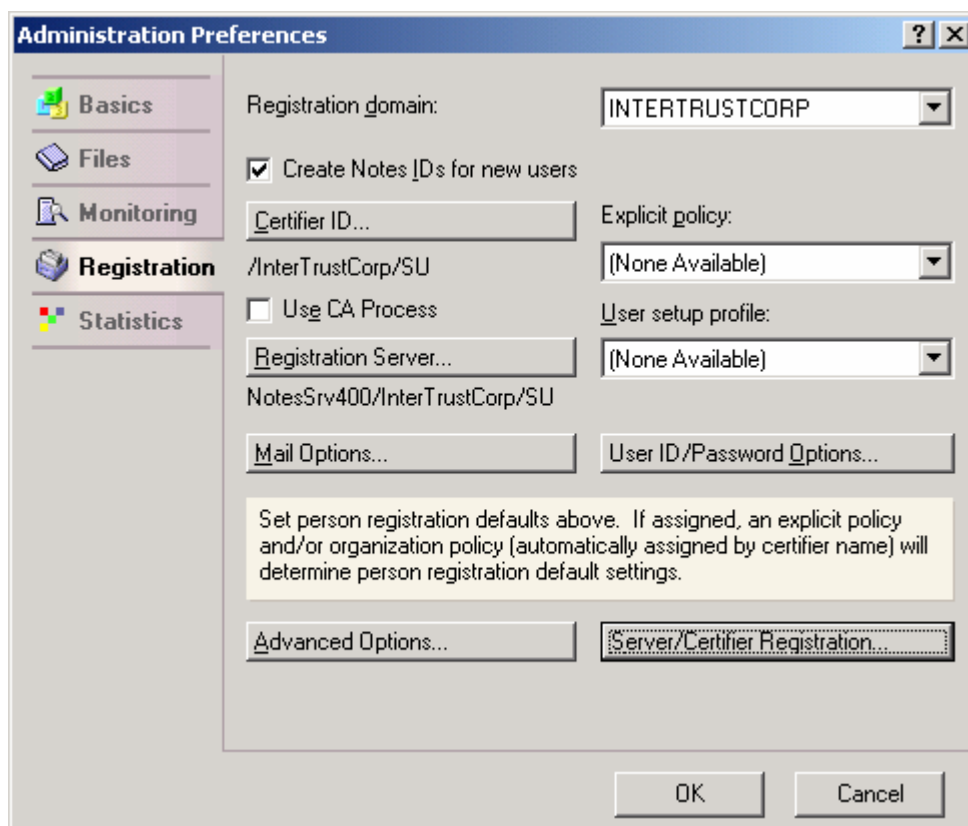


Рис. 156 Здесь можно задать множество «значений по умолчанию» для регистрации

1.23. 1.1. Использование Domino Web Administrator для администрирования серверов броузером

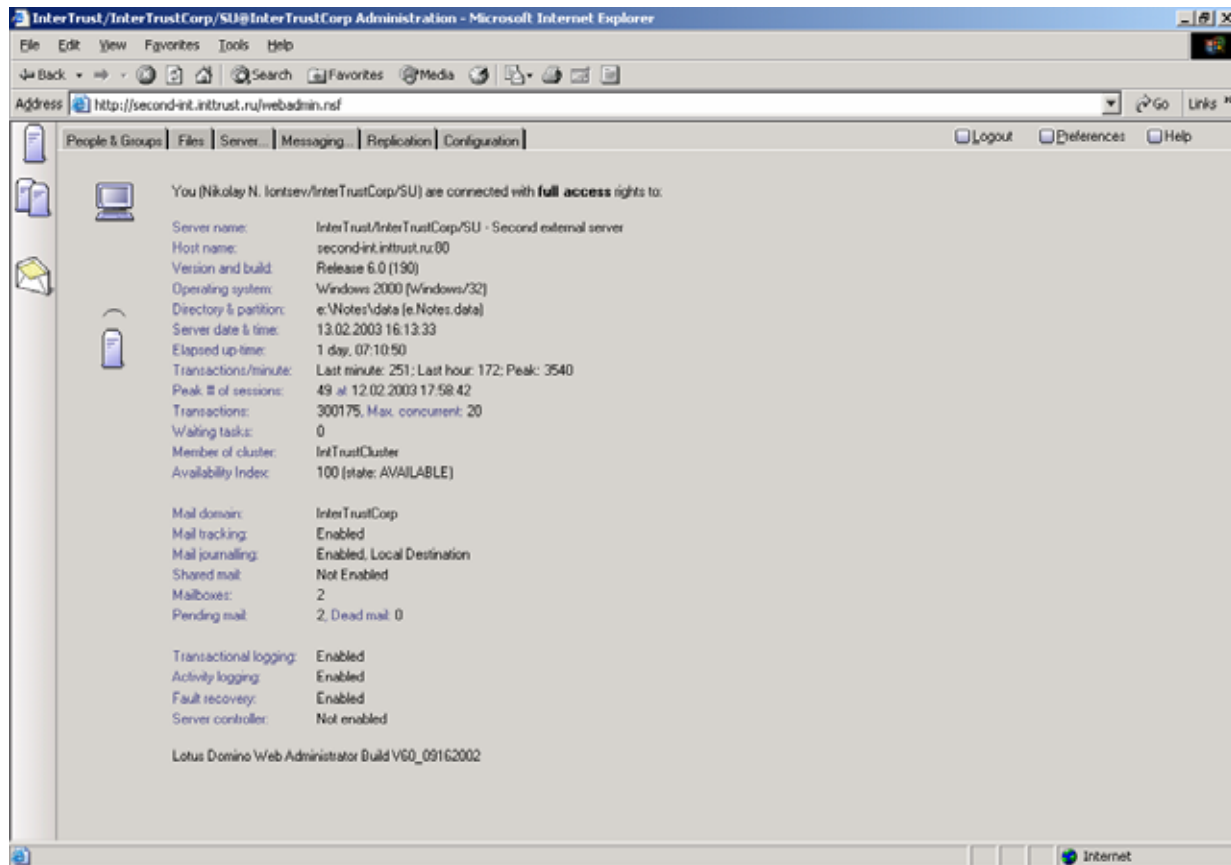


Рис. 157 Начало работы – [http\[s\]://host/webadmin.nsf](http[s]://host/webadmin.nsf)

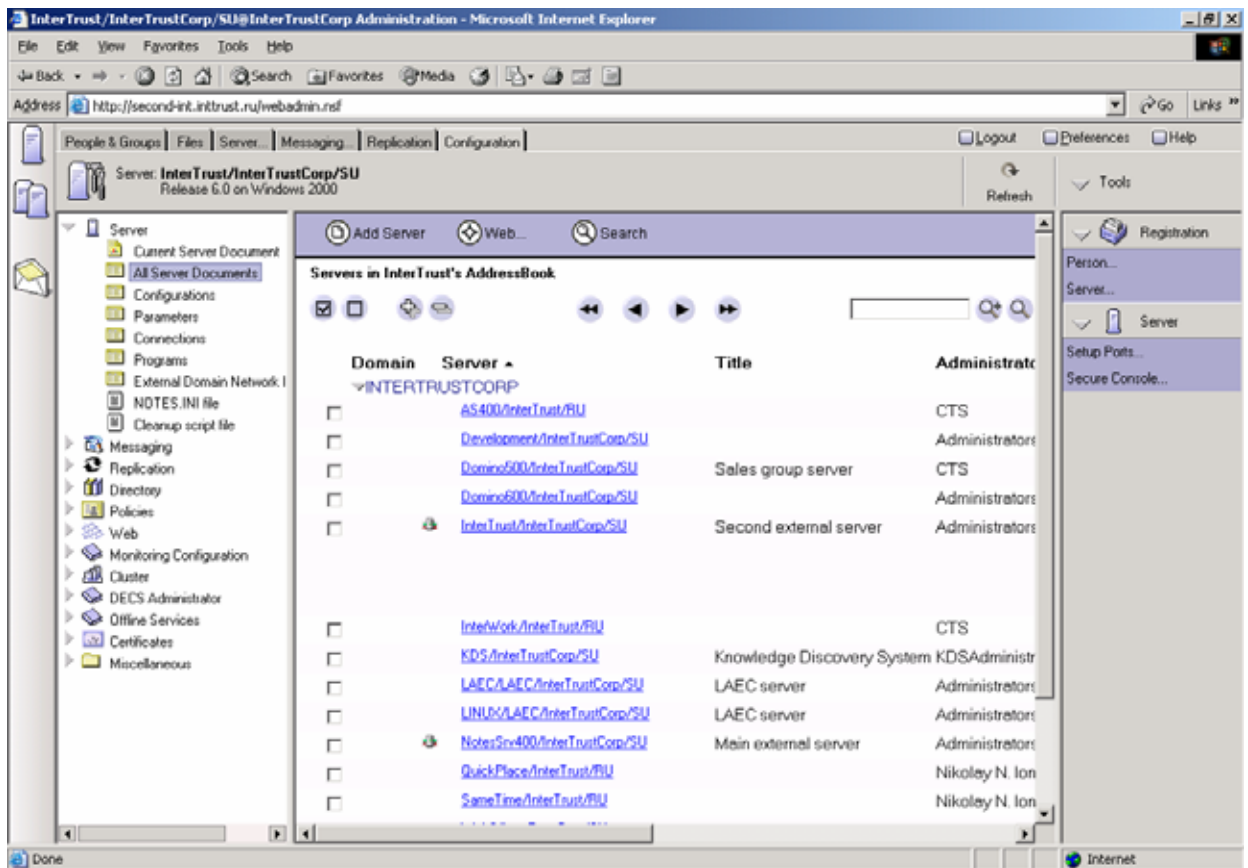


Рис. 158 Закладка Configuration

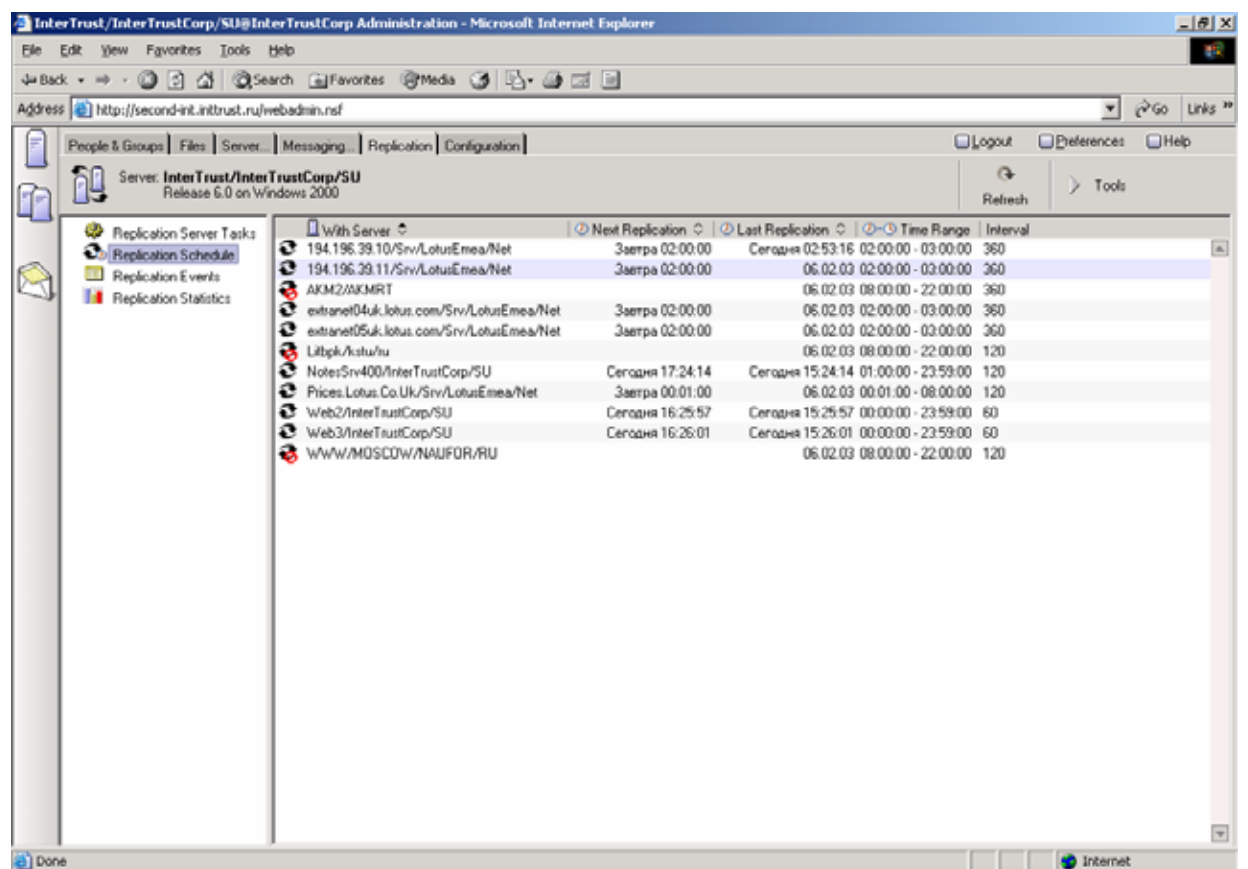


Рис. 159 Закладка Replication

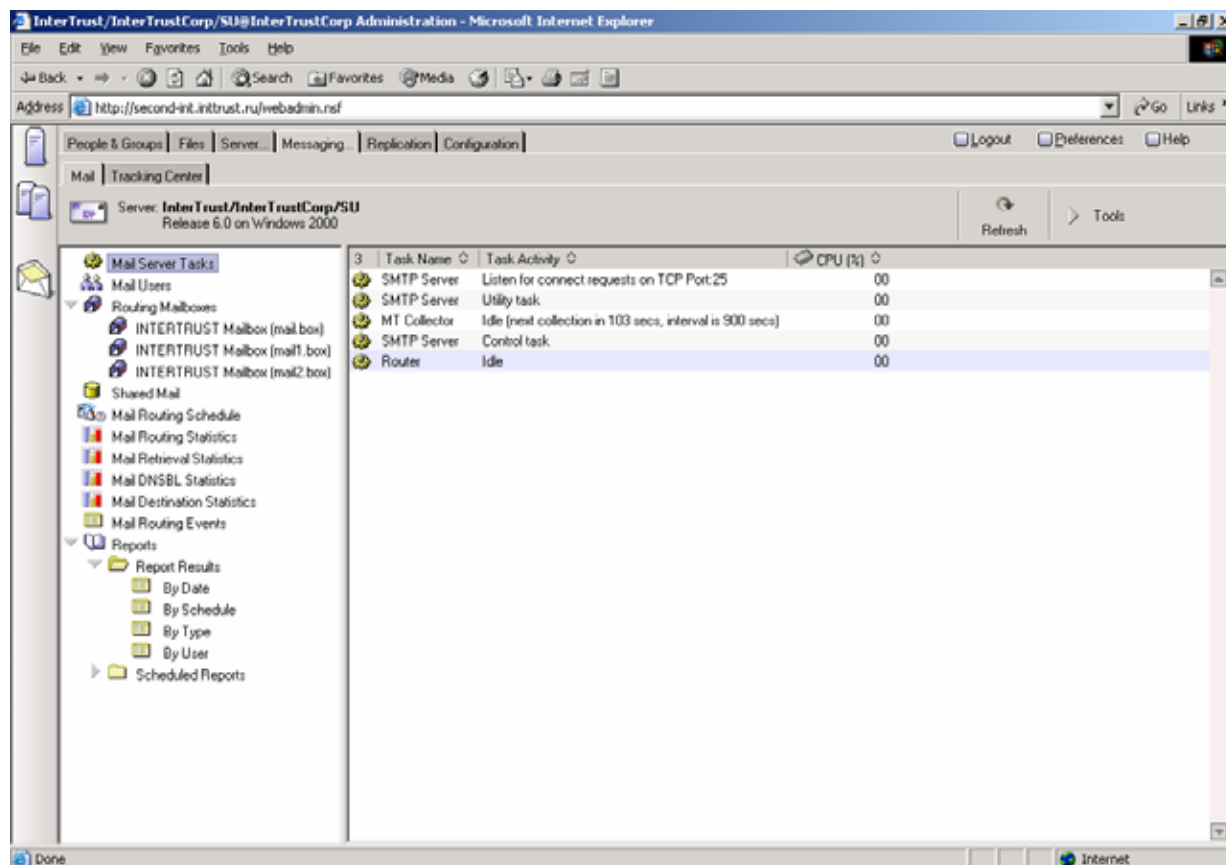


Рис. 160 Закладка Messaging

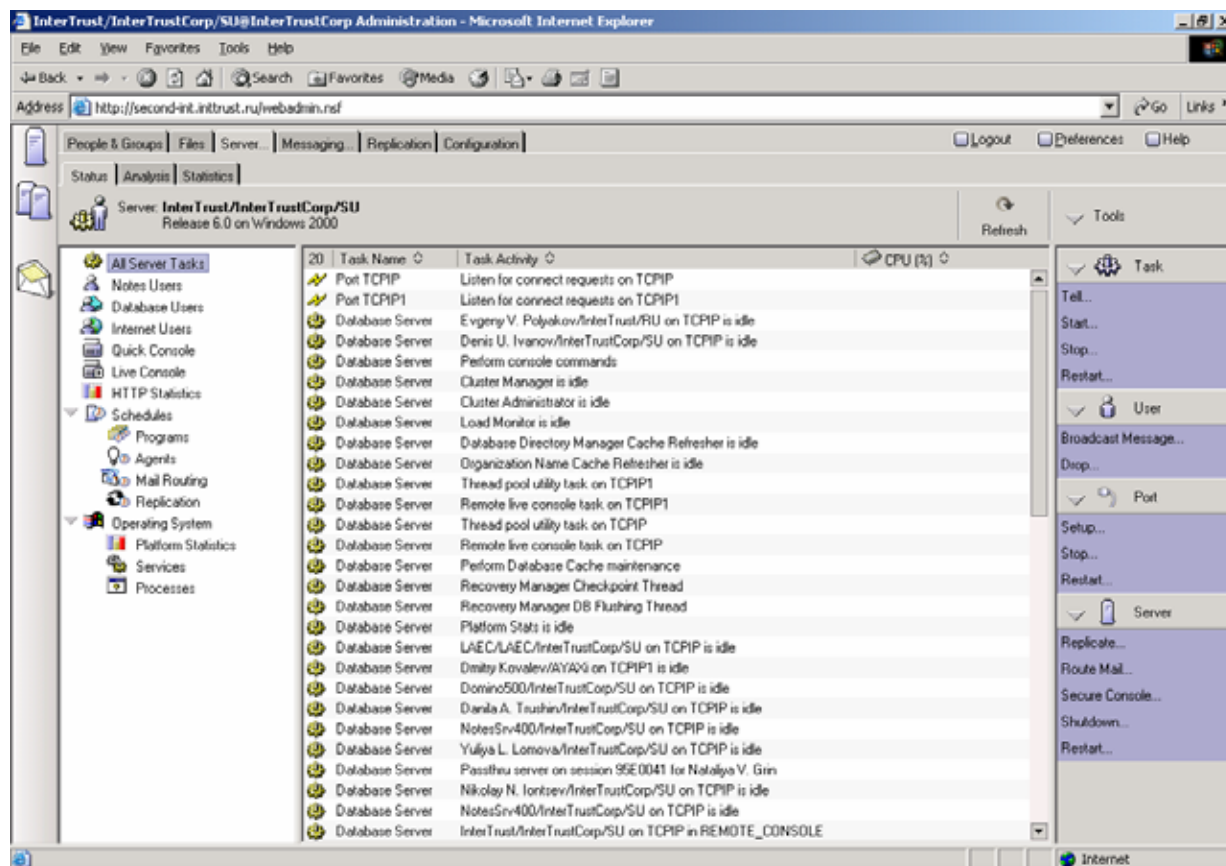


Рис. 161 Закладка Server

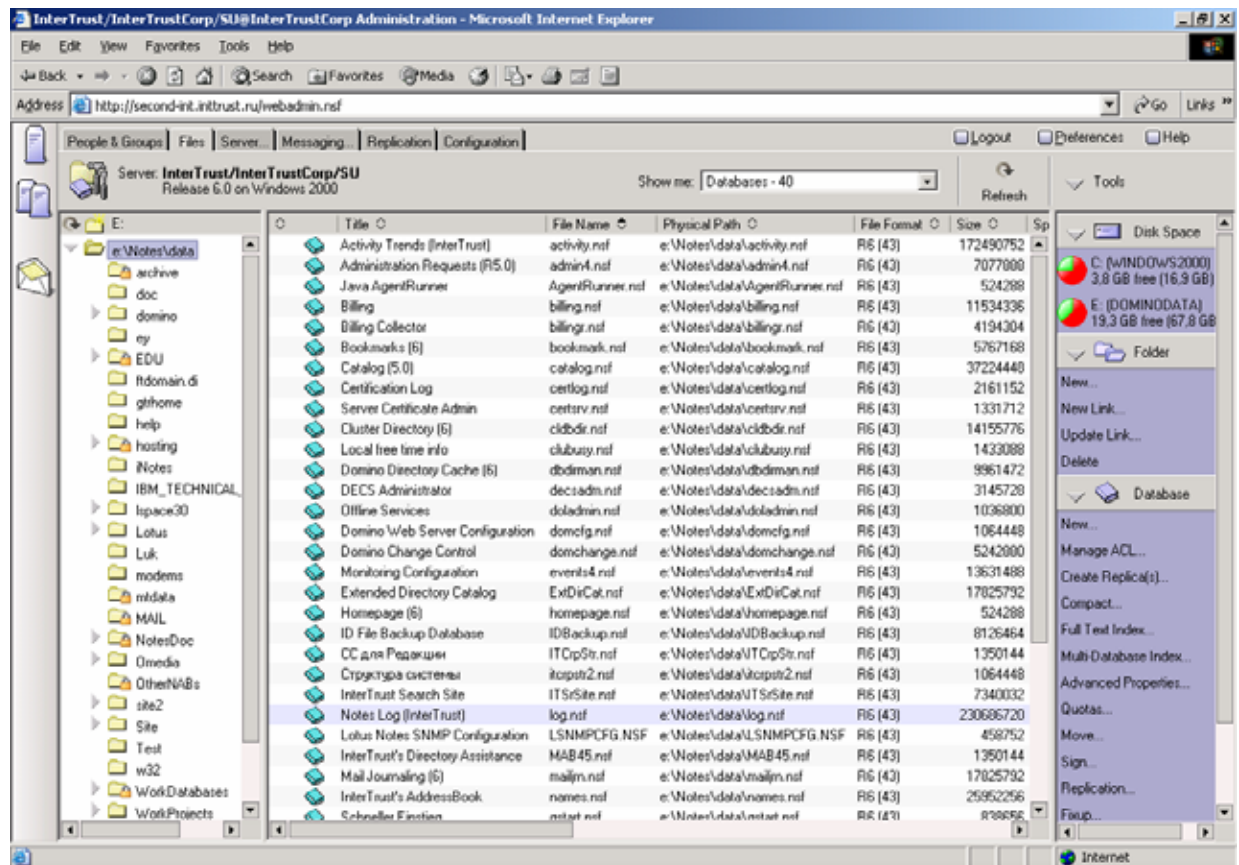


Рис. 162 Закладка Files

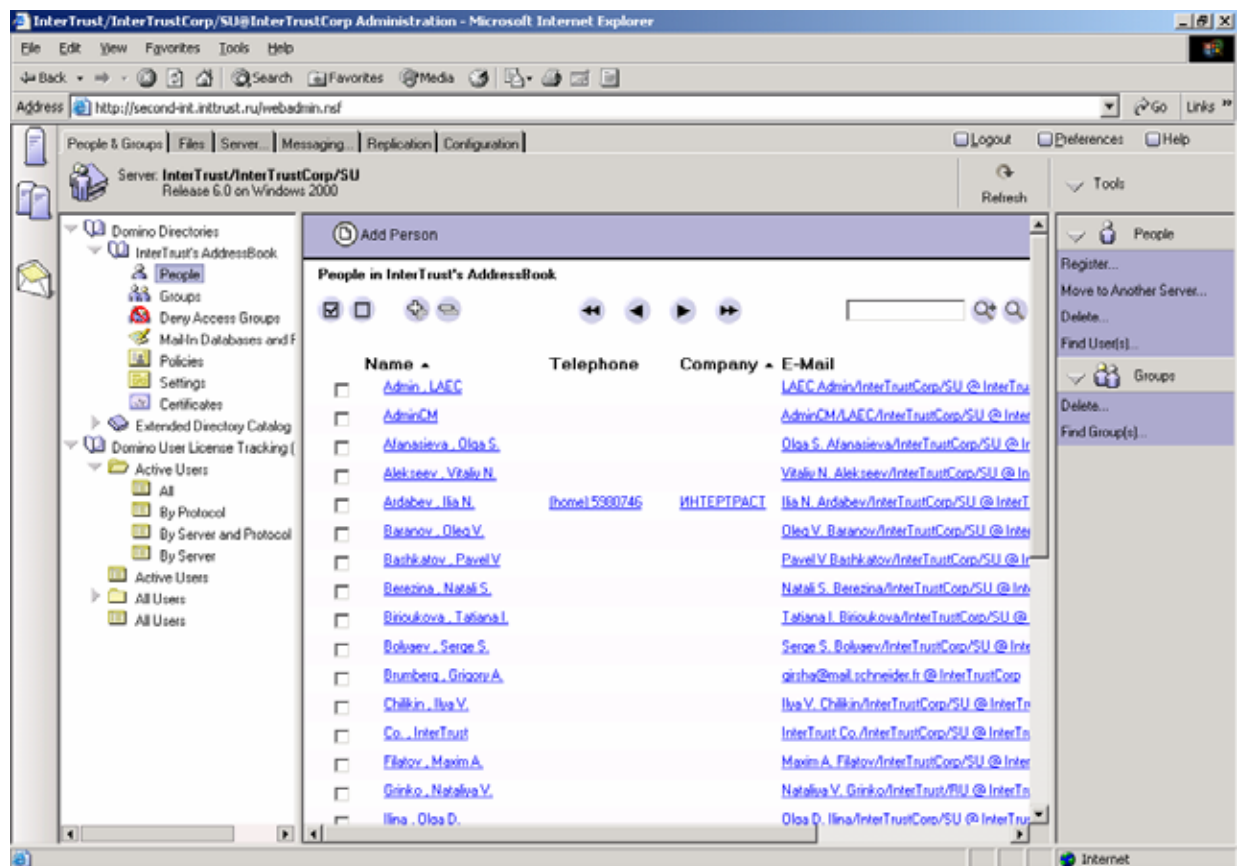


Рис. 163 Закладка People & Group

1.24. 1.1. Использование Domino Controller и Domino Console

- • Позволяют управлять сервером Domino, включая его перезапуск и выдачу команд операционной системы
- • Написаны на Java

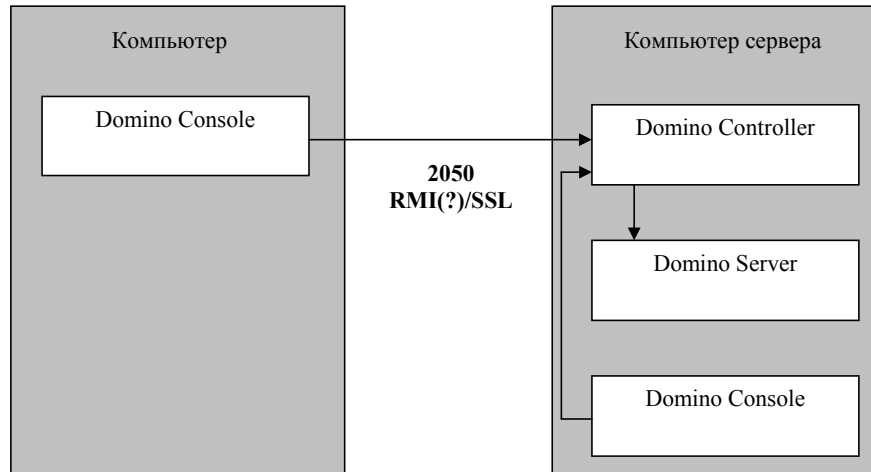


Рис. 164 Логика работы

1.24.1. 1.1.1. Domino Controller

- • Функционирует на компьютере сервера Domino, даже когда сам сервер Domino остановлен
- • Запускается командой **nserver -jc -c**
- • Затем автоматически запускает сервер Domino
- • «Слушает» порт 2050 в ожидании обращений от Domino Console

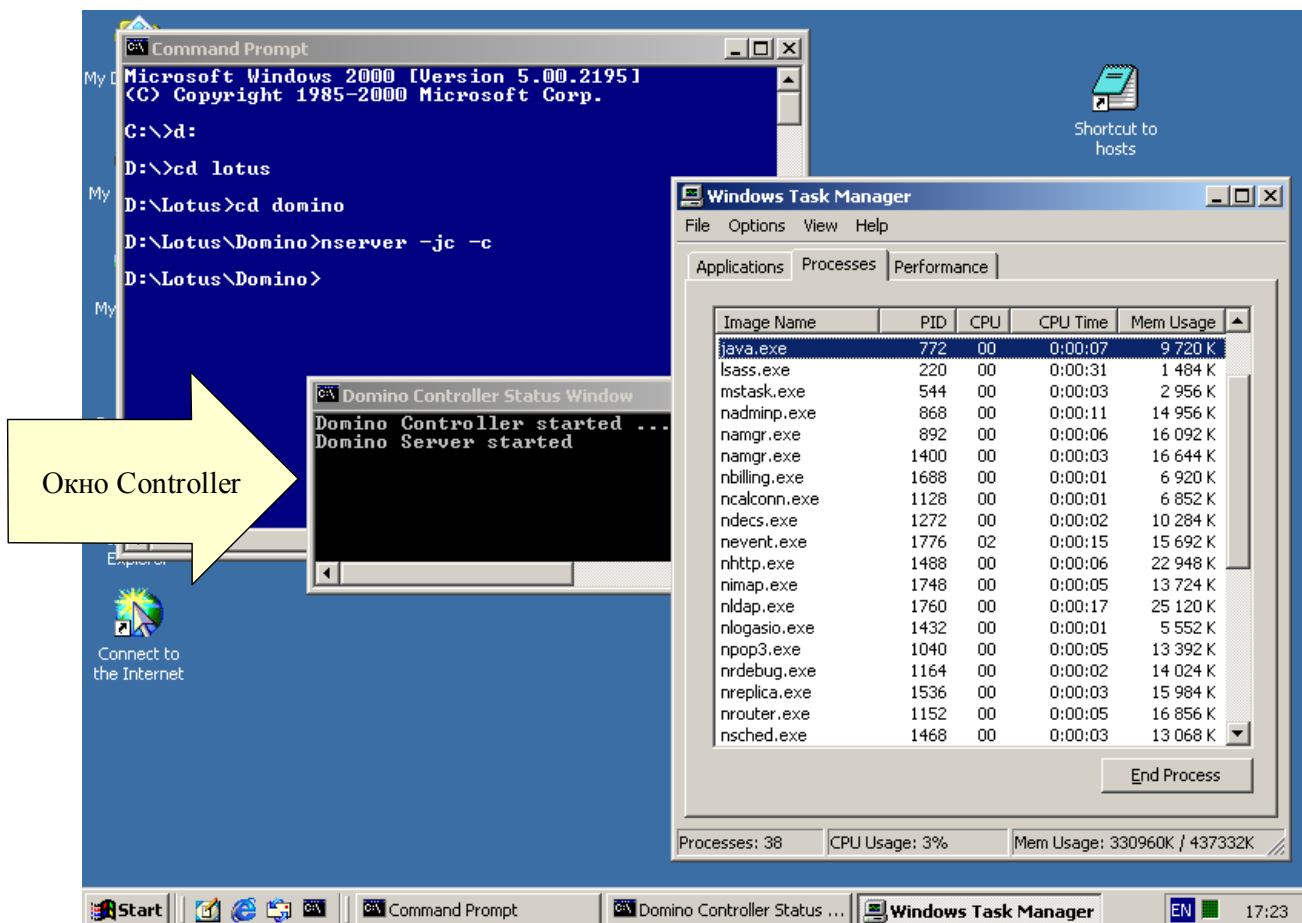


Рис. 165 Контроллер запустил сервер без «привычной» консоли

Все ключи

Ключи	Запускается
nserver -jc	Controller, server и Domino Console
nserver -jc -c	Controller и server
nserver -jc -s	Controller и Domino Console
nserver -jc -c -s	Только Controller

1.24.2. 1.1.2. Domino Console

- • Функционирует на любом компьютере, поддерживающем Java
- • «Дистрибутив»: dconsole.jar, jconsole.exe (NT/W2K) или jconsole (UNIX), каталог jvm
- • Запускается командой **jconsole**
- • Работает с Controller по порту 2050 (SSL)

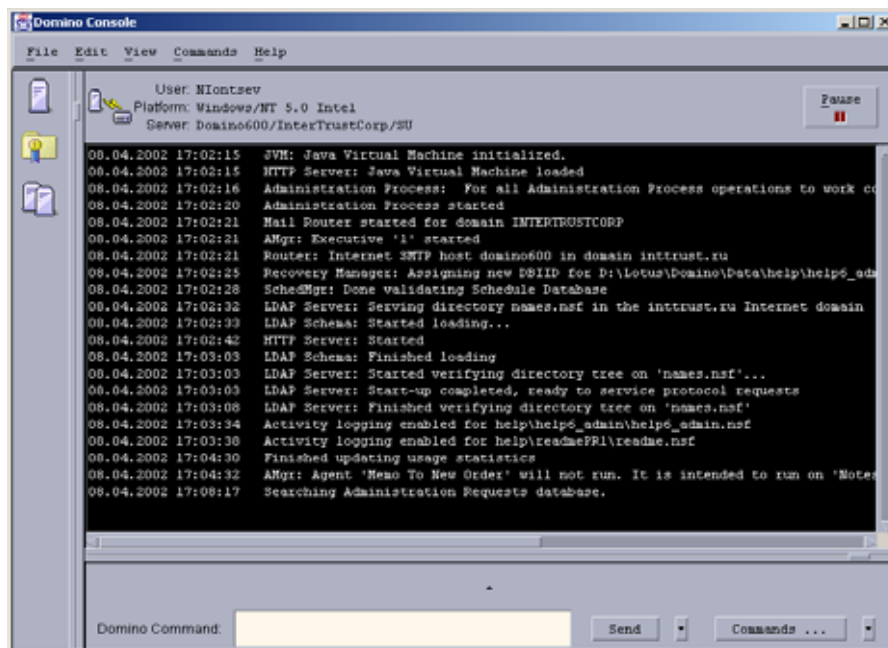


Рис. 166 Консоль сервера в jconsole

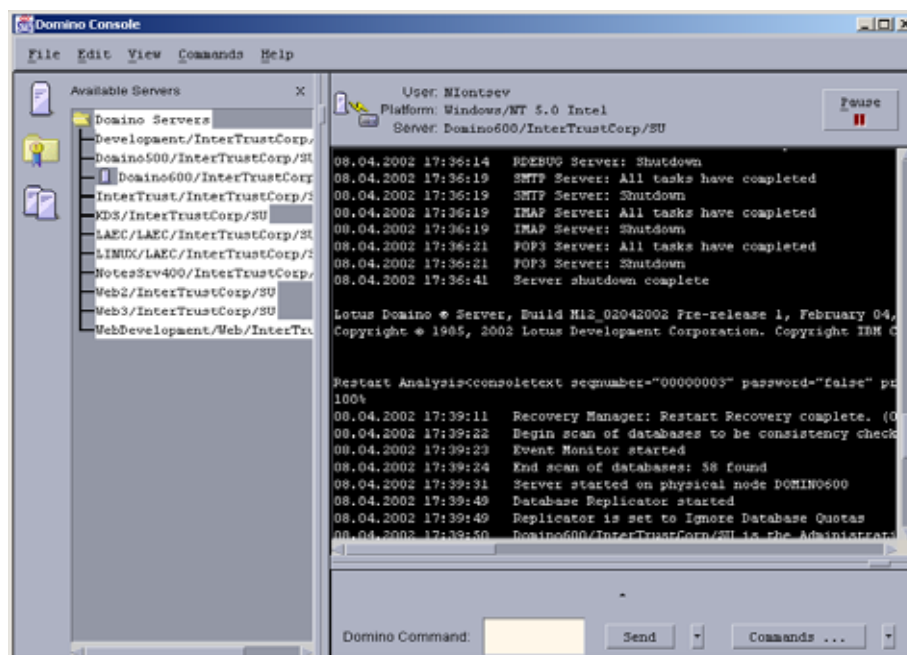


Рис. 167 Момент перезапуска сервера в jconsole

- Команда, посылаемая операционной системе, имеет формат **\$ команда**, например: **\$ dir *.***
- Правом посылать команды операционной системе обладают Full Access administrator, System Administrator и Restricted System Administrator (последний только Restricted System Commands)

1.25. 1.1. Документы Group и использование групп

Multi-purpose group: Developers

Basics | Comments | Administration

Basics

Group name:	『 Developers 』
Group type:	『 Multi-purpose 』
Category:	『 』
Description:	『 Company\Разработчики из компании ИнтерТраст 』
Mail Domain:	『 』
Internet Address:	『 』
Members:	『 Administrators Alexander M. Savelyew/InterTrustCorp/SU Alexey S. Telekovsky/InterTrustCorp/SU Andrey O. Kadnikow/InterTrustCorp/SU Denis U. Ivanov/InterTrustCorp/SU Ekaterina P. Loginova/InterTrustCorp/SU Evgeny V. Polyakov/InterTrust/RU

Group type description

'Multi-purpose' groups are the default group type and used in most situations. They can be used for access control and email purposes.

Рис. 167 Документ Group

Типы групп:

- • **Multi-purpose** – многоцелевая (для любых применений).
- • **Access Control List only** – только для решения вопросов доступа к серверу и базе.
- • **Mail only** – список адресов (для рассылки).
- • **Servers only** – для использования в документах Connection и в клиенте Администратора для группировки серверов.
- • **Deny List only** – для запрета доступа к серверу или порту. Administration Process не удаляет членов из групп этого типа.

Ограничения (взяты из Admin Help 6, но вызывают сомнение – по сведениям из KB еще в R5 максимальное количество уровней вложенности групп было увеличено до 20):

- • Максимальная длина имени 62 символа
- • Допустимые символы: A - Z, 0 - 9, & - . _ ' / (ampersand, dash, period, space, underscore, apostrophe и forward slash)
- • При передаче почты 5 уровней вложенности, для остальных целей – 6 уровней.

В группы должны добавляться полные имена субъектов – в точности как первый элемент из поля-списка User name в документе Person.

Количество элементов в поле Members ограничено максимальным размером поля типа текстовой список с флагом Summary (не более 32K в 6.x и не более 15K в предшествующих версиях). На практике это ограничение обходится использованием вложенных групп.

1.25.1. 1.1.1. Закладка People & Groups, окно Groups – Manage

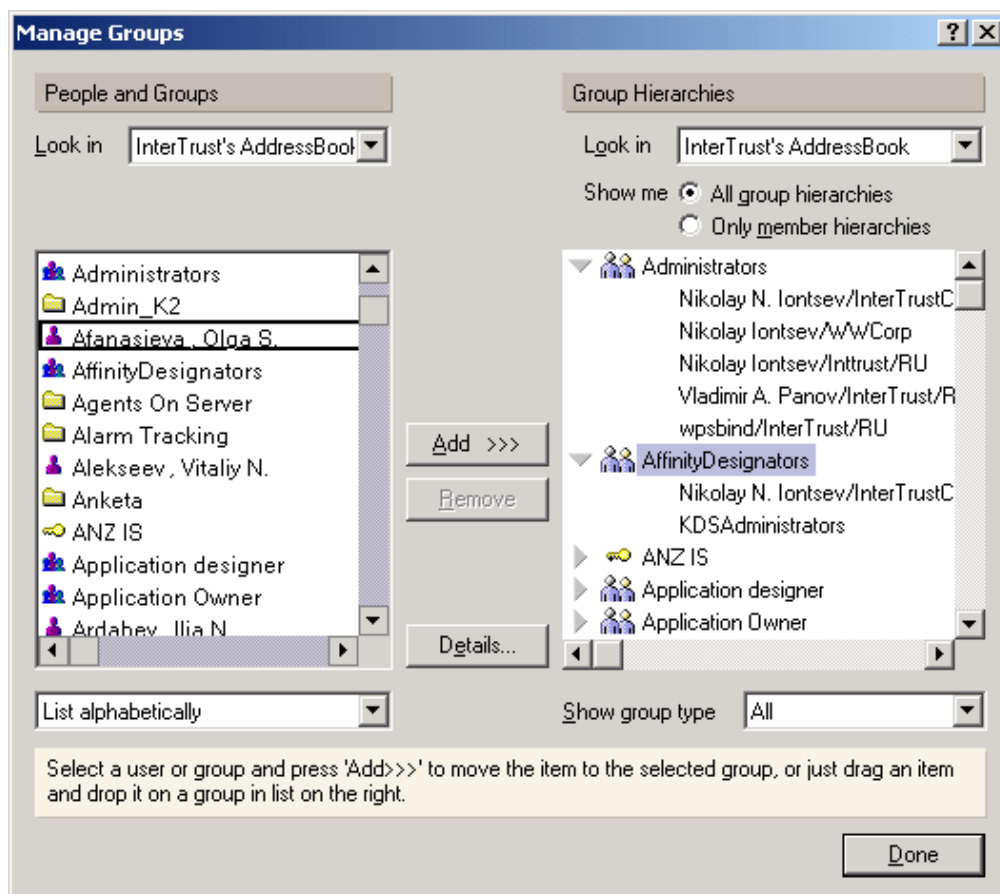


Рис. 168 «Режим» All group hierarchies

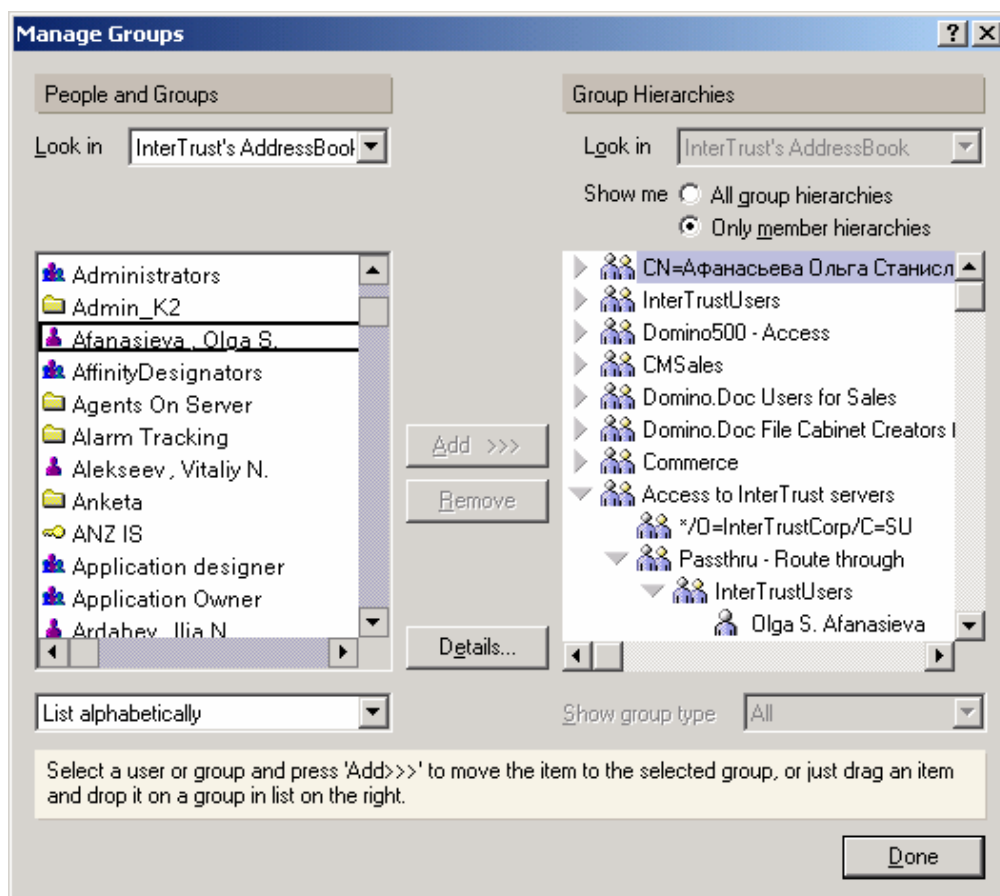


Рис. 169 «Режим» Only member hierarchies

1.26. 1.1. Управление доступом к серверу в документе Server

Server : InterTrust/InterTrustCorp/SU			
Basics Security Ports Server Tasks Internet Protocols MTAs Miscellaneous Transactional Logging Shared Mail Administration			
Administrators		Programmability Restrictions	Who can -
Full Access administrators:	Administrators	Run unrestricted methods and operations:	InterTrust - Run unrestricted agents, InterTrust/InterTrustCorp/SU, Sametime Development/Lotus Notes Companion Products Administrators, Lotus Notes Template Development/Lotus Notes
Administrators:	Administrators, InterTrust/InterTrustCorp/SU	Sign agents to run on behalf of someone else:	
Database Administrators:		Sign agents to run on behalf of the invoker of the agent:	
Full Remote Console Administrators:	Administrators	Run restricted LotusScript/Java agents:	InterTrust - Run restricted agents
View-only Administrators:		Run Simple and Formula agents:	InterTrust - Run personal agents
System Administrator:	Administrators	Sign script libraries to run on behalf of someone else:	
Restricted System Administrator:		Note: The following settings are obsolete in Notes 6. They are used for compatibility with prior versions.	
Restricted System Commands:		Run restricted Java/Javascript/COM:	
Administer the server from a browser (pre-Notes 6 servers only):	Administrators	Run unrestricted Java/Javascript/COM:	
Security Settings		Internet Access	
Compare Notes public keys against those stored in Directory:	☐ Yes ☒ No	Internet authentication:	Fewer name variations with higher security
Allow anonymous Notes connections:	☐ Yes ☒ No		
Check passwords on	☒ Enabled ☐ Disabled		
Notes IDs:			
Server Access	Who can -	Passthru Use	Who can -
Access server:	☐ users listed in all trusted directories and Access to InterTrust servers	Access this server:	*/
Not access server:	Terminations	Route through:	Passthru - Route through
Create databases & templates:	InterTrustUsers, LocalDomainServers	Cause calling:	Passthru - Cause calling
Create new replicas:	InterTrust - Replica makers	Destinations allowed:	
Create master templates:	InterTrustUsers, LocalDomainServers		
Allowed to use monitors:	Administrators, InterTrustUsers		
Not allowed to use monitors:			
Trusted servers:	NotesSrv400/InterTrustCorp/SU		

Рис. 170 Закладка Security документа Server

Доступ к серверу определяют четыре фактора: успешное выполнение процедуры аутентификации, сравнение открытого ключа со значением из Каталога Domino сервера, проверка пароля и список управления доступом к серверу.

1. Процедура аутентификации. Если в поле Allow anonymous Notes connections выбрано No, сервер и обращающийся к нему субъект (оба с иерархическими именами) должны иметь сертификат-компоненту от общего сертификатора или взаимные сертификаты. Если ни первое, ни второе не выполняются, в доступе будет отказано и

будет получено сообщение «The server's Domino Directory does not contain any cross certificates capable of authenticating you».

Однако выбором Yes в поле Allow anonymous Notes connections документа Server можно разрешить доступ к серверу любым серверам и клиентам, даже если для них процедура аутентификации завершилась неуспешно. Такой клиент получает доступ к серверу под именем Anonymous.

2. Сравнение открытого ключа со значением из Каталога Domino сервера. Если в документе Server в поле Compare Notes public keys... выбрано Yes, открытый ключ обращающегося к серверу, «уверенно определенный» сервером в ходе процедуры аутентификации, сравнивается со значением открытого ключа этого субъекта из документа Server или Person в Каталоге Domino сервера. При несовпадении ключей попытка доступа отвергается. Такая возможность предотвращает доступ к серверу лиц, «похитивших» ID-файл клиента и знающих его пароль, после того, как «обнаруживший факт хищения» клиент сменит открытый (и, одновременно, секретный) ключ в своем ID-файле. Факт же отсутствия соответствующего документа Server или Person в Каталоге Domino сервера не позволяет провести проверку и тоже влечет отказ в доступе.

3. Проверка пароля. Обеспечивает сравнение хэша пароля ID-файла обращающегося к серверу пользователя с хэшем пароля, хранящимся в документе Person в Каталоге Domino сервера. При несовпадении хэшей попытка доступа отвергается. Проверка паролей должна быть включена в документе Server в поле Check password... и в документе Person (явно или посредством политики).

4. Список управления доступом к серверу. Если в доступе к серверу было отказано и получено сообщение «Server Error: You are not authorized to access the server», это означает, что три предыдущих проверки завершились успехом, однако доступ явно запрещен в т.н. списке управления доступом к серверу.

Под списком управления доступом к серверу подразумевается поля Access server и Not access server из группы полей Server Access документа Server или перечисляемый ниже набор переменных из файла NOTES.INI сервера.

Поле Access server может содержать список имен, групп или шаблонов имен тех, кому разрешен доступ к серверу, а поле Not access server - список тех, кому доступ запрещен. Если оба поля Access server и Not access server пусты, любой прошедший три предыдущих проверки получает доступ к серверу. Если поле Access server не пусто, субъект должен входить в содержащийся в поле список, но не входить в список, содержащийся в поле Not access server, если последнее не пусто.

«Галочка» в поле users listed in all trusted directories разрешает доступ к серверу только пользователей из Каталога Domino и других доступных серверу через Directory Assistance каталогов, имеющих в соответствующем документе из Directory Assistance «пометку» Trusted. Заметьте, что в это множество входят только пользователи, но не серверы, поэтому для обеспечения доступа серверов обычно нужно добавлять в следующее поле группу LocalDomainServers.

Кроме того, в файле NOTES.INI могут задаваться переменные, регулирующие доступ к серверу через его конкретный порт.

- ● **Allow_Access_<имя порта>** - список имеющих доступ к серверу через его порт <имя порта>. Например, Allow_Access_COM1 может задавать список тех, кто имеет доступ к серверу через порт COM1.
- ● **Deny_Access_<имя порта>** - список тех, кому запрещен доступ к серверу через его порт <имя порта>.

Наконец, при доступе к серверу через сервер-посредник «начинают работать» поля Access this server:, Route through, Cause calling и Destinations allowed из группы полей Passthru use документа Server.

1.26.1. 1.1.1. Активизация изменений в полях, отвечающих за доступ к серверу

В полях, управляющих доступом к серверу, надо использовать группы. При изменении информации в полях необходим перезапуск сервера. Изменение же состава групп не требует перезапуска сервера.

1.26.2. 1.1.2. Устранение проблем доступа к серверу

- • **The server's Domino Directory does not contain any cross certificates capable of authenticating you** – обеспечить нужные взаимные сертификаты в каталоге Domino сервера или NAMES.NSF пользователя.
- • **You are not authorized to use the server** – добавить в группу, обеспечивающую доступ и удалить из группы, закрывающей доступ.
- • **Your public key was not found in the Name and Address Book** – выбрано сравнение открытого ключа, но в NAMES.NSF не обеспечен документ на обращающегося с серверу пользователя или сервер. Встречается при репликациях между серверами: Connection A->B типа Pull-Push, на А выбрано, на В – нет => В «сам себя не пускает» на А. Так же возможно сообщение о несовпадении ключей...
- • При «включенной» проверке пароля сообщение о несовпадении пароля пользовательского ID-файла или о том, что ID-файл «заблокирован» – проблема устраняется в документе Person на закладке Administration: поле Password digest «очищают», и, если надо, поле Check password изменяют.

1.27. 1.1. Управление доступом к каталогам с помощью Directory Links и Directory ACLs

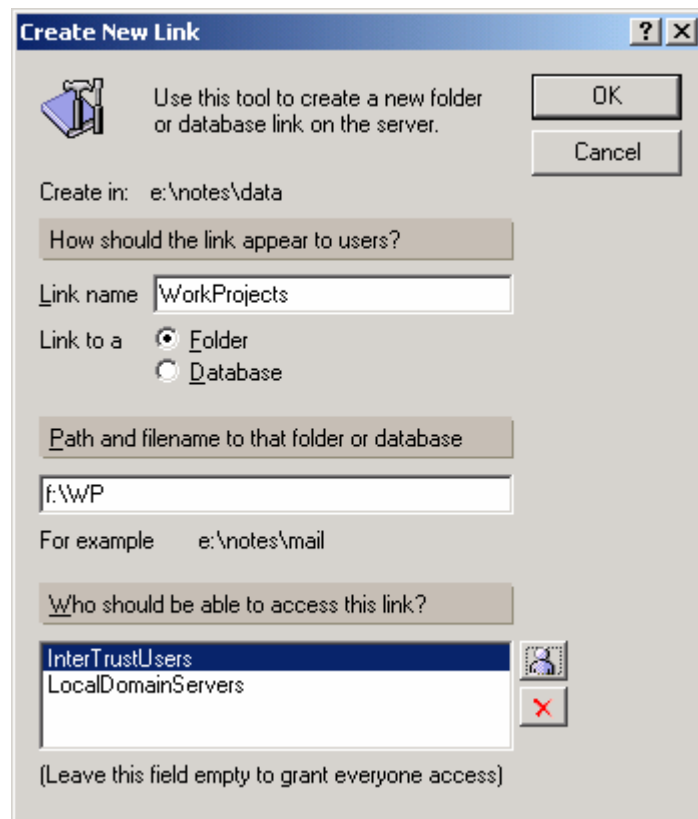


Рис. 171 Directory Link

Directory Link должен «ссылаться» на каталог ВНЕ каталога data. Сохраняется в файле <link name>.DIR. Не скрывает каталог, но ограничивает доступ к нему.

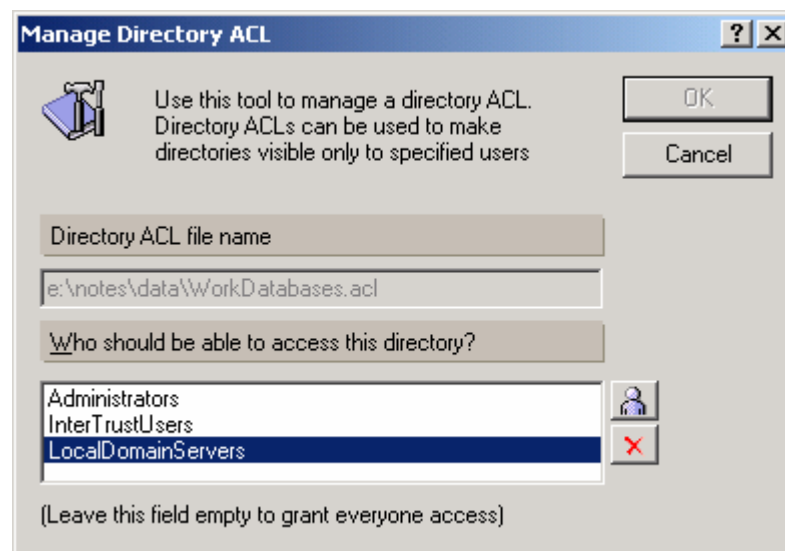


Рис. 172 Directory ACL

Directory ACL применяется к каталогу в data. Сохраняется в файле <имя каталога>.ACL. На не-xSP-сервере нужно добавить **Enable_ACL_Files=1** в NOTES.INI. Скрывает каталог и ограничивает доступ к нему.

1.28. 1.1. Механика работы списка управления доступом базы (ACL)

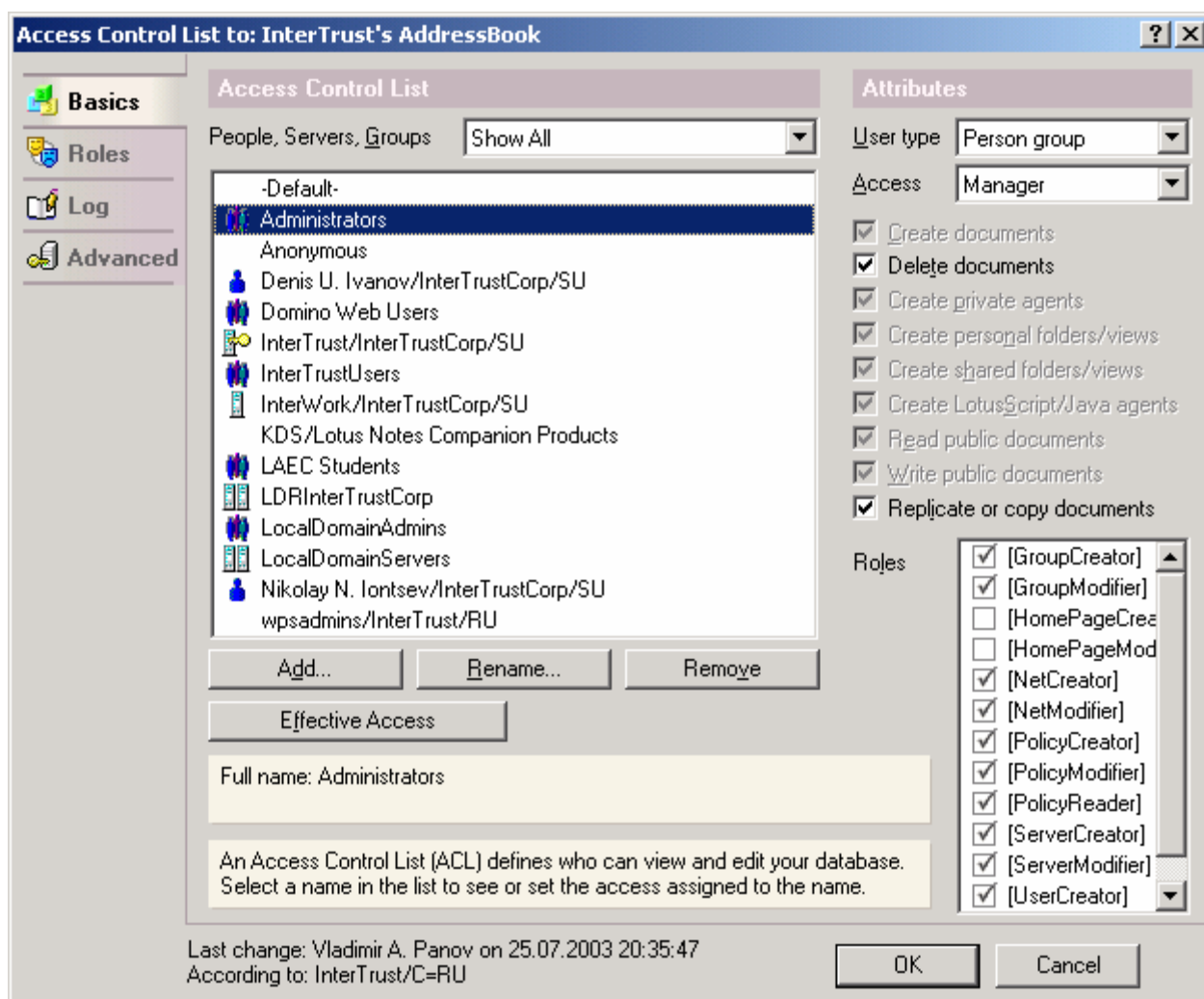


Рис. 173

Каждая база Notes имеет список управления доступом (Access Control List, ACL), определяющий, какие пользователи, группы пользователей, и серверы могут иметь к ней доступ и какие задачи в этой базе они могут исполнять.

ACL включает две составляющих:

- список элементов ACL, каждый из которых содержит имя субъекта (пользователя, сервера или группы), его уровень доступа к базе и дополнительные свойства;
- список ролей вместе с назначением субъектов на роли.

Используется семь **уровней доступа**.

 **Manager** (Менеджер) может выполнять все возможные действия в базе данных - чтение, запись, редактирование документов, создание, модификация и удаление элементов дизайна (форм, видов, агентов...). Менеджер, в отличие от более низких уровней доступа, может также изменять ACL, настройки репликаций, установки локального шифрования базы и удалять базу данных. База данных всегда имеет по крайней мере одного менеджера.

 **Designer** (Дизайнер), в отличие от более низких уровней доступа, может создавать, модифицировать и удалять элементы дизайна (поля, формы, виды, общих агентов...), модифицировать репликационные формулы базы, создавать индекс

полнотекстового поиска. И, конечно, выполнять те же самые действия, что и субъекты с более низким уровнем доступа

 **Editor** (Редактор) может читать, создавать и редактировать все документы в базе данных (в том числе и созданные другими пользователями), но не может изменить элементы дизайна, ACL и прочие атрибуты, присущие более высоким уровням доступа.

 **Author** (Автор) может читать существующие документы и создать новые, но может редактировать только документы, автором которых он является (поле типа Authors документа содержит имя этого субъекта).

 **Reader** (Читатель) может читать документы, но не может добавлять новые или редактировать существующие.

 **Depositor** (Депозитор) может добавлять новые документы, но не может читать существующие, потому что попросту «не видит» их в видах базы.

No Access (Нет доступа). Пользователь не может открыть базу данных.

Кроме того, для каждого уровня доступа имеется свой собственный набор дополнительных флагов, уточняющих возможности на уровне. Ниже приведены все возможные флаги, но без учета уровня доступа, для которого они имеют смысл:

- • Create documents – может создавать документы;
- • Delete documents – может удалять документы;
- • Create private agents – может создавать личных агентов;
- • Create personal folders/views – может создавать личные виды и папки;
- • Create shared folders/views – может создавать общие виды и папки;
- • Create LotusScript/Java Agents – может создавать агентов на LotusScript и Java;
- • Read public documents – может читать общедоступные документы;
- • Write public documents – может создавать общедоступные документы;
- • Replicate or copy documents (R6) – может реплицировать или копировать документы.

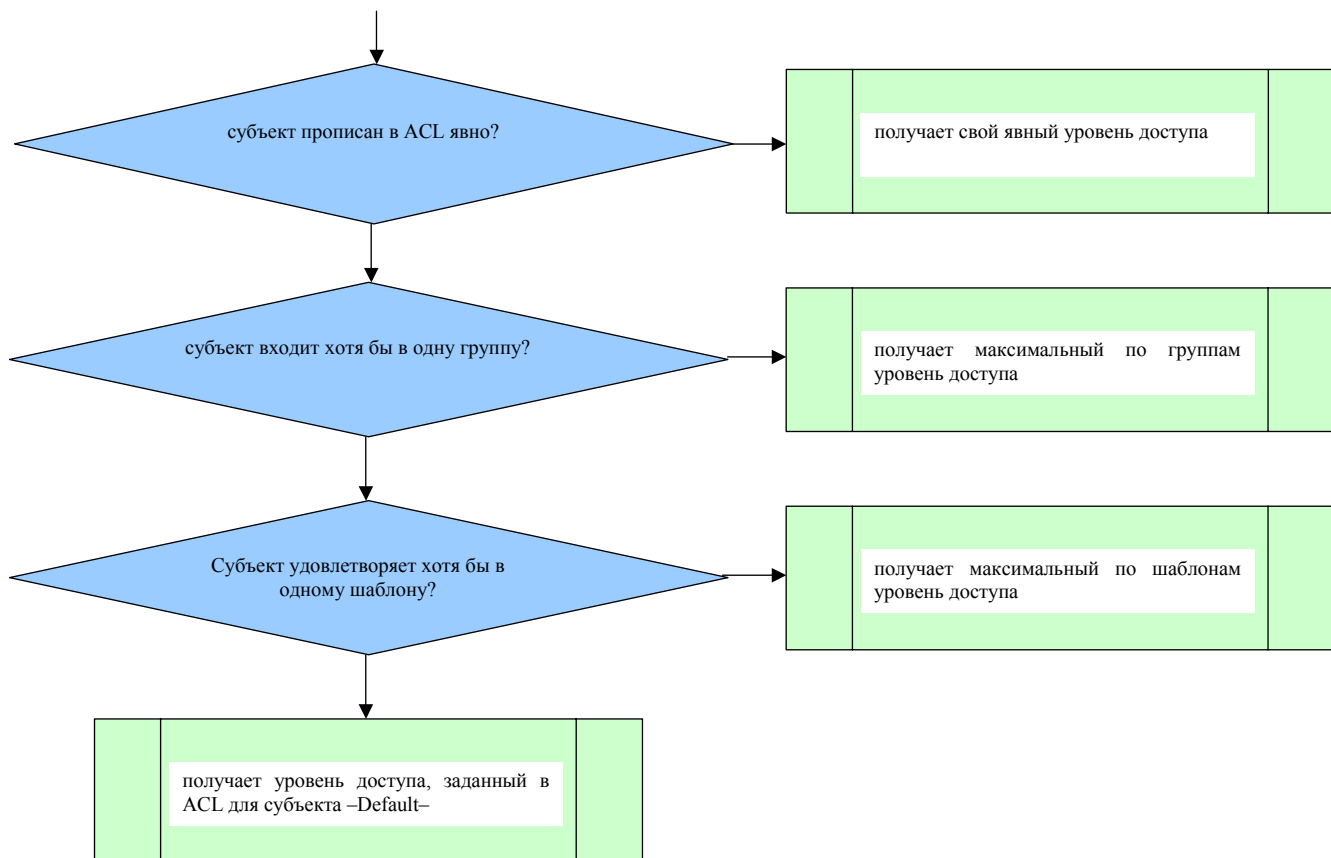


Рис. 174 Логика работы ACL

Роли доступа используются для управления доступом пользователей или групп к определенным формам, видам или агентам в базе данных.

Дизайнер может предусмотреть при создании некоторых форм, видов или агентов, что доступ к ним должны иметь только те лица, которых впоследствии менеджер базы назначит на эту роль, а не все имеющие необходимый уровень доступа в ACL. Дизайнер (обычно при разработке базы он имеет и права менеджера) добавляет названия ролей в ACL базы. Например, **[FormReadAccess]** (название роли не «длиннее» 15 символов). Затем он использует эти названия ролей при определении доступа к некоторым формам или видам. При разработке агентов на LotusScript соответствующая проверка, назначен или нет запустивший агента пользователь на роль, выполняется в самом агенте. Если пользователь не назначен на роль, агент попросту не выполняет своего действия.

Менеджер базы впоследствии назначает (на закладке Basics щелчком мыши по названию роли при «выбранном» субъекте) на эту роль пользователей базы из числа имеющихся в ACL. Выполняемые менеджером изменения в списках назначенных на роль не требуют изменения доступа в использующих эту роль формах, видах и агентах. Только назначенные на роль смогут воспользоваться использующими роли формами, видами и агентами - простого присутствия в ACL недостаточно.

На закладке Log содержится информация о том, кто, когда и что изменял в ACL базы.

Access Control List to: InterTrust's AddressBook

Basics
Roles
Log
Advanced

Administration server
☐ None
☒ Server InterTrust/InterTrustCorp/SU

Action
 Modify all Readers and Authors fields

If you wish to change the Administration Server for this database, it is recommended that you change the replica on InterTrust/InterTrustCorp/SU.

☒ Enforce a consistent Access Control List across all replicas
☒ Enable Extended Access

Disabling extended access control permanently removes access restrictions previously set on categories of documents and on individual documents.

Maximum Internet name and password Editor

Look Up User Types for 'Unspecified' Users

Pressing this button will perform a Domino Directory lookup for each user in the Access Control List who is listed as an 'Unspecified' user type. If the name is found, the appropriate user type (e.g. Server, Person, etc.) will be set in the ACL.

Last change: Vladimir A. Panov on 25.07.2003 20:35:47
 According to: InterTrust/C=RU

OK Cancel

Рис. 175

На последней закладке, во-первых, можно задать для базы сервер администрирования и уточнить, должна ли серверная задача Administration Process вносить изменения в поля типа Readers и Authors при операциях изменения имен или удаления пользователей.

Во-вторых, менеджер базы данных может обеспечить, чтобы список управления доступа (ACL) оставался тем же самым во всех репликах базы. Для этого менеджер на закладке Advanced выбирает опцию Enforce a consistent Access Control List across all replica («предписать непротиворечивый список управления доступом во всех репликах этой базы данных»). Выбор этой опции не только гарантирует, что ACL будет оставаться одинаковой во всех репликах базы на серверах, но и то, что ACL будет оставаться одинаковой и будет функционировать в репликах на станциях пользователей. Если же эта опция не выбрана, пользователи имеют доступ менеджера к своим локальным репликам, а следовательно, могут менять их ACL, даже если в реплике на сервере они не имеют такого уровня доступа, хотя такие локальные изменения в ACL не поступают в реплику на сервере.

Поддержка ACL в репликах на станциях тем не менее не является настоящим средством защиты, если вы физически не гарантируете безопасность станции или не применяете локального шифрования. Во-первых, зная имя группы, использованное в ACL, всегда можно создать группу с таким именем и включить в ее состав пользователя, которому необходим доступ. Во-вторых, зная полное имя пользователя, фигурирующего в ACL, можно создать новый ID-файл с таким именем (но, конечно, другими ключами) и

получить «под ним» доступ к локальной базе. Кроме того, серверные программы могут «обходить» список управления доступа, предписанный для локальных реплик.

Чтобы обеспечить распространение репликационных установок во все реплики базы на других серверах, следует выбрать данную опцию в реплике на том сервере, который имеет доступ менеджера во всех других серверных репликах, иначе репликация будет неудачной - сервер не сможет изменить ACL в репликах базы на других серверах. В сообщениях о неудаче репликации по этой причине вы встретите слова «inconsistent ACL».

В-третьих, имеется возможность указать максимальный уровень доступа к этой базе при использовании протоколов HTTP, POP3, IMAP, LDAP, DPOP с аутентификацией «вводом имени и пароля».

В-четвертых, кнопка Look Up User Types for «Unspecified» Users обеспечивает проверку фигурирующих в ACL имен по адресной книге и конкретизацию их типа: Person, Server, Person Group, Server Group, Mixed Group. Нажмите кнопку и вернитесь на первую закладку - в типах имен могут произойти изменения. Для чего это необходимо? Например, администратор сервера может запустить на сервере клиента Notes и работать под ID сервера с базой, если в ACL для имени сервера задан тип Unspecified. Но он не сможет этого сделать, если в ACL для имени сервера задан тип Server.

1.28.1. 1.1.1. Определение эффективного уровня доступа пользователя к базе

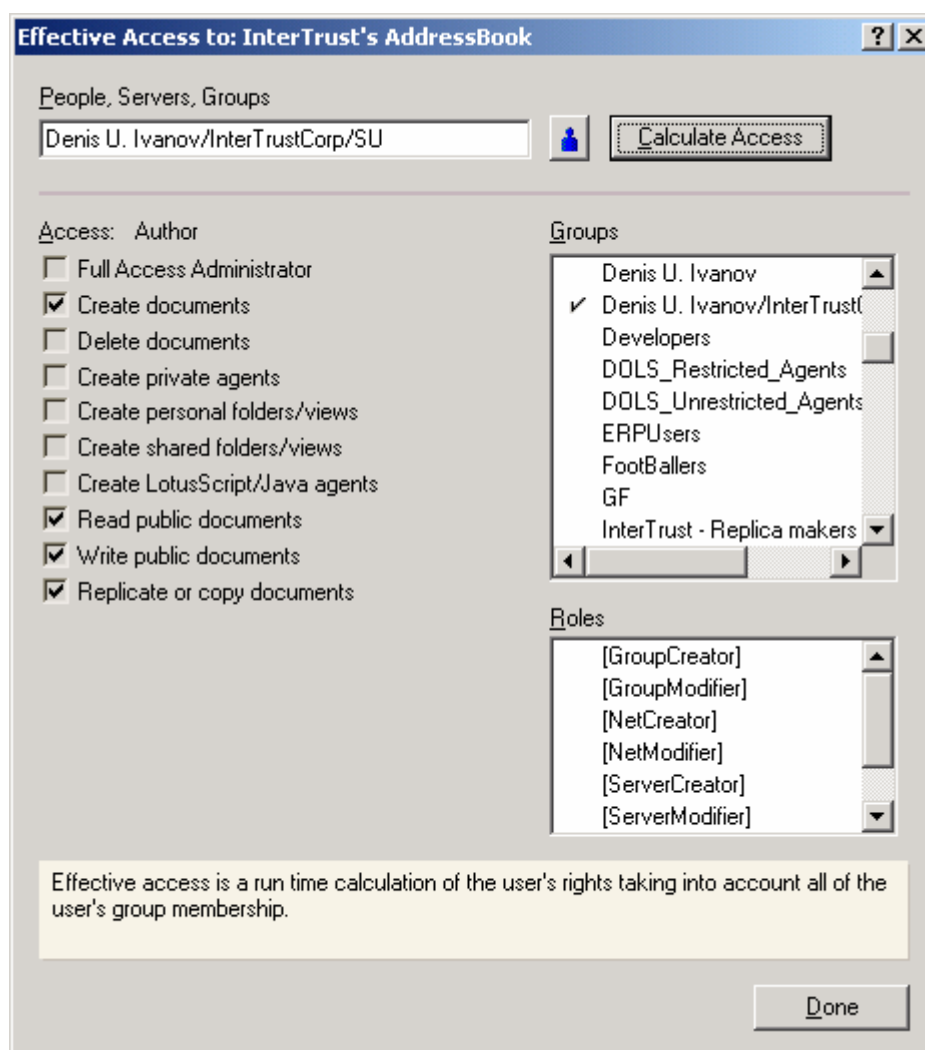


Рис. 176 Окно кнопки Effective Access

1.29. 1.1. Механика работы полей типа Authors и Readers

1.29.1. 1.1.1. Ограничение доступа к документу с использованием полей типа Readers

Поля типа Readers - один из эффективных способов контроля за тем, кто может «видеть» документ в базе данных, расположенной на сервере. Поля типа Readers можно «узнать» при просмотре полей документа в окне свойств документа на закладке Fields: хотя тип поля Readers «показывается» как Text, его параметр Field Flags будет содержать SUMMARY READ-ACCESS NAMES.

Документ, содержащий поля типа Readers, будет «виден» тем, кто явно или как член группы присутствует хотя бы в одном поле типа Readers из документа. Кроме того, такой документ будет «виден» и тем, кто явно или как член группы присутствует хотя бы в одном поле типа Authors из документа. Доступ же пользователя к документу определяется его доступом к базе данных. Так, читатель базы, присутствующий в поле типа Readers документа, «видит» документ и может открыть его только в режиме чтения. Редактор базы, присутствующий в поле типа Readers документа, «видит» документ и может открыть его как в режиме чтения, так и в режиме редактирования. Однако, например, менеджер базы, отсутствующий в полях типа Readers документа, «не видит» этот документ и поэтому вообще не может его открыть.

Поля типа Readers могут быть предусмотрены в форме разработчиком базы. Для этого используется или свойство формы Default Read access for documents created with this form, или в форме просто создаются собственные поля типа Readers. Когда по такой форме создается документ, в нем будут автоматически созданы предусмотренные поля типа Readers.

Даже если в форме не были предусмотрены поля типа Readers, любой пользователь, способный перевести документ в режим редактирования, может «защитить документ от посторонних», воспользовавшись закладкой с изображением ключа в окне свойств документа. В результате в документе по сохранению появится поле \$Readers, а его параметр Field Flags имеет значение SUMMARY READ-ACCESS.

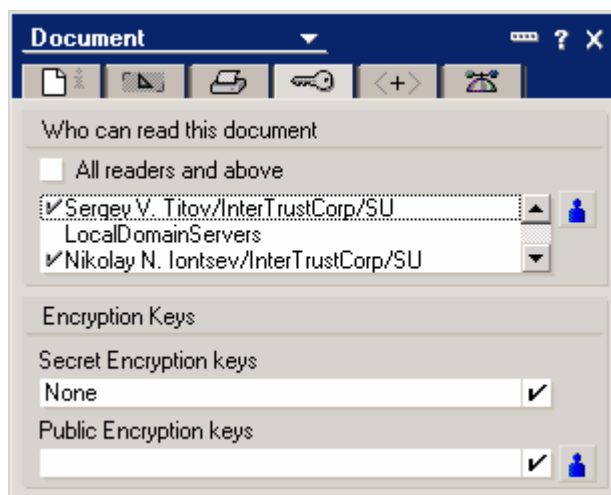


Рис. 177 Ограничение доступа на чтение документа

Документ, «скрытый от посторонних» хотя бы одним из этих способов, не может быть скопирован. Иными словами, если вы «не видите» документ в базе, расположенной на сервере, вы и не можете его скопировать «с сервера на локал». В том числе и когда делаете копию или реплику всей базы средствами Notes.

1.29.2. 1.1.2. Ограничение доступа на редактирование документа

Если пользователь или сервер имеет в ACL базы доступ автора, но не указан индивидуально или как член группы хотя бы в одном поле типа Authors этого документа, он не сможет редактировать такой документ в расположенной на сервере базе. Иными словами, Joe Smith/Acme, который имеет доступ автора к базе DISC.NSF, может редактировать только те документы, хотя бы в одном поле типа Authors которых содержится имя Joe Smith/Acme. Для имеющих к базе доступ редактора или выше поля типа Authors не запрещают редактировать документ.

1.30. 1.1. Уровни доступа администраторов в документе Server

1.30.1. 1.1.1. Принцип работы

Server : LINUX/LAEC/InterTrustCorp/SU

Basics | Security | Ports | Server Tasks | Internet Protocols | MTAs | Miscellaneous

Administrators

Full Access administrators: Administrators

Administrators: Administrators, LINUX/LAEC/InterTrustCorp/SU, LAEC - Remote Console

Database Administrators:

Full Remote Console Administrators: Administrators, LAEC - Remote Console

View-only Administrators: LAEC Instructors

System Administrator: Administrators

Restricted System Administrator:

Restricted System Commands:

Administer the server from a browser (pre-Notes 6 servers only): LAEC - Administer from browser, Administrators, LAEC - Remote Console

Рис. 178 Закладка Security документа Server

	Некоторые команды OS	Любые команды OS	Как администратор R 5	Обслуживание баз	Ограниченное использование удаленной консоли	Полное использование удаленной консоли
Full Access Administrators	✓	✓	✓	✓	✓	✓
Administrators			✓	✓	✓	✓
Database Administrators				✓		
Full Remote Console Administrators					✓	✓
View-Only Administrators					✓	
System Administrators	✓	✓				
Restricted System Administrators	✓					

Full Access Administrators имеют права администратора R 5 плюс:

- • Доступ Manager-а ко всем базам независимо от ACL баз и возможность «видеть» в базах все документы независимо от содержимого их полей Readers. Только для этого необходимо еще «включить опцию» Administration - Full Access Administration в меню клиента администратора. Если опция в клиенте администратора включена, такой же доступ предоставляется из любого клиента R6, запущенного на данном компьютере
- • Все права в плане программирования
- • Все права passthru
- • Возможность выполнять любые команды OS
- • На них не распространяются и им доступны для изменения Deny Access list
- • Это подобно уровню **root** в UNIX.

Administrators имеют те же права, как у администраторов R5:

- • Могут посылать команды на консоль сервера
- • Могут выполнять работы по обслуживанию баз
- • Могут отслеживать сообщения и их темы

Database Administrators выполняют работу по обслуживанию баз:

- • Назначают сервер администрирования базы в ACL
- • Создают, уплотняют (compact) и удаляют базы, реплики и главные шаблоны (master templates).
- • Управляют индексами полнотекстового поиска.
- • Управляют ссылками на каталоги и базы, управляют доступом к каталогам ([Directory ACL](#)).
- • Управляют свойствами и прочими атрибутами баз, например, квотами.

Full Remote Console Administrators могут удаленно выполнять любые команды сервера Domino (но не OS).

View-Only Administrators могут выполнять на сервере Domino только «безопасное подмножество» команд (SHOW SERVER, SHOW TASKS...). В принципе не могут повлиять на работу сервера.

System Administrators могут удаленно выполнять на компьютере сервера любые команды OS.

- • Для посылки команд OS используется Domino Console, а на сервере их принимает и исполняет Domino Controller
- • Команды конечно же не любые, а в рамках прав экаунта (пользователя), под которым был запущен Domino Controller.

Restricted System Administrators могут удаленно выполнять на компьютере сервера только набор команд OS, перечисленный в поле Restricted System Commands документа Server.

Administer the server from a browser (только для серверов версии ниже R6):

- • Разрешает использовать Web Administrator (WebAdmin.nsf) для администрирования сервера
- • Влечет изменение в ACL и назначение соответствующие роли (через ADMINP)

SECURE_DISABLE_FULLADMIN = 1 запрещает полный доступ. Может быть внесено только непосредственно в NOTES.INI и требует перезапуска сервера.

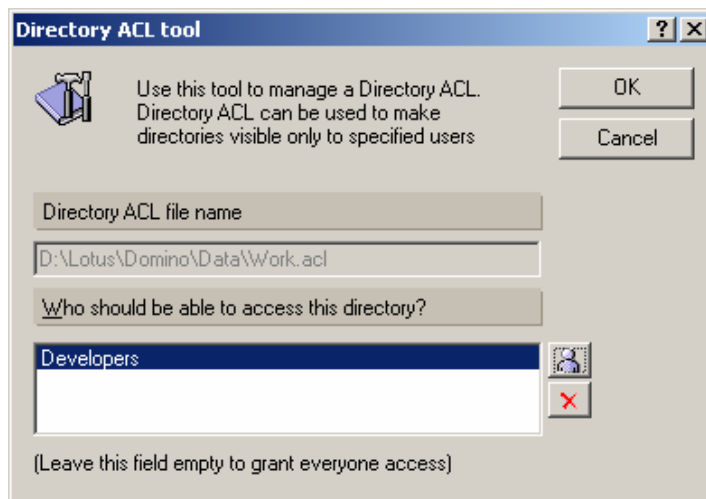


Рис. 179. Список управления доступом к каталогу

- Чтобы эта полезная возможность полнофункционально работала на не xSP-сервере, нужно добавить **Enable_ACL_Files=1** в NOTES.INI.
- Был упомянут еще один вариант установки серверов Domino – xSP. Позволяет поддерживать («хостить») на серверах xSP-домена много разных организаций, так что каждая организация «думает и видит, что это будто бы только ее сервера». Все серверы xSP-домена работают как xSP-серверы. Ставится такой домен запуском **setup.exe –asp** при установке первого сервера, все последующие серверы должны ставиться с этим же ключом. В таком домене в клиенте администратора на закладке Configuration «не серые» операции **Hosted Organizations**. Как переделать существующий обычный домен в xSP-домен, не переустанавливая серверы, я не знаю, в документации об этом не говорится, на вопросы в бизнес-партнерский форум IBM отвечает, что это невозможно, а мои эксперименты успехов не дали.

1.31. 1.1. Extended ACL (xACL) - расширенный список управления доступом

Задумано для создания безопасной модели делегирования административных полномочий

- • Расширяет возможности «обычной» ACL, позволяя управлять доступом к документам и полям в них
- • Действует по принципу «усечения» возможностей, предоставляемых «обычной» ACL
- • Есть в Domino Directory и Administration Requests

1.31.1. 1.1.1. Установка xACL

Первоначально организовать поддержку xACL может менеджер базы, выбрав флаги Enforce a consistent ACL... и Enable Extended Access

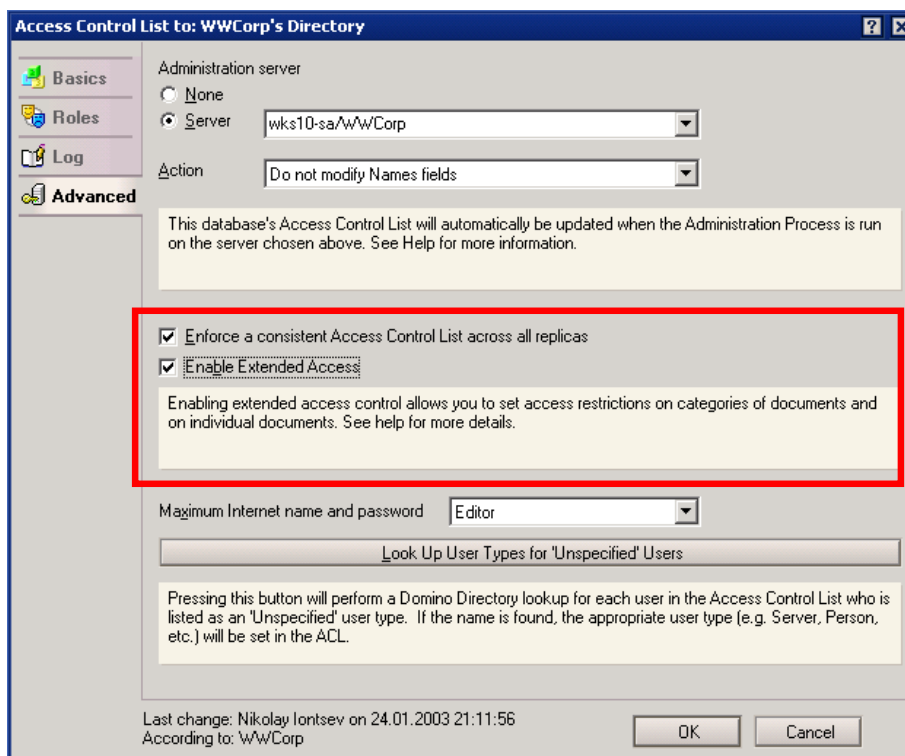


Рис. 181 Выбрав флаги, нажать OK

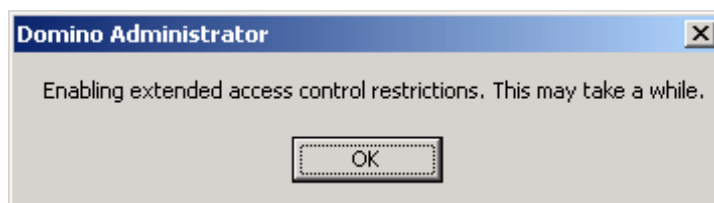


Рис. 182 Секунд через 10-30 здесь тоже нажать OK

После этого доступ к xACL выполняется кнопкой Extended Access

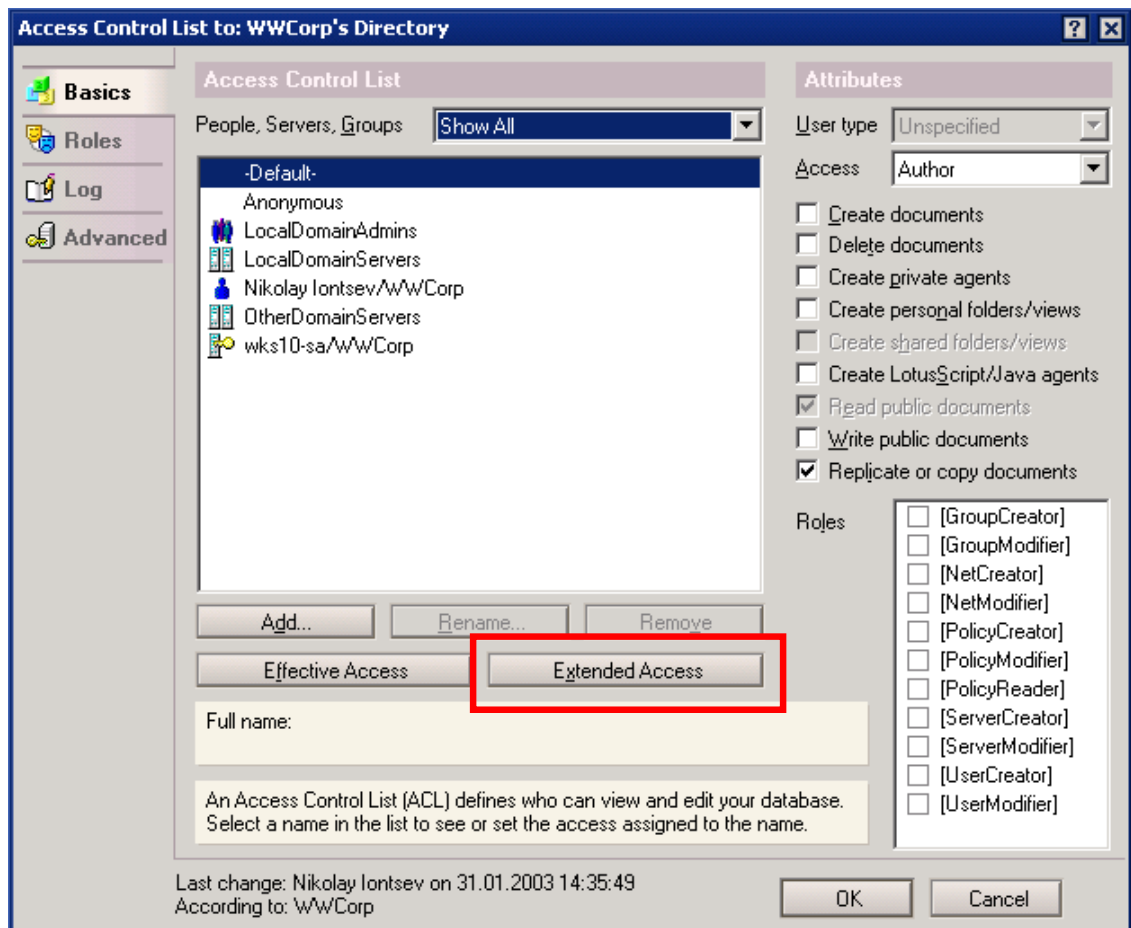


Рис. 183

1.31.2. 1.1.2. xACL - контроль доступа к документам

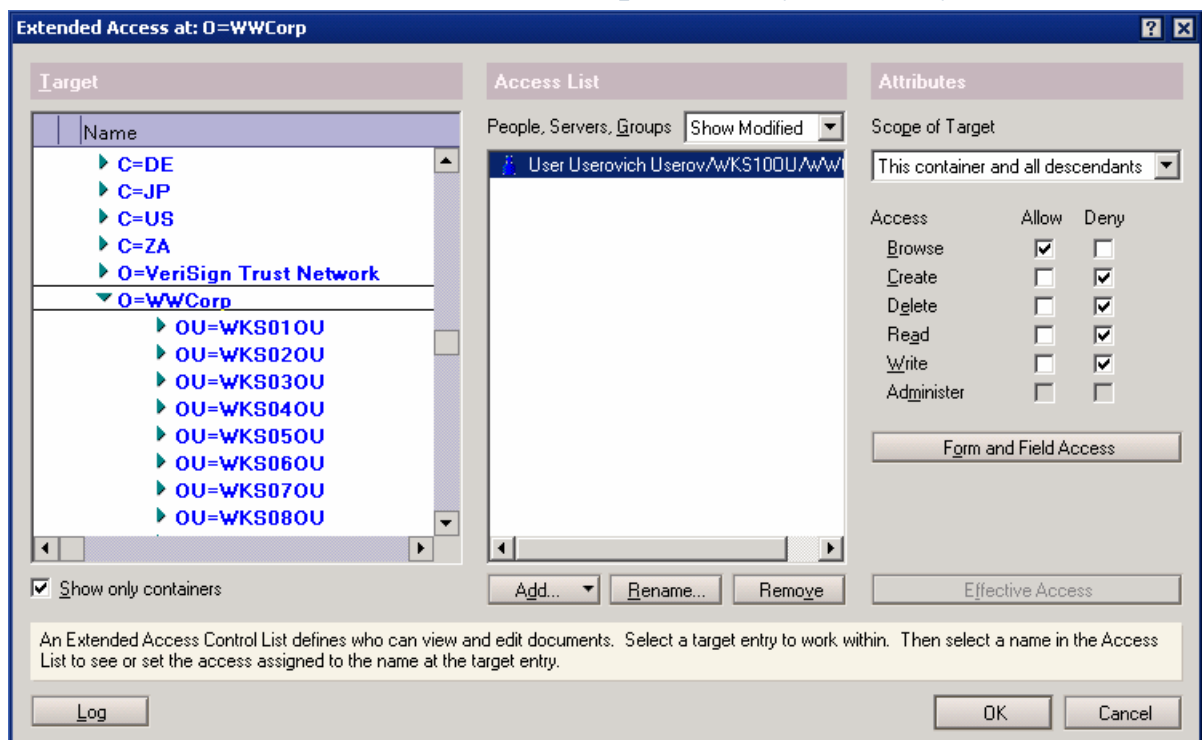


Рис. 184

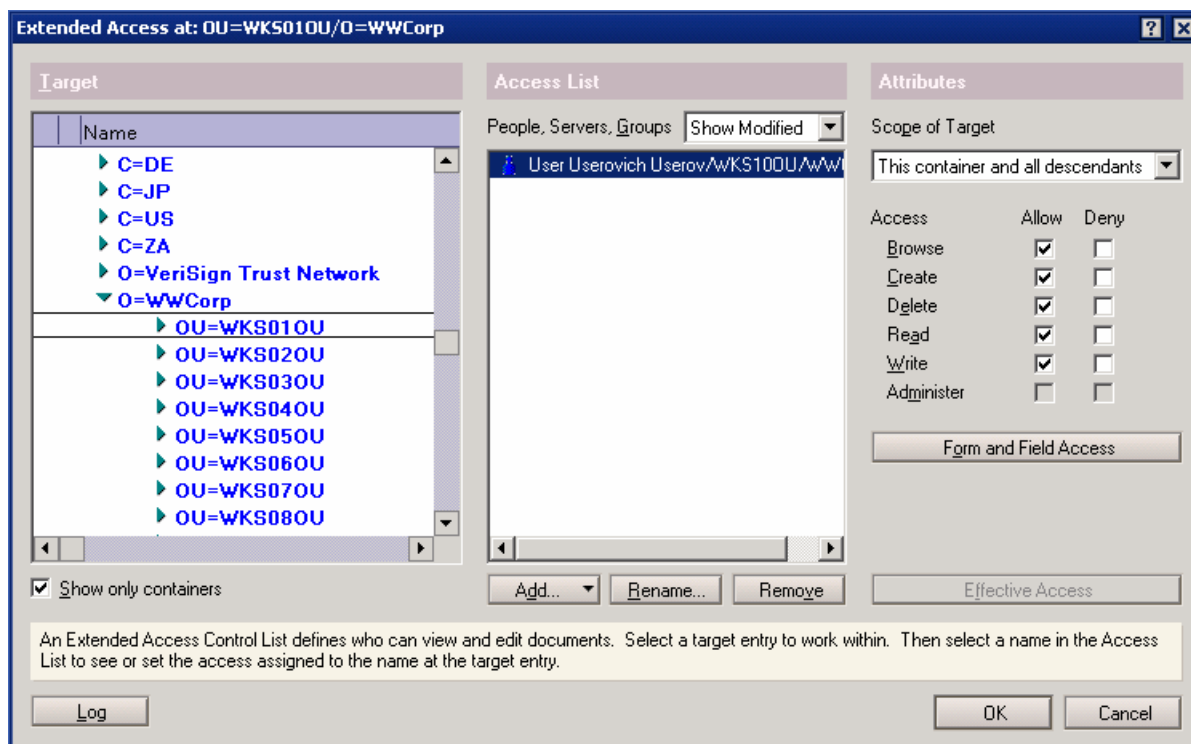


Рис. 185

Общий принцип - к документам данного контейнера (Target) данный субъект (Subject) имеет такой-то доступ (Access).

1.31.2.1. 1.1.2.1. Target - множество документов, на которое распространяется влияние xACL

- • / (root)
- • с опцией This container only- все «неиерархические» документы,
- • с опцией This container and all descendants - вообще все документы базы
- • категория (/WWCorp) - только к «иерархическим» документам данного контейнера включая или нет все его подконтейнеры
- • с опцией This container only- только этот контейнер,
- • с опцией This container and all descendants - этот контейнер и его подконтейнеры
- • документ - конкретный документ

Физически иерархия берется из скрытого вида (\$XACL) , который создается при «включении» xACL (поэтому и пауза перед окном Рис. 182 – строился вид...)

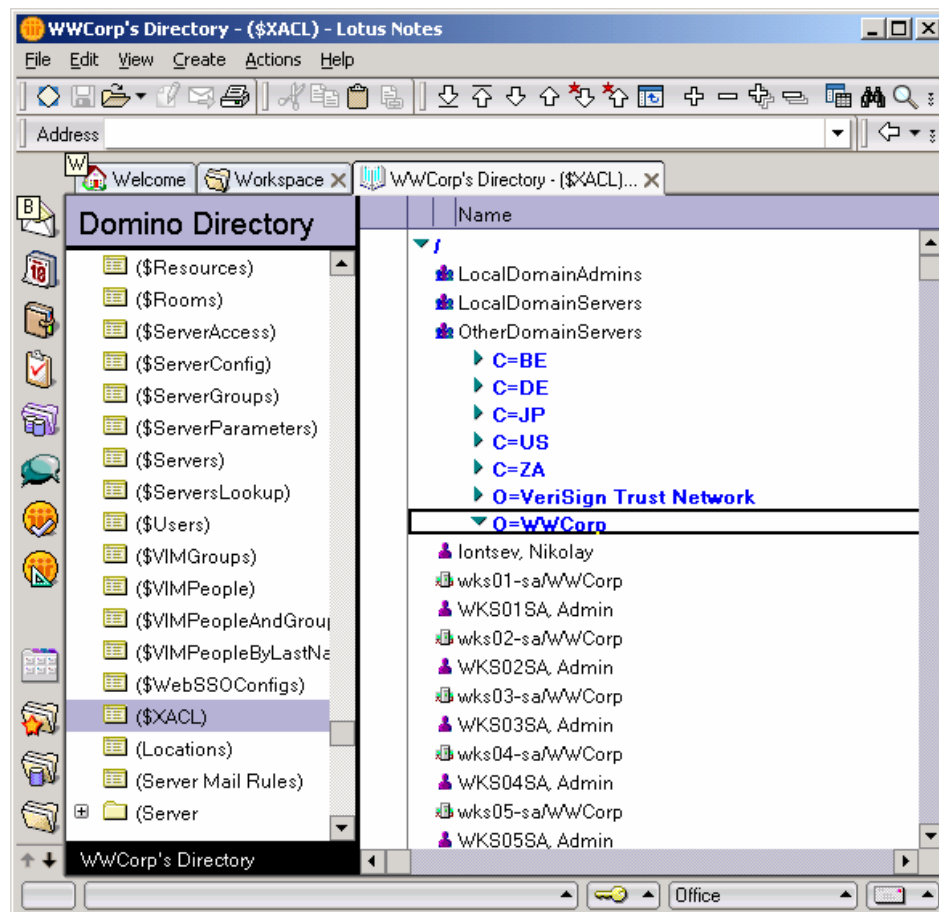


Рис. 186 Скрытый вид (\$XACL)

1.31.2.2. 1.1.2.2. Subject - к кому относится/применяется эта хACL

- • конкретное имя пользователя или сервера
- • Anonymous – не аутентифицированный
- • Self – все пользователи к своим собственным (Owner) документам в этом контейнере
- • имя группы
- • шаблон иерархических имен, например, */West/Acme
- • -Default- все остальные (относительно данной хACL, а не всей ACL!)

Если -Default- явно не указан в данной хACL, для «него» применяются ограничения для -Default- из ближайшей сверху по иерархии документов хACL, а при отсутствии таковой - права для -Default- из ACL. Собственно говоря, здесь наблюдается обычное наследование...

1.31.2.3. 1.1.2.3. Access - предоставляемый доступ по хACL

- • Browse - можно ли «видеть» документы выбранного множества в видах (не означает «читать по форме»)
- • Create - можно ли создавать документы выбранного множества
- • Delete - можно ли удалять документы выбранного множества
- • Read - можно ли читать документы выбранного множества
- • Write - можно ли редактировать документы выбранного множества
- • Administer - можно ли субъектам с доступом Designer или Editor по ACL управлять доступом по хACL к документам выбранного множества (Manager's могут это и без хACL)

1.31.2.4. 1.1.2.4. Простой пример использования из Student Guide

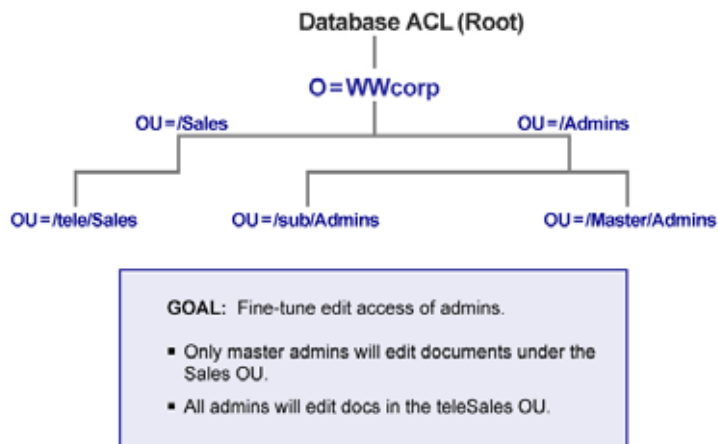


Рис. 187 Все админы «живут» в поддереве /Admins/WWCorp, но там две подветви: /sub/Admins/WWCorp и /Master/Admins/WWCorp. Есть подразделение /Sales/WWCorp, а в нем подразделение /tele/Sales/WWCorp. Задача состоит в том, чтобы редактировать документы /Sales/WWCorp могли только админы */Master/Admins, однако */Admins, включая */sub/Admins, могли редактировать документы /tele/Sales/WWCorp.

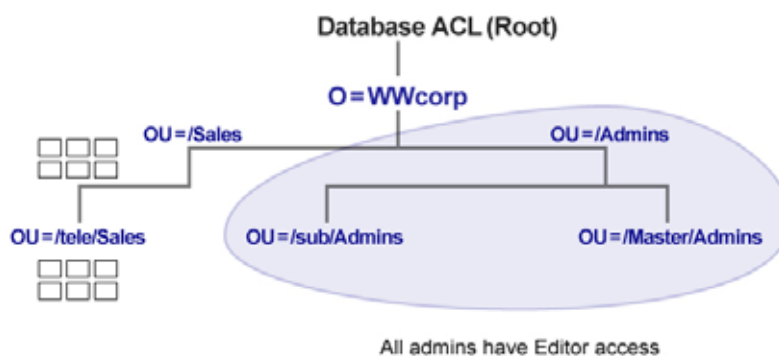


Рис. 188 Решение таково. По ACL */Admins имеют доступ Editor.

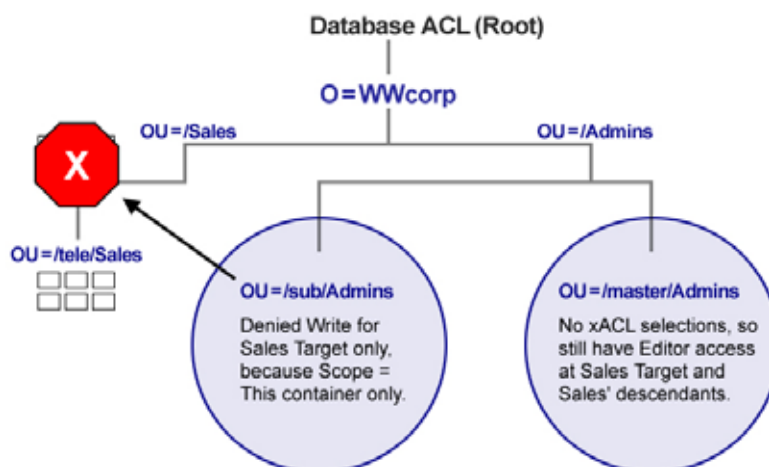


Рис. 189 На */sub/Admins создается xACL, запрещающая «писать» (Write) в контейнер /Sales/WWCorp (только в этот контейнер, не включая подконтейнеры)

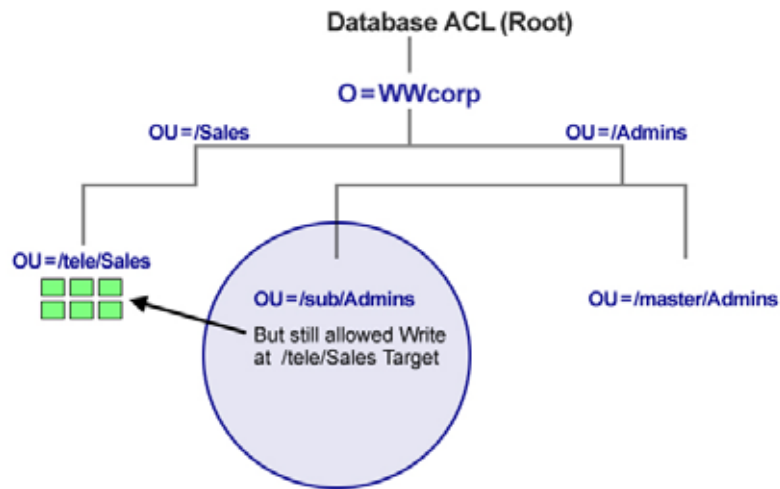


*Рис. 190 При такой xACL */sub/Admins не запрещается «писать» (Write) в контейнер /tele/Sales/WWCorp*

1.31.2.5. 1.1.2.5. Более сложный пример с наследованием и его «перекрыванием» на Рис. 184 и Рис. 185

Рис. 184. User-y Userovich-y Userov-y/WKS10OU/WWCorp в множестве документов /WWCorp (включая его подконтейнеры) разрешается только «видеть» документы в видах. Все остальное ему запрещено. Даже читать документы (открывать по форме) ему нельзя...

Рис. 185. Однако тому же User-y Userovich-y Userov-y/WKS10OU/WWCorp в множестве документов /WKS10OU/WWCorp (включая его подконтейнеры) разрешается выполнять любые операции с документами.

Здесь продемонстрирован один из общих принципов xACL:

- доступ, заданный на более высоком уровне иерархии документов, автоматически наследуется подчиненными ему уровнями иерархии документов
- на необходимом уровне иерархии документов наследование обычно «перекрывают»

1.31.3. 1.1.3. xACL - контроль доступа к формам и полям

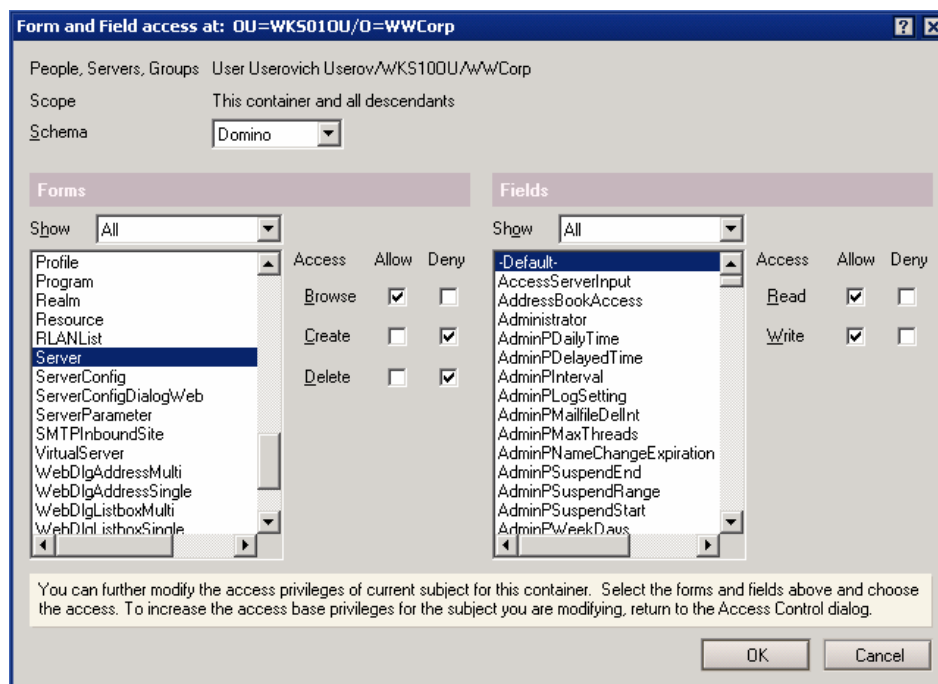


Рис. 191

Левая половина окна отвечает за доступ к документам по выбранной форме, правая часть (совместно с левой) отвечает за доступ к полям в документах. Каждое отдельно для Domino и для LDAP.

1.31.3.1. 1.1.3.1. Доступ в xACL к документам заданной формы

- • Subject (People, Servers, Groups) - для кого применяются эти разрешения
- • Scope - они применяются при обращении к множеству документов в данном контейнере и его контейнерах-потомках
- • Form - по какой форме документ; -Default- - все формы, для которых не определен собственный доступ
- • Access - доступ:
- • Browse - можно ли «видеть» (здесь в смысле «открывать на чтение») документы выбранной формы в выбранном контейнере
- • Create - можно ли создавать документы выбранной формы в выбранном контейнере
- • Delete - можно ли удалять документы выбранной формы в выбранном контейнере

А на примере Рис. 191 это выглядит просто:

User-y Userovich-y Userov-y/WKS10OU/WWCorp в множестве документов /WKS10OU/WWCorp (включая его подконтейнеры) документы по форме Server разрешается «видеть», но нельзя создавать и удалять. А изменять те существующие, которые он «видит»? Ответ на этот вопрос содержится не здесь, а на Рис. 185: поскольку есть доступ Write к множеству документов /WKS10OU/WWCorp, субъект может изменять существующие документы.

1.31.3.2. 1.1.3.2. Доступ в xACL к полям документов заданной формы

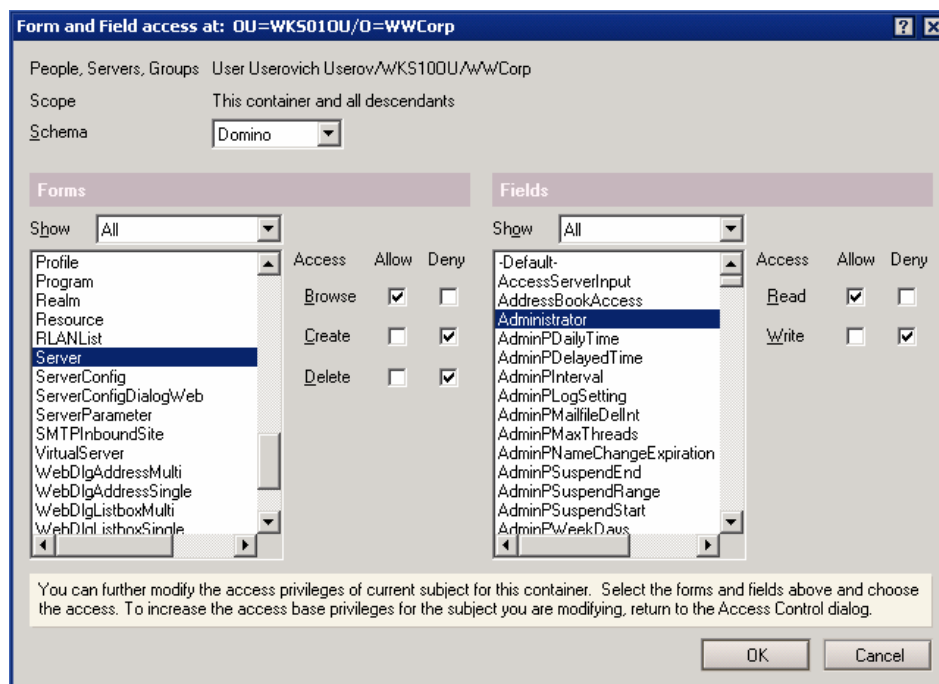


Рис. 192

- • Subject (People, Servers, Groups) - для кого применяются эти разрешения
- • Scope - они применяются при обращении к множеству документов в данном контейнере и его контейнерах- потомках
- • Form - по какой форме документ; -Default- - все формы, для которых не определен собственный доступ
- • Field - какое поле; -Default- - все поля, для которых не определен собственный доступ
- • Access - доступ:
- • Read - может ли читать значение указанного поля в документе выбранной формы из выбранного множества. Требуется Read для документа
- • Write - может ли редактировать значение указанного поля в документе выбранной формы из выбранного множества. Требуется Write для документа

А на примере Рис. 192 это выглядит просто:

User-y Userovich-y Userov-y/WKS10OU/WWCorp в множестве документов /WKS10OU/WWCorp (включая его подконтейнеры) в документах по форме Server поле Administrators разрешается читать, но нельзя изменять. А другие поля изменять можно, поскольку доступ Write для документа у субъекта имеется...

1.31.4. 1.1.4. Общие правила xACL

- • Права по xACL не могут быть выше прав по ACL. Например, xACL не может дать прав на изменение документа тому, кто Reader по ACL
- • Доп. привилегии по xACL не могут быть выше доп. привилегий по ACL. Например, xACL не может дать прав на удаление документа тому, кто не имеет такой привилегии по ACL
- • Ограничения xACL не распространяются на Manager по ACL - хотя бы потому, что у Manager по ACL достаточно прав для «полного снятия» xACL.
- • xACL позволяет дать субъекту к документам более низкого уровня в иерархии больший доступ, чем к документам более высокого уровня. Например, кто-то может иметь запрет на чтение всех документов (root), но читать или изменять документы /Sales/Acme

- • Права, данные имени в xACL, могут отличаться от эффективных прав для этого имени. Права, установленные явно в xACL, комбинируются с правами, унаследованными от ACL и xACL по уровням иерархии сверху. При этом возможны конфликты прав...

1.31.4.1. 1.1.4.1. Наследование прав в xACL

- • доступ, заданный на более высоком уровне иерархии документов, автоматически наследуется подчиненными ему уровнями иерархии документов
- • на необходимом уровне иерархии документов наследование обычно «перекрывают»

Уровень	Права
/Acme	AdminsAcme - Write,...; -Default- - Read
/West/Acme	AdminsWestAcme - Write,...
/East/Acme	AdminsEastAcme - Write,...

1.31.4.2. 1.1.4.2. Разрешение конфликтов наследования для Subject в xACL

- • «This container only» всегда имеет больший приоритет, чем «This container and all descendants»
- • по типам: явное имя (и Anonymous) → Self → член группы → удовлетворяет шаблону (*/*Acme) → -Default-
- • если Subject входит несколько раз в один тип (член двух групп GroupA и GroupB или удовлетворяет трем шаблонам), запреты преобладают над разрешениями (в отличие от ACL!)

	GroupA	GroupB	Effective Access
Read (doc)	Allow	No setting	Allow
Create (doc)	Allow	Deny	Deny
Delete (doc)	No setting	Deny	Deny

1.31.4.3. 1.1.4.3. Effective Access

В связи с тем, что в результате наследования и разрешения конфликтов наследования окончательные (эффективные) права по крайней мере сразу не очевидны, в ACL и элементах xACL имеется кнопка Effective Access.

Effective Access at: /WKS010U/WWCorp

People, Servers, Groups

User Userovich Userov/WKS100U/WWCorp

Calculate Access

Default Access		Modified Forms	Modified Fields	
Browse	☒		Access	
Create	☐		Browse	☐
Delete	☐		Create	☐
Read	☒		Delete	☐
Write	☒			
Administer	☐			

Database Access

Access: Author

Full Access Administrator ☐

Create documents ☐

Delete documents ☐

Create private agents ☐

Create personal folders/views ☐

Create shared folders/views ☐

Create LotusScript/Java ☐

Read public documents ☒

Write public documents ☐

Replicate or copy documents ☒

Access Derived From

-Default-

*AwKS100U/WWCorp

*AwWCorp

User Userovich Userov

☒ User Userovich Userov

Effective access is a run time calculation of your rights taking into account all of your group membership.

Done

Рис. 193

Effective Access at: /WKS010U/WWCorp

People, Servers, Groups

User Userovich Userov/WKS100U/WWCorp

Calculate Access

Default Access		Modified Forms	Modified Fields	
Browse	☒	Server	Access	Administrator
Create	☐		Browse	☒
Delete	☐		Create	☐
Read	☒		Delete	☐
Write	☒			
Administer	☐			

Database Access

Access: Author

Full Access Administrator ☐

Create documents ☐

Delete documents ☐

Create private agents ☐

Create personal folders/views ☐

Create shared folders/views ☐

Create LotusScript/Java ☐

Read public documents ☒

Write public documents ☐

Replicate or copy documents ☒

Access Derived From

-Default-

*AwKS100U/WWCorp

*AwWCorp

User Userovich Userov

☒ User Userovich Userov

Effective access is a run time calculation of your rights taking into account all of your group membership.

Done

Рис. 194

1.31.5. 1.1.5. Упражнение

После установки xACL проведите следующий эксперимент.

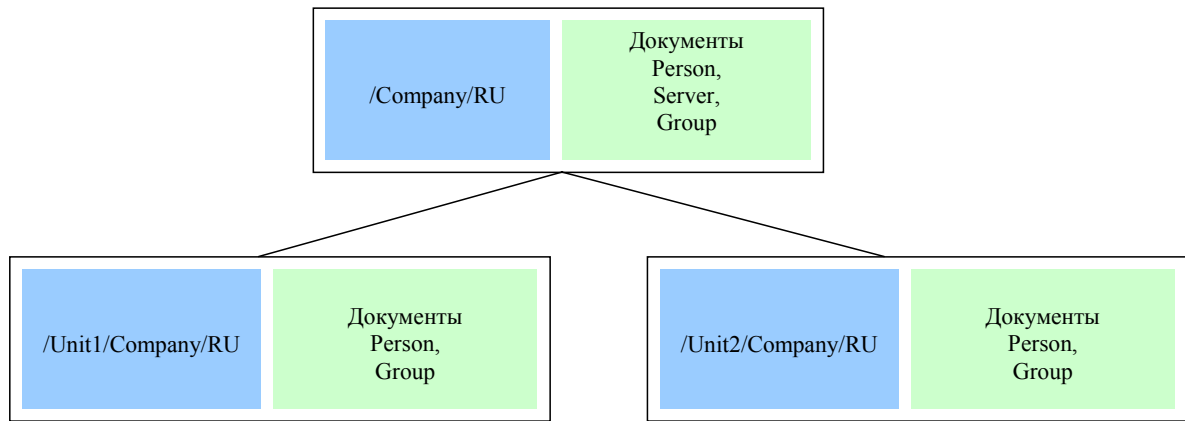


Рис. 195 Если контейнеры /Unit1/Company/RU или /Unit2/Company/RU пусты, создайте в них группы с иерархическими именами наподобие Group1/Unit1/Company/RU, Group2/Unit2/Company/RU (это допустимо в R6 и полезно на практике)

Пусть имеются два пользователя User1/Company/RU и User2/Company/RU, не входящие в группу LocalDomainAdmins. Делаем следующее:

- • ACL для User1/Company/RU и User2/Company/RU: Editor с назначением на роли GroupCreator, GroupModifier, UserCreator, UserModifier
- • xACL для User1/Company/RU:
 - • контейнер /Company/RU с подконтейнерами: видит все документы, но может только читать их
 - • контейнер /Unit1/Company/RU: может редактировать все документы
- • xACL для User2/Company/RU:
 - • контейнер /Company/RU с подконтейнерами: не видит никаких документов
 - • контейнер /Unit2/Company/RU: видит и может редактировать все документы

Проверяем, работает ли так, как того ожидаем...

1.32. 1.1. База Certification Log

1.32.1. 1.1.1. Создание базы Certification Log

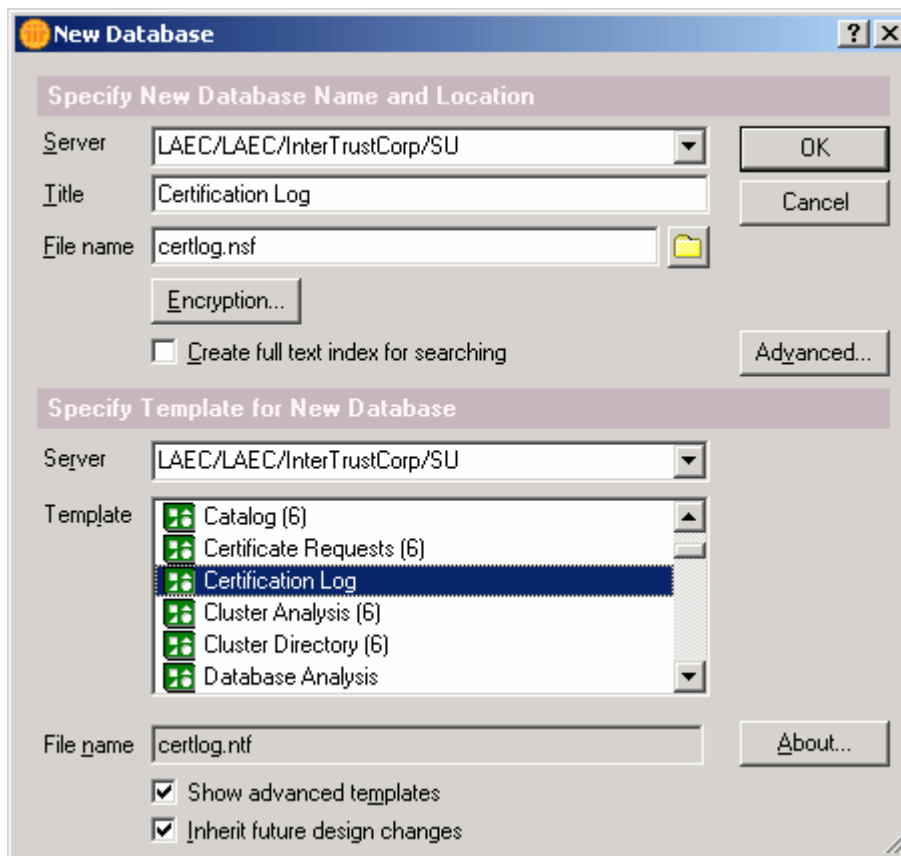


Рис. 195 Создание базы certlog.nsf. Во всех версиях, предшествующих R6, ее создавали «вручную». Только в R6 она создается автоматически, но лишь на первом сервере домена, при установке...

Обычно в домене имеет один идентификатор реплики. Поэтому создается как новая на одном из серверов, а затем делается реплика на остальные серверы.

1.32.2. 1.1.2. Операция Certification-Certification Log

Просто открывает базу certlog.nsf с сервера, который выбран в Administration Preferences клиента администратора на закладке Registration на кнопке Registration Server.

1.33. 1.1. Замена сертификата в ID-файле

1.33.1. 1.1.1. Операция Certification-Certify

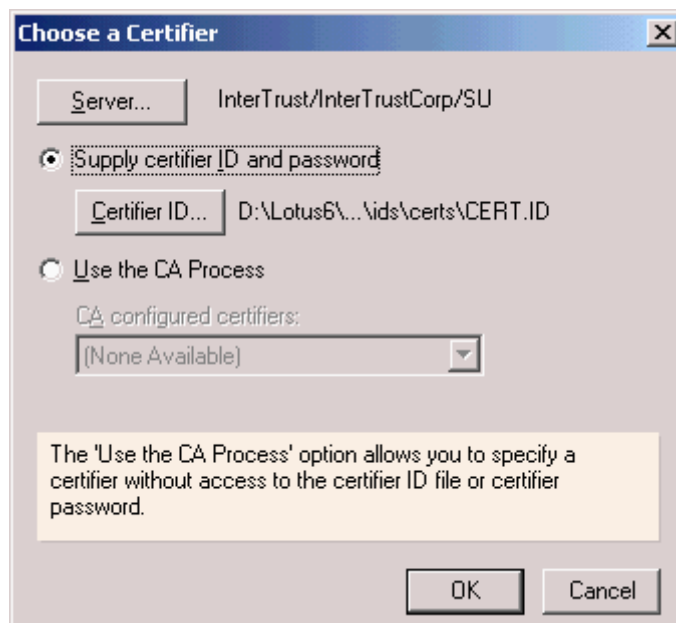


Рис. 196 Кнопкой Server задается «регистрационный сервер» - в NAMES.NSF этого сервера, в документ Person, Server или Certifier будет помещена копия нового сертификата

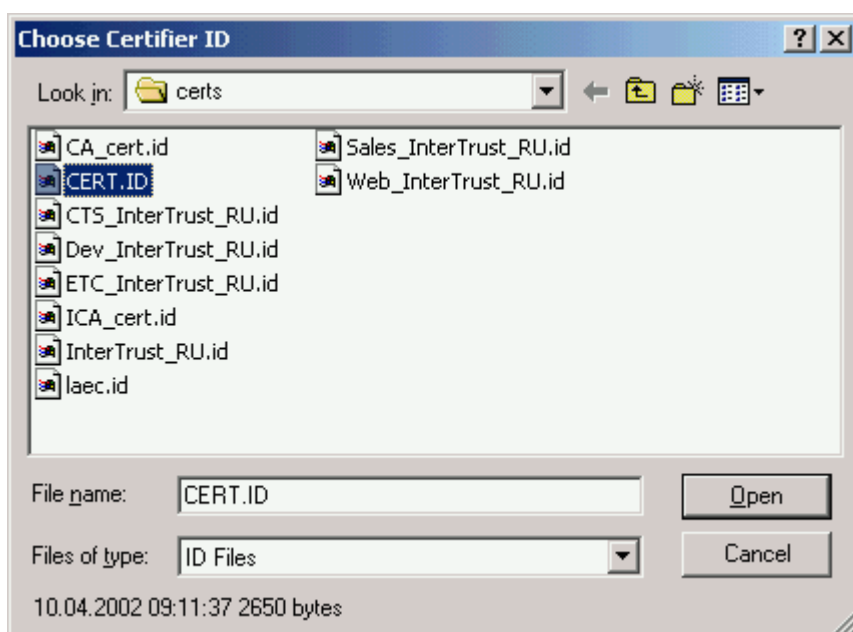


Рис. 197 Выбор ID-файла сертификатора. Определяет, каким именем (ID-файлом) подписывается сертификат



Рис. 198 Пароль ID-файла сертификатора

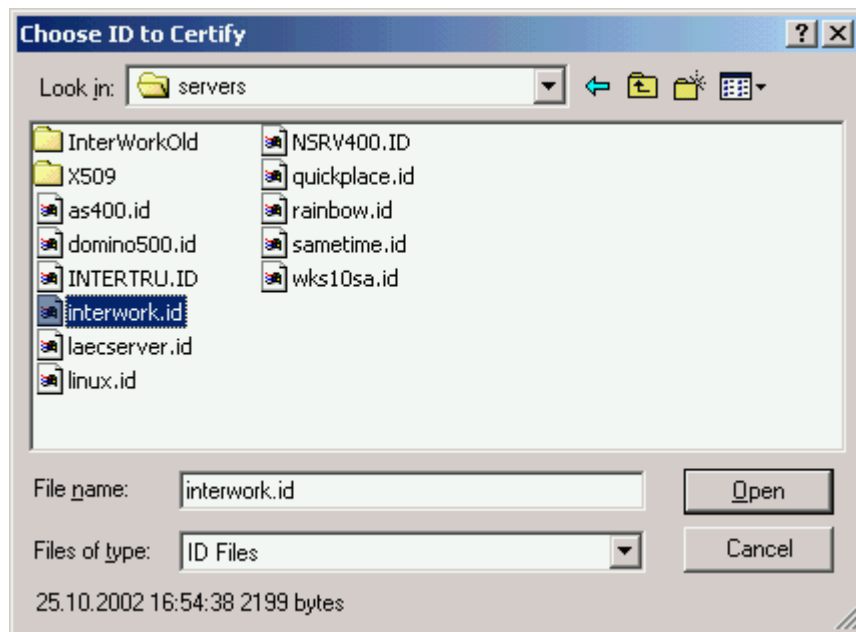


Рис. 199 Выбор ID-файла, в какой помещается подписанный сертификат. Если этот ID-файл имеет пароль, потребуется его ввести

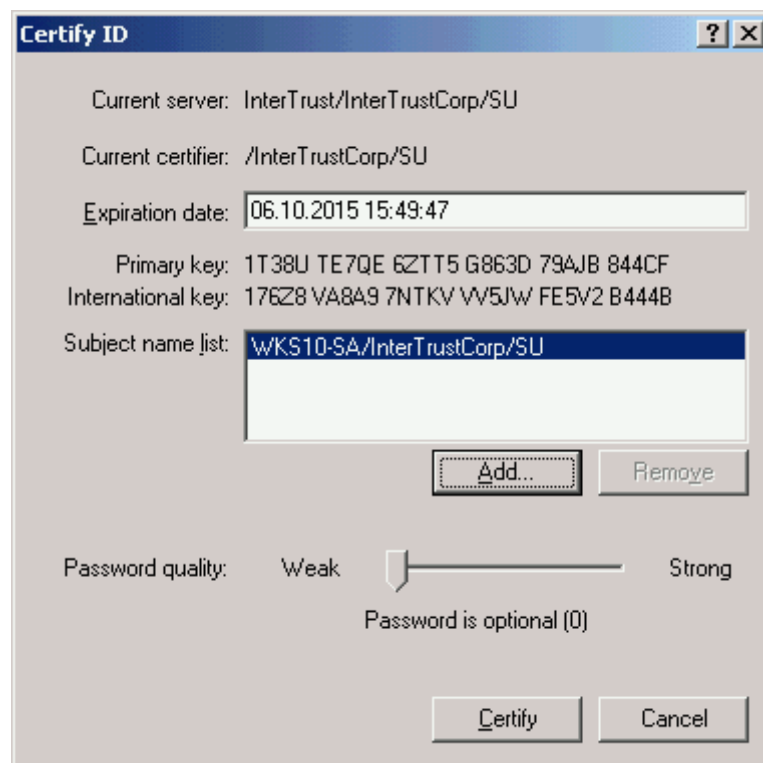


Рис. 200 «Основное окно» - можно продлить сертификат, добавить альтернативное имя (но не серверу!), изменить требуемое качество пароля...

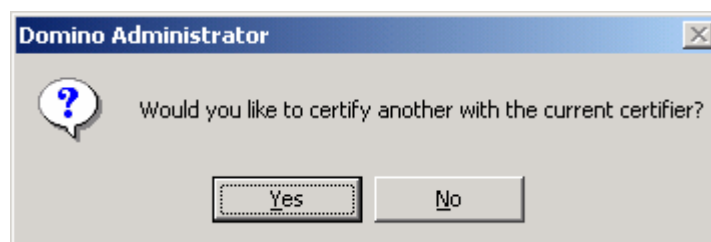


Рис. 201 С этим же ID-файлом сертификатора операцию можно повторять для других ID-файлов (цикл начиная с Рис. 199)...

Синхронно копия нового сертификата записывается в соответствующий документ в Каталоге Domino на «регистрационном» сервере (выбран на кнопке Server на Рис. 196).

1.33.2. 1.1.2. Продление сертификатов в ID-файлах серверов и сертификаторов

Поскольку операция заменяет сертификат непосредственно в ID-файле, ее применяют для ID-файлов серверов и сертификаторов (нет другого варианта), но редко применяют для ID-файлов пользователей (есть другой вариант, не требующий, чтобы пользователь предоставил свой ID-файл и ввел его пароль).

1.33.3. 1.1.3. Альтернативные имена и их назначение

Пользователь в ID-файле может иметь два имени (но не более двух!) - основное (обычно, «английское») и альтернативное (например, «русское»).

The screenshot shows the 'User Security' dialog box with the 'Your Names' tab selected. The left sidebar contains icons for 'Security Basics', 'Your Identity', 'Your Names', 'Your Certificates', 'Your Smartcard', 'Identity of Others', 'What Others Do', 'Notes Data', and 'Mail'. The main area is titled 'Your Notes Names' and contains the following fields and text:

- User name:** Nikolay N. Iontsev/InterTrustCorp/SU
- Alternate user name:** Ионцев Николай Николаевич/ИнтерТраст/RU
- Alternate Language:** Russian
- Aliases:** A list box containing 'Nikolay N. Iontsev', 'Nikolay Iontsev', and 'Iontsev'. Below the list is a 'Name Changes...' button.
- Your Internet Email Name(s):** A section with the field 'Internet email name' set to 'niontsev@intrust.ru'. Below this field is explanatory text: 'People outside of Notes can contact you using this Internet email name. The Notes mail router may also support other Internet email names for you. Ask your administrator for details.'

At the bottom right are 'OK' and 'Close' buttons.

Рис. 202 Альтернативное имя в свойствах ID-файла пользователя

Назначение альтернативных имен выполняется при регистрации новых пользователей или ресертификации существующих. Для этого ID-файл сертификатора должен иметь альтернативные имена. ID-файл сертификатора может иметь более двух имен, причем «по мере спуска по дереву имен наблюдается вложенность».

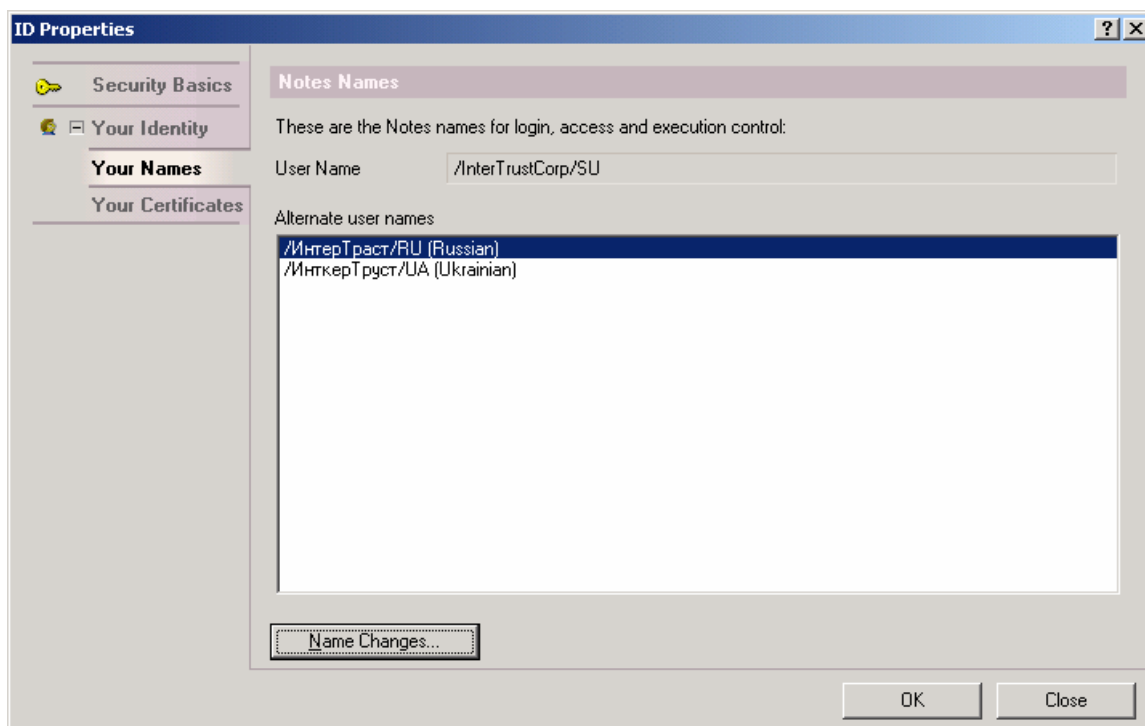


Рис. 203 Альтернативные имена в свойствах ID-файла сертификатора

Например, ID-файл сертификатора организации /Асте имеет поддержку имен на английском, французском, немецком, шведском и русском. Дерево имен «ветвится» на /America/Асте и /Еуропа/Асте. ID-файл сертификатора /America/Асте имеет поддержку имен на английском и французском. ID-файл сертификатора /Еуропа/Асте имеет поддержку имен на английском, французском, немецком, шведском и русском. Пользователь User1/America/Асте имеет английское имя и может иметь альтернативное французское имя. Пользователь User1/Еуропа/Асте имеет английское имя и может иметь еще одно альтернативное имя: на французском, немецком, шведском или русском.

- • Серверы альтернативных имен иметь не должны.
- • ID-файл с альтернативным именем не работает на клиенте R4

Процесс назначения альтернативных имен должен идти по дереву имен сверху вниз - от сертификатора верхнего уровня к сертификаторам подчиненных уровней и далее к пользователям.

Добавление альтернативного имени в ID-файл сертификатора

- • Certification - Certify.
- • Выбрать ID сертификатора и ввести пароль.
- • Выбрать этот же ID-файл или ID-файл «напрямую подчиненного уровня» и ввести пароль.
- • Нажать кнопку Add.

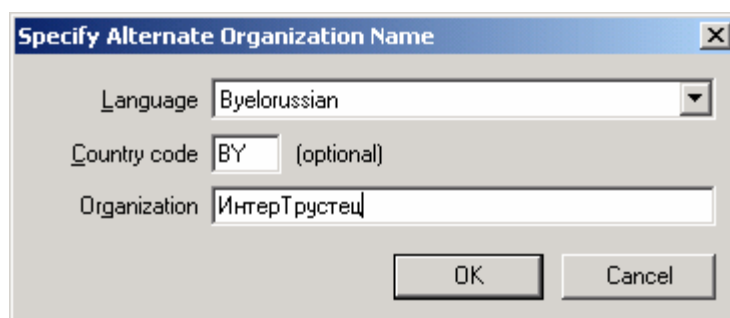


Рис. 204 Окно по кнопке Add для ID-файла сертификатора организации

Для ID-файла сертификатора организации указать альтернативный язык, код страны на этом языке (если надо) и название организации на этом языке. Для ID-файла сертификатора оргединицы задать язык и название оргединицы на этом языке. Нажать Ok.

- ● Нажать Certify.

Добавление альтернативного имени в ID-файл пользователя

- ● Новый пользователь – выбрать язык и имя при регистрации в окне User Registration.
- ● Существующий пользователь – вариантов несколько, лучше порекомендовать Tools – People – Recertify...
-

Альтернативное имя надо вводить в формате «**Фамилия Имя Отчество**», например, «**Иванов Иван Иванович**», а не «Иван Иванович Иванов», поскольку сортировка и поиск по альтернативному имени в стандартных видах NAMES.NSF организованы по «единой строке, без разбивки ее на компоненты»...

1.34. 1.1. Выпуск взаимных сертификатов

1.34.1. 1.1.1. Операции Certification-Cross Certify и Cross Certify Key

1.34.1.1. 1.1.1.1. Операция Certification-Cross Certify

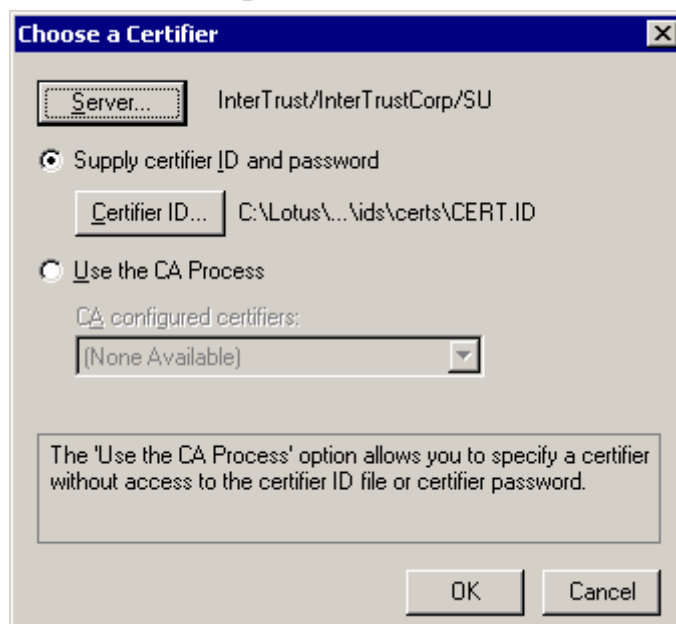


Рис. 205 Регистрационный сервер и ID-файл, от имени которого будет выпускаться взаимный сертификат

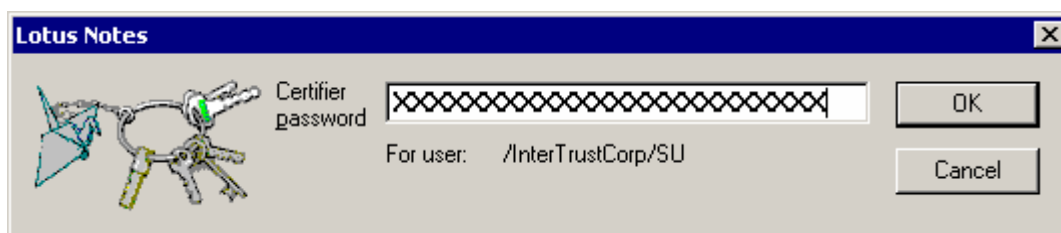


Рис. 206 Пароль этого ID

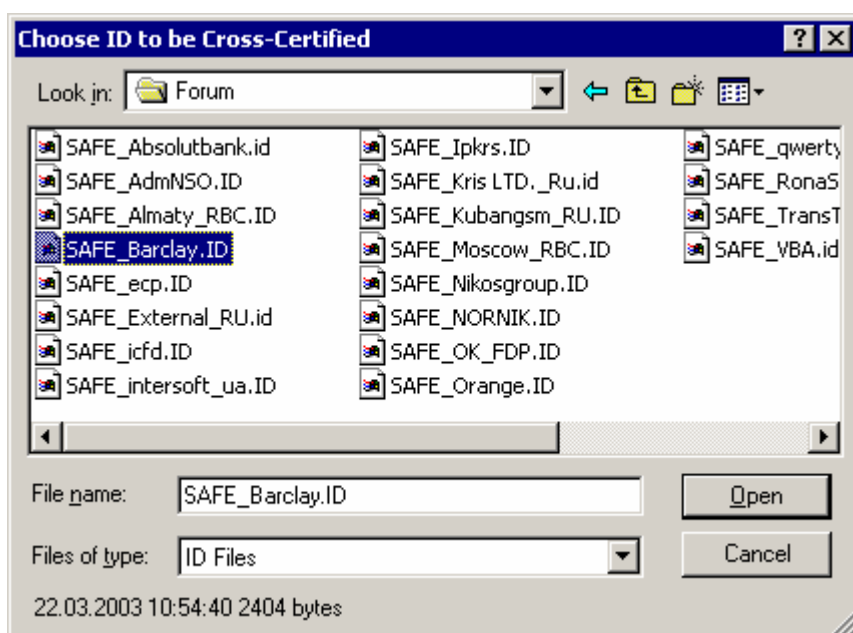


Рис. 207 Выбирается «безопасная копия» или (реже) «живой» ID-файл, «на который» выпускается взаимный сертификат

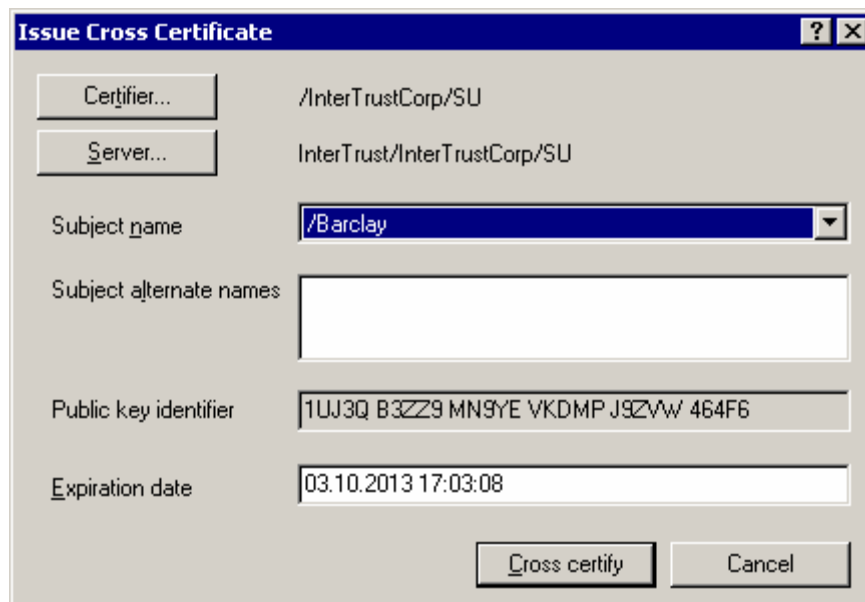


Рис. 208 «Основное окно»

- **Certifier** – от имени кого выпускается сертификат. Одновременно – это имя и его предки по дереву имен текущей организации смогут использовать этот сертификат в ходе процедуры аутентификации.
- **Server** – в какую NAMES.NSF помещается сертификат – в серверную или локальную клиента. Одновременно – кто этот сертификат потом может найти.
- **Subject name** – на чье имя выпускается сертификат. Это имя и его предки (из внешней организации) пройдут процедуру аутентификации в текущей организации.
- Операция повторяется «зеркально» в другой организации...

1.34.1.2. 1.1.1.2. Операция Cross Certify Key

Считается анахронизмом...

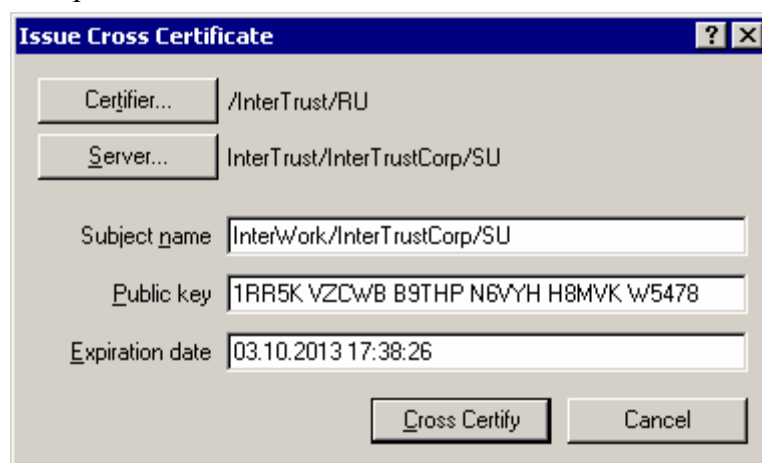


Рис. 209 Вместо передачи «безопасной копии» сообщается имя и открытый ключ, которые надо ввести в данном окне, являющемся аналогом «основного окна» на Рис. 208

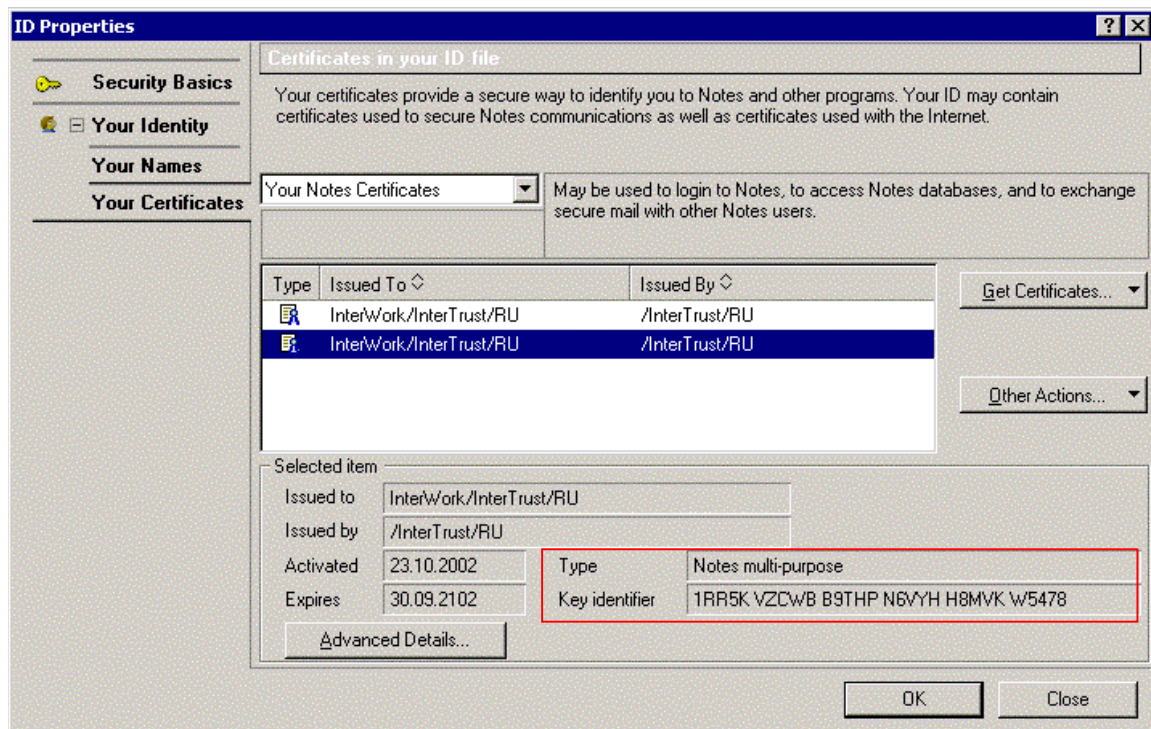
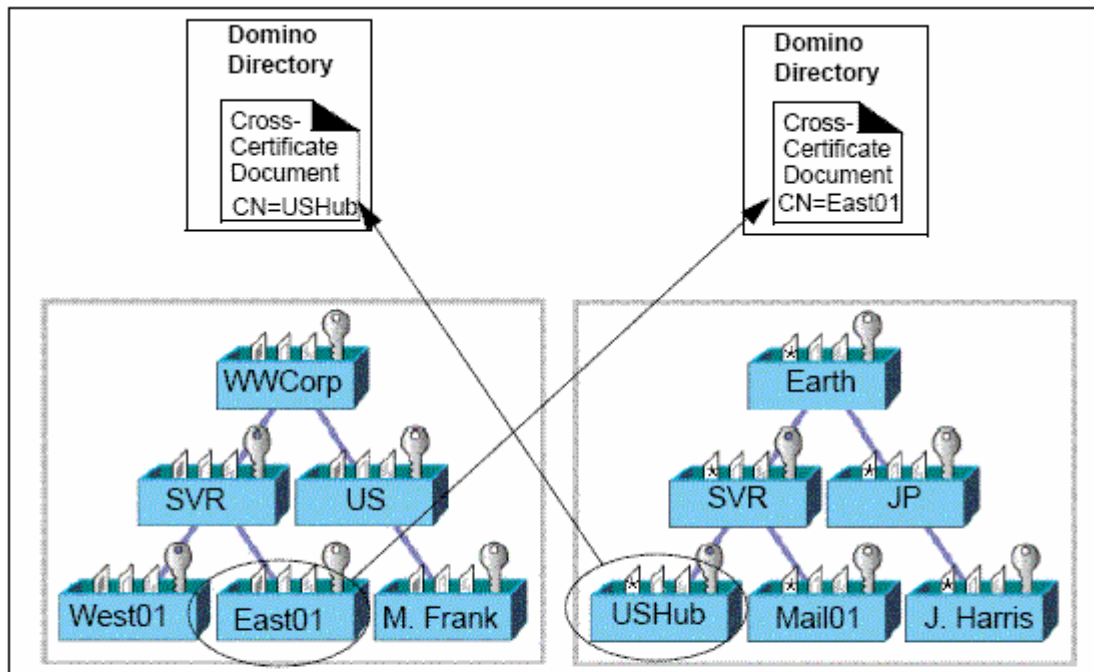


Рис. 210 Что за ключ такой там надо вводить?

**1.34.2. 1.1.2. Взаимная (кросс-) сертификация между
сертификаторами, между сертификатом и сервером, между серверами
и между любыми ID-файлами**



The following table shows the cross-certificates.

Cross-Certificate issued by	Cross-Certificate issued to	Cross-Certificate stored in Directory for
East01/SVR/WWCorp	USHub/SVR/Earth	WWCorp Domain
USHub/SVR/Earth	East01/SVR/WWCorp	Earth Domain

Рис. 211 Иллюстрация к вопросу, между какими узлами деревьев имен можно выпускать взаимные сертификаты

1.34.3. 1.1.3. Выпуск взаимного сертификата «на лету»

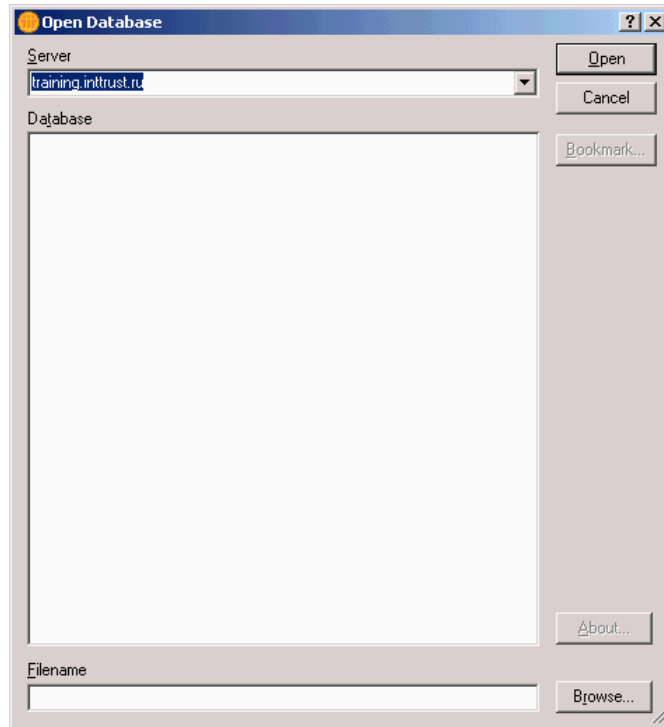


Рис. 212 Админ организации A из клиента делает попытку обратиться к серверу из организации B



Рис. 213 Получает окно об отсутствии взаимного сертификата в локальной NAMES.NSF – такое встречается реже

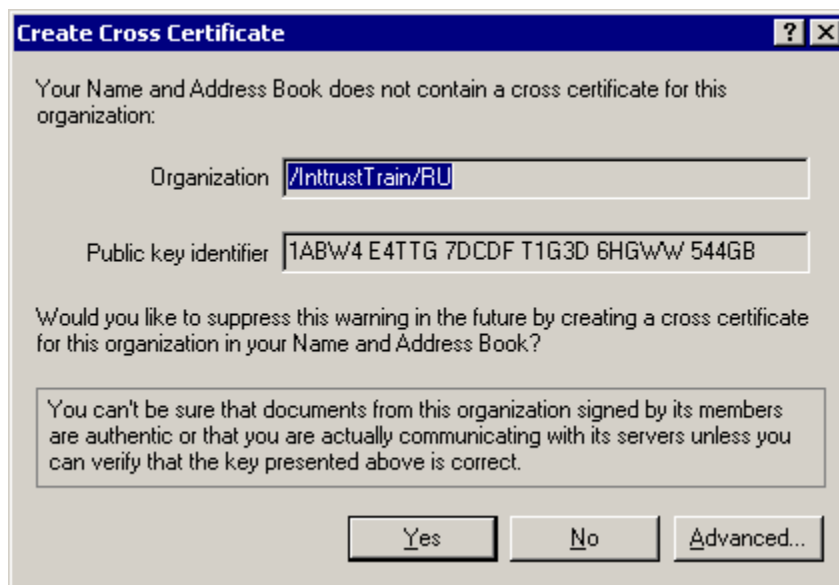


Рис. 214 Или получает такое окно об отсутствии взаимного сертификата в локальной NAMES.NSF – чаще

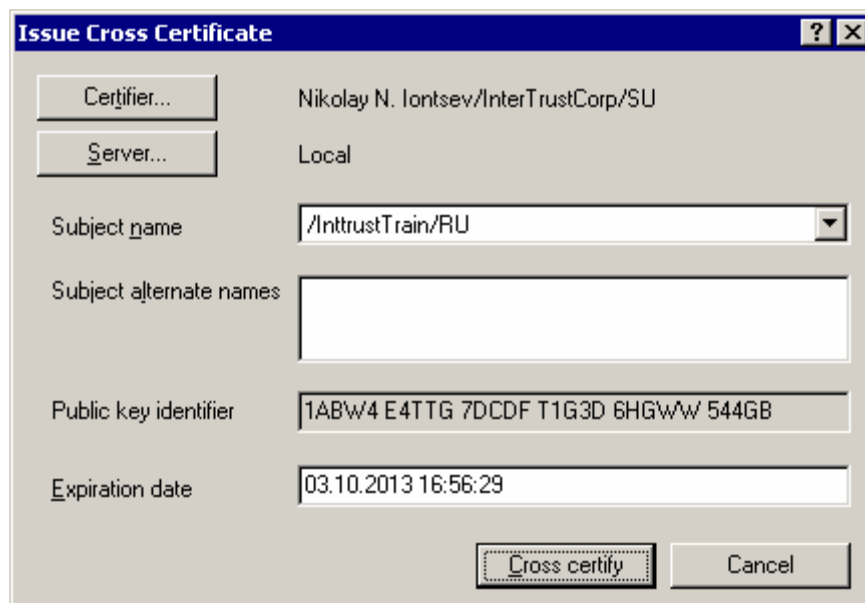


Рис. 215 На кнопке Certifier выбирает ID-файл сертификатора и вводит пароль

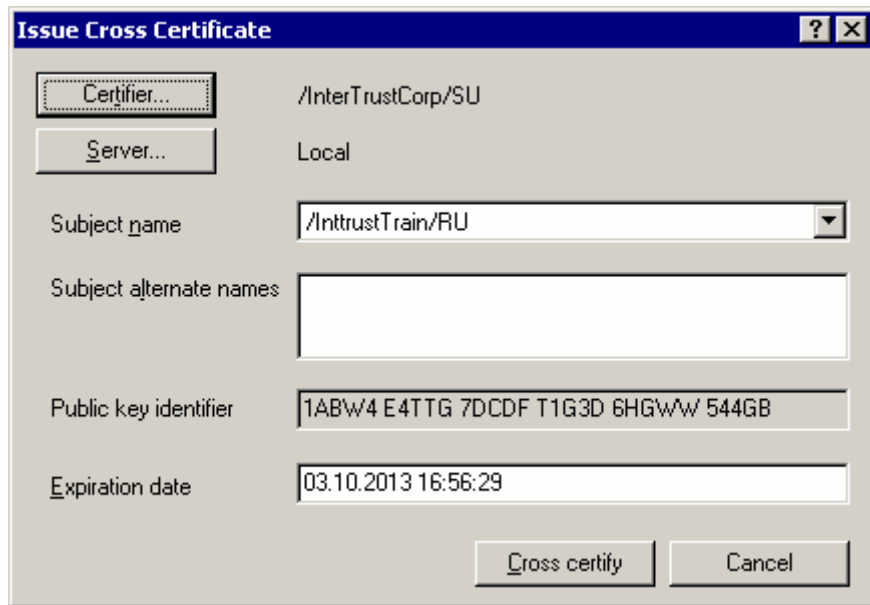


Рис. 216 Кнопкой Cross certify выпускает взаимный сертификат, который затем копирует как документ из локальной NAMES.NSF в серверную

Админ организации В из клиента делает попытку обратиться к серверу из организации А и выполняет все то же самое «зеркально».

1.35. 1.1. Назначение ID-файлу нескольких паролей

1.35.1. 1.1.1. Операция Certification-Edit Multiple Passwords

Если вы имеете информацию, которая должна охраняться так, чтобы только несколько одновременно присутствующих пользователей, но не каждый в отдельности, смогли получить к ней доступ, вы можете зарегистрировать фиктивного пользователя и назначать его ID-файлу множественные пароли. Имя фиктивного пользователя может быть указано в ACL баз для обеспечения доступа к ним, в ID-файле фиктивного пользователя могут содержаться ключи шифрования, обеспечивая шифрование документов в базах, и, наконец, фиктивный пользователь может получать зашифрованную почту. Затем вы «добавляете реальных пользователей» в этот ID-файл. Каждому из реальных пользователей назначается свой собственный пароль. В свойствах ID-файла с множественными паролями указывается количество реальных пользователей (как минимум один, но обычно два или более), которые должны собраться вместе и последовательно ввести свои пароли, чтобы стало возможным воспользоваться таким ID-файлом. Например, вы можете назначать четыре пароля для ID-файла, но требовать ввода только любых двух из четырех паролей, чтобы воспользоваться этим ID-файлом. Но возможен и «вырожденный» вариант, когда назначается несколько паролей, но для того, чтобы воспользоваться ID-файлом, необходимо ввести любой из этих паролей. Множественные пароли могут быть назначены и существующему ID-файлу. Любой пароль, назначенный ID-файлу до назначения ему нескольких паролей, после назначения нескольких паролей перестает действовать.

Такая возможность полезна, когда вы не хотите давать полномочий пользоваться ID-файлом сертификатора одному лицу, а как минимум двум одновременно присутствующим лицам.

Для создания ID-файла с множественными паролями вы должны пригласить всех необходимых администраторов и совместно с ними проделать следующее.

- • Вы начинаете процедуру. Выбираете в меню Certification-Edit Multiple Passwords. В появившемся окне выбираете ID-файл, которому назначаются множественные пароли, и вводите его «старый» пароль.

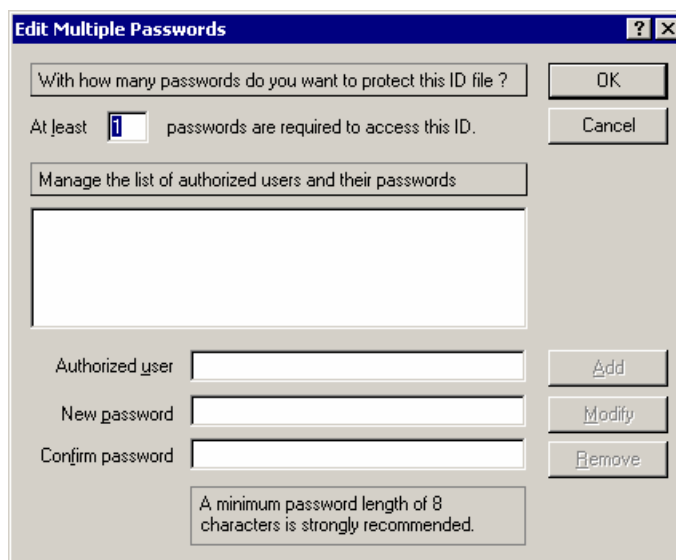


Рис. 217 Окно Edit Multiple Passwords

- • Затем каждый из приглашенных администраторов, один за другим, но отдельно от других, вводит свое имя в поле Authorized User, свой пароль в поле New Password и в поле Confirm Password, после чего нажимает кнопку Add для добавления информации о нем в ID-файл.

With how many passwords do you want to protect this ID file ?

At least passwords are required to access this ID.

Manage the list of authorized users and their passwords

Authorized user: Nikolay Iontsev

New password: [masked]

Confirm password: [masked]

A minimum password length of 8 characters is strongly recommended.

Buttons: OK, Cancel, Add, Modify, Remove

Рис. 218 Первый администратор ввел свое имя и пароль, но еще не нажал кнопку Add

With how many passwords do you want to protect this ID file ?

At least passwords are required to access this ID.

Manage the list of authorized users and their passwords

Nikolay Iontsev

Authorized user: Vladimir Panov

New password: [masked]

Confirm password: [masked]

A minimum password length of 8 characters is strongly recommended.

Buttons: OK, Cancel, Add, Modify, Remove

Рис. 219 Второй администратор ввел свое имя и пароль, но еще не нажал кнопку Add

- • Вы завершаете создание «многопарольного» ID-файла вводом количества паролей для его использования и нажатием кнопки Ok. Количество паролей должно быть не более количества администраторов, назначенных этому ID-файлу.

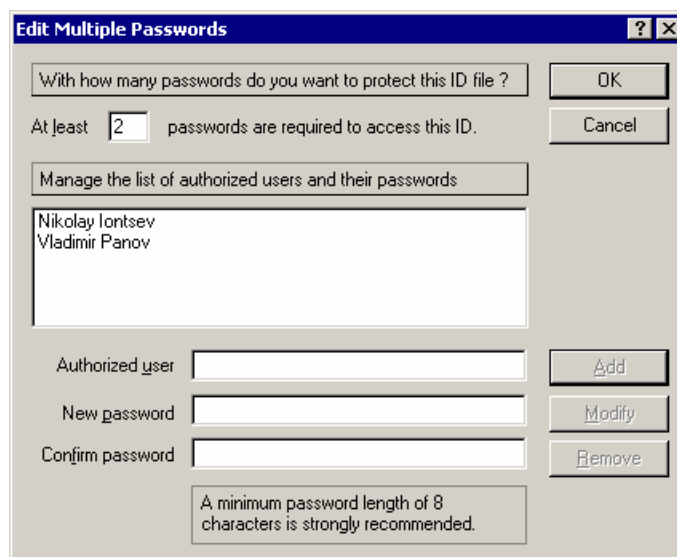


Рис. 220 Установка количества требуемых паролей в поле At least ...

Чтобы воспользоваться таким ID-файлом, нужно ввести соответствующее число паролей.

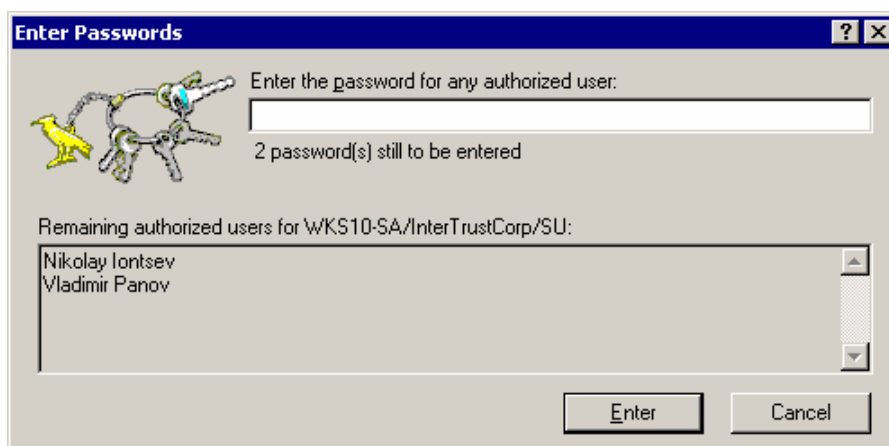


Рис. 221 Перед вводом первого пароля

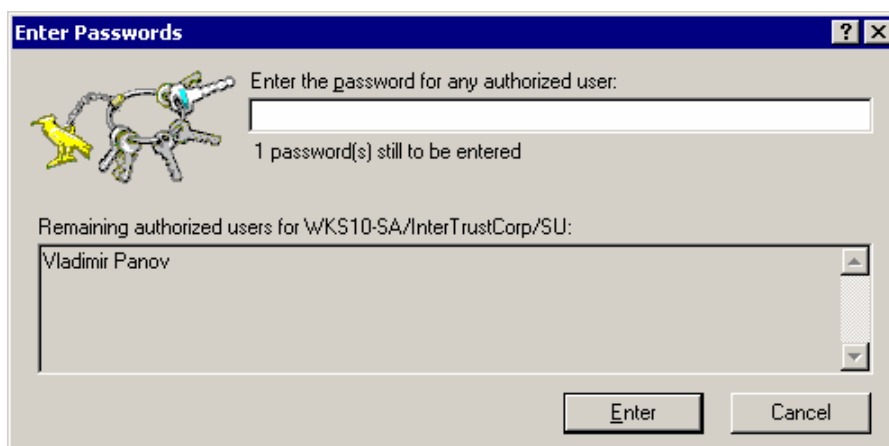


Рис. 222 После ввода первого пароля, но перед вводом второго

Когда вы применяете операцию Edit Multiple Passwords к ID-файлу, уже имеющему несколько паролей, станут доступны кнопки Remove, Modify и Add. Они позволяют удалить из списка пользователей ID-файла выбранного пользователя, внести для него необходимые изменения в имя или пароль или добавить нового пользователя. При этом можно изменить и количество паролей, необходимых для использования этого ID-файла.

1.36. 1.1. Регистрация сертификатов оргединиц

1.36.1. 1.1.1. Операция Registration-Organizational Unit

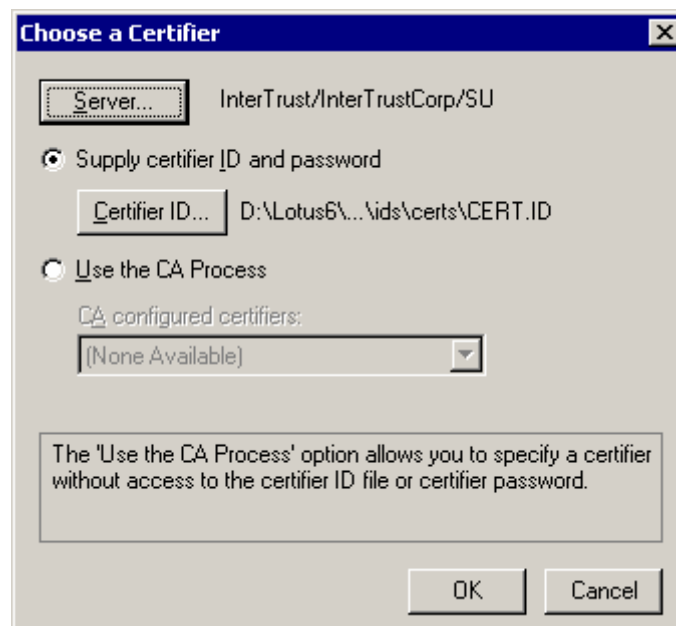


Рис. 223 ID-файл сертификатора, «под которым» создается ID-файл сертификатора оргединицы

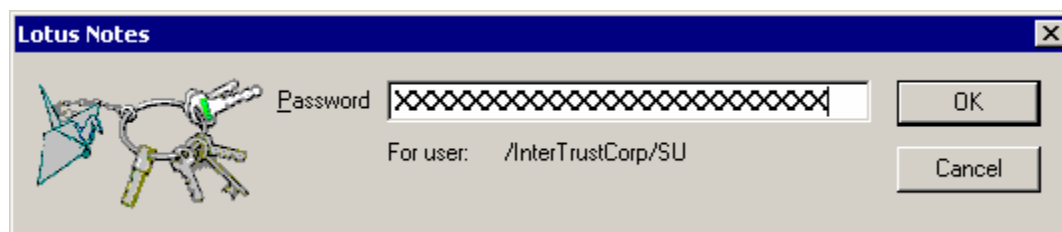


Рис. 224 Его пароль

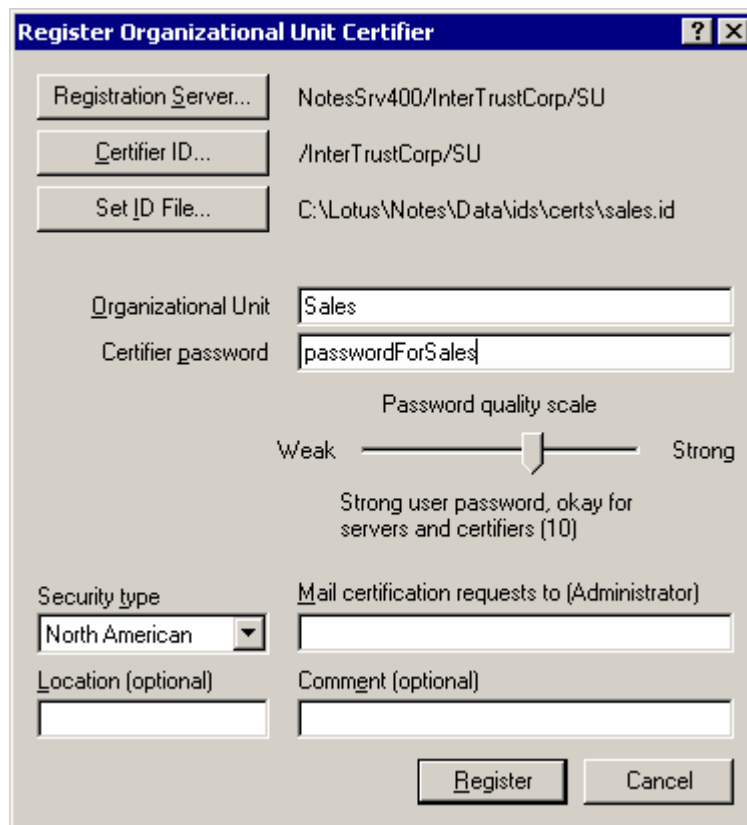


Рис. 225 Имя создаваемой оргединицы и пароль для ее ID-файла

Далее: альтернативные имена, обеспечение возможности восстановления забытых паролей, обеспечение доступа к системным базам для владельца...

1.36.2. 1.1.2. Уровень доступа к базам Domino Directory, Certification Log и Administration Requests для сертификатора

- • Names.nsf – автор с назначением на роль Person Creator и Person Modifier
- • Certlog.nsf – автор с правом создания документов, но без права удаления
- • Admin4.nsf – автор с правом создания и удаления документов

1.36.3. 1.1.3. Обсуждение подходов к выбору дерева имен для организации

«Золотая середина»:

- • Много уровней, почти отражает структуру организации – в именах просматривается структура организации (обычно нехорошо по соображениям безопасности), но самое главное – много работы по переводу пользователей из подразделения в подразделение...
- • Один уровень – допустимо в одной организации, но владельцу ID-файла сертификатора приходится делать много работы при большом количестве пользователей
- • Два уровня по территориальному или «крупно-функциональному» признаку – обычно хорошо. Например, так построено дерево имен в /Lotus: /CAM/Lotus, /MUC/Lotus, /MSK/Lotus...

1.37. 1.1. Регистрация нового сертификатора организации

1.37.1. 1.1.1. Операция Registration-Organization

Register Organization Certifier [?] [X]

Registration Server... InterTrust/InterTrustCorp/SU

Set ID File... C:\Lotus\Notes\Data\ids\certs\scala.id

Organization name Scala

Country code RU (optional)

Certifier password passwordForScala

Password quality scale

Weak ————— Strong

Strong user password, okay for servers and certifiers (10)

Security type North American

Mail certification requests to (Administrator)

Location (optional)

Comment (optional)

Register Cancel

Рис. 226 Имя организации, код страны и пароль для создаваемого ID-файла

Вопрос не в том, как создать, а в количестве работы по переводу существующей инфраструктуры «под него».

1.38. 1.1. Архивирование ID-файлов и восстановление их паролей

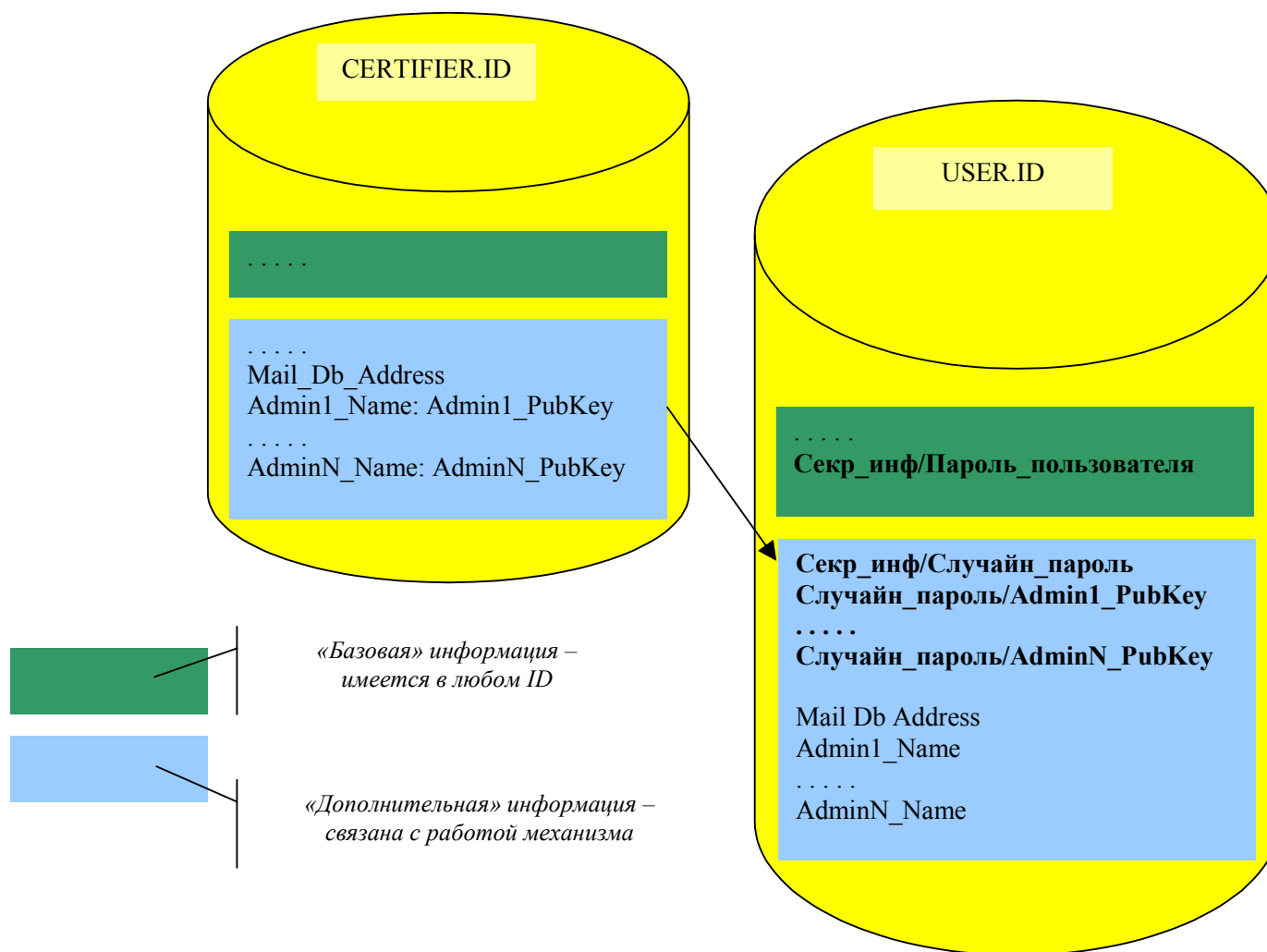


Рис. 227 Логика работы механизма

В ID-файл сертификатора добавляется дополнительная информация: адрес почтовой базы (Mail_Db_Address) и имена и открытые ключи авторизованных администраторов (AdminX_Name и AdminX_PubKey).

При регистрации под таким ID-файлом сертификатора, например, пользователя, в ID-файл пользователя так же добавляется дополнительная информация: вторая копия секретной информации, зашифрованная на случайным образом сгенерированном пароле (**Секр_инф/Случайн_пароль**), случайным образом сгенерированный пароль, зашифрованный по RSA на открытых ключах авторизованных администраторов (**Случайн_пароль/AdminX_PubKey**), а так же имена авторизованных администраторов (AdminX_Name) и адрес почтовой базы (Mail_Db_Address).

В результате «появляются два входа» в ID-файл пользователя. «Первый вход» обычный – пользователь вводит пароль ID-файла, на нем дешифрируется первая копия секретной информации, что дает секретный ключ пользователя и его ключи шифрования. «Второй вход» используется в случае, когда пользователь забыл пароль. Авторизованный администратор, работая под своим ID-файлом, обретает возможность дешифровать (по RSA на своем секретном ключе) случайным образом сгенерированный пароль из ID-файла пользователя и сообщить его пользователю. Пользователь, введя этот пароль, обретает возможность дешифровать на нем вторую копию своей секретной информации и тут же, зашифровав ее на новом пароле, заменить ею первую копию секретной информации.

По адресу почтовой базы при работе механизма будут присылаться сообщения с копией ID-файла (в момент первоначальной регистрации) или с присоединенным файлом, содержащим информацию для восстановления «забытого пароля» (при изменениях в ID-файле, влекущих изменение случайным образом сгенерированного пароля). Имена авторизованных администраторов создают пользователю «контекст» - он знает, к кому обратиться за помощью.

Дана лишь «общая понятийная логика» работы механизма – реально все несколько сложнее (например, пользователь может получать «пароли восстановления» от нескольких авторизованных администраторов...)

1.38.1. 1.1.1. Операции Certification-Edit Recovery Information и Extract Recovery Password

1.38.1.1. 1.1.1.1. Предварительная подготовка

Операция 1. Создание почтовой базы данных для хранения информации, используемой для восстановления ID-файлов (database for backup IDs)

- • Создайте на сервере, к которому имеют доступ все пользователи и серверы домена, базу данных. Обычно она создается по шаблону обыкновенной почтовой базы.
- • В ACL базы задайте для -Default- уровень доступа No access, а для авторизованных администраторов - уровень доступа Reader.
- • Создайте в каталоге Domino документ Mail-in database для этой базы.
В эту базу (почтой по заданному Вами в документе Mail-in database адресу базы) будет доставляться информация, используемая для восстановления ID-файлов.

Операция 2. Назначение авторизованных администраторов

- • В Domino Administrator перейдите на закладку Configuration.
- • Из меню Tools выберите Certification>Edit Recovery Information.
- • Откройте ID-файл сертификатора.
- • Введите его пароль.
- • Нажмите кнопку Add. Затем выполните следующее:
 - • Выберите имя администратора, авторизованного восстанавливать ID-файлы. Нажмите кнопку Add.
 - • Повторите это для каждого из авторизованных администраторов.
 - • Нажмите кнопку ОК, когда «авторизуете» всех.
- • Нажмите кнопку Address и выберите адрес почтовой базы, в которую будет доставляться информация, используемая для восстановления ID-файлов.
- • Введите количество авторизованных администраторов, необходимое для восстановления ID-файла.
- • Нажмите кнопку ОК.

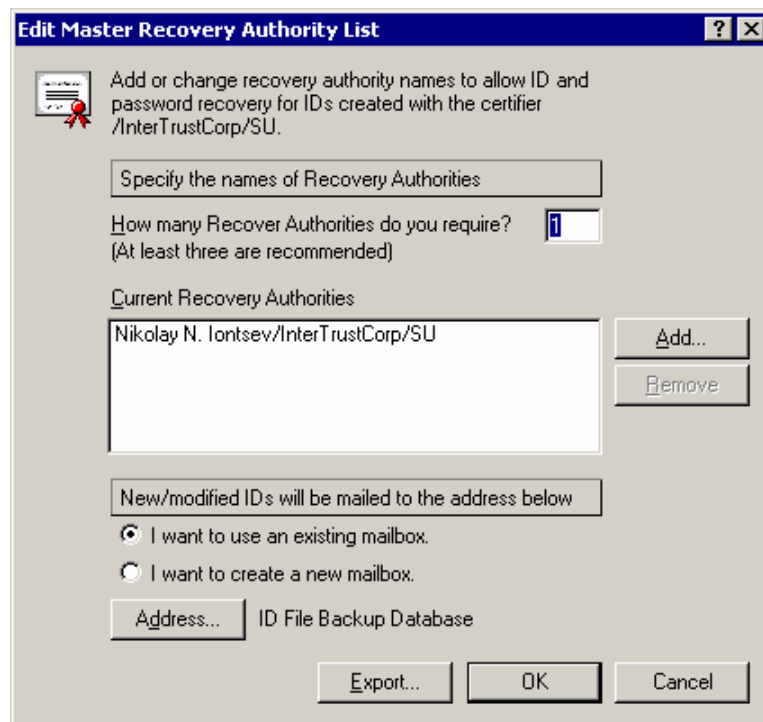


Рис. 228 Окно Edit Recovery Information

1.38.1.2. 1.1.1.2. Получение информации для восстановления ID-файлов для существующих ID-файлов

Операция 1. Администратор выполняет запрос на получение/обновление Recovery Information для существующего ID-файла:

- • В Domino Administrator перейдите на закладку Configuration.
- • Из меню Tools выберите Certification>Edit Recovery Information.
- • Откройте ID-файл сертификатора. Введите его пароль.
- • Выберите Export. Введите пароль ID-файла сертификатора.
- • Заполните поля для отправки запроса пользователю. Нажмите кнопку Send.

Операция 2. Пользователь «отвечает» на запрос:

- • Откройте почтовое сообщение от администратора.
- • Выберите в меню Actions>Accept Recovery Information. Введите пароль своего ID-файла.
- • Заполните поля для отправки информации для восстановления ID-файла в почтовую базу. Нажмите кнопку Send.

Important point(s)

- • Backup file information is automatically included in the body of the message sent by the administrator.
- • ID files with recovery information will be automatically backed up after any of the following major changes to the ID file:
 - • Initial registration
 - • Accepting new recovery information
 - • Generating a new public key
 - • Processing a name change
 - • Creating a new document encryption key

1.38.1.3. 1.1.1.3. Пользователь утратил пароль своего ID-файла и вынужден начать восстановление этого ID-файла

Операция 1. Действия пользователя:

- В R5 выберите в меню клиента File>Tools>Recover ID и выберите ID-файл, который надо восстановить.
- В R6 перезапустите клиента, введите пустой пароль в окне, а затем нажмите кнопку Recover Password и выберите ID-файл, который надо восстановить.

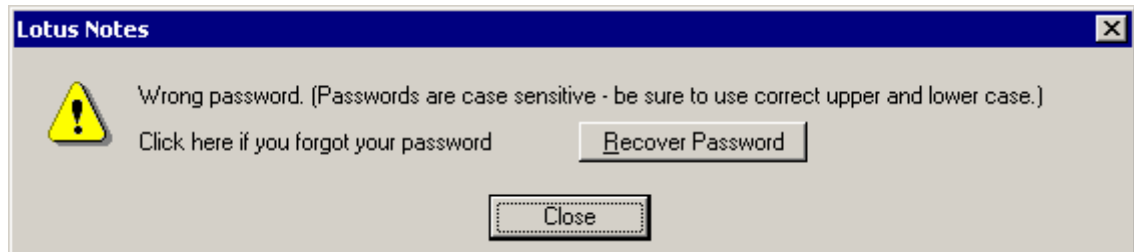


Рис. 229 Кнопка Recover Password

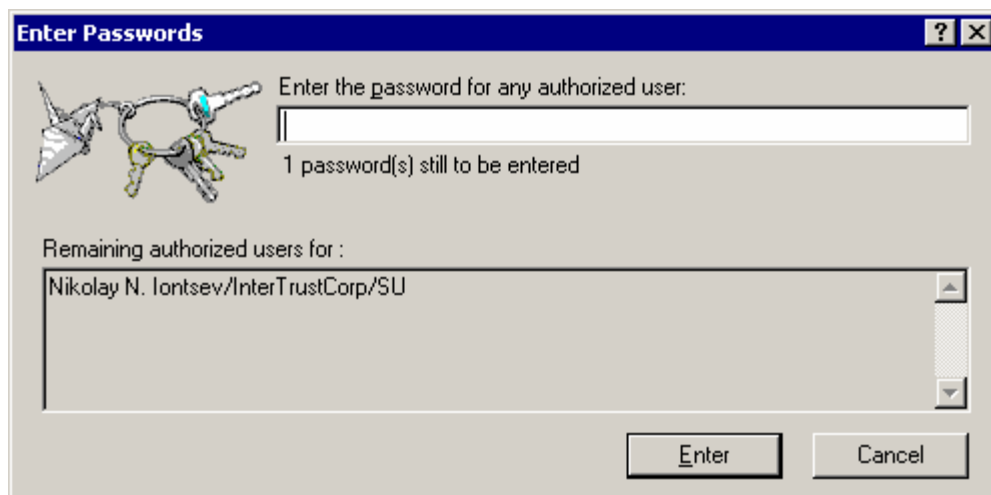


Рис. 230 В этом окне пользователь должен ввести пароли, полученные от авторизованных администраторов

- Вступите в контакт с администратором, имя которого указано в списке в полученном диалоговом окне. Он сообщит вам первый пароль для восстановления ID-файла (это не пароль самого ID-файла). Введите этот пароль в окне.
- Повторите предыдущий пункт нужное количество раз для других администраторов.
- В результате ID-файл перейдет в состояние задания для него нового пароля.

Операция 2. Действия авторизованного администратора по получению пароля для восстановления ID-файла пользователя:

- Отсоединить из созданной вами почтовой базы «последний по времени» файл с информацией для восстановления пароля этого пользователя на диск. Если файла в базе нет, взять вместо него копию ID-файла пользователя, для которой он забыл пароль.
- В Domino Administrator с закладки Configuration из меню Tools выбрать Certification>Extract Recovery Password.
- Выбрать отсоединенный на диск файл.
- Сообщить пользователю полученную в окне «цепочку цифр» (третья строка, после двоеточия).



Рис. 231 Окно Extract Recovery Password, пароль в третьей строке после двоеточия...

Important point(s)

Once an ID file has been recovered, users should:

- ● Regenerate the ID file recovery information by accepting new recovery information or re-accepting the recovery information previously sent by the administrator (чтобы пользователю «не пришлось кушать бумажку», на которой записан пароль восстановления).
- ● Generate a new Notes key pair to limit the chance of someone being able to use a stolen ID file.

1.39. 1.1. Server-Based Certification Authority и серверная программа CA Process (CA) в контексте ID-файлов сертификатов Notes

1.39.1. 1.1.1. Возможность выпуска сертификатов Notes с использованием Server-Based CA

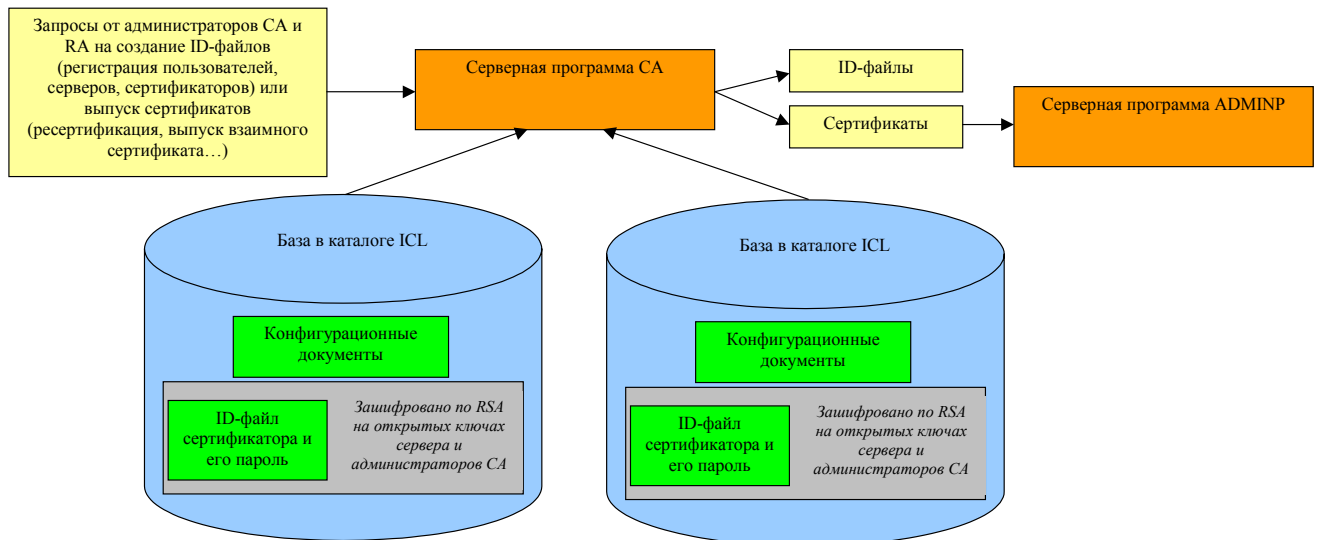


Рис. 232 Логика работы

1.39.2. 1.1.2. Миграция ID-файла сертификатора в Server-Based CA

Операция Certification-Migrate Certifier для ID сертификатов Notes

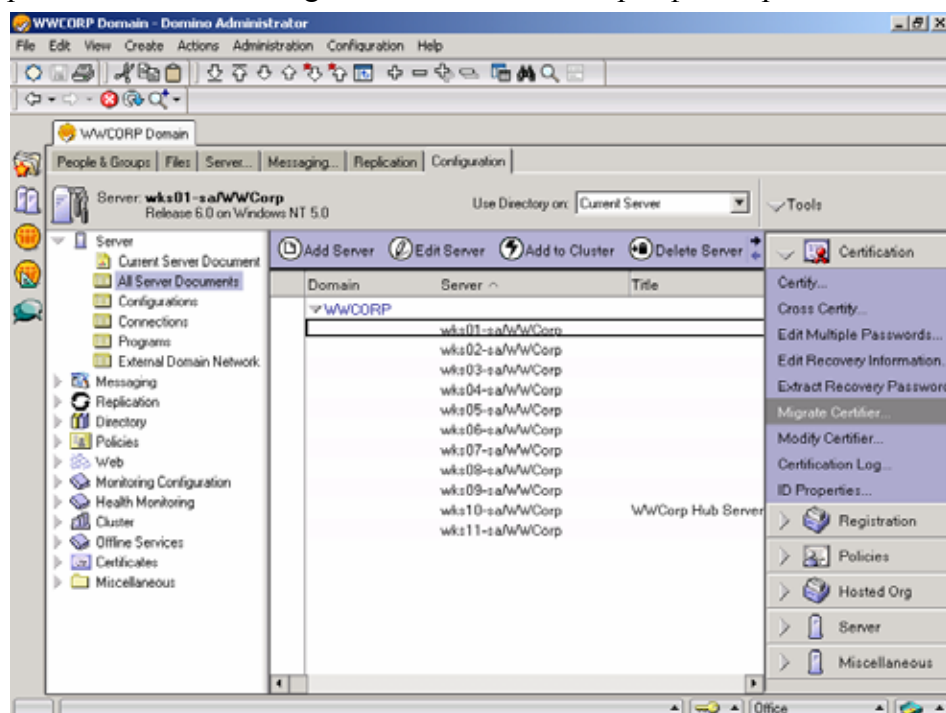


Рис. 233 Запуск процесса из клиента Администратора

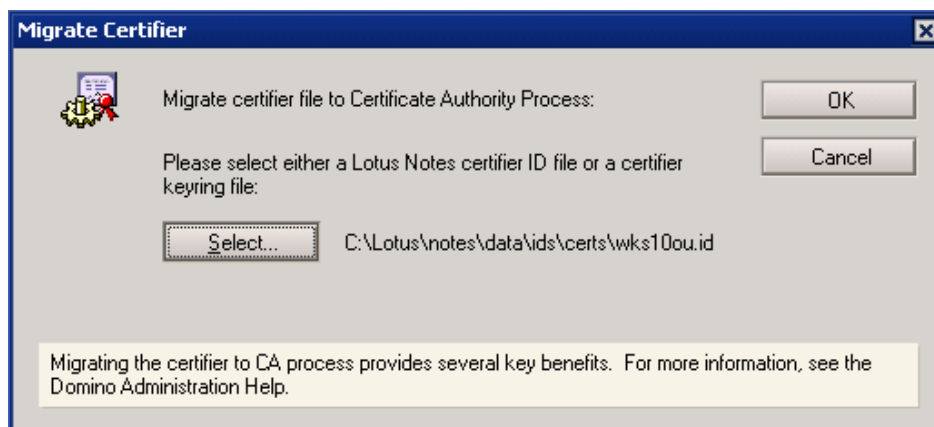


Рис. 234 Выбор мигрируемого ID-файла сертификатора (естественно, он должен быть предварительно создан)



Рис. 235 Ввод пароля

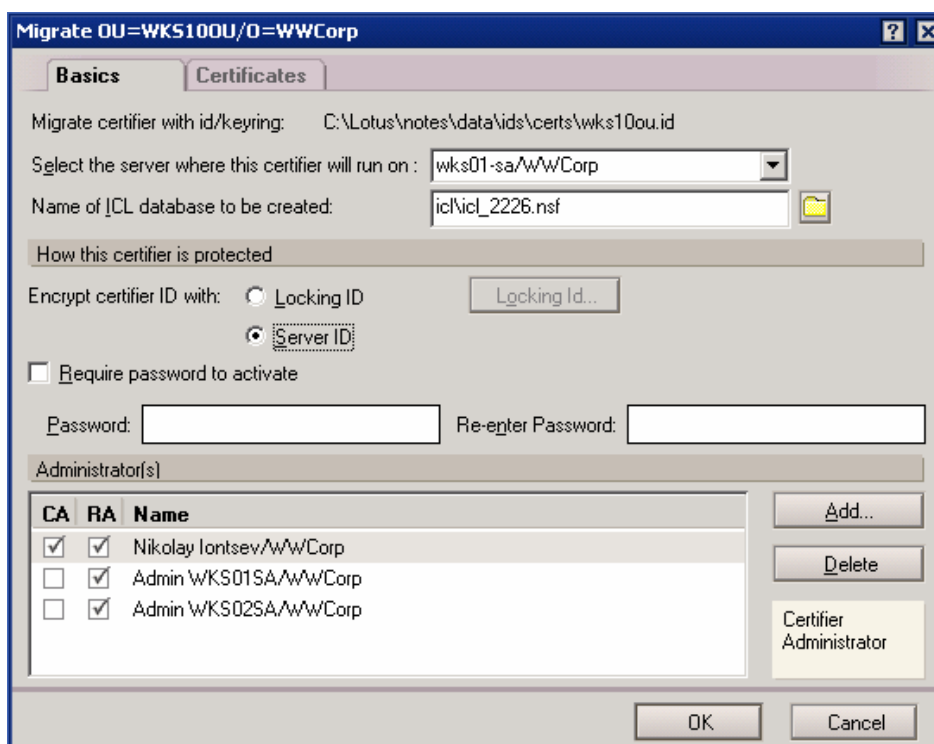


Рис. 236 Выбор сервера, на котором программа СА будет «поддерживать сертификатора», имени файла базы ICL, способа защиты (ID-файлом сервера без или с дополнительной опцией защиты паролем или специально созданным для этих целей ID-файлом), а так же списка администраторов СА и RA

Защита мигрированных ID-файлов сертификаторов паролем или ID-файлом с паролем

Option	Security level	Password required	Action required
Encrypt ID with	Lowest	None	None

Server ID			
Encrypt ID with Server ID + Password	Medium	Password	If you choose to encrypt the certifier ID with the server ID and password, you need to activate the certifier. Use the tell command: tell ca activate <password>
Encrypt ID with Lock ID	Highest	Registered user ID and password	If you choose to encrypt the certifier ID with a lock ID, the certifier is locked when you create it. Use the tell command: tell ca unlock <idfile><pass word>

Migrate OU=WKS100U/O=WWCorp

Basics | **Certificates**

Certificate Duration for EE Certificate

Default: 24 months
Minimum: 0 months
Maximum: 2400 months

Certificate Duration for CA Certificate

Default: 240 months
Minimum: 0 months
Maximum: 2400 months

The above settings apply to the certificate this certifier will issue.

OK Cancel

Рис. 237 Параметры выпускаемых сертификатов. EE (End-Entity) Certificate – сертификат для пользователя или сервера, CA (Certificate Authority) Certificate – сертификат для сертификатора

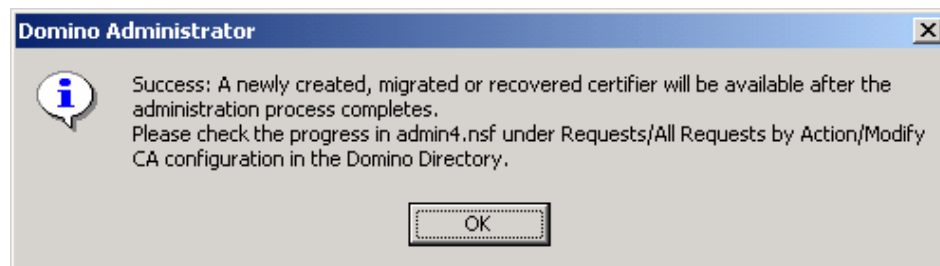


Рис. 238 Первый шаг миграции успешен, остается дождаться второго шага, выполняемого программой ADMINP

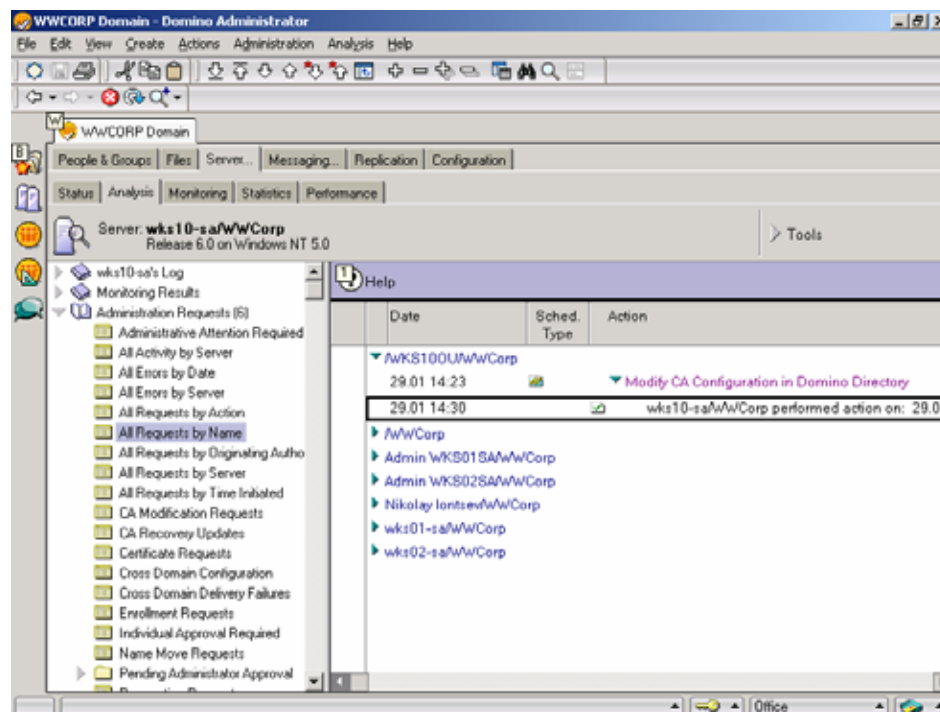


Рис. 239 ADMINP «мигрировала сертифицикатора»

1.39.3. 1.1.3. Изучение базы ICL и документа Certifier

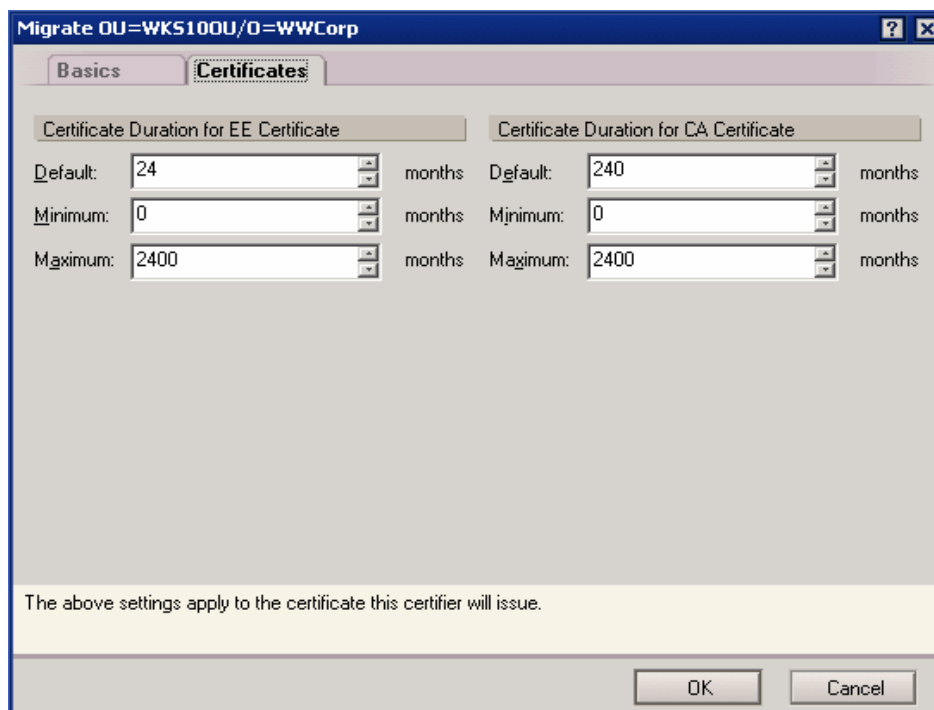


Рис. 240 Изучение изменившегося документа Certifier в каталоге Domino – закладка Basics

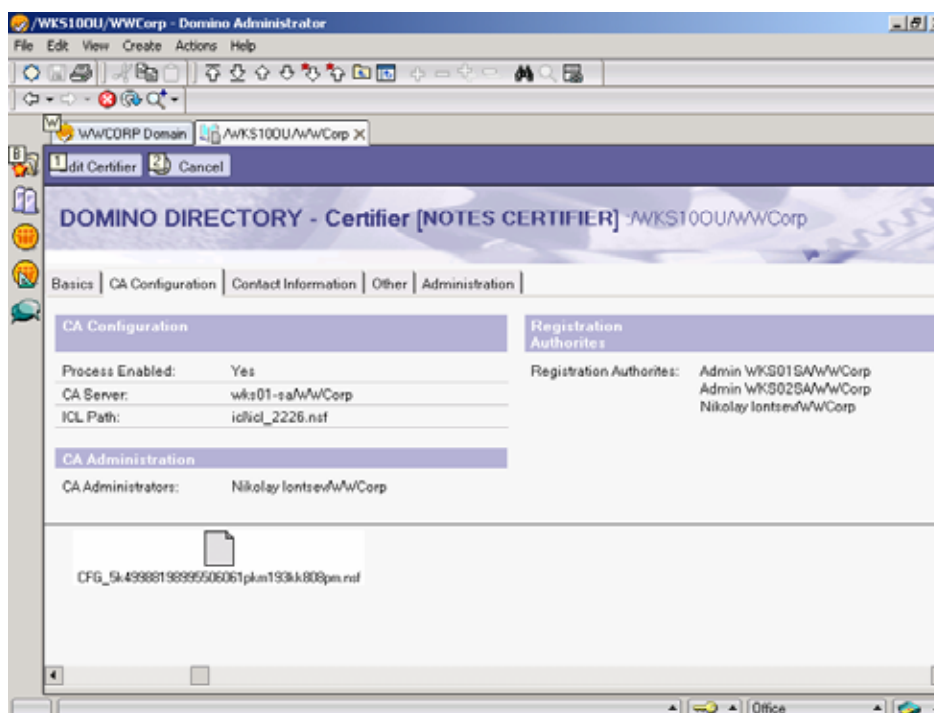


Рис. 241 Изучение изменившегося документа Certifier в каталоге Domino – закладка CA Configuration

1.39.4. 1.1.4. Ключи серверной программы CA Process и ее запуск

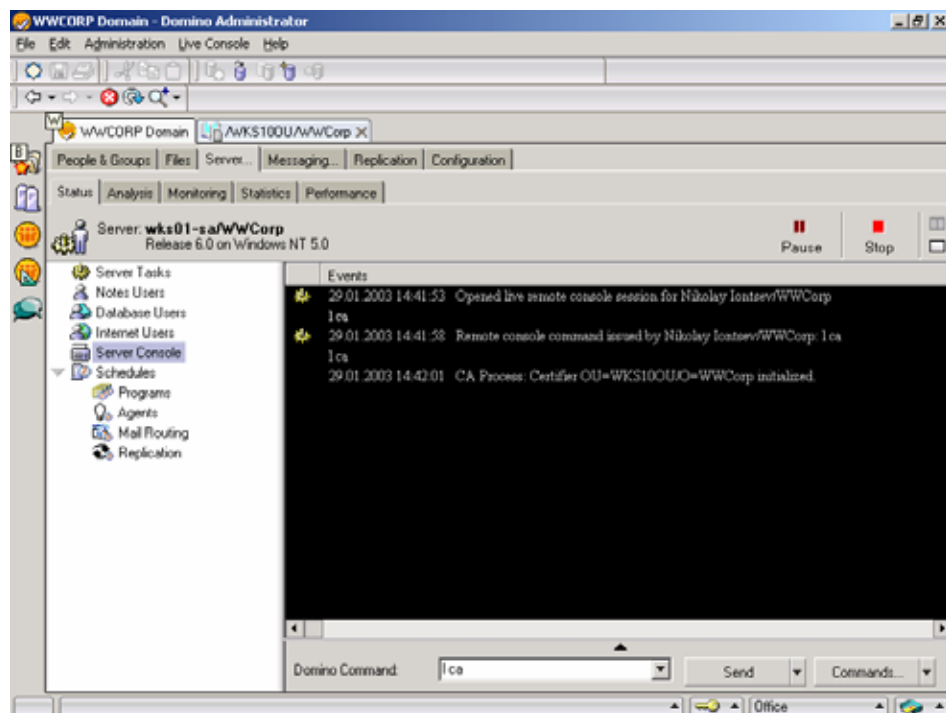


Рис. 242 Запуск программы СА

Команда	Результат
tell ca quit	Завершает программу СА.
tell ca stat	Displays summary information for the certifiers using the CA process; this includes the certifier's number, its hierarchical name, certifier type (Notes or Internet), whether it is active, and name of the ICL database.
tell ca show queue number	Display a list of pending certificate requests, revocation requests, and configuration modification requests for a specific certifier, using its number from the results of the "tell ca status" command. You can also use * to show this information for all certifiers that are using the CA process.
tell ca activate certifier number password	Activate a certifier if the certifier is created with "Require password to activate certifier," or use this for any certifier that has been deactivated. Activation is enabled during CA setup and creation. Activate a specific certifier by entering its number from the results of the 'tell ca status' command. Or you can actually unlock all server ID/password-protected certifiers at one time with this command, if you specify "*" for the certifier number. The CA process then prompts you for the password for each certifier.
tell ca deactivate certifier number	Deactivate a certifier. You will need to activate it again in order for it to process any request. Use * to deactivate everything, or deactivate a specific certifier by entering its number from the results of the 'tell ca status' command.
tell ca lock idfile	Lock all certifiers that were set up with a lock ID, as

	specified during CA setup.
tell ca unlock idfile password	Unlock all certifiers using the ID and password that comprise the lock ID. The lock ID is specified during CA setup.
tell ca CRL issue certifier number	Issue a non-regular CRL for a specific certifier, where certifier number is the number of the certifier specified in the results of the "tell ca status" command.
tell ca CRL push certifier number	Push a certifier's latest regularly scheduled CRL to the Domino Directory, where certifier number is the number of the certifier specified in the results of the "tell ca status" command.
tell ca CRL info certifier number [s/S/n/N]	Display CRL information for a specified certifier, where certifier number is the number of the certifier specified by the 'tell ca status' command. Use s or S for regularly scheduled CRLs, and n or N for non-regularly scheduled CRLs.
tell ca refresh	Force the CA process to refresh its list of certifiers. As a result: newly configured certifiers will be added to the CA process previously unlocked certifiers will need to be unlocked again previously activated certifiers may need to be activated again, if the activation password has changed the Notes certifier ID file in idstorage will be updated with the latest certificate information
tell ca help	List tell ca options

1.39.5. 1.1.5. Регистрация пользователя

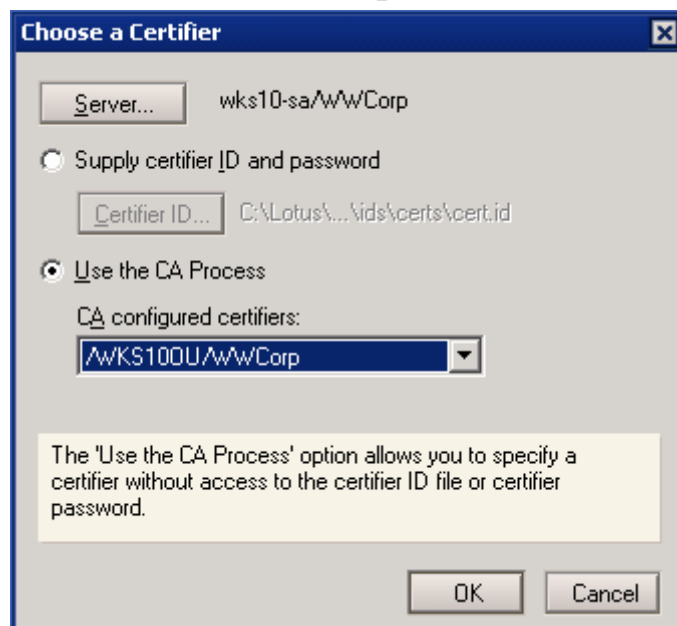


Рис. 243 Выбирается регистрация с использованием программы СА и соответствующий сертификат



Рис. 244 Мигрированный ID-файл сертификатора не содержит информации для восстановления забытых паролей – не существенно, но надо обеспечить

Register Person -- New Entry

Provide name, password and other basic information for the new person. To view/edit additional registration settings, check the 'Advanced' checkbox below.

Registration Server... wks10-sa/ww/Corp

First name: User Middle name: Userovich Last name: Userov Short name: UUserov

Password: 11111111 Mail system: Lotus Notes Explicit policy: (None Available)

Password Options...

No organization policy assigned to this person

Policy Synopsis...

☒ Create a Notes ID for this person

☒ Advanced New Person Migrate People... Import Text File... [Green Checkmark] [Red X]

Registration Queue (local):

User Name	Registration Status	Date

Register All Register Delete Options... Views... Done

Рис. 245 На закладке Basics никаких отличий

Register Person -- New Entry

Basics

Mail system: Lotus Notes Mail Server... wks10-sa/WW/Corp

Mail file name: mail\userov Mail file template: Lotus SmartSuite Library (6) Mail (R6) Microsoft Office Library (6) Personal Address Book Personal Journal (R6) TeamRoom (6)

☒ Create file now ☐ Create file in background

Mail File Replicas... About... mail6.ntf

Mail file owner access: Editor

☐ Create full text index ☐ Set database quota 0 MB ☐ Set warning threshold 0 MB

☒ Advanced New Person Migrate People... Import Text File... [OK] [Cancel]

Registration Queue (local):

User Name	Registration Status	Date

Register All Register Delete Options... Views... Done

Рис. 246 На закладке Mail никаких отличий

Register Person -- New Entry

Basics

Mail Internet Address Information

Internet address Internet Domain

UserUserov@intrust.ru intrust.ru

Address name format Separator

FirstName LastName None

Supply internet address format settings for the selected people or person. The Internet address is created using the person's name, the internet domain and internet address format components. It must be unique in the address book.

☒ Advanced New Person Migrate People... Import Text File... [OK] [Cancel]

Registration Queue (local):

User Name	Registration Status	Date

Register All Register Delete Options... Views... Done

Рис. 247 На закладке Address никаких отличий

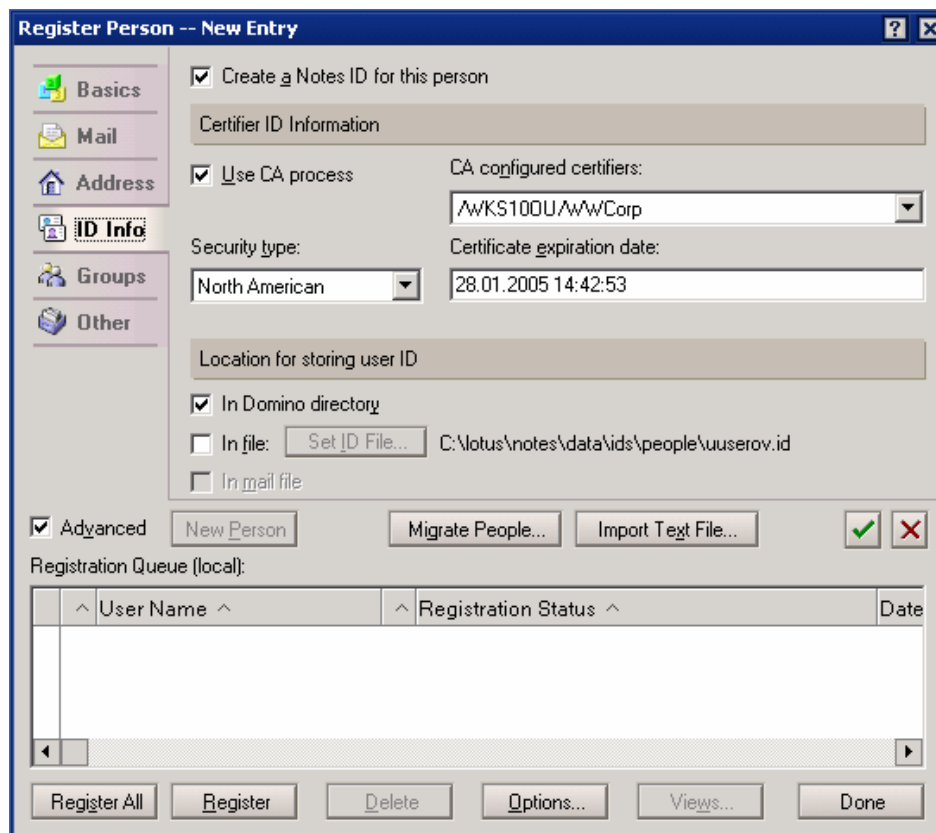


Рис. 248 Отличия только на закладке ID Info, далее никаких отличий нет

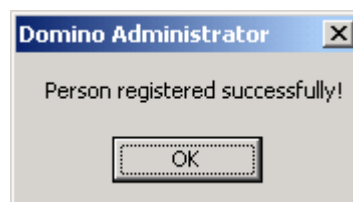


Рис. 249 Пользователь зарегистрирован

Чтобы регистрировать пользователей в Domino Web Administrator (база webadmin.nsf в браузере), сначала необходимо добавить сервер, содержащий эту базу webadmin.nsf, на роль RA для мигрированного сертификата. Сервер, через программу HTTP которого выполняется регистрация, может быть другим, нежели сервер, несущий программу CA. Для каждого сервера, через программу HTTP которого работают с базой webadmin.nsf, будут доступны только те мигрированные сертификаты, для которых этот сервер назначен на роль RA.

1.39.6. 1.1.6. Операция Certification-Modify Certifier в контексте ID сертификатов Notes

1.39.6.1. 1.1.6.1. Domino Directory

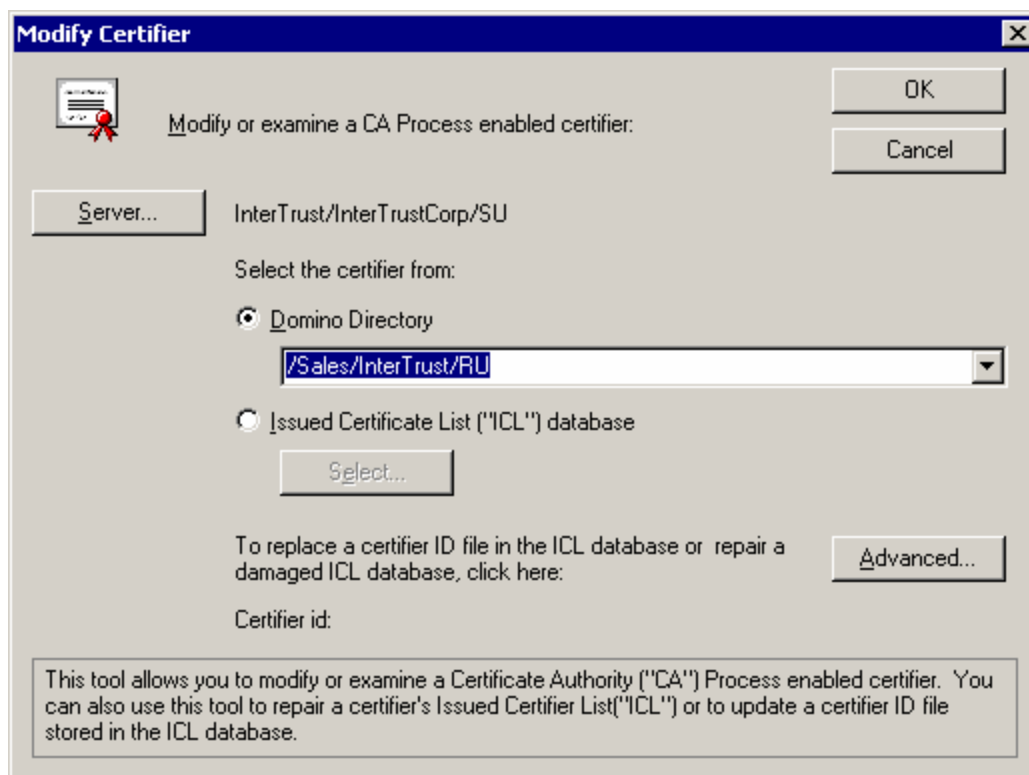


Рис. 250 Ok

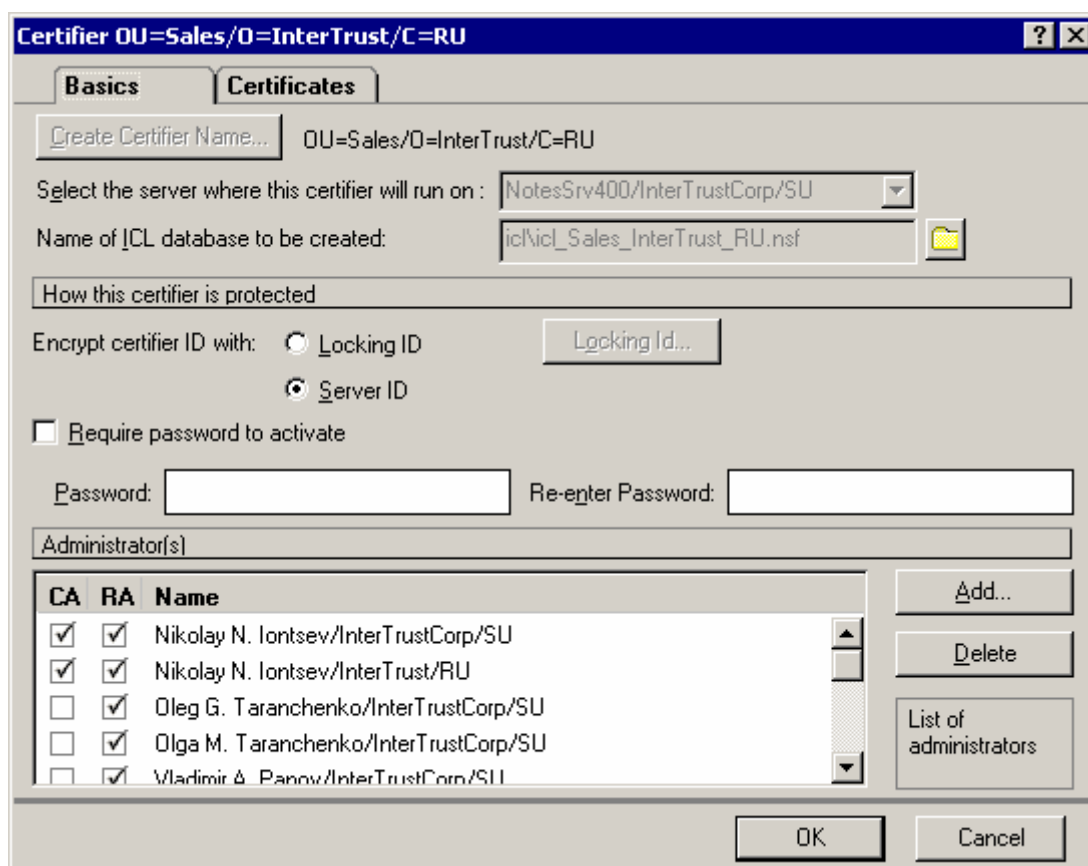


Рис. 251 Можно управлять составом админов CA и RA и менять способ защиты ID-файла сертификатора

Certifier OU=Sales/O=InterTrust/C=RU [?] [X]

Basics | **Certificates**

Certificate Duration for EE Certificate		Certificate Duration for CA Certificate			
Default:	24	months	Default:	240	months
Minimum:	0	months	Minimum:	0	months
Maximum:	2400	months	Maximum:	2400	months

The above settings apply to the certificate this certifier will issue.

OK Cancel

Рис. 252 Можно изменить параметры по умолчанию

1.39.6.2. 1.1.6.2. ICL...

Modify Certifier [X]

 Modify or examine a CA Process enabled certifier:

OK Cancel

Server... NotesSrv400/InterTrustCorp/SU

Select the certifier from:

☐ Domino Directory

[None Assigned]

☒ Issued Certificate List ("ICL") database

Select... ic\icl_Sales_InterTrust_RU.nsf

To replace a certifier ID file in the ICL database or repair a damaged ICL database, click here: **Advanced...**

Certifier id: C:\Lotus\Notes\Data\ids\certs\Sales_InterTrust_RU.id

This tool allows you to modify or examine a Certificate Authority ("CA") Process enabled certifier. You can also use this tool to repair a certifier's Issued Certifier List("ICL") or to update a certifier ID file stored in the ICL database.

Рис. 253 Select + Advanced

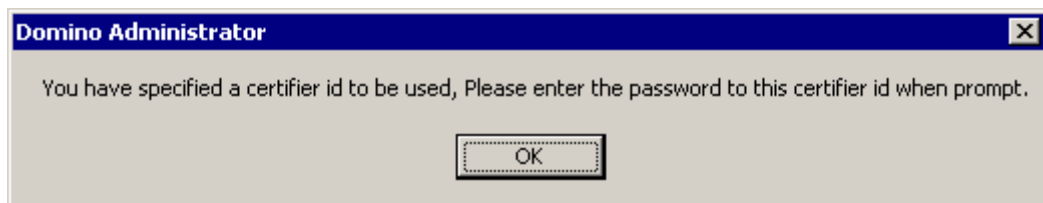


Рис. 254

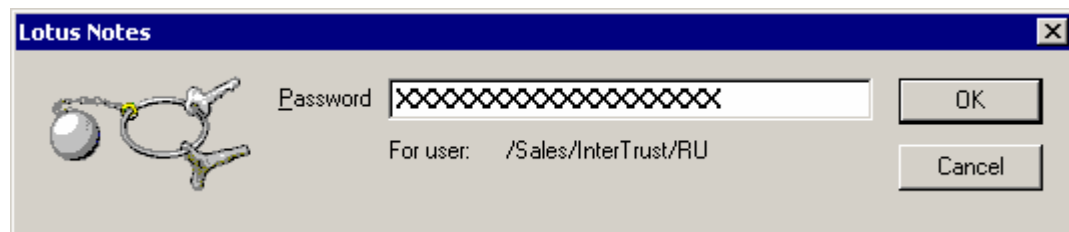


Рис. 255

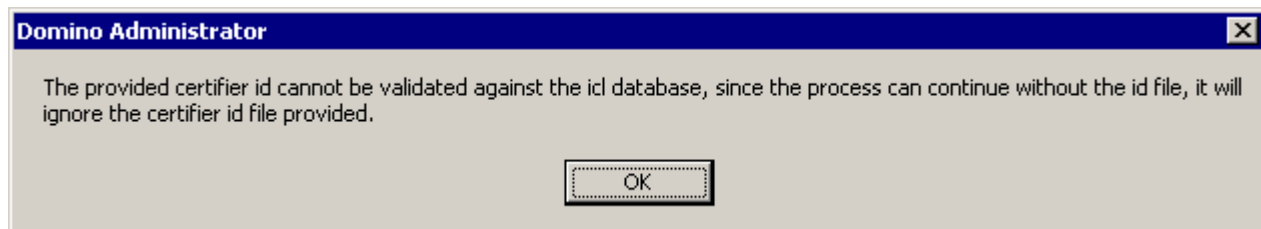


Рис. 256 Увы, далее окно Рис. 251 и Рис. 252...

1.40. 1.1. Подробности регистрации серверов

- • Операция Registration-Server
- • Регистрация без использования и с использованием CA Process

1.41. 1.1. Подробности регистрации пользователей

- • Операция Registration-Person
- • Опции регистрации пользователя
- • Регистрация без использования и с использованием CA Process

1.41.1. 1.1.1. Регистрация пользователей «из файла»

Order	Parameter	Enter
1	Last name	The last name of the user. This parameter is required.
2	First name	The first name of the user.
3	Middle initial	The middle initial of the user.
4	Organizational unit	A name for another level to add to the hierarchical name. This name distinguishes between two users who have the same name and are certified by the same certifier.
5	Password	A password for the user. This parameter is required.
6	ID file directory	The directory in which you want to store the user's ID. You can store the ID in this directory in addition to or instead of as an attachment in the Domino Directory. You must create the directory before registration. For this parameter to take effect, select the In File option on the ID Info panel for storing the user ID. This parameter overrides the default ID directory shown in the Register Person - New Entry dialog box.
7	ID file name	The name you want to assign to the ID file. This file name applies only if you store an ID in an ID file directory. If you do not specify a user ID file name, the name on the ID is based on the person's name.
8	Mail server name	The name of the user's mail server. This parameter overrides the one you select during registration.
9	Mail file directory	The mail file directory for the user.
10	Mail file name	The name for the user's mail file. If you do not use this parameter, the name is based on the person's name if the person uses Notes mail.
11	Location	Descriptive location information that is added to the user's Person document. If someone addresses mail to this user and there is another user with the same name, Notes displays the location to help the sender distinguish the two users.
12	Comment	An identifying comment that is added to the user's Person document.
13	Forwarding address	The full route to the user -- for example, JSmith@acme.com. If you don't enter this information in the text file, you can edit the Forwarding address field in the user's Person document. This parameter is required for Other and Other Internet mail users.
14	Profile	The name of the user setup profile.
15	Local administrator	The name of a user who has Author access to the Domino Directory. This person can modify the user's Person document.
16	Internet address	The Internet address of the user. This parameter is required for Lotus Notes, POP3, iNotes, and IMAP mail.
17	Short name	This name is entered by default. A short name is used to create a return Internet address if the Internet address is not entered.
18	Alternate name	The alternate name of the user. Note that the certifier ID used to register this user must contain the alternate name language.
19	Alternate org unit	A word that distinguishes two users who have the same name and are certified by the same certifier ID. Note that the certifier ID used

		to register this user must contain the alternate name language.
20	Mail template file	The file name of the mail template you want to use.

Пример файла:

```
Ivanov;Ivan;I.;;password1;;;Sales/InterTrust/RU;;;;;;Иванов Иван
Иванович;;inotes6.ntf
Petrov;Petr;P.;;password2;;;Sales/InterTrust/RU;;;;;;Петров Петр
Петрович;;inotes6.ntf
Sidorov;Sidor;S.;;password3;;;Sales/InterTrust/RU;;;;;;Сидоров Сидор
Сидорович;;inotes6.ntf
```

Рис. 257 Import Text File

Рис. 258 Выбор файла

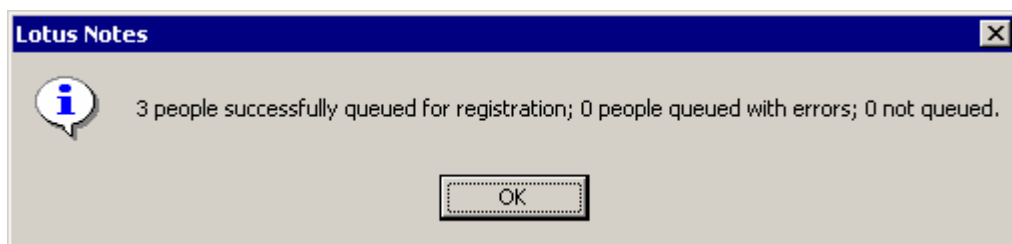


Рис. 259 Подтверждение о загрузке

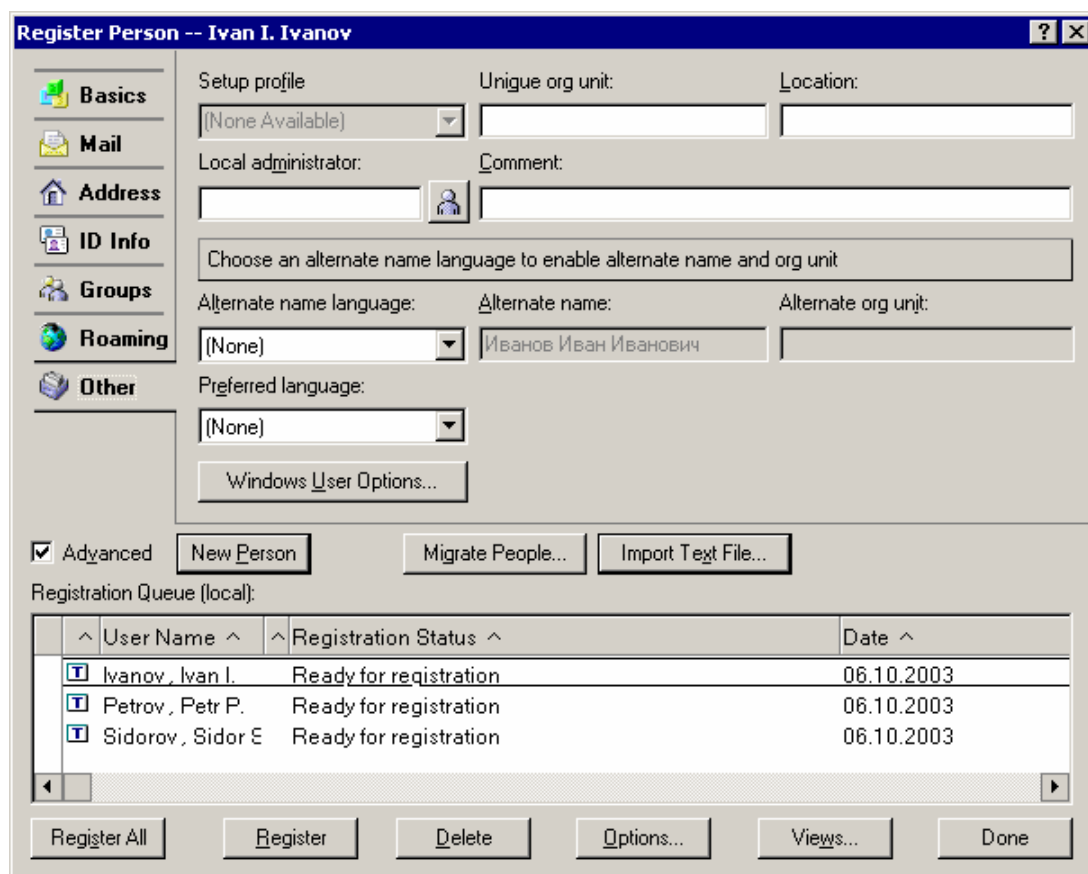


Рис. 260 Анализ того, что загрузилось, и затем кнопка Register All

1.41.2. 1.1.2. «Миграция» пользователей

В R6 имеется возможность мигрировать пользователей из cc:Mail, Microsoft Mail, Microsoft Exchange, Windows NT Domain, Microsoft Active Directory, LDIF File и LDAP Directory Server (кнопка Migrate People в окне регистрации).

Кроме того, имеются средства для миграции Personal Mail Data (программа NUPGRADE.EXE в каталоге клиента администратора):

- • cc:Mail — NUPGRADE.EXE 1
- • Microsoft Mail — NUPGRADE.EXE 2
- • Microsoft Exchange — NUPGRADE.EXE 3
- • Microsoft Outlook Express — NUPGRADE.EXE 4

В классе по желанию слушателей можно продемонстрировать миграцию пользователей и групп из Microsoft Active Directory и с LDAP-сервера. Подробности миграции из других систем описаны в [Upgrade Guide](#) и в Lotus Domino Administrator 6 Help.

1.42. 1.1. Управление пользователями Notes на основе политик

Для упрощения администрирования в R6 введен механизм политик.

1.42.1. 1.1.1. Тип и состав политики

Политики бывают двух типов:

- • **Explicit** – «явные». Такая политика может применяться к/назначаться пользователю в его документе Person
- • **Organizational** – «организационные» - основанные на дереве имен организации. Без явного назначения они применяются ко всем пользователям этой оргединицы и всем ее «политикам-потомкам».

Политики состоят из наборов параметров (Settings) – «субполитик».

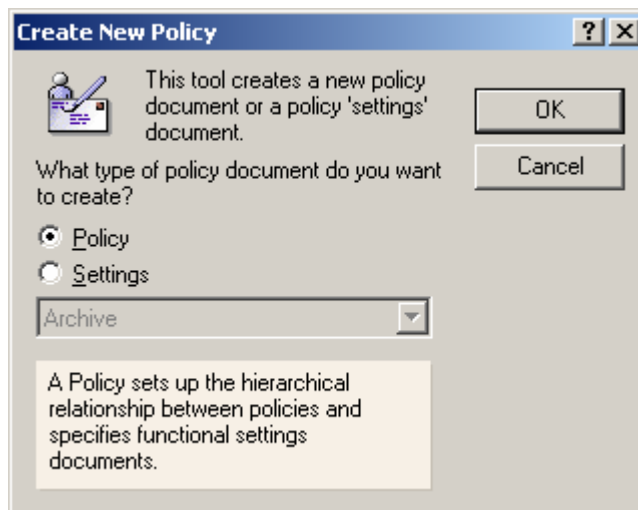


Рис. 261 Окно Tools-Policies-Create

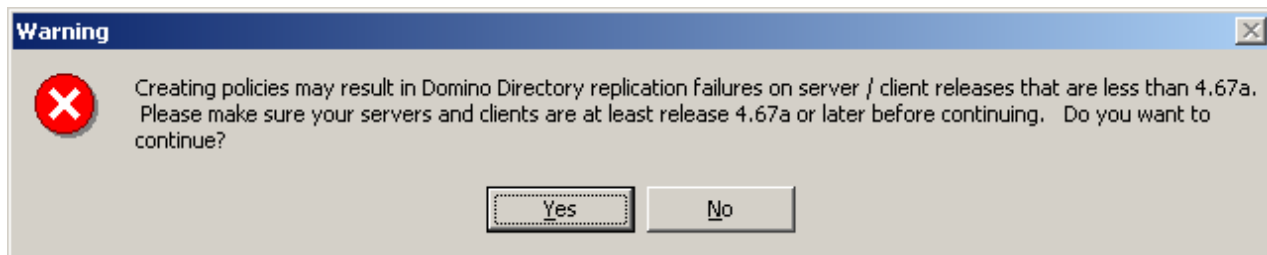


Рис. 262 Предупреждение – все серверы и клиенты должны быть $\geq 4.67a$

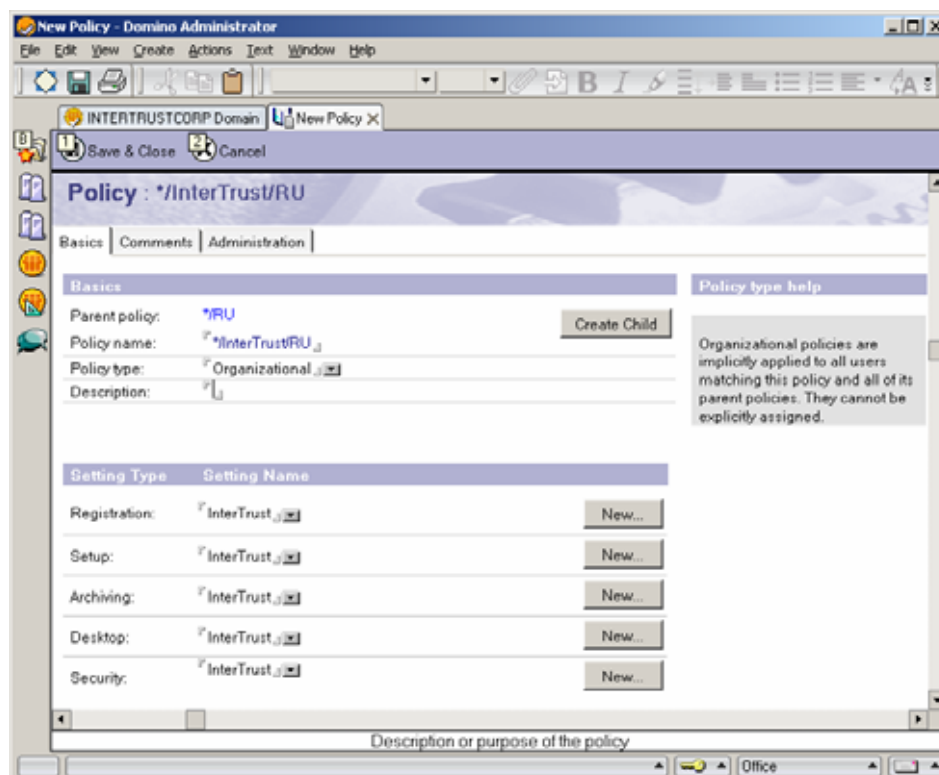


Рис. 263 «Организационная» политика и ее субполитики

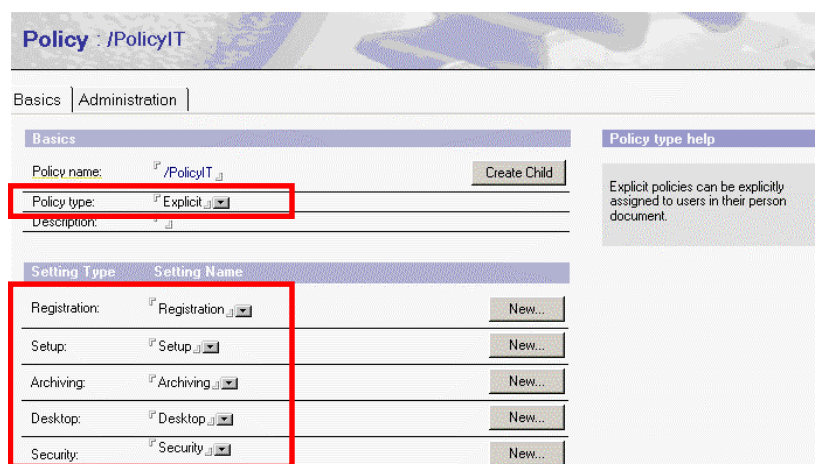


Рис. 264 «Явная» политика и ее субполитики

1.42.2. 1.1.2. Разновидности наборов параметров (Settings) – «субполитик»

Субполитики бывают пяти разновидностей:

- • **registration** - по поводу регистрации (статика)
- • **setup** - по поводу установки клиента: параметры настройки, документы в локальной адресной книге и т.п. (статика)
- • **archiving** - на предмет архивирования почтового ящика (динамика)
- • **desktop** - по поводу пользовательского рабочего пространства - обеспечивает полное управление клиентскими bookmarks и homepage (динамика)
- • **security** - на тему сложности, смены и синхронизации паролей и управления ECL клиентов (динамика)

«Организационные» политики автоматически применяется к пользователю в зависимости от иерархии его имени. Так, для пользователя Test T

Testikovsky/Sales/InterTrust/RU эффективная политика наследуется от следующих политик:

- */InterTrust/RU
- */Sales/InterTrust/RU

Явная политика явно назначается пользователю или группе и имеет приоритет над организационной.

- Пользователю - People&Groups - People - Assign Policy...
- Группе - то есть каждому ее члену - People&Groups - Groups - Assign Policy...

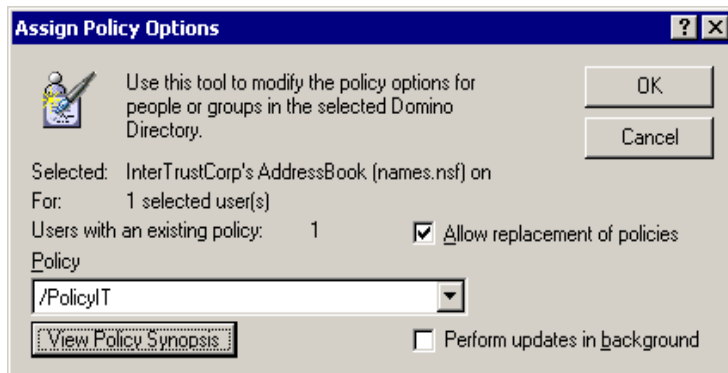


Рис. 265 Назначение «явной» политики пользователю

Назначенная пользователю явная политика заносится в документ Person.

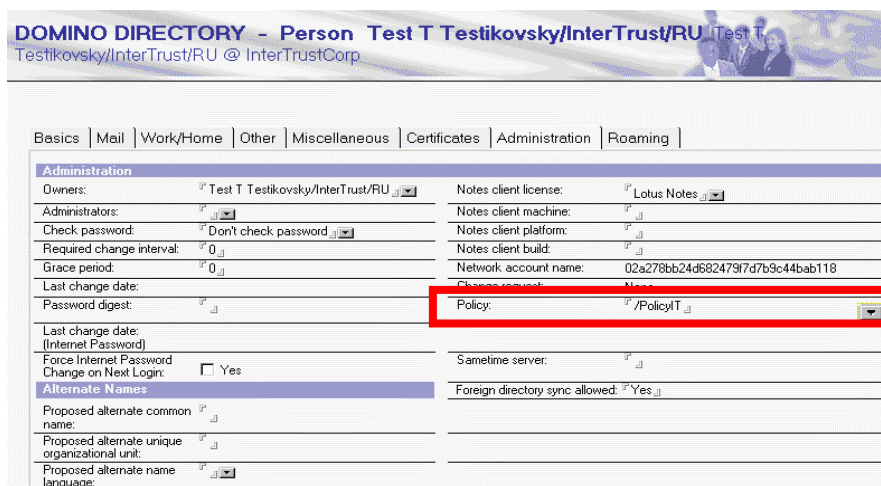


Рис. 266 Назначение «явной» политики пользователю в документе Person

1.42.3. 1.1.3. Наследование параметров политик

Параметр (суб)политики может:

- быть определенным в данной политике (Inherit from parent policy и Enforce in child policies не выбраны)
- явно наследоваться из родительской политики (выбран Inherit from parent policy)
- явно быть «навязан» в данной политике для всех ее дочерних политик (выбран Enforce in child policies)

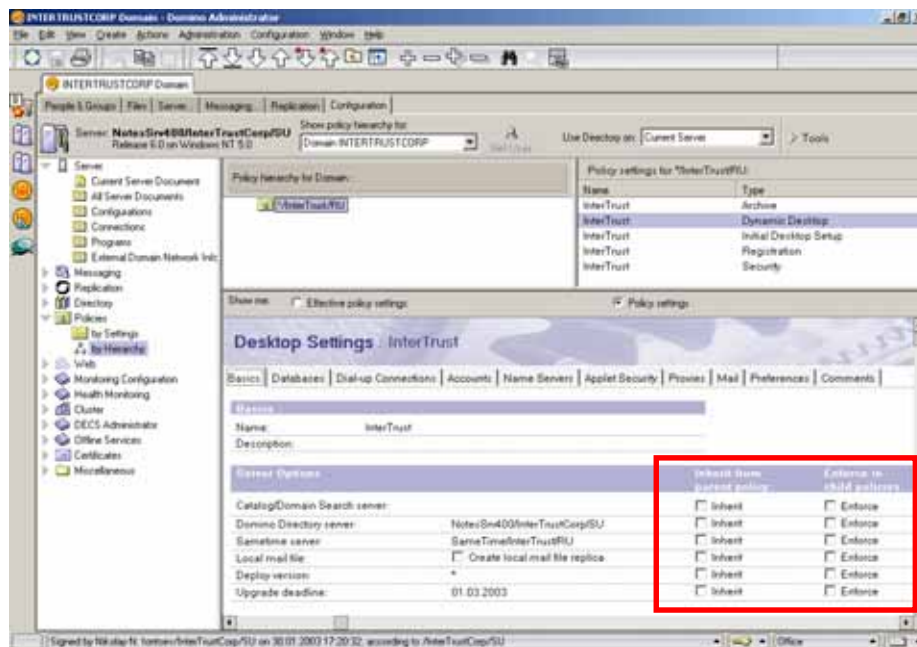


Рис. 267 Наследование параметров политик

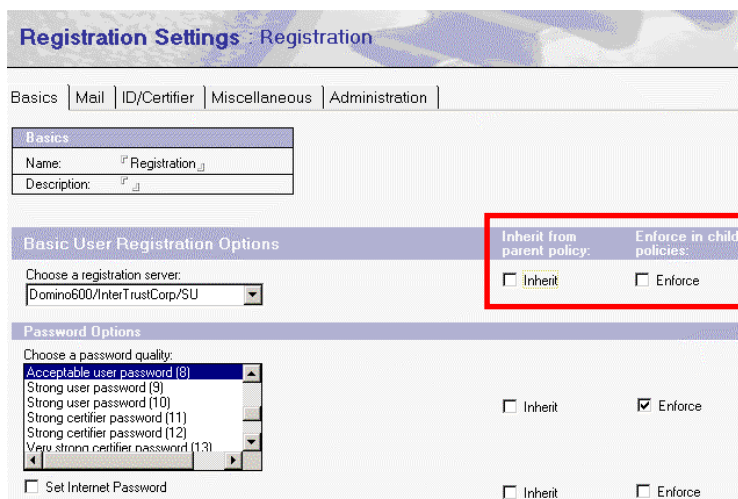
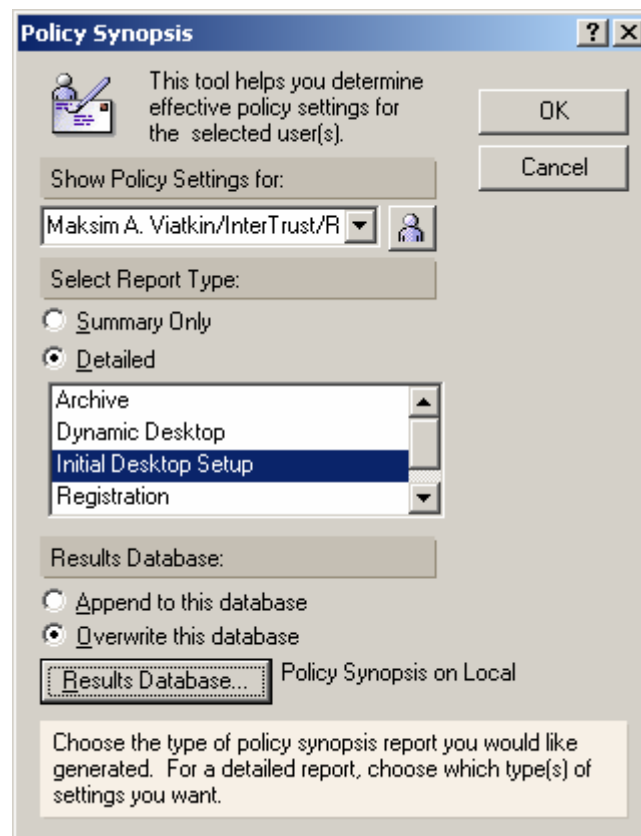


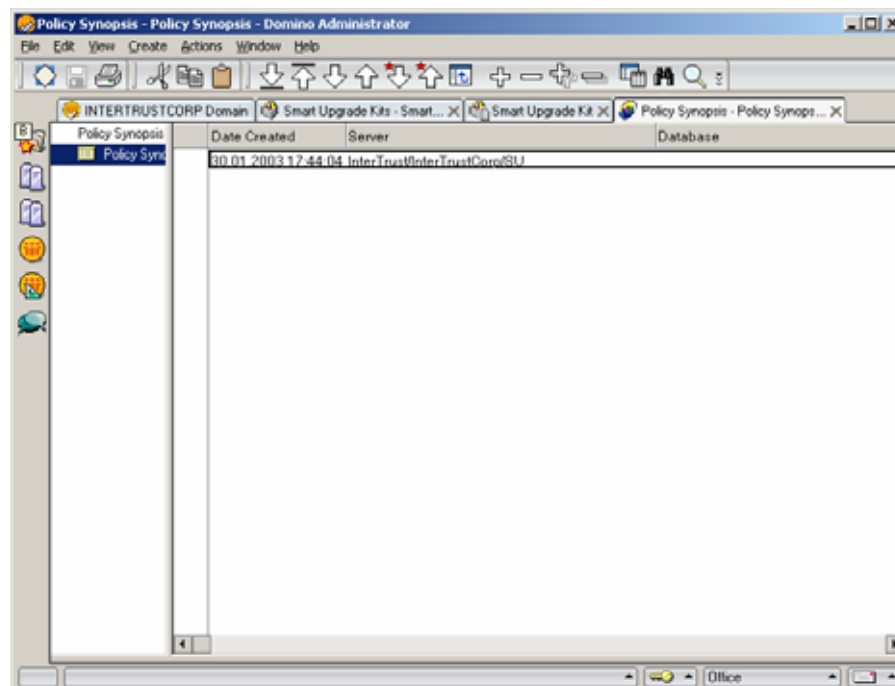
Рис. 268 Наследование параметров политик

1.42.4. 1.1.4. Policy Synopsis для пользователя

Поскольку параметры политик наследуются и зачастую трудно оценить результат наследования, встает вопрос о вычислении «эффективной» (получившейся в результате наследования) политики по отношению к конкретному пользователю.



Puc. 269 Tools – People - Policy Synopsis



Puc. 270 Baza Policy Synopsis

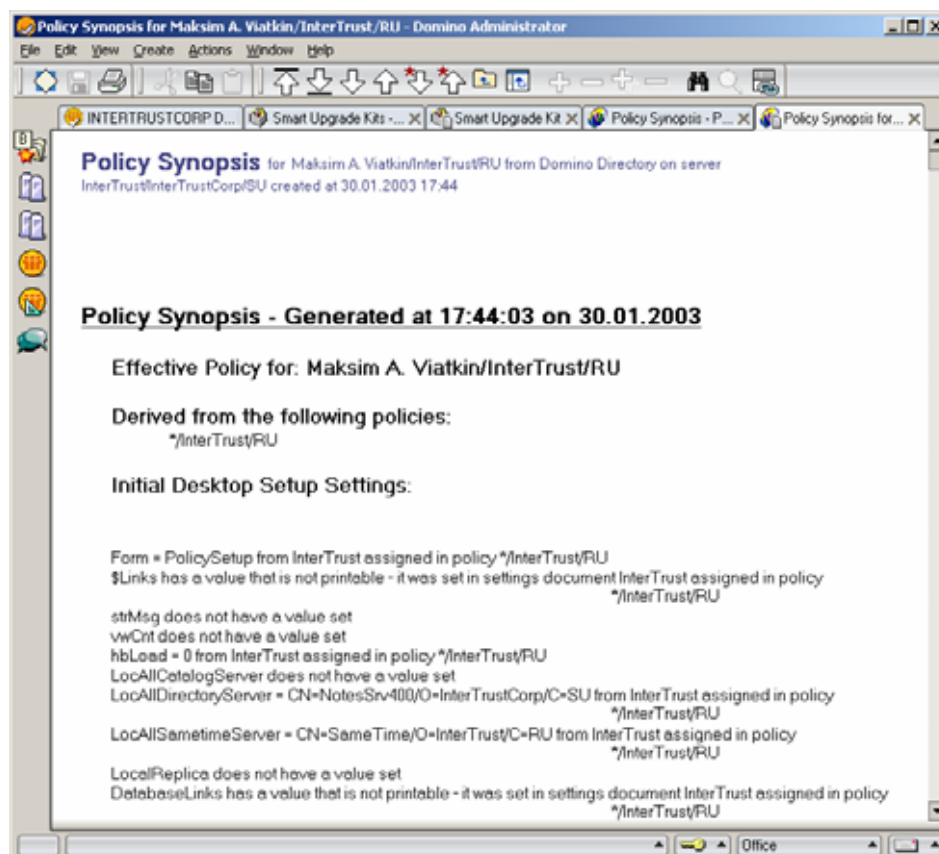


Рис. 271 Документ в базе

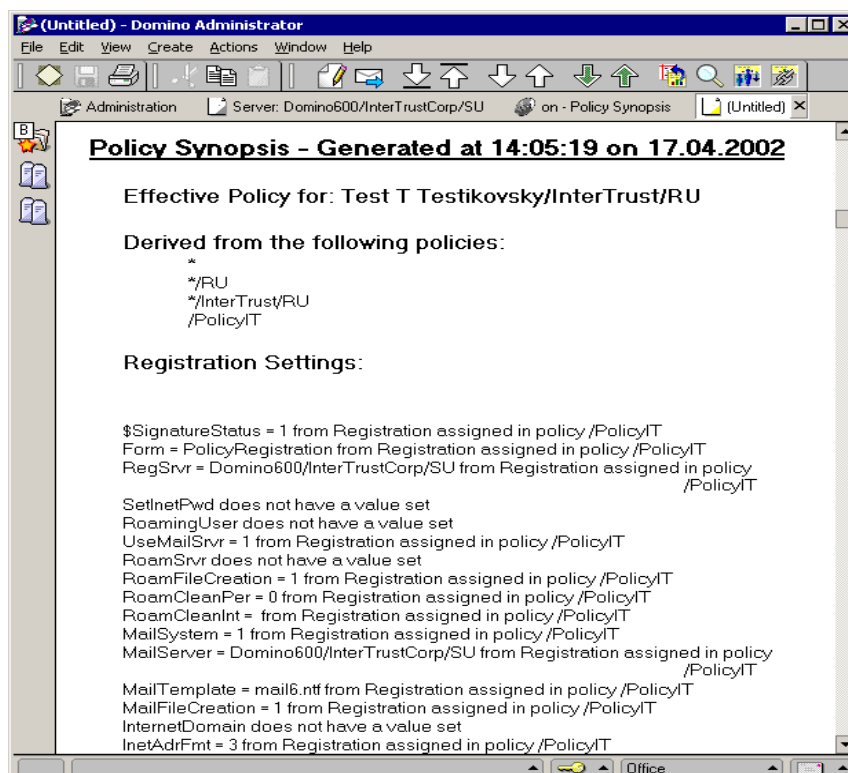


Рис. 272 Еще один документ. Упоминание несуществующих «политик» * и */RU – «глюк» ранних версий

1.42.5. 1.1.5. Пример синхронизации паролей Notes и Internet с использованием политики

Создайте организационную политику для оргединицы в Вашей организации, например /OU2/WKSXXSAOU/WWCorp.

Создайте субполитики, в частности типа Security.

Далее желательно достичь следующего:

- ● Синхронизация паролей Notes и Internet (учебный пример, для рабочего применения не рекомендуется).
- ● Устанавливается в субполитике Security, закладка Password Management, поле Update Internet Password When Notes Client Password Changes.
- ● Для проверки в клиенте Notes переключитесь на ID Вашего пользователя (из /OU2/WKSXXSAOU/WWCorp),
 - ● смените в документе Person пароль в поле Internet Password на password1,
 - ● затем смените пароль в ID на password2 (File, Security, User Security...),
 - ● выйдите из всех клиентов,
 - ● запустите броузер и попробуйте открыть клиентский почтовый ящик - должен «сработать» password2.
- ● Создайте явную политику с уникальным именем, используя ту же субполитику Security, и примените ее ко второму пользователю. Попробуйте повторить предыдущий эксперимент.
- ● Рассмотрите вычисление эффективных политик.

1.43. 1.1. Поддержка нескольких пользователей на одном компьютере (Shared Clients)

- • Обеспечивает персонализированную среду на совместно-используемых компьютерах
- • Дает возможность многим пользователям совместно использовать один компьютер
- • Допустимо только для «чистого» клиента Notes (не клиента Designer или Administrator)
- • Используется стандартная возможность Windows 2000/XP иметь для каждого пользователя компьютера свое «рабочее пространство»:
 - • Каталог программ **\Program Files\Lotus\Notes** содержит общие для всех пользователей программы, DLL и др. файлы; там нет баз и шаблонов (*.nsf, *.ntf)
 - • Общая для всех пользователей часть каталога данных **\Documents and Settings\All Users\Application Data\Lotus\Notes\Data** содержит «стартовый» notes.ini, общие базы и шаблоны (agentrunner.nsf, readme.nsf, \help*.nsf, *.ntf)
 - • Личная часть каталога данных **\Documents and Settings\UserName\Local Settings\Application Data\Lotus\Notes\Data** содержит данные конкретного пользователя UserName (notes.ini, user.id, bookmark.nsf, journal.nsf, headline.nsf, log.nsf, names.nsf)
- • Необходим соответствующий выбор на первой фазе установки клиента Notes
- • Для каждого нового пользователя при первом запуске клиента выполняется вторая фаза установки («стартовый» notes.ini), что создает личную часть каталога данных
- • Совмещение Roaming User и MultipleUser Installation поддерживается и дает новых полезных вариантов...

1.43.1. 1.1.1. Установка клиента – фаза 1 (Install)

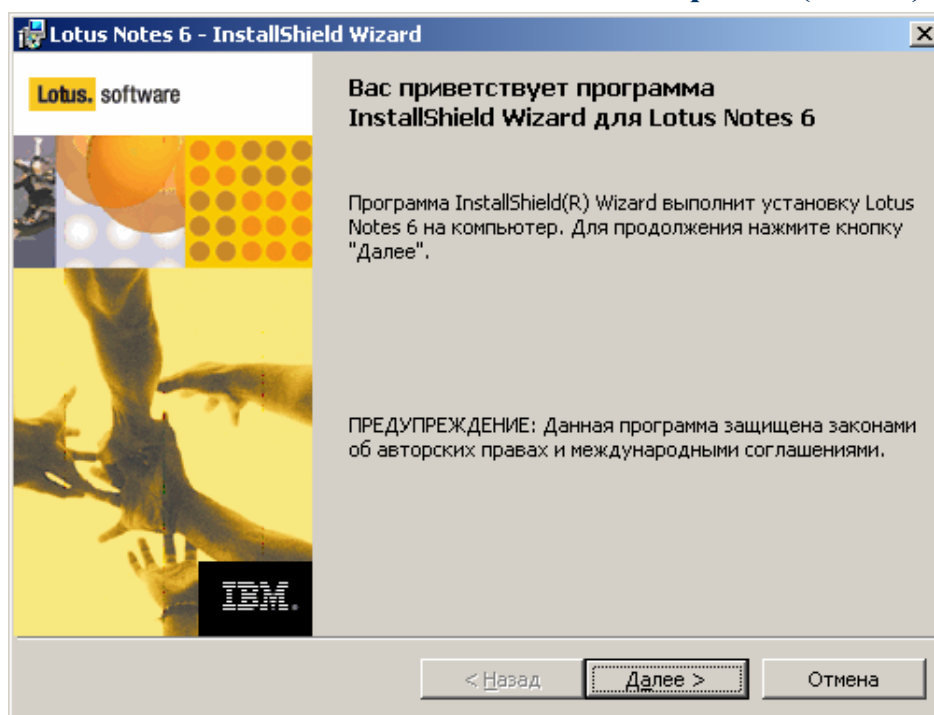


Рис. 273 Пользователь Win2000-XP под экауном ADMIN, позволяющим устанавливать новые программы и изменять реестр, начинает первую фазу установки

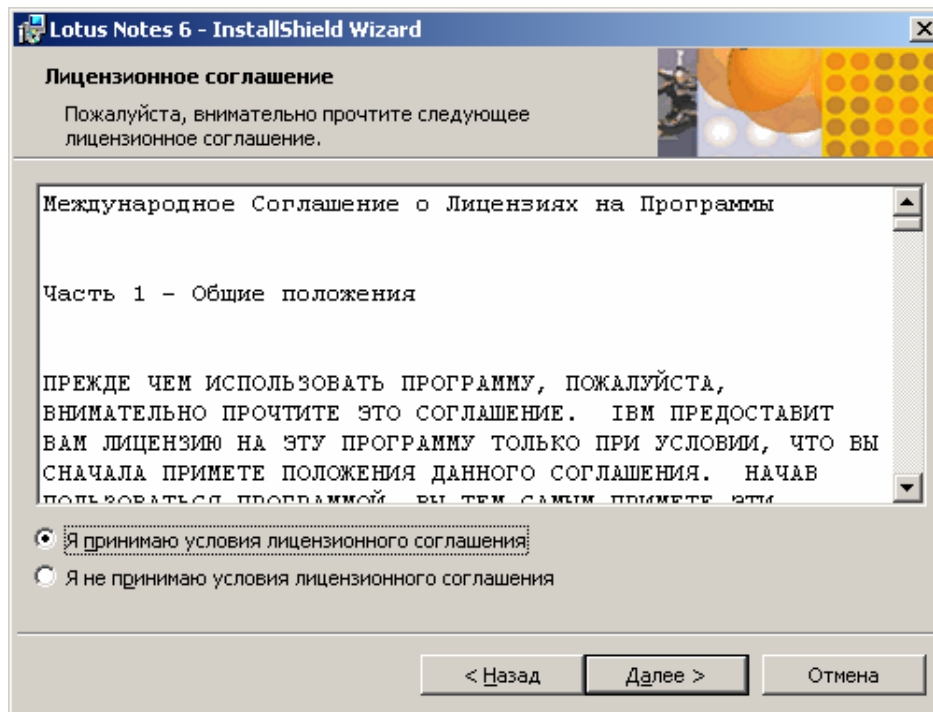


Рис. 274

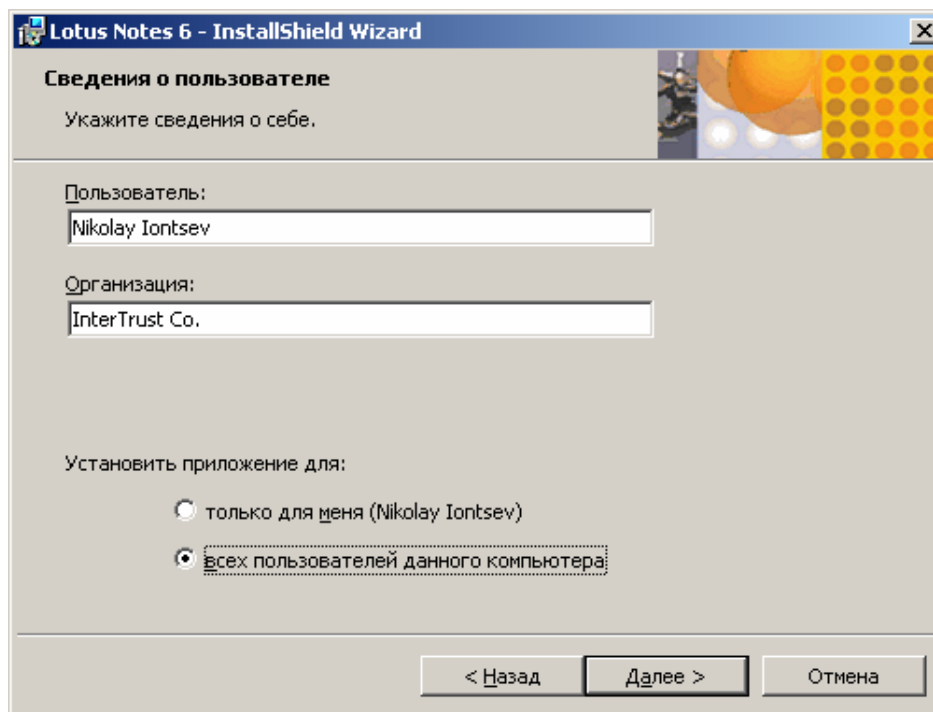


Рис. 275

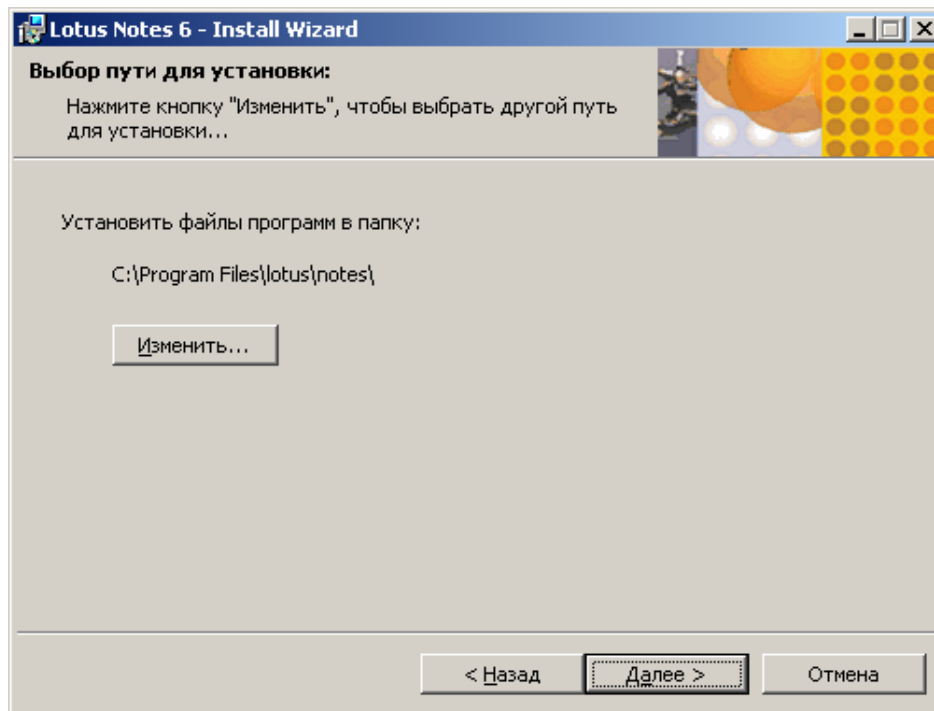


Рис. 276 Определен каталог программ

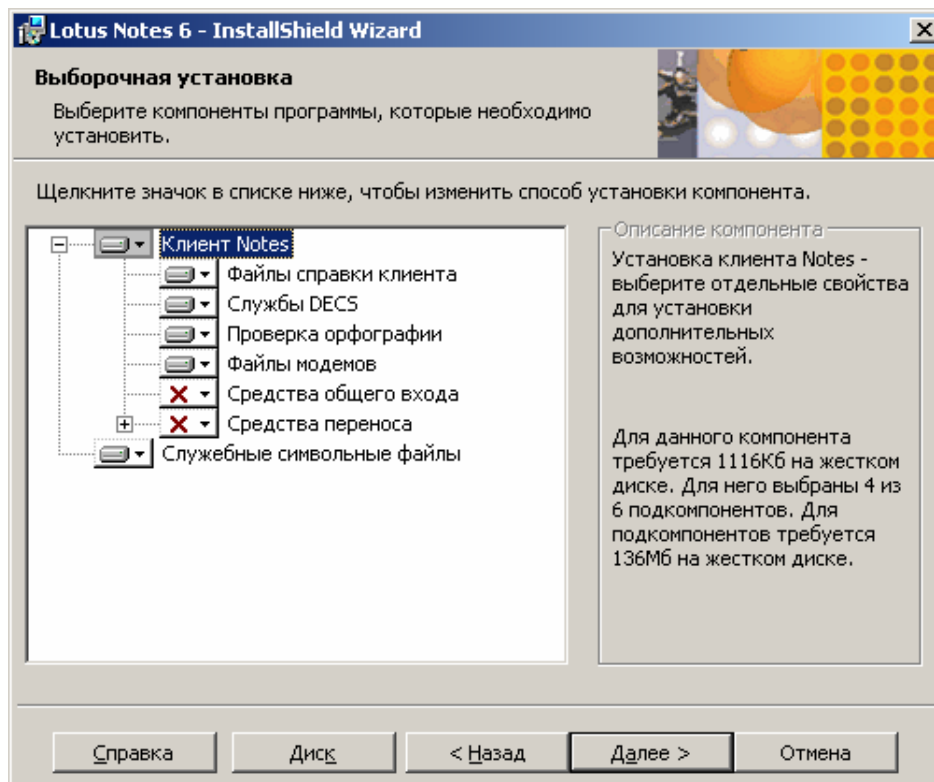


Рис. 277

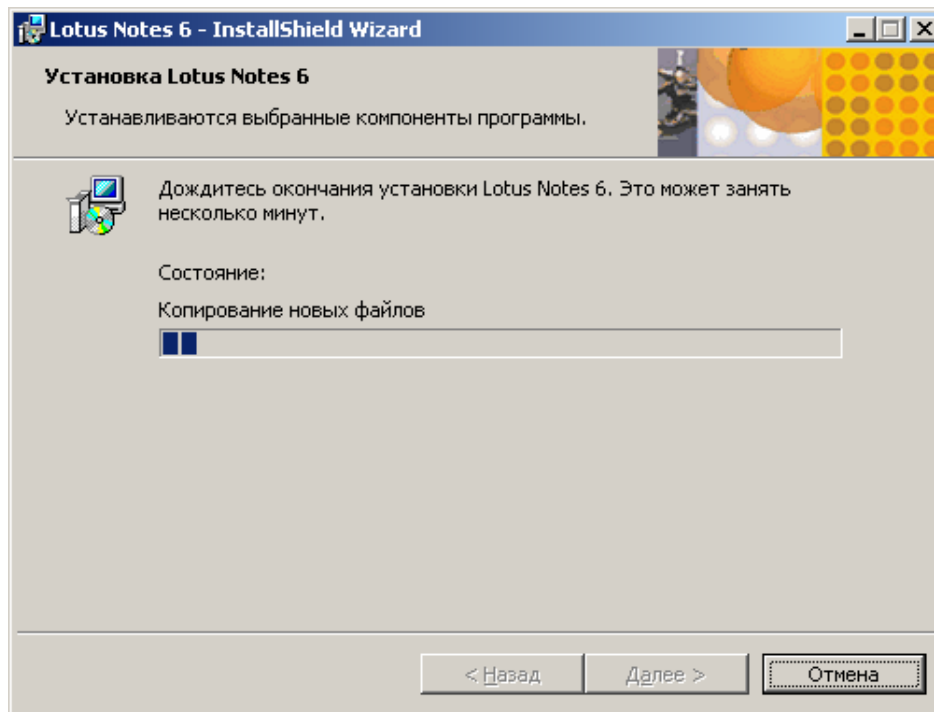


Рис. 278

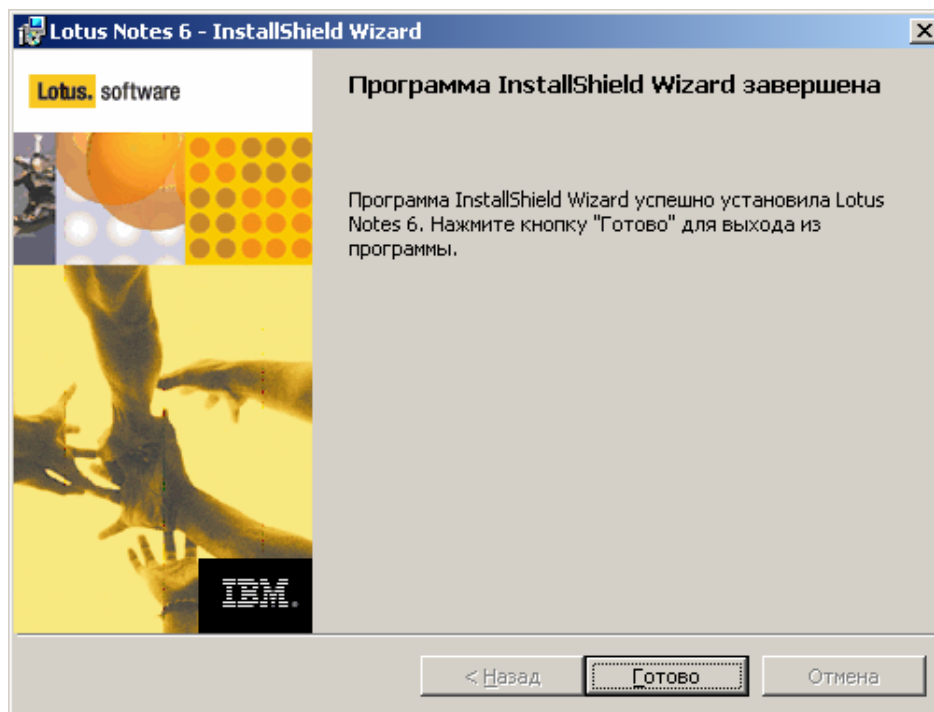


Рис. 279

1.43.2. 1.1.2. Вторая фаза установки (Setup) первым пользователем

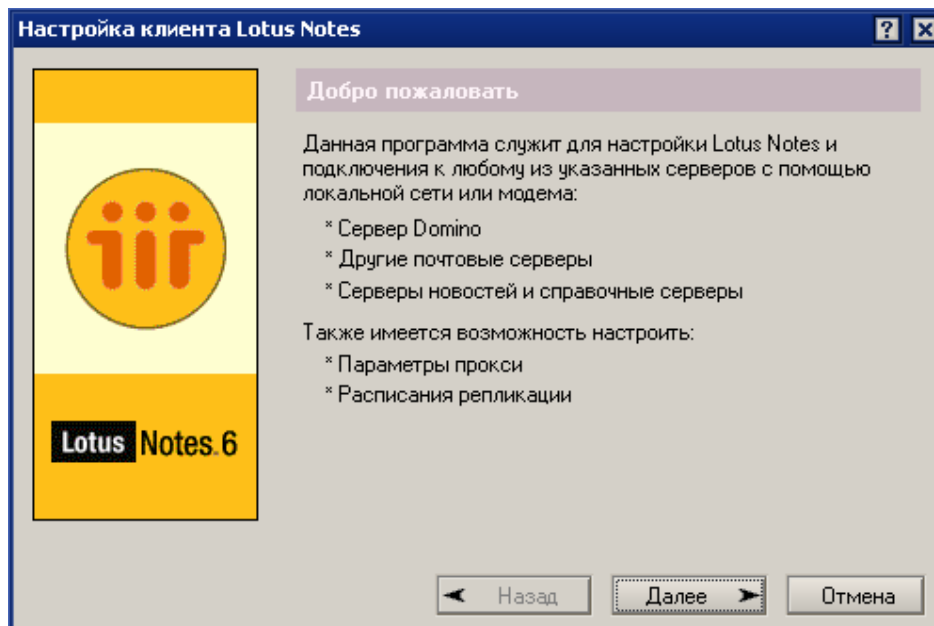


Рис. 280 Пользователь Win2000-XP под экаунтом ADMIN запустил клиента Notes

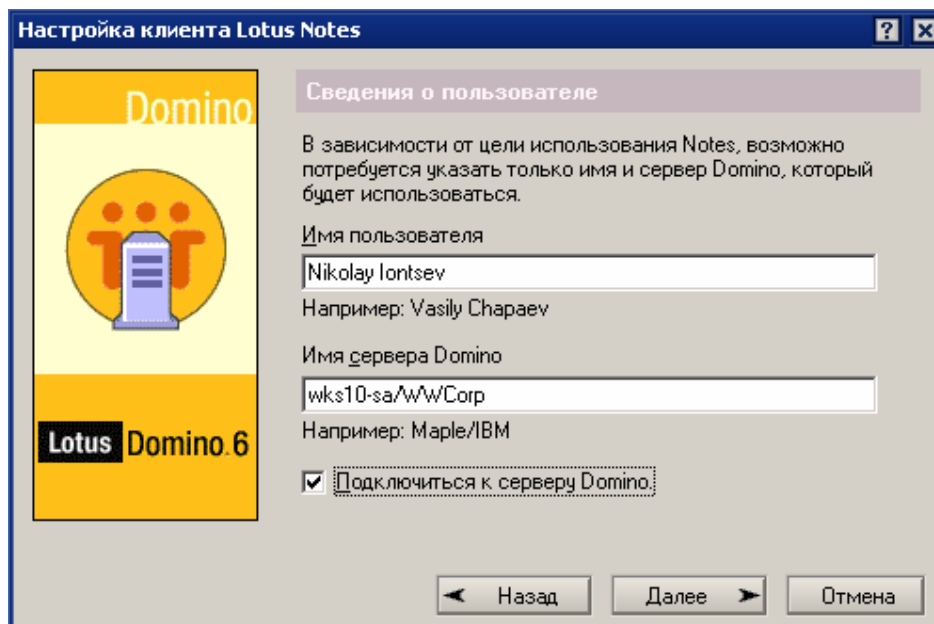


Рис. 281 Nikolay Iontsev – имя в Notes пользователя с экаунтом ADMIN

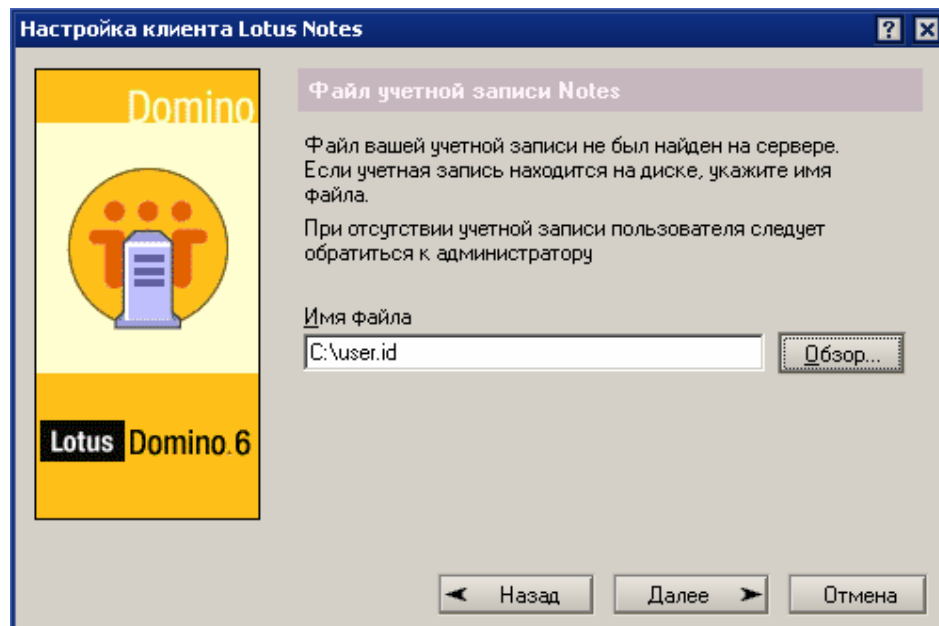


Рис. 282

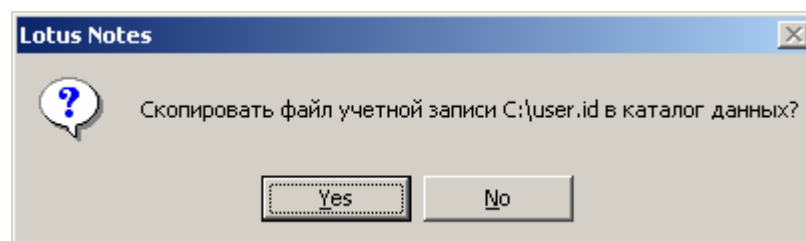


Рис. 283

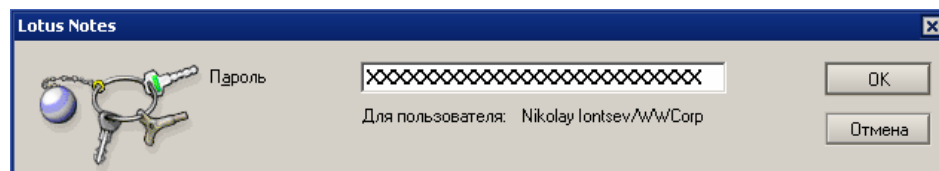


Рис. 284

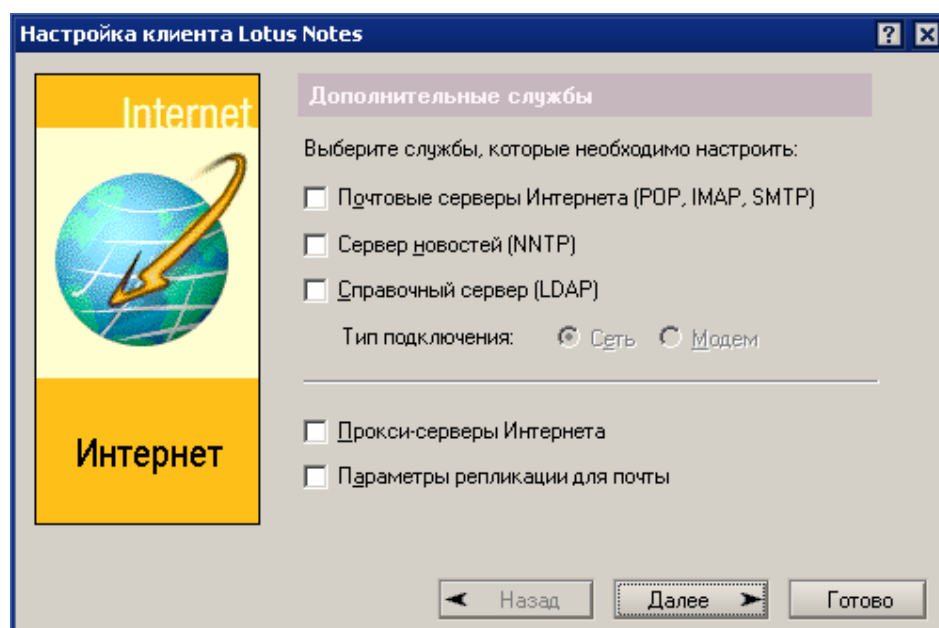


Рис. 285

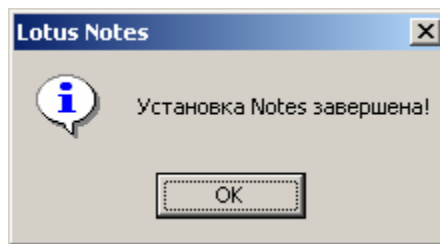


Рис. 286

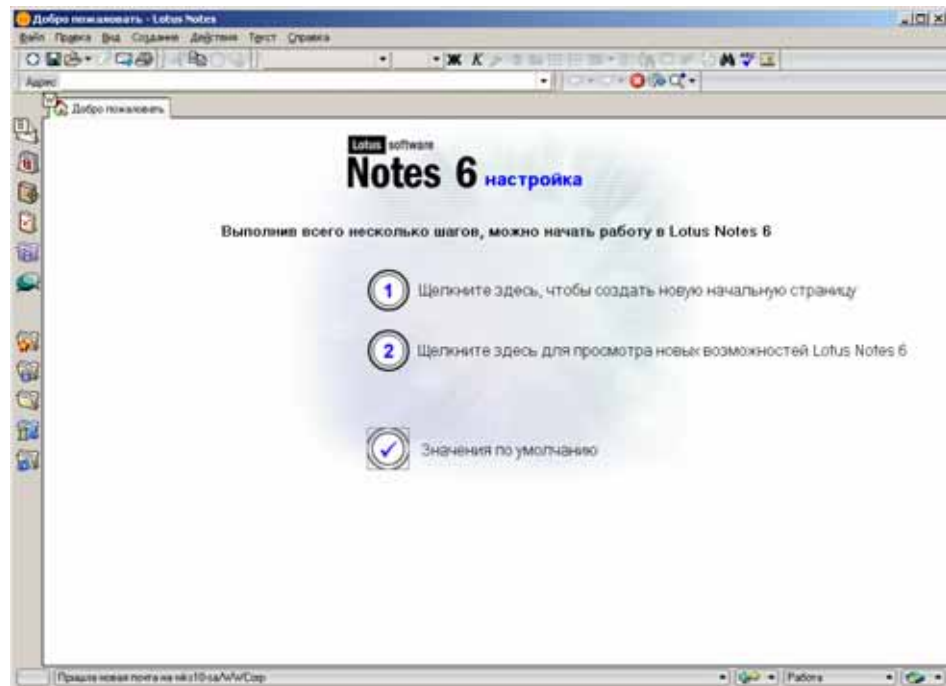


Рис. 287

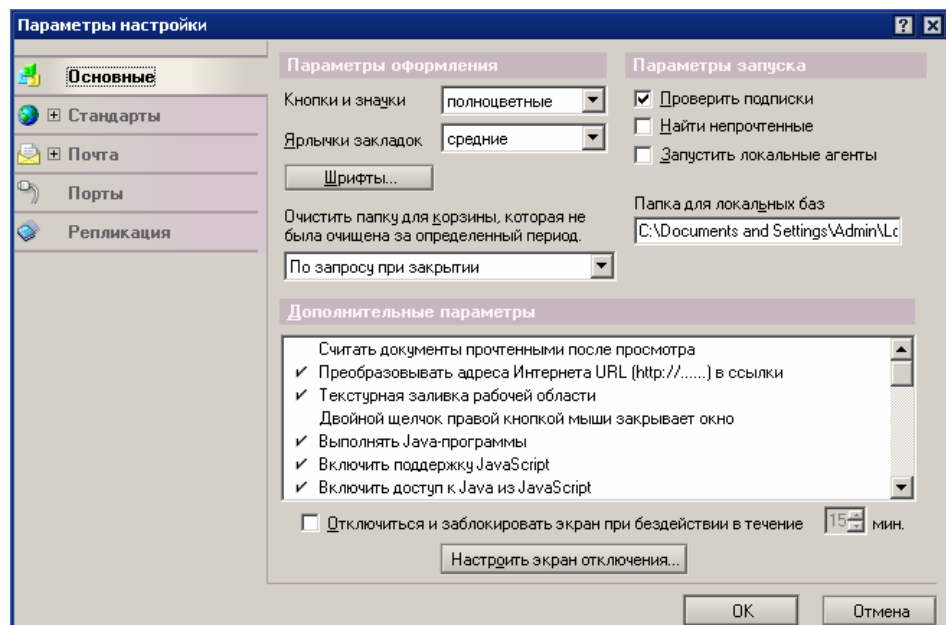


Рис. 288 Видно, что каталог для локальных баз C:\Documents and Settings\Admin\Local Settings\Application Data\Lotus\Notes\Data

1.43.3. 1.1.3. Вторая фаза установки (Setup) вторым пользователем

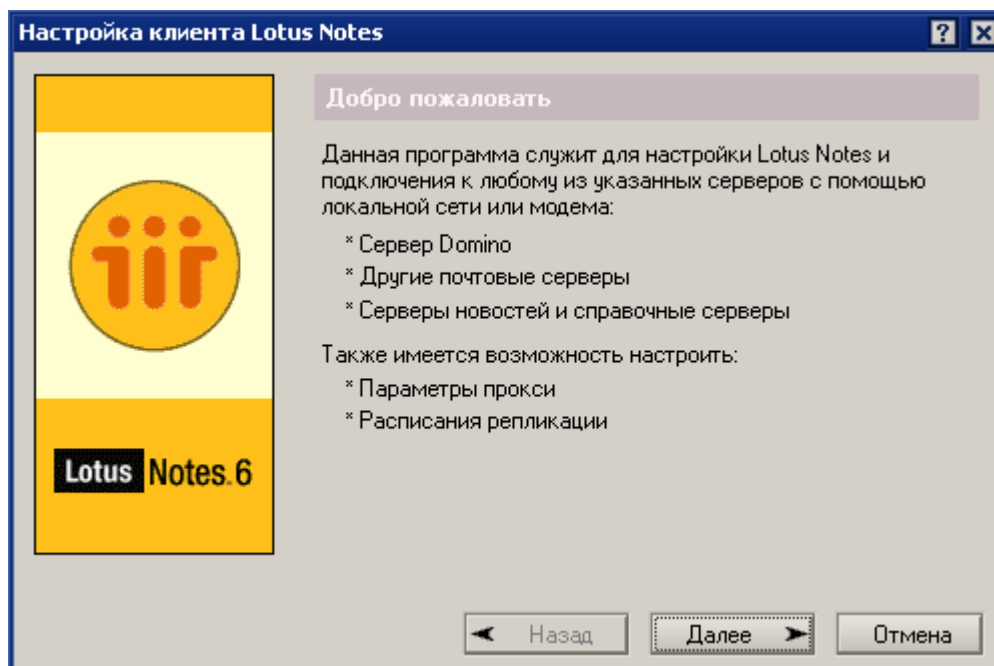


Рис. 289 Пользователь Win2000-XP под экаунтом ADMINISTRATOR запустил клиента Notes

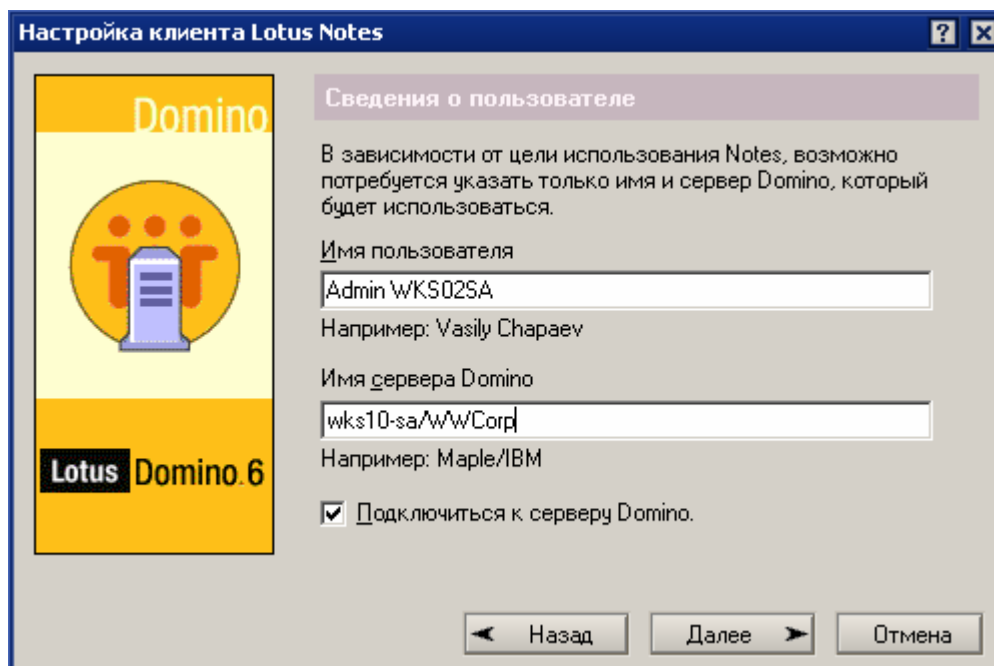


Рис. 290 Admin WKS02SA – имя в Notes пользователя с экаунтом ADMINISTRATOR

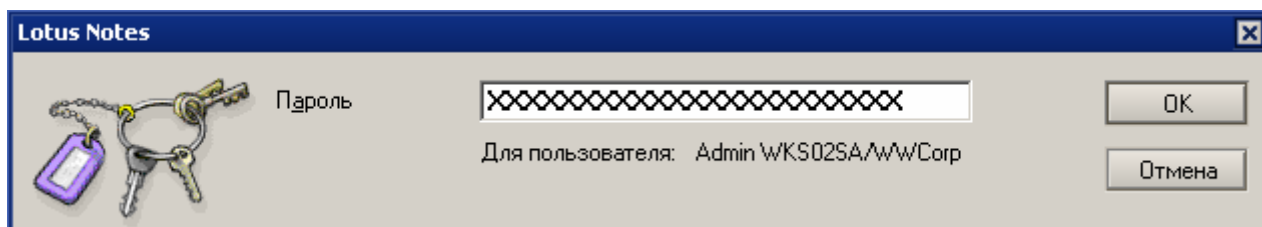


Рис. 291

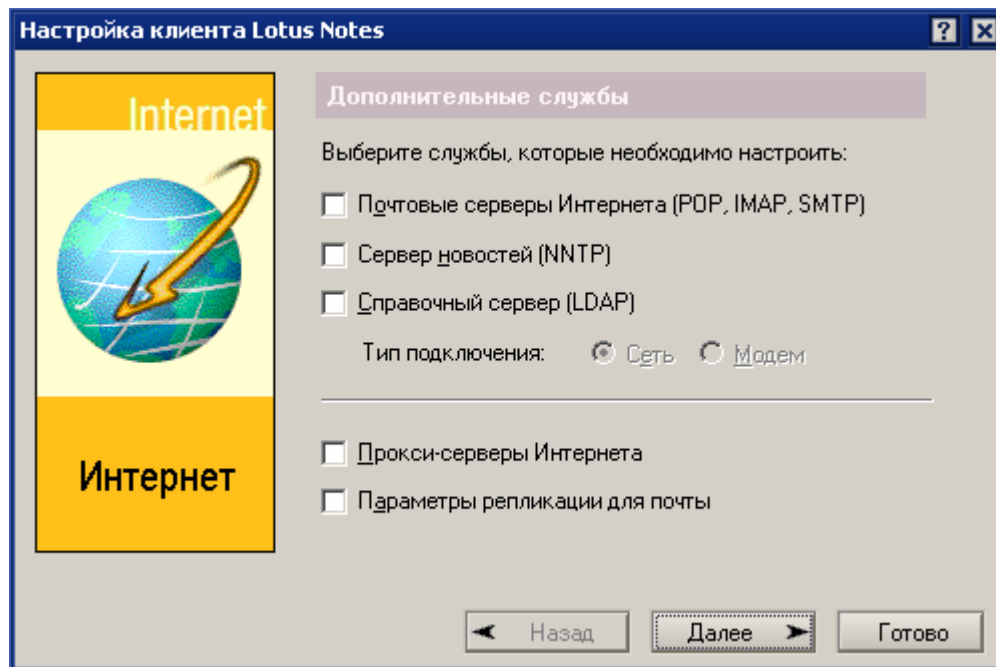


Рис. 292

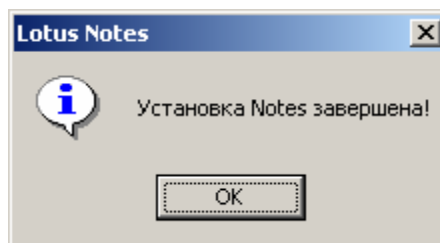


Рис. 293

1.43.4. 1.1.4. Исследование того, что получается в результате

1.43.4.1. 1.1.4.1. Фаза 1

Каталог программ **C:\Program Files\Lotus\Notes** содержит общие для всех пользователей программы, DLL и др. файлы; там нет баз и шаблонов (*.nsf, *.ntf).

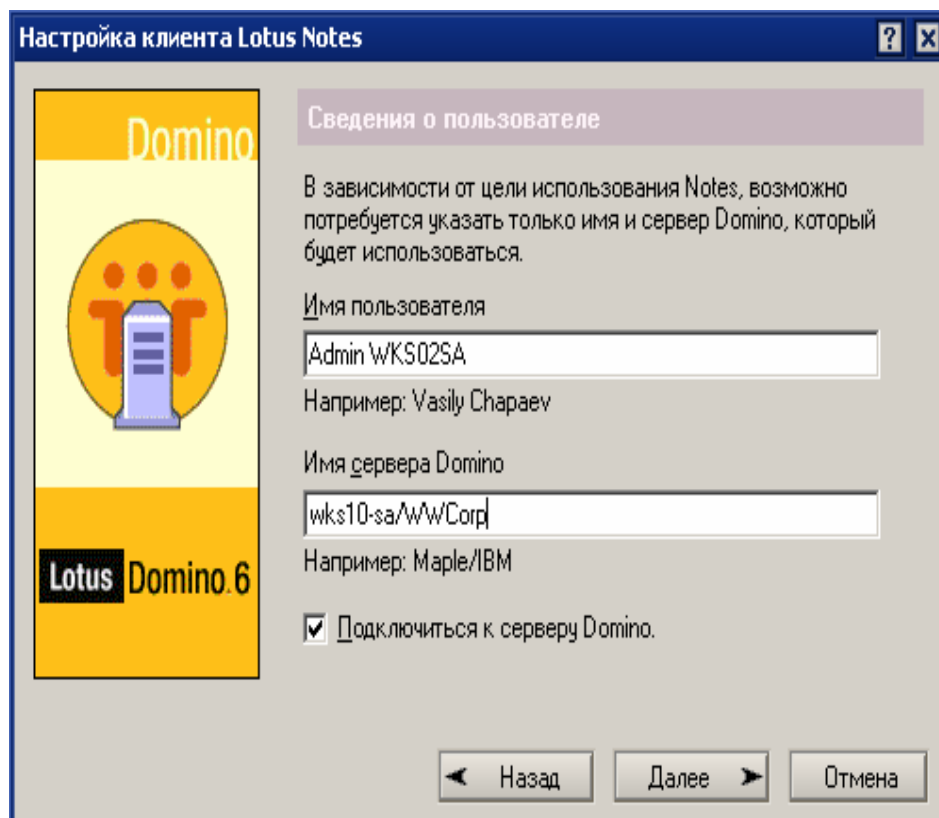


Рис. 294

Общая для всех пользователей часть каталога данных **C:\Documents and Settings\All Users\Application Data\Lotus\Notes\Data** содержит «стартовый» notes.ini, общие базы и шаблоны (agentrunner.nsf, readme.nsf, \help*.nsf, *.ntf)

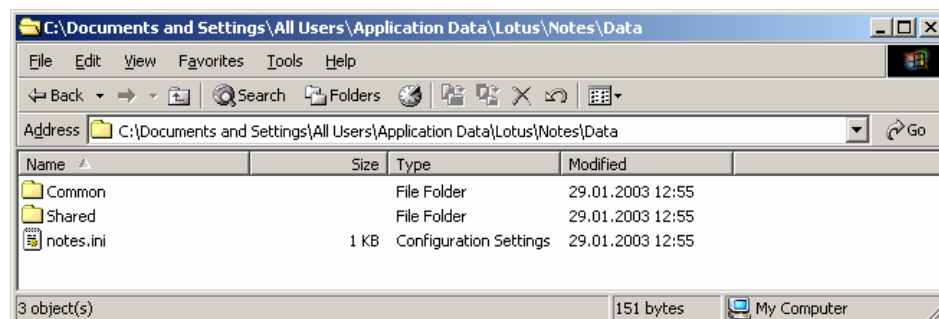


Рис. 295

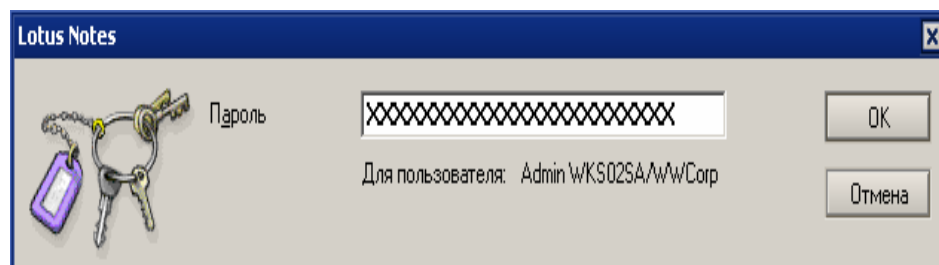


Рис. 296 «стартовый» notes.ini

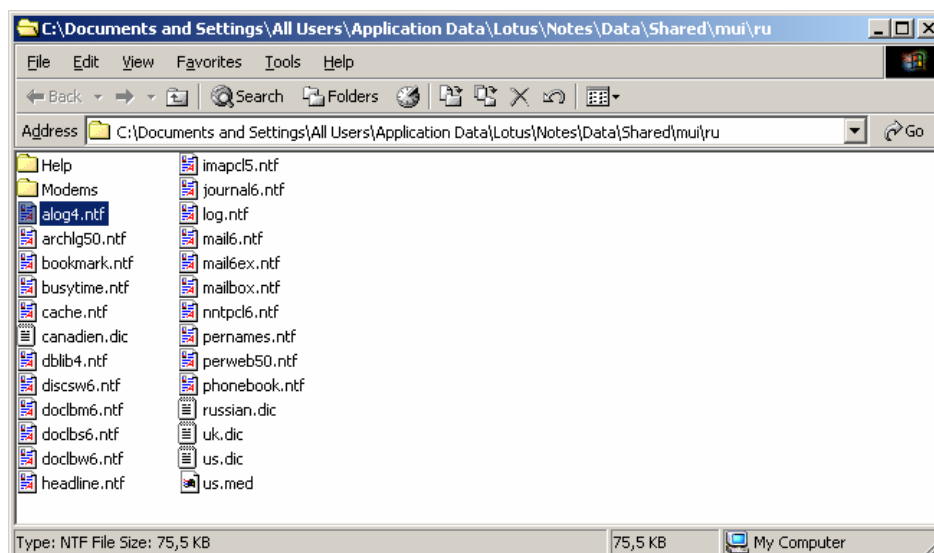


Рис. 297 Общие шаблоны и словари

1.43.4.2. 1.1.4.2. Фаза 2, пользователь с экаунтом Admin

Личная часть каталога данных **\Documents and Settings\Admin\Local Settings\Application Data\Lotus\Notes\Data** содержит данные конкретного пользователя UserName (notes.ini, user.id, bookmark.nsf, journal.nsf, headline.nsf, log.nsf, names.nsf)

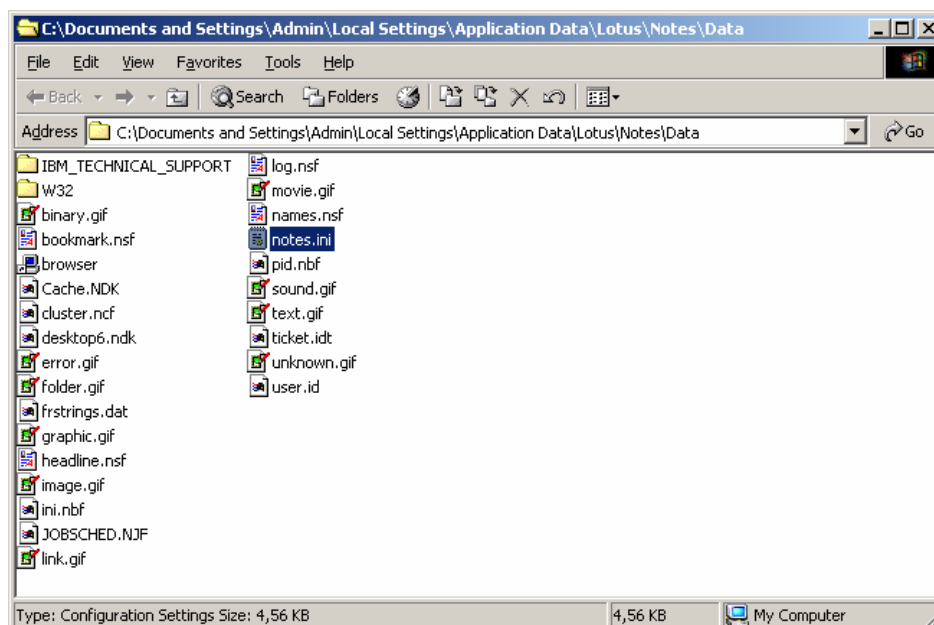


Рис. 298

1.43.4.3. 1.1.4.3. Фаза 2, пользователь с экаунтом Administrator

Личная часть каталога данных **\Documents and Settings\Administrator\Local Settings\Application Data\Lotus\Notes\Data** содержит данные конкретного пользователя UserName (notes.ini, user.id, bookmark.nsf, journal.nsf, headline.nsf, log.nsf, names.nsf)

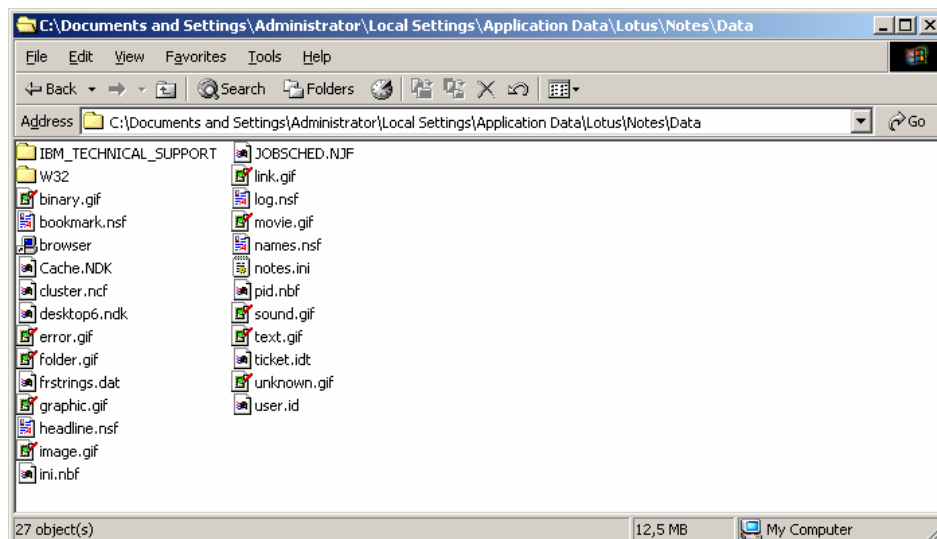


Рис. 299

1.43.4.4. 1.1.4.4. Местоположения User.id, notes.ini и names.nsf

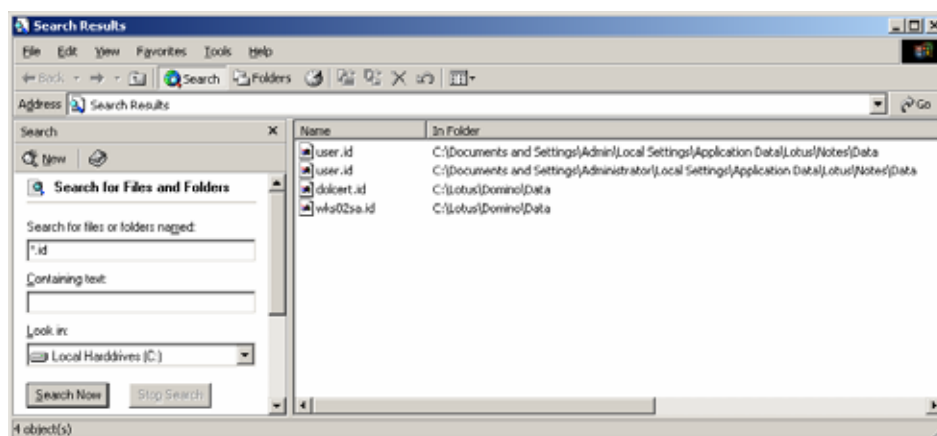


Рис. 300

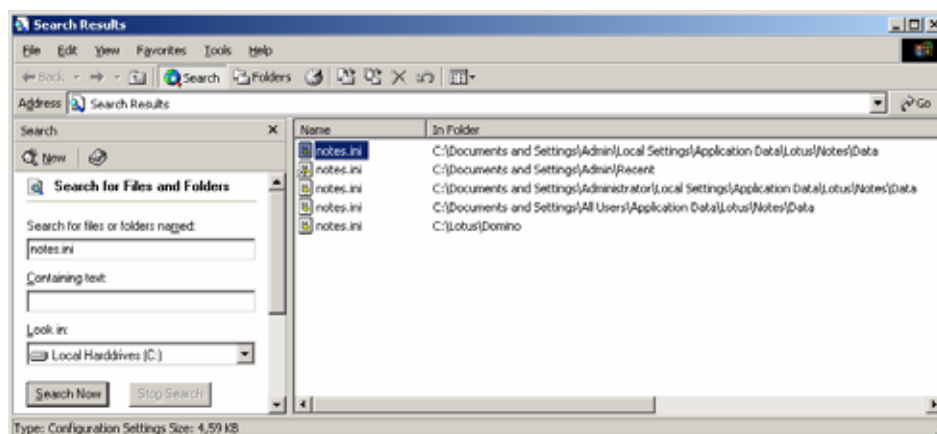
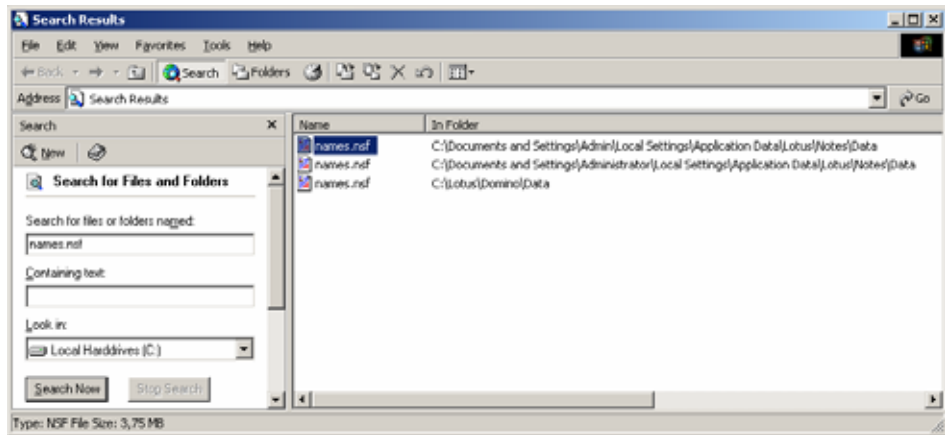


Рис. 301



1.44. 1.1. Возможности автоматизации установки клиентов Notes

1.44.1. 1.1.1. Ключи программы Setup клиента

В Help-е на эту тему много ошибок...

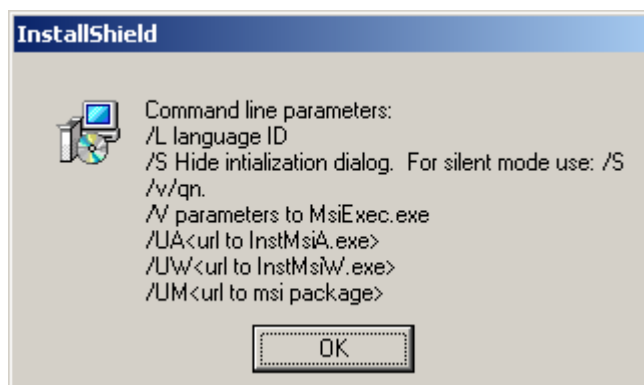


Рис. 303 `setup /?` дает ключи

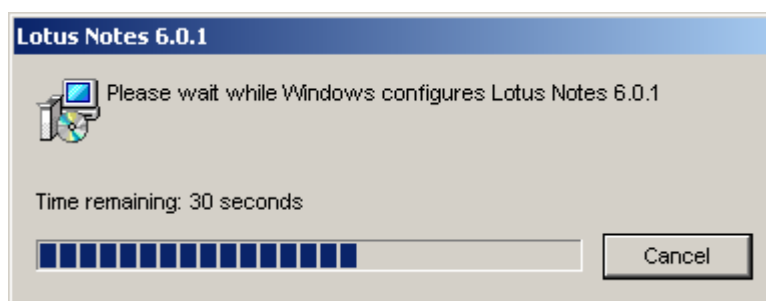


Рис. 304 `setup /S /v/qb` - без пробела `/v/qb` – ставит с «прогрессбаром»

`setup /S /v/qn` - без пробела `/v/qn` – «полное молчание, даже не говорит, что завершился»

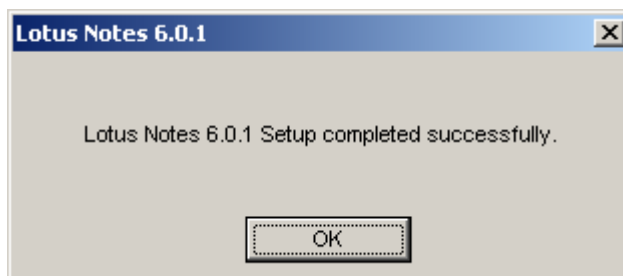


Рис. 305 `setup /S /v/qn+` - без пробела `/v/qn+` - «полное молчание, но в конце говорит, что завершился»

1.44.2. 1.1.2. Использование InstallShield Tuner for Notes

Продукт ставится и запускается. Продукт потребует времени на изучение, но, похоже, переопределить можно очень многое. Делается локальная копия дистрибутива. В продукте делается файл MST. Проводятся эксперименты. При успехе дело идет в серию.

Несколько вариантов запуска установки:

<code>C:\dis>msiexec /I "Lotus Notes 6.msi"</code>	<code>TRANSFORMS=3.mst</code>
<code>[PROGDIR="c:\NNN" DATADIR="c:\NNN\data"]</code>	- с диалогами
<code>C:\dis>msiexec /I "Lotus Notes 6.msi"</code>	<code>TRANSFORMS=3.mst</code>
<code>[PROGDIR="c:\NNN" DATADIR="c:\NNN\data"] /qn</code>	- в полном молчании
<code>C:\dis>msiexec /I "Lotus Notes 6.msi"</code>	<code>TRANSFORMS=3.mst</code>
<code>[PROGDIR="c:\NNN" DATADIR="c:\NNN\data"] /qb</code>	- с прогрессбаром

1.45. 1.1. Roaming Users Support - поддержка «перемещающихся» пользователей

1.45.1. 1.1.1. Назначение

- • Поддерживается с версии 6.01.
- • Обеспечивает пользователю его личную (персонализированную) среду в клиентах Notes на нескольких компьютерах.
- • Дает возможность перемещающимся пользователям работать с любого компьютера, на котором установлен клиент Notes.
- • Рабочее пространство пользователей, включая адресную книгу (в ней обычно содержится также ID-файл, необходимая часть параметров NOTES.INI и пользовательские словари в виде присоединенных файлов), базу закладок и журнал, централизованно сохраняется на сервере Domino – Roaming-сервере.
- • Данные пользователя в клиенте Notes на его очередном компьютере в конце сеанса по выбору сохраняются или очищаются.

1.45.2. 1.1.2. Более подробно

Пользователь имеет несколько компьютеров и хочет, чтобы его «контекст» следовал за ним.

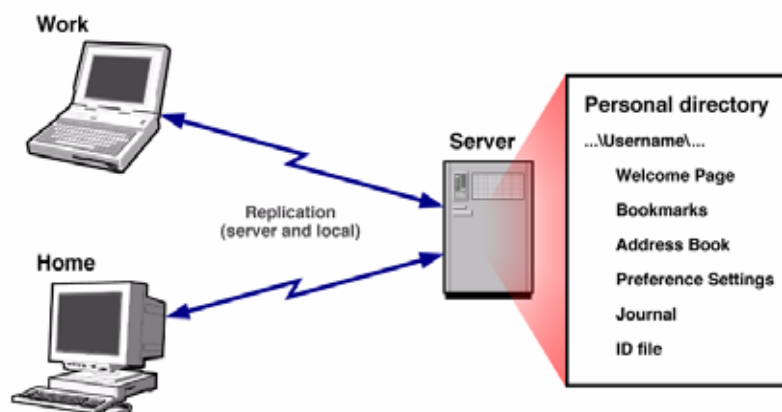


Рис. 306 Общий принцип

Перемещающийся пользователь при первой установке клиента получает на локальный компьютер с Roaming-сервера реплики своей персональной адресной книги (names.nsf), базы закладок (bookmark.nsf) и журнала (journal.nsf). В дальнейшем при каждом открытии и завершении сеанса эти базы реплицируются с серверными репликами на Roaming-сервере.

При конфигурировании дополнительного компьютера реплики этих баз аналогично берутся с Roaming-сервера.

В дальнейшем в каталог пользователя на Roaming-сервере могут быть добавлены реплики других баз – они тоже станут реплицироваться при запуске и останове клиента.

Поскольку ID-файл пользователя обычно сохраняется в адресной книге, пользователю не нужно «носить ID-файл с собой».

1.45.3. 1.1.3. Параметры регистрации для перемещающегося пользователя

Стандартизация параметров настройки для перемещающихся пользователей достигается политиками регистрации - они задаются один раз, а затем нужная политика применяется при регистрации пользователей.

Параметры настройки для перемещающихся пользователей могут быть заданы для и каждого пользователя при его регистрации - но это требует больше работы администратора.

1.45.3.1. 1.1.3.1. Roaming Registration Options в документе Registration Policy

Registration Settings: InterTrust - Full Access Administration - Domino Administrator

File Edit View Create Actions Text Window Help

INTERTRUSTCORP Domain ... Vasily Vasilyevich Roamingov's... Registration Settings: InterTrust

1 Save & Close 2 Cancel 3 Inheritance 4 Enforcement

Registration Settings : InterTrust

Basics | Mail | ID/Certifier | Miscellaneous | Comments | Administration

Basics

Name: InterTrust
Description:

Basic User Registration Options	Inherit from parent policy:	Enforce in child policies:
Choose a registration server: InterTrust/InterTrustCorp/SU	☐ Inherit	☐ Enforce
Password Options		
Choose a password quality: Acceptable user password (8)	☐ Inherit	☐ Enforce
☐ Set Internet Password	☐ Inherit	☐ Enforce
Roaming Options		
☒ Roaming User	☐ Inherit	☐ Enforce
☒ Use mail server for roaming server	☐ Inherit	☐ Enforce
☒ Create roaming files now	☐ Inherit	☐ Enforce
☐ Create roaming files in background	☐ Inherit	☐ Enforce
Clean-up at Notes shutdown	☐ Inherit	☐ Enforce

Use the currently designated mail server as the roaming server

Office

Рис. 307 Roaming Registration Options в документе Registration Policy

1.45.3.2. 1.1.3.2. Регистрация перемещающегося пользователя

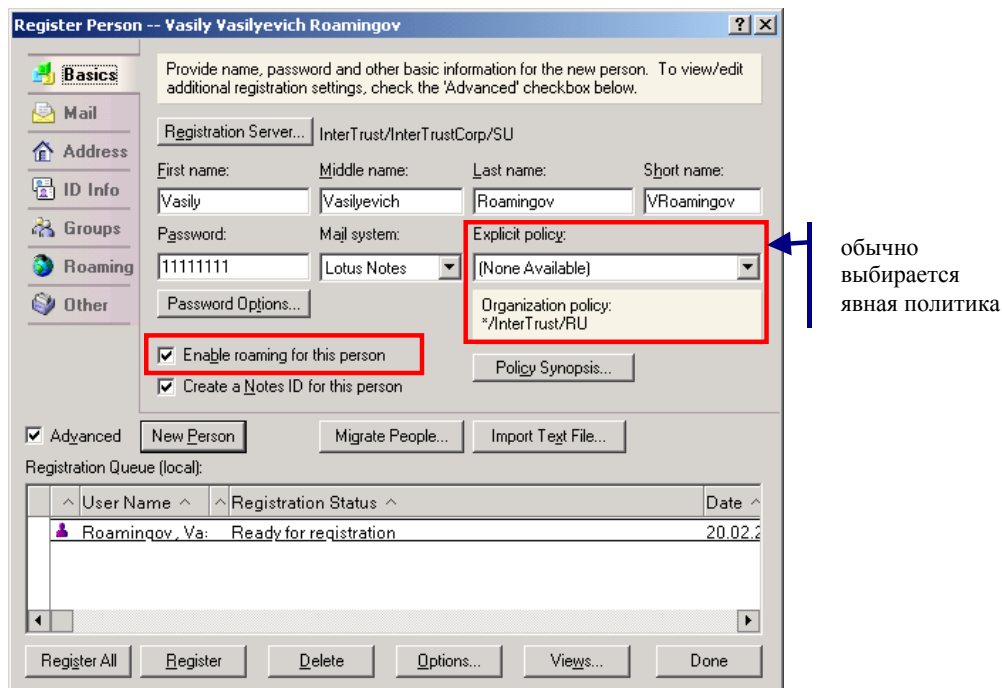


Рис. 308 Закладка Basics

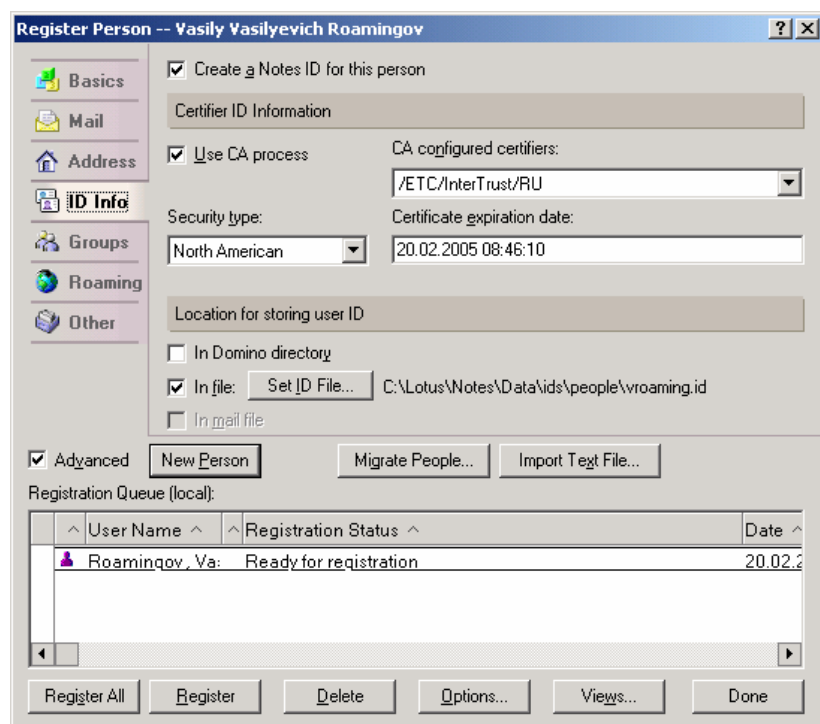


Рис. 309 Для повторения – регистрация с использованием СА

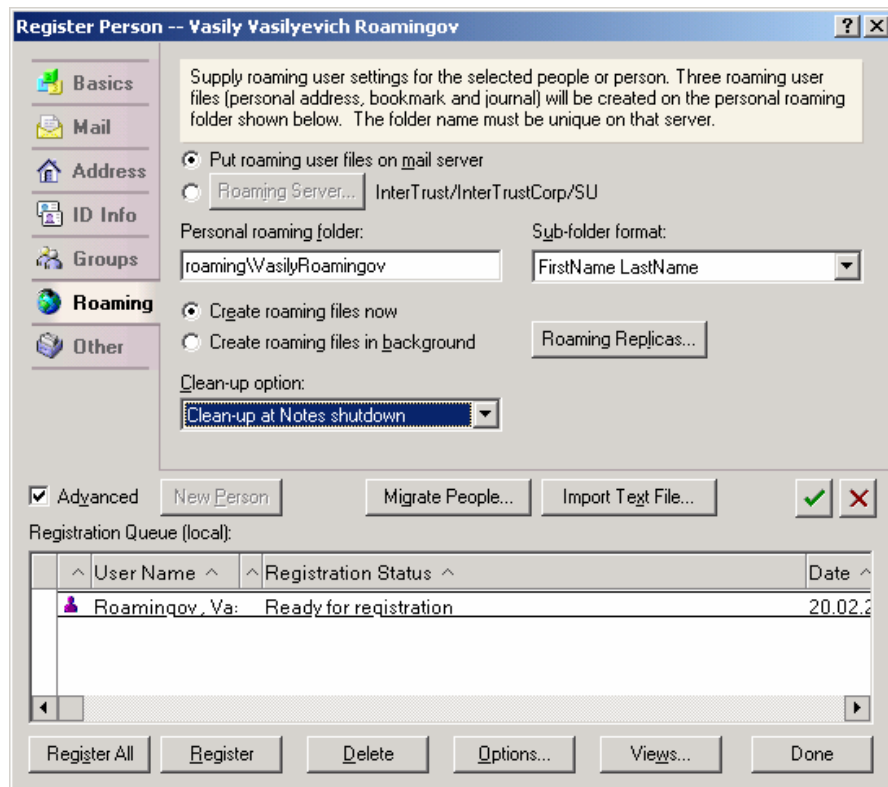


Рис. 310. Закладка Roaming

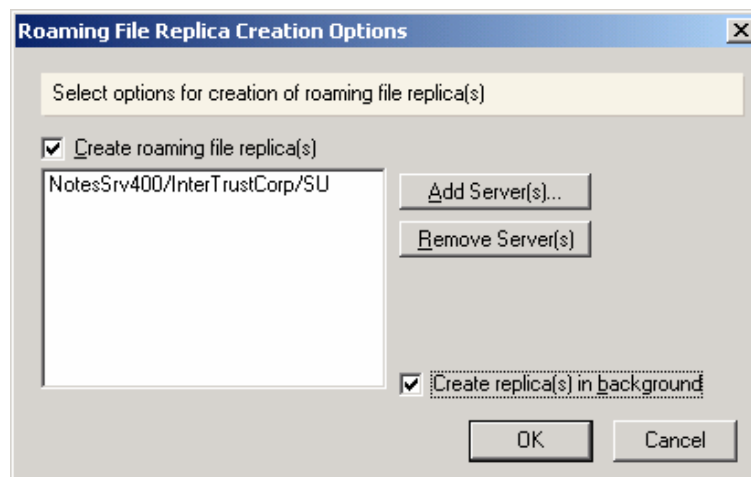


Рис. 311 Окно кнопки Roaming Replicas

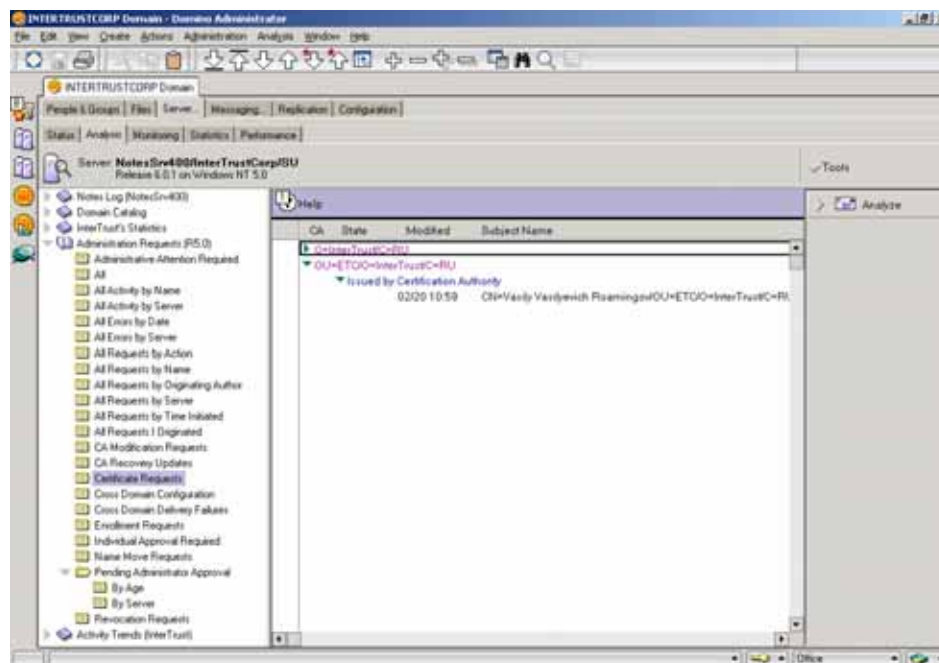


Рис. 312 Для повторения – регистрация с использованием СА, база admin4.nsf

1.45.3.3. 1.1.3.3. Закладка Roaming User в документе Person

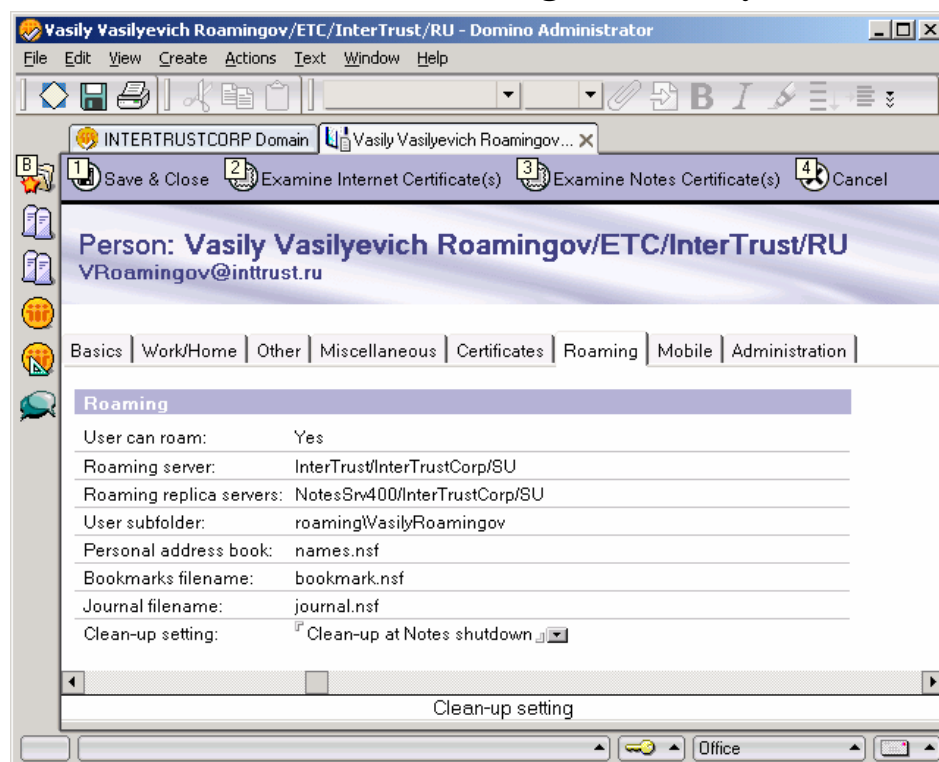


Рис. 313 Закладка Roaming User в документе Person

1.45.4. 1.1.4. Преобразование обычных пользователей в перемещающихся и наоборот

Из клиента администратора Person & Group - Tools - People – Roaming.

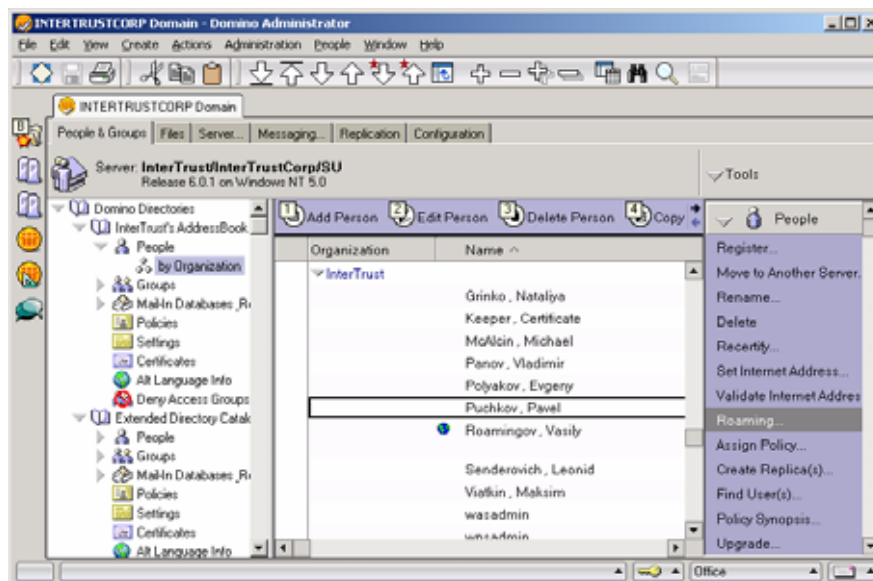


Рис. 314 Выбран обычный пользователь

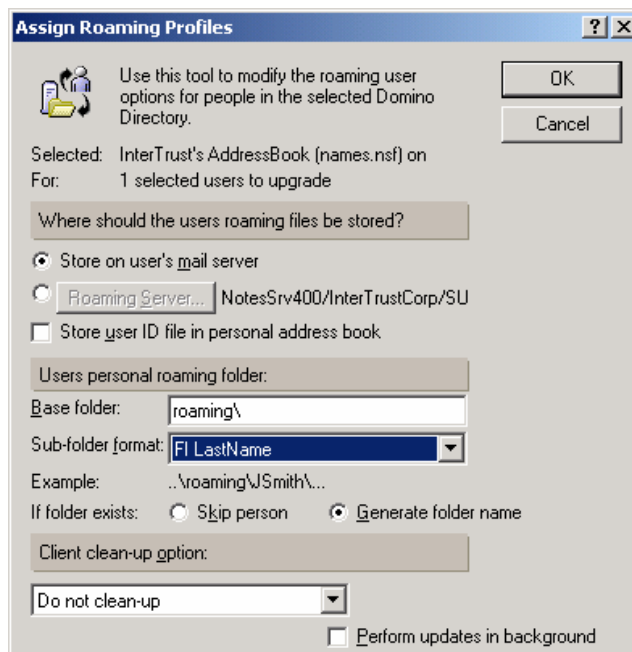


Рис. 315 Создание Roaming Profile. Обратите внимание на флаг Store user ID in personal address book

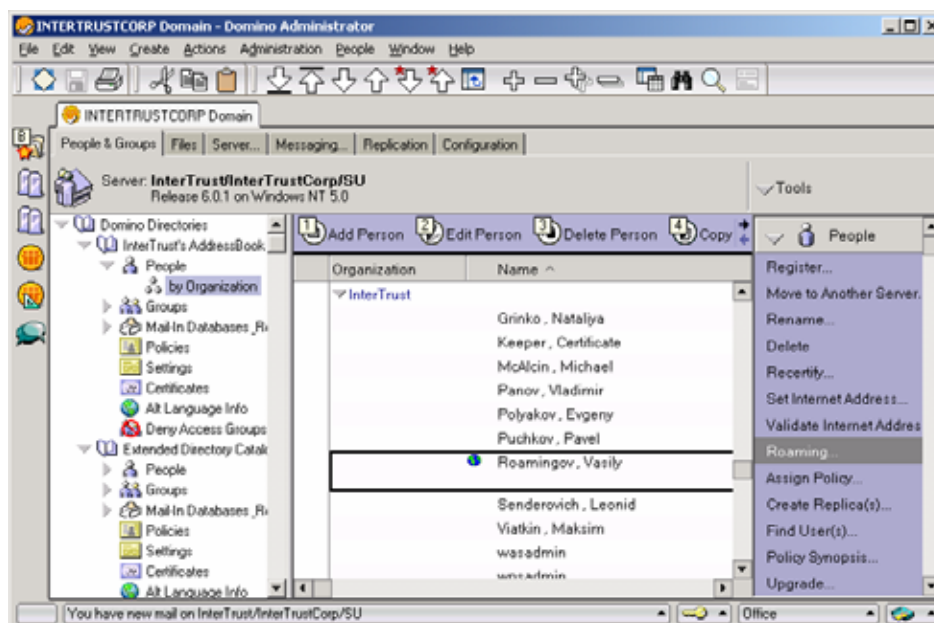


Рис. 316 Выбран перемещающийся пользователь

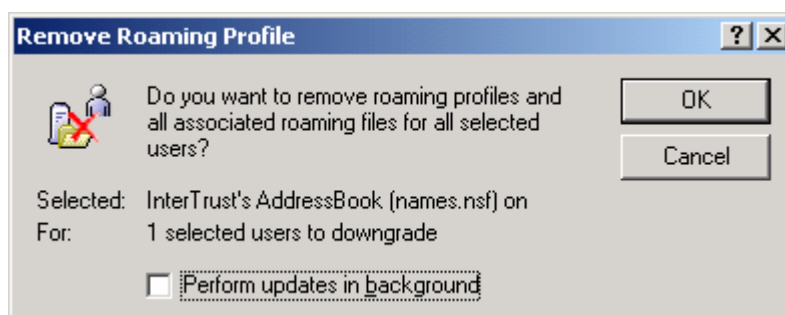


Рис. 317 Удаление Roaming Profile

1.45.5. 1.1.5. Выясненные вопросы

При первоначальной регистрации ID помещается в документ Person или в файл, но не в локальную адресную книгу пользователя на Roaming-сервере. При первом входе в клиента (использовалась установка MultiUser) ID «перемещается» из документа Person на станцию или берется «с дискеты». При закрытии первой сессии в клиенте ID переносится в локальную адресную книгу пользователя на Roaming-сервере. При последующих входах в клиента по имени и паролю ID копируется на станцию, как, впрочем, и все остальное.

Базы, «положенные» в каталог на Roaming-сервере, успешно реплицируются на станцию. Но не desktop6.ndk (проверялось). Поэтому самого простого и привычного «пространства с закладками» Вы пользователю не обеспечите – только фолдеры и ссылки из bookmark.nsf. Далее вырезка из readme:

Please be aware that the following items do not replicate, and can't be expected to have the same data on all computers used.

- Signature files
- IMAP and NNTP proxy databases
- Notes.INI file (except for User Preferences stored in the Personal Address Book)
- Desktop.dsk file
- Cache.ndk file
- Headline.nsf
- Private views
- Any other data files or databases that are not replicated to the roaming subdirectory on the server

Так что реплицируется не весь контекст...

1.45.6. 1.1.6. Недостаточно ясные в настоящее время вопросы

- • [Store user ID in personal address book \(optional\)](#): Places the user's ID in their own local personal address book.

Данная опция есть в окне преобразования обычного пользователя в перемещающегося. Процесс реализуется задачей ADMINP.

- • [The user ID is double-encrypted for added security before being attached.](#)

ID-файл, сохраняемый в адресной книге, «дважды зашифрован». Принцип шифрования пока непонятен. Можно предположить, что на открытом ключе сервера (RSA) и на пароле пользователя (один ключ).

- • Кроме того, при регистрации есть «серая» опция сохранения ID в почтовом файле. Очевидно, что это и есть место хранения ID-файла, используемого при дешифрировании зашифрованной почты в контексте iNotes. Но опция «серая», даже при выборе шаблона iNotes...
- • Изучение NotesPeek-ом адресной книги пока выявило наличие в ней профильного документа roaminguserid со следами параметров из NOTES.INI, но не самого ID-файла – нужно бы снять копию клиентской адресной книги после курсов и повторить эксперимент.

1.46. 1.1. Smart Upgrade - автоматический абгрейт клиентов R6

Возможность автоматического абгрейта клиентов R6:

- администратор получает пакет обновления («полный» или incremental), помещает его в базу Smart Update и назначает пользователям
- клиент R6 обнаруживает, что ему назначен пакет, и выполняет установку пакета обновления

1.46.1. 1.1.1. Предварительная подготовка

- Администратор создает на сервере базу Smart Upgrade по шаблону Smart Upgrade Kits

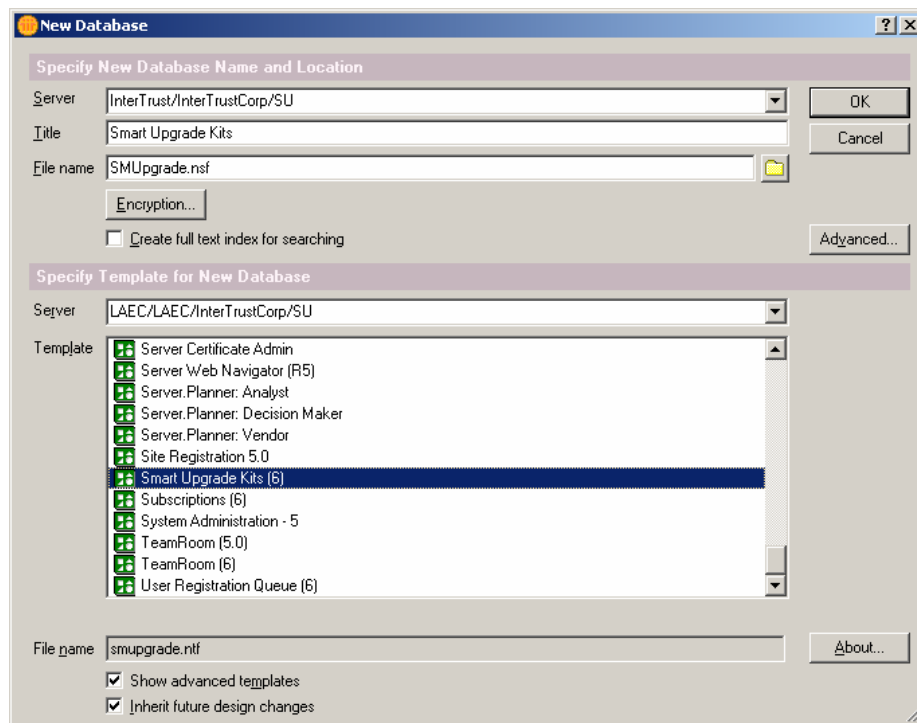


Рис. 318 Создание базы Smart Upgrade

- Ссылка на эту базу добавляется в документ Configuration Settings

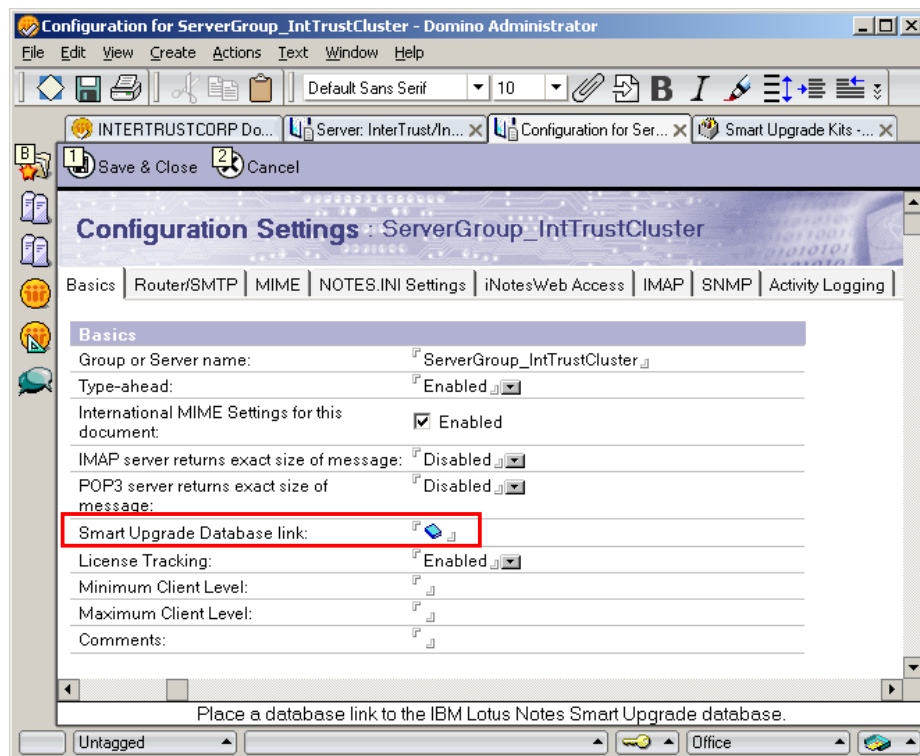


Рис. 319 Ссылка на эту базу в документе Configuration Settings

1.46.2. 1.1.2. «Оформление» пакета

- Администратор получает пакет обновления (например, скачивает с <http://www.lotus.com/ldd>)
- Создает в базе Smart Update документ, соответствующий пакету обновления

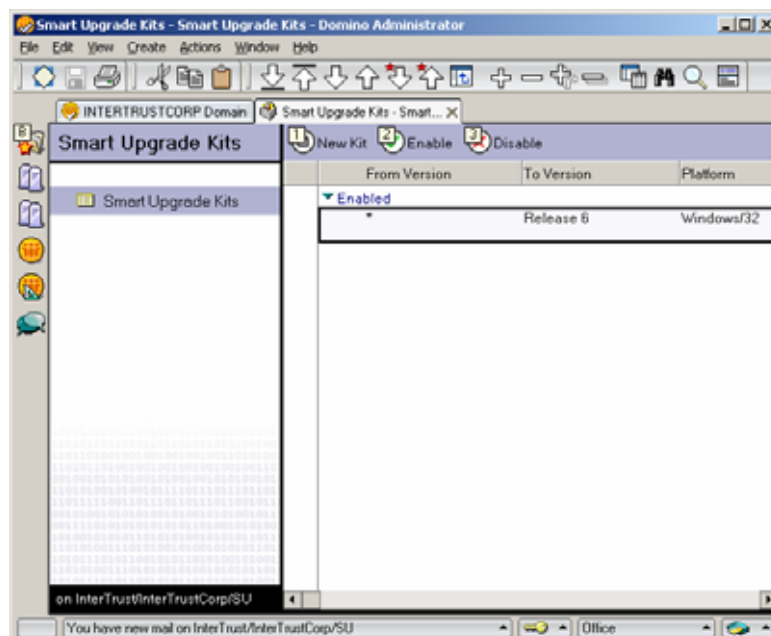


Рис. 320 Создает в базе Smart Update новый документ кнопкой New Kit

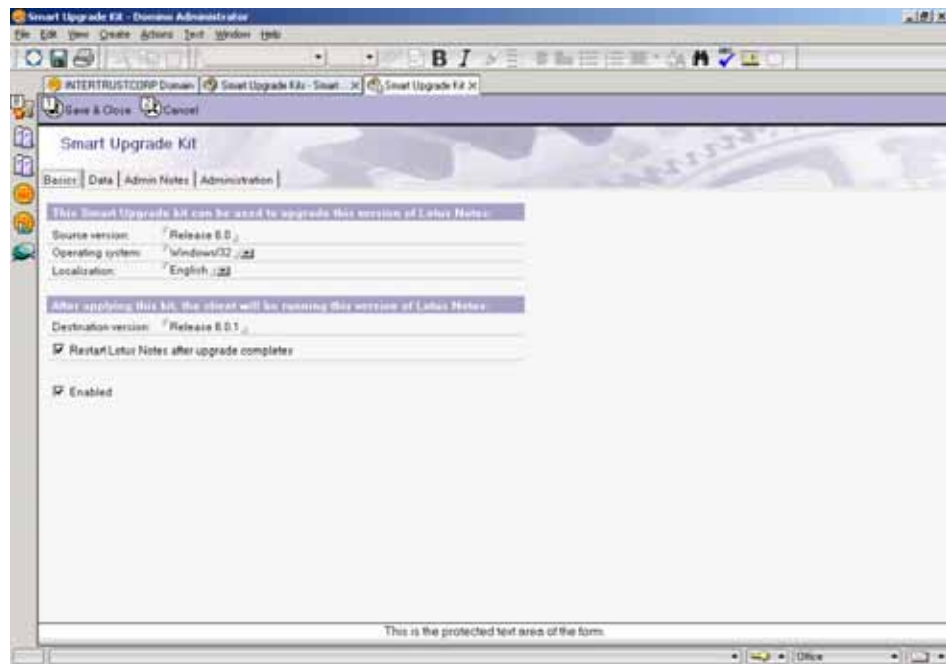


Рис. 321 Закладка Basics

- На закладке Data задает ссылку на местоположение пакета:
- либо присоединенный файл
- либо сетевой путь

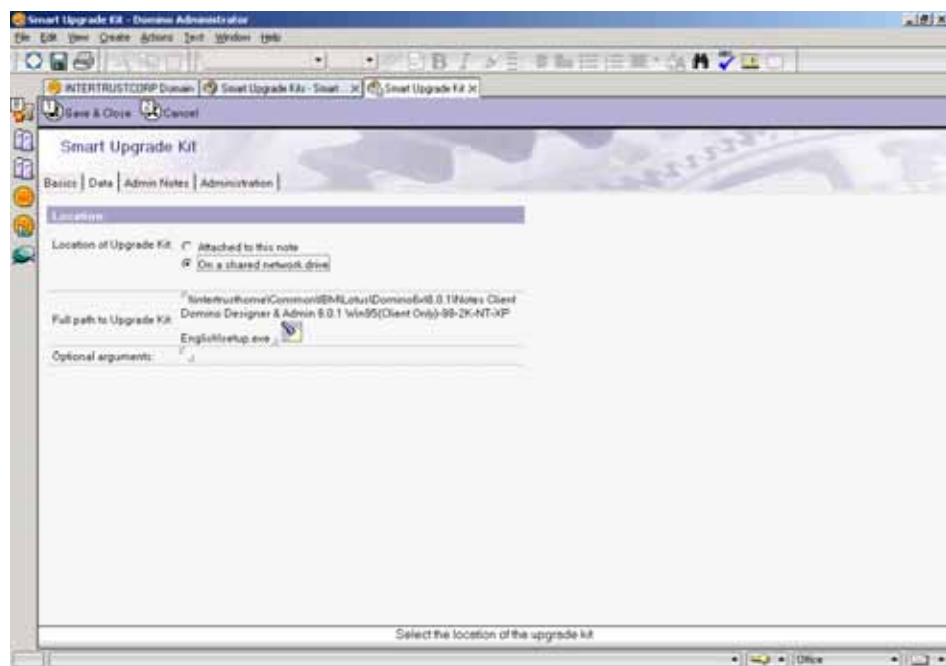


Рис. 322 Закладка Data

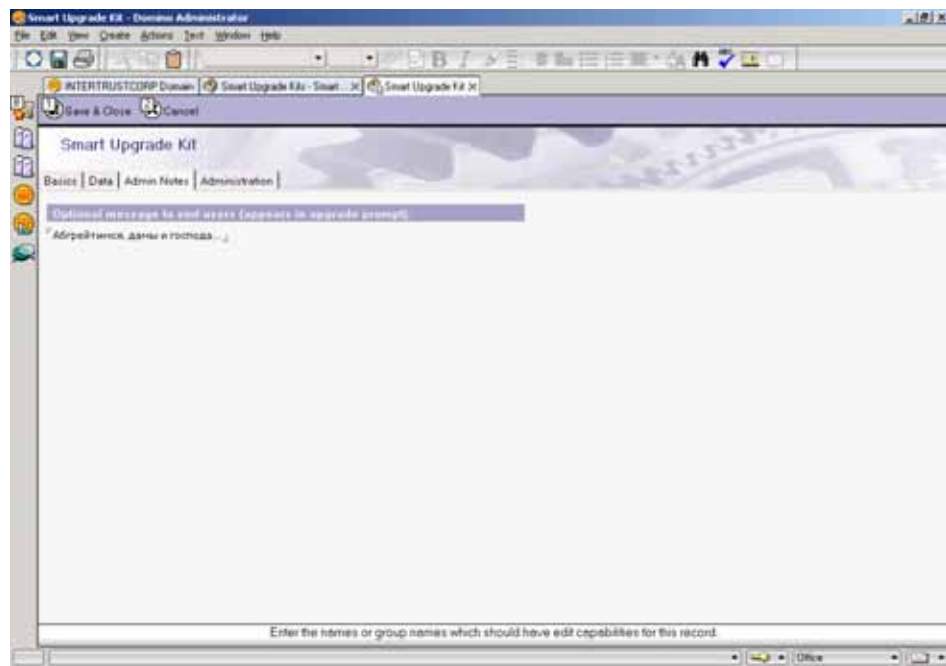


Рис. 323 Закладка Admin Notes

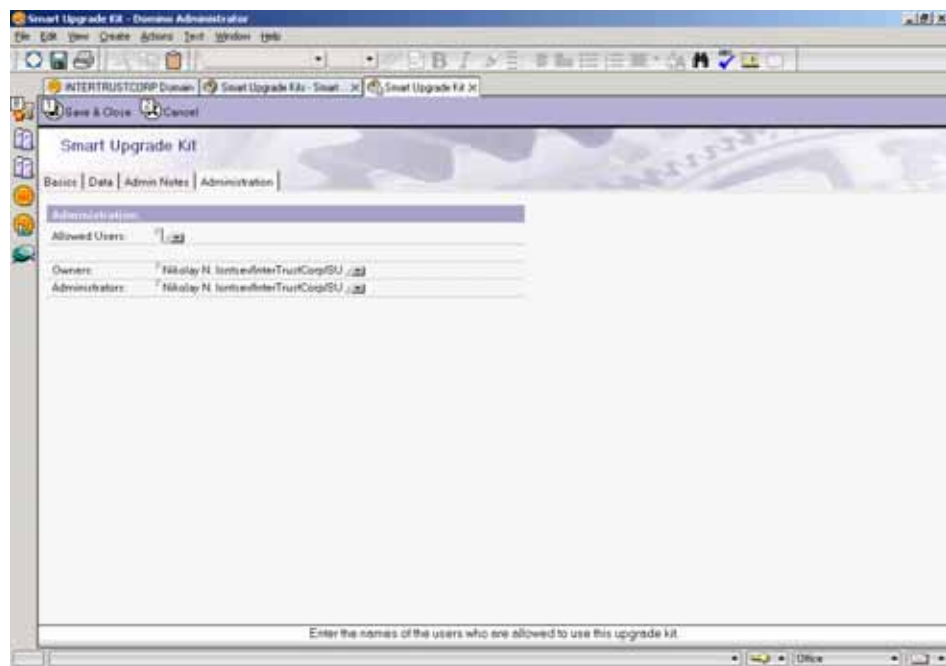


Рис. 324 Закладка Administration

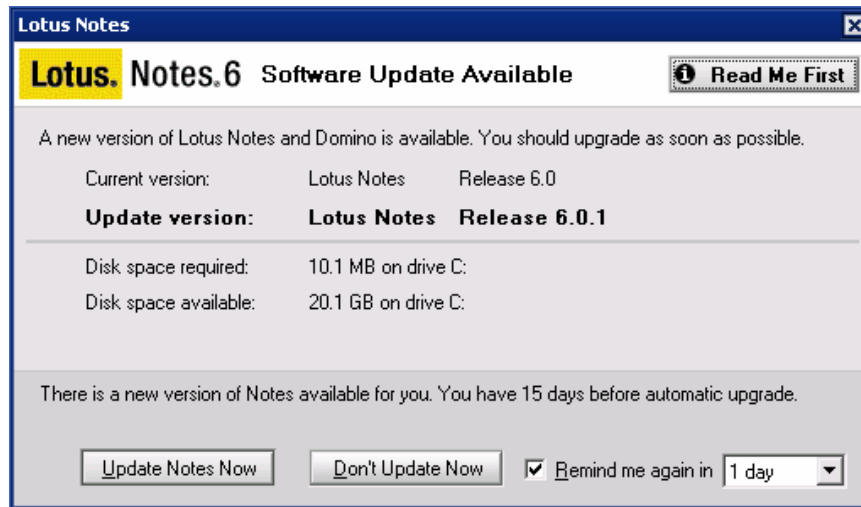


Рис. 327 Окно с предложением выполнить абгрейт

- • Пока время «вежливого предложения» не прошло, пользователь может отказываться от абгрейта или выполнить его в удобное время, выбрав в меню File - Tools - Notes Smart Update
- • Когда же время «вежливого предложения» истекло, абгрейт выполняется принудительно
- • При абгрейте происходит следующее:
 - • назначенный пользователю пакет копируется во временный каталог на компьютере клиента
 - • клиент R6 завершается, запуская «после себя» установку пакета из временного каталога
 - • пакет устанавливается
 - • стартует обновленный клиент R6
- • Откровенно говоря, возможны самые разные исходы такой установки...

1.47. 1.1. Серверная программа Administration Process (ADMINP) и операции, выполняемые с ее использованием

1.47.1. 1.1.1. Назначение и логика работы программы ADMINP

Назначение – автоматизированное выполнение трудоемких операций на серверах.

Причиной появления программы Administration Process (в R4) явилось применение в Notes «децентрализованной и распределенной в пространстве» системы защиты информации: сервер «защищается» в Каталоге Domino, базы данных - в их списках управления доступом, отдельные документы в базах - полями типа Readers и Authors в самих документах... Любые изменения в именах при такой системе защиты сопряжены с выполнением изменений «во многих местах на многих серверах». Аккуратно и быстро «вручную» выполнять такие изменения в больших доменах весьма трудоемко. Поэтому начинающим администраторам рекомендуется уделить достаточно времени изучению программы Administration Process на практике - без использования этой программы «удержать в руках» систему защиты большого домена практически невозможно.

По умолчанию программа Administration Process (ADMINP) запускается при старте сервера и работает до его останова. При первом запуске программы Administration Process на сервере автоматически создается база данных Administration Requests (ADMIN4.NSF).

Когда администратор, «неявно открыв» Каталог Domino, создает запросы на изменение имени пользователя или сервера, ресертификацию ID пользователя и сервера, удаление пользователя, сервера или группы (включая при этом и изменения в списках управления доступом во многих базах данных на многих серверах) и т.п., эти запросы сначала заносятся в базу данных Administration Requests того сервера, на котором был открыт Каталог Domino, и только затем программа Administration Process выполняет на сервере каждый такой запрос.

Для того чтобы запрошенные изменения происходили на всех серверах домена, на этих серверах должны присутствовать реплики базы Administration Requests. Заботиться об этом обычно не нужно, поскольку в процессе установки очередного сервера в домене на нем автоматически создается реплика базы Administration Requests (с того же сервера, с которого реплицировался Каталог Domino). Запросы поступают во все реплики базы Administration Requests путем репликаций, а исполняются программой Administration Process на соответствующих серверах. В немногих простых случаях запрос выполняется «за один шаг». Однако чаще выполнение первого запроса влечет создание одного или нескольких запросов для выполнения «на следующем шаге».

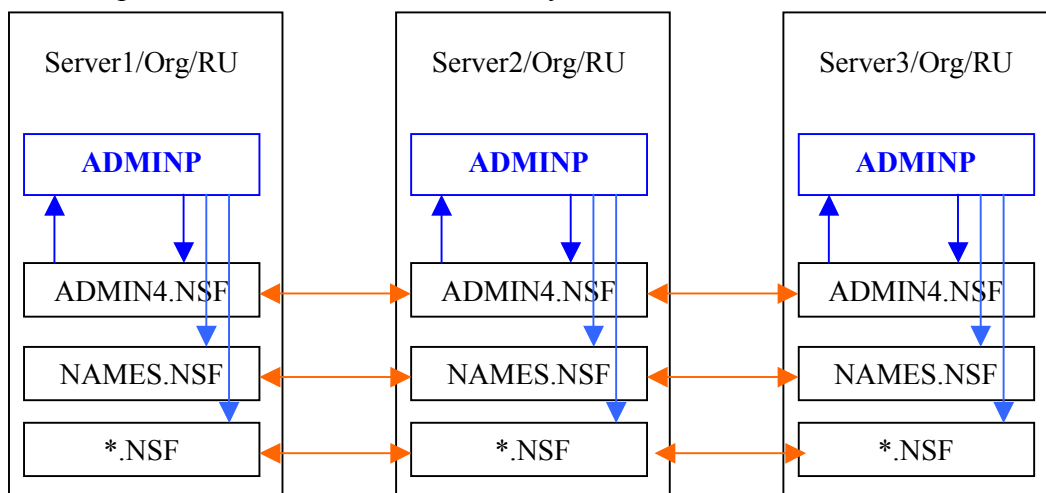


Рис. 328 Логика работы программы

1.47.2.

1.1.2. База ADMIN4.NSF

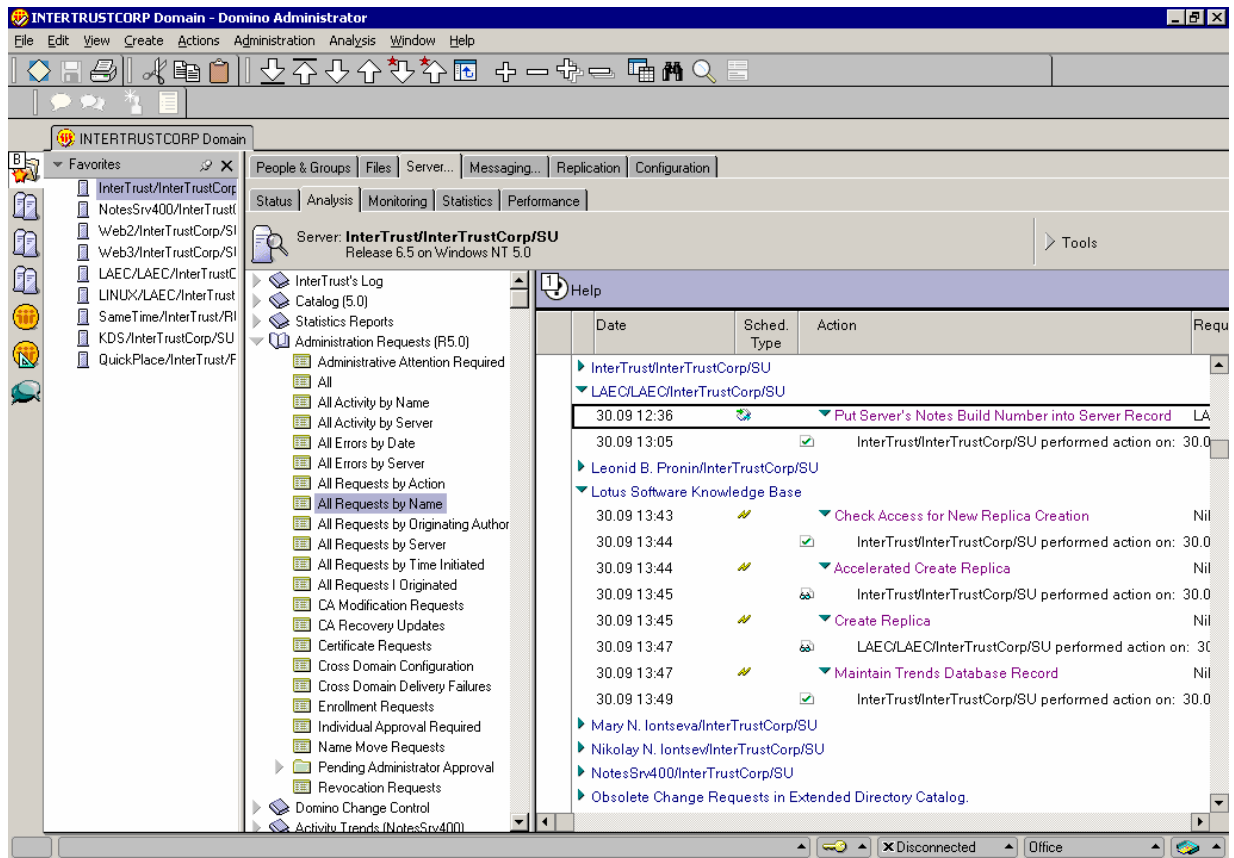


Рис. 329 База Admin4.nsf в клиенте Администратора. Запросы – фиолетового цвета, «протоколы выполнения запросов» – черного цвета

Sched. Type – типы запросов с точки зрения «оперативности» их исполнения:

- «по появлению» - приблизительно через минуту после поступления запроса в базу Administration Requests,
- «интервал» - в соответствии с установкой Interval (по умолчанию каждые 60 минут),
- «раз в день» - в соответствии с установкой Execute once a day requests at (по умолчанию в 12 часов дня),
- «раз в неделю» - в соответствии с установками Start executing on и Start executing at (по умолчанию в воскресенье в 12 часов дня),
- «через две недели» - в соответствии с установкой Interval between purging mail file and deleting used object store (по умолчанию раз в 14 дней),
- «администратор» - после того, как администратор обнаружит запрос в базе и выполнит необходимые действия по запросу.

1.47.3.

1.1.3. Понятие сервера администрирования базы

Это сервер, программа Adminp которого вносит изменения в данную реплику базы (в ACL и документы). Такой сервер должен быть назначен для каждой базы (иначе изменения в базу не вносятся) и должен быть назначен только один (иначе несколько программ Adminp внесут изменения каждая в свою реплику базы и это может привести к возникновению репликационных конфликтов).

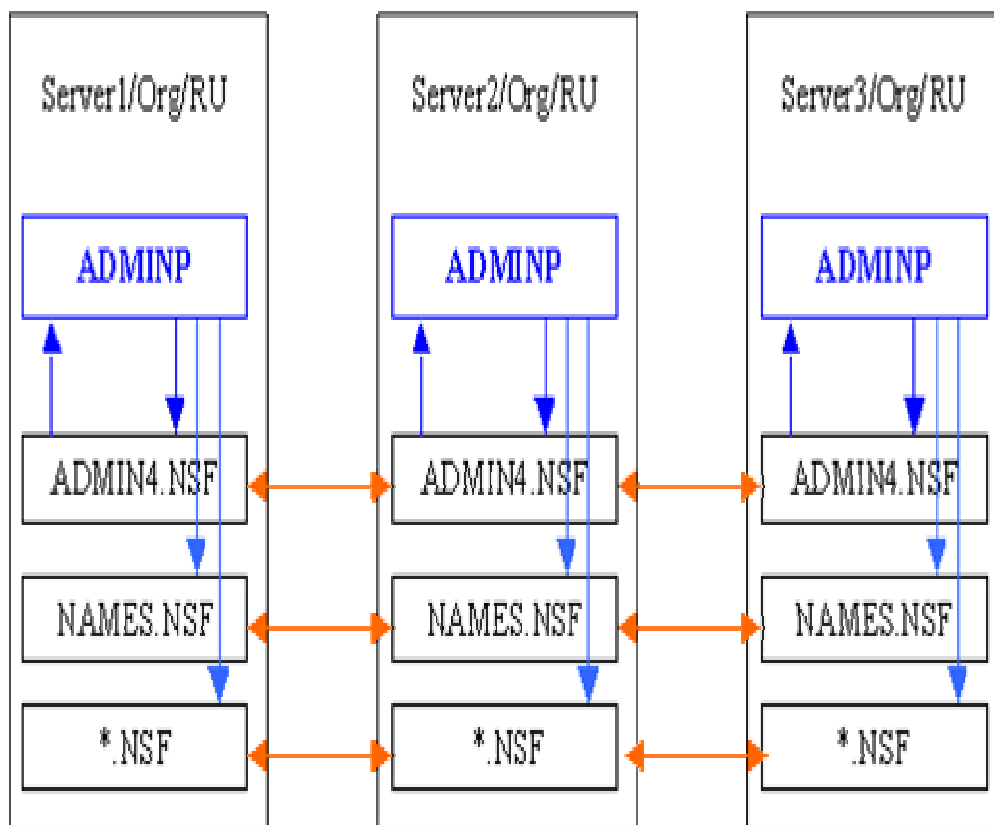


Рис. 330 Закладка Advanced в ACL базы

1.47.4. 1.1.4. Конфигурирование программы ADMINP

Server : LAEC/ETC/InterTrust/RU

Basics | Security | Ports | Server Tasks | Internet Protocols | MTAs | Miscellaneous | Transactional Logging | Shared Mail | Administration

Administration Process | Agent Manager | Domain Catalog | Directory Cataloger | Internet Cluster Manager | Web Retriever | Remote Debug Manager

Basics Maximum number of threads: 3	Mailfile Deletion Interval Interval between purging mail file and deleting when using object store: 1 day(s)
Normal Request Settings Interval: 10 minutes Execute once a day requests at: 22:00	Delayed Request Settings Start executing on: Sun, Mon, Tue, Wed, Thu, Fri, Sat day(s) Start executing at: 23:00
Miscellaneous Mail file moves expire after: 21 days Store Admin Process log entries when status of no change is recorded: Yes ☐ Suspend Admin Process at: Restart Admin Process at:	

Рис. 331 Документ Server, закладка Server Tasks – Administration Process

- **Interval** - частота в минутах, с которой программа проверяет появление запросов в базе Administration Requests и выполняет запросы с частотой исполнения «через интервал». По умолчанию - 60 минут.
- **Execute once a day requests at** – время для выполнения «ежедневных» запросов (запросы на внесение изменений в документы Person и "Rename person in unread lists"). По умолчанию - 12 часов дня.

- • **Start executing on** и **Start executing at** - по каким дням недели и во сколько времени должны выполняться «еженедельные» запросы (запросы на внесение изменений в поля типов Authors и Readers и на поиск общих (shared) и частных (private) элементов дизайна, созданных удаляемым пользователем). По умолчанию - в воскресенье в 12 часов дня.
- • **Interval between purging mail file and deleting used object store** - интервал времени от удаления почтового ящика до удаления связанных с ним тел сообщений в SCOS. По умолчанию 14 дней.
- • **Maximum number of threads** – количество потоков программы. Каждый поток одновременно обрабатывает один запрос. По умолчанию 3 потока. При большом количестве запросов можно увеличить количество потоков – работа будет выполняться быстрее. При изменении нужно перезапускать программу: `tell adminp q` и затем `load adminp`.
- • **Mail file moves expire after** – через сколько дней запросы на перемещение почтового файла должны считаться устаревшими. По умолчанию 21 день, допустимые значения от 7 до 60 дней.
- • **Store Admin Process log entries when status of no change is recorded** – запросы на изменение в ACL, полях типов Readers, Authors и Names fields management, а так же на управление почтовыми файлами обычно выполняются всеми серверами, но часто влекут создание ответных документов со статусом наподобие «This name did not appear anywhere» или «This file is not on this server». Чтобы такие ответные документы не засоряли базу Admin4.nsf, можно выбрать Yes.
- • **Suspend Admin Process at** – остановить обработку запросов в это время.
- • **Restart Admin Process at** – возобновить обработку запросов в это время.
-

Команды, которые можно передать программе Administration Process

- • **Tell Adminp Process All** - выполнить все типы новых и модифицированных запросов, кроме Delete unlinked mail file.
- • **Tell Adminp Process New** - программа должна проверить только те запросы, которые появились или были модифицированы после момента предыдущей проверки базы, и выполнить их
- • **Tell Adminp Process Interval** - выполнить запросы, которые должны выполняться непосредственно по появлению, а также те, которые должны выполняться в соответствии с установкой Interval.
- • **Tell Adminp Process People** - выполнить только запросы на внесение изменений в документы Person в Каталоге Domino.
- • **Tell Adminp Process Daily** - выполнить новые и модифицированные «ежедневные» запросы.
- • **Tell Adminp Process Delayed** - выполнить запросы, которые должны выполняться в соответствии с установками Start executing on и Start executing at («еженедельные»).
- • **Tell Adminp Process Time** - выполнить все типы новые и модифицированные запросы Delete unlinked mail file.
- • **Tell Adminp Show Databases** - позволяет получить список названий и имен файлов тех баз, для которых данный сервер назначен сервером администрирования, а так же баз, для которых сервер администрирования не назначен.

Замечание перед работой...

Вообще говоря, нельзя запускать одновременно две операции на одного и того же субъекта. Очевидно, если один процесс переименования пользователя еще не завершился, а уже запущен второй процесс переименования, вас ждут проблемы...

1.47.5. 1.1.5. Ресертификация пользователей (продление срока

действия сертификата в ID-файле пользователя, назначение альтернативных имен...) - операция People & Groups - People-Recertify

Сначала изучите документы Person – «иерархию» первого имени в поле-списке User Name. Выбираемый вами для создания нового сертификата пользователю ID-файл сертификатора должен быть тем же самым, как и тот, которым был создан текущий сертификат.

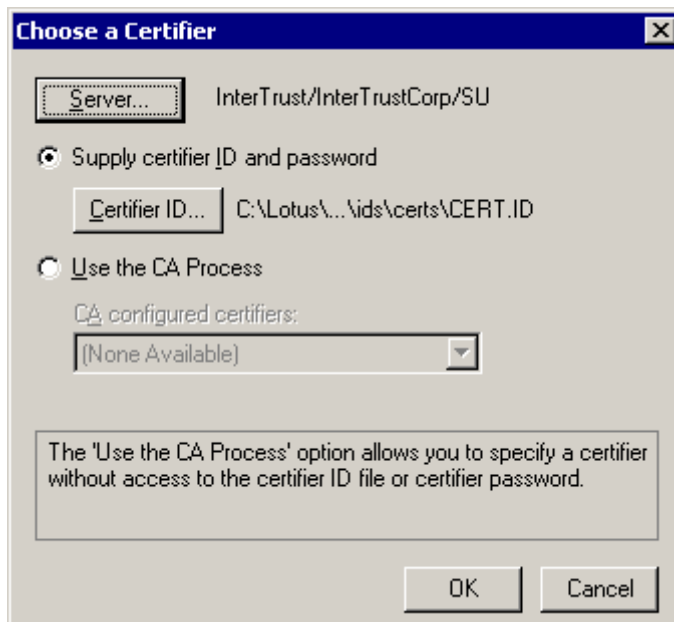


Рис. 332

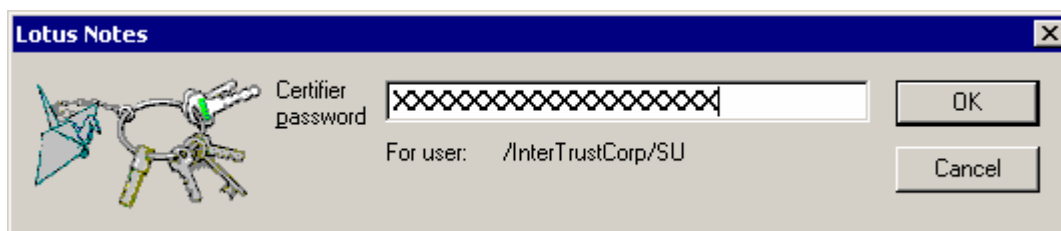


Рис. 333

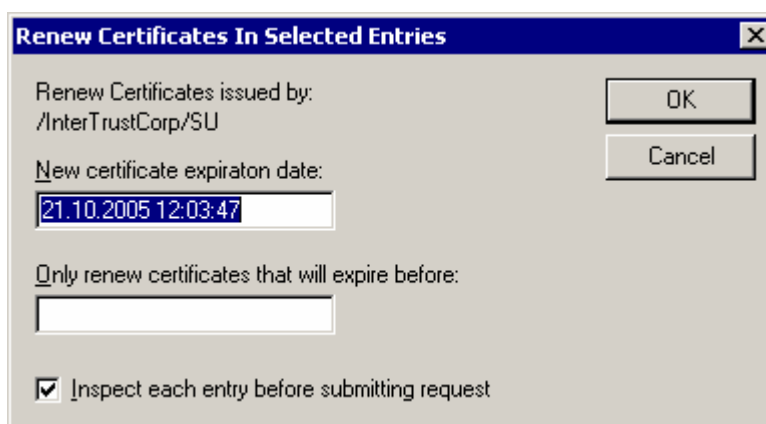


Рис. 334 Выбрав много документов Person и задав в поле Only renew certificates that will expire before дата-временное значение, вы «обновите» сертификаты только тем, у кого они истекут до этого момента времени

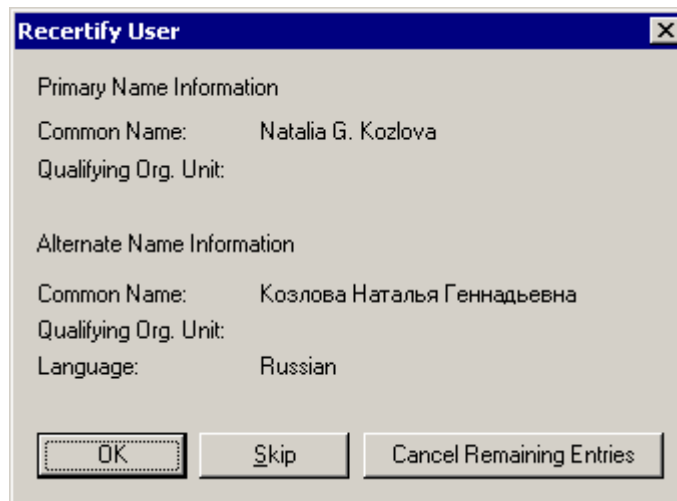


Рис. 335 Окно будет, если в предыдущем выбрана «галка» Inspect... Такое окно выдается на каждого предварительно выбранного пользователя. Кнопкой Ok вы выпускаете сертификат и передаете запрос программе ADMINP, кнопкой Skip пропускаете пользователя.

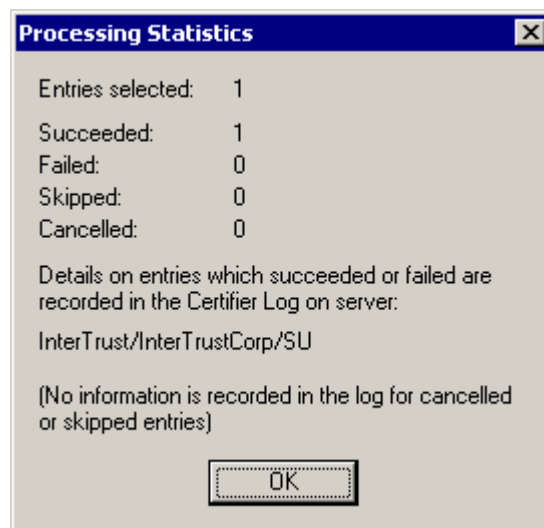


Рис. 336

ADMINISTRATION PROCESS - Request

*Action:	Recertify Person in Domino Directory
*Server(s) to perform the action:	Administration Server for the Domino Directory
*Name(s) to perform the action on:	Natalia G. Kozlova/InterTrustCorp/SU
*Action requested by:	Nikolay N. Iontsev/InterTrustCorp/SU
*Name of process to perform action:	Adminp
Certified public key:	0300E602 E16B0D82 15G0162B 009700BC E47917DD 03G00302 00012086 00AD4062 00416B25 G0024FG0 0258DD2D 00C66D25 00AC4A2C 00A17025 C301A077 00AD4062 00416B25 G0024FG0 0258DD2D 00C66D25 00AC4A2C 00A17025 C34F3D49 6E746572 54727573 74436F72 702F433D 5355434E 3D4E6174 616C6961 20472E20 4B6F7A6C 6F76612F 4F3D496E 74657254 72757374 436F7270 2F433D53 55A38194 30819130 818E060B 60864801 86F80E02 02030104 7F307DA0 021600A1 77317530 73160272 75306D31 0B300906 03550406 13025255 311D301B 06035504 0A1E1404 18043D04 42043504 40042204 40043004 41044231

Рис. 337 Новый сертификат содержится в созданном вами запросе

Date	Sched. Type	Action	Requester
▼ Natalia G. Kozlova/InterTrustCorp/SU			
22.10 12:20		▼ Recertify Person in Domino Directory	Nikolay N. Iontsev
22.10 12:22		InterTrust\InterTrustCorp/SU performed action on: 22.10 12:22	

Рис. 338 Созданный вами запрос реплицируется на сервер администрирования каталога Domino. «Через интервал» появляется ответный документ, означающий, что новый сертификат был помещен ADMINP в документ Person. Затем документ Person реплицируется по Каталогам Domino и с этого момента сервер домена, аутентифицировавший этого пользователя, «замечит», что в документе Person новый сертификат, передаст его на клиента Notes, а клиент Notes заменит им старый сертификат в пользовательском ID-файле... Только любопытный пользователь увидит, что в строке статуса его клиента промелькнуло сообщение об этом событии

Операция работает и в случае, когда сертификат в ID-файле пользователя уже истек.

1.47.6. 1.1.6. Изменение имен пользователей (CN) - операция People & Groups - People-Rename

Сначала изучите документы Person – «иерархию» первого имени в поле-списке User Name. Выбираемый вами для создания нового сертификата пользователю ID-файл сертификатора должен быть тем же самым, как и тот, которым был создан текущий сертификат. Иными словами, иерархия в имени пользователя при этой операции не должна изменяться – изменяется только Common Name, а так же альтернативное имя, прочие «мелочи» и срок действия сертификата.

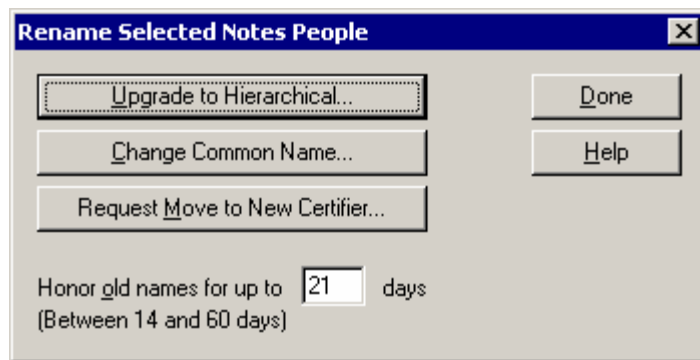


Рис. 339 Кнопка Change Common Name. Поле Honor...можно расценивать как срок истечения запроса на переименование

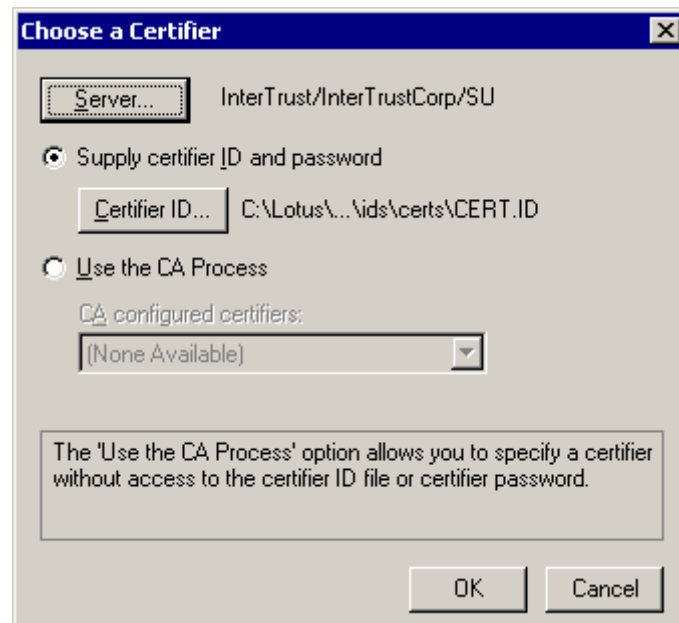


Рис. 340

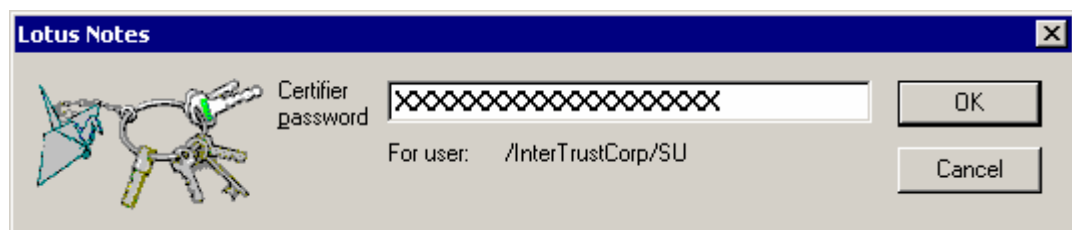


Рис. 341

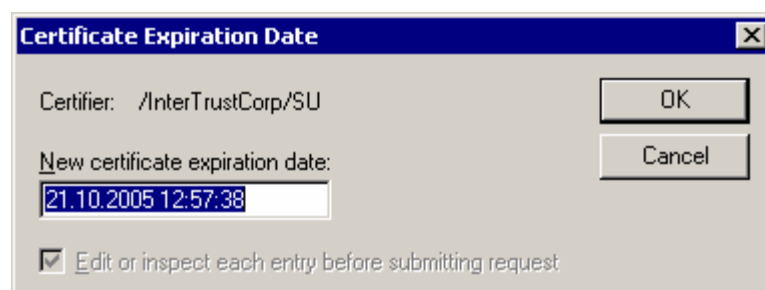


Рис. 342

Rename Person

New Primary Name Information

First name:

Middle name:

Last name:

User19

Qualifying Org. Unit:

LAEC

(optional)

Short name:

User19

(optional)

Internet address:

User19@intrust.ru

(optional)

☐ Rename Windows NT User Account

Specifying a new Internet address results in the old Internet address being added as the next to last entry in the User name field

New Alternate name Information

Common name:

Qualifying Org. Unit:

(optional)

Original language:

New language:

Russian

OK

Skip

Cancel Remaining Entries

Rename Person

New Primary Name Information

First name:

Пользователь

Middle name:

Last name:

User19

Qualifying Org. Unit:

LAEC

(optional)

Short name:

User19

(optional)

Internet address:

User19@intrust.ru

(optional)

☐ Rename Windows NT User Account

Specifying a new Internet address results in the old Internet address being added as the next to last entry in the User name field

New Alternate name Information

Common name:

Пользователь 19

Qualifying Org. Unit:

(optional)

Original language:

New language:

Russian

OK

Skip

Cancel Remaining Entries

Рис. 343 Слева – до изменений, справа – после

Processing Statistics

Entries selected:

1

Succeeded:

1

Failed:

0

Skipped:

0

Cancelled:

0

Details on entries which succeeded or failed are recorded in the Certifier Log on server:

InterTrust/InterTrustCorp/SU

(No information is recorded in the log for cancelled or skipped entries)

OK

Рис. 344

	Date	Sched. Type	Action	Requester
			▶ User06/LAEC/InterTrustCorp/SU ▶ User07/LAEC/InterTrustCorp/SU ▼ User19/LAEC/InterTrustCorp/SU	
	22.10 13:48		Initiate Rename in Domino Directory	Nikolay N. Iontsev
	22.10 13:50		InterTrust/InterTrustCorp/SU performed action on: 22.10 13:50	

Рис. 345 Новый сертификат содержится в созданном вами запросе. Созданный вами запрос реплицируется на сервер администрирования каталога Domino. «Через интервал» появляется ответный документ, означающий, что новый сертификат был помещен ADMINP в документ Person. Затем документ Person реплицируется по Каталогам Domino и с этого момента сервер домена, аутентифицировавший этого пользователя, «замечит», что в документе Person новый сертификат, и передаст его на клиента Notes...

Если добавлялось только альтернативное имя, никаких «видимых» проявлений на клиенте не будет (сертификат конечно изменится). Не будет и продолжения обработки в базе Admin4.nsf – ведь более менять ничего и не надо.

Если изменялось основное имя, в клиенте R6 тоже не будет никаких «видимых» проявлений на клиенте не будет («молчаливая» замена сертификата). В R4/5 в этот момент клиент получал диалоговое окно, в котором мог согласиться или отвергнуть смену имени. Но в любом случае только после этого события будет продолжена обработка в базе Admin4.nsf – ведь изменять старое имя на новое нужно еще во множестве мест.

	Date	Sched. Type	Action	Requester
▼	User19/LAEC/InterTrustCorp/SU			
	22.10 14:12		▼ Initiate Rename in Domino Directory	Nikolay N. Iontsev/InterTrust
	22.10 14:13		InterTrust/InterTrustCorp/SU performed action on: 22.10 14:13	
	22.10 14:14		▼ Rename Person in Domino Directory	InterTrust/InterTrustCorp/SU
	22.10 14:21		InterTrust/InterTrustCorp/SU performed action on: 22.10 14:21	
	22.10 14:21		▼ Rename in Access Control List	InterTrust/InterTrustCorp/SU
	22.10 14:21		InterTrust/InterTrustCorp/SU performed action on: 22.10 14:21	
	22.10 14:24		NotesSvc400/InterTrustCorp/SU performed action on: 22.10 14:24	
	22.10 14:26		LAEC/ETC/InterTrust/RU performed action on: 22.10 14:26	
	22.10 14:28		LINUX/LAEC/InterTrustCorp/SU performed action on: 22.10 14:28	
	22.10 14:21		▼ Rename in Person Documents	InterTrust/InterTrustCorp/SU
	22.10 14:21		InterTrust/InterTrustCorp/SU performed action on: 22.10 14:21	
	22.10 14:21		▼ Rename Person in Unread List	InterTrust/InterTrustCorp/SU
	22.10 14:21		InterTrust/InterTrustCorp/SU performed action on: 22.10 14:21	
	22.10 14:26		LAEC/ETC/InterTrust/RU performed action on: 22.10 14:26	
	22.10 14:21		▼ Rename Person in Free Time Database	InterTrust/InterTrustCorp/SU
	22.10 14:22		LAEC/LAEC/InterTrustCorp/SU performed action on: 22.10 14:22	
	22.10 14:21		▼ Rename Person in Free Time Database	InterTrust/InterTrustCorp/SU
	22.10 14:22		LAEC/LAEC/InterTrustCorp/SU performed action on: 22.10 14:22	
	22.10 14:21		▼ Rename in Reader/Author fields	InterTrust/InterTrustCorp/SU
	22.10 14:26		LAEC/ETC/InterTrust/RU performed action on: 22.10 14:26	
	22.10 14:28		InterTrust/InterTrustCorp/SU performed action on: 22.10 14:28	
	22.10 14:22		▼ Rename Person in Calendar Entries and Profiles in Mail File	InterTrust/InterTrustCorp/SU
	22.10 14:23		LAEC/LAEC/InterTrustCorp/SU performed action on: 22.10 14:23	

Рис. 346 Ход процесса

Basics		Mail	
First name:	Пользователь	Mail system:	Notes
Middle name:		Domain:	InterTrustCorp
Last name:	User19	Mail server:	LAEC/LAEC/InterTrustCorp/SU
User name:	Пользователь User19/LAEC/InterTrustCorp/SU Пользователь User19 User19/LAEC/InterTrustCorp/SU User19	Mail file:	mailuser19
Alternate name:	Пользователь 19/АЦО Lotus/ИнтерТраст/RU Russian	Forwarding address:	
Short name/UserID:	User19	Internet address:	User19@intrust.ru
Personal title:		Format preference for incoming mail:	Keep in senders' format
Generational qualifier:		When receiving unencrypted mail, encrypt before storing in your mailfile:	No
Internet password:	(GwOsWVd5IsVijTtzaUy)		
Preferred language:			
		Real-Time Collaboration	
		Sametime server:	SameTime/InterTrust/RU

Рис. 347 Старые имена сохраняются в списке User Name – это необходимо для нормального хождения почты «по старым адресам»

1.47.7. 1.1.7. Изменение положения пользователя в иерархии (дереве имен) организации - операция People & Groups - People-Rename

Процесс «перевода» запускает «старый» сертификат пользователя.

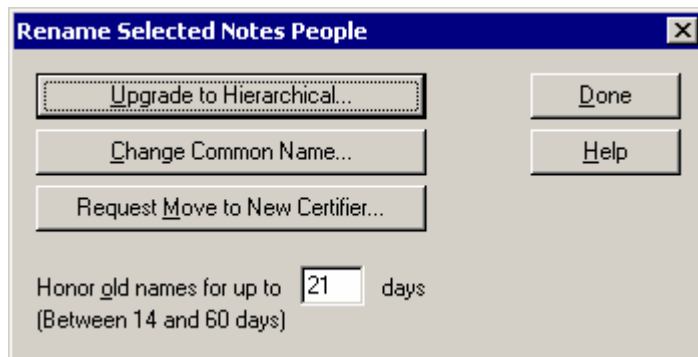


Рис. 348 Кнопка Request Move to New Certifier

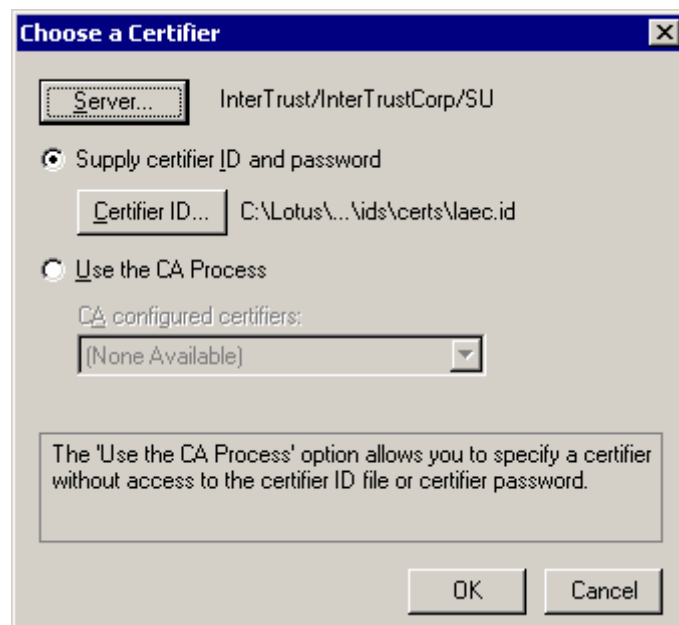


Рис. 349 ID «старого» сертификатора

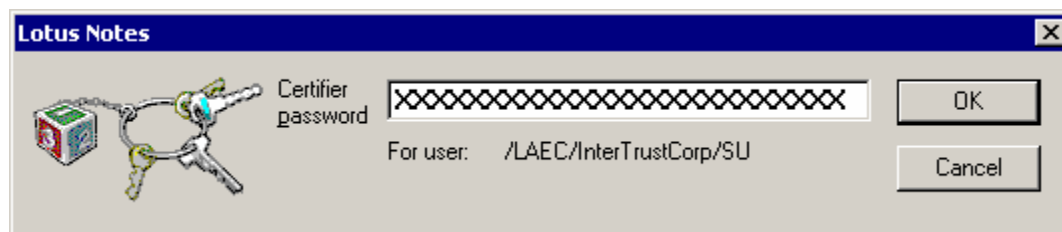


Рис. 350

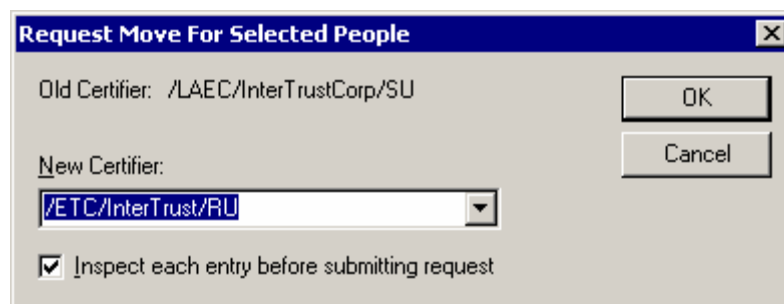


Рис. 351 Сбылась 5-летняя мечта Notes-овых админов всего мира – имя нового сертификатора можно выбрать...

Rename Person [X]

Primary Name Information

Common Name: Пользователь User19

Qualifying Org. Unit:

Alternate Name Information

Common Name: Пользователь 19

Qualifying Org. Unit:

Language: Russian

☒ Allow the primary name to be changed when the name is moved.
(All systems must be running R5.04 or higher for this to work)

OK Skip Cancel Remaining Entries

Рис. 352 Смотреть тут нечего, поэтому «галка» в предыдущем окне по умолчанию не стоит...

Processing Statistics [X]

Entries selected: 1

Succeeded: 1

Failed: 0

Skipped: 0

Cancelled: 0

Details on entries which succeeded or failed are recorded in the Certifier Log on server:
InterTrust/InterTrustCorp/SU

(No information is recorded in the log for cancelled or skipped entries)

OK

Рис. 353 «Старый» сертификат создал запрос на перевод...

	Date	Sched. Type	Action	Requester
▼	Пользователь User19/LAEC/InterTrustCorp/SU			
	22.10 14:47		Move Person's Name in Hierarchy	Nikolay N. Iontsew

Рис. 354 Однако запрос будет оставаться в таком состоянии, пока его не обнаружит и не выполнит «новый» сертификат

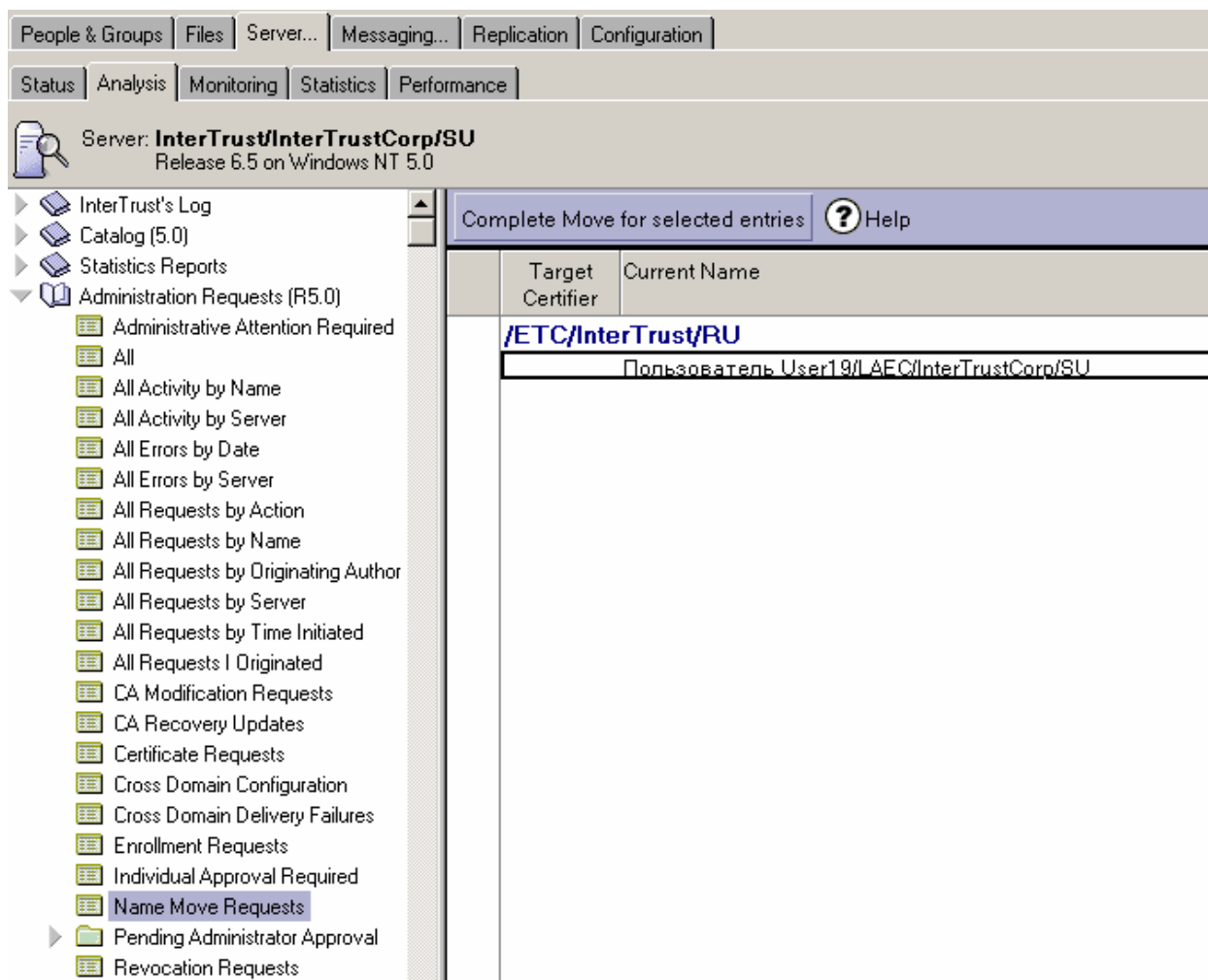


Рис. 355 «Место», в котором сертификаторы «находят» запросы на перевод «к ним» новых сотрудников. Кнопка *Complete Move for selected entries*

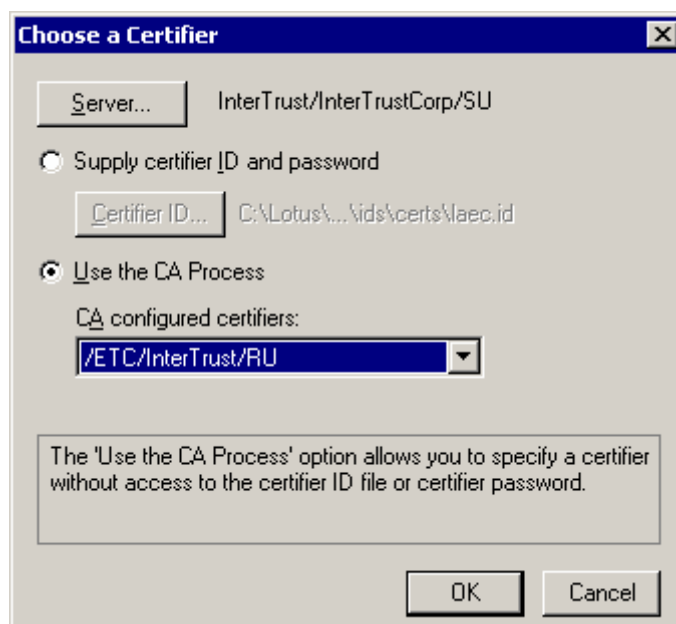
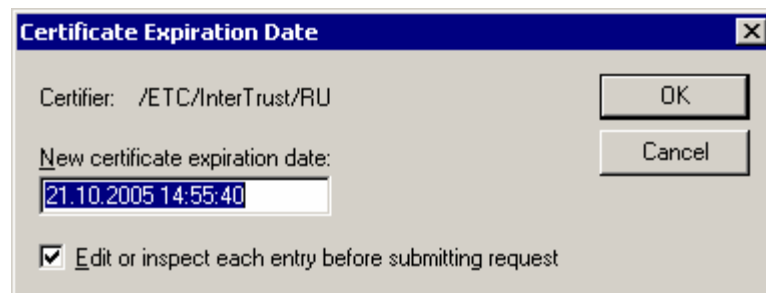


Рис. 356 Выбор ID-файла сертификатора



Certificate Expiration Date

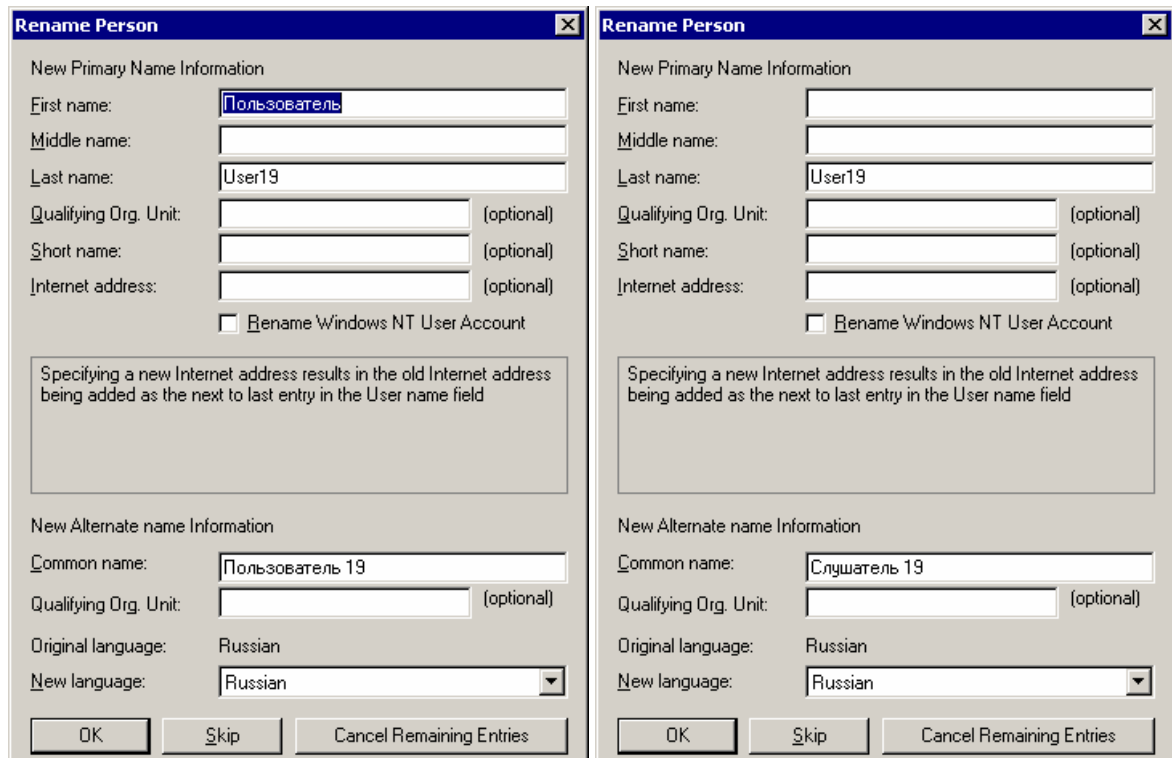
Certifier: /ETC/InterTrust/RU

New certificate expiration date:

☒ Edit or inspect each entry before submitting request

OK Cancel

Рис. 357



Rename Person

New Primary Name Information

First name:

Middle name:

Last name:

Qualifying Org. Unit: (optional)

Short name: (optional)

Internet address: (optional)

☐ Rename Windows NT User Account

Specifying a new Internet address results in the old Internet address being added as the next to last entry in the User name field

New Alternate name Information

Common name:

Qualifying Org. Unit: (optional)

Original language: Russian

New language:

OK Skip Cancel Remaining Entries

Rename Person

New Primary Name Information

First name:

Middle name:

Last name:

Qualifying Org. Unit: (optional)

Short name: (optional)

Internet address: (optional)

☐ Rename Windows NT User Account

Specifying a new Internet address results in the old Internet address being added as the next to last entry in the User name field

New Alternate name Information

Common name:

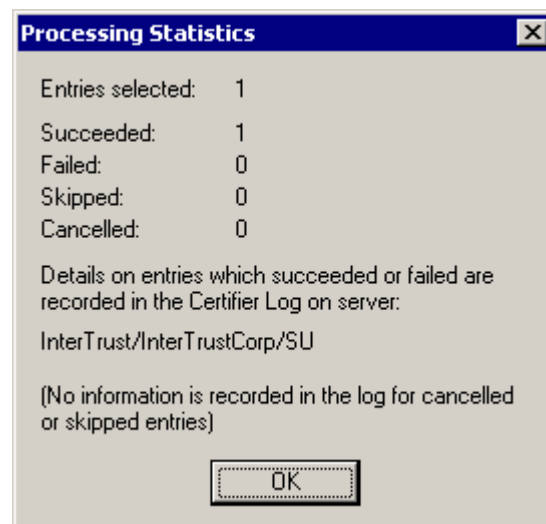
Qualifying Org. Unit: (optional)

Original language: Russian

New language:

OK Skip Cancel Remaining Entries

Рис. 358 Слева – до изменений, справа – после



Processing Statistics

Entries selected: 1

Succeeded: 1

Failed: 0

Skipped: 0

Cancelled: 0

Details on entries which succeeded or failed are recorded in the Certifier Log on server:
 InterTrust/InterTrustCorp/SU

(No information is recorded in the log for cancelled or skipped entries)

OK

Рис. 359 Запрос отработан...

Пользователь User19/LAEC/InterTrustCorp/SU		
22.10 14:47		Move Person's Name in Hierarchy Nikolay N. Iontsew/InterTrus
22.10 15:00		Nikolay N. Iontsew/InterTrustCorp/SU performed action on: 22.10 15:00
22.10 15:01		Initiate Rename in Domino Directory NotesSrv400/InterTrustCorp
22.10 15:02		InterTrust/InterTrustCorp/SU performed action on: 22.10 15:02

Рис. 360 После этого появляется запрос Initiate..., который выполняется «через интервал». Только теперь новый сертификат попадает в документ Person, и пользователь обретает возможность «принять его» в свой ID-файл

People & Groups
Files
Server...
Messaging...
Replication
Configuration

Status
Analysis
Monitoring
Statistics
Performance

Server: **InterTrust/InterTrustCorp/SU**
Release 6.5 on Windows NT 5.0

Tools

InterTrust's Log
Catalog (5.0)
Statistics Reports
Administration Requests (R)
Administrative Attention
All
All Activity by Name
All Activity by Server
All Errors by Date
All Errors by Server
All Requests by Action
All Requests by Name
All Requests by Original
All Requests by Server
All Requests by Time Ir
All Requests I Originate
CA Modification Reque
CA Recovery Updates
Certificate Requests
Cross Domain Configur.
Cross Domain Delivery
Enrollment Requests
Individual Approval Re
Name Move Requests
Pending Administrator /
Revocation Requests

Help

CA	State	Modified	Subject Name
CN=InterTrust Certification Authority/O=InterTrust/ST=Moscow/C=RU ▶ Issued by Certification Authority ▶ O=InterTrust/C=RU ▶ OU=DewO=InterTrust/C=RU ▶ OU=ETC/O=InterTrust/C=RU ▶ Issued by Certification Authority			
		10/22 03:01	CN=User19/OU=ETC/O=InterTrust/C=RU
		10/16 10:47	CN=LINUX/OU=ETC/O=InterTrust/C=RU
		10/16 10:44	CN=LAEC/OU=ETC/O=InterTrust/C=RU
		10/16 10:30	CN=LINUX/OU=ETC/O=InterTrust/C=RU
		10/16 10:30	CN=LAEC/OU=ETC/O=InterTrust/C=RU
		02/20 10:59	CN=Vasily Vasilyevich Roamingow/OU=ETC/O=InterTrust/C=RU

Рис. 361 Только вот выпускала новый сертификат программа CA

User Security

Security Basics

Your Identity

Your Names

Your Certificates

Your Smartcard

Identity of Others

What Others Do

Notes Data

Mail

Your Notes Names

These are your Notes names for login, access and execution control:

User name: User19/ETC/InterTrust/RU

Alternate user name: Слушатель 19/Учебный центр/Компания ИнтерТраст/RU

Alternate Language: Russian

Aliases are other names that can be entered for you in mail and other Notes applications. Aliases may provide shortcuts to entering your user name and are matched to your name via directory lookup. These are not used for login, access or execution control.

Your aliases: User19
Пользователь User19/LAEC/InterTrustCorp/SU
Пользователь User19
User19/LAEC/InterTrustCorp/SU

Name Changes...

Your Internet Email Name(s)

Internet email name: User19@inttrust.ru

People outside of Notes can contact you using this Internet email name. The Notes mail router may also support other Internet email names for you. Ask your administrator for details.

OK Close

Рис. 362 В R6 на клиенте опять никаких «видимых» проявлений – приходится изучать ID-файл, чтобы удостовериться, что сертификат уже принят...

Date	Sched. Type	Action	Requester
Пользователь User19/LAEC/InterTrustCorp/SU			
22.10 14:47		Move Person's Name in Hierarchy	Nikolay N. Iontsev/InterTr
22.10 15:00		Nikolay N. Iontsev/InterTrustCorp/SU performed action on: 22.10 15:00	
22.10 15:01		Initiate Rename in Domino Directory	NotesSrv400/InterTrustC
22.10 15:02		InterTrust/InterTrustCorp/SU performed action on: 22.10 15:02	
22.10 15:09		Rename Person in Domino Directory	InterTrust/InterTrustCorp/
22.10 15:12		InterTrust/InterTrustCorp/SU performed action on: 22.10 15:12	
22.10 15:12		Rename in Access Control List	InterTrust/InterTrustCorp/
22.10 15:13		SameTime/InterTrust/RU performed action on: 22.10 15:13	
22.10 15:14		NotesSrv400/InterTrustCorp/SU performed action on: 22.10 15:14	
22.10 15:20		LAEC/ETC/InterTrust/RU performed action on: 22.10 15:20	
22.10 15:22		InterTrust/InterTrustCorp/SU performed action on: 22.10 15:22	
22.10 15:12		Rename in Person Documents	InterTrust/InterTrustCorp/
22.10 15:12		Rename Person in Unread List	InterTrust/InterTrustCorp/
22.10 15:12		Rename Person in Free Time Database	InterTrust/InterTrustCorp/S
22.10 15:20		LAEC/LAEC/InterTrustCorp/SU performed action on: 22.10 15:20	
22.10 15:20		Rename Person in Calendar Entries and Profiles in Mail File	InterTrust/InterTrustCorp/S
22.10 15:21		LAEC/LAEC/InterTrustCorp/SU performed action on: 22.10 15:21	

Рис. 363 Далее начинается процесс переименования на серверах. Он выполняется в принципе в автоматическом режиме и точно так же, как в предыдущем разделе. Здесь этот процесс еще полностью не завершен...

1.47.8. 1.1.8. Создание реплик почтовых файлов пользователей на другие серверы - операция People & Groups - People-Create Replica(s)

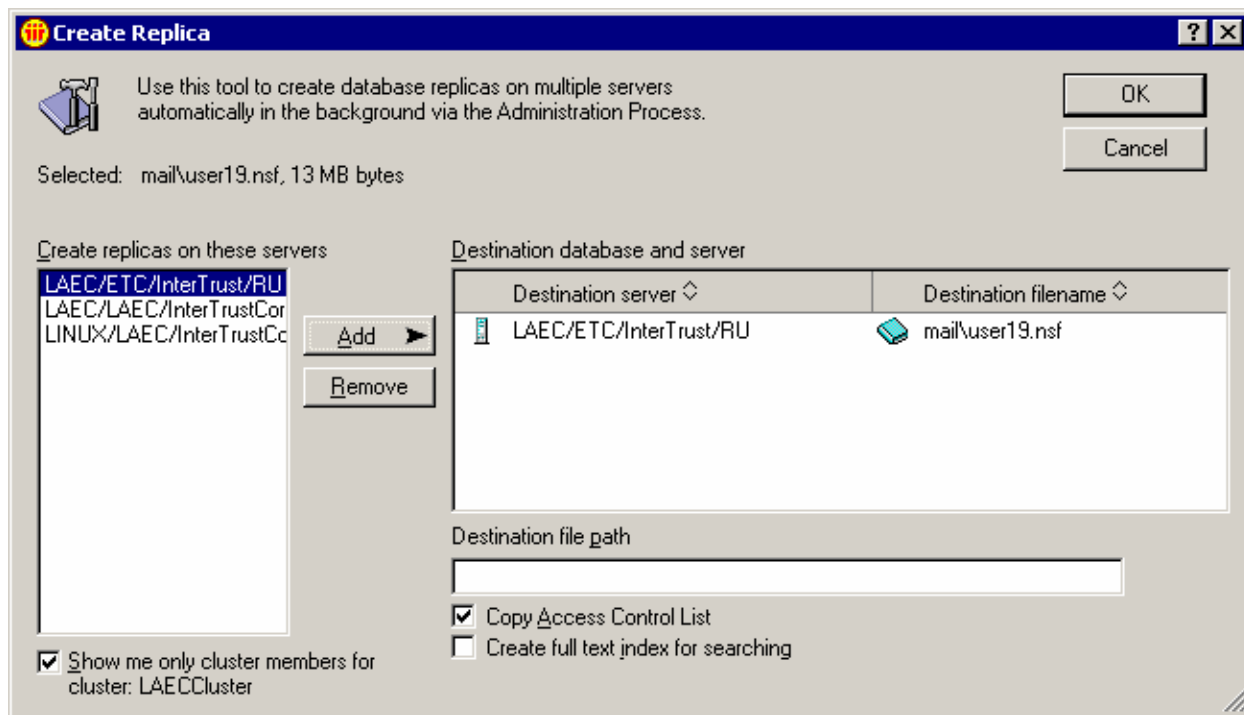


Рис. 364

	Date	Sched. Type	Action	Requester
▼	User19			
	22.10 15:38	🔧	▼ Check Access for New Replica Creation	Nikolay N. Iontsev/InterTrustCo
	22.10 15:39	✅	LAEC/LAEC/InterTrustCorp/SU performed action on: 22.10 15:39	
	22.10 15:39	🔧	▼ Accelerated Create Replica	Nikolay N. Iontsev/InterTrustCo
	22.10 15:40	🔧	LAEC/LAEC/InterTrustCorp/SU performed action on: 22.10 15:40	
	22.10 15:45	🔧	▼ Maintain Trends Database Record	Nikolay N. Iontsev/InterTrustCo
	22.10 15:45	✅	LAEC/LAEC/InterTrustCorp/SU performed action on: 22.10 15:45	

Рис. 365 Получается, что это самая обычная операция создания реплики посредством ADMINP – только имя исходного файла берется из документа Person

1.47.9. 1.1.9. Перемещение почтовых файлов пользователей на другие серверы - операция People & Groups - People-Move to Another Server

Move User(s) To Another Server [?] [X]

Use this tool to move user mail and roaming files in the background using the Administration Process.

Selected: User19/ETC/InterTrust/RU

Destination: LAEC/ETC/InterTrust/RU

☐ Move roaming files into this folder on LAEC/ETC/InterTrust/RU:
 roaming\

☒ Move mail files into this folder on LAEC/ETC/InterTrust/RU:
 mail\

☐ Link to Object Store
☐ Delete old replicas in current cluster

Select the server(s) and path(s) you want to create the mail files(s) on:

	Additional mail server:	Folder:
☒	LAEC/ETC/InterTrust/RU	mail\
☐	LAEC/LAEC/InterTrustCorp/SU	
☐	LINUX/LAEC/InterTrustCorp/SU	

Select the folder in which you would like to move the user's mail and roaming files. To enable replica creation of mail files, check the destination server and choose a folder.

OK Cancel

Рис. 366

Domino Administrator [X]

Request(s) to move 1 user's mail and/or roaming file(s) have been successfully submitted to the Administration Request database.

OK

Рис. 367

	Date	Sched. Type	Action	Requester
▼	User19/ETC/InterTrust/RU			
	22.10 15:09	⚡	▶ Change User Password in Domino Directory	InterTrust/InterTrustCorp/SU
	22.10 15:55	⚡	▼ Check Mail Server's Access	Nikolay N. Iontsev/InterTrustC
	22.10 15:55	📧	LAEC/LAEC/InterTrustCorp/SU performed action on: 22.10 15:55	
	22.10 16:00	⚡	▼ Create New Mailfile Replica	Nikolay N. Iontsev/InterTrustC
	22.10 16:01	✅	LAEC/LAEC/InterTrustCorp/SU performed action on: 22.10 16:01	
	22.10 16:01	⚡	▼ Maintain Trends Database Record	Nikolay N. Iontsev/InterTrustC
	22.10 16:02	✅	LAEC/LAEC/InterTrustCorp/SU performed action on: 22.10 16:02	
	22.10 16:01	⚡	▼ Add New Mailfile Fields	Nikolay N. Iontsev/InterTrustC
	22.10 16:02	✅	InterTrust/InterTrustCorp/SU performed action on: 22.10 16:02	
	22.10 16:02	📧	Monitor New Mailfile Fields	Nikolay N. Iontsev/InterTrustC

Рис. 368 В этой точке процесс «ожидает» открытия пользователем своего почтового ящика...
 Ожидание может длиться 21 день (поле Mail file moves expire after в документе Server)...

Date	Sched. Type	Action	Requester
22.10 16:02		▼ Monitor New Mailfile Fields	Nikolay N. Ion
22.10 16:10		LAEC/ETC/InterTrust/RU performed action on: 22.10 16:10	
22.10 16:10		▼ Replace Mailfile Fields	Nikolay N. Ion
22.10 16:12		InterTrust/InterTrustCorp/SU performed action on: 22.10 16:12	
22.10 16:18		▼ Update Client Information in Person Record	User19/ETC/li
22.10 16:18		InterTrust/InterTrustCorp/SU performed action on: 22.10 16:18	
22.10 16:18		▼ Push Changes to New Mail Server	Nikolay N. Ion
22.10 16:23		LAEC/LAEC/InterTrustCorp/SU performed action on: 22.10 16:23	
22.10 16:23		▼ Get Mail File Information for Deletion	Nikolay N. Ion
22.10 16:24		LAEC/LAEC/InterTrustCorp/SU performed action on: 22.10 16:24	
22.10 16:24		▼ Approve Mail File Deletion	Nikolay N. Ion
22.10 16:25		Nikolay N. Iontsev/InterTrustCorp/SU performed action on: 22.10 16:25	
22.10 16:25		▼ Request Mail File Deletion	Nikolay N. Ion
22.10 16:26		InterTrust/InterTrustCorp/SU performed action on: 22.10 16:26	
22.10 16:26		▼ Delete Mailfile	Nikolay N. Ion
22.10 16:38		LAEC/LAEC/InterTrustCorp/SU performed action on: 22.10 16:38	

Рис. 369 После первого открытия клиентом своего почтового ящика процесс вступает во вторую фазу. При втором открытии клиентом почтового ящика вносятся изменения в документ Location – новый почтовый сервер. Удаление реплики почтового ящика на прежнем сервере требует подтверждения администратором.

1.47.10. 1.1.10. Преобразование «обычных» пользователей в «перемещающихся» и наоборот - операция People & Groups - People-Roaming

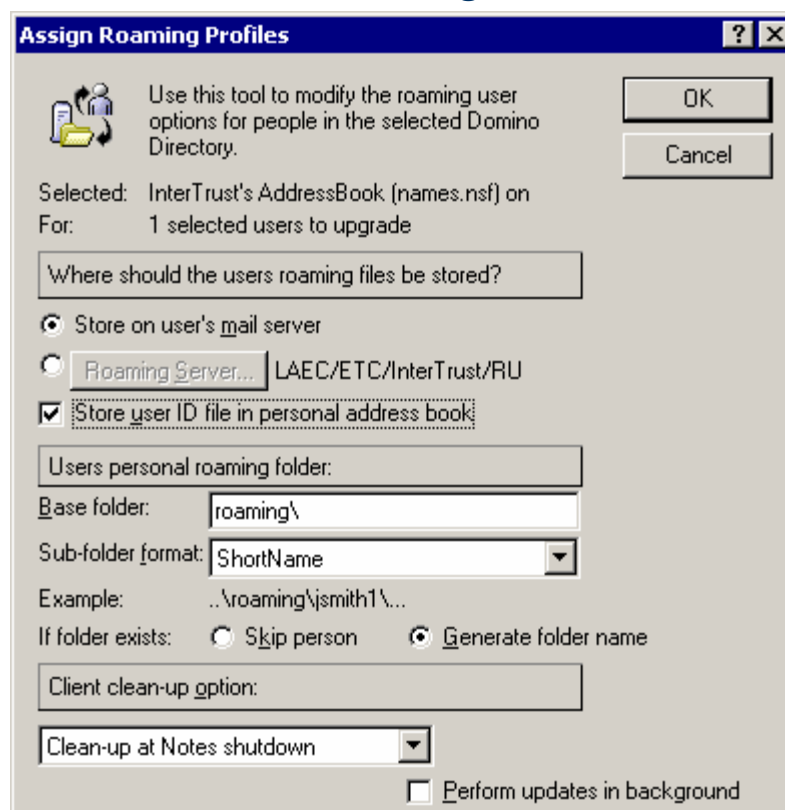


Рис. 370

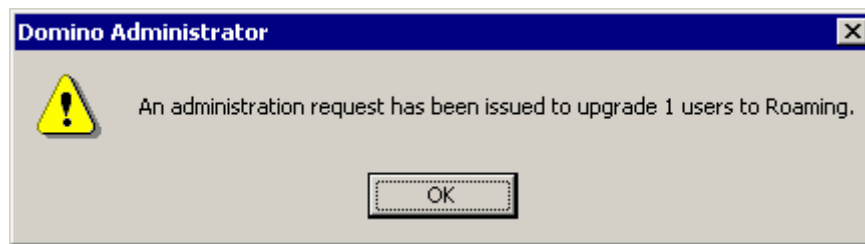


Рис. 371

	Date	Sched. Type	Action	Requester
▼	User19/ETC/InterTrust/RU			
	22.10 15:09	⚡	► Change User Password in Domino Directory	InterTrust/Inte
	22.10 16:58	⚡	▼ Update Roaming User State in Person Record	Nikolay N. lor
	22.10 16:58	✓	InterTrust/InterTrustCorp/SU performed action on: 22.10 16:58	
	22.10 17:10	⚡	▼ Create Roaming User's Replica Stubs	Nikolay N. lor
	22.10 17:13	✓	LAEC/ETC/InterTrust/RU performed action on: 22.10 17:13	
	22.10 17:13	⚡	▼ Update Roaming User Information in Person Record	Nikolay N. lor
	22.10 17:16	✓	InterTrust/InterTrustCorp/SU performed action on: 22.10 17:16	
	22.10 17:16	⚡	▼ Monitor Roaming User's Replica Stubs	Nikolay N. lor
	22.10 17:25	✓	LAEC/ETC/InterTrust/RU performed action on: 22.10 17:25	
	22.10 17:25	⚡	▼ Update Roaming User State in Person Record	Nikolay N. lor
	22.10 17:26	✓	InterTrust/InterTrustCorp/SU performed action on: 22.10 17:26	

Рис. 372 Ход процесса

По окончании обработки запроса Update Roaming User State in Personal Record и репликации сервера администрирования каталога Domino с Roaming-сервером пользователь пускает клиента Notes. ID-файл находится на машине пользователя – под ним пользователь работал ранее в «обычном» режиме. Происходит следующее.

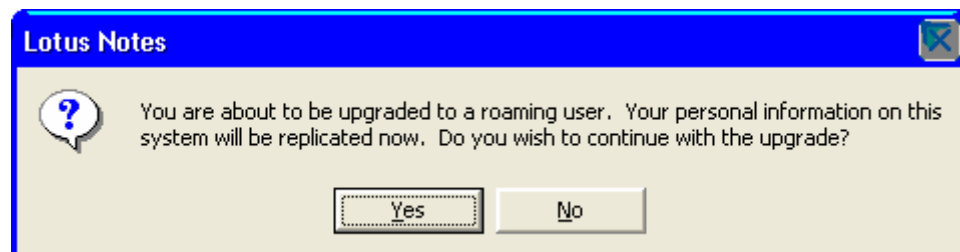


Рис. 373

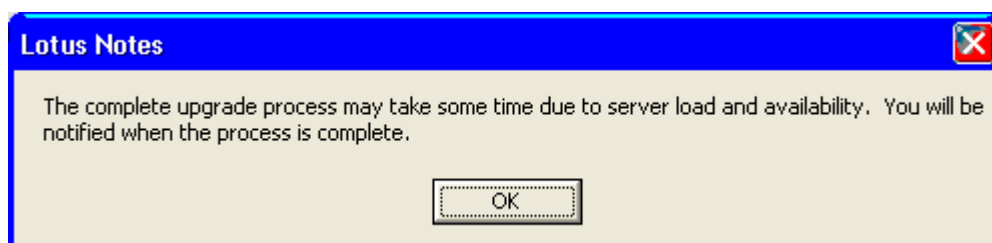


Рис. 374 Далее пользователь продолжает работу...

При попытке выхода из клиента происходит следующее.

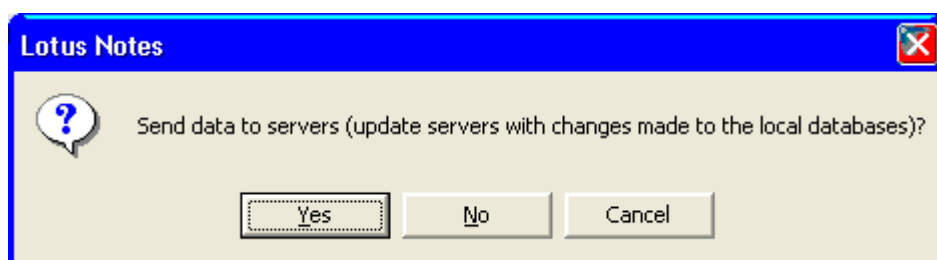


Рис. 375

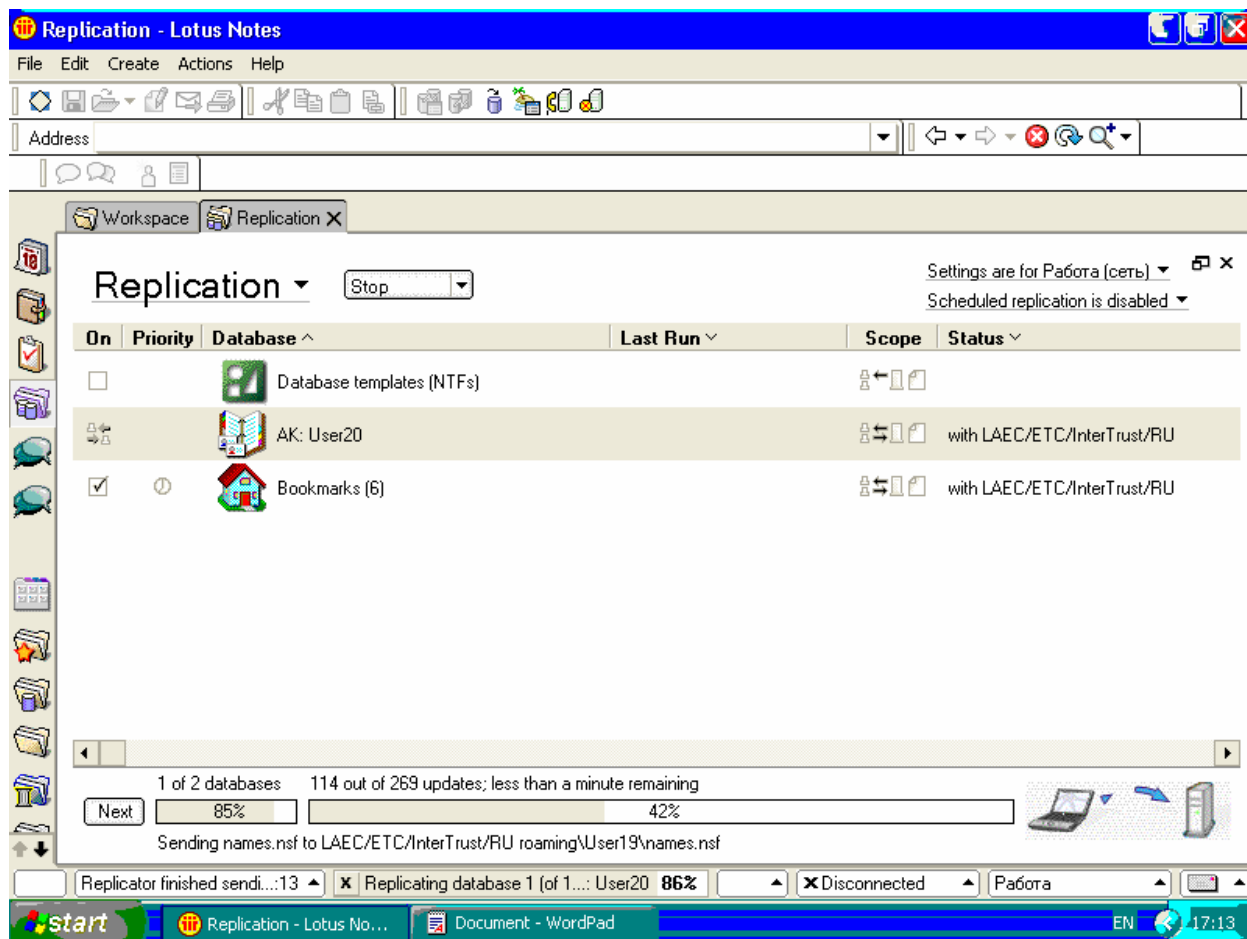


Рис. 376 Создаются реплики Адресной книги и базы закладок («журнала» не было). Надо полагать, именно в этот момент ID-файл помещается в Адресную книгу (так просили при создании запроса)

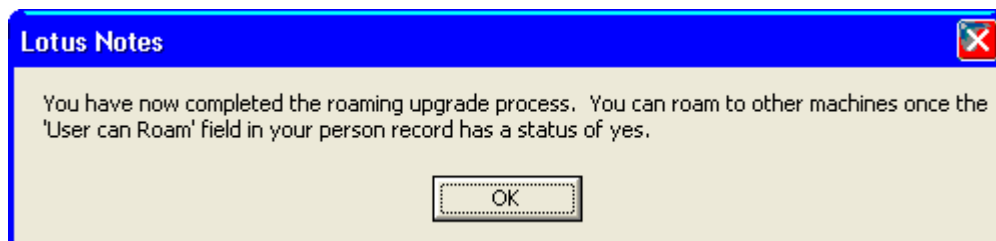


Рис. 377 На этом клиент закрылся...

Судя по времени, после этого в автоматическом режиме выполняются еще минимум 3 запроса.

Копия ID-файла остается на компьютере клиента. Я еще пару раз запускал клиента, наблюдая обычные «начальные» и «завершающие» репликации. Затем из принципа переименовал ID-файл перед следующим запуском – клиент не запустился. Пришлось «вычистить» NOTES.INI и провести повторно вторую фазу установки клиента. Клиент

успешно установился, извлек ID из адресной книги (нигде более его не было) и запустился, что подтверждает наличие ID в локальной адресной книге.

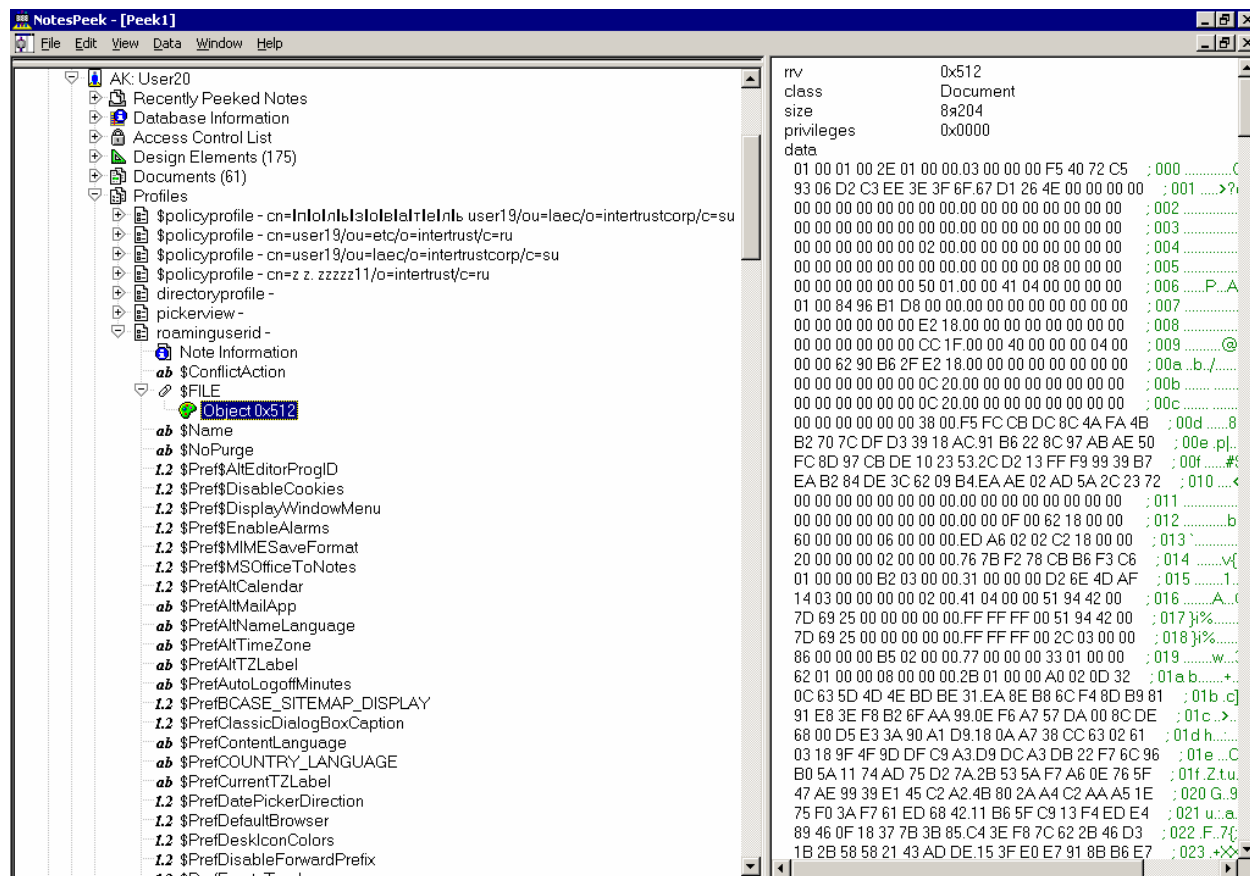


Рис. 378 Возможно, ID хранится в этом профильном документе...

Рассмотрим обратный процесс... Прежде всего убедитесь, что клиент сохранил ID-файл.

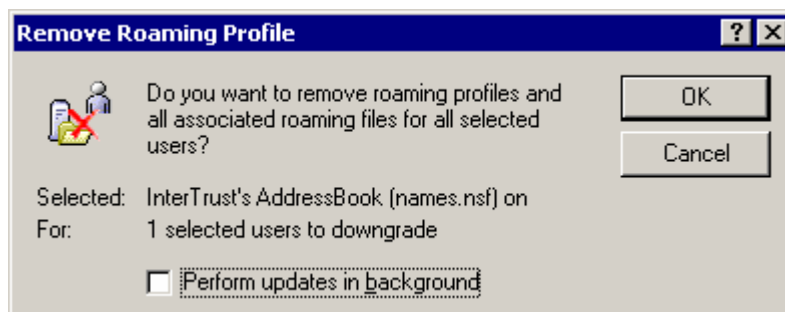


Рис. 379

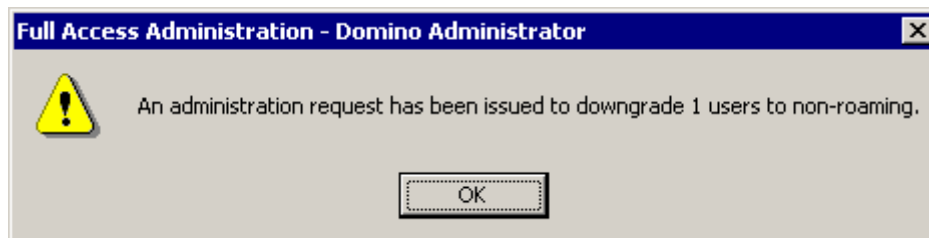


Рис. 380

Без вмешательства пользователя (клиент не запускался пока) процесс дошел до такой точки.

	Date	Sched. Type	Action	Requester
▼	User19/ETC/InterTrust/RU			
	22.10 15:09	⚡	► Change User Password in Domino Directory	InterTrust/Inte
	22.10 18:21	⚡	▼ Update Roaming User State in Person Record	Nikolay N. Iontsev/lr
	22.10 18:22	✓	InterTrust/InterTrustCorp/SU performed action on: 22.10 18:22	
	22.10 18:22	⚡	▼ Remove Roaming User's Roaming Files	Nikolay N. Iontsev/lr
	22.10 18:23	✓	LAEC/ETC/InterTrust/RU performed action on: 22.10 18:23	
	22.10 18:23	⚡	▼ Get Replica Information for Deletion	Nikolay N. Iontsev/lr
	22.10 18:24		LAEC/LAEC/InterTrustCorp/SU performed action on: 22.10 18:24	
	22.10 18:24	✓	LAEC/ETC/InterTrust/RU performed action on: 22.10 18:24	
	22.10 18:24		InterTrust/InterTrustCorp/SU performed action on: 22.10 18:24	
	22.10 18:24		NotesSrv400/InterTrustCorp/SU performed action on: 22.10 18:24	
	22.10 18:24		LINUX/LAEC/InterTrustCorp/SU performed action on: 22.10 18:24	
	22.10 18:28		SameTime/InterTrust/RU performed action on: 22.10 18:28	
	22.10 18:23	⚡	▼ Get Replica Information for Deletion	Nikolay N. Iontsev/lr
	22.10 18:24		LAEC/LAEC/InterTrustCorp/SU performed action on: 22.10 18:24	
	22.10 18:24	✓	LAEC/ETC/InterTrust/RU performed action on: 22.10 18:24	
	22.10 18:24		InterTrust/InterTrustCorp/SU performed action on: 22.10 18:24	
	22.10 18:24		NotesSrv400/InterTrustCorp/SU performed action on: 22.10 18:24	
	22.10 18:24		LINUX/LAEC/InterTrustCorp/SU performed action on: 22.10 18:24	
	22.10 18:28		SameTime/InterTrust/RU performed action on: 22.10 18:28	
	22.10 18:24	⚡	Approve Replica Deletion	Nikolay N. Iontsev/lr
	22.10 18:24	⚡	Approve Replica Deletion	Nikolay N. Iontsev/lr

Рис. 381 Не торопись, админ... Убедись, что клиент сохранил ID-файл. Хотя в этот момент клиент уже не сможет «переустановиться», по крайней мере теоретическая возможность отката назад еще существует...

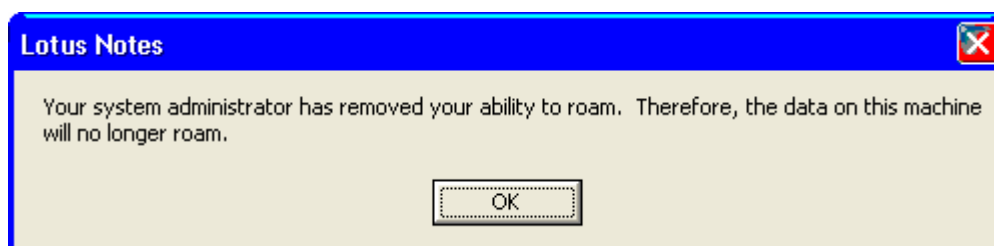


Рис. 382 При запуске клиента пользователь был предупрежден

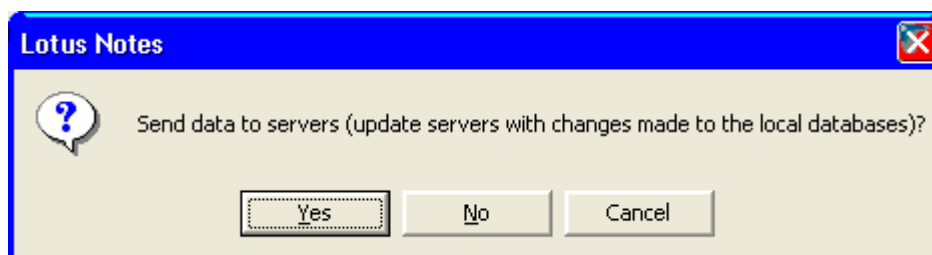


Рис. 383 перед выходом появилось окно, но репликации уже запрещены, ничего не произошло

22.10 18:24		▼ Approve Replica Deletion	Nikolay N. Iontsev/Inter
22.10 18:40		Nikolay N. Iontsev/InterTrustCorp/SU performed action on: 22.10 18:40	
22.10 18:24		▼ Approve Replica Deletion	Nikolay N. Iontsev/Inter
22.10 18:40		Nikolay N. Iontsev/InterTrustCorp/SU performed action on: 22.10 18:40	
22.10 18:40		▼ Request Replica Deletion	Nikolay N. Iontsev/Inter
22.10 18:40		InterTrust/InterTrustCorp/SU performed action on: 22.10 18:40	
22.10 18:40		▼ Request Replica Deletion	Nikolay N. Iontsev/Inter
22.10 18:40		InterTrust/InterTrustCorp/SU performed action on: 22.10 18:40	
22.10 18:40		▼ Delete Replica	Nikolay N. Iontsev/Inter
22.10 18:41		LAEC/ETC/InterTrust/RU performed action on: 22.10 18:41	
22.10 18:40		▼ Delete Replica	Nikolay N. Iontsev/Inter
22.10 18:41		LAEC/ETC/InterTrust/RU performed action on: 22.10 18:41	

Рис. 384 Все, реплики удалены...

1.47.11. 1.1.11. Удаление пользователей - операция People & Groups - People-Delete

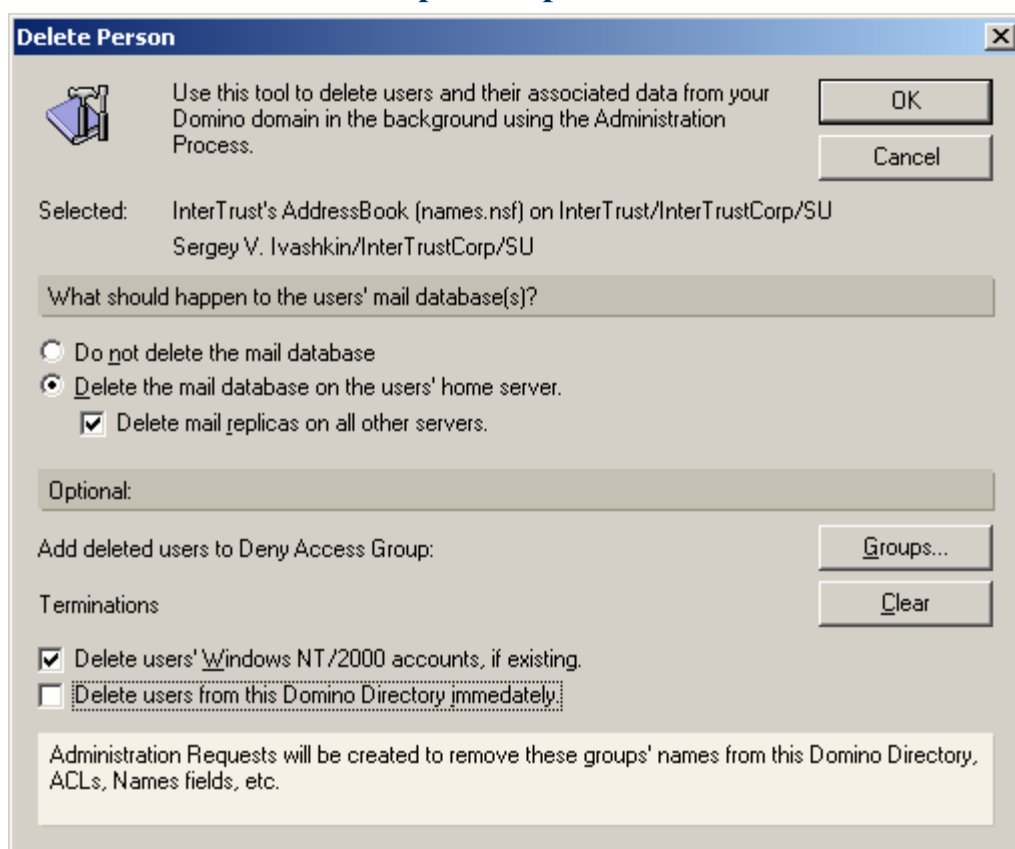


Рис. 385 Запуск операции

	Date	Sched. Type	Action	Requester
▼ Sergey V. Ivashkin/InterTrustCorp/SU				
	22.08 12:49		▼ Delete Person in Domino Directory	Nikolay N. Iontsev/lr
	22.08 12:55		InterTrust/InterTrustCorp/SU performed action on: 22.08 12:55	
	22.08 12:55		Delete in Person Documents	Nikolay N. Iontsev/lr
	22.08 12:55		▼ Delete in Access Control List	Nikolay N. Iontsev/lr
	22.08 12:53		Domino500/InterTrustCorp/SU performed action on: 22.08 12:53	
	22.08 12:57		LAEC/LAEC/InterTrustCorp/SU performed action on: 22.08 12:57	
	22.08 12:59		NotesSrv400/InterTrustCorp/SU performed action on: 22.08 12:59	
	22.08 13:05		InterWork/InterTrust/RU performed action on: 22.08 13:05	
	22.08 13:05		InterTrust/InterTrustCorp/SU performed action on: 22.08 13:05	
	22.08 13:06		LINUX/LAEC/InterTrustCorp/SU performed action on: 22.08 13:06	
	22.08 13:12		SameTime/InterTrust/RU performed action on: 22.08 13:12	
	22.08 13:17		Rainbow/Dev/InterTrust/RU performed action on: 22.08 13:17	
	22.08 13:17		Web3/InterTrustCorp/SU performed action on: 22.08 13:17	
	22.08 13:20		QuickPlace/InterTrust/RU performed action on: 22.08 13:20	
	22.08 13:20		Web2/InterTrustCorp/SU performed action on: 22.08 13:20	
	22.08 13:26		Development/InterTrustCorp/SU performed action on: 22.08 13:26	
	22.08 13:27		AS400/InterTrust/RU performed action on: 22.08 13:27	
	22.08 13:38		WebDevelopment/Web/InterTrustCorp/SU performed action on: 22.08 13:38	
	22.08 12:55		▼ Get Mail File Information for Deletion	Nikolay N. Iontsev/lr
	22.08 12:56		NotesSrv400/InterTrustCorp/SU performed action on: 22.08 12:56	
	22.08 12:56		▼ Approve Mail File Deletion	Nikolay N. Iontsev/lr
	22.08 13:20		Nikolay N. Iontsev/InterTrustCorp/SU performed action on: 22.08 13:20	
	22.08 13:20		▼ Request Mail File Deletion	Nikolay N. Iontsev/lr
	22.08 13:20		InterTrust/InterTrustCorp/SU performed action on: 22.08 13:20	
	22.08 13:20		▼ Delete Mailfile	Nikolay N. Iontsev/lr
	22.08 13:29		NotesSrv400/InterTrustCorp/SU performed action on: 22.08 13:29	
	22.08 13:29		▼ Get Mail File Information for Deletion	Nikolay N. Iontsev/lr
	22.08 13:22		Domino500/InterTrustCorp/SU performed action on: 22.08 13:22	
	22.08 13:30		NotesSrv400/InterTrustCorp/SU performed action on: 22.08 13:30	
	22.08 13:30		InterTrust/InterTrustCorp/SU performed action on: 22.08 13:30	
	22.08 13:34		WebDevelopment/Web/InterTrustCorp/SU performed action on: 22.08 13:34	
	22.08 13:35		SameTime/InterTrust/RU performed action on: 22.08 13:35	
	22.08 13:35		LAEC/LAEC/InterTrustCorp/SU performed action on: 22.08 13:35	
	22.08 13:35		InterWork/InterTrust/RU performed action on: 22.08 13:35	
	22.08 13:36		QuickPlace/InterTrust/RU performed action on: 22.08 13:36	
	22.08 13:38		Development/InterTrustCorp/SU performed action on: 22.08 13:38	
	22.08 13:38		LINUX/LAEC/InterTrustCorp/SU performed action on: 22.08 13:38	
	22.08 13:39		AS400/InterTrust/RU performed action on: 22.08 13:39	
	22.08 13:30		▼ Approve Mail File Deletion	Nikolay N. Iontsev/lr
	22.08 13:32		Nikolay N. Iontsev/InterTrustCorp/SU performed action on: 22.08 13:32	
	22.08 13:32		▼ Request Mail File Deletion	Nikolay N. Iontsev/lr
	22.08 13:32		InterTrust/InterTrustCorp/SU performed action on: 22.08 13:32	
	22.08 13:32		▼ Delete Mailfile	Nikolay N. Iontsev/lr
	22.08 13:35		InterTrust/InterTrustCorp/SU performed action on: 22.08 13:35	

Рис. 386 Процесс выполнения

Администратор должен подтвердить удаление почтовых файлов. В данном случае имелись 2 реплики почтового файла, подтверждать удаление потребовалось для каждой.

1.47.12. 1.1.12. Создание реплик баз на другие серверы - операция Files - Database-Create Replica(s)

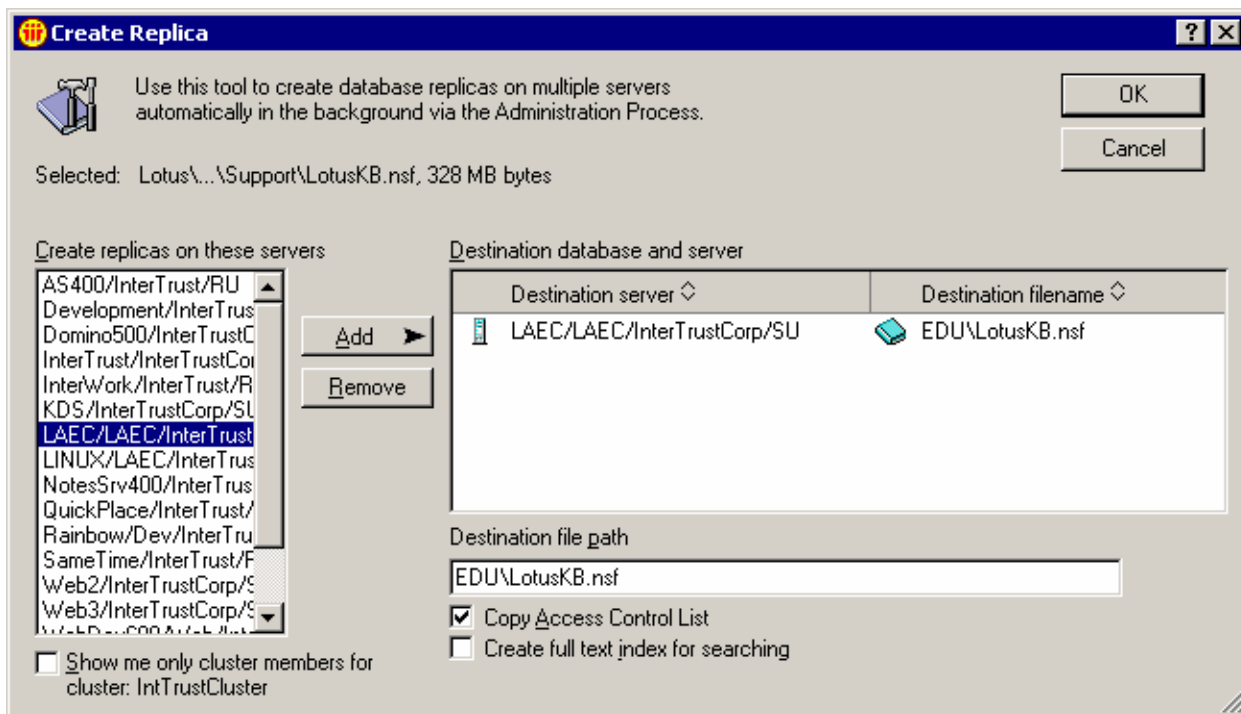


Рис. 387 Запуск операции

Date	Sched. Type	Action	Requester
Lotus Software Knowledge Base			
30.09 13:43	✓	Check Access for New Replica Creation	Nikolay N. Iontsev/InterTrustCorp/SU
30.09 13:44	✓	InterTrust/InterTrustCorp/SU performed action on: 30.09 13:44	
30.09 13:44	✓	Accelerated Create Replica	Nikolay N. Iontsev/InterTrustCorp/SU
30.09 13:45	✓	InterTrust/InterTrustCorp/SU performed action on: 30.09 13:45	
30.09 13:45	✓	Create Replica	Nikolay N. Iontsev/InterTrustCorp/SU
30.09 13:47	✓	LAEC/LAEC/InterTrustCorp/SU performed action on: 30.09 13:47	
30.09 13:47	✓	Maintain Trends Database Record	Nikolay N. Iontsev/InterTrustCorp/SU
30.09 13:49	✓	InterTrust/InterTrustCorp/SU performed action on: 30.09 13:49	

Рис. 388 Процесс выполнения

1.47.13. 1.1.13. Перемещение баз на другие серверы - операция Files - Database-Move

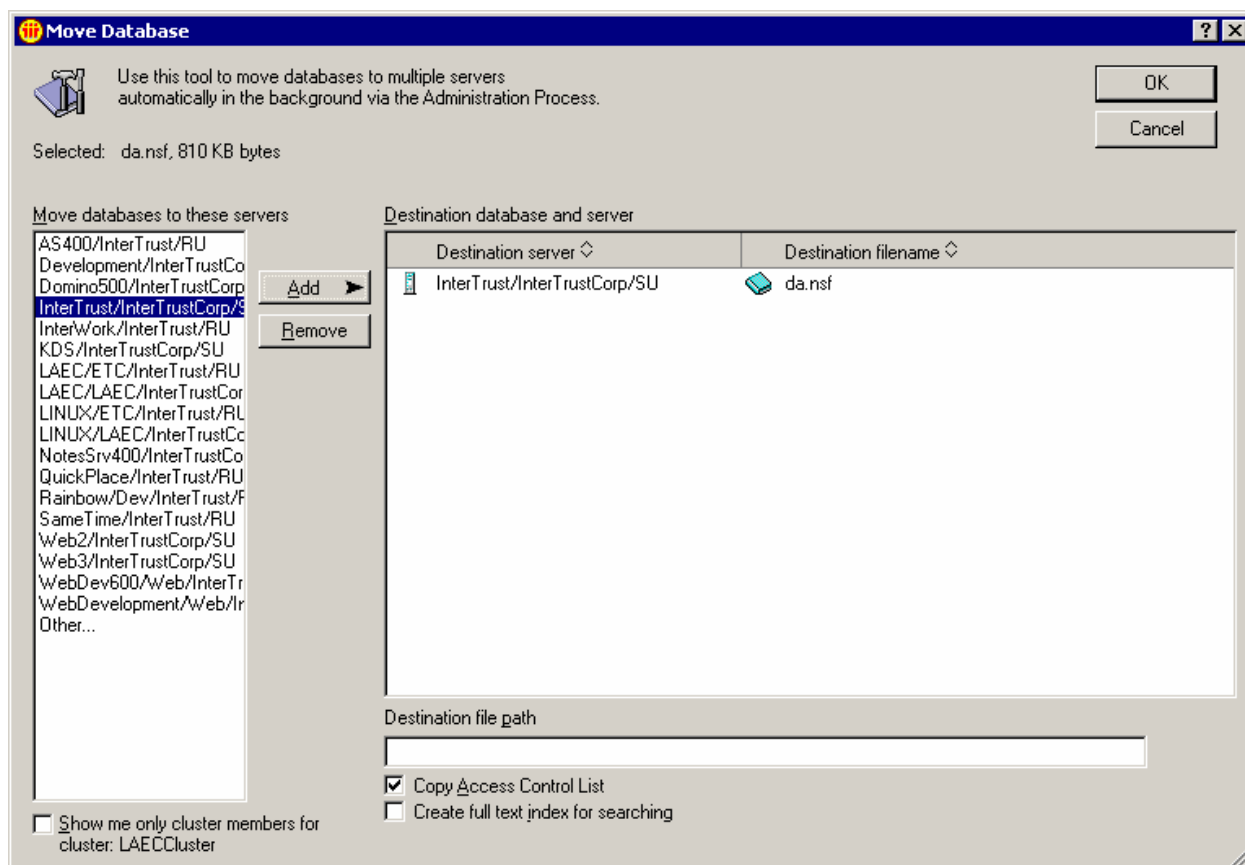


Рис. 389

	Date	Sched. Type	Action	Requester
▼ AF Change Log 2.5 - Ш				
	30.09 10:48	⚡	▼ Check Access for Move Replica Creation	Danila A. Trushin/InterTrust
	30.09 10:49	✓	InterTrust/InterTrustCorp/SU performed action on: 30.09 10:49	
	30.09 10:49	⚡	▼ Accelerated Create Replica	Danila A. Trushin/InterTrust
	30.09 10:50	🔄	InterTrust/InterTrustCorp/SU performed action on: 30.09 10:50	
	30.09 10:50	🌐	▼ Delete Original Replica after Move	Danila A. Trushin/InterTrust
	30.09 11:00	✓	InterTrust/InterTrustCorp/SU performed action on: 30.09 11:00	
	30.09 10:50	⚡	▼ Maintain Trends Database Record	Danila A. Trushin/InterTrust
	30.09 10:55	✓	InterTrust/InterTrustCorp/SU performed action on: 30.09 10:55	
	30.09 10:53	⚡	▼ Check Access for Move Replica Creation	Danila A. Trushin/InterTrust
	30.09 11:00	✓	InterTrust/InterTrustCorp/SU performed action on: 30.09 11:00	
	30.09 11:00	⚡	▼ Accelerated Create Replica	Danila A. Trushin/InterTrust
	30.09 11:01	🔄	InterTrust/InterTrustCorp/SU performed action on: 30.09 11:01	
	30.09 11:01	🌐	▼ Delete Original Replica after Move	Danila A. Trushin/InterTrust
	30.09 11:11	✓	InterTrust/InterTrustCorp/SU performed action on: 30.09 11:11	
	30.09 11:01	⚡	▼ Maintain Trends Database Record	Danila A. Trushin/InterTrust
	30.09 11:04	✓	InterTrust/InterTrustCorp/SU performed action on: 30.09 11:04	

Рис. 390 Процесс выполнения

1.47.14.

1.1.14.

Удаление групп - операция People & Groups - Groups-Delete

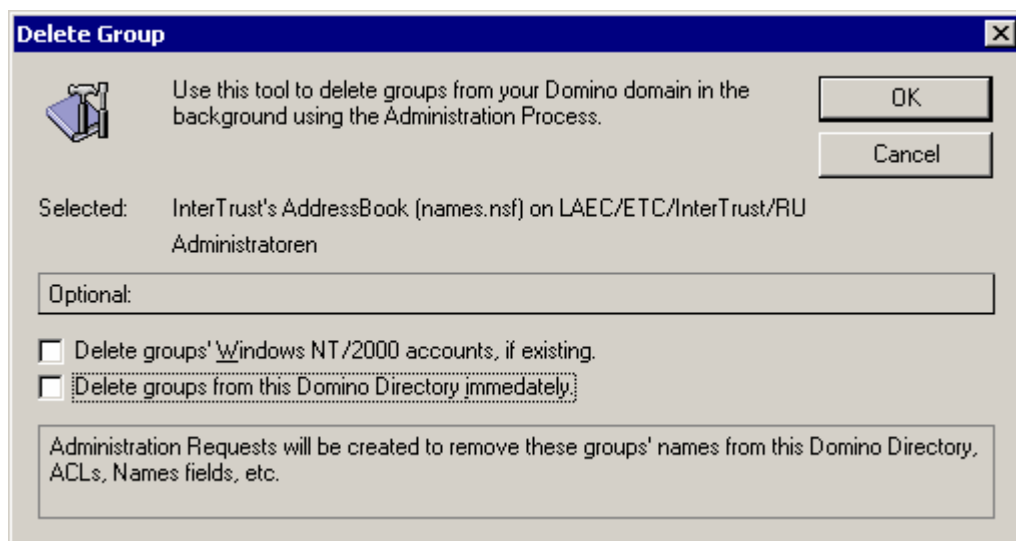


Рис. 391

	Date	Sched. Type	Action	Requester
▼	Administratoren			
	21.10 10:27		► Find Name in Domain	Nikolay N. Iontsev/Inter
	22.10 09:16		▼ Delete Group in Domino Directory	Nikolay N. Iontsev/Inter
	22.10 09:22		InterTrust/InterTrustCorp/SU performed action on: 22.10 09:22	
	22.10 09:22		▼ Delete in Person Documents	Nikolay N. Iontsev/Inter
	22.10 13:50		InterTrust/InterTrustCorp/SU performed action on: 22.10 13:50	
	22.10 09:22		▼ Delete in Access Control List	Nikolay N. Iontsev/Inter
	22.10 09:24		NotesSrv400/InterTrustCorp/SU performed action on: 22.10 09:24	
	22.10 09:28		LAEC/LAEC/InterTrustCorp/SU performed action on: 22.10 09:28	
	22.10 09:28		LINUX/LAEC/InterTrustCorp/SU performed action on: 22.10 09:28	
	22.10 09:30		LAEC/ETC/InterTrust/RU performed action on: 22.10 09:30	
	22.10 09:32		QuickPlace/InterTrust/RU performed action on: 22.10 09:32	
	22.10 09:32		InterTrust/InterTrustCorp/SU performed action on: 22.10 09:32	
	22.10 09:33		SameTime/InterTrust/RU performed action on: 22.10 09:33	
	22.10 09:33		Domino500/InterTrustCorp/SU performed action on: 22.10 09:33	
	22.10 09:33		WebDevelopment/Web/InterTrustCorp/SU performed action on: 22.10 09:33	
	22.10 09:38		Web2/InterTrustCorp/SU performed action on: 22.10 09:38	
	22.10 09:39		AS400/InterTrust/RU performed action on: 22.10 09:39	
	22.10 09:41		Development/InterTrustCorp/SU performed action on: 22.10 09:41	
	22.10 09:41		InterWork/InterTrust/RU performed action on: 22.10 09:41	
	22.10 09:47		Web3/InterTrustCorp/SU performed action on: 22.10 09:47	
	22.10 09:50		Rainbow/Dev/InterTrust/RU performed action on: 22.10 09:50	
	22.10 13:50		▼ Delete in Reader/Author fields	Nikolay N. Iontsev/In
	22.10 14:04		InterTrust/InterTrustCorp/SU performed action on: 22.10 14:04	
	22.10 14:26		LAEC/ETC/InterTrust/RU performed action on: 22.10 14:26	
	22.10 15:45		LAEC/LAEC/InterTrustCorp/SU performed action on: 22.10 15:45	

Рис. 392 Процесс выполнения

1.47.15. 1.1.15. Переименование групп - операция People & Groups - Actions-Rename Group

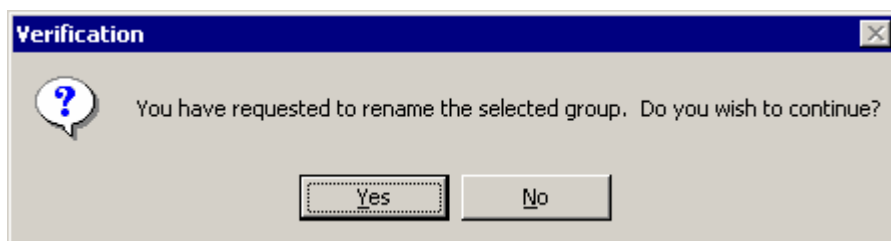


Рис. 393

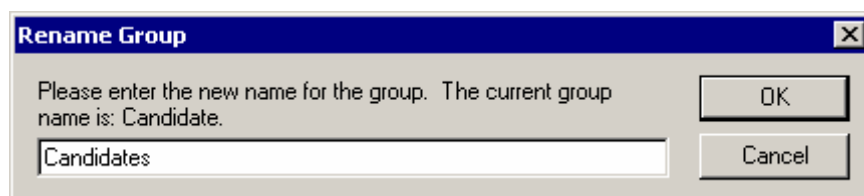


Рис. 394

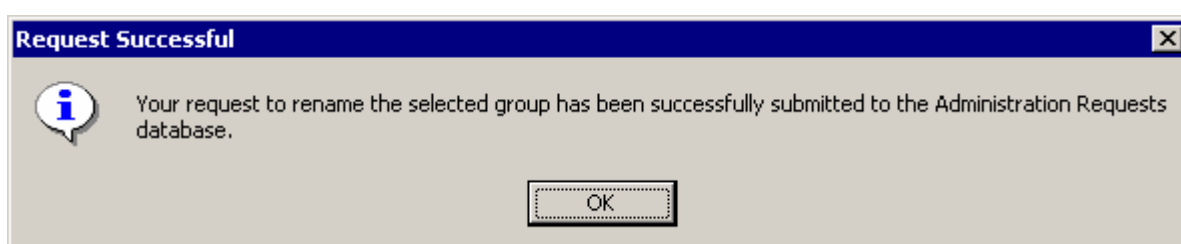


Рис. 395

	Date	Sched. Type	Action	Requester
▼	Candidate			
	22.10 16:54		▼ Rename Group in Domino Directory	Nikolay N. I
	22.10 17:02		InterTrust/InterTrustCorp/SU performed action on: 22.10 17:02	
	22.10 17:02		▼ Rename Group in Person Documents	Nikolay N. I
	22.10 17:25		InterTrust/InterTrustCorp/SU performed action on: 22.10 17:25	
	22.10 17:02		▼ Rename Group in Access Control List	Nikolay N. I
	22.10 17:04		QuickPlace/InterTrust/RU performed action on: 22.10 17:04	
	22.10 17:04		NotesSrv400/InterTrustCorp/SU performed action on: 22.10 17:04	
	22.10 17:05		Domino500/InterTrustCorp/SU performed action on: 22.10 17:05	
	22.10 17:08		LAEC/LAEC/InterTrustCorp/SU performed action on: 22.10 17:08	
	22.10 17:08		AS400/InterTrust/RU performed action on: 22.10 17:08	
	22.10 17:08		LINUX/LAEC/InterTrustCorp/SU performed action on: 22.10 17:08	
	22.10 17:10		LAEC/ETC/InterTrust/RU performed action on: 22.10 17:10	
	22.10 17:11		Development/InterTrustCorp/SU performed action on: 22.10 17:11	
	22.10 17:12		SameTime/InterTrust/RU performed action on: 22.10 17:12	
	22.10 17:12		InterTrust/InterTrustCorp/SU performed action on: 22.10 17:12	
	22.10 17:13		InterWork/InterTrust/RU performed action on: 22.10 17:13	
	22.10 17:15		WebDevelopment/Web/InterTrustCorp/SU performed action on: 22.10 17:15	
	22.10 17:25		▼ Rename Group in Reader/Author fields	Nikolay N.
	22.10 17:30		LAEC/ETC/InterTrust/RU performed action on: 22.10 17:30	

Рис. 396 Ход процесса

1.47.16. 1.1.16. Поиск экземпляров имени сервера, группы и пользователя - операции Server-Analysis - Tools-Analyze-Find Server,

People & Groups - Tools-Groups-Find Group(s), People & Groups - Tools-People-Find User(s)

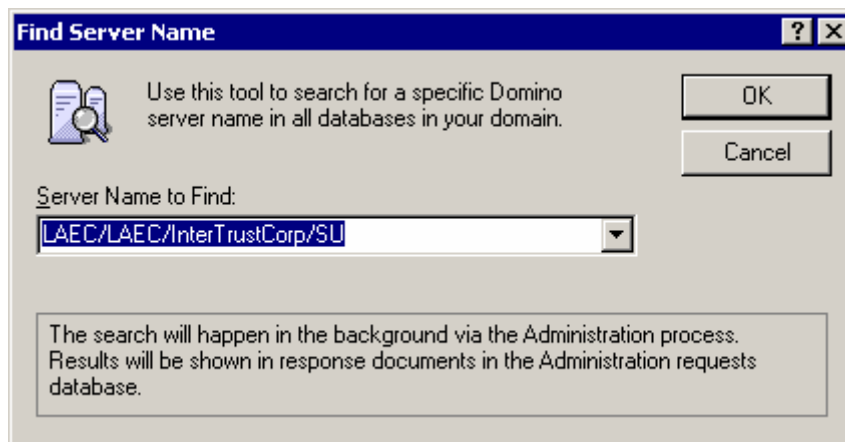


Рис. 397 Для поиска сервера окно с выбором, для поиска группы или пользователя нужно предварительно выбрать их в виде

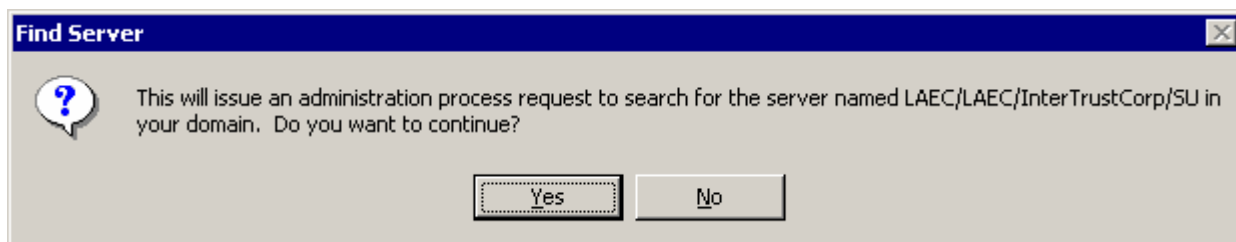


Рис. 398 Запрос передается ADMINP

	Date	Sched. Type	Action	Requester
▶	LAEC/ETC/InterTrust/RU			
▼	LAEC/LAEC/InterTrustCorp/SU			
	21.10 10:25		Find Name in Domain	Nikolay N. Iontsev/InterTrustCorp/SU
	21.10 10:28		LAEC/LAEC/InterTrustCorp/SU performed action on: 21.10 10:28	
	21.10 10:28		LINUX/LAEC/InterTrustCorp/SU performed action on: 21.10 10:28	
	21.10 10:32		LAEC/ETC/InterTrust/RU performed action on: 21.10 10:32	
	21.10 10:34		NotesSrv400/InterTrustCorp/SU performed action on: 21.10 10:34	
	21.10 10:42		SameTime/InterTrust/RU performed action on: 21.10 10:42	

Рис. 399 Запрос поиска сервера

ADMINISTRATION PROCESS - Log

Action:	Find Name in Domain
Link to request:	
Action requested by:	Nikolay N. Iontsev/InterTrustCorp/SU
Server responding to request:	LAEC/LAEC/InterTrustCorp/SU
Start time:	10:28:08 Сегодня
End time:	10:34:13 Сегодня
Links to items found in Database ACL's:	The following database ACLs were found to contain (LAEC/LAEC/InterTrustCorp/SU): 
Perform request again?:	☐ Yes

Рис. 400 Базы, в ACL которых встречается сервер

Date	Sched. Type	Action	Requester
▼ LAEC Admin/InterTrustCorp/SU			
21.10 10:26		▼ Find Name in Domain	Nikolay N. Iontsev
21.10 10:28	☒	LAEC/LAEC/InterTrustCorp/SU performed action on: 21.10 10:28	
21.10 10:28		LINUX/LAEC/InterTrustCorp/SU performed action on: 21.10 10:28	
21.10 10:32		LAEC/ETC/InterTrust/RU performed action on: 21.10 10:32	
21.10 10:32	☒	InterTrust/InterTrustCorp/SU performed action on: 21.10 10:32	
21.10 10:34		NotesSrv400/InterTrustCorp/SU performed action on: 21.10 10:34	
21.10 10:42		SameTime/InterTrust/RU performed action on: 21.10 10:42	

Рис. 401 Запрос поиска пользователя – в документах ссылки на базы, в ACL которых он встречается, и каталог Domino, где есть документ Person

Date	Sched. Type	Action	Requester
▼ Administratoren			
21.10 10:27		▼ Find Name in Domain	Nikolay N. Iontsev
21.10 10:28		LAEC/LAEC/InterTrustCorp/SU performed action on: 21.10 10:28	
21.10 10:28		LINUX/LAEC/InterTrustCorp/SU performed action on: 21.10 10:28	
21.10 10:32		LAEC/ETC/InterTrust/RU performed action on: 21.10 10:32	
21.10 10:32	☒	InterTrust/InterTrustCorp/SU performed action on: 21.10 10:32	
21.10 10:36		NotesSrv400/InterTrustCorp/SU performed action on: 21.10 10:36	
21.10 10:42		SameTime/InterTrust/RU performed action on: 21.10 10:42	

Рис. 402 Запрос поиска группы – анализ документов показывает, что группа встречается только в каталоге Domino и не была еще нигде использована в ACL

1.47.17. 1.1.17. Некоторые другие операции

1.47.17.1. 1.1.17.1. «Самоочистка» от устаревших запросов на изменение имен

	Date	Sched. Type	Action	Requester
▼ Obsolete Change Requests in Extended Directory Catalog.				
	08.10.2002 22:0		▼ Delete Obsolete Change Requests	NotesSrv400/InterTrustCorp/SU
	06.10 21:00		InterTrust/InterTrustCorp/SU performed action on: 06.10 21:00	
▼ Obsolete Change Requests in InterTrustCorp's AddressBook.				
	29.10.2002 21:0		▼ Delete Obsolete Change Requests	InterTrust/InterTrustCorp/SU
	30.09 21:01		InterTrust/InterTrustCorp/SU performed action on: 30.09 21:01	
	01.10 21:00		InterTrust/InterTrustCorp/SU performed action on: 01.10 21:00	
	02.10 21:00		InterTrust/InterTrustCorp/SU performed action on: 02.10 21:00	
▼ Obsolete Change Requests in InterTrustCorp's Web Users N&A.				
	01.10.2002 22:0		▼ Delete Obsolete Change Requests	NotesSrv400/InterTrustCorp/SU
	30.09 22:00		NotesSrv400/InterTrustCorp/SU performed action on: 30.09 22:00	
	01.10 22:00		NotesSrv400/InterTrustCorp/SU performed action on: 01.10 22:00	
	02.10 22:00		NotesSrv400/InterTrustCorp/SU performed action on: 02.10 22:00	
	03.10 22:00		NotesSrv400/InterTrustCorp/SU performed action on: 03.10 22:00	
	04.10 22:00		NotesSrv400/InterTrustCorp/SU performed action on: 04.10 22:00	
	05.10 22:00		NotesSrv400/InterTrustCorp/SU performed action on: 05.10 22:00	
	06.10 21:00		InterTrust/InterTrustCorp/SU performed action on: 06.10 21:00	
	06.10 22:00		NotesSrv400/InterTrustCorp/SU performed action on: 06.10 22:00	

Рис. 403 «Самоочистка» от устаревших запросов на изменение имен

1.47.17.2. 1.1.17.2. Слежение за сменой пароля, запоминание версии клиента, включение агента OutOffice пользователем «без прав»

▼	Olga S. Afanasieva/InterTrustCorp/SU			
	17.10 09:00		▼ Change User Password in Domino Directory	
	17.10 09:01		InterTrust/InterTrustCorp/SU performed action on: 17.10 09:01	

Рис. 404

▼	Danila A. Trushin/InterTrustCorp/SU			
	17.10 13:48		▼ Update Client Information in Person Record	Da
	17.10 13:49		InterTrust/InterTrustCorp/SU performed action on: 17.10 13:49	
	20.10 20:53		▼ Change User Password in Domino Directory	Inte
	20.10 20:54		InterTrust/InterTrustCorp/SU performed action on: 20.10 20:54	
	21.10 12:17		▼ Set Web User Name and Enable Scheduled Agent	Da
	21.10 12:17		NotesSrv400/InterTrustCorp/SU performed action on: 21.10 12:17	

Рис. 405

The "Set Web user name and enable schedule agent" request is generated when a Web user with Editor access to their mail file sets the "Out of Office" agent.

1.47.17.3. 1.1.17.3. Серия запросов при регистрации (СА) и установке нового сервера

	Date	Sched. Type	Action
▼	keyfile.kyr		
	16.10 10:44		▼ Create SSL Certificate and Keyring File
	16.10 11:59	☒	LAEC/ETC/InterTrust/RU performed action on: 16.10 11:59
	16.10 10:47		Create SSL Certificate and Keyring File
▼	LAEC		
	16.10 10:44		▼ Recertify Server in Domino Directory
	16.10 10:48	☒	InterTrust/InterTrustCorp/SU performed action on: 16.10 10:48

Рис. 406 Сертификат Notes при регистрации. Затем keyring-файл, но уже после запуска сервера

	Date	Sched. Type	Action
▼	LAEC/ETC/InterTrust/RU		
	16.10 10:44		▼ Store Certificate in Domino or LDAP Directory
	16.10 10:45	☒	InterTrust/InterTrustCorp/SU performed action on: 16.10 10:45
	16.10 11:13		▼ Put Server's Notes Build Number into Server Record
	16.10 12:08	☒	InterTrust/InterTrustCorp/SU performed action on: 16.10 12:08
	16.10 11:59		▼ Enable Server's SSL Ports in Domino Directory
	16.10 12:01	☒	InterTrust/InterTrustCorp/SU performed action on: 16.10 12:01
	16.10 12:01		▼ Monitor Server's SSL Status in Domino Directory
	16.10 12:04	☒	LAEC/ETC/InterTrust/RU performed action on: 16.10 12:04
	16.10 12:07		▼ Update Server's Protocol Information
	16.10 12:18	☒	InterTrust/InterTrustCorp/SU performed action on: 16.10 12:18
	16.10 12:07		▼ Store Server's CPU count
	16.10 12:08	☒	InterTrust/InterTrustCorp/SU performed action on: 16.10 12:08
	16.10 12:07		▼ Store Server's Platform in Server Record
	16.10 12:08	☒	InterTrust/InterTrustCorp/SU performed action on: 16.10 12:08
	16.10 12:07		▼ Set Directory Filename
	16.10 12:08	☒	InterTrust/InterTrustCorp/SU performed action on: 16.10 12:08

Рис. 407

1.47.17.4. 1.1.17.4. Server\Analysis\Tools\Open Fault Reports...

Create New Fault Reports Database

The Fault Reports database for domain 'INTERTRUSTCORP' needs to be created. Please select a server, file name and database title:

Server:

LAEC/ETC/InterTrust/RU

File name:

Indfr.nsf

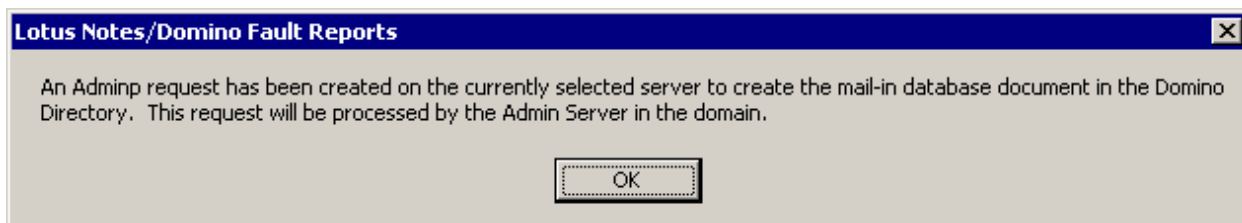
Title:

Lotus Notes/Domino Fault Reports

Create

Cancel

Рис. 408



Puc. 409

Using Lotus Notes/Domino Fault Reports



This database records faults from the Domino server or the Notes workstation.

For each fault report that is received, the following information is displayed:

- o Domino server name for server faults or Notes user name for workstation faults
- o Notes or Domino version
- o Operating system version
- o Time that the fault occurred and how long the server or workstation had been in use prior to the fault
- o The fault message and the resulting call stack if applicable
- o For workstation faults, user comments on what they were doing at the time of the fault (if applicable)

Composing Documents

You cannot compose documents for this database. The documents are created from mail messages that are generated by the server or workstation when it is restarted after a fault.

Puc. 410

	Date	Sched. Type	Action	Requester
	▼ Lotus Notes/Domino Fault Reports			
	22.10 09:10	⚡	▼ Create Mail-In Database	Nikolay N. Iontsev
	22.10 09:11		InterTrust/InterTrustCorp/SU performed action on: 22.10 09:11	

Puc. 411

Mail-In Database: Lotus Notes/Domino Fault Reports

Basics

Other

Comments

Administration

Basics	Location
Mail-in name: Lotus Notes/Domino Fault Reports	Domain: INTERTRUSTCORP
Description: Mail-in database for fault reports from Notes clients and Domino servers	Server: LAEC/ETC/InterTrustRU
Internet Address:	File name: Indfr.nsf
Internet message storage: No Preference	
Encrypt incoming mail: No	

Puc. 412

1.47.17.5. 1.1.17.5. Список всевозможных запросов R6 (Help)

Administration Process Requests - One Domain

- • Add Internet Certificate
- • Add resource
- • Add servers to a cluster
- • Approve person's name change request
- • Change HTTP password in Domino Directory

- • Change user password in Domino Directory
- • Copy server public key
- • Create hosted organization storage
- • Create IMAP delegation requests
- • Create mail files during setup
- • Create Mail-in database
- • Create replica
- • Create a Roaming User
- • Delegate mail file
- • Delegate mail file on administration server
- • Delegate Web mail file
- • Delete database
- • Delete group in Domino Directory
- • Delete hosted organization
- • Delete person in Domino Directory
- • Delete Policy in Domino Directory
- • Delete resource
- • Delete roaming user
- • Delete server name in Domino Directory
- • Downgrade user from Roaming to Non-Roaming user
- • Find name in domain
- • Maintain Trends database record
- • Modify CA Configuration in the Domino Directory
- • Modify ID recovery information in Domino Directory
- • Modify resource
- • Modify user information stored in the Domino Directory
- • Move database from a cluster server
- • Move database from a non-cluster server
- • Move a mail file from one server to another
- • Move roaming user to another server
- • Place server's Notes build number into Server record
- • Recertify Certificate Authority in Domino Directory
- • Recertify servers
- • Recertify users
- • Register hosted organization
- • Remove servers from cluster
- • Rename group
- • Rename person
- • Rename person - name change refused
- • Request to create ISpy database
- • Retract database
- • Set Directory Assistance field

- • Set directory filename
- • Set password fields
- • Set user name and enable schedule agent
- • Set Web admin fields
- • Set Web user name and enable scheduled agent
- • Sign database with server's ID file
- • Store CA Policy Information in the Domino Directory
- • Store certificate in Domino or LDAP Directory
- • Store Certificate Revocation List in Domino or LDAP Directory
- • Store directory type in Server record
- • Store server's CPU count
- • Store server's DNS host name
- • Update client information in Person Record
- • Update external domain information
- • Update domain catalog configuration
- • Update license tracking information in Domino Directory
- • Update roaming user information in Person record
- • Update non-roaming user to roaming user
- • Update server protocol information
- • Upgrade server to hierarchical
- • Web set Soft Deletion Expire Time

Administration Process Requests - Time-based execution

The following requests are generated when moving databases or creating database replicas as part of a recommended resource balancing plan as determined by IBM Tivoli Analyzer for Lotus Domino.

- • Check access for new replica creation
- • Check access for move replica creation
- • Check mail server's access
- • Check access for non-cluster move replica

Administration Process Requests - Multiple Domains

- • Create Replica
- • Delete Server
- • Delete person
- • Rename person from flat to hierarchical
- • Rename server from flat to hierarchical

1.47.18. 1.1.18. Устранение проблем в работе Administration Process

Прежде, чем использовать Administration Process, проверьте и обеспечьте следующее.

- • Сервер администрирования Каталога Domino версии R6.

- ● На серверах присутствует реплика базы «Протокол сертификаций» - CERTLOG.NSF. Создана соответствующая организации иерархия сертификаторов. Сертификаторы, которые будут регистрировать или ресертифицировать пользователей и серверы, имеют к этой базе, по крайней мере, доступ автора с правом создавать документы.
- ● В файле NOTES.INI серверов в строке ServerTasks= <программы, запускаемые при старте сервера> присутствует программа Adminp.
- ● Вы, как основной администратор, имеете к базе Administration Requests доступ менеджера. В список управления доступом (ACL) базы Administration Requests добавлены все администраторы и сертификаторы (или их группы) с доступом не ниже автора с правом создания документов.
- ● Вы, как основной администратор, имеете к Каталогу Domino доступ менеджера. В ACL Каталога Domino добавлены все администраторы и сертификаторы (или их группы) с доступом не ниже автора с правом создания и удаления документов и назначением хотя бы на одну из ролей GroupModifier, ServerModifier, UserModifier. Всем другим лицам, группам и серверам также предоставлен необходимый доступ.
- ● Для «практически всех» других баз назначен сервер администрирования. Если есть реплика базы на сервере R6, нужно выбирать ее сервером администрирования сервер R6.
- ● Изменения, выполненные в ACL баз на исходно выбранных серверах, распространились репликациями на остальные серверы домена.

1.48. 1.1. Ликвидация сервера с переносом его функций и баз на другой сервер (Decommission Server Analysis)

«Полезный советчик» при ликвидации сервера с переносом его функций и баз на другой сервер.

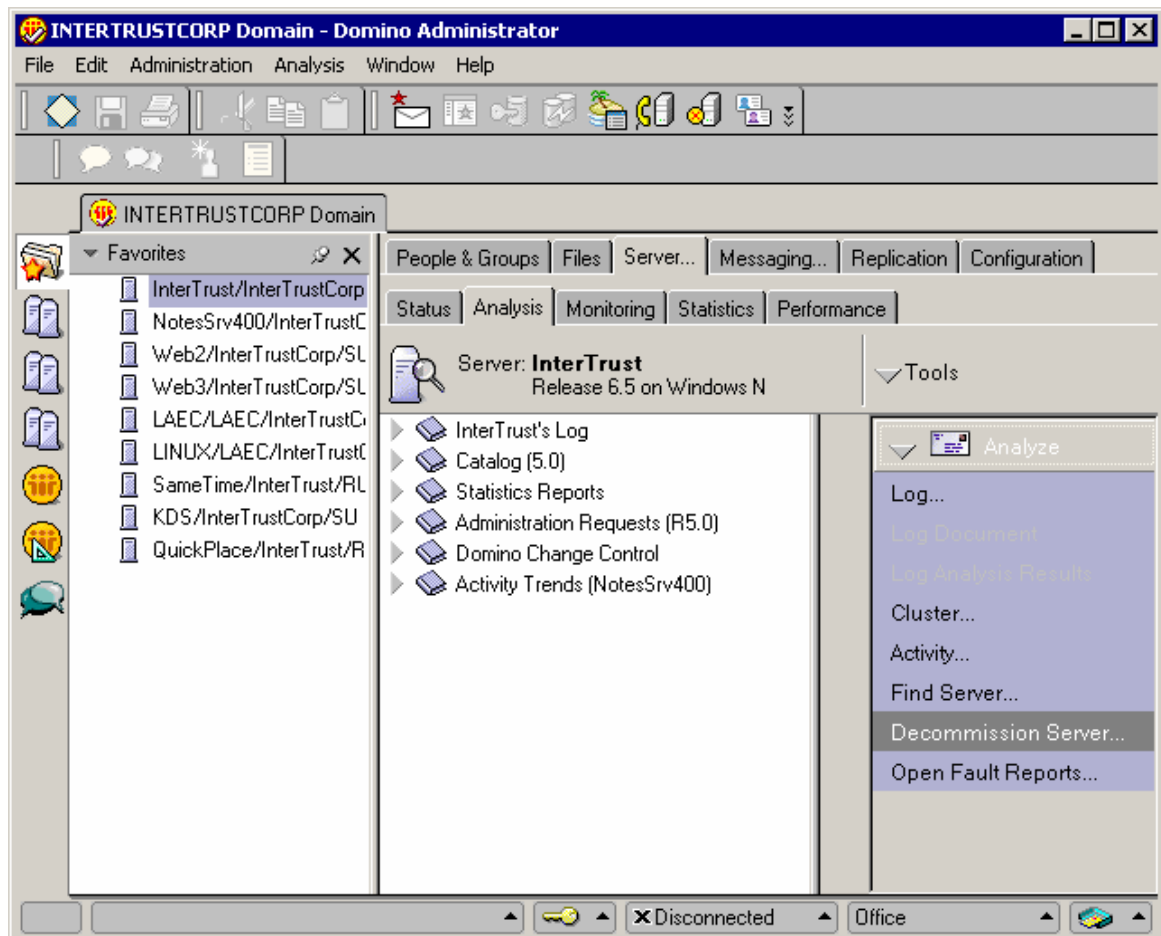


Рис. 413 «Запуск» операции

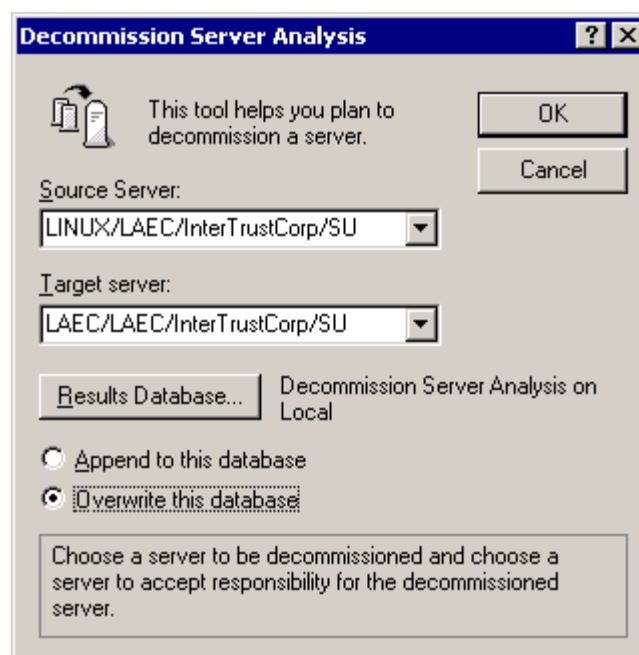


Рис. 414 LINUX ликвидируем, весь функционал переносим на LAEC

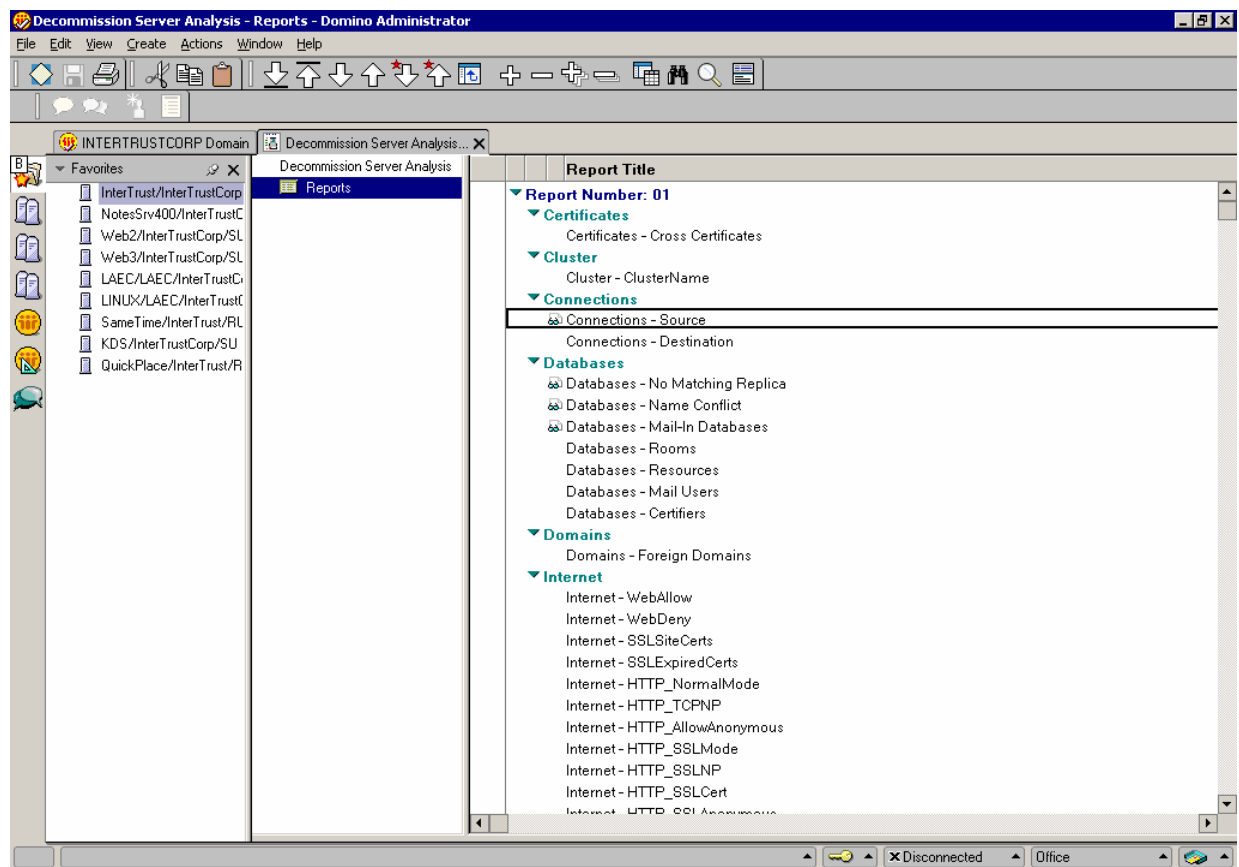


Рис. 415 После «раздумий» открывается локальная база Decommission Server Analysis

DECOMMISSION SERVER REPORT	
Details	
Report Number:	
Report category:	Connections
Report title:	Connections - Source
Report date:	15:52 Сегодня
Server to be decommissioned:	LINUX/LAEC/InterTrustCorp/SU
Server to accept responsibility:	LAEC/LAEC/InterTrustCorp/SU
Report details:	The following connection sources available on source server LINUX/LAEC/InterTrustCorp/SU are NOT available on target server LAEC/LAEC/InterTrustCorp/SU: LAEC/LAEC/InterTrustCorp/SU Local Area Network Replication

Рис. 416 Документы в ней (особенно с «очками») поясняют...

DECOMMISSION SERVER REPORT	
Details	
Report Number:	
Report category:	Internet
Report title:	Internet - HTTP_CSDefault
Report date:	15:51 Сегодня
Server to be decommissioned:	LINUX/LAEC/InterTrustCorp/SU
Server to accept responsibility:	LAEC/LAEC/InterTrustCorp/SU
Errors:	Invalid value specified. Internet - HTTP_CSDefault.
Report details:	HTTP_CSDefault are NOT the same: HTTP_CSDefault on server LINUX/LAEC/InterTrustCorp/SU is 7. HTTP_CSDefault on server LAEC/LAEC/InterTrustCorp/SU is 98.

Рис. 417 в чем разница в конфигурации серверов...

DECOMMISSION SERVER REPORT	
Details	
Report Number:	
Report category:	Databases
Report title:	Databases - No Matching Replica
Report date:	15:51 Сегодня
Server to be decommissioned:	LINUX/LAEC/InterTrustCorp/SU
Server to accept responsibility:	LAEC/LAEC/InterTrustCorp/SU
Report details:	The following files on source server LINUX/LAEC/InterTrustCorp/SU do NOT have replicas on the target server LAEC/LAEC/InterTrustCorp/SU: - webadmin.ntf - help\readme.nsf - log.nsf - reports.nsf - certsrv.nsf - statrep.nsf - webadmin.nsf - statmail.nsf - domlog.nsf - iNotes\Forms5.nsf - iNotes\Forms6.nsf - EDU\ADLS\ADCourse.NSF - EDU\AD270\InstructorDemo.nsf - EDU\AD270\test.nsf - EDU\AD270\testR6.nsf - EDU\AD270\Instructor Demo.nsf - EDU\AD270\Instructor Demo111.nsf

Рис. 418 какие реплики нужно создать...

DECOMMISSION SERVER REPORT	
Details	
Report Number:	
Report category:	Databases
Report title:	Databases - Name Conflict
Report date:	15:51 Сегодня
Server to be decommissioned:	LINUX/LAEC/InterTrustCorp/SU
Server to accept responsibility:	LAEC/LAEC/InterTrustCorp/SU
Report details:	The following files on source server LINUX/LAEC/InterTrustCorp/SU have name conflicts with files on the target server LAEC/LAEC/InterTrustCorp/SU: - webadmin.ntf - help\readme.nsf - log.nsf - reports.nsf - certsrv.nsf - statrep.nsf - webadmin.nsf - statmail.nsf - domlog.nsf - iNotes\Forms5.nsf - iNotes\Forms6.nsf - mtdata\mtstore.nsf - doladmin.nsf - dbdirman.nsf - schema.nsf - iNotes6.ntf

Рис. 419 какие базы «конфликтуют» по именам...

Однако осуществлять процесс переноса вам придется «своими руками»...

1.49. 1.1. Восстановление после крахов сервера

1.49.1. 1.1.1. Автоматический перезапуск сервера (Automatic Fault Recovery - WinNT и UNIX)

- Возможность сервера Domino обнаружить свой крах, завершить «остатки своих задач», освободить ресурсы и автоматически перезапуститься без вмешательства администратора
- Если ID сервера с паролем и возможность Fault Recovery разрешена, пароль запоминается в памяти системного ядра и извлекается оттуда рестартующим сервером
- Fault Recovery поддерживает Domino partitions - серверы. При крахе одного partition-сервера перезапускается только он
- К Domino Controller возможность никакого отношения не имеет...

1.49.1.1. 1.1.1.1. Конфигурирование

Возможность «включается» в документе Server.

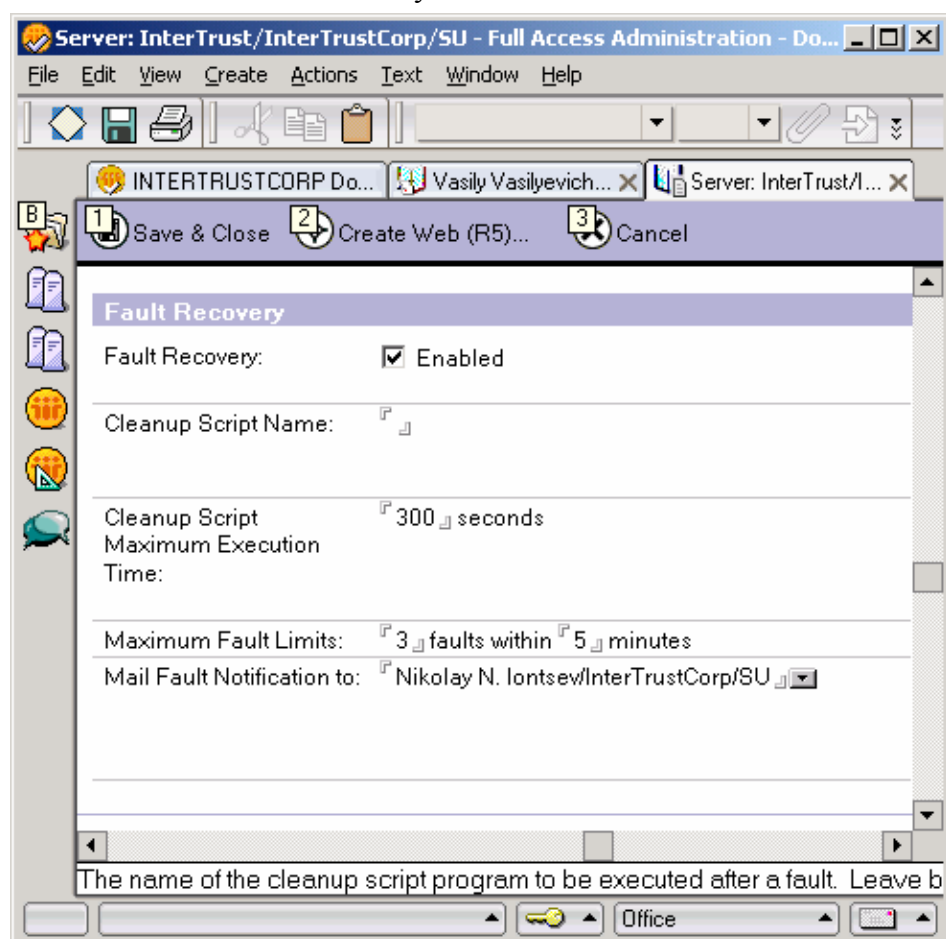


Рис. 420 Документ Server, закладка Basics, группа полей Fault Recovery

Перед рестартом может быть выполнен скрипт или программа. По умолчанию запускается nsd.exe

На ее выполнение отводится заданное время в секундах (по умолчанию 5 минут)

Во избежание «зацикливания» количество рестартов за интервал времени ограничивается.

Администраторам высылаются уведомления.

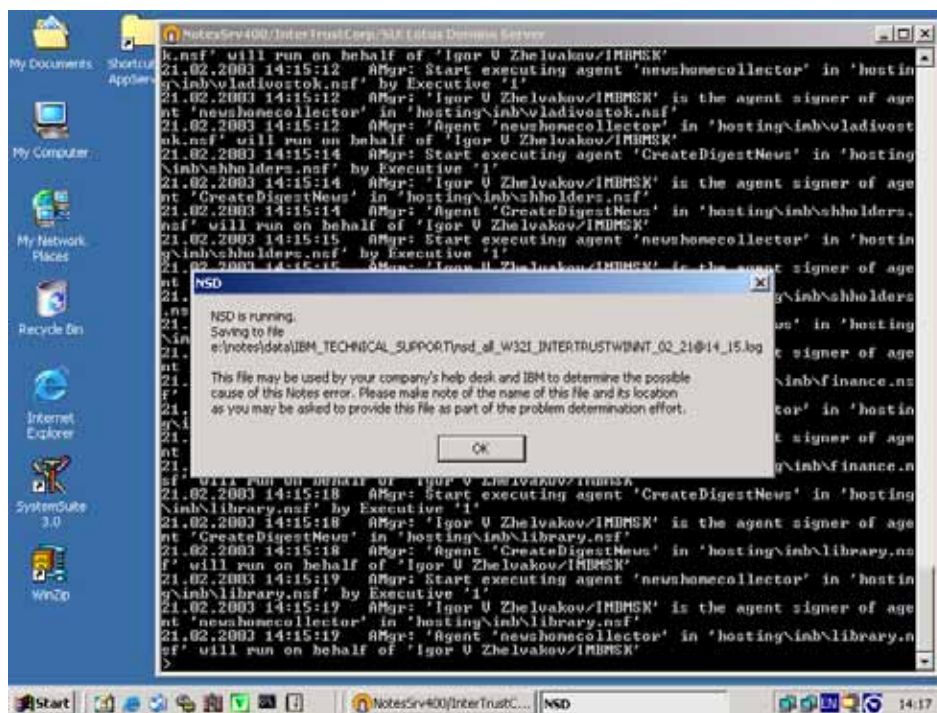


Рис. 421 Результат будет выглядеть так...

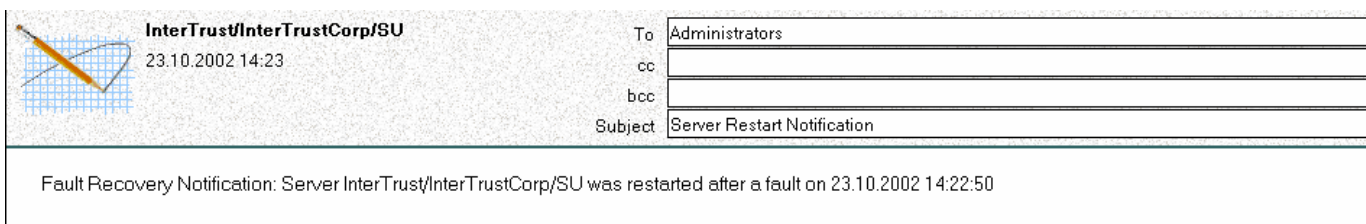


Рис. 422 А после рестарта админы получают письмо...

1.49.2. 1.1.2. Поиск и устранение причин крахов сервера

Краш из-за повреждения базы. Сообщения "Unable to copy database", "Unable to copy document" или подобные. В общем действия следующие:

- Запуск Fixup по базам, если не используется протоколирование транзакций или база дисковой структуры R4.
- Запуск Fixup -J по базам, если используется протоколирование транзакций и база дисковой структуры выше R4. Часто «самовылечивается» при рестарте сервера.

Краш при обновлении индекса вида базы:

- Load updall *database*name -r
- Если не спасло: создать реплику базы под новым именем файла, удалить исходную базу, переименовать реплику в прежнее имя.

Краш Router – обычно проблемы в MAIL[N].BOX:

- Переименовать MAIL[N].BOX.
- Перезапустить сервер – он создаст новый MAIL[N].BOX.
- Скопировать сообщения из старых MAIL[N].BOX в новый MAIL[N].BOX.

1.50. 1.1. Типы серверных программ

Серверная программа - разработанная с учетом специальных соглашений программа для работы на сервере Domino. Соглашения по разработке серверных программ можно найти в документации, входящей в состав Notes API.

Серверные программы бывают двух разновидностей:

- • **Add-In Program** - обычно запускается при старте сервера и работает до его завершения, получает «задания на выполнение работ» от других программ сервера через очередь событий или посредством циклического опроса чего-либо, «показывает свое состояние» по команде консоли Show Task и обычно может принимать и выполнять собственные команды, передаваемые ей по команде консоли Tell. Типичный пример - маршрутизатор почты Mail Router.
- • **Main Program** - запускается по расписанию или команде консоли для выполнения какого-либо однократного действия, после чего автоматически завершается. Обычно может «показывать свое состояние» по команде консоли Show Task. Обычно может быть запущена и непосредственно из операционной системы, когда сервер Domino остановлен. Типичный пример – «уплотнитель баз» Database Compactor.

1.51. 1.1. Варианты организации запуска серверных программ по расписанию

- • **Файл Notes.INI, параметр ServerTasksAtX, X= 1,2,...,11,12,13,...,23**

ServerTasks=Billing, Replica, Router, Update, AMgr, Adminp, Sched, CalConn, Collect, HTTP, IMAP, LDAP, DIIOp, CA

ServerTasksAt1=Catalog, Design

ServerTasksAt2=UpdAll, Object Collect mailobj.nsf

ServerTasksAt3=Object Info -Full

ServerTasksAt5=Statlog

- • **Документ Program**

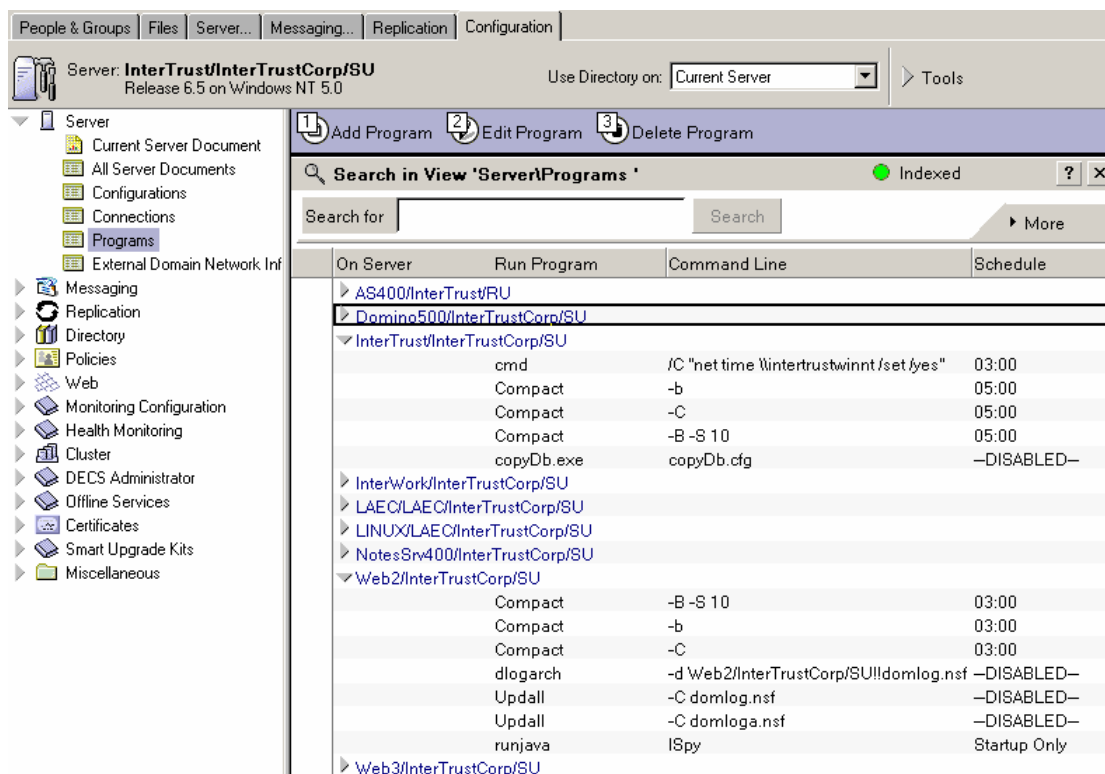


Рис. 423 Вид Programs из NAMES.NSF в клиенте администратора

Program: Compact

Basics Administration

Basics		Schedule	
Program name:	Compact	Enabled/disabled:	Enabled
Command line:	-B -S 10	Run at times:	03:30 each day
Server to run on:	LINUX/LAEC/InterTrustCorp/SU	Repeat interval of:	0 minutes
Comments:	Уплотнение по месту с возвращением неиспользуемого пространства файловой системы	Days of week:	Wed

Рис. 424 Документ Program, эквивалентный команде консоли Load Compact -B -S 10 в 03:30 каждую среду

- • **Nserver –с “команда_консоли”**

Например, nserver –с “load ldap”, nserver –с “tell ldap q”, nserver –с “restart server”, nserver –с “q”. Запускается второй процесс nserver, он обнаруживает наличие первого процесса nserver, передает команду первому процессу и завершается. Удобно для применения в команде at. Однако в R6 это работает при одном экземпляре сервера на

компьютере (не partitioned server). Работает также nserver -q, но немного иначе – в R6.5 «дожидается» завершения основного процесса, после чего завершается сам.

1.52. 1.1. Программы Cataloger (CATALOG) и Domain Indexer (DOMIDX)

Программа Catalog поддерживает в актуальном состоянии базу CATALOG.NSF с информацией о базах, находящихся на данном сервере. Эта база обычно является репликой на каждом из серверов домена, а потому часто содержит информацию обо всех базах в домене.

Отличия R5/6 от R4:

- в документе, описывающем базу в CATALOG.NSF, очень много полезной информации о базе (даже весь ACL базы)
- в CATALOG.NSF содержится информация обо всех базах и шаблонах (флаг List in Database Catalog в R5/6 игнорируется), но в стандартных видах отображается информация только о базах с флагом List in Database Catalog.
- База CATALOG.NSF используется доменным индексером для поддержания индекса полнотекстового поиска по домену.

1.52.1. 1.1.1. Два режима работы программы CATALOG

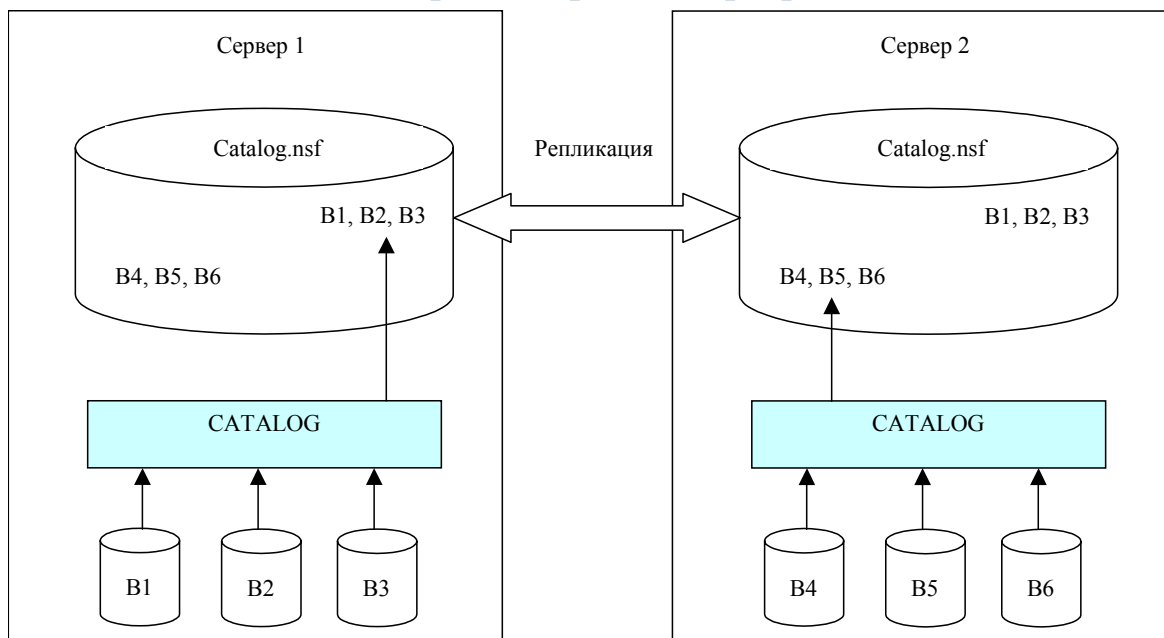


Рис. 425 Обычный режим

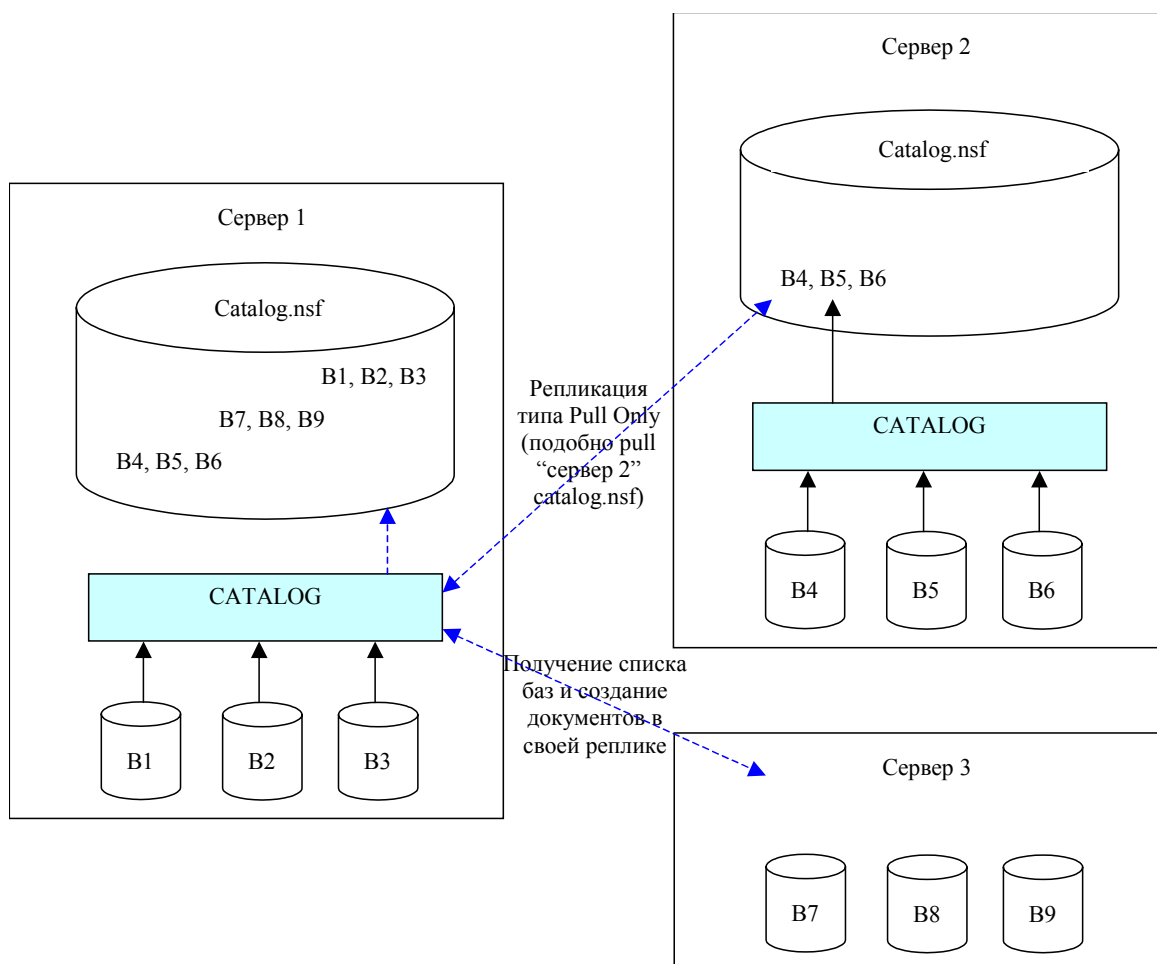


Рис. 426 Режим Domain Catalog

1.52.2. 1.1.2. Конфигурирование и запуск CATALOG

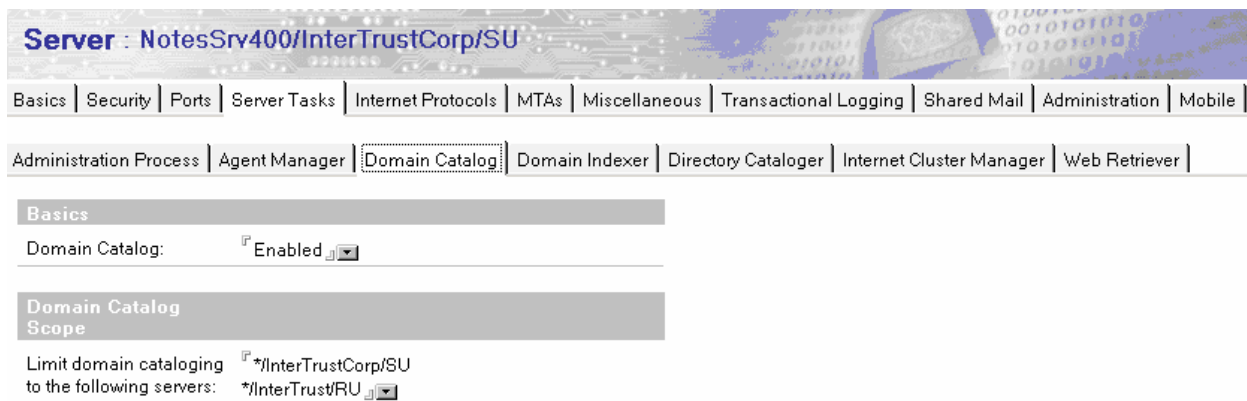


Рис. 427 Режим Domain Catalog

Поле Limit domain cataloging to the following servers ограничивает множество серверов домена, с которых программа CATALOG «собирает» информацию о базах. Если поле пусто, программа CATALOG «собирает» информацию о базах всех доступных серверов домена.

1.52.3. 1.1.3. База CATALOG.NSF

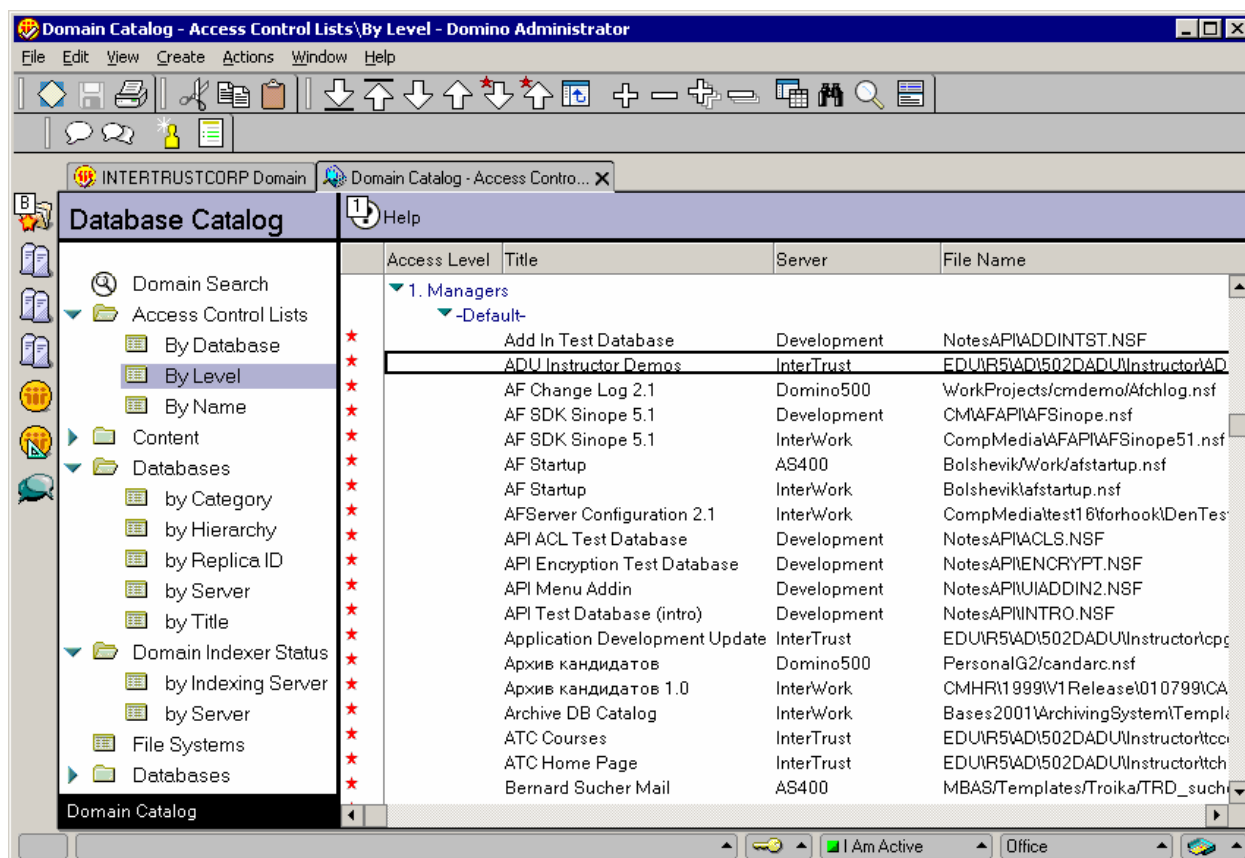


Рис. 428 Группа видов Access Control Lists может быть полезна для «централизованного контроля» ACL баз на серверах домена

1.52.4. 1.1.4. Назначение и логика работы DOMIDX

Создание индекса полнотекстового поиска по многим базам на разных серверах домена. Может индексировать и файлы, «лежащие в файловой системе» (т.е. не только присоединенные файлы, находящиеся в документах баз). При выполнении поиска учитываются права доступа пользователей к базам (ACL) и документам в базах (поля Readers).

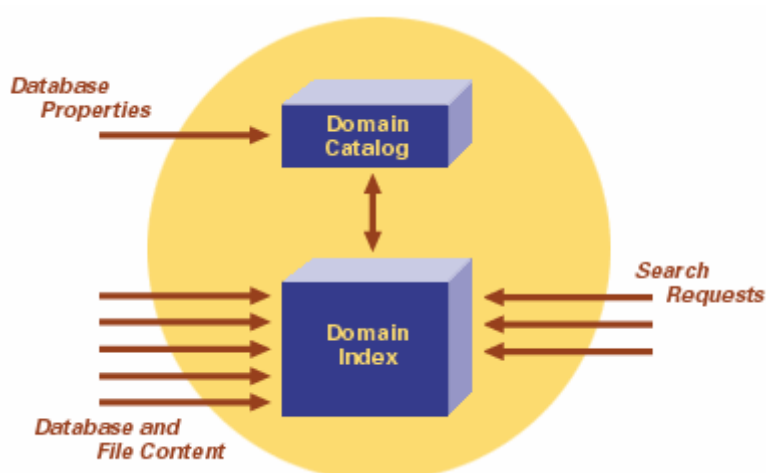


Рис. 429 База CATALOG.NSF для доменного индекса является источником информации о базах, которые должны быть проиндексированы (флаг Include in multi-database indexing)

1.52.5. 1.1.5. Конфигурирование и запуск DOMIDX

Для баз, информация из которых должна включаться в индекс полнотекстового поиска по домену, «включить» свойство Include in multi-database indexing. В массовом

порядке это удобнее делать из Администратора с закладки Files, далее меню Tools, а в нем Database>Multi-Database Index.

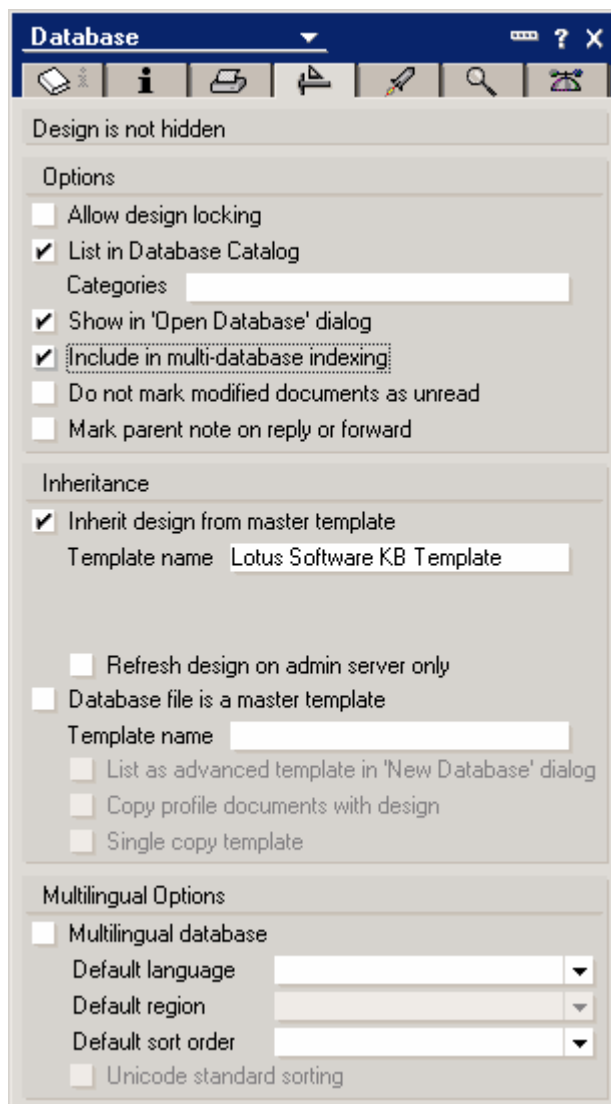


Рис. 430 Флаг *Include in multi-database indexing* в окне свойств базы

Сконфигурировать программу CATALOG в режиме Domain Catalog (Рис. 427).

Разрешить запуск и задать расписание работы доменного индексера в документе Server на закладке Server Tasks>Domain Indexer.

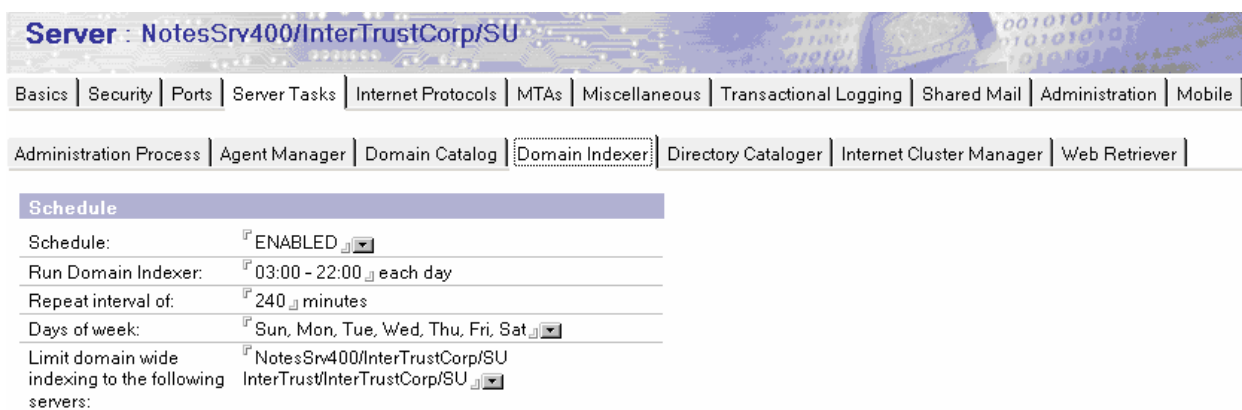


Рис. 431 Конфигурирование доменного индексера. Поле *Limit domain wide indexing...* ограничивает множество серверов, базы со свойством *Include in multi-database indexing* которых

должны индексироваться. Если поле пусто, индексируются все базы со свойством Include in multi-database indexing, для которых в базе CATALOG.NSF имеются документы

Проверить, что базы CATALOG.NSF на данном сервере нет. Если есть, удалить ее (имеется в виду, что она была создана для «обычного» режима). Запустить задачу Catalog командой консоли **load catalog**. Программа Catalog создаст и заполнит информацией новую базу Catalog (режим Domain Catalog). Кроме того, посредством программы Adminp будет автоматически создана группа LocalDomainCatalogServers.

Добавить в файл NOTES.INI параметр FT_SUMM_DEFAULT_LANGUAGE=English командой set config, чтобы «суммаризатор» (Summarizer) пользовался english.is (russian.is нет). «Суммаризатор» выбирает из документа, удовлетворяющего поисковому запросу, несколько предложений «со словами» из поискового запроса. По этим предложениям пользователь может оценить степень соответствия документа тому, что он ищет, не открывая сам документ. Работа «суммаризатора» по выборке из документа таких предложений для каждого языка определяется файлом <имя_языка>.is в каталоге программ сервера.

Перезапустить сервер – доменный индексер запустится автоматически. Можно не перезапускать сервер, а запустить доменный индексер командой консоли **load domidx**. Domain Indexer создаст индекс полнотекстового поиска по домену (физически находится в каталоге lotus\domino\data\ftdomain.di). Дождаться, пока будут проиндексированы выбранные базы (имеющие флаг Multi-Database Index), обратить внимание на загрузку процессора в это время.

Для индексирования файлов, «лежащих в файловой системе», в базе CATALOG.NSF из вида File Systems создается документ.

DATABASE CATALOG - File System

File Systems

Basics

Server name to index files on: Development/InterTrustCorp/SU

File Systems to Index

Current file system list:

- D:\Lotus\Domino\Data\Borneo\Import (R) () Borneo\Import

Deleted file system list:

Last file system set by: Vladimir A. Panov\InterTrustCorp/SU at 05.02.2002 16:19

Рис. 432 Документ File System

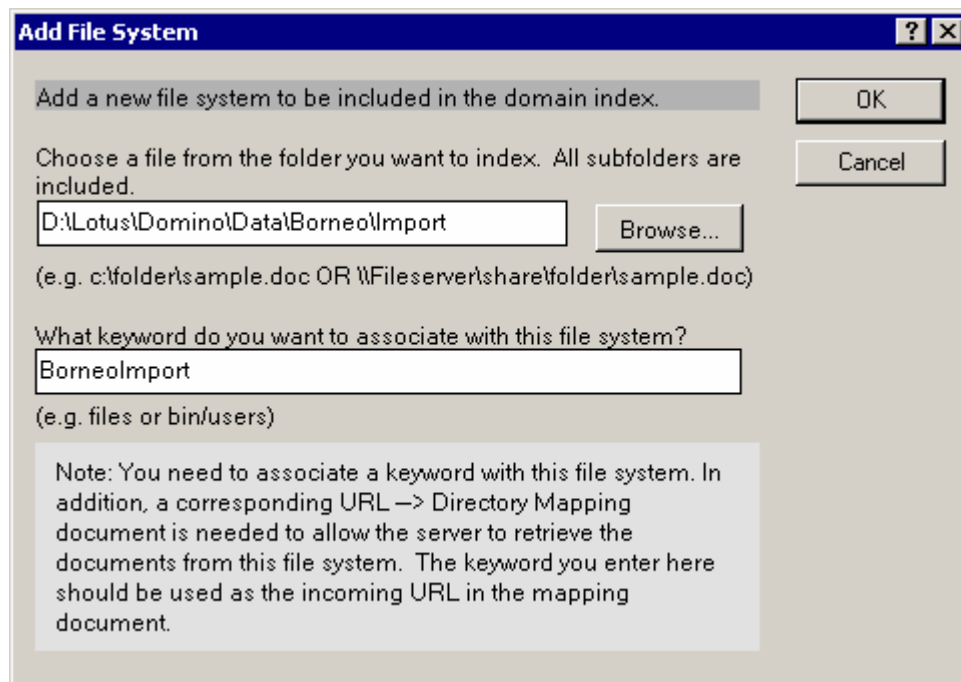


Рис. 433 Окно по кнопке Add...

С путем в первом поле обычно все понятно – оттуда доменный индексер читает индексируемые файлы. А текст во втором поле очень важен для того, чтобы пользователь смог «скачать» найденный файл. В любом случае (поиск клиентом Notes или браузером) найденный файл передается на компьютер пользователя по протоколу HTTP. Допустим, пользователь по поисковому запросу нашел нужный файл. Пусть реальный путь к найденному файлу будет D:\Lotus\Domino\data\Borneo\Import\folder1\folder2\file.doc. В этом случае URL для «скачивания» файла будет иметь вид http://hostname/BorneoImport/folder1/folder2/file.doc. Поэтому у вас 2 варианта поведения при заполнении второго поля:

- Создать в каталоге D:\Lotus\Domino\data\domino\HTML, автоматически доступном программе HTTP, каталог **Files** и помещать в него файлы для индексирования. Этот каталог указать в первом поле (полный путь C:\Lotus\Domino\data\domino\HTML\Files или domino\HTML\Files). Во втором поле «написать» **Files**.
- Размещать каталоги индексируемых файлов где угодно. Но создавать для программы HTTP документы Mapping/Redirection типа URL->Directory.



Рис. 434 Документ Mapping/Redirection muna URL->Directory...

R5 Mapping/Redirection for Development/InterTrustCorp/SU				
Basics	Site Information	Mapping	Access	Administration
Mapping				
Incoming URL string:	BorneoImport			
Target server directory:	D:\Lotus\Domino\data\Borneo\Import			

Рис. 435 ... разрешает программе HTTP передавать в браузер файлы из каталога D:\Lotus\Domino\data\Borneo\Import по URL вида http://hostname/BorneoImport/имя-файла

Некоторые параметры NOTES.INI, относящиеся к доменному индексеру:

- • FTG_No_Summary=1 «Суммаризатор» не должен выдавать контекст, когда пользователь не имеет доступа к документу.
- • FT_DOMAIN_DIRECTORY_NAME = *directory* Местоположение доменного индекса.
- • FT_INDEX_ATTACHMENTS=2 Не индексировать присоединенные файлы из документов индексированных баз.
- • FT_DOMAIN_IDXTHDS=*number of threads* Число потоков доменного индекса (по умолчанию 2 на процессор). Каждый поток индексирует или обновляет индекс отдельной базы. Очень сильно влияет на загрузку компьютера и скорость индексирования. В среднем скорость индексирования составляет 0.2 – 0.5 Гб информации в час.

1.52.6. 1.1.6. Использование индекса полнотекстового поиска «по домену»

Клиент Notes:

- • Указать имя Search Server в документе Location.
- • Выбрать из меню File>Preferences>Location Preferences.
- • На закладке Servers в поле Search server ввести имя сервера, поддерживающего поисковый индекс по домену - клиент будет обращаться к этому серверу при запросах на поиск по домену.
- • Сохранить и закрыть документ Location.
- • Из меню «кнопки с лупой» (правый верхний угол окна клиента) выбрать Domain Search

Броузер:

- • Из браузера http://hostname/catalog.nsf/DomainQuery

- • Чтобы «увидеть» результаты работы «суммаризатора», необходимо в поисковой форме выбрать опцию Detailed Results.
- • Чтобы «находить» проиндексированные файлы «из файловой системы», в поисковой форме в секции More должна быть выбрана опция File System.

1.52.7. 1.1.7. Упражнение

Сконфигурировать программы CATALOG и DOMIDX, проделав действия, рассмотренные в разделе 7.3.5. Индексирование файлов «в файловой системе» выполняется по желанию слушателя. Рассмотреть виды и документы в базе GATALOG.NSF. Проверить функционирование «поиска по домену» из клиента Notes и браузера (7.3.6).

**1.52.8. 1.1.8. Краткий обзор других продуктов Lotus,
обеспечивающих полнотекстовый и иной поиск по большим объемам
распределенных данных**

- ● IBM Lotus Extended Search 4.0
- ● Lotus Discovery Server 2.0.1
-

1.53. 1.1. Программа Agent Manager (AMGR)

1.53.1. 1.1.1. Назначение, архитектура и логика работы программы

Исполняет агентов в базах на сервере.

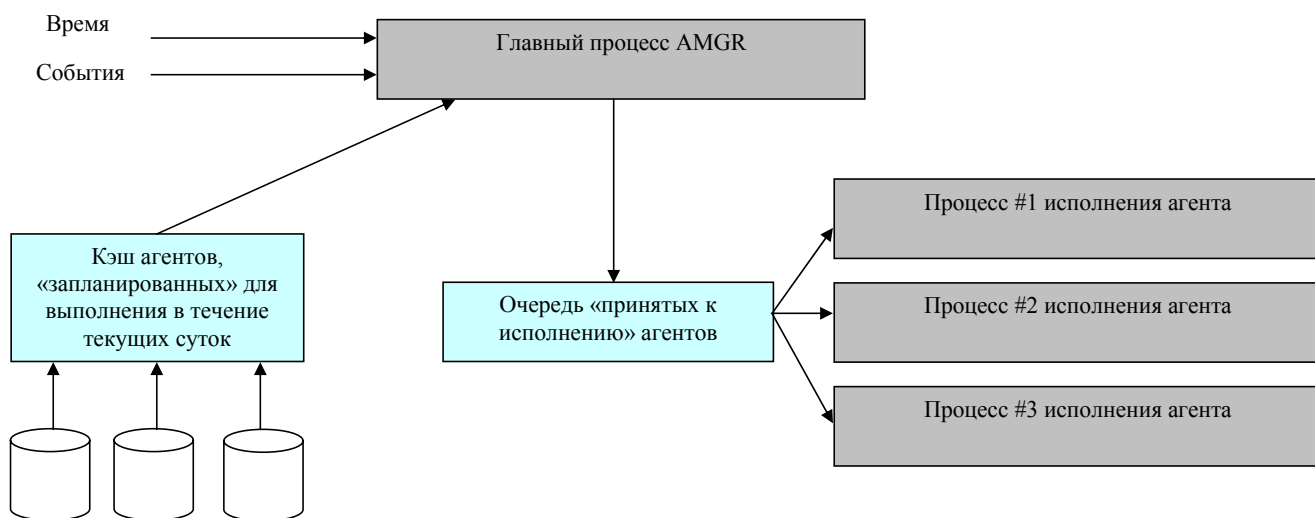


Рис. 1 Архитектура и логика работы

Агенты, написанные на языках Java или LotusScript, в зависимости от использованных их разработчиком языковых возможностей и методов встроенных классов, могут быть **«ограниченными по возможностям»** (restricted) или **«неограниченными по возможностям»** (unrestricted). «Неограниченные по возможностям» агенты могут работать с файлами, изменять системное время, отправлять почту, запускать другие программы или вызывать функции из стандартных или созданных их разработчиком библиотек динамической компоновки, то есть в принципе имеют как полный доступ к компьютеру сервера Domino, так и возможность передать информацию с этого компьютера на другие компьютеры. Такие агенты «в руках добропорядочного разработчика» могут выполнять сложные и «полезные» для вашей организации операции, а «в руках недобропорядочного разработчика» потенциально способны «нанести вред» вашей организации. Вопрос о «полезности» или «вредности» конкретного агента может быть решен администратором только посредством анализа всех его исходных текстов. Каждый агент автоматически «подписывается» разработчиком, когда тот сохраняет агента в базе. А у администратора имеется возможность разрешать или запрещать запуск на сервере агентов, созданных конкретными разработчиками. В ситуации «полного недоверия» администратор может разрешить запуск на сервере только «своих собственных» агентов, а от разработчиков требовать предоставления созданных ими агентов, и, после анализа их исходных текстов, «пересохранять агентов под своим ID-файлом, за своей подписью».

Когда наступает условие для запуска агента, главный процесс Agent Manager выполняет следующее:

1. Проверяет, кем «подписан» агент и (R6) от чьего имени он должен выполняться. Обычно агент подписан тем разработчиком, который последним сохранил этого агента.

3. Если агент написан на языке LotusScript или Java, проверяет по коду агента, является ли он «ограниченным» или «неограниченным» по своим возможностям. Проверка означает просмотр списка вызываемых агентом функций и методов классов и поиск их во встроенной таблице методов классов и функций «с неограниченными возможностями».

2. Проверяет информацию из документа Server, чтобы определить, разрешил ли администратор сервера запускать на нем такого агента.
4. Если выполнение разрешено, передает агента в очередь на исполнение.

AMGR выполняет выполняет агентов со следующими условиями запуска:

- • **On event** (по событию)
 - • After new mail has arrived – после доставки Router-ом сообщения в почтовую базу
 - • After documents are created or modified – после создания или модификации документа в базе
- • **On schedule** (по расписанию)
 - • More than once a day – чаще, чем раз в сутки (минимальная частота 5 минут)
 - • Daily – раз в сутки
 - • Weekly – раз в неделю
 - • Monthly – раз в месяц

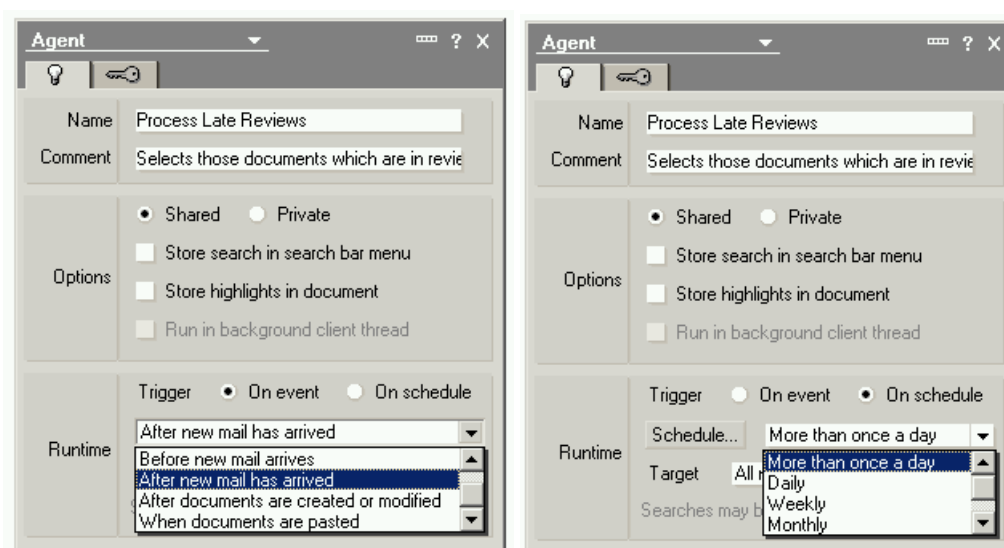


Рис. 2 Агенты по событию и расписанию, выполняемые AMGR

AMGR выполняет не всех агентов в базах и не весь созданный разработчиками и выполняемый на сервере код:

- • Агенты, запускаемые на клиенте, выполняются на этом клиенте. В том числе и агенты в локальных базах клиента, выполняемые по расписанию (флаг Enable scheduled local agents в User Preferences на закладке Basics)
- • Агенты, запускаемые на клиенте, могут вызывать агентов, выполняющихся на сервере - последние выполняются в потоках самого сервера, а не программой AMGR
- • Агенты, «запускаемые из браузера» по событиям WebQueryOpen, WebQuerySave и URL <http://Host/Database/AgentName?OpenAgent>, выполняются программой HTTP в потоках генерации страниц или выделенном потоке в зависимости от выбора в поле Run web agents concurrently на закладке Internet Protocols – Domino Web Engine документа Server
- • Агенты по событию Before new mail arrived выполняются программой Router в потоках доставки (Delivery)
- • «Удаленные вызовы» выполняются программой ДПОР.

1.53.2. 1.1.2. Конфигурирование программы

Server : LAEC/LAEC/InterTrustCorp/SU

[Basics](#) | [Security](#) | [Ports](#) | [Server Tasks](#) | [Internet Protocols](#) | [MTAs](#) | [Miscellaneous](#) | [Transactional Logging](#) | [Shared Mail](#) | [Administration](#)

[Administration Process](#) | [Agent Manager](#) | [Domain Catalog](#) | [Directory Cataloger](#) | [Internet Cluster Manager](#) | [Web Retriever](#) | [Remote Debug Manager](#)

Basics

Refresh agent cache: 00:00

Daytime Parameters	Nighttime Parameters
Start time: 08:00	Start time: 20:00
End time: 20:00	End time: 08:00
Max concurrent agents: 1	Max concurrent agents: 2
Max LotusScript/Java execution time: 10 minutes	Max LotusScript/Java execution time: 15 minutes
Note: The following setting only applies to servers running R4.6 and earlier	Note: The following setting only applies to servers running R4.6 and earlier
Max % busy before delay: 50	Max % busy before delay: 70

Рис. 3 Документ Server, закладка Server Tasks – Agent Manager

Refresh agent cache. Кэш Agent Manager содержит список агентов, «запланированных» для выполнения в течение текущих суток. В данном поле дается время, когда программа должна обновлять список агентов, запланированных для выполнения в течение суток, а так же занести в LOG.NSF информацию об агентах, выполненных за предыдущие сутки.

Daytime и Nighttime Start и End Time. Эти поля «разбивают» сутки на два отрезка – «дневное» и «ночное» время. По умолчанию «дневное» время с 8 утра до 8 вечера, а «ночное» - с 8 вечера до 8 утра. Для каждого отрезка времени для Agent Manager выделяется то или иное количество ресурсов, обычно меньшее в «дневное» время и относительно большее в «ночное» время. Отрезки «дневного» и «ночного» времени не должны пересекаться. Во время суток, не принадлежащее ни к «дневному», ни к «ночному» отрезкам, программа вообще не будет выполнять никаких агентов.

Daytime и Nighttime Max concurrent agents. Только один агент может выполняться в одной базе данных в одно и то же время, но агенты в разных базах данных на том же самом сервере могут выполняться одновременно, однако в количестве не большем, чем определено в этом поле. Значение по умолчанию - 1 для «дневного» времени и 2 для «ночного» времени. Согласно указанному вами значению главный процесс Agent Manager запускает соответствующее число своих процессов исполнения агентов, которые отображаются по команде Show Task как **Agent Manager Executive '1': статус**, **Agent Manager Executive '2': статус** ... Каждый из этих процессов одновременно может исполнять только одного агента. Количество этих процессов обычно различно на «дневном» и «ночном» отрезках времени.

Daytime и Nighttime Maximum LotusScript/Java execution time. Эти поля ограничивают время, отводимое на выполнение одного агента, написанного на языке LotusScript или Java, на «дневном» и «ночном» отрезках времени. Если такой агент не успевает завершиться за заданное время, то процесс исполнения агента прекращает выполнять его. Данная возможность введена, в частности, для предотвращения потери производительности сервера из-за заикливания «недостаточно отлаженных» агентов.

Daytime и Nighttime Max % busy before delay. В версиях R5 и R6 более не используются...

Кроме того, на работу Agent Manager оказывают влияние следующие параметры из файла NOTES.INI:

- • **AMgr_NewMailAgentMinInterval = значение.** Задаёт минимальное время (в минутах), которое должно пройти между последовательными выполнениями одного и того же агента, запускаемого по факту доставки почты (mail-triggered). Значение по умолчанию 0.
- • **AMgr_NewMailEventDelay = значение.** Задаёт время задержки (в минутах) перед выполнением агента, запускаемого по факту доставки почты (от момента обнаружения события доставки почты до выполнения агента). Значение по умолчанию 1.
- • **AMgr_DocUpdateAgentMinInterval = значение.** Задаёт минимальное время (в минутах), которое должно пройти между выполнением агента, запускаемого по факту изменения документа в базе (update-triggered), на одном и том же документе. Значение по умолчанию 30. Установка в 0 – не отсутствие задержки, а некоторая «минимально допустимая задержка по умолчанию».
- • **AMgr_DocUpdateEventDelay = значение.** Задаёт время задержки (в минутах) перед выполнением агента, запускаемого по факту создания нового или изменения существующего документа в базе (от момента обнаружения события изменения документа до выполнения агента). Значение по умолчанию 5.
- • **AMgr_SchedulingInterval = значение.** Agent Manager периодически проверяет, не появилось ли новых агентов, которые ему нужно выполнять. Данный параметр задаёт задержку в минутах перед запуском процесса, выполняющего эту проверку (Agent Manager's scheduler). Допустимые значения от 1 минуты до 60 минут. По умолчанию 1 минута.
- • **AMgr_UntriggeredMailInterval = значение.** Задержка в минутах между запусками процесса, выполняющего проверку появления почты «не по событию» (Agent Manager's check for untriggered mail). Допустимые значения от 1 минуты до 1440 минут. По умолчанию 60 минут.
- • **AMgr_WeekendDays = день1, день2, ...** Когда агент запускается по расписанию, для него в окне Schedule доступна опция **Don't run on weekends**, запрещающая выполнение этого агента по выходным дням. Данный параметр содержит список дней, которые считаются выходными (воскресенье = 1, понедельник = 2, ..., суббота = 7). Значение по умолчанию для уик-энда - суббота (7) и воскресенье (1).
- • **Log_AgentManager = значение** Значение 1 требует протоколировать (на консоли сервера и в базе LOG.NSF) факт запуска каждого агента, значение 2 – только факт успешного запуска агента, а значение 0 - не протоколировать.

Имеется возможность запрещать в конкретной базе выполнение всех агентов, запускаемых по расписанию, приходу почты или модификации документа. Для этого в окне свойств базы на закладке Basics необходимо установить опцию **Disable background agents for this database**.

1.53.3. 1.1.3. Права для выполнения агентов на сервере R5

SERVER: training01/R5/US/ETC/InterTrust/RU

Basics | **Security** | Ports | Server Tasks | Internet Protocols | MTAs | Miscellaneous | Transactional Logging | Administration

Security Settings Compare Notes public keys against those stored in Directory: ☐ Yes ☒ No Allow anonymous Notes connections: ☐ Yes ☒ No Check passwords on Notes IDs: ☐ Enabled ☒ Disabled	Web Server Access Web server authentication: ☐ More name variations with lower security
Server Access Who can - Only allow server access to users listed in this Directory: ☐ No Access server: Not access server: Create new databases: Administrators Create replica databases: Administrators Allowed to use monitors: Not allowed to use monitors: Administer the server from a browser: Admin/R5/US/ETC/InterTrust/RU	Pass thru Use Who can - Access this server: Route through: Cause calling: Destinations allowed:
Agent Restrictions Who can - Run personal agents: Administrators Run restricted LotusScript/Java agents: Administrators, LocalDomainServers, ServersMSC, AdminMSC Run unrestricted LotusScript/Java agents: training01/R5/US/ETC/InterTrust/RU, ServersMSC, AdminMSC	Java/COM Restrictions Who can - Run restricted Java/Javascript/COM: Run unrestricted Java/Javascript/COM:

Рис. 4 Документ Server R5, закладка Security

1.53.4. 1.1.4. Права для выполнения агентов на сервере R6



Рис. 5 Это ссылка на статью Юлии Кадашевич (Julie Kadashevich) в LDD (Today.nsf)

- Агент, выполняющийся на одном сервере, может иметь доступ к другому серверу – поле Trusted servers в самом конце закладки Security документа Server должно содержать список серверов, агенты которых могут иметь доступ к базам на данном сервере.
- Пользователь с правами редактора в базе может разрешать или запрещать запуск агента, например, Out Of Office. Как это достигается, смотрите в статье LDD.
- Новые поля Programmability Restrictions (Agent Security).

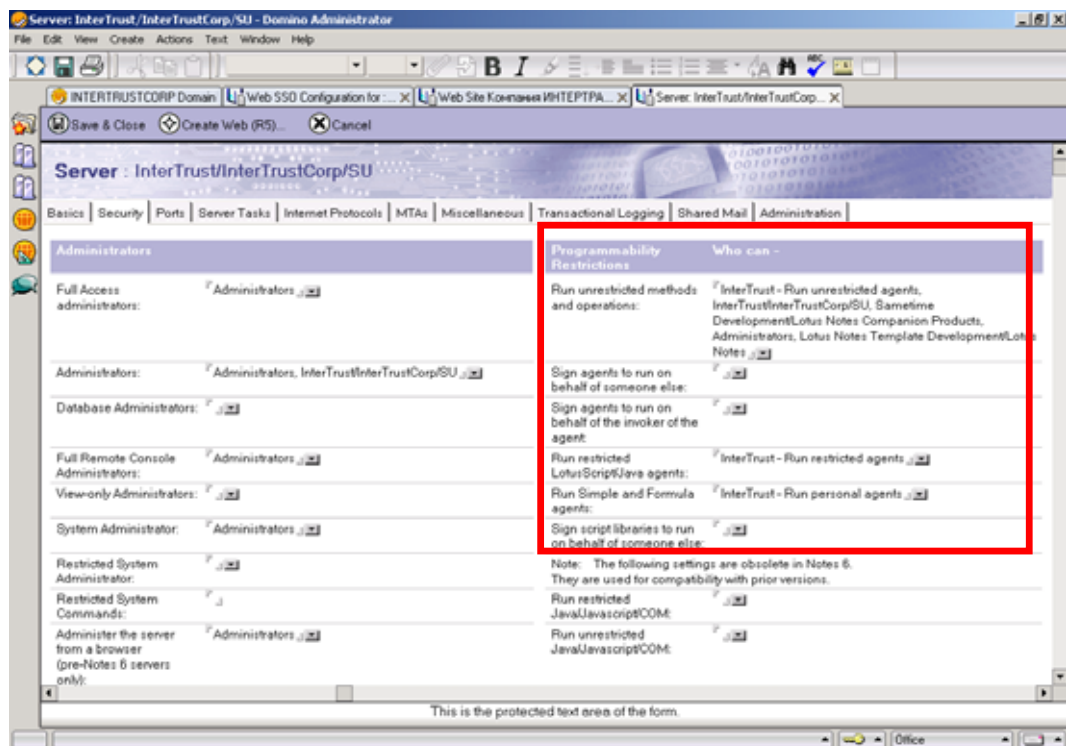


Рис. 6 Документ Server R6, закладка Security

Перед выполнением агента проверяется «вхождение» имени, с правами которого агент будет выполняться (имени подписавшего агента; имени того, от чьего имени агент должен выполняться; имени запустившего агента) в три следующих поля.

- **Run unrestricted methods and operations** – имена тех, чьи агенты выполняются сервером без ограничений. Касается любых агентов и не-агентов: LotusScript, Java, JavaScript, COM и ДПОР и любых действий, ими выполняемых: access the system by manipulating system time, file I/O, and operating system commands... «Пусто» означает «никто за исключением Full Access Administrators, самого сервера и Lotus Notes Template Development». Дополнительно входящие в это поле имеют возможность создавать («подписывать») агентов, выполняющихся от имени других (не разработчика, подписавшего агента), а так же создавать («подписывать») библиотеки скриптов, используемые в агентах, выполняемых от имени других.
- **Run restricted LotusScript/Java agents** - имена тех, чьи агенты с ограниченными возможностями, написанные на LotusScript или Java, выполняются сервером. «Пусто» трактуется как «никто», кроме тех, у кого права Run unrestricted.
- **Run Simple and Formula agents** - имена тех, чьи агенты, написанные на простых действиях или @-формулах, как private так и shared, выполняются сервером. По умолчанию поле пустое, что трактуется как «все».

Следующие три поля регламентируют возможность создания агента, выполняемого от имени других, теми разработчиками, которые не указаны в поле Run unrestricted methods and operations.

- **Sign agents to run on behalf of someone else** – имена тех, кто может подписывать агентов с ограниченными возможностями, выполняемых сервером от имени других (не разработчика, подписавшего агента). Касается только агентов со свойством \$OnBehalf, выполняемых по расписанию. Например, такой агент, созданный разработчиком, но выполняемый от имени пользователя, указанного разработчиком в поле \$OnBehalf, получит доступ в почтовый ящик этого пользователя. По умолчанию поле пустое, что трактуется как «никто», за исключением явно или неявно указанных в поле Run unrestricted methods and operations. Сам сервер и Lotus Notes Template Development всегда обладают этим правом.
- **Sign script libraries to run on behalf of someone else** - имена тех, кто может подписывать библиотеки скриптов, используемые в агентах, выполняемых от имени других (не

подписавшего агента). По умолчанию пусто, что означает «все». Сам сервер, Lotus Notes Template Development и указанные в поле Run unrestricted methods and operations всегда имеют это право.

- **Sign agents to run on behalf of the invoker of the agent** - имена тех, кто может подписывать агентов, выполняемых от имени запустившего агента. Например, web-агент, запускаемый от имени пользователя. По умолчанию пусто, что означает «все». Сам сервер, Lotus Notes Template Development и указанные в поле Run unrestricted methods and operations всегда имеют это право.

1.53.5. 1.1.5. Устранение проблем с выполнением агентов

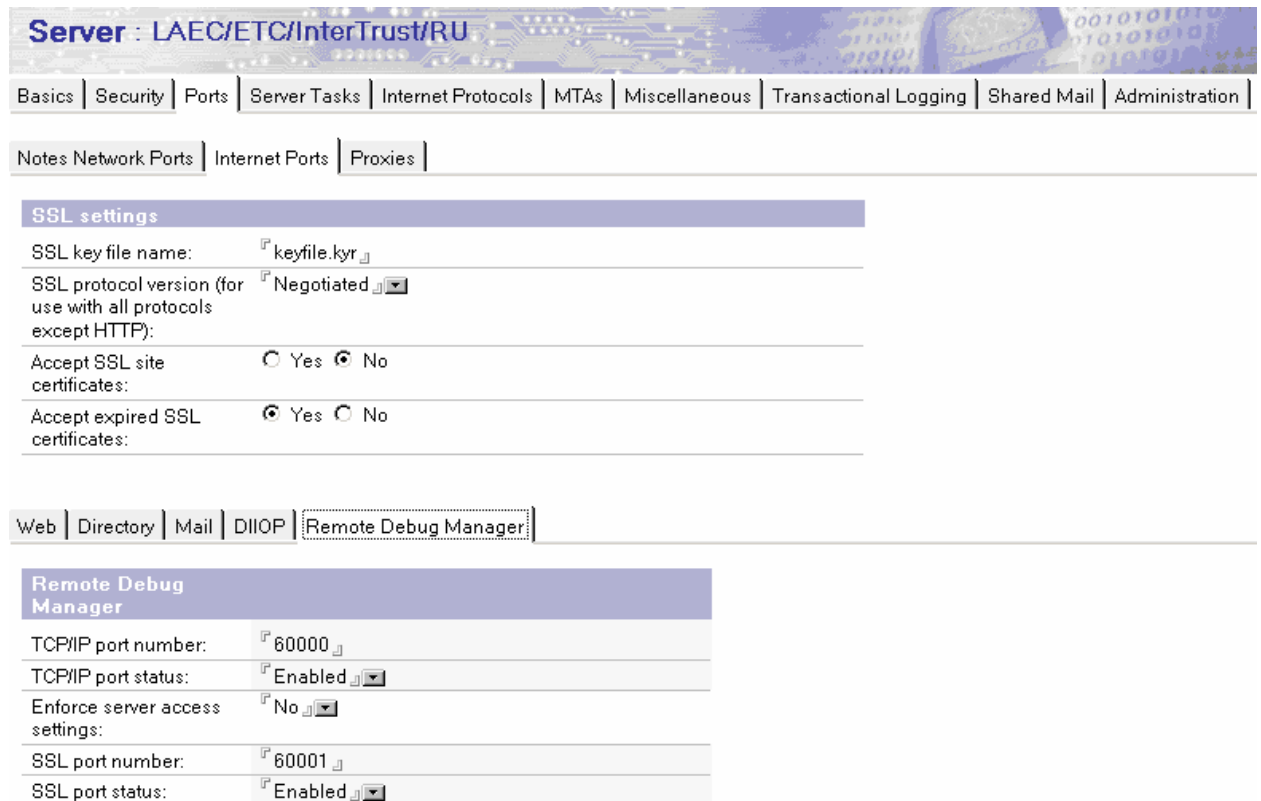
Command	Result
Tell Amgr Cancel	Cancels the scheduled agent that is currently running. Specify the agent to be cancelled by entering these arguments: "db name" 'agent name' Example: Tell Amgr Cancel "DatabaseName.nsf" 'AgentName' Note You can use the Tell Amgr Schedule command to determine which agents can be cancelled.
Tell Amgr Debug	Displays either the current debug settings for the Agent Manager or lets you set new ones. When using this command to set debug values, you can use the same flags used by the Debug_AMgr command in the NOTES.INI file. These settings take effect immediately; you do not need to restart the Agent Manager or the server.
Tell Amgr Run	Runs the agents that you designate with these arguments: "db name" 'agent name' Example: Tell Amgr Run "DatabaseName.nsf" 'AgentName'
Tell Amgr Pause	Pauses scheduling of agents
Tell Amgr Quit	Stops the Agent Manager on a server.
Tell Amgr Resume	Resumes scheduling of agents.
Tell Amgr Schedule	Shows the schedule for all agents scheduled to run for the current day. In addition, the command shows the agent trigger type, the time the agent is scheduled to run, the name of the agent, and the name of the database on which the database runs. Checking the Agent Manager schedule lets you see if an agent is waiting in one of the Agent Manager queues. Agent Manager 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	This command shows a snapshot of the Agent Manager queues and displays the Agent Manager settings in the Server document.

1.54. 1.1. Программа Remote Debug Server (RDEBUG)

1.54.1. 1.1.1. Назначение и конфигурирование

Назначение – удаленная отладка разработчиками на сервере агентов, написанных на LotusScript.

ServerTasks=Update, Replica, Router, AMgr, AdminP, CalConn, Sched, Statlog, DIIOP, DEC S, HTTP, IMAP, LDAP, POP3, **Rdebug**, runjava ChangeMan



Server : LAEC/ETC/InterTrust/RU

Basics | Security | Ports | Server Tasks | Internet Protocols | MTAs | Miscellaneous | Transactional Logging | Shared Mail | Administration

Notes Network Ports | Internet Ports | Proxies

SSL settings

SSL key file name:

SSL protocol version (for use with all protocols except HTTP):

Accept SSL site certificates: ☐ Yes ☒ No

Accept expired SSL certificates: ☒ Yes ☐ No

Web | Directory | Mail | DIIOP | Remote Debug Manager

Remote Debug Manager

TCP/IP port number:

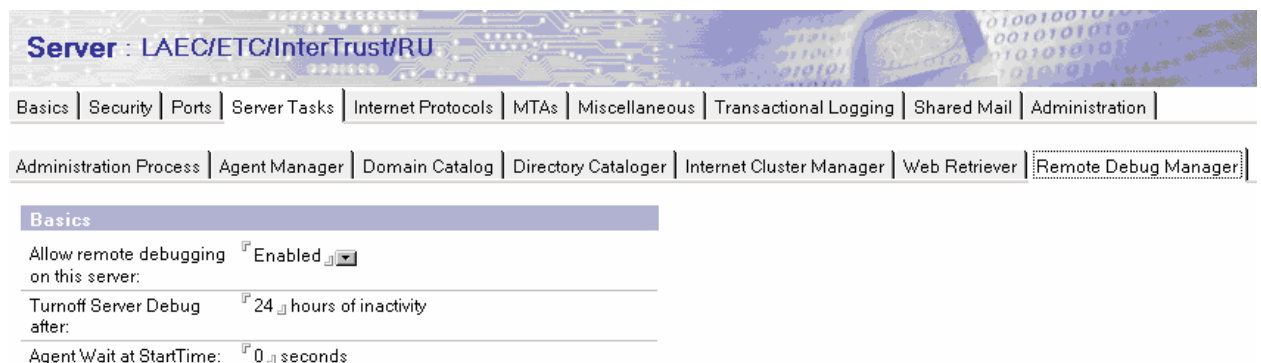
TCP/IP port status:

Enforce server access settings:

SSL port number:

SSL port status:

Рис. 440 Разрешить порт, используемый отладчиком



Server : LAEC/ETC/InterTrust/RU

Basics | Security | Ports | Server Tasks | Internet Protocols | MTAs | Miscellaneous | Transactional Logging | Shared Mail | Administration

Administration Process | Agent Manager | Domain Catalog | Directory Cataloger | Internet Cluster Manager | Web Retriever | Remote Debug Manager

Basics

Allow remote debugging on this server:

Turnoff Server Debug after: hours of inactivity

Agent Wait at StartTime: seconds

Рис. 441 Конфигурирование

Turnoff Server Debug after – автоматический останов через 24 часа неиспользования или –1, чтобы программа сама никогда не завершалась.

Agent Wait at Start Time – пауза перед выполнением агента, позволяющая разработчику подключиться к программе удаленным отладчиком. Рекомендуется задать 60 – 120 секунд.

1.54.2. 1.1.2. Удаленная отладка агентов на сервере

В Designer создаем агента...

Рис. 442 Свойства агента

Рис. 443 Разрешать запуск по расписанию необязательно, но сервер должен быть выбран

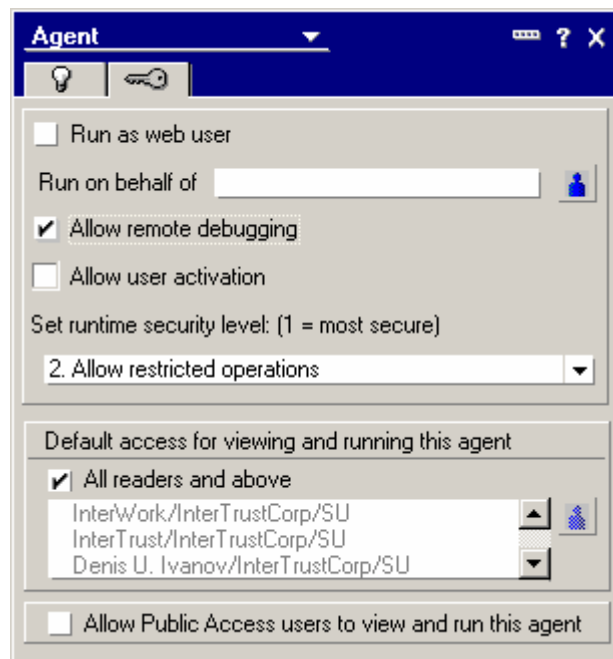


Рис. 444 Флаг Allow remote debugging обязателен

Sub Initialize

Print "*** Agent statred..."**

Sleep 60

Print "***** Agent go..."

Dim session As New NotesSession

Dim db As NotesDatabase

Set db = session.CurrentDatabase

REM Open xml file named after current database

Dim stream As NotesStream

Set stream = session.CreateStream

filename\$ = "c:\dxl\" & Left(db.FileName, Len(db.FileName) - 3) & "dxl"

If Not stream.Open(filename\$) Then

 MessageBox "Cannot open " & filename\$,, "Error"

 Exit Sub

End If

Call stream.Truncate

REM Create note collection

Dim nc As NotesNoteCollection

Set nc = db.CreateNoteCollection(False)

nc.SelectDocuments = True

Call nc.BuildCollection

REM Export note collection as DXL

Dim exporter As NotesDXLExporter

Set exporter = session.CreateDXLExporter(nc, stream)

Call exporter.Process

Print "***** Agent ended..."

End Sub



Рис. 445 В Designer открываем окно удаленной отладки – File-Tools-Remote Debugger. Переключаемся в клиента администратора и пускаем агента с удаленной консоли командой `tell amgr run names.nsf 'RDebugTest'`. Возвращаемся в это окно...

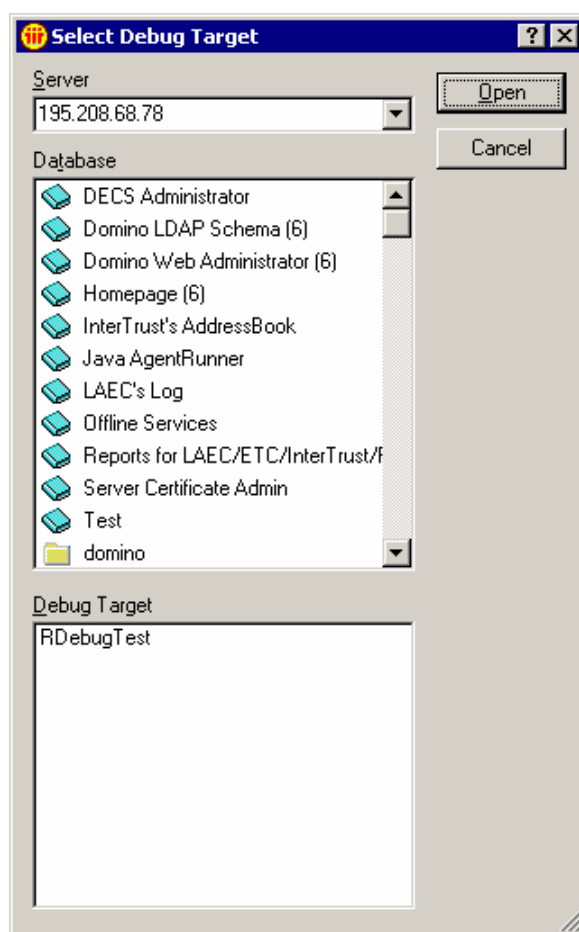


Рис. 446 «Кликаем» Select debug target и в полученном диалоговом окне выбираем нужный сервер и базу. Если агент уже запустился, но еще не завершился, во фрейме Debug Target появляется имя агента. «Кликаем» имя агента или нажимаем кнопку Open...

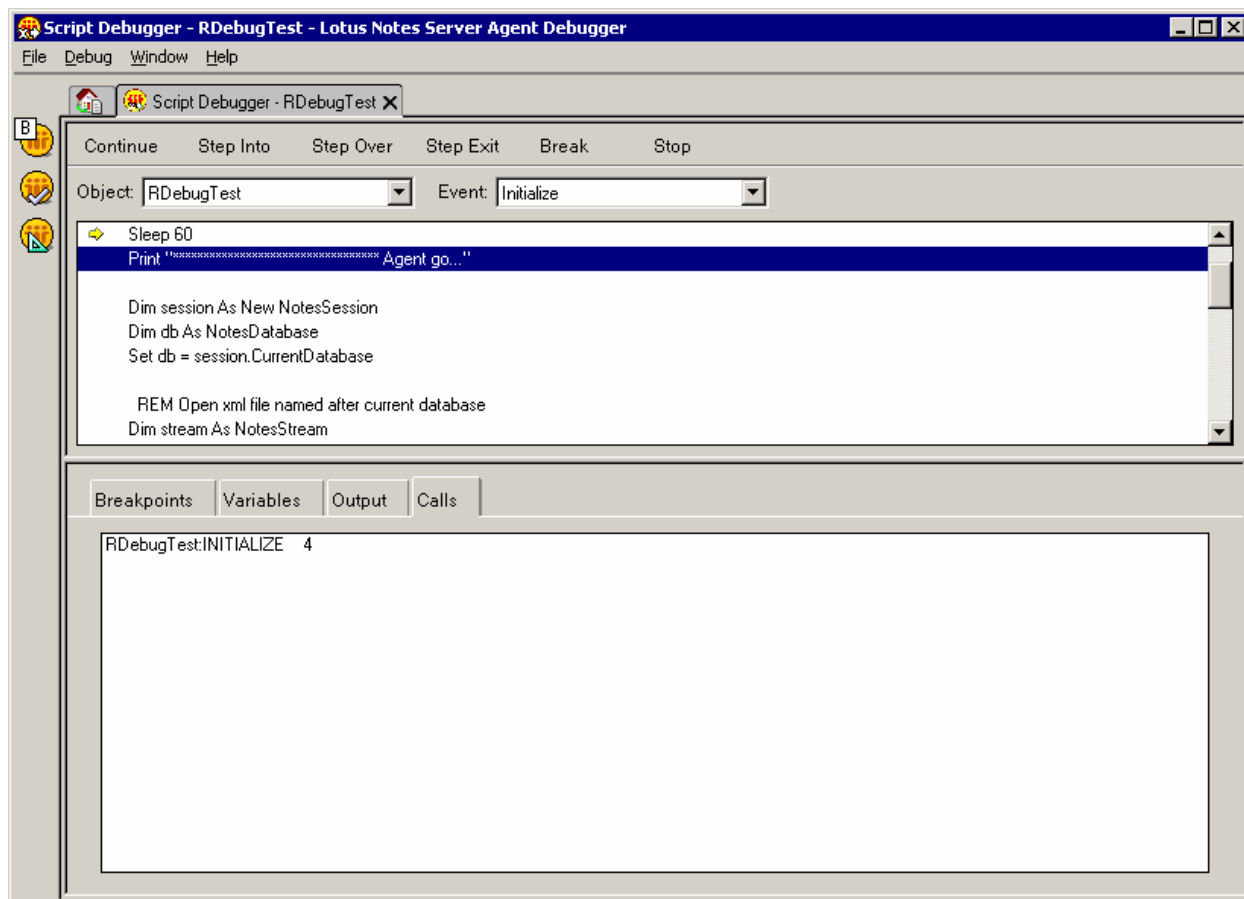


Рис. 447 Появляется окно Script Debugger, в котором и ведется отладка...

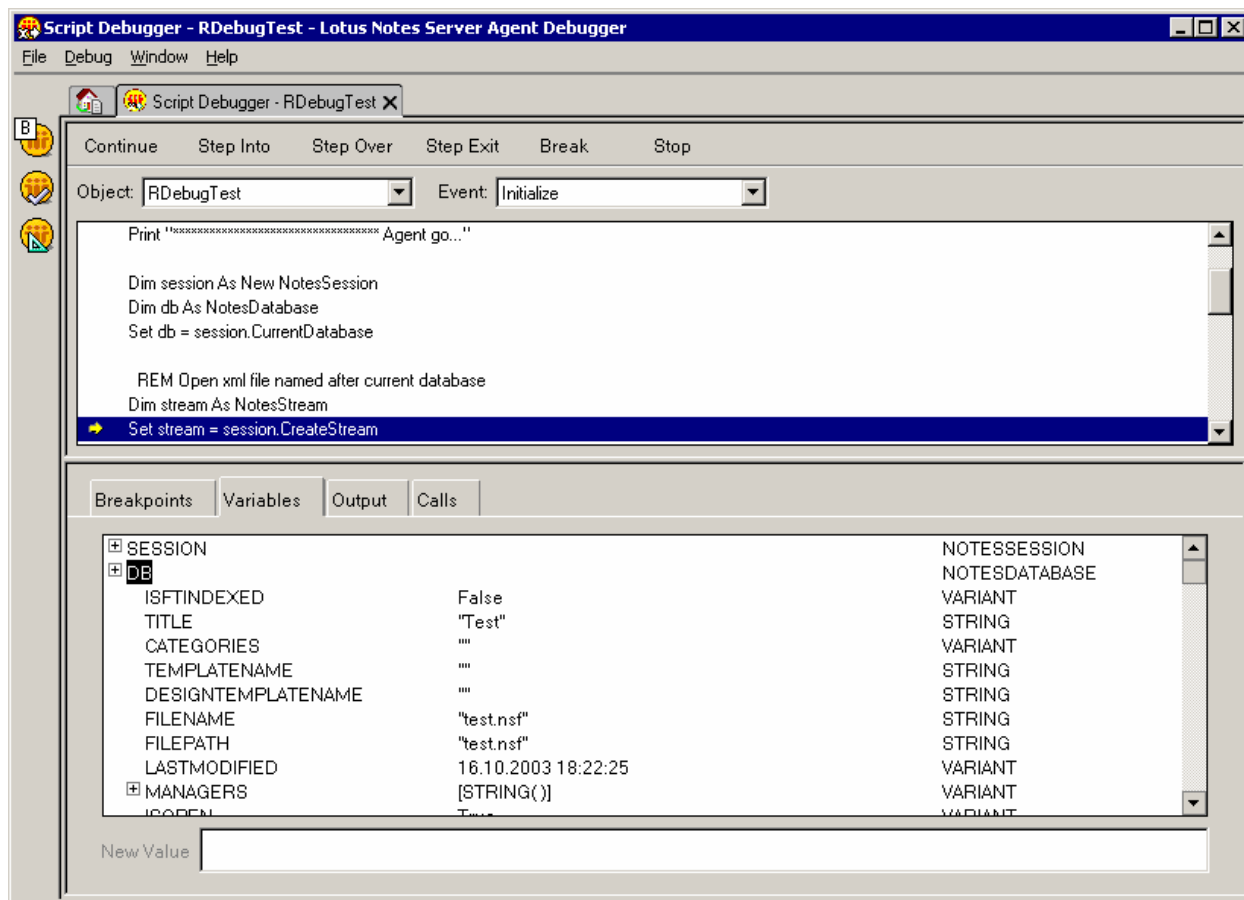


Рис. 448 Идет отладка...

1.55. 1.1. Программа Designer (Design)

1.55.1. 1.1.1. Логика процесса приведения элементов дизайна баз в соответствие с шаблоном

Программа Design по умолчанию запускается сервером в 1 час ночи. Назначение программы – привести элементы дизайна баз в соответствие с шаблонами.

Программа просматривает все файлы баз на сервере и, в зависимости от их свойств, создает два списка:

- список баз, которые наследуют дизайн с шаблона;
- список баз, которые являются шаблонами.

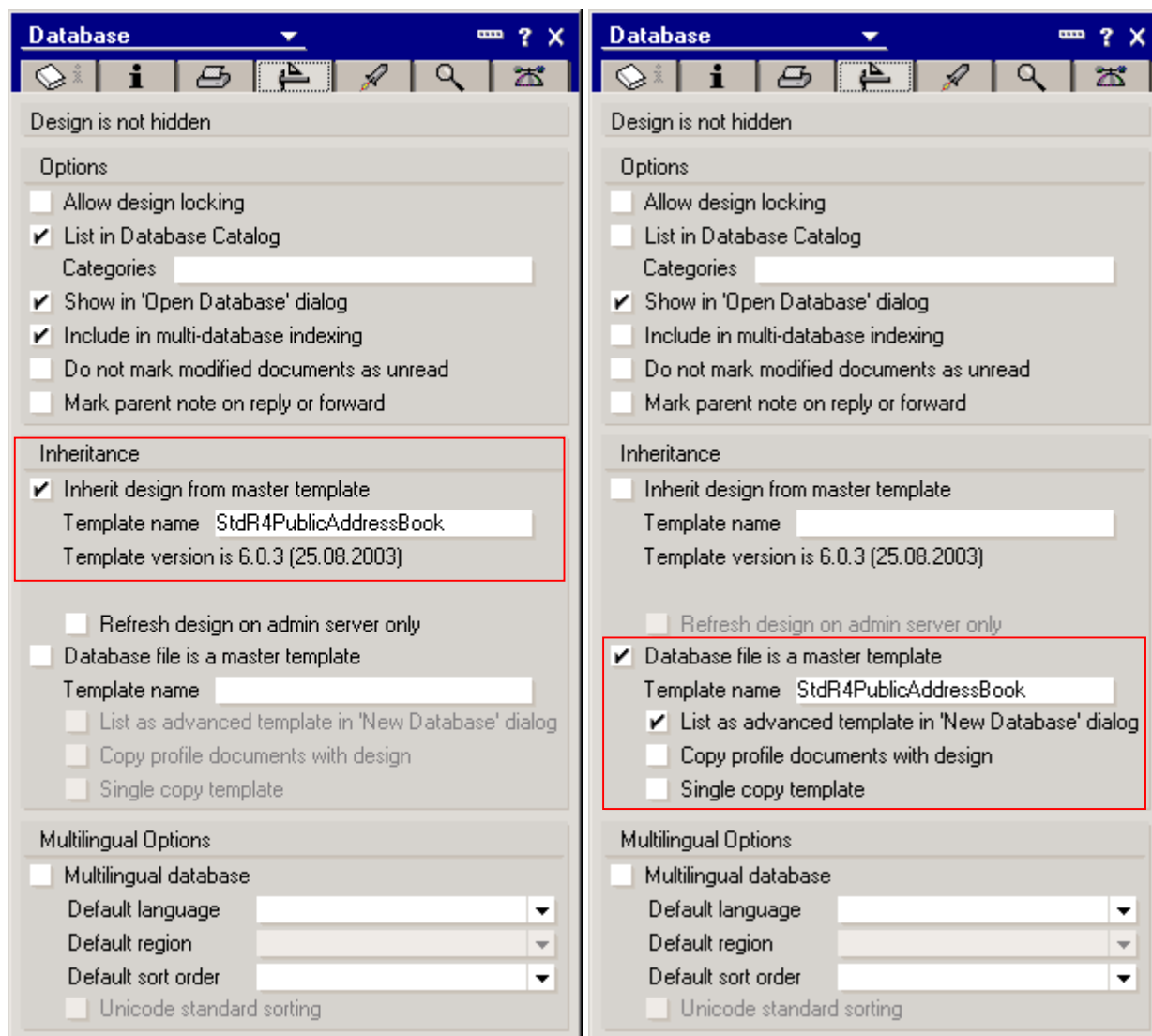


Рис. 449 Слева – база NAMES.NSF, которая наследует дизайн с шаблона с именем StdR4PublicAddressBook. Справа – база PUBNAMES.NTF, которая является шаблоном с именем StdR4PublicAddressBook

Далее для каждой базы, наследующей дизайн с некоторого шаблона с именем TemplateName (первый список), выполняется поиск базы, которая является шаблоном с именем TemplateName (второй список). Шаблон должен быть найден – в противном случае в LOG.NSF появляется сообщение наподобие «Warning: Cannot locate design template 'AFServerConfiguration2.5' used by 'AFServer Configuration 2.5'». Возможен случай, когда на сервере окажется несколько баз, являющихся шаблоном с именем TemplateName – в таком случае в LOG.NSF появляются сообщения наподобие «Warning: Both mail50.ntf

and test\mail501.ntf claim to be Design Template 'StdR50Mail'». Из нескольких шаблонов сначала выбираются те, которые имеют расширение NT* (если есть), затем – один, имеющий «меньшее» в лексикографическом порядке имя.

Если шаблон найден или выбран из нескольких, начинается сопоставление элементов дизайна в базе и шаблоне. Сопоставление элементов дизайна выполняется по их именам и алиасам (значение поля \$Title), а не по универсальным идентификаторам UNID (документ 1097253 из базы знаний).

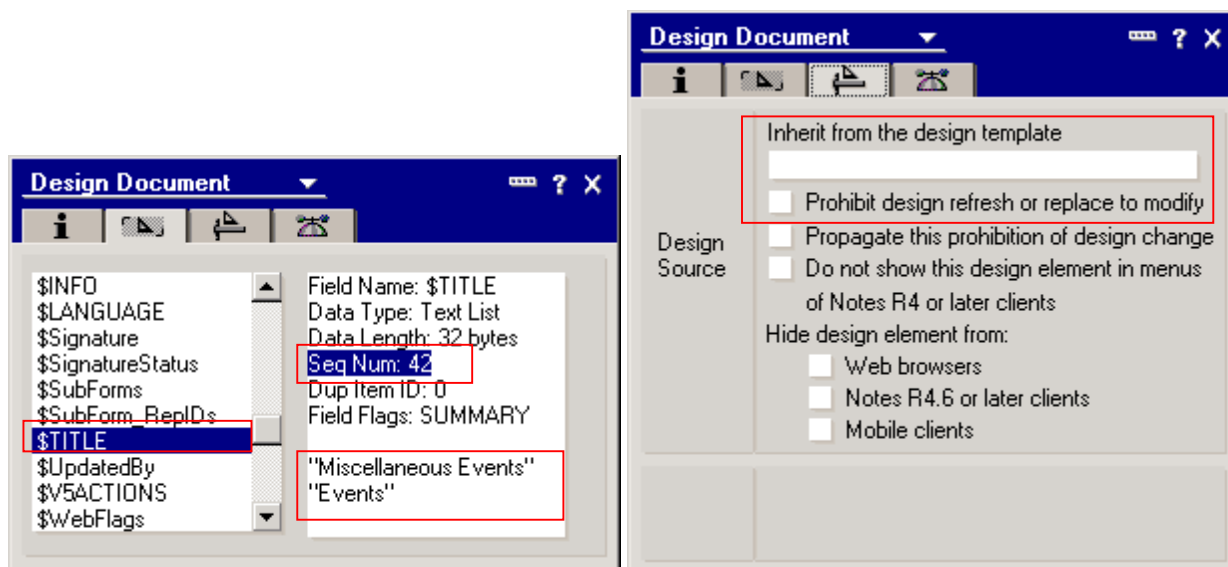


Рис. 450 Свойства элемента дизайна – слева имя и алиасы элемента дизайна в поле \$Title и количество модификаций в свойстве Seq Num, справа – два «чистых» поля, означающих, что элемент дизайна наследуется из шаблона, указанного в свойствах файла базы, и что заменять этот элемент дизайна не запрещено

Если элемент дизайна наследуется из шаблона, указанного в свойствах файла базы, и заменять этот элемент дизайна не запрещено, выполняется следующее:

- если в базе и шаблоне имеется элемент дизайна с одинаковым \$Title, при различии Seq Num или времен модификации элемент дизайна в базе заменяется элементом дизайна из шаблона;
- если в шаблоне имеется элемент дизайна с \$Title, которого нет в базе, он копируется в базу;
- если в базе имеется элемент дизайна с \$Title, которого нет в шаблоне, он удаляется из базы

Рассмотренная выше схема работы отражает не все особенности. Во-первых, элемент дизайна в базе может быть запрещено обновлять или заменять – когда выбрана опция Prohibit design refresh or replace to modify. Во-вторых, конкретный элемент дизайна в базе может наследоваться не из шаблона, который указан в свойствах базы, а из шаблона, который указан в свойствах элемента дизайна – когда поле Inherit from the design template содержит имя шаблона TemplateName для данного элемента дизайна.

Операция замены элементов дизайна (Replace) отличается от операции обновления элементов дизайна (Refresh) в сущности одним шагом – старое имя шаблона в свойствах базы сначала заменяется на новое.

Отметим аналогию между программами сервера Domino (применяются ко многим базам) и операциями из клиента Notes (применяются к конкретной базе):

- обновление элементов дизайна, выполняемое программой Design ~

- операция File-Database-Refresh Design;
- замена элементов дизайна, выполняемая утилитой Convert ~
- операция File-Database-Replace Design.

1.55.2. 1.1.2. Новые аспекты программы Design в R6

1.55.2.1. 1.1.2.1. Ключи

Command line option	Description
-d <i>directory name</i>	Synchronizes the databases in a directory relative to the data directory. For example, to synchronize databases in the directory DATA\SALES, specify -d SALES.
-f <i>filename</i>	Synchronizes a specific database. For example, to synchronize the database DATA\SALES.NSF, specify -f SALES.NSF.
-i <i>name</i>	Synchronizes the databases specified by <i>name</i> , which can be a database, folder, or filename that contains a list of paths, each of which can be a database or a folder.

1.55.2.2. 1.1.2.2. Замена дизайна только на сервере администрирования базы

Свойство базы **Refresh design on admin server only**.

1.55.2.3. 1.1.2.3. Поле Create master templates в документе Server

Рассматриваемые здесь поля находятся в документе Server на закладке Security.

В версиях до R6 поле **Create databases & templates** определяет тех, кто может создавать на сервере новые базы и шаблоны. Поле по умолчанию пусто, что трактуется как «разрешено всем».

В версиях R6 сохранилось поле **Create databases & templates** - оно определяет тех, кто может создавать на сервере новые базы и, но только из клиентов R5, «бесполезные» шаблоны с пустым полем Template Name. Поле по умолчанию пусто, что трактуется как «разрешено всем».

В версиях R6 добавлено поле **Create master templates**, которое определяет тех, кто может создавать на сервере «нормальные» шаблоны. По умолчанию поле пусто, что трактуется как «не разрешено никому».

Разделение возможности создавать базы и шаблоны в R6 является совершенно обоснованным по соображениям безопасности. Однако при абгрейте сервера R5 на R6 и установке нового сервера R6 может служить источником недоразумений – пока поле Create master templates пусто, никто не сможет создавать «нормальные» новые шаблоны. Из клиента R5 копия шаблона на сервер создается успешно, но при этом поле Template Name в копии «молча очищается». В клиенте R6 в такой ситуации выдается сообщение «You do not have sufficient access to create master templates on this server». Аналогичное сообщение можно встретить при установке на сервер R6 некоторых программных продуктов, в процессе установки создающих на сервере новые шаблоны (в частности Lotus Enterprise Integrator/ LEI 6.0).

1.55.2.4. 1.1.2.4. Single Copy Template (SCT)

➤  **стр. 262 - 265**

1.56. 1.1. Подсистема Free Time system

1.56.1. 1.1.1. Назначение и логика работы подсистемы учета свободного времени

Система учета свободного времени (Free Time system) включает две серверных программы: Schedule Manager (SCHED) и Calendar Connector (CALCONN). Запуск этих программ обычно автоматически «прописывается» в переменной ServerTasks в файле NOTES.INI сервера, когда вы устанавливаете сервер Domino.

Пользователь разрешает использование информации о своем свободном времени в документе Calendar Profile его почтового ящика.

Preferences

Mail | Calendar & To Do | Access & Delegation

Basics | Display | Scheduling | Alarms | To Do | Autoprocess | Colors

Your Availability

Specify which days and at what times you are available for meetings. When someone schedules a meeting, they will be shown that you are only available during the specified times.

Day of Week	Time (for example, 09:00 - 12:00, 13:00 - 17:00, but not 17:00 - 05:00)
☐ Sunday	
☒ Monday	10:00 - 21:00
☒ Tuesday	10:00 - 18:30
☒ Wednesday	10:00 - 21:00
☒ Thursday	10:00 - 18:30
☒ Friday	10:00 - 21:00
☐ Saturday	

Time Zone: Local time

When Adding an Entry to Your Calendar

Check for conflicts with other entries:

- ☒ When adding appointments, accepting meetings, scheduling a new meeting
- ☐ Note a conflict if entry occurs outside available hours described above

For new meetings, the Scheduler initially shows:

- ☐ Schedule details for each participant
- ☒ Suggested best times for meeting

Рис. 451 Диапазоны рабочего времени

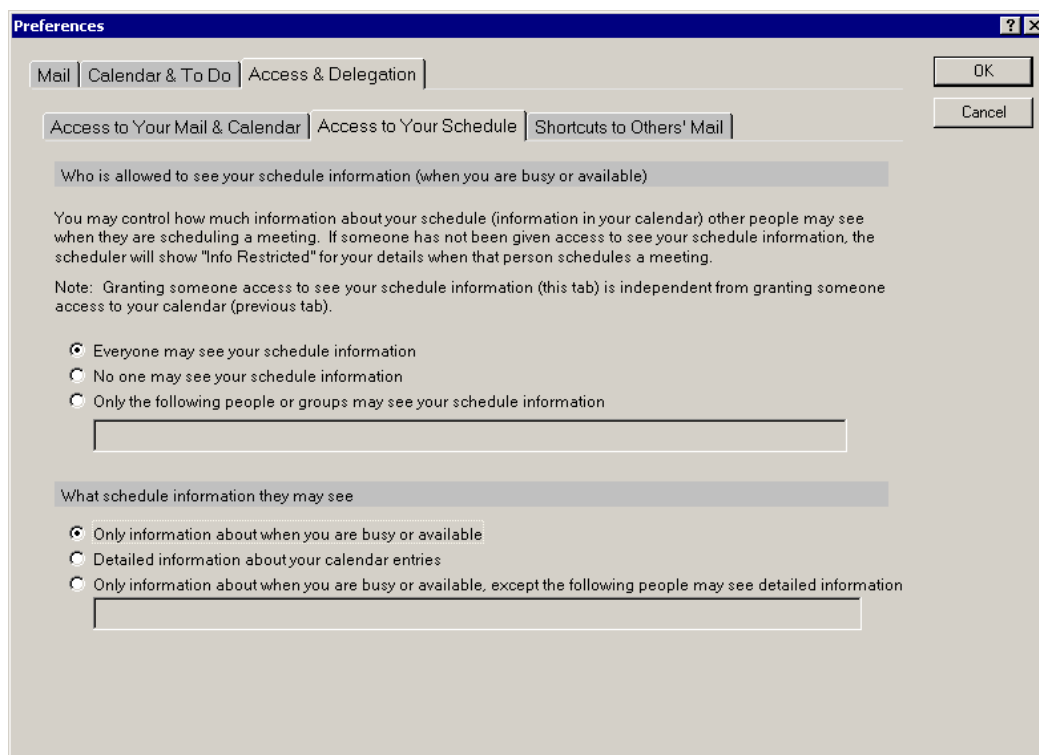


Рис. 452 Управление доступностью информации о свободном и занятом времени

1.56.1.1. 1.1.1.1. Программа Schedule Manager (SCHED)

При первом запуске программа Schedule Manager создает на «своем» сервере базу данных BUSYTIME.NSF (если сервер не член кластера) или CLUBUSY.NSF (если сервер в кластере, реплика на серверах кластера) и в этой базе создает «входы» для каждого пользователя, для которого этот сервер является почтовым сервером (поле MailServer в документе Person). Schedule Manager функционирует на сервере постоянно и каждый раз, когда пользователи вносят изменения в свои календари (создают calendar entries), он немедленно заносит эти изменения в свою базу BUSYTIME.NSF/CLUBUSY.NSF. Это гарантирует, что база BUSYTIME.NSF/CLUBUSY.NSF на каждом почтовом сервере постоянно находится в синхронном состоянии с информацией из календарей пользователей. Даже если вы удалите базу данных BUSYTIME.NSF/CLUBUSY.NSF, при следующем запуске Schedule Manager вновь создаст ее и заполнит соответствующей информацией из почтовых ящиков пользователей этого сервера. Обратите внимание, что только Schedule Manager имеет доступ к базе данных BUSYTIME.NSF/CLUBUSY.NSF.

Говоря более строго, программа Schedule Manager создает в базе BUSYTIME.NSF/CLUBUSY.NSF «входы» для каждой базы данных этого сервера, имеющей документ Calendar Profile, и заносит в базу BUSYTIME.NSF/CLUBUSY.NSF информацию о диапазонах свободного времени (рабочего времени) за исключением диапазонов занятого времени, указанных в имеющихся в базе calendar entries. Чаще всего документ Calendar Profile имеют почтовые ящики пользователей, а так же базы Resource Reservations.

Когда пользователь хочет пригласить одного или несколько человек на встречу и выбирает поиск свободного времени приглашаемых, к работе подключается Schedule Manager. В первую очередь он находит по Каталогу Domino домена местоположения почтовых серверов и почтовых ящиков приглашаемых лиц. Затем Schedule Manager ищет информацию о свободном времени каждого приглашаемого лица в базе BUSYTIME.NSF/CLUBUSY.NSF на почтовом сервере приглашаемого лица. Schedule Manager возвращает список дат и времен возможных встреч и количество «доступных» лиц.

1.56.1.2. 1.1.1.2. Программа Calendar Connector (CALCONN)

Всякий раз, когда пользователь, почтовый ящик которого находится на одном сервере, запрашивает информацию о свободном времени пользователя, почтовый ящик которого находится на другом сервере, к работе подключается программа Calendar Connector. Программа использует информацию из Каталога Domino, чтобы найти путь между почтовым сервером запрашивающего информацию пользователя и почтовым сервером пользователя, информацию о свободном времени которого запрашивается. Обратите внимание, что эти серверы могут находиться и в разных доменах Notes. Найдя путь и установив соединение, программа Calendar Connector передает его системе учета свободного времени необходимый запрос, а «ответ» на этот запрос возвращает своей программе Schedule Manager.

1.56.1.3. 1.1.1.3. Пример выполнения запросов о свободном времени

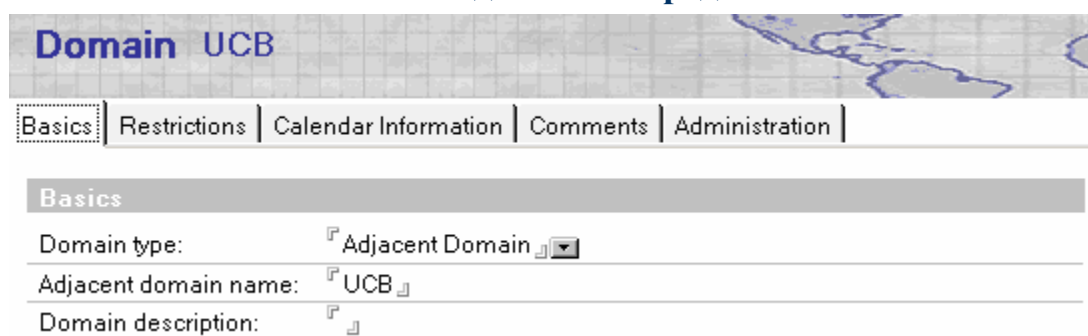
Предположим, что пользователь Иван Иванович, почтовый ящик которой находится на сервере А, хочет узнать, когда свободен пользователь Иван Никифорович, чтобы договориться с ним о встрече. При этом происходит примерно следующее.

- • Иван Иванович в своем почтовом ящике создает приглашение на встречу с Иваном Никифоровичем и нажимает кнопку поиска свободного времени.
- • Клиент Ивана Ивановича посылает запрос о свободном времени на его почтовый сервер (сервер А).
- • Система учета свободного времени ищет документ Person для Ивана Никифоровича в Каталоге Domino сервера А.
- • Если находит, то определяет из его поля MailServer имя почтового сервера Ивана Никифоровича, и затем выполняет одно из следующего.
 - • Если почтовый сервер Ивана Никифоровича тот же сервер А, система учета свободного времени ищет свободное время Ивана Никифоровича непосредственно в базе BUSYTIME.NSF/CLUBUSY.NSF на этом сервере и затем отображает полученную информацию Ивану Ивановичу.
 - • Если почтовым сервером Ивана Никифоровича является сервер В из того же домена, что и сервер А, система учета свободного времени на сервере А передает запрос на сервер В. Система учета свободного времени на сервере В находит необходимую информацию в базе BUSYTIME.NSF/CLUBUSY.NSF на сервере В, возвращает ее системе учета свободного времени на сервере А, и полученная информация отображается у Ивана Ивановича.
- • Но если поле CalendarDomain в документе Person Ивана Никифоровича не пусто и содержит имя домена, отличающееся от имени его почтового домена, это означает, что Иван Никифорович пользуется другой системой для планирования времени. Тогда система учета свободного времени направляет запрос о свободном времени Ивана Никифоровича в этот домен.
- • Если система учета свободного времени не находит документ Person для Ивана Никифоровича в Каталоге Domino сервера А, это означает, что почтовый ящик Ивана Никифоровича находится в другом домене. Если имя домена явно содержится в адресе Ивана Никифоровича или если иерархическое имя Ивана Никифоровича дает достаточно информации для определения имени его домена, система учета свободного времени ищет в общей адресной книге документ формы Domain для домена Ивана Никифоровича и затем выполняет одно из следующего.
 - • Если был найден документ формы Domain типа Adjacent Domain («Соседний домен»), система учета свободного времени обращается к информации из поля Calendar server name этого документа. Это поле может содержать имя сервера из домена Ивана Никифоровича, который «умеет» принимать запросы о свободном времени. Если поле не пусто, система учета свободного времени выполняет запрос на этот сервер. Если поле Calendar server name пусто, информация о свободном времени Ивана Никифоровича недоступна.

- Если был найден документ формы Domain типа Non-adjacent Domain («Несоседний домен»), система учета свободного времени обращается к информации из поля Route requests through calendar server этого документа. Это поле может содержать имя сервера из соседнего домена, который «умеет» передавать запросы о свободном времени на сервер в несоседнем домене Ивана Никифоровича. Если поле не пусто, система учета свободного времени передает запрос на этот сервер. Если поле Route requests through calendar server пусто, информация о свободном времени Ивана Никифоровича недоступна.
- Если система учета свободного времени находит документ формы Domain типа Foreign Domain («Чужой домен»), это знает, что Иван Никифорович пользуется другой системой для планирования времени, например, MS Exchange. Поле Calendar server name в документе Foreign Domain должно содержать имя сервера, который «умеет» принимать запросы о свободном времени, а поле CalendarSystem должно содержать тип используемого приложения для планирования времени. Система учета свободного времени выполняет запрос о свободном времени Ивана Никифоровича на указанный в поле CalendarServer сервер.
- Если система учета свободного времени не находит в Каталоге Domino никаких документов формы Domain для домена Ивана Никифоровича, информация о свободном времени Ивана Никифоровича недоступна.

Запрос о свободном времени будет также терпеть неудачу, если сервер Ивана Никифоровича или один из серверов «в цепочке» не функционирует.

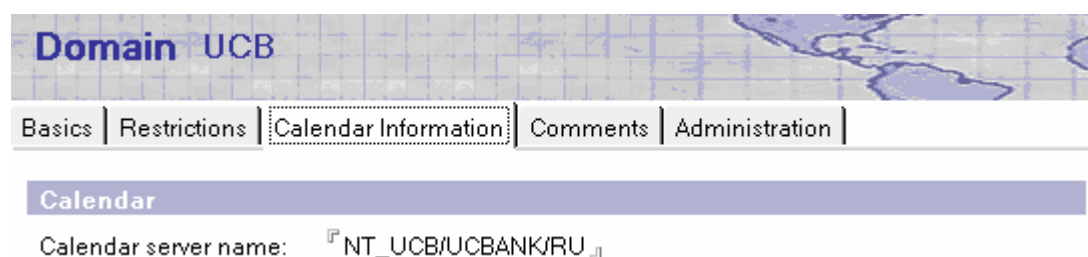
1.56.2. 1.1.2. Конфигурирование программы CALCONN в многодоменной среде



The screenshot shows the 'Domain UCB' configuration window with the 'Basics' tab selected. The 'Domain type' is set to 'Adjacent Domain'. The 'Adjacent domain name' is 'UCB'. The 'Domain description' is empty.

Domain UCB	
Basics	Restrictions Calendar Information Comments Administration
Basics	
Domain type:	Adjacent Domain
Adjacent domain name:	UCB
Domain description:	

Рис. 453 Соседний домен



The screenshot shows the 'Domain UCB' configuration window with the 'Calendar Information' tab selected. The 'Calendar server name' is 'NT_UCB/UCBANK/RU'.

Domain UCB	
Basics	Restrictions Calendar Information Comments Administration
Calendar	
Calendar server name:	NT_UCB/UCBANK/RU

Рис. 454 Сервер, на который передается запрос

Domain ACK

Basics | Restrictions | Calendar Information | Comments | Administration

Basics

Domain type: Non-adjacent Domain

Mail sent to domain: ACK

Route through domain: SunFire

Domain description:

Рис. 455 Несоседний домен

Domain ACK

Basics | Restrictions | Calendar Information | Comments | Administration

Calendar

Route requests through calendar server: Gateway/SunFire/RU

Рис. 456 Сервер, через который передается запрос

Конфигурирование других систем планирования времени осуществляется посредством документа Domain типа Foreign Domain. В полях Calendar server name и Calendar system выбирается имя сервера Domino и тип «чужой» системы планирования времени. Подробнее о поддержке таких систем в R6 лучше узнать поиском в базе знаний (обратите внимание на документ [7003551](#)).

1.56.3. 1.1.3. Создание базы Resource Reservations и сопутствующие операции

На сервере создается база Resource Reservations по шаблону Resource Reservations (6) (RESRC60.NTF). В базе создаются документ Site Profile и для него документы Resource. Создание документов Resource влечет появление запросов Add Resource программе ADMINP для создания соответствующих документов в Каталоге Domino. Изменять или удалять документы Resource необходимо в этой же базе, поскольку это тоже влечет создание запросов Modify Resource или Delete Resource программе ADMINP для изменения или удаления соответствующих документов в Каталоге Domino. Запрос на удаление ресурса в базе ADMIN4.NSF требует подтверждения администратором.

Site

Site name: ИнтерТраст

Domain name: InterTrustCorp

Resource Reservation server: InterTrust/InterTrustCorp/SU

Resource Reservation filename: MAILResRes01.nsf

Рис. 457 Site Profile

Resource

Type	Resource Information	Owner Options	Availability Settings

Resource type: ☒ Room
☐ Other

Other comments:
 『 』

Рис. 458 Тип ресурса

Resource

Type	Resource Information	Owner Options	Availability Settings

Name: Комната для переговоров/ИнтерТраст
 Site: ИнтерТраст
 Capacity: 『10』
 Description: 『 』

Other comments:
 『 』

Рис. 459 Room («помещение») имеет Capacity («вместимость»), Other – не имеет...

Resource

Type	Resource Information	Owner Options	Availability Settings

Ownership type: ☒ -None-
☐ Only owner can book resource
☐ Only select list of people can book resource
☐ Only select list of people can book resource via autoprocessing - all others require owner approval
☐ Temporarily disable reservations

Other comments:
 『 』

Рис. 460 Тип «владения» задает «политику» резервирования ресурса

Resource

Type	Resource Information	Owner Options	Availability Settings

☒ Sunday: 『09:00 - 17:00』
☒ Monday: 『09:00 - 19:00』
☒ Tuesday: 『09:00 - 19:00』
☒ Wednesday: 『09:00 - 19:00』
☒ Thursday: 『09:00 - 19:00』
☒ Friday: 『09:00 - 19:00』
☐ Saturday:

Other comments:
 『 』

Рис. 461

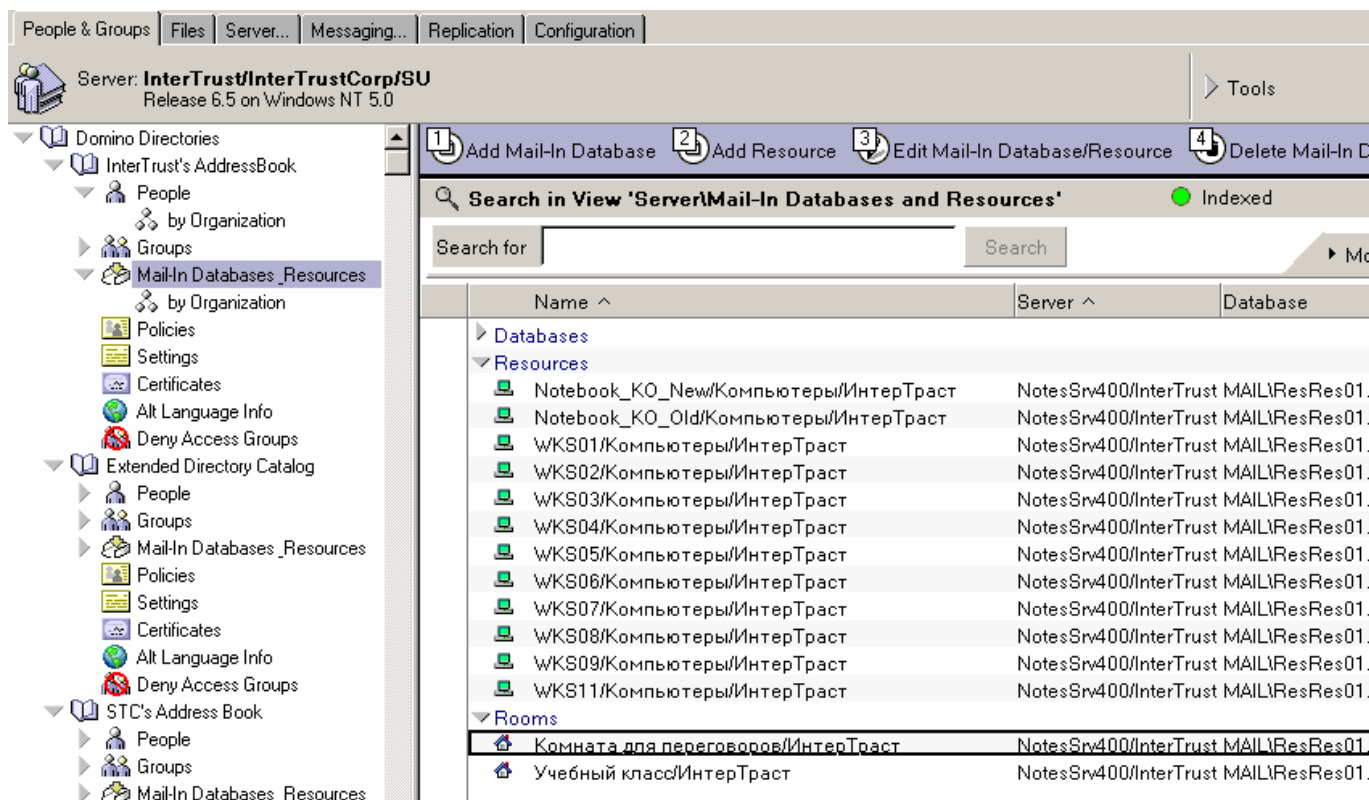


Рис. 462 Ресурсы в каталоге Domino созданы Adminp

1.56.4. 1.1.4. Поиск и устранение неисправностей

Command	Result
Tell Sched Stats	Displays totals of reservations and appointments in the free time database.
Tell Sched Show <i>username</i>	Displays the specified user's schedule on the server console. Use this command to investigate problems in the free time database.
Tell Sched Validate	Immediately validates a free time database on a server. Validation occurs by default at 2 AM; however, you can use this command to force it to occur sooner. Another way to force validation is to stop and restart the Schedule Manager. Validation can take some time. You must issue this command at all servers where mail files have been removed and/or added to ensure that old free time information is removed and new free time information is added to the free time database on the server. Don't use this command when you add a new user. The Administration process creates Person documents for users in the Domino Directory before creating their mail file on their mail server. Schedule Manager watches for database creations and automatically picks up new users' mail files.
Tell Sched Validate <i>username</i>	Validates the information for the specified user. This command is faster than using the Tell Sched Validate command because it allows you to validate individual users, rather than validating all of the data on a server.
Tell Sched Quit	Stops the Schedule Manager task on a server.

Пересоздание баз BUSYTIME.NSF/CLUBUSY.NSF

- На сервере или всех серверах кластера остановить программы
- tell sched q
- tell calconn q

dbcache flush

- ● На сервере или всех серверах кластера переименовать или удалить базы BUSYTIME.NSF/CLUBUSY.NSF
- ● На сервере или всех серверах кластера запустить программы
load sched
load calconn

Sched_Purge_Interval=*number of days*. Specifies how many days prior to the current day to keep busytime data. A value of 0 means data is never purged. Default: 7.

1.57. 1.1. Программа Database Compactor (COMPACT)

1.57.1. 1.1.1. Назначение

Основное назначение – устранение из баз неиспользуемого пространства. Однако есть множество других «мелких» функций...

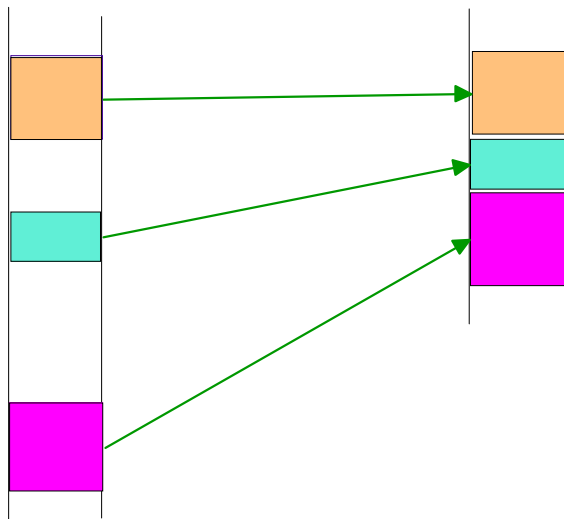


Рис. 463 Алгоритм уплотнения «копированием» в R4/5/6

Уплотнение баз формата R5/6 происходит:

- • «по месту» - не требуется дополнительного дискового пространства
- • On-line - во время уплотнения базы с ней могут работать пользователи и серверы

Когда неиспользуемое пространство в базе «осталось в конце файла», оно может быть возвращено файловой системе. В результате время уплотнения значительно (в несколько раз) сокращается.

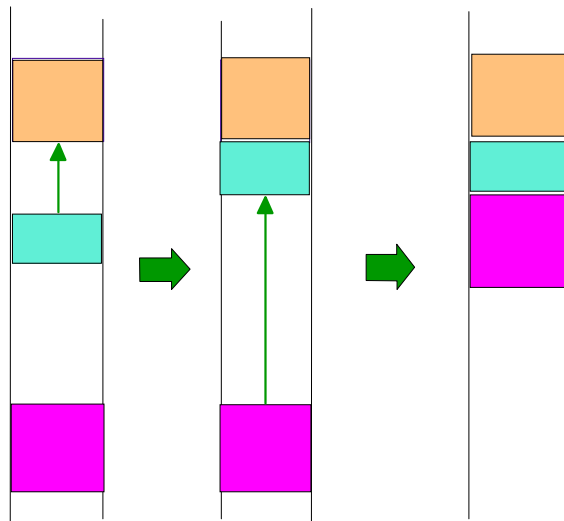


Рис. 464 Алгоритм уплотнения «на месте» в R5/6

1.57.2. 1.1.2. Ключи

Compact - Basics

Option	Command-line equivalent	Description
Compact only this database or folder (To specify databases to	<i>database path</i> Specify any additional options after the	To compact a database in the Domino data folder, enter the file name, for example SALES.NSF. To

compact using the Files tab, select the databases in the files pane.)	database path.	compact databases in a folder within the data folder, specify the database path relative to the data folder. For example, to compact all databases in the folder DATA\SALES, specify SALES. If you choose "Compact all databases" (or don't specify a database path at the command line) Compact compacts all databases in the data folder and in folders within the data folder.

Compact - Options

Option	Command-line equivalent	Description
Compact database only if unused space is greater than <i>x</i> percent	-S <i>percent</i>	Compacts all databases with a specified percent of unused space. For example, if you specify 10, databases with 10% or more recorded unused space are compacted. Note that the unused space calculation is not always a reliable measure of unused space.
Discard any built view indexes	-D	Discards built view indexes. Use this option to compact databases just before you store them on tape, for example. Does copy-style compacting.
Keep or revert database to previous format	-R	Compacts databases without converting to the current release file format of the server that stores the databases or reverts databases in the current release file format to the previous release file format. For example, on Domino 6 servers, this option compacts Domino 5 databases without converting them to the Domino 6 file format and converts Domino 6 databases to the Domino 5 file format. This option uses copy-style compacting.

Compact - Style

Option	Command-line equivalent	Description
In-place (recommended)	-b	Uses in-place compacting and recovers unused space without reducing the file size, unless there's a pending structural change to a database, in which case copy-style compacting occurs. This is the recommended method of compacting.
In-place with file size reduction	-B	Uses in-place compacting, recovers unused space and reduces file size, unless there's a pending structural change in which case copy-style

		compacting occurs. If you use transaction logging, do full database backups after compacting completes.
Copy-style	-c	Uses copy-style compacting. Use this option, for example, to solve database corruption problems.
Copy-style: Allow access while compacting	-L	Enables users to continue to access databases during compacting. If a user edits a database during compacting, compacting is canceled. This is useful only when copy-style compacting is done.
Copy-style: Ignore errors and proceed	-i	Enables compacting to continue even if it encounters errors such as document corruption. Only used for copy-style compacting.

Compact - Advanced

Option	Command-line equivalent	Description
Document table bitmap optimization: Off	-f	Disables "Document table bitmap optimization" database property. Does copy-style compacting.
Document table bitmap optimization: On	-F	Enables "Document table bitmap optimization" database property. Does copy-style compacting.
Don't support specialized response hierarchy: Off	-h	Disables "Don't support specialized response hierarchy" database property; in other words, support specialized response hierarchy. Does copy-style compacting.
Don't support specialized response hierarchy: On	-H	Enables "Don't support specialized response hierarchy" database property; in other words, do not support specialized response hierarchy. Does copy-style compacting.
Enable transaction logging: Off	-t	Disables transaction logging.
Enable transaction logging: On	-T	Enables transaction logging.
Don't maintain unread marks: Off	-u	Disables "Don't maintain unread marks" database property; in other words, maintain unread marks.
Don't maintain unread marks: On	-U	Enables "Don't maintain unread marks" database property; in other words, do not maintain unread marks.

Compact - Archive

Option	Command-line equivalent	Description
Archive only	-A	Archives and deletes documents from a database without compacting the database.
Archive and then compact	-a	Archives and deletes documents from a database and then compacts the database.
Delete and then archive	-j	Deletes documents from a

		database and then compacts the database.

По заданному в файле списку баз

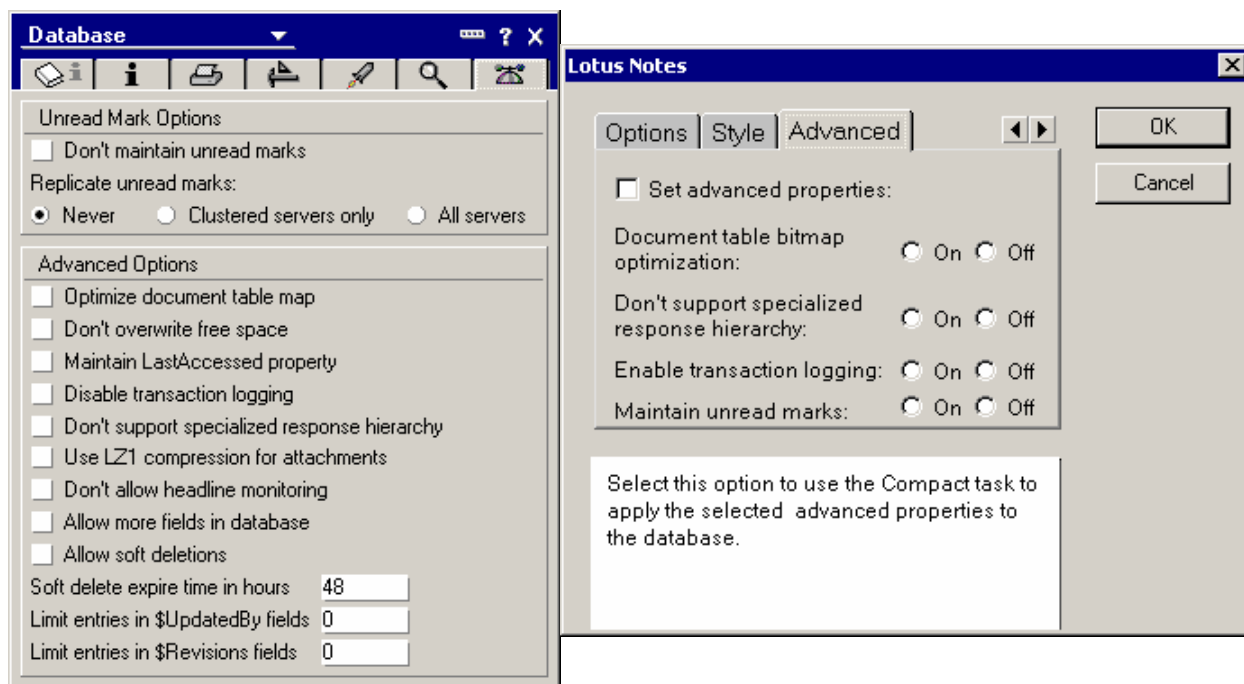
Список баз и каталогов заносится в текстовый файл с расширением .IND.

load fixup filename.ind

load updall filename.ind

load compact filename.ind

1.57.3. 1.1.3. Свойства базы данных на закладке Advanced и связь некоторых из них с программой COMPACT



Property	Tab	To optimize performance/size	Improves database performance?	Reduces database size?
Allow use of stored forms in this database	Basics	Deselect option	Yes	Yes
Display images after loading	Basics	Select option	Yes	No
Don't maintain unread marks	Advanced	Select option	Yes	Yes
Document table bitmap optimization	Advanced	Select option	Yes	No
Don't overwrite free space	Advanced	Select option	Yes	No
Maintain LastAccessed property	Advanced	Deselect option	Yes	No
Don't support specialized response hierarchy	Advanced	Select the option	Yes	Slightly
Don't allow headline monitoring	Advanced	Select the option	Prevents performance degradation	No
Limit entries in \$UpdatedBy fields	Advanced	Select the option and specify the number of entries \$UpdatedBy fields can contain	Yes	Yes
Limit entries in \$Revisions	Advanced	Select the option	Yes	Yes

fields		and specify a limit on the number of entries \$Revisions fields can contain. The suggested limit is 10 entries.		

1.57.3.1. 1.1.3.1. Optimize Document Table map

Очень значительно ускоряет обновление или перестройку индексов видов в базе, имеющей много документов и много «маленьких» видов (подобно КATALOGу Domino):

- • Формула отбора вида должна содержать & Form="xxx"
- • Ссылки на документы одной формы «сначала помещаются» в отдельные коллекции
- • Индексы видов строятся и обновляются по этим коллекциям, а не по коллекции из всех документов в базе. Поэтому при обновлении или перестроении индекса вида индексер оперирует документами из одной таблицы, а не из всей базы
- • После выбора свойства необходим Compact -C (копированием)

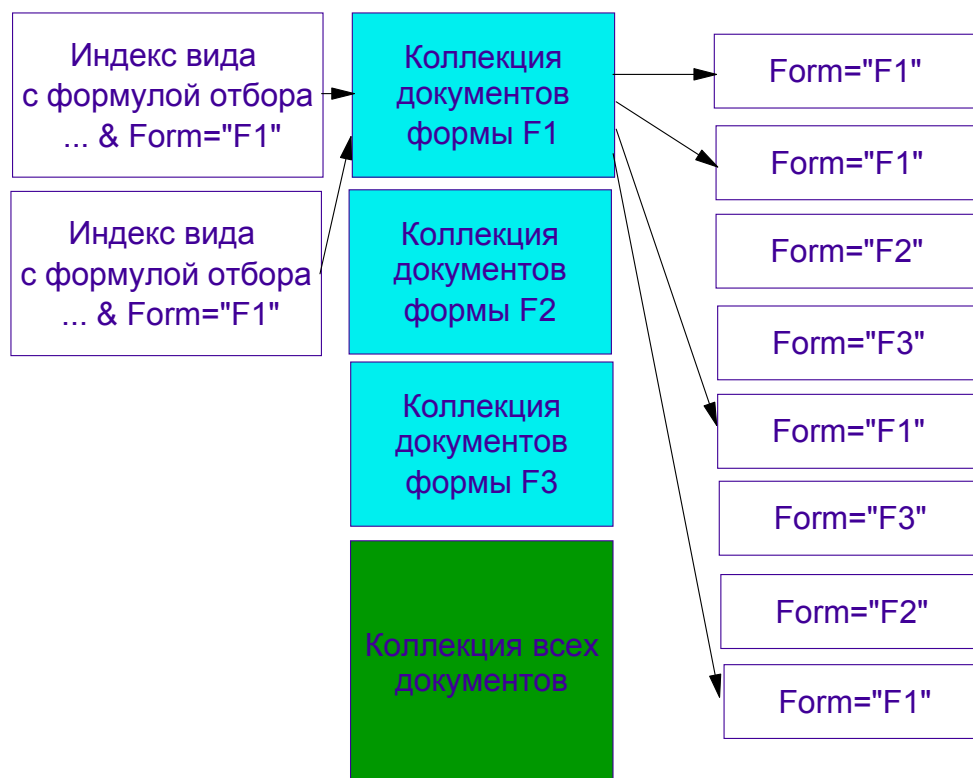


Рис. 465 Иллюстрация к свойству Optimize Document Table map

1.57.3.2. 1.1.3.2. Автоматическое архивирование баз сервером

Необходимо запускать задачу Compact по расписанию с нужным ключом архивирования...

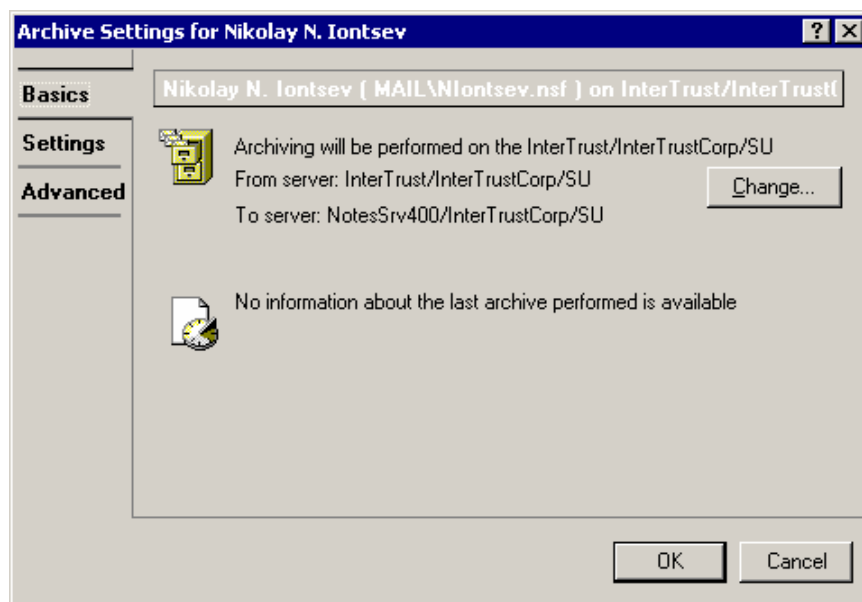


Рис. 466 Параметры архивирования базы, закладка Basics

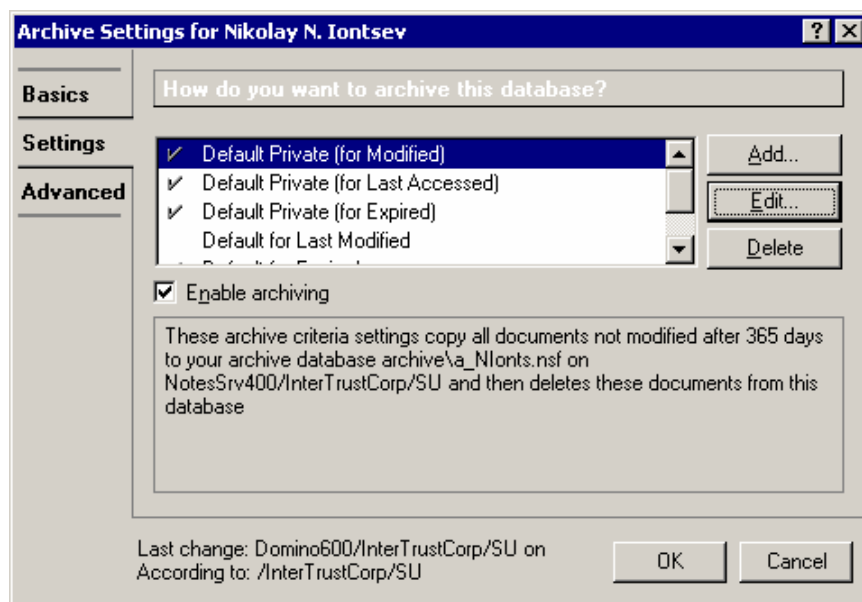


Рис. 467 Параметры архивирования базы, закладка Settings

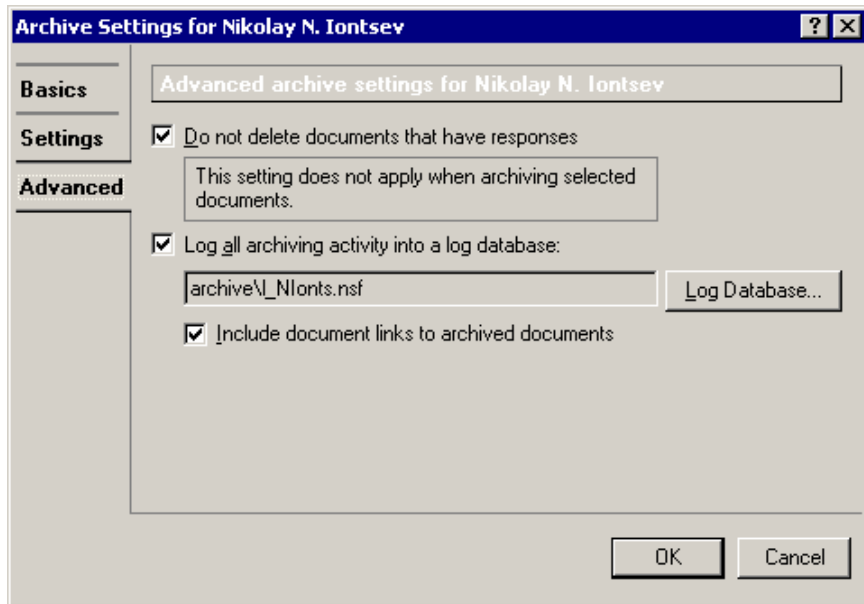


Рис. 468 Параметры архивирования базы, закладка Advanced

1.58. 1.1. Подсистема поддержки индексов видов и индексов полнотекстового поиска баз (NIF Subsystem, Full-Text services, Update, UPDALL, CHRONOS)

1.58.1. 1.1.1. Индексы видов и индексы полнотекстового поиска баз

Индекс вида (не путайте с индексом полнотекстового поиска) хранится в самой базе и необходим для того, чтобы клиент Notes мог оперативно предъявлять пользователю содержимое вида - оно формируется на основе индекса вида в базе.

Виду, как элементу дизайна (документ специального типа (view note), содержащий название вида, формулу отбора документов, набор колонок с формулами вычисления значений, способами сортировки, внешним оформлением и т.п.), в файле базы соответствует объект, называемый **индексом вида**. Индекс вида является коллекцией, содержащей минимум три различных индекса:

- индекс, отсортированный по UNID;
- индекс, отсортированный в соответствии с отношениями parent-child документов;
- индекс, отсортированный согласно его элементу дизайна (как определил в колонках разработчик вида). Если были выбраны альтернативные сортировки, таких индексов может быть несколько.

Для хранения индекса используется структура, называемая B-Tree Structure («двоичное дерево»). Присущие этому алгоритмы обеспечивают быстрый поиск, добавление и удаление «строк вида». Однако по мере проведения многих операций добавления и удаления «двоичное дерево» имеет тенденцию становиться несбалансированным, что уменьшает эффективность работы с индексом.

Индекс полнотекстового поиска хранится отдельно от базы в каталоге <имя_базы>.FT. Индекс полнотекстового поиска необходим, чтобы находить в базе документы с указанными в запросе полнотекстового поиска словами.

Индексы видов и индексы полнотекстового поиска не реплицируются – в реплике на каждом сервере они создаются заново, если это необходимо.

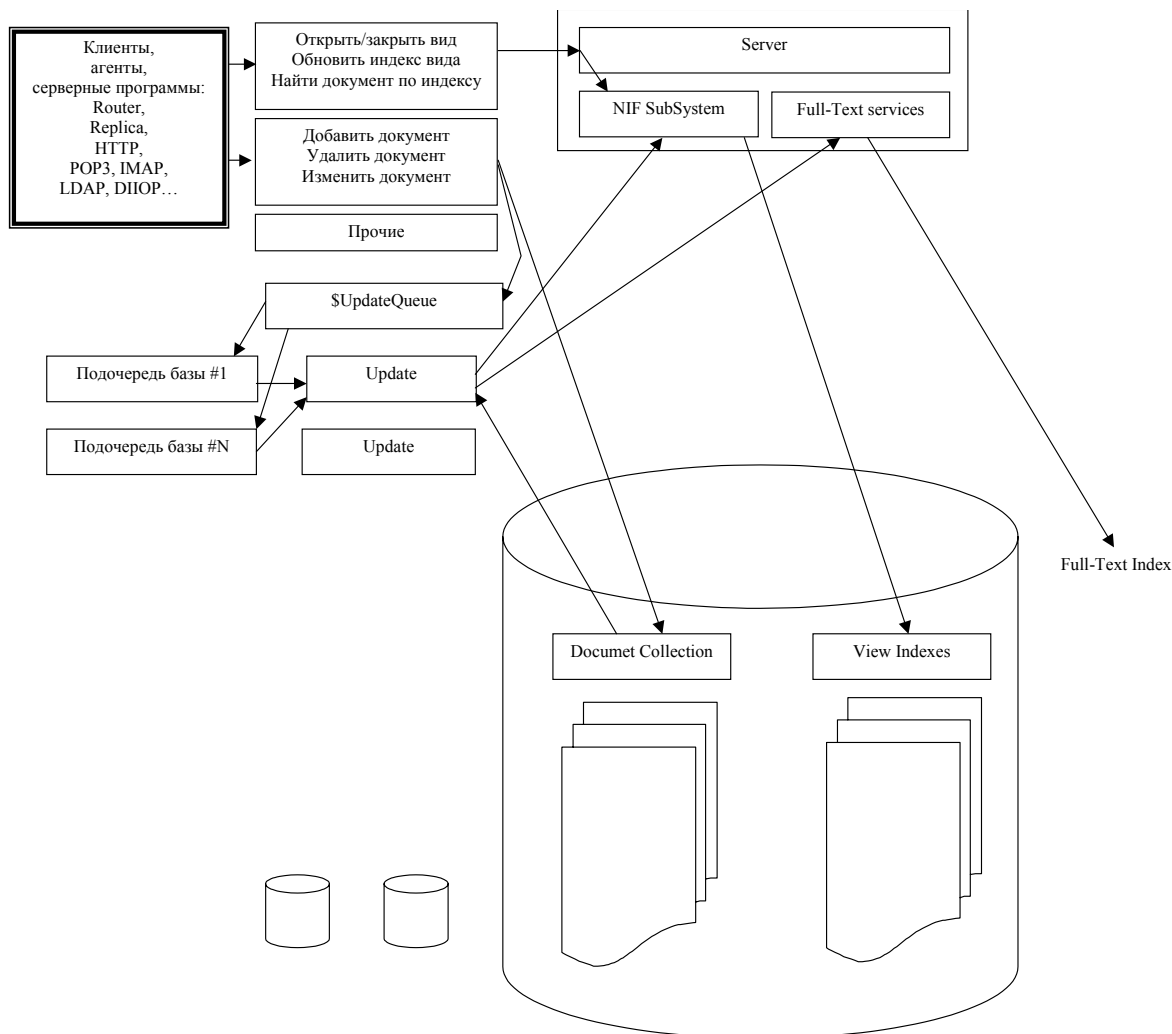


Рис. 469

1.58.2. 1.1.2. Notes Index Facility (NIF) и Full-Text services

Notes Index Facility (NIF) представляет собой множество функций, позволяющих серверу Domino поддерживать информацию из документов (data notes) актуальной в индексах видов. В частности, операции:

- • открыть/закрыть вид
- • обновить индекс вида
- • найти документ по индексу

целиком выполняются NIF. Большинство этих операций выполняется NIF, когда пользователи открывают и закрывают базы данных. Только NIF (а не программа Update) обновляет индексы видов в базе, когда пользователь переключается между видами. Например, если пользователь, находясь в одном виде, изменяет документ, затем переключается на другой вид и быстро возвращается в исходный вид, он уже «видит в виде» выполненные им изменения. Это объясняется как раз тем, что NIF (а не программа Update) уже успела обновить индекс этого вида. Можно остановить на сервере все программы Update, однако NIF, как подсистема самого сервера, будет продолжать поддержку и обновление индексов видов по запросам пользователей. Аналогичное будет происходить и по таким же запросам, исходящим от других программ сервера, в частности, от выполняемых сервером агентов.

У вида есть два свойства, которые связаны напрямую с обновлением и удалением его индексов: Refresh – способ обновления индекса и Discard – способ удаления индекса.

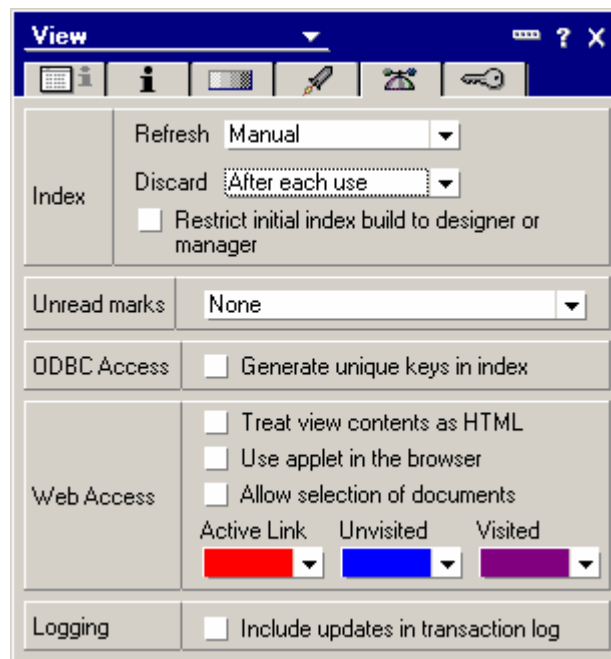


Рис. 470 Индекс такого вида обновляется только NIF (не Update).

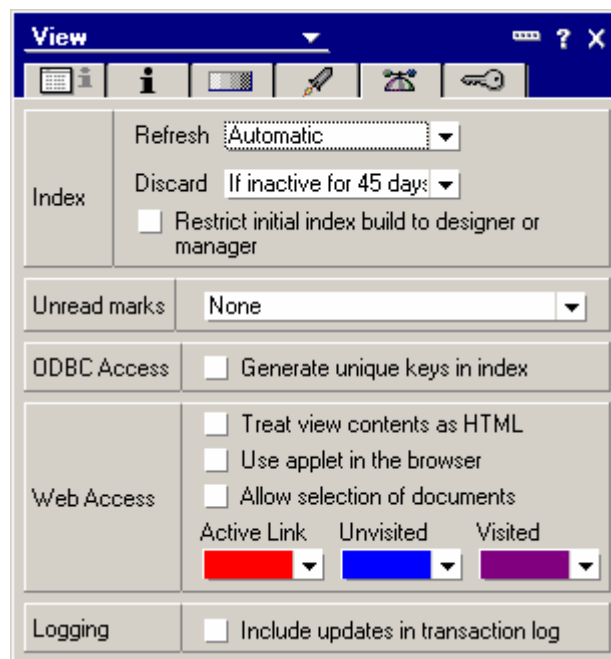


Рис. 471 Однако индекс такого вида должен обновляться сервером (программой Update) даже тогда, когда ни один пользователь не работает с ним (через NIF)

NIF использует область памяти для кэширования индексов видов, называемую NSF Buffer Pool. Пул содержит объекты, называемые страницами (Pages). Размер страницы 4 Кбайта. Обмен информацией из индекса вида между клиентом и сервером осуществляется как раз страницами. По мере того, как пользователь прокручивает вид, сервер подкачивает информацию из индекса вида в кэш и постранично передает клиенту. По умолчанию пул занимает примерно 1/4 - 3/8 оперативной памяти компьютера сервера. Прямое управление размером пула выполняется параметром NSF_BUFFER_POOL_SIZE (в байтах) или NSF_BUFFER_POOL_SIZE_MB (в Мб). Косвенное управление может осуществляться параметром PercentAvailSysResources. Будьте осторожны с этими параметрами...

Имеется еще пул с «созвучным» названием - NIF Pool. Полное назначение его неизвестно. По крайней мере, один из вариантов его использования – в него сервер при

старте загружает индекс вида (\$Users), чтобы более быстро выполнять поиск имен, не используя NIF. Прямое отношения к рассматриваемой теме этот пул не имеет.

Full-Text services представляют собой набор функций, отвечающих за создание, поддержку и удаление индексов полнотекстового поиска локальных баз и осуществление такого поиска по запросам клиентов и серверных программ.

1.58.3. 1.1.3. Серверная программа Update (Indexer) - оперативная поддержка индексов на сервере

Серверная программа Update (на консоли представлена под именем Indexer) по умолчанию включена в файл NOTES.INI в список ServerTasks, а потому загружается автоматически при запуске сервера.

Программа Update осуществляет поддержку индексов видов, имеющих свойство Refresh = Auto...:

- **Automatic** – индекс должен быть создан автоматически, т.е. Update, и обновляться постоянно (по событиям изменения документов в базе), даже если пользователи не открывают его;
- **Auto, after first use** – индекс должен быть создан только при первом его использовании пользователем, но после этого должен обновляться Update постоянно (по событиям изменения документов в базе), даже если пользователи более не открывают его;
- **Auto, at most every** – индекс должен быть создан автоматически, т.е. Update, и должен обновляться, даже если пользователи не открывают его, но с заданной частотой, а не по событиям изменения документов в базе.

Update обновляет соответствующие индексы видов в базе данных, когда пользователь или серверная программа, например Replicator, создают, модифицируют или удаляют документы в этой базе. Когда необходимо, Update создает индексы видов. Кроме прочего Update создает индексы полнотекстового поиска и модифицирует их, если они имеют частоту обновления Immediate.

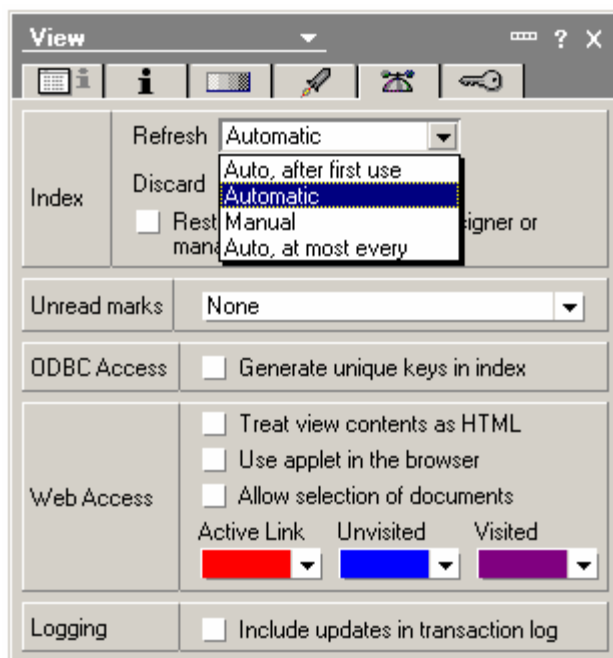


Рис. 472 Все варианты индексов с Auto... - «клиенты» Update

Сервер Domino поддерживает очередь запросов на изменение индексов видов и индексов полнотекстового поиска в базах данных - \$UpdateQueue. Размер очереди – 500 элементов (запросов). Запросы в эту очередь поступают от различных серверных

программ, которые создают, модифицируют или удаляют документы в базах. Появлению запроса в очереди предшествует событие создания, модификации или удаления документа в базе, фиксируемое изменением поля DATAMODIFIEDTIME в заголовке базы. В запросе в очереди \$UpdateQueue содержится только полный путь к базе. Программа Update опрашивает эту очередь каждые 5 секунд. Как только она находит в очереди запрос, она извлекает его и помещает во внутреннюю подочередь запросов к конкретной базе.

Запросы из подочереды к конкретной базе выполняются не сразу, а только по прошествии Update_Suppression_Time=minutes (по умолчанию 5) минут после появления первого запроса в подочереды. При этом выполняется не первый запрос из подочереды, а, «за один вызов», сразу все накопившиеся в ней запросы.

Выполнение запроса прежде всего сводится к выявлению тех индексов видов, которые Update должна обновить. Очевидно, индексы видов со свойством Refresh=Manual, а так же несуществующие индексы видов (кроме несуществующих, но еще не удаленных, со свойством Refresh=Automatic) из рассмотрения сразу исключаются. Среди оставшихся индексов видов выявляются те, для которых время последней модификации индекса (поле MODIFIEDTIME в заголовке индекса) меньше времени последней модификации базы (поле DATAMODIFIEDTIME в заголовке базы). Для таких индексов видов вызовом функций из NIF (очевидно, при этом затраты процессорного времени «списываются» на Update) и выполняется обновление. Обновление индекса вида (в контексте Update) означает просмотр коллекции всех документов в базе и текущего индекса вида и:

- • для тех документов, которых нет в индексе вида, но согласно формуле отбора они должны быть там – добавление в индекс;
- • для тех документов, которые еще есть в индексе вида, но уже удалены из базы – удаление из индекса;
- • для тех документов, которые изменились в базе, но это изменение не зафиксировано в индексе – модификация в индексе.

Встречаются случаи, когда в индекс вида вносится только немного (значительно меньше, чем документов в виде) изменений – например, вид со статическими значениями в формулах колонок, а в базе изменилось несколько документов.

Однако встречаются и случаи, когда в индекс вида при обновлении полностью заменяется – например, вид с использованием «динамического» (функция @Now...) значения в колонке.

Если база, в которой выполнено обновление индексов видов, имеет еще и индекс полнотекстового поиска с частотой обновления Immediate («непосредственно при создании, удалении или модификации документа»), помимо изменения индексов видов программа Update обновляет индекс полнотекстового поиска, осуществляя вызов функций из Full-Text services (очевидно, при этом затраты процессорного времени тоже «списываются» на Update).

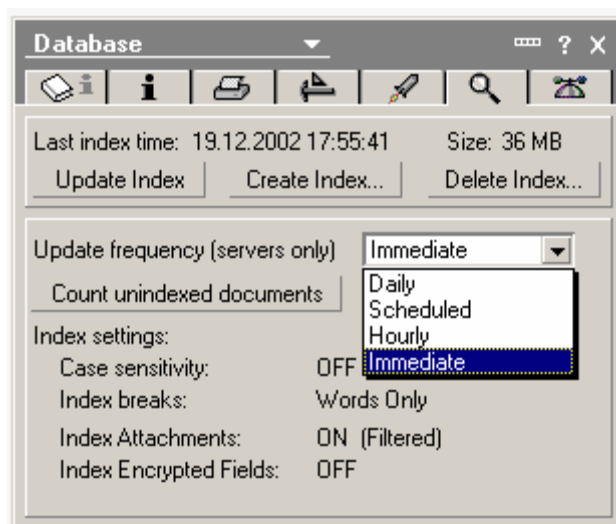


Рис. 473 Частота обновления индекса полнотекстового поиска базы

В целях сохранения дискового пространства на сервере программа Update также занимается «инициализацией удаления» индексов длительно неиспользуемых видов. Если разработчик базы данных не указал для вида опцию, касающуюся частоты удаления его индекса, т.е. в поле с меткой **Discard index:** выбрано значение по умолчанию **If inactive for 45 days** - «если не использовался 45 дней» (в предшествующих версиях было **Never** - «никогда»), то программа Update «поставит» индекс этого вида «как подлежащий удалению», если он никем не использовался в течение 45 дней.

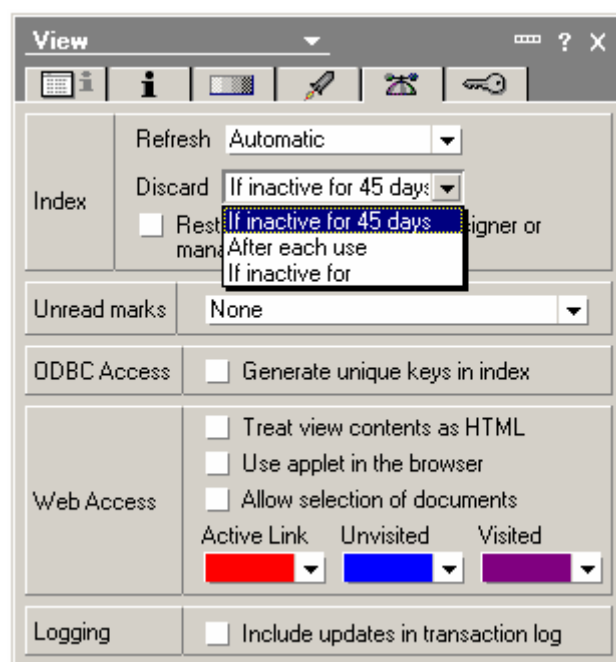


Рис. 474 Выбор частоты удаления индекса вида в окне свойств вида

Можно использовать в NOTES.INI переменную **Default_Index_Lifetime_Days=<число дней>**, чтобы изменить «время жизни индексов видов по умолчанию». Если же для вида была определена частота удаления индекса (**If inactive for x days** – «если не использовался в течении x дней»), программа Update будет удалять индекс с заданной частотой.

Можно запускать на сервере сразу несколько программ Update, устанавливая в NOTES.INI переменную **Updaters** (число программ Update, запускаемых при старте сервера) или вручную с консоли (командой Load Update). Это может ускорить обновление индексов, но при условии, что компьютер сервера имеет соответствующий запас

производительности. Общая рекомендация состоит в запуске «по Update на процессор». Два разных Update могут одновременно обновлять разные индексы видов в одной базе, но никогда не могут одновременно обновлять один и тот же индекс вида. На консоли сервера иногда встречаются ситуации, когда согласно выдаче команды Show Task два Update одновременно обновляют один и тот же вид в одной базе. По информации из базы знаний такое означает лишь то, что один из Update «просто ждет на семафоре», пока другой не завершит обновление индекса. Отметим также, что команда консоли **Tell Update Quit** приводит к завершению сразу всех запущенных на сервере программ Update. Однако для того, чтобы автоматическое обновление индексов на сервере действительно происходило, серверу необходима хотя бы одна программа Update... Тем не менее, на способности пользователей открывать виды в базах останова всех Update не отразится – как отмечалось выше, пользователи работают через сам сервер и NIF...

Отметим параметр **View_Rebuild_Dir=D:\REBUILD** (не забудьте обратный слеш в конце). В этом каталоге Update и UpdAll создают свои временные файлы. Помещение этого каталога на «быстрый диск» (например, RAID с «чередованием») довольно значительно поднимает быстроедействие...

1.58.4. 1.1.4. Серверная программа Update All (UPDALL) - ежедневное обслуживание индексов на сервере

Серверная программа Updall запускается на сервере по умолчанию в 2 часа ночи (это задается в NOTES.INI переменной ServerTasksAt2) и модифицирует во всех базах на этом сервере все существующие индексы видов и все индексы полнотекстового поиска. Чтобы запретить программе Updall автоматически модифицировать индексы полнотекстового поиска, можно использовать переменную **Update_No_Fulltext** в NOTES.INI.

Есть неподтвержденное подозрение, что для индексов видов UPDALL без ключей выполняет нечто похожее на балансировку двоичного дерева с освобождением неиспользуемых сегментов информации. Подозрение основано на том, что размеры индексов с утра меньше и работают индексы быстрее, тогда как к вечеру размер несколько увеличивается и уменьшается время поиска. Чтобы не полагаться на это подозрение, запускайте периодически UPDALL -R.

Если вы запускаете Updall вручную или посредством документа Program, вы можете дополнительно задавать аргументы, которые определяют, как программа работает. Формат команды для запуска UpdAll: **Load Updall [database] [аргументы]**. Аргументы могут быть следующими:

- • **-V** модифицирует индексы видов, к которым обращались по крайней мере раз, но не модифицирует индексы полнотекстового поиска
- • **-C** создает все до этого не существовавшие индексы видов и модифицирует индексы полнотекстового поиска
- • **-R** перестраивает заново все индексы видов, к которым обращались по крайней мере раз, и модифицирует индексы полнотекстового поиска. Но это может потребовать много времени, так что использовать аргумент -R целесообразно только при исправлении поврежденных индексов в базах
- • **-F** модифицирует индексы полнотекстового поиска, но не модифицирует индексы видов
- • **-X** перестраивает заново все индексы полнотекстового поиска
- • **-S** модифицирует индексы полнотекстового поиска, для которых назначена частота обновления Scheduled (по расписанию), Hourly (каждый час) и Immediate (непосредственно).
- • **-H** модифицирует индексы полнотекстового поиска с частотой обновления Hourly (каждый час)
- • **database -T viewtitle** модифицирует индекс вида viewtitle в базе database.

Вы можете использовать имя базы данных как дополнительный параметр, причем с опцией -T он всегда необходим. Например, команда **Load Updall SALES.NSF -R** перестраивает индексы видов и модифицирует индекс полнотекстового поиска только в базе данных SALES.NSF. Чтобы перестроить только один вид в базе, можно воспользоваться командой **Load Updall filename -R -T viewname**. Однако то же самое часто можно сделать и с клиента Notes:

- • выбрать вид, который нужно перестроить
- • нажать SHIFT+F9, чтобы перестроить только индекс этого вида, или CTRL+SHIFT+F9, чтобы перестроить индексы всех видов в базе.

Отметим, что у программы Updall есть еще два параметра (-A и -B). Они относятся к возможности полнотекстового поиска сразу по многим базам (не DomIdx).

Updall - Basic options

Option in Task - Start tool	Command-line option	Description
Index all databases	<i>databasepath</i>	"Only this database" updates only the specified database. To update a database in the Domino data folder, enter the file name, for example, SALES.NSF. To update databases in a folder within the data folder, specify the database path relative to the data folder, for example, DOC\README.NSF.
Index only this database or folder		"Index all databases" (or no database path) updates all databases on the server.
Update this view only	<i>database</i> <i>viewtitle</i>	-T Updates a specific view in a database. Use, for example, with -R to solve corruption problems.

Updall - Update options

Option in Task - Start tool	Command-line option	Description
Update: All built views	-V	Updates built views and does not update full-text indexes.
Update: Full text indexes	-F	Updates full-text indexes and does not update views.
Update: Full text indexes: Only those with frequency set to: Immediate	-H	Updates full-text indexes assigned "Immediate" as an update frequency.
Update: Full text indexes: Only those with frequency set to: Immediate or Hourly	-M	Updates full-text indexes assigned "Immediate" or "Hourly" as an update frequency.
Update: Full text indexes: Only those with frequency set to: Immediate or Hourly or Daily	-L	Updates full-text indexes assigned "Immediate," "Hourly," or "Daily" as an update frequency.

Updall - Rebuild options

Option in Task - Start tool	Command-line option	Description
Rebuild: Full-text indexes	-X	Rebuilds full-text indexes and does not rebuild

only		views. Use to rebuild full-text indexes that are corrupted.
Rebuild: All used views	-R	Rebuilds all used views. Using this option is resource-intensive, so use it as a last resort to solve corruption problems with a specific database.
Rebuild: Full-text indexes and additionally: All unused views	<i>database -C</i>	Rebuilds unused views and a full-text index in a database. Requires you to specify a database.

Updall - Search Site options

Option in Task - Start tool	Command-line option	Description
Update database configurations: Incremental	-A	Incrementally updates search-site database configurations for search site databases.
Update database configurations: Full	-B	Does a full update of search-site database configurations for search site databases.

1.58.5. 1.1.5. Серверная программа Chronos (CHRONOS)

В Notes/Domino R3 эта программа выполняла фоновых агентов в базах на сервере, а так же обновляла индексы полнотекстового поиска баз с частотой обновления hourly.

В Domino R4/5/6 агентов в базах выполняет Agent Manager (AMGR), а «за Chronos» осталась лишь функция обновлять индексы полнотекстового поиска с частотой Hourly. Запускает программу сервер каждый час, никаких настроек программа не требует. Просто не удивляйтесь фактам ее запуска и знайте, «кто» обновляет индексы полнотекстового поиска с частотой Hourly.

1.58.6. 1.1.6. Операция Files - Database-Manage Views

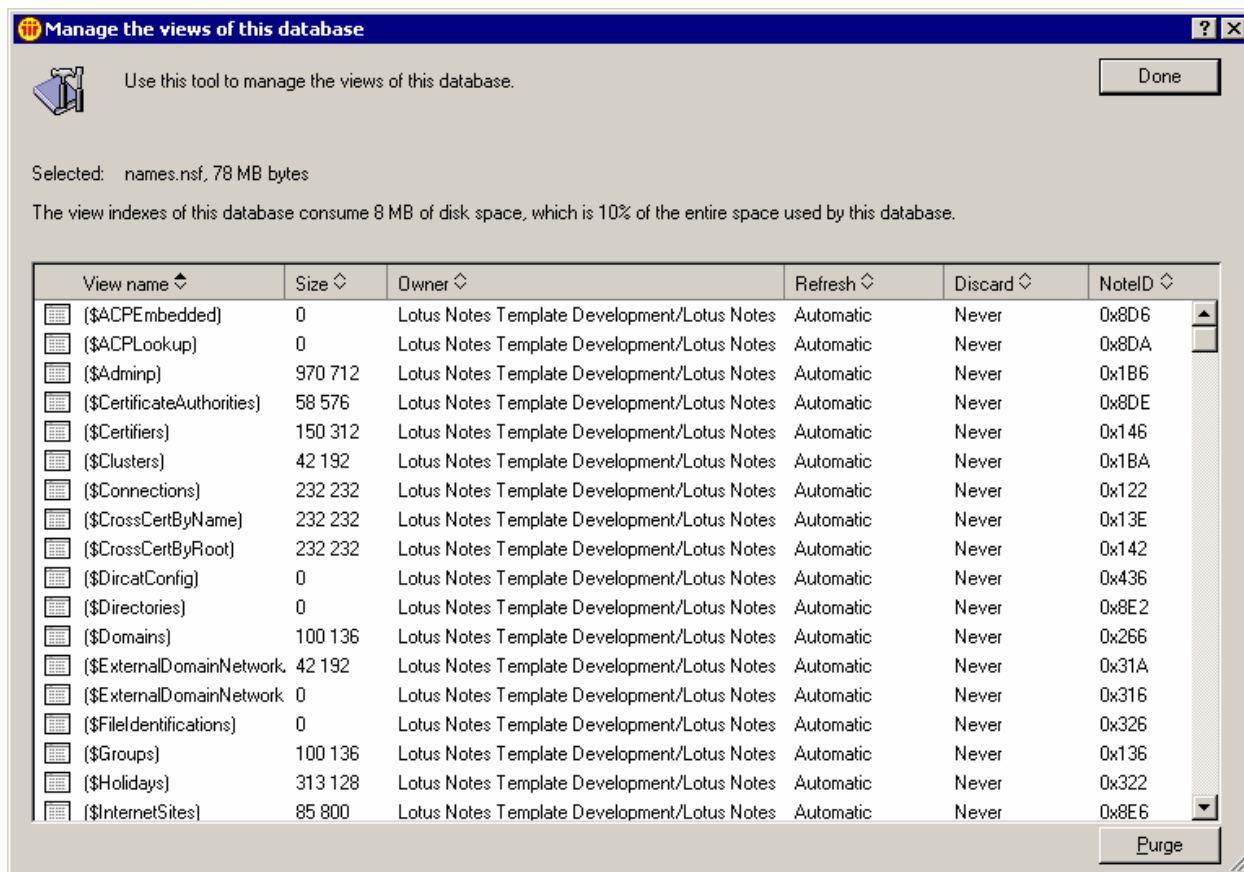


Рис. 475 Окно с размерами индексов видов. «Непостроенные» индексы имеют размер 0

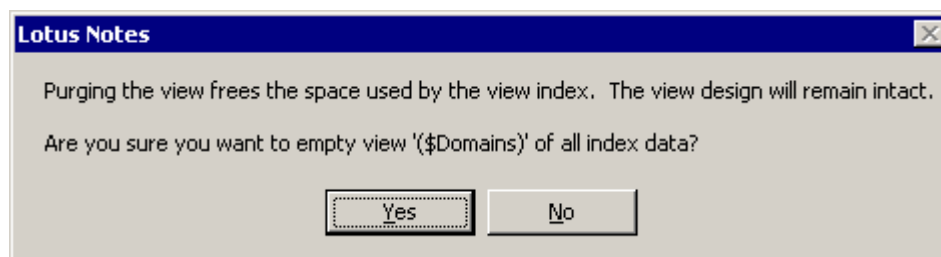


Рис. 476 Кнопкой Purge выполняется удаление индекса вида

1.58.7. 1.1.7. Причины, приводящие к повышенной нагрузке на NIF Subsystem, и мероприятия по снижению нагрузки

Причин обычно две:

- Отсутствие контроля над свойствами видов со стороны разработчика и администратора, вызванное непониманием принципов работы подсистемы
- Слабая производительность компьютера

Мероприятия по снижению нагрузки могут быть трех сортов:

- Если сильно загружен Update, включить протоколирование (LOG_UPDATE=2) и, наконец, разобраться, какие конкретно индексы видов создают нагрузку. Выставить для индексов «экономные» свойства, переделать виды, убрав «динамику», отказаться от видов вовсе. Подробности в документе 184780 (старая база знаний). Бывают случаи, что Update на конкретном виде постоянно загружает процессор процентов на 40-80. Обычно это происходит на виде, в формуле отбора которого, или, еще хуже, в функциях колонок, использованы «дата-временные» функции, а частота обновления выбрана Automatic. Индекс этого вида обновляется каждые 5 минут (Update_Suppression_Time=minutes, по умолчанию 5). При малом количестве документов одно обновление занимает меньше 5 минут, поэтому полной загрузки Update не наблюдается. С ростом количества документов наступает предел, когда одно обновление занимает ≥ 5 минут, что уже означает полную загрузку Update, и именно этот

момент обычно фиксируется администратором. Надо временно увеличить Update_Suppression_Time и «разобраться» с видом.

- • Если предыдущее не помогает, можно (очень осторожно!) увеличить NSF_BUFFER_POOL_SIZE . Однако согласно материалам IBM Lotus на индексах видов с большим количеством документов это поднимает производительность не более чем на 8-15%.
- • Тогда остается заменять «железо» и «разносить задачи» по нескольким серверам...

1.58.8. 1.1.8. Ссылки

Основным источником информации по теме служит база знаний:

- • Документ 7003075 (новая база знаний) - [The Indexer and Its Functionality](#)
- • Документ 184780 (старая база знаний) - [Domino Database Indexing and Performance: Getting Control of the Update Task](#)

1.59. 1.1. Программа Database Fixup (FIXUP) - анализ и устранение повреждений в базах

1.59.1. 1.1.1. Логика работы, аспекты применения, ключи

Серверная программа Database fixup проверяет находящиеся на сервере базы данных на наличие в них «поврежденных» индексов видов, папок и документов и удаляет те индексы видов, папки и документы, в которых были обнаружены повреждения.

Наиболее часто повреждение базы данных случается:

- при неправильном завершении операционной системы (аппаратная перезагрузка компьютера, сбой питания, крах операционной системы или иные неподходящие процедуры ее закрытия),
- при принудительном завершении («снятии») сервера Domino средствами операционной системы,
- из-за неправильной работы с базой данных из программы, использующей Notes API.

Во время своей работы сервер Domino открывает запрашиваемые пользователями базы данных и в течение некоторого времени поддерживает их в открытом состоянии. Некоторые системные базы данных, например, LOG.NSF, MAIL.BOX или NAMES.NSF, открываются при старте сервера и остаются в открытом состоянии до его завершения. При штатном завершении сервера (командой консоли Quit или Exit) последний «закроет» все открытые им базы данных. Однако при нештатном завершении сервера некоторые из баз могут остаться в незакрытом состоянии.

Когда вы снова запускаете сервер, он самостоятельно запускает программу FIXUP в фоновом режиме. Программа FIXUP прежде всего обрабатывает базу «Протокол работы сервера» (LOG.NSF), чтобы в нее можно было заносить информацию о возможных последующих обнаруженных повреждениях и выполненных «исправлениях». Затем программа FIXUP обрабатывает «незакрытые» базы данных. Для каждой «незакрытой» базы она:

- проверяет каждое поле в каждом документе на наличие повреждений;
- удаляет поврежденные документы, но так, что эти удаления не повлекут удалений соответствующих документов в других репликах данной базы.

Если программа FIXUP «не успеет» обработать «незакрытые» базы до того, как запустится сервер, а пользователи попытаются открыть такую базу, они получают сообщение «This database cannot be opened because a consistency check of it is in progress».

При старте сервера может быть запущено несколько параллельно работающих программ FIXUP, чтобы сократить общее время обработки поврежденных баз. По умолчанию при старте запускается до двух программ FIXUP в расчете на каждый имеющийся на сервере процессор. Максимальное количество одновременно запускаемых при старте сервера программ FIXUP может задаваться переменной **Fixup_Tasks** в NOTES.INI. Фактическое число выполненных программ обычно меньше заданного значения Fixup_Tasks. Например, если Fixup_Tasks = 4, но только одной базе данных имеются повреждения, выполнится только одна программа FIXUP.

Обратите внимание на следующие моменты. Во-первых, при автоматическом запуске программа FIXUP не выполняет проверку поврежденных индексов видов и папок в базах. Во-вторых, база данных, которая повреждена, но «корректно закрыта», вообще не обрабатывается при автоматическом запуске программы FIXUP.

В таких случаях администратору приходится запускать программу FIXUP «вручную». Поводом для этого может послужить получение пользователем сообщения о

повреждении базы, обнаружение пользователем некорректной информации в виде базы (невозможно открыть вид, в колонках вида «непонятные» символы, информация в документе и в виде не синхронна, в базе нет документов, представленных в виде) или обнаружение администратором соответствующие сообщения в базе «Протокол работы сервера» (LOG.NSF). Приведем некоторые сообщения, появляющиеся в LOG.NSF и свидетельствующие о наличии повреждений в базах:

- • Поврежденный документ
 - • «Document NT <document number> in database <database name> is damaged:»
 - • «Document is damaged or obsolete (unrecognized data type)»
 - • «Document is damaged or obsolete (unrecognized field)»
- • Некорректно (в «физическом» смысле) удаленный документ
 - • «Document NT <document number> in database <database name> has been deleted»
- • Поврежденный индекс вида
 - • «Page format is incorrect»
 - • «Invalid CNO vector - position == 0»
 - • «Container integrity has been lost - rebuild».

При запуске «вручную» FIXUP способна обрабатывать не только поврежденные документы, но и поврежденные индексы видов или папки.

FIXUP не может обрабатывать уже открытые базы данных, и базы данных не могут быть открыты, когда FIXUP «работает» на них. Учтите, что системные базы данных (например, LOG.NSF, MAIL.BOX или NAMES.NSF) при работе сервера всегда открыты.

При желании можно запускать программу FIXUP по расписанию. Общая рекомендация в этом случае - один раз в неделю в «не пиковые» часы.

Остается рассмотреть вопрос о последствиях применения программы FIXUP. Если программа удаляет поврежденный индекс вида, «ничего страшного» не происходит. Этот индекс вида будет построен сервером заново - при попытке пользователя открыть вид, «ночном» выполнении программы UPDALL или в иных ситуациях. Если же программа FIXUP удаляет поврежденный документ, этот документ «не восстановится автоматически». Для его восстановления необходимо иметь либо резервную копию базы, выполненную средствами операционной системы, либо реплику этой базы на другом сервере Domino. В первом случае придется со станции вручную перенести необходимые документы через буфер обмена из резервной копии в восстанавливаемую базу. Во втором случае поможет механизм репликаций. Программа FIXUP всегда удаляет поврежденный документ «без следов», так что при репликации он не влечет удаления соответствующего документа в реплике базы на другом сервере. Зато «нормальный» документ из реплики на другом сервере при репликации должен добавляться в восстанавливаемую реплику, как новый документ. Однако при этом возможны некоторые нюансы, связанные с логикой работы истории репликаций и поля CutOff Date.

Fixup options in Fixup tool and Task - Start tool	Command-line equivalent	Description
Fixup all databases Fixup only this database or folder	<i>databasepath</i> .	"Fixup only this database or folder" runs Fixup only on a specified database or all databases in a specified folder. To run Fixup on a database in the Domino data folder, enter the file name, for example SALES.NSF. To run Fixup on a database or databases in folders

		within the data folder, enter the path relative to the data folder. For example, to run Fixup on all databases in the DATA\SALES folder, specify SALES. "Fixup all databases" or no command line database path runs Fixup on all databases on the server. Note To specify databases or folders to run on using the Fixup tool, select the database(s) or folder(s). Имя_базы_или_каталога - необязательный параметр. Он определяет имя базы данных или каталога с базами, которые необходимо обработать. Если вы не указали базу данных или каталог, FIXUP обрабатывает все базы данных на сервере
Report all processed databases to log file	-L	Reports to the log file every database that Fixup opens and checks for corruption. Without this argument, Fixup logs only actual problems encountered. Требуется протоколировать информацию о каждой базе, обработанной FIXUP, даже если в базе отсутствуют повреждения. Без этого параметра FIXUP протоколирует только обнаруженные и «исправленные» ею повреждения.
Scan only since last fixup	-I	When you run Fixup on a specific database, Fixup checks only documents modified since Fixup last ran. Without this option, Fixup checks all documents. «Заставляет» программу FIXUP проверять только те документы, которые изменились с момента предшествующего запуска программы.
Scan all documents	-F	When you run Fixup on all databases, Fixup checks all documents in the databases. Without this option, Fixup checks only documents modified since it last ran. Note To specify this option using the Fixup tool, deselect "Scan only since last fixup."
Perform quick fixup	-Q	Checks documents more quickly but less thoroughly. Without this option, Fixup checks documents thoroughly.
Exclude views (faster)	-V	Prevents Fixup from running on views. This option reduces the time it takes

		Fixup to run. Use if view corruption isn't a problem. «Запрещает» программе FIXUP проверять и «исправлять» виды (но не папки) - проверяются документы и папки. Это сокращает общее время работы программы.
Don't purge corrupted documents	-N	Prevents Fixup from purging corrupted documents so that the next time Fixup runs or the next time a user opens the database, Fixup must check the database again. Use this option to salvage data in documents if the corruption is minor or if there are no replicas of the database. «Запрещает» программе FIXUP удалять поврежденные документы - будет происходить лишь обнаружение повреждений, но «без грубого лечения посредством удаления всего испорченного».
Optimize user unread lists	-U	Reverts ID tables in a database to the previous release format. Don't select this option unless Customer Support recommends doing so.
Fixup transaction-logged databases	-J	Runs on databases that are enabled for transaction logging. Without this option, Fixup generally doesn't run on logged databases. If you are using a certified backup utility, it's important that you schedule a full backup of the database as soon after Fixup finishes as possible.
Fixup open databases	-O	If you run Fixup on open databases, Fixup takes the databases offline to perform the fixup. This is the default if you run Fixup and specify a database name. Without this option, when you do not specify database names, Fixup does not run on open databases.
Don't fixup open databases	-Z	Applies only to running Fixup on a single database. When a database isn't taken offline and is in use, then Fixup is not run. This is the default when Fixup is run on multiple databases.
Verify only	-C	Verifies the integrity of the database and reports errors. Does not modify the database (for example, does not purge corrupted documents).
Fixup subdirectories	-Y	Runs Fixup on databases in subfolders

		(subdirectories).
Don't fixup subdirectories	-y	Does not run Fixup on databases in subfolders (subdirectories).

1.59.2. 1.1.2. Способы «лечения» поврежденных баз

- • Запустить Fixup для удаления поврежденных индексов видов и документов.
- • Запустить Updall для перестроения поврежденных индексов видов и индексов полнотекстового поиска. Если проблема только в поврежденных индексах, запустить Updall до Fixup.
- • Нажать SHIFT+F9 для перестроения одного индекса вида или CTRL+SHIFT+F9 для перестроения всех индексов видов в базе.
- • Запустить Compact -c , если поврежденная база «не вылечивается» Fixup.
- • Создать реплику базы.

1.60. 1.1. Подсистема протоколирования транзакций (Transaction Logging)

1.60.1. 1.1.1. Назначение и принцип работы

Используемые алгоритмы базируются на Algorithm for Recovery and Isolation Exploiting Semantics (ARIES), который был разработан IBM Almaden Research Center. ARIES так же используется в DB2, MQ Series, ADSM...

Протоколирование выбирается, по умолчанию его нет. Если выбрано, то любое изменение в документах базы ODS R5/6 записывается в «протокол транзакций», а только потом проводится в файл базы.

Протокол ассоциирован с каталогом данных сервера. На один каталог данных создается один «протокол транзакций». Протокол транзакций физически состоит из набора файлов-сегментов и файла-декриптора. Логически «протокол транзакций» содержит «записи о транзакциях».

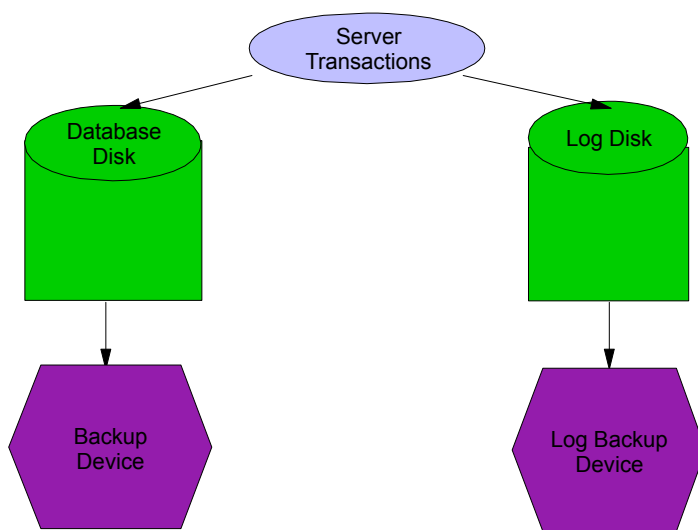


Рис. 477 Общая архитектура

- • Запись о транзакции (содержит изменения, которые необходимо выполнить в документе базы) записывается в буфер с отметкой «незавершенная». Буфер, когда он заполнен, записывается на диск в «протокол транзакций».
- • Только после этого отдельные процессы выполняют все связанные с транзакцией операции ввода/вывода в самих базах - информация никогда не записывается в базы, пока запись о транзакции не сохранена на диске.
- • Если операция в базах успешно завершилась, эта транзакция в «протоколе транзакций» отмечается как завершенная.
- • Если не завершилась - значит транзакция в «протоколе транзакций» остается отмеченной как незавершенная. Тогда, обычно при рестарте сервера, из баз будут устранены «незавершенные изменения», а затем незавершенные транзакции из протокола транзакций будут проведены в базы.
- • DBIID (DataBase Instance Identifier) - идентифицирует базу в протоколе транзакций
- • LogID - идентифицирует протокол транзакций сервера
- • LSN (Log Sequence Number) - 8-байтовый адрес записи в протоколе, который сохраняется в самой базе

1.60.2. 1.1.2. Конфигурирование и использование протоколирования транзакций

Конфигурирование выполняется в документе Server.

Server : InterTrust/InterTrustCorp/SU

Basics | Security | Ports | Server Tasks | Internet Protocols | MTAs | Miscellaneous | **Transactional Logging** | Shared Mail | Administration

Basics

Transactional logging: ☐ Enabled ☒ Disabled

Log path:

Logging style: ☐ Circular ☒ Sequential

Use all available space on log device: ☐ Yes ☒ No

Maximum log space: MB

Automatic fixup of corrupt databases: ☐ Enabled ☒ Disabled

Runtime/Restart performance: ☐ Standard ☒ High

Quotas

Quota enforcement: ☐ Check filesize when extending the file ☒ No

Рис. 478 Конфигурирование в документе Server

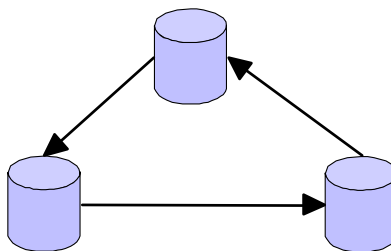


Рис. 479 Circular Logging

- • выбор по умолчанию
- • файлы сегментов «заполняются по кольцу» - экономим на дисковом пространстве
- • 192MB minimum - 4GB maximum
- • более «свежие» записи о транзакциях перекрывают «по кольцу» более «старые»
- • восстановление возможно в пределах имеющегося «в кольце» протокола
- • файлы сегментов не могут быть выгружены (для них backup не имеет смысла)

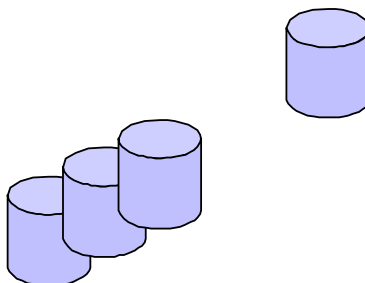


Рис. 480 Archive Logging

- • новые файлы-сегменты создаются по потребности
- • они могут выгружаться с применением R5/6-compliant backup product
- • восстановление возможно всегда
- • предпочтителен, но:
 - • дисковое пространство

- • средства backup, которые ... «стоят денег»

Первый запуск сервера после «включения протоколирования»...

Когда сервер перезапускается после «включения протоколирования»:

- • все базы R5/6 получают DBIIDs
 - • DBIID и LogID записываются в заголовки баз
- Далее все операции с базами протоколируются, кроме:
- • Fixup
 - • Compact
 - • обновления индексов видов (в R6 это возможно)

Восстановление после краха (Crash Recovery)

Время восстановления после краха зависит только от предшествующей краху «активности» и обычно составляет одну-две минуты

При этом анализируется протокол транзакций и база:

- • выполняются незавершенные транзакции, имеющиеся в протоколе транзакций
- • из базы убираются изменения, не зарегистрированные в протоколе транзакций
- • если база не может быть восстановлена, она помечается как «поврежденная», и тогда два варианта:
 - • автоматический Fixup по поврежденным базам
 - • «ручное» вмешательство

Transaction logging (Performance)

Поднимает время отклика клиенту и производительность сервера (см. [статью LDD](#)).

Backup и протоколирование транзакций

По теории надо регулярно выполнять два варианта backup:

- • редкий полный backup баз
- • частый backup самого протокола транзакций

Тогда восстановление должно происходить так:

- • восстановить базы с ленты...
- • восстановить протокол (если и он был потерян)
- • выполнить «накат вперед» по протоколу

Но чем это делать? Lotus предоставляет

- • Online backup API
- • Online restore API

а сторонние разработчики на нем пишут продукты...

1.60.3. 1.1.3. Протоколирование транзакций для индексов видов (View Logging)

В R6 обещано в области протоколирования транзакций было много... Реально осуществлено (в плане очевидного расширения функционала) весьма мало... Вероятно, это связано со сменой генеральной линии развития продукта - попыткой замены «хранилища» NSF на «хранилище» в DB2.

View Logging - протоколирование транзакций для индексов видов

- • Возможность восстанавливать индексы видов при их повреждениях, не перестраивая их заново

- • в R5 такого нет - только для документов...
- • Принцип работы - все изменения в индексах видов (постранично) записываются в протокол транзакций для обеспечения возможности восстановления и отката
- • Дизайнер должен выбрать опцию Include updates in transactional log в окне свойств вида или папки

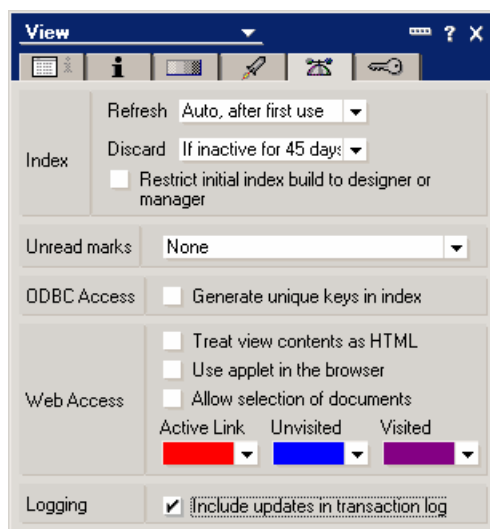


Рис. 481 Опция Include updates in transactional log в окне свойств вида или папки

- • Естественно на сервере должно быть разрешено протоколирование транзакций и оно не должно быть запрещено для данной базы

Стиль Linear ведения протокола транзакций

Linear logging is like circular logging, except it allows more than 4GB. Use linear logging if the size of the log needed between full database backup intervals is greater than 4GB, and you are not using archive media

1.60.4. 1.1.4. Краткий обзор средств для Backup сервера

Tivoli Data Protection for Lotus Domino, referred to as the Domino Application Client, is an application that backs up and restores Lotus Domino databases. The Domino Application Client provides a connection between a Domino Server and the Tivoli Storage Manager (TSM) Server, allowing Domino data to be protected and managed by TSM. When archival logging is active on the Domino Server, this application also archives transaction log files and retrieves the log files during database recovery. Database backups and transaction log file archives are stored on TSM server storage.

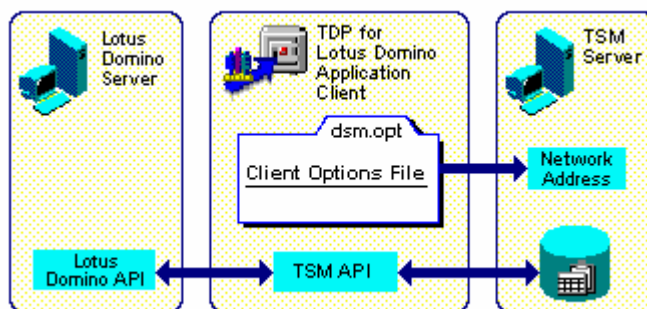


Рис. 482 «Принципальная» схема

The Domino Application Client helps protect and manage Lotus Domino Server data by making it easy to perform the following actions:

- • Backup online Lotus Domino databases

- • Maintain multiple backup versions of the Domino databases
- • Archive Lotus Domino transaction log files when archival logging is in effect
- • Restore any backup version of a Lotus Domino database and apply changes since the backup from the transaction log
- • **Restore Domino databases to a specific point in time**
- • Expire database backups automatically based on version limit and retention period
- • Expire archived transaction log files when they are no longer needed
- • Obtain online context-sensitive, task, and conceptual help
- • View online documentation for the Domino Application Client
- • Automate scheduled backups

Date: 02.12.2002

Company	Product Name	NT	WIN2K	OS/390 zSeries	AS/400 iSeries	AIX pSeries	Solaris	Linux
Tivoli http://www.tivoli.com/products/index/data_protection_domino/index.html	Tivoli Data Protection for Lotus Domino	x	x	x		x	x	
Veritas http://www.veritas.com	Netbackup 3.2	x				x	x	
	Netbackup 3.4	x	x			x	x	
Legato Systems, Inc. http://www.legato.com/	Networker Module for Lotus	x	x			x	x	Beta
Commvault http://www.commvault.com	Commvault Galaxy	x	x					
EMC http://www.emc.com/	EMC Data Manager for Lotus Notes Domino R5 Servers	x	x					
IBM http://www-1.ibm.com/servers/eserver/series/service/brms/	Backup Recovery & Media Services for iSeries (BRMS)				x			

1.61. 1.1. Мониторинг серверов Domino

1.61.1. 1.1.1. Настройка уровня подробности протоколирования в базу LOG.NSF

Setting	Description
Log	Specifies the contents of the log file and controls other logging actions.
Log_AgentManager	Specifies whether or not the start of agent execution is recorded in the log file and shown on the server console.
Log_Console	Enforces logging of server console command output, which can otherwise be prevented if the command is prefixed with an exclamation point (!).
Log_DirCat	Logs information about the Directory Catalog task to the Miscellaneous Events view of the log file (LOG.NSF).
Log_Replication	Specifies the level of logging of replication events performed by the current server.
Log_Sessions	Specifies whether individual sessions are recorded in the log file and displayed on the console.
Log_Tasks	Specifies whether the current status of server tasks is recorded in the log file and displayed on the console.
Log_Update	Specifies the level of detail of Indexer events displayed at the server console and in the log file.
Log_View_Events	Specifies whether messages generated when views are rebuilt are recorded in the log file.
Mail_Log_To_MiscEvents	Determines whether all mail event messages are displayed in the Miscellaneous Events view of the log file

1.61.2. 1.1.2. Программа Statistics (STATLOG)

Программа обновляет информацию об использовании баз данных, находящихся на данном сервере, как в базе «Протокол работы сервера» (LOG.NSF), так и в самих базах (окно User Activity). По умолчанию запускается в 5 часов утра.

Информация об использовании баз заносится программой Statistics в базу LOG.NSF «безоговорочно». Получить эту информацию можно в следующих видах базы LOG.NSF.

- **Database - Usage** Информация о каждом использовании каждой базы данных пользователями и серверами. Документы Session содержат количество документов, прочитанных и записанных в сеансе. Документы Activity показывают количество времени, в течение которого база данных использовалась (включая использование в уровне вида, когда никакие документы не были открыты) и количество документов, прочитанных и записанных за день, неделю, месяц и с момента создания.
- **Database - Sizes** Имеется столбец, дающий количество использований базы в течение последней недели.
- **Usage - By User** Для каждого сеанса пользователя или сервера можно получить информацию о документах, использованных в этом сеансе.

С другой стороны, в каждой базе данных из диалогового окна User Activity обычно можно получить информацию об использовании только этой базы. Это окно "вызывается" из окна свойств базы кнопкой User Activity на закладке Information. Управление же окном User Activity доступно только менеджеру базы. Выбором опции **Record Activity** менеджер "требуется" сбора информации об использовании базы. Опция **Activity is Confidential** "делает" информацию об использовании базы доступной только лицам, имеющим к этой базе доступ менеджера или дизайнера.

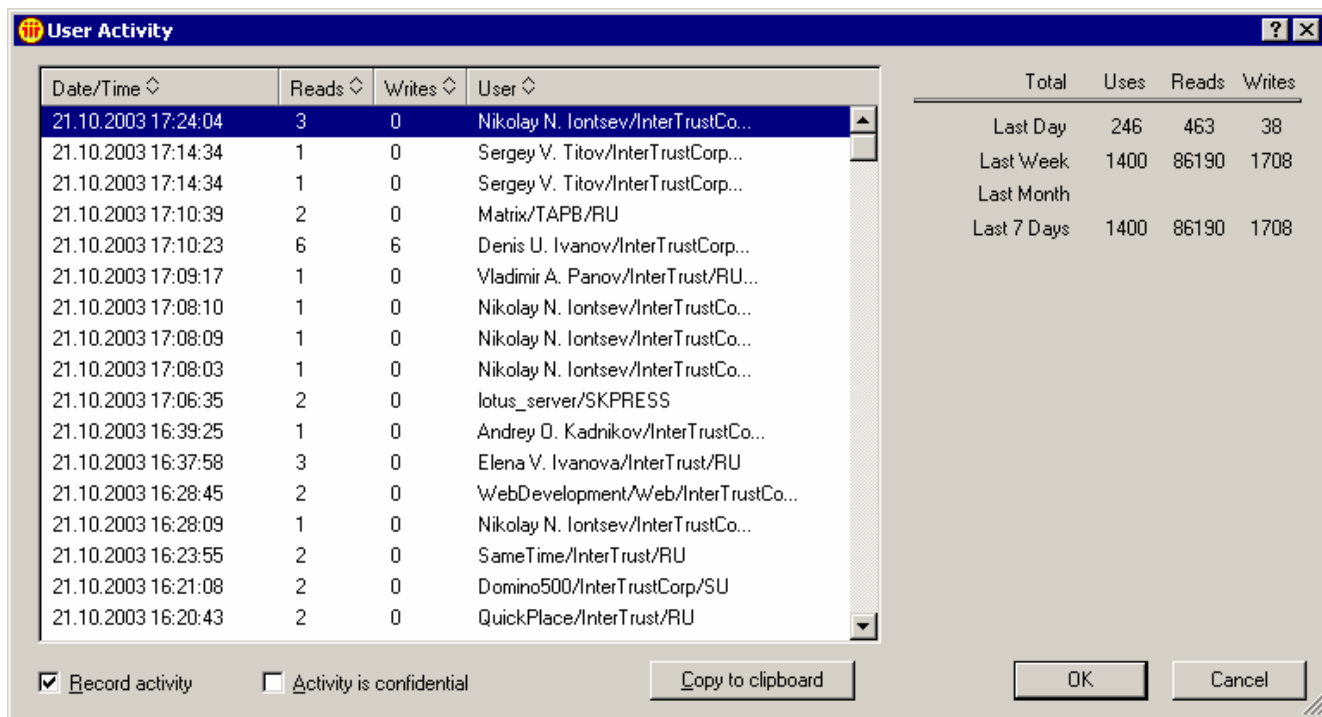


Рис. 483 Окно User Activity

Если опция Record Activity была «включена» для базы, программа Statlog будет обновлять информацию об использовании этой базы непосредственно в самой базе, если же опция «выключена» - не будет обновлять. Однако сбор информации об использовании непосредственно в базе «добавляет» 64Кб к размеру этой базы.

По умолчанию программа Statlog, обнаружив на сервере базу, для которой менеджер еще ни разу не изменял опцию Record Activity, «включит» эту опцию и тем самым активизирует сбор информации. Чтобы сохранять дисковое пространство, администратор может добавить в файл NOTES.INI переменную **No_Force_Activity_Logging=1**. В этом случае программа Statlog, обнаружив базу, для которой менеджер еще ни разу не изменял опцию Record Activity, «выключит» эту опцию и тем самым «запретит» сбор информации. Однако «при любом раскладе» менеджер базы может затем явно «включить или выключить» сбор информации.

1.61.3. 1.1.3. Программа Stats (STATS)

На серверах R6 программа по умолчанию не запускается. На серверах предшествующих версий, напротив, автоматически запускается при старте сервера. При первом запуске создает почтовую базу STATMAIL.NSF и документ mail-in database для этой базы «на адрес» формата “<CN_сервера> Stats/<Имя_организации>”, например, Domino500 Stats/InterTrustCorp.

Может отправлять «статистику» по почте в ответ на подписанное администратором письмо специального вида, направляемое по адресу “<CN_сервера> Stats/<Имя_организации>”. При получении такого письма на консоли сервера появляется сообщение наподобие «Stats: Processing query for CN=Nikolay N. Iontsev/O=InterTrustCorp/C=SU» и отправителю письма возвращается ответное письмо с требуемой «статистикой».

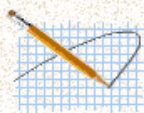
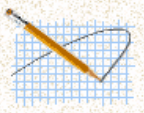
 Nikolay N. Iontsev/InterTrustCorp/SU 01.12.2003 12:32	To	Domino500 Stats/InterTrustCorp
	cc	
	bcc	
	Subject	mail

Рис. 484 Пример письма с запросом на получение «статистики» (аналог show stat mail)

 Domino500 Stats/InterTrustCorp 01.12.2003 12:26	To	 Nikolay N. Iontsev/InterTrustCorp/SU
	cc	
	bcc	
	Subject	Re: mail

Mail.AverageDeliverTime	0
Mail.AverageServerHops	0
Mail.AverageSizeDelivered	0
Mail.CurrentByteDeliveryRate	0
Mail.CurrentByteTransferRate	0
Mail.CurrentMessageDeliveryRate	0
Mail.CurrentMessageTransferRate	0
Mail.DBCacheEntries	0
Mail.DBCacheHits	0
Mail.DBCacheReads	0
MAIL.Dead	0
Mail.Delivered	1
Mail.Deliveries	1
Mail.Domain	INTERTRUSTCORP
MAIL.Hold	0
Mail.MaximumDeliverTime	0
Mail.MaximumServerHops	0
Mail.MaximumSizeDelivered	0
Mail.MinimumDeliverTime	0
Mail.MinimumServerHops	0
Mail.MinimumSizeDelivered	0
Mail.TotalKBTransferred	1
Mail.TotalKBTransferred.NRPC	1
Mail.TotalPending	0
Mail.TotalRouted	2
Mail.TotalRouted.NRPC	2
Mail.Transferred	1
Mail.Transferred.NRPC	1
MAIL.Waiting	0
MAIL.WaitingForDNS	0
MAIL.WaitingRecipients	0

Рис. 485 Пример ответного письма на запрос на получение «статистики» (аналог show stat mail)

Кроме того, программа позволяет получать «статистику» с другого сервера по команде консоли Load stats <CN_сервера> [класс_статистики], например, load stats notessrv400 mail.

Поскольку практической целесообразности в функционале программы STATS обычно не наблюдается, в R6 программа по умолчанию не запускается.

1.61.4. 1.1.4. Показатели функционирования серверов (statistics)

Сервер Domino накапливает значения показателей своего функционирования («статистику») в памяти сервера и выдает ее всем потребителям.

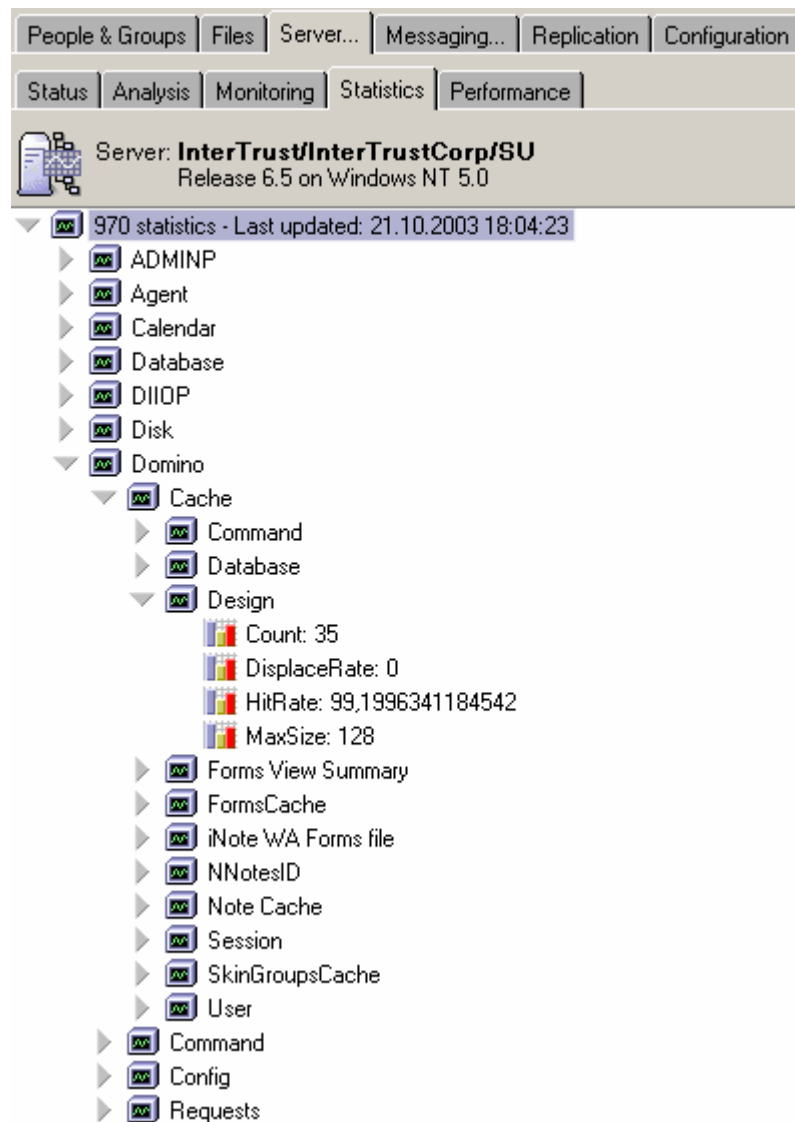


Рис. 486 Аналог Show Stat в клиенте администратора

1.61.5. 1.1.5. Мониторинг серверов из клиента администратора

People & Groups Files Server... Messaging... Replication Configuration															
Status Analysis Monitoring Statistics Performance															
Monitoring profiles: By State ☐ Show me past error states only Favorites Stop															
Hea	19:09:03 - 19:09:34	Adm	Age	Dat	Eve	Ind	Rep	Rou	Sta	Users	Dead	Hold	Waiting	Availabi	ElapsedTime
-	InterTrust/InterTrustCorp/SU	👤	👤	👤	👤	👤	👤	👤	-	18	0	0	0	54	1 day 05:50
-	NotesSrv400/InterTrustCorp/SU	👤	👤	👤	👤	👤	👤	👤	-	15	48	0	1	14	3 days 20:29
-	LAEC/ETC/InterTrust/RU	👤	👤	👤	👤	👤	👤	👤	-	13	0	0	0	100	08:51
-	Web3/InterTrustCorp/SU	👤	👤	👤	👤	👤	👤	👤	-	2	0	0	0	100	20 days 06:04
-	Web2/InterTrustCorp/SU	👤	👤	👤	👤	👤	👤	👤	-	2	0	0	0	100	20 days 05:40
-	SameTime/InterTrust/RU	👤	👤	👤	👤	👤	👤	👤	-	1	0	0	0	100	11 days 21:26
-	LINUX/LAEC/InterTrustCorp/SU	👤	👤	👤	👤	👤	👤	👤	-	1	0	0	0	100	19 days 01:16
-	QuickPlace/InterTrust/RU	👤	👤	👤	👤	👤	👤	👤	👤	0	0	0	0	100	13 days 08:23
-	LAEC/LAEC/InterTrustCorp/SU	👤	👤	👤	👤	👤	👤	👤	-	0	0	0	0	100	1 day 08:26
-	KDS/InterTrustCorp/SU	-	👤	👤	-	👤	👤	👤	-	0	0	0	0	100	5 days 23:42
?	LINUX/ETC/InterTrust/RU	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Рис. 487 Мониторинг серверов из клиента администратора

1.61.6. 1.1.6. Построение графиков показателей функционирования серверов в клиенте администратора (Statistics Charting, Realtime & Historical)

1.61.6.1. 1.1.6.1. Настройка в File – Preferences – Administrator Preferences

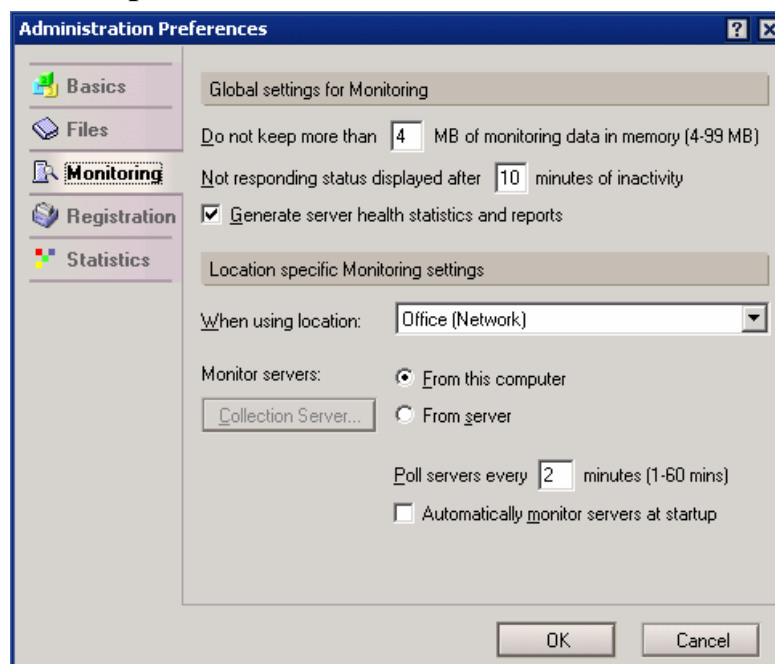


Рис. 488 Закладка Monitoring

- Monitor servers – from this computer – клиент администратора сам выполняет опрос серверов и сохраняет результаты в локальной базе statrep.nsf
- Poll servers every N minutes – частота опроса
- Generate server health statistics and reports – вычислять группу показателей «здоровья серверов» и сохранять их значения (reports)

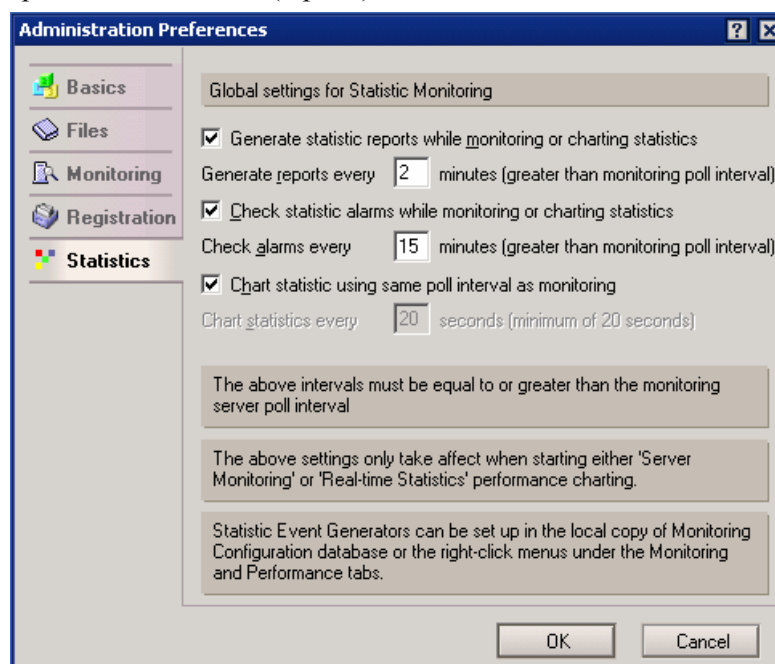


Рис. 489 Закладка Statistics

- • Generate statistics reports while monitoring or charting statistics – сохранение значений показателей при мониторинге и построении графиков
- • Generate reports every N minutes – частота сохранения значений $\geq$ частоты опроса
- • Chart statistic
 - • using same pool interval as monitoring – с частотой опроса
 - • every N seconds – с частотой N секунд

1.61.6.2. 1.1.6.2. Realtime Statistics – графики показателей в реальном времени

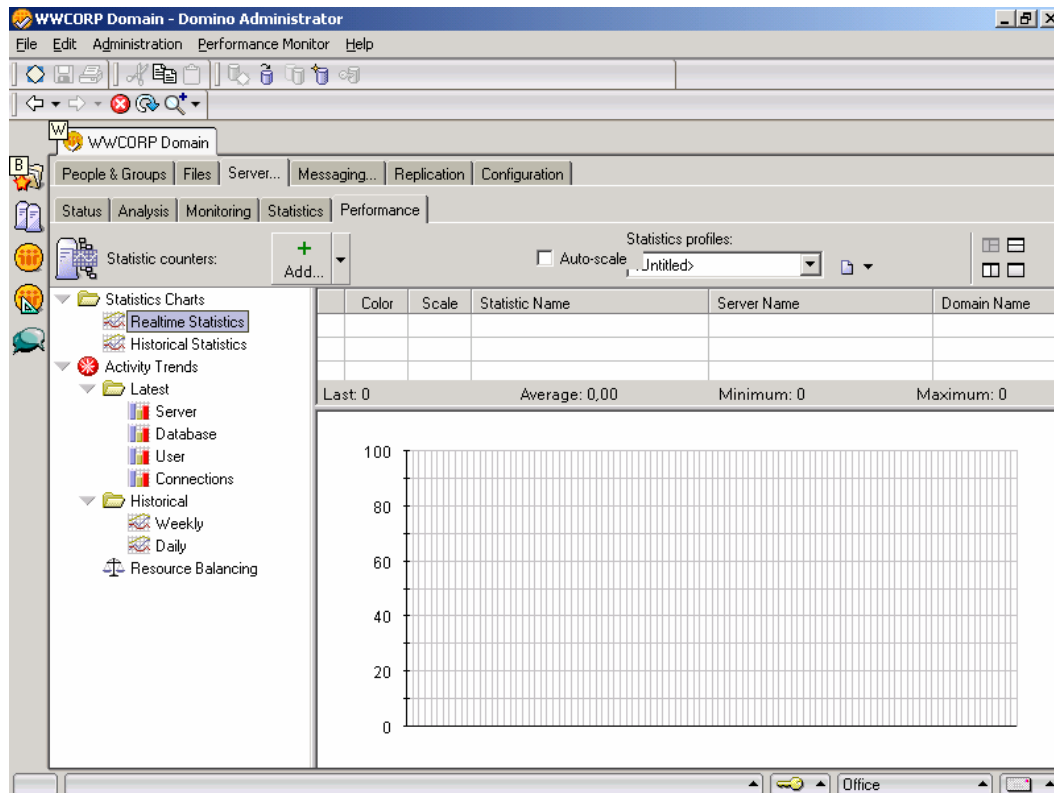


Рис. 490 На закладке Server – Performance – Realtime statistics кнопкой Add (+) «на график» добавляют представляющие интерес показатели

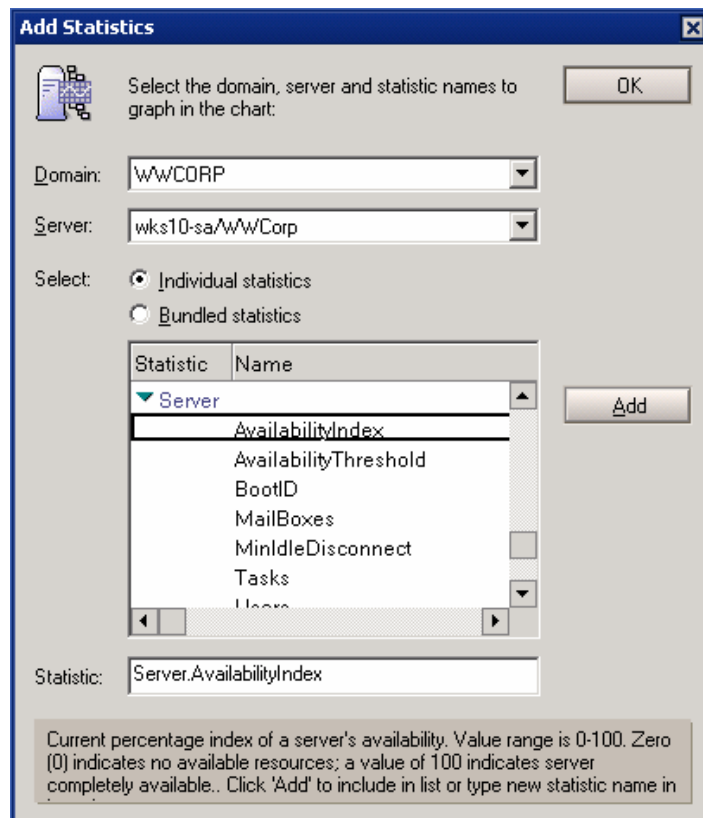


Рис. 491 Индекс доступности сервера

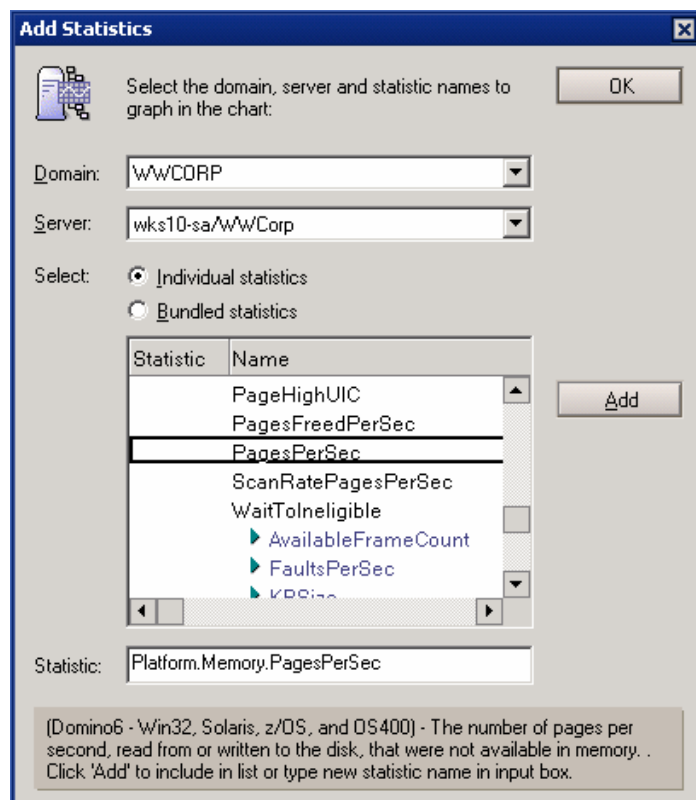


Рис. 492 Количество страниц, обмениваемых в секунду между памятью и файлом свопинга

Add Statistics [X]

Select the domain, server and statistic names to graph in the chart:

Domain:

Server:

Select: ☒ Individual statistics
☐ Bundled statistics

Statistic	Name
	LPARPctCpuUtil
	PctCombinedCpuUtil
	PctTotalPrivilegedCpuUtil
	PctTotalUserCpuUtil
	TotalNumProcs
	ContextSwitchesPerSec
	CPUQueueLen
	LPARPctCpuUtil

Add

Statistic:

(Domino6 - Solaris, Win32, and AIX) - The total CPU percentage utilization running in the user mode of all CPUs in the system. . Click 'Add' to include in list or type new statistic name in input box.

Рис. 493 Утилизация процессора в пользовательском режиме

Add Statistics [X]

Select the domain, server and statistic names to graph in the chart:

Domain:

Server:

Select: ☒ Individual statistics
☐ Bundled statistics

Statistic	Name
	ContextSwitchesPerSec
	CPUQueueLen
	LPARPctCpuUtil
	PctCombinedCpuUtil
	PctTotalPrivilegedCpuUtil
	PctTotalUserCpuUtil
	TotalNumProcs
	ContextSwitchesPerSec

Add

Statistic:

(Domino6 - Solaris, Win32, and AIX) - The total CPU percentage utilization in privileged (kernel) mode of all CPUs in the system. . Click 'Add' to include in list or type new statistic name in input box.

Рис. 494 Утилизация процессора в режиме ядра

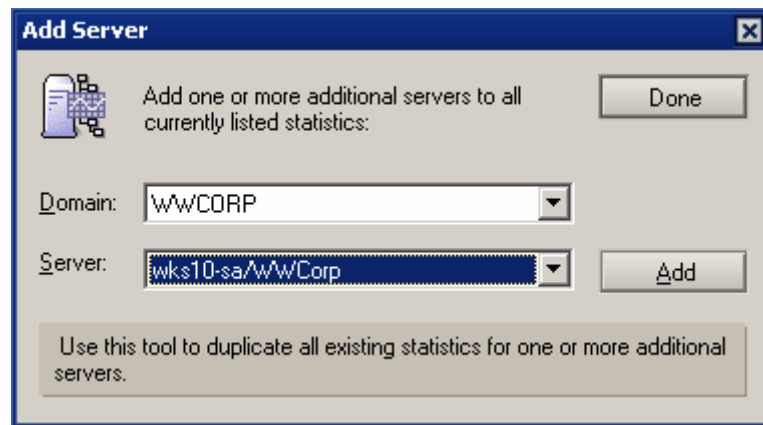


Рис. 495 Кнопкой «треугольник вниз» рядом с кнопкой Add можно «повторить выбранные показатели по другому серверу»

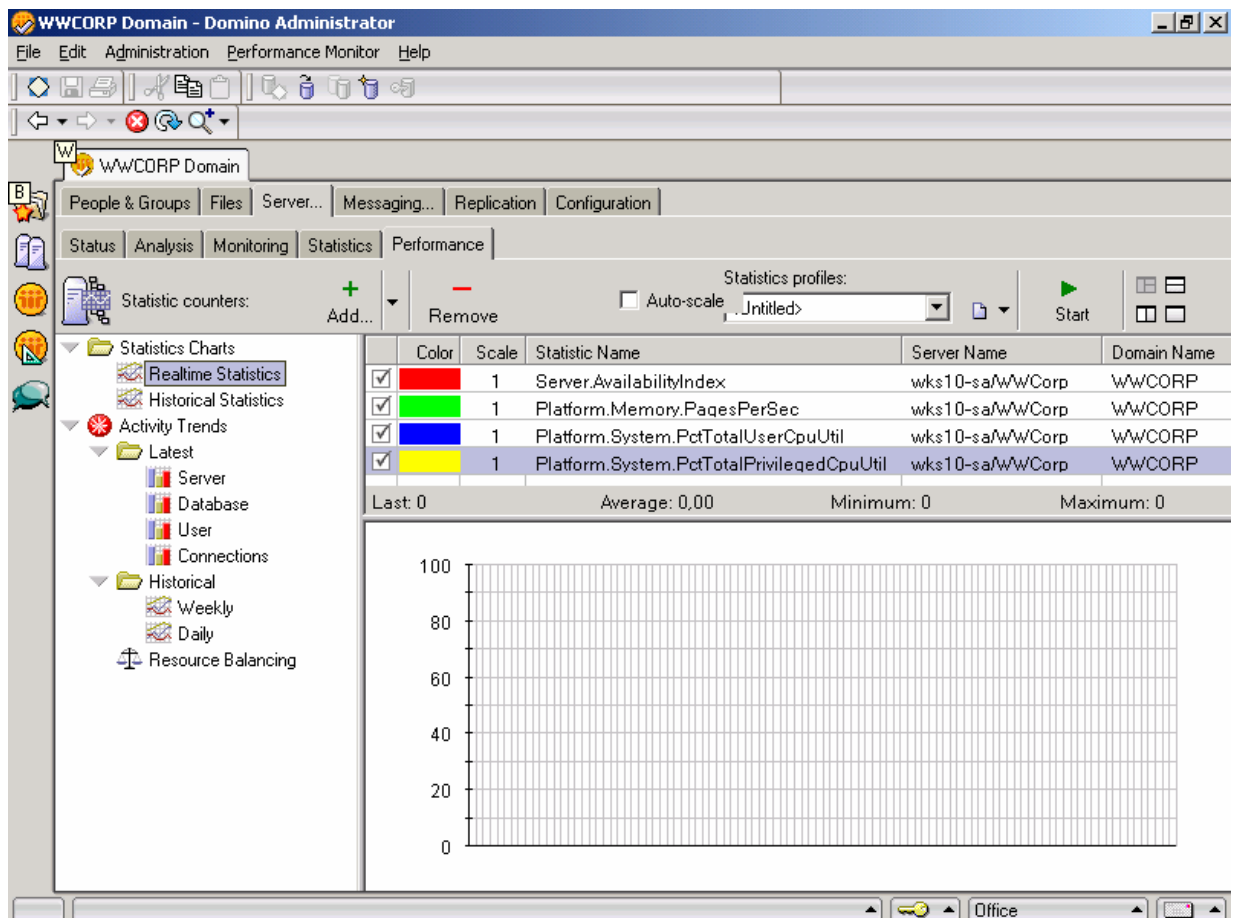


Рис. 496 Кнопкой справа от combobox-a Statistics Profiles можно сохранить информацию о «добавленных» на график показателях

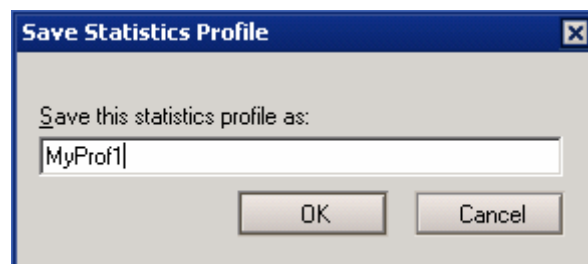


Рис. 497 Присвоение названия Statistics Profile

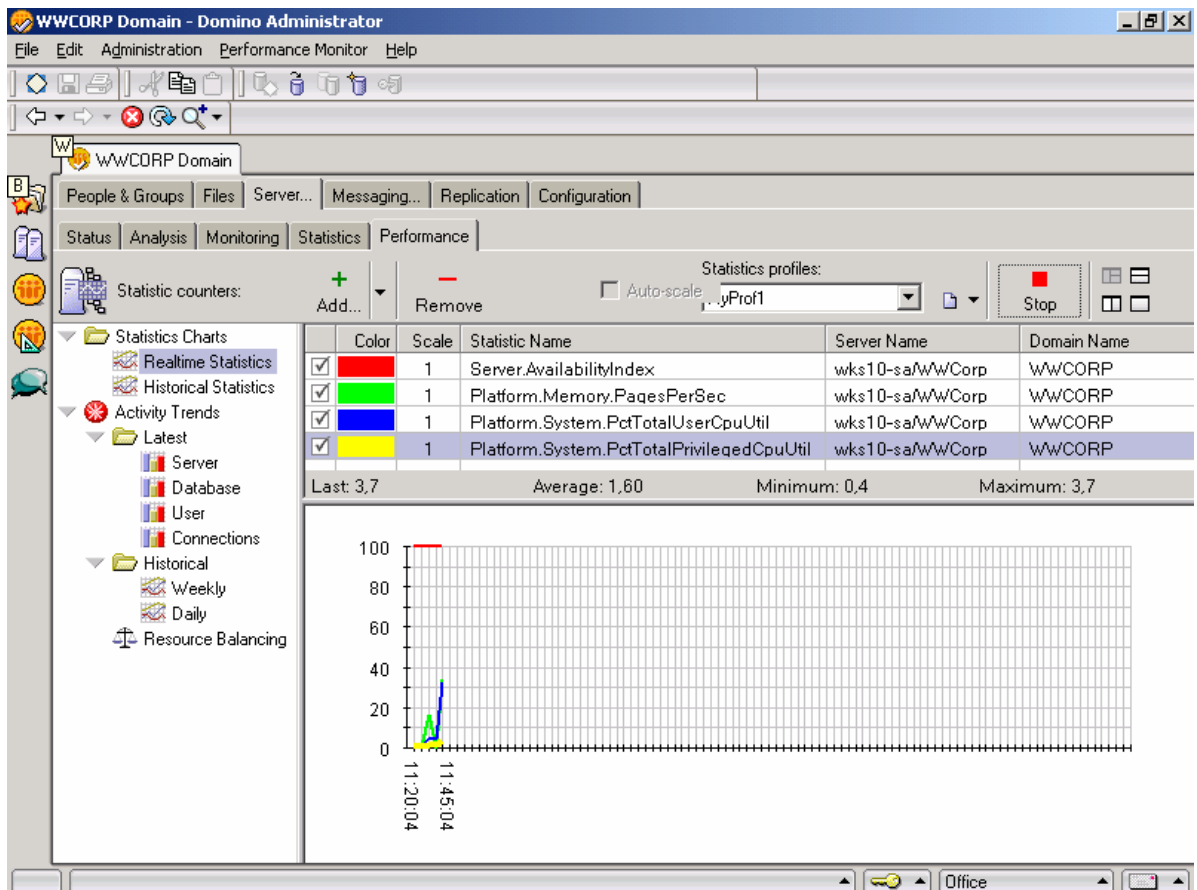


Рис. 498 Кнопкой Start (Рис. 496) запускается процесс построения графиков

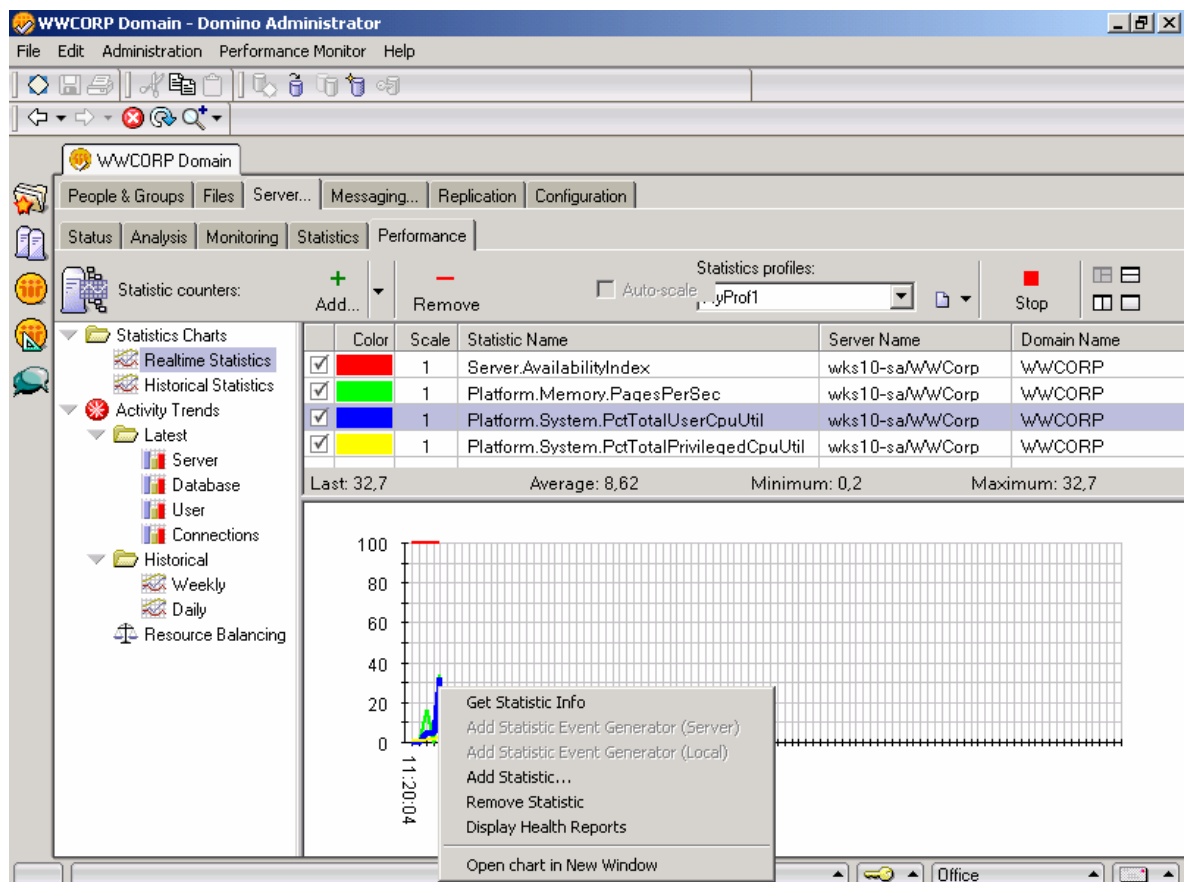


Рис. 499 Правой кнопкой мыши можно получить всплывающее меню

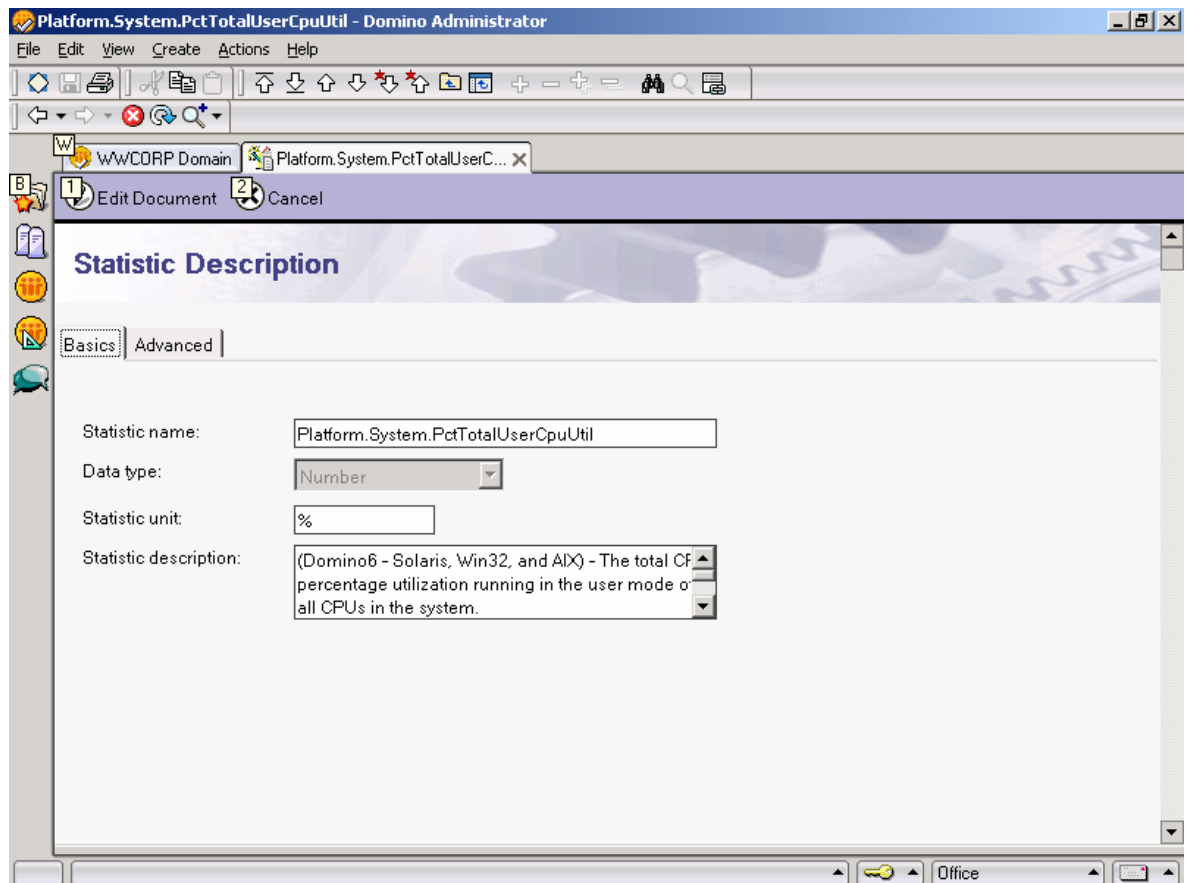


Рис. 500 Get statistic info – информация о показателе, на котором находился курсор мыши

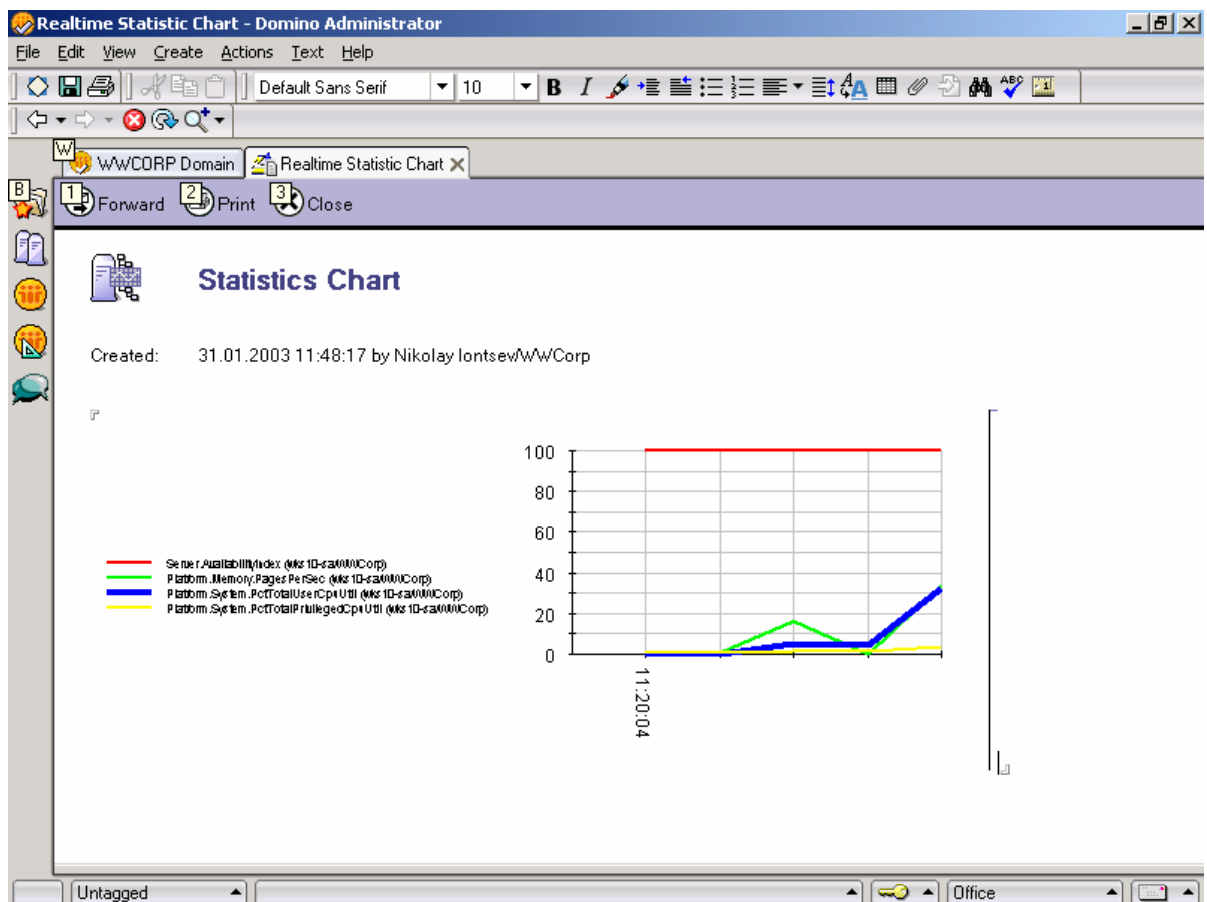


Рис. 501 Open Chart in New window...

1.61.6.3. 1.1.6.3. Historical Statistics – графики сохраненных значений показателей

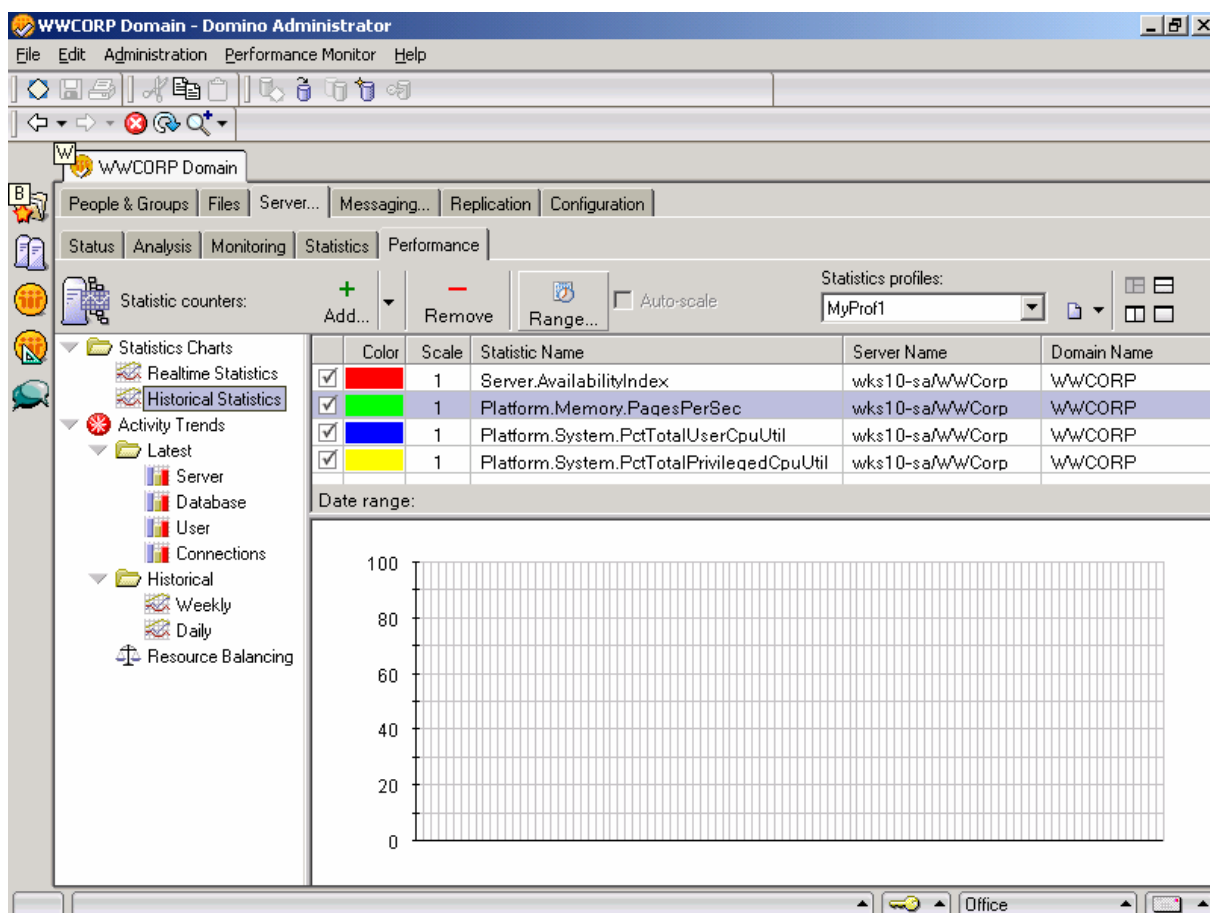


Рис. 502 На закладке Server – Performance – Historical statistics кнопкой Range выбирается диапазон времени

The dialog box 'Select Range for Historical Statistics Charting' is shown. It contains the following fields and controls:

- Domain:** A dropdown menu with 'WWCORP' selected.
- Server:** A dropdown menu with 'Local' selected.
- Start date:** A date field showing '17.01.2003'.
- End date:** A date field showing '31.01.2003'.
- Range:** A label indicating the selected date range.
- Select time range:** A checkbox that is currently unchecked.
- OK** and **Cancel** buttons.

A note at the bottom states: 'Historical statistics data will be obtained from the database 'statrep.nsf' on the selected server above.'

Рис. 503 Диапазон может быть длительностью в несколько дней

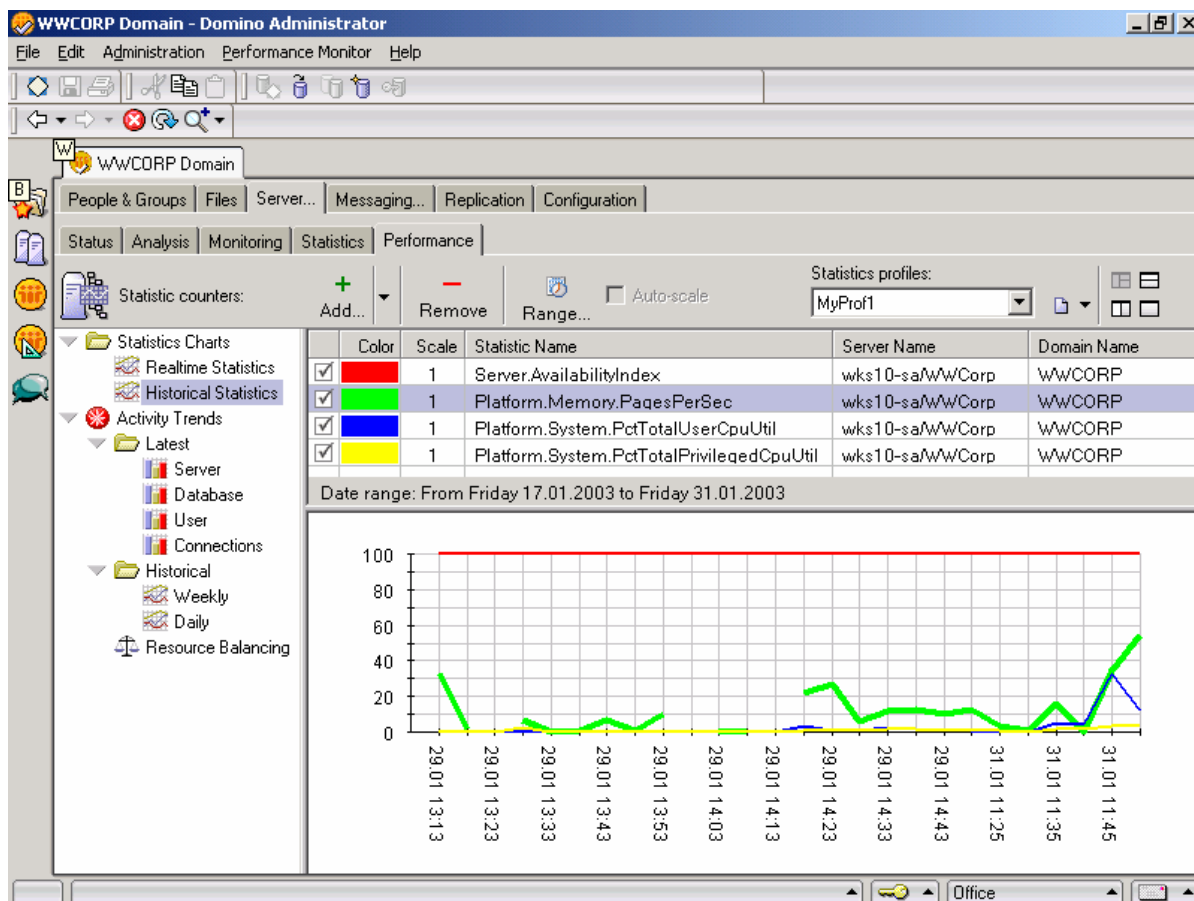


Рис. 504 Графики сохраненных в локальной statrep.nsf показателей

Select Range for Historical Statistics Charting

Select the domain, server and date/time range for the selected statistics to chart:

Domain: WWCORG

Server: Local

Start date: 29.01.2003 16 End date: 30.01.2003 16

Range: 29.01.2003 16 30.01.2003 16

☒ Select time range:

Start time: 08:00 End time: 17:00

Historical statistics data will be obtained from the database 'statrep.nsf' on the selected server above.

OK Cancel

Рис. 505 Диапазон может быть длительностью и в несколько часов

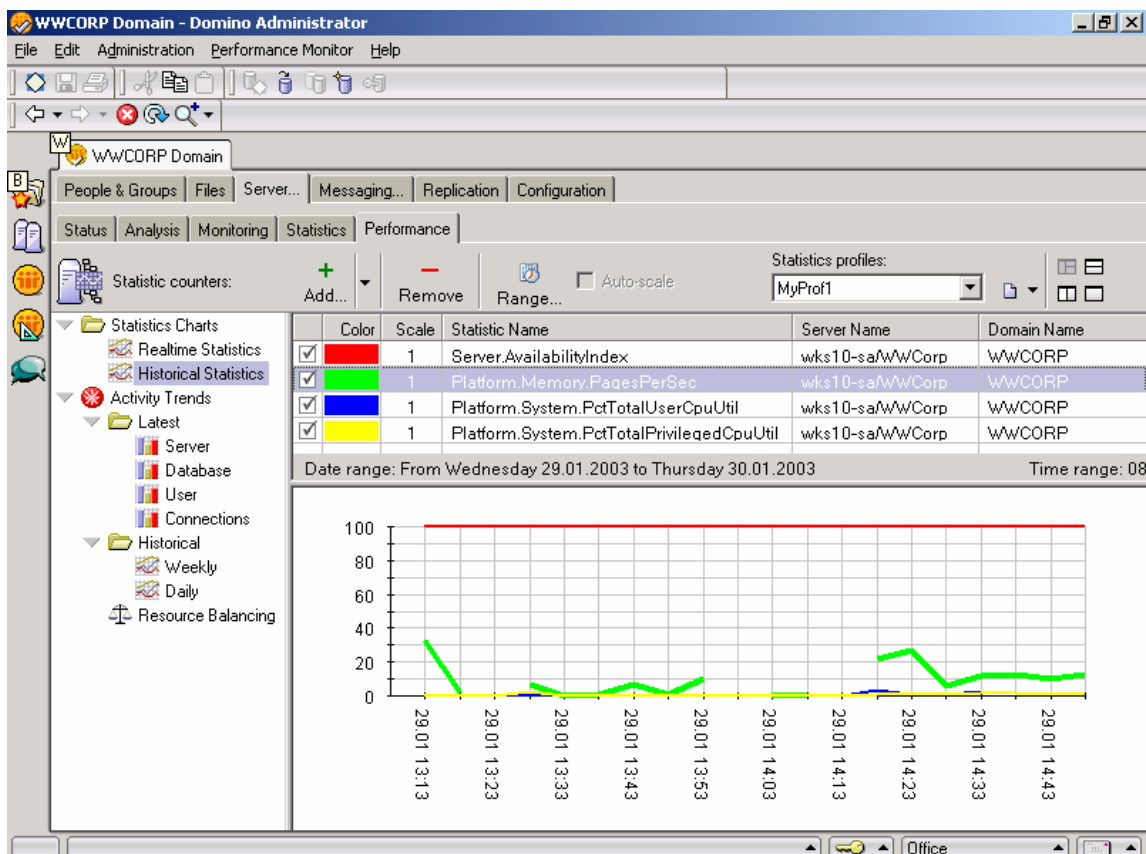


Рис. 506 Графики сохраненных в локальной statrep.nsf показателей

1.61.7. 1.1.7. Программа Billing (BILLING)

Задача Billing предназначена для сбора информации, необходимой для составления счетов за использование серверов Domino. Сервер Domino помещает необходимую для этого информацию в очередь сообщений задачи Billing. Задача Billing периодически опрашивает эту очередь сообщений и заносит необходимую информацию в специальную базу данных или файл.

Классы информации, которая должна отслеживаться сервером Notes и затем протоколироваться задачей Billing, перечисляются в переменной **BillingClass** в файле NOTES.INI. Например, если задано
BillingClass=Session,Database,Document,Replication,Mail,Agent

то требуется отслеживать всю возможную информацию. Рассмотрим возможные классы.

- **Session** Отслеживаются начало и окончание каждой сессии с сервером составления счетов (сервер, на котором работает задача Billing), включая выполненные за время сессии действия, в частности, редактирование документов или репликации.
- **Database** Отслеживаются моменты открытия и закрытия баз на сервере составления счетов пользователями и другими серверами, а также продолжительность использования этих баз.
- **Document** Отслеживаются обращения (для чтения или записи) только к некоторым документам в базах данных на сервере составления счетов. Такие документы должны содержать поля с именами \$ChargeRead и (или) \$ChargeWrite типа Number (Currency) со значением, по смыслу интерпретируемым как «цена обращения к документу».
- **Replication** Отслеживается репликация, инициированные сервером составления счетов с другими серверами или станциями пользователей с данным сервером.
- **Mail** Отслеживаются факты отправления почтовых сообщений с сервера составления счетов на другие серверы (включая имена отправителя и получателя).

- • **Agent** Отслеживается время, затраченное сервером составления отчетов на выполнение агентов.

Переменная **BillingAddinRuntime=*n*** (из файла NOTES.INI) задает количество секунд, отводимых задаче Billing на извлечение сообщений из очереди и запись информации о них в базу или файл. Значение по умолчанию 10 секунд. По истечении этого «кванта времени» задача приостанавливает свою работу, даже если в очереди остались необработанные сообщения.

Переменная **BillingAddinWakeup=*n*** (из файла NOTES.INI) задает интервал в секундах, с которым задача Billing повторяет процесс извлечения сообщений из очереди и записи информации о них в базу или файл. Значение по умолчанию 60 секунд. Естественно, что значение переменной BillingAddinWakeup должно быть больше, чем значение переменной BillingAddinRuntime.

Задача Billing заносит необходимую информацию в специальную базу данных или файл, в зависимости от того, что вы укажете в качестве значения переменной **BillingAddinOutput** в файле NOTES.INI. Если BillingAddinOutput=1, информация записывается в базу данных BILLING.NSF, если BillingAddinOutput=8 - в «двоичный» файл BILLING.NBF, если BillingAddinOutput=9 - одновременно и в базу BILLING.NSF, и в файл BILLING.NBF.

База данных BILLING.NSF автоматически создается задачей Billing при первом запуске (по шаблону BILLING.NTF). В стандартном шаблоне базы предусмотрен набор видов для представления содержащейся в базе информации. В то же время имеется возможность усложнять дизайн этой базы, добиваясь желаемых способов отображения информации из документов.

Billing		Agent Name & Database Name ^	Elapsed Run Time, sec
Agents By Username			
Agents By Username - NI			
Document By Username			
Http Requests			
Mail By Originator			
Replication By Server			
Sessions			
Database Opens By User			
Network Traffic By User			
		▼ Denis U. Ivanov	18 785,62
		▶ CheckSources : site3/bussig.nsf	11 444,89
		▶ ProcessRTD : site3/busrtd.nsf	6 786,35
		▶ ProcessSignals : site3/bussig.nsf	554,38
		▼ Ilia N. Ardabev	54,77
		▶ ArchivAndRemove : WorkProjects/MID/prepDocs.nsf	54,77
		▼ InterTrust Co.	179,79
		▶ ProcessNewDiggest : WorkProjects/artgallery/subscribe.nsf	179,79
		▶ ProcessNewMail MailRobot : WorkProjects/MID/WEB/robot.nsf	0,00
		▼ Natalia G. Kozlova	0,56
		▶ (WeeklyUpdateCounter) WeeklyUpdateCounter : WorkProjects/Mars/tds.nsf	0,56
		▼ Nikolay N. Iontsev	2 841,66
		▼ NotesSrv400	33,60
		▶ agHousekeeping\$ServerL3 : webadmin.nsf	20,65
		▶ Periodic Archive : nntp/nd000051.nsf	1,04
		▶ Periodic Archive : nntp/nd000052.nsf	0,60
		▶ Periodic Archive : nntp/nd000054.nsf	0,66
		▶ Periodic Archive : nntp/nd000055.nsf	1,18
		▶ Update Tasks Update Tasks : mail/dtrushin.nsf	1,45
		▶ Update Tasks Update Tasks : mail/obaranov.nsf	5,60
		▶ UpdateMailIn : WorkDatabases/BASES400/Secretariat/ITSsbd1.NSF	2,42
		▼ Oleg G. Taranchenko	4 615,26
		▶ HelpDesk : mail/TechSupp.nsf	68,13
		▶ HotTask : Omedia/V5_new/MONITOR.NSF	1,99
		▶ HotTask : WorkDatabases/Arbeit/MONITOR.NSF	1,73
		▶ HotTask : WorkDatabases/BASES400/office21/monitor.nsf	3,11

Рис. 507 База данных BILLING.NSF - информация об выполненных агентах

Файл BILLING.NBF так же автоматически создается, если при запуске задача Billing обнаруживает его отсутствие. Это не текстовый, а «записеориентированный» файл относительно несложной структуры. Каждая его запись содержит свою длину, тип записи и соответствующую типу информацию. Администраторы, заинтересованные в специфических способах представления содержащейся в файле информации, могут разработать для этого собственные программы.

1.61.8. 1.1.8. Подсистема сбора статистики и обработки событий

1.61.8.1. 1.1.8.1. Логика работы подсистемы

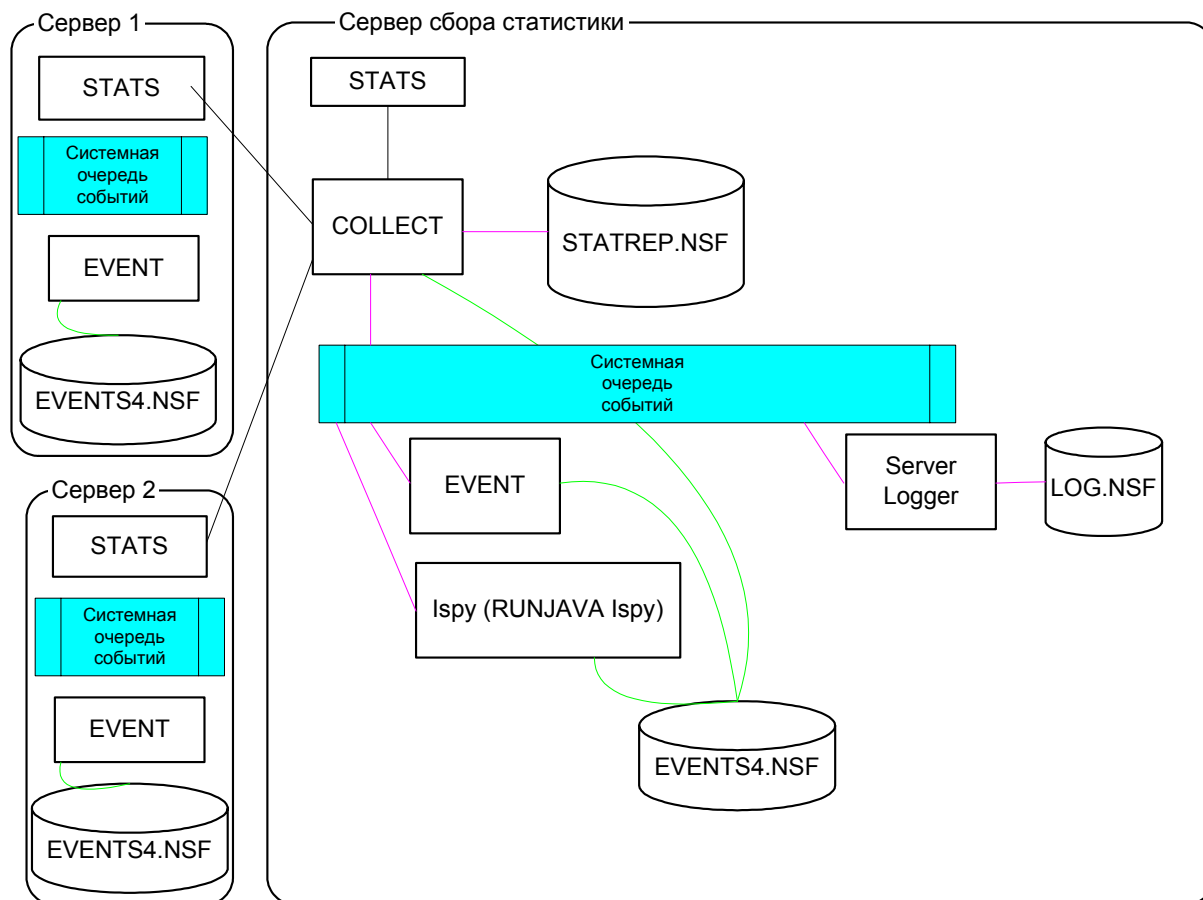


Рис. 508

1.61.8.2. 1.1.8.2. Программы Statistic Collector (COLLECT), Ispy (RUNJAVA Ispy) и Event Monitor (EVENT)

Задача Collect предназначена для сбора статистической информации с многих серверов. Ее загружают только на том сервере, где собирается статистика с других серверов, а не на каждом из серверов получения статистики. Будучи соответственно настроенной, задача может генерировать события класса Statistics при выходе выбранных показателей за выбранные границы.

Задача Ispy написана на Java и запускается как RUNJAVA Ispy. Задача может тестировать работу почтовой системы, работу серверов Domino и любых других серверов (проверка регулярным обращением по порту). Если что-то перестает работать, задача генерирует события.

Задача Event является обработчиком событий. Выбирая из системной очереди необходимые события, она заданным образом «реагирует» на них.

1.61.8.3. 1.1.8.3. Базы данных, используемые в подсистеме сбора статистики и обработки событий



EVENTS4.NSF - Monitoring Configuration (Statistics & Events) - база для управления функционированием всей системы мониторинга серверов (реплика на каждом сервере).



STATREP.NSF - база, в которой собирается статистика и сводные отчеты, а также протоколируются события (обычно только одна база на сервере сбора статистики).

1.61.8.4. 1.1.8.4. Серверы сбора статистики

1.61.8.5. 1.1.8.5. Генераторы событий (Event Generators) и их создание

Database Event Generator

Event Number: NNIV-5DXCBX

Basics | Replication | Unused Space | User Inactivity | Other

Database to monitor

File name: Site\etc.nsf

Server(s):

☐ All in the domain

☒ Only the following:

LINUX/LAEC/InterTrustCorp/SU

What to monitor

- ☒ Monitor ACL Changes:
- ☒ Monitor replication:
- ☒ Monitor unused space:
- ☒ Monitor for user inactivity:

Рис. 509

Database Event Generator

Event Number: NNIV-5DXCBX

Basics | Replication | Unused Space | User Inactivity | Other

Server(s) with which the database must replicate

☒ All in the domain

☐ Only the following:

Replication timeout

Timeout: 24 hours

Рис. 510

Database Event Generator

Event Number: NNIV-5DXCBX

Basics | Replication | Unused Space | User Inactivity | **Other**

Event

Generate a Database event of severity:

Warning (high) ▼

Create a new event handler for this event.

Enablement

☐ Disable this event generator

Puc. 511

Domino Server Event Generator

Event Number: NNIV-48TDZN

Basics | Probe | Other

Target server(s)

Server(s):

InterTrust/InterTrustCorp/SU,
NotesSrv400/InterTrustCorp/SU



Probing server (source)

Server:

LAEC/LAEC/InterTrustCorp/SU



Access

Interval: Minutes

- ☐ Check just the ability to access the destination server
☒ Check the ability to access the destination server and open this database:

File name: NAMES.NSF

Puc. 512

Domino Server Event Generator

Event Number: NNIV-4STDZN

Basics | Probe | Other

Ports

☐ Perform probe using any available port

Ports to use:

TCPIP

Time

Timeout threshold: Msecs

Resulting statistic

SERVER.<Probing Server>.<Destination Server>

Puc. 513

Domino Server Event Generator

Event Number: NNIV-4STDZN

Basics | Probe | Other

Event

On timeout, generate a Server event of severity:

Create a new event handler for this event.

Enablement

☐ Disable this event generator

Puc. 514

Server Statistic Collection

Created: 21.03.2003

Basics | Options

Collecting server

Server:

NotesSrv400/InterTrustCorp/SU

Collect from

- ☒ All servers in this domain
- ☐ All servers that are not explicitly listed to be collected
- ☐ From the following servers:

Puc. 515

Server Statistic Collection

Created: 21.03.2003

Basics | Options

☒ Log statistics to a database

Database to receive reports (file name): statrep.nsf

Collection report interval: 120 minutes

Collection alarm interval: 30 minutes

Statistic Filters:

- ☐ Adminp
- ☐ Agent
- ☐ Calender
- ☐ Comm
- ☐ Database
- ☐ DECS
- ☐ Disk
- ☐ FT
- ☐ HTTP
- ☐ ICM
- ☐ Imap

Puc. 516

Statistic Event Generator

Event Number: NNIV-5SJKR9

Basics | Threshold | Other

Server(s) to monitor

☐ All in the domain

☒ Only the following:

Development/InterTrustCorp/SU,
InterTrust/InterTrustCorp/SU,
NotesSrv400/InterTrustCorp/SU

Statistic to monitor

Statistic to monitor: MAIL.Dead

Description: Number of dead (undeliverable) messages in MAIL.BOX

Puc. 517

Statistic Event Generator

Event Number: NNIV-5SJKR9

Basics | Threshold | Other

Threshold

Generate the event when:

☐ The statistic is LESS THAN the threshold value

☒ The statistic is GREATER THAN the threshold value

☐ The statistic is a MULTIPLE of the threshold value

Threshold: 2 messages

Puc. 518

Statistic Event Generator

Event Number: NNIV-5SJKR9

Basics | Threshold | Other

Event

Generate a Statistic event of severity: Warning (high)

Create a new event handler for this event.

Enablement

☐ Disable this event generator

Рис. 519

Хватит, наверное...

1.61.8.6. 1.1.8.6. Обработчики событий (Event Handlers) и их создание

Event Handler

Created: 16.11.99

Basics | Event | Action

Server(s) to monitor

☒ Notify of the event on any server in the domain

☐ Notify of the event only on the following servers:

Notification trigger

Trigger:

☐ Any event that matches a criteria

☐ A built-in or add-in task event

☒ A custom event generator

Рис. 520

Event Handler
Created: 16.11.99

Basics | **Event** | Action

Custom Event Generator

Select the event:

Summary:
 Server(s): -All Servers-
 Database: names.nsf
 Event severity: Warning (high)

Details...

Рис. 521 Без глюков жить никак нельзя...

Event Handler
Created: 16.11.99

Basics | Event | **Action**

Notification

Mail

Mailing address: Nikolay N. Iontsev/InterTrustCorp/SU

Enablement

☒ Enable this notification
☐ Disable this notification
☐ Enabled only during these times:

Рис. 522

1.61.9. 1.1.9. Подсистема протоколирования активности (Activity Logging)

- • Уточнение функций Activity Logging и Activity Trends
- • Конфигурирование Activity Logging и Activity Trends
- • Анализ использования сервера посредством Activity Analysis
- • Программа Activity Trend Collector (TRENDS) и база ACTIVITY.NSF
- • Анализ данных в базе ACTIVITY.NSF

Activity Logging - протоколирование активности, Activity Trends Analysis - анализ тенденций

1.61.9.1. 1.1.9.1. Настройка

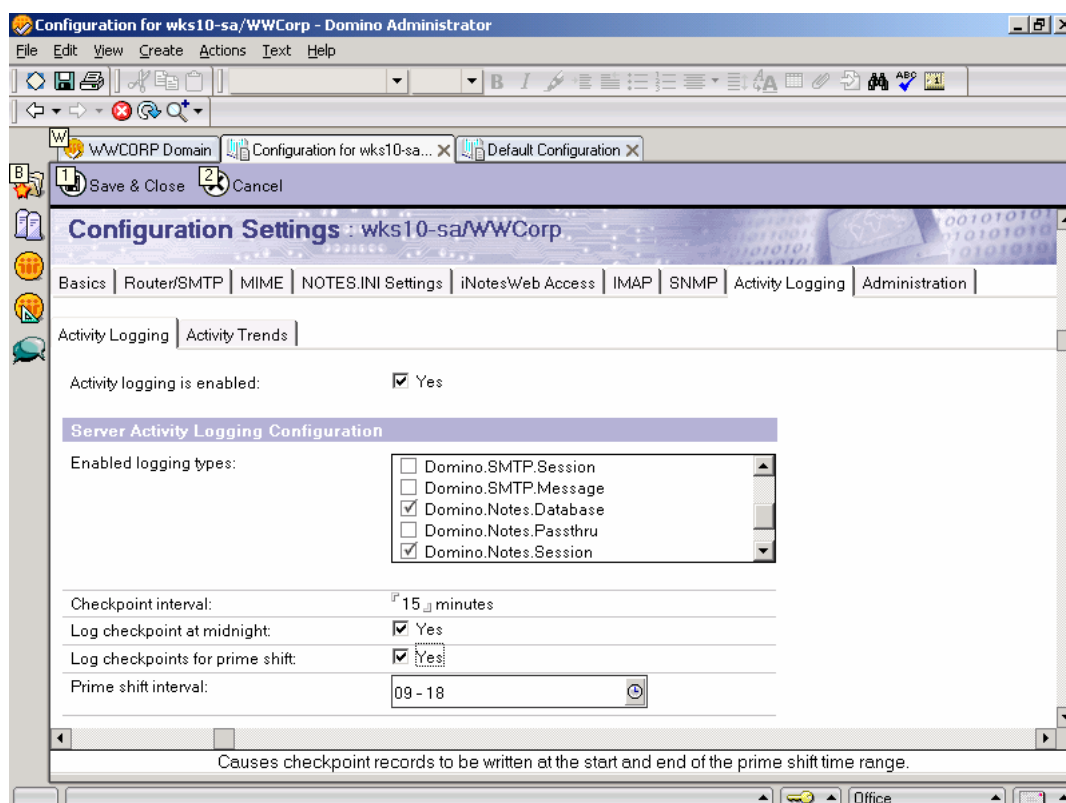


Рис. 523 Документ Configuration settings – закладка Activity Logging – Activity Logging

Разрешено протоколирование активности и выбраны протоколируемые типы активностей. Протоколируемая информация заносится в базу log.nsf в документы в виде записей специального формата (records). В начале и конце каждой сессии с сервером записываются записи о начале (Open и Authorization records) и конце (Close record) сессии. В пределах сессии каждые 15 минут записывается «контрольная запись» (Checkpoint record) о текущем состоянии сессии, если Checkpoint interval = 15 минут. Кроме того «контрольная запись» по каждой сессии записывается в 24:00 (так необходимо для Activity Trends) и в начале и конце интервала наибольшей загрузки (prime shift – «основная смена», работа ЭВМ в рабочие часы данного учреждения).

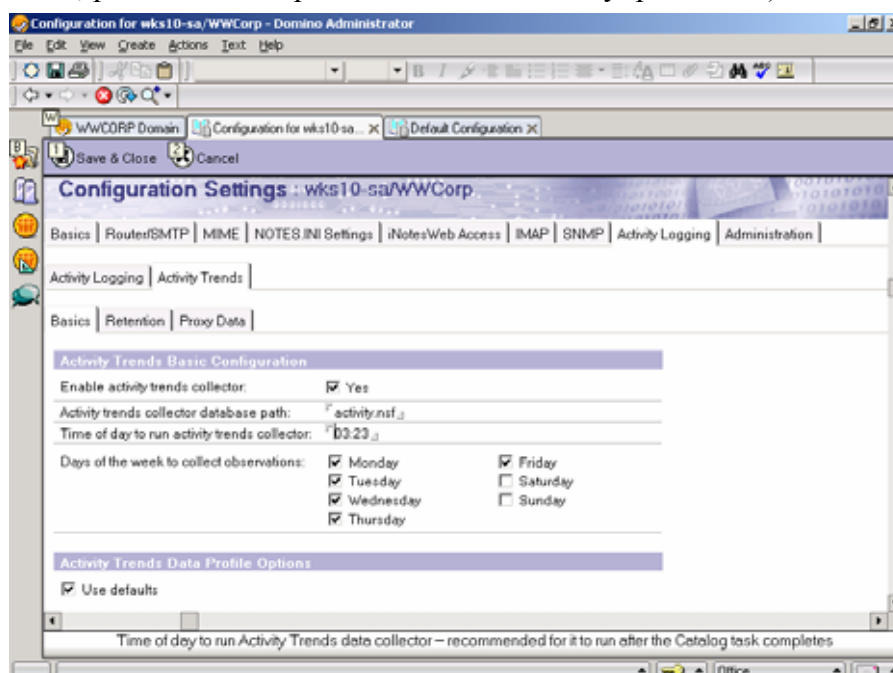


Рис. 524 Документ Configuration settings – закладка Activity Logging – Activity Trends – Basics

Разрешен запуск сервером в 3:23 (после завершения работы программы CATALOG) программы Activity Trend Collector (TRENDS). Программа выбирает записи об активности из log.nsf, обрабатывает их и записывает данные наблюдений (observations) в базу activity.nsf. Данные наблюдений заносятся в базу activity.nsf только по выбранным дням недели.

Если выбрано Use defaults, для рассматриваемых ниже параметров Activity Trend Collector выбираются значения по умолчанию.

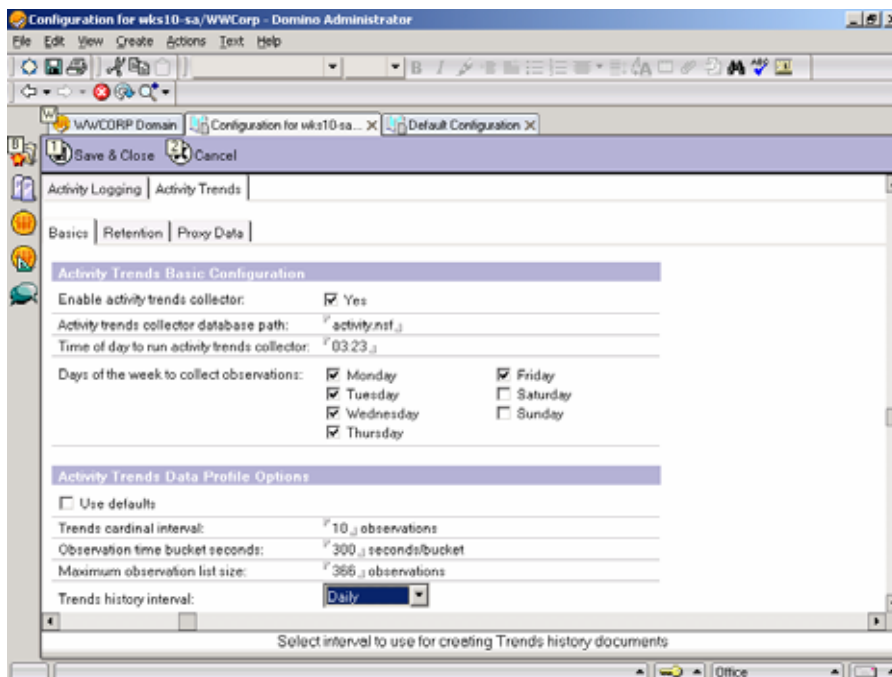


Рис. 525 Документ Configuration settings – закладка Activity Logging – Activity Trends – Basics

Если не выбирать Use defaults, можно самому выбрать необходимые параметры Activity Trend Collector:

- Trends cardinal interval (по умолчанию 10 дней) – при вычислении тенденций (trends, тренды) по данным наблюдений с наибольшим весом учитываются предшествующие 10 наблюдений. Так, если данные наблюдений заносятся в activity.nsf только по рабочим дням (5 дней в неделю), то при значении 10 тенденции вычисляются за две недели.
- Observation time bucket (seconds) (по умолчанию 300) – данные наблюдений представляют собой «набор отсчетов» по каждому 5 минутам (300 секунд) в течении суток, $1440/5 = 288$ отсчетов в сутки.
- Maximum observation list size (по умолчанию 366)– за сколько предшествующих дней хранится информация в базе activity.nsf. По умолчанию за год. Затем новые данные «перезаписывают» старые, чтобы база не разрасталась в размерах.
- Trends history interval (по умолчанию неделя) – интервал создания документов Trend history в базе activity.nsf. В период изучения рекомендуется уменьшить.

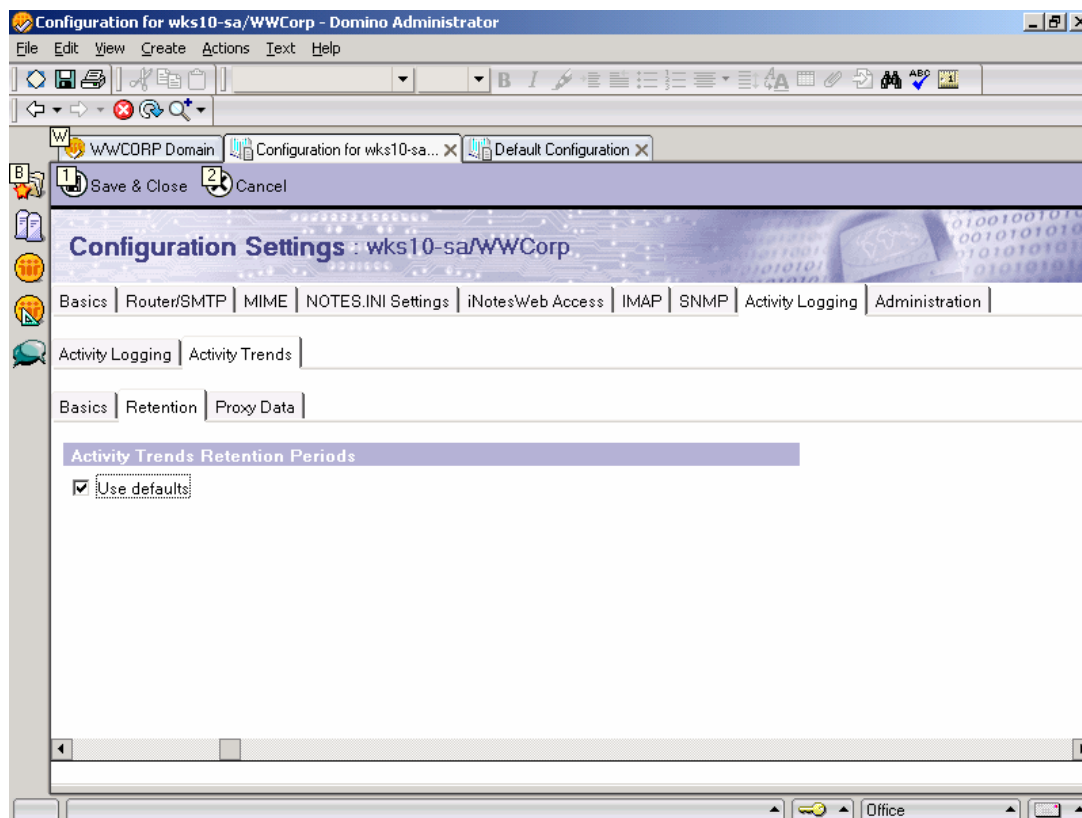


Рис. 526 Документ Configuration settings – закладка Activity Logging – Activity Trends – Retention

Закладка Retention определяет продолжительность хранения данных в базе activity.nsf. По умолчанию значения следующие:

- • Server history - 366 days
- • Server observations -15 days
- • Database observations - 10 days
- • User observations - 10 days
- • Connection observations - 10 days
- • Inactive database trends - 10 days
- • Inactive user trends - 28 days
- • Inactive connection trends - 28 days
- • Run log - 20 days

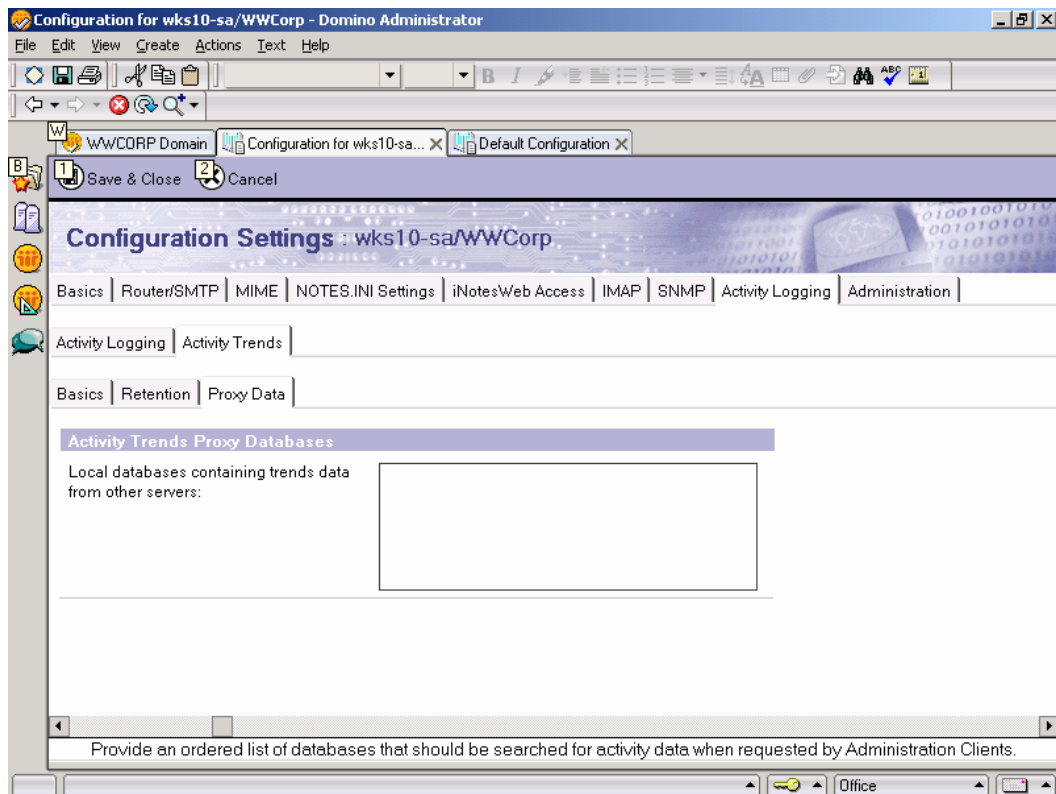


Рис. 527 Документ Configuration settings – закладка Activity Logging – Activity Trends – Proxy Data

Может содержать список локальных баз типа activity.nsf, содержащих данные об активности с других серверов.

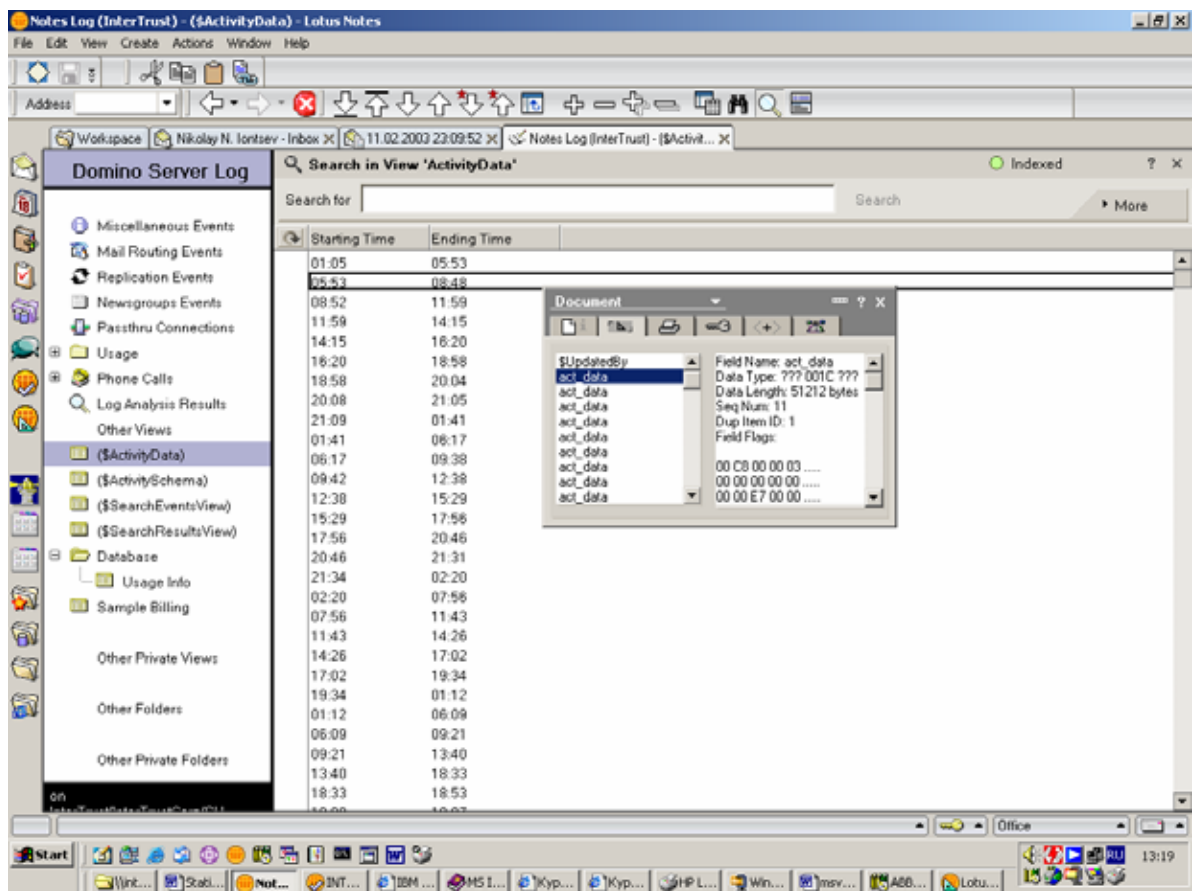


Рис. 528 Протоколируемая информация действительно помещается в базу log.nsf...

1.61.9.2. 1.1.9.2. Использование

Database Pathname	Connects	Connect Seconds	Transactions
Alexander M. Savelyev/InterTrustCorp/SU	108	30 814	13
mail1.box	7	3 614	
mail2.box	11	4 056	
MAIL\asaveye.nsf	84	20 625	11
MAIL\asavel.nsf	2	93	
WorkDatabases\Arbeitcd_lib.nsf	2	1 253	
WorkDatabases\ArbeitIT4SET.NSF	2	1 173	
Alexey S. Telekovsky/InterTrustCorp/SU	138	29 320	11
EDU\IR5\Documents.nsf	2	1 070	
log.nsf	2	1 105	
Lotus\Notes\NIC\Support\KBNV11.NSF	2	1 087	
mail1.box	12	2 080	
mail2.box	9	3 180	
mail\atelekov.nsf	93	11 968	8
MAIL\spam.nsf	2	1 063	
names.nsf	2	293	
OtherNABs\LukMsc.nsf	2	1 069	
Site\itforum.nsf	2	1 076	

Рис. 529 База Activity Trends – activity.nsf

Без IBM Tivoli Analyzer for Lotus Domino – просто изучать виды в базе. Большинство видов имеет два варианта – за все время суток и за интервал наибольшей нагрузки (Prime [shift]). При неспешном рассмотрении Вы найдете здесь много интересного и полезного. Вид {Run Log} содержит протокол запусков Activity Trend Collector.

1.61.10. 1.1.10. IBM Tivoli Activity Trends Analysis & Resource Balancing - анализ тенденций и балансировка ресурсов

- Установка IBM Tivoli Analyzer for Lotus Domino на клиента администратора
- Первичная настройка Tivoli Analyzer
- Activity Trends Analysis - анализ тенденций
- Resource Balancing - балансировка ресурсов
- Программа Change Manager (RUNJAVA ChangeMan) и ее база данных

1.61.10.1. 1.1.10.1. Установка и первичная настройка IBM Tivoli Analyzer for Lotus Domino

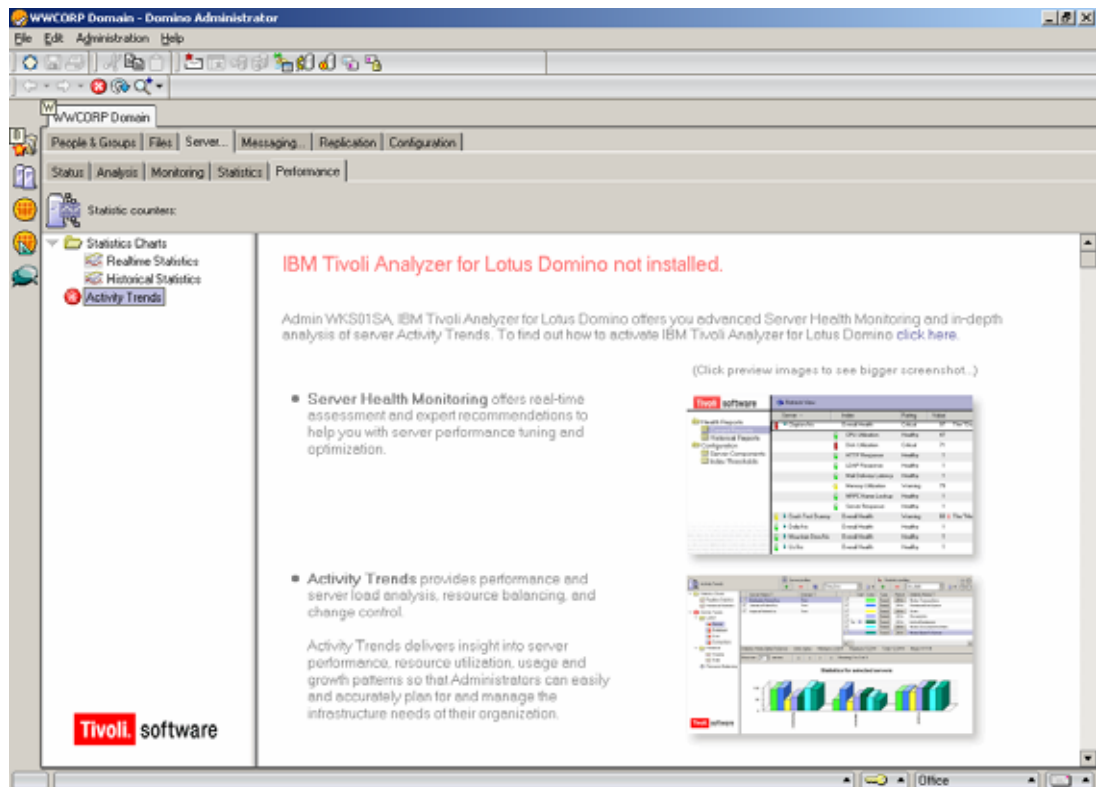


Рис. 530 Вид закладки Server-Performance-Activity Trends в клиенте Администратора, когда IBM Tivoli Analyzer for Lotus Domino не установлен

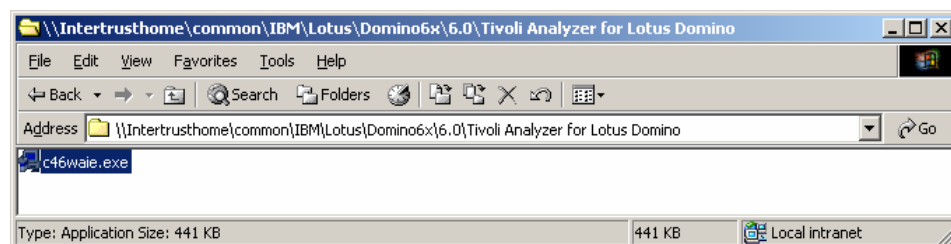


Рис. 531 Запуск программы установки IBM Tivoli Analyzer for Lotus Domino на компьютере, где установлен клиент Администратора

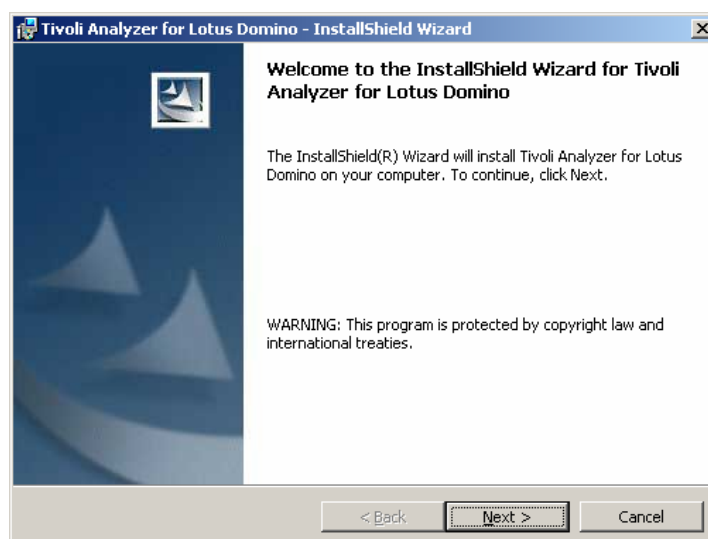


Рис. 532 Первое окно

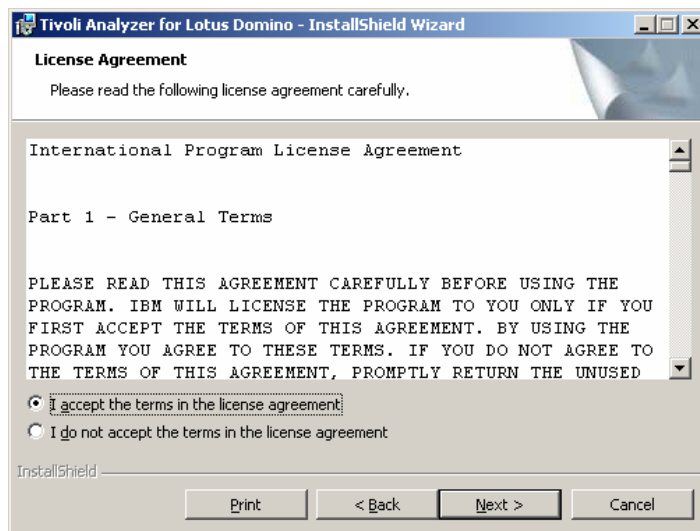


Рис. 533 Второе окно – согласны с лицензионным соглашением

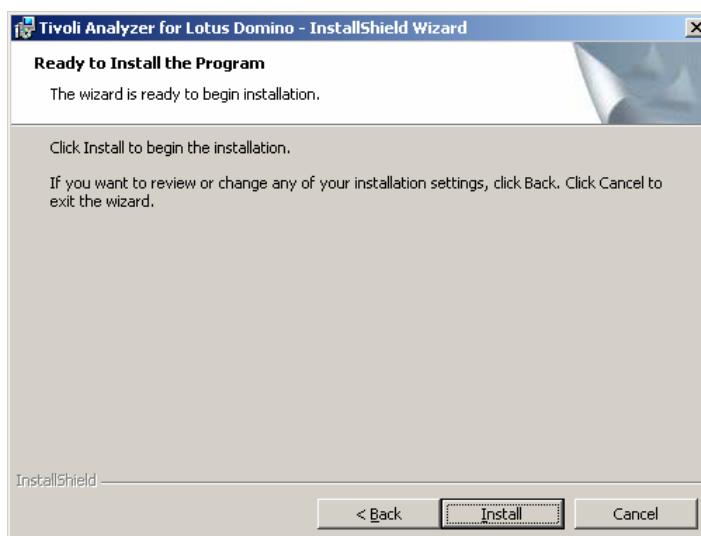


Рис. 534 Начало установки

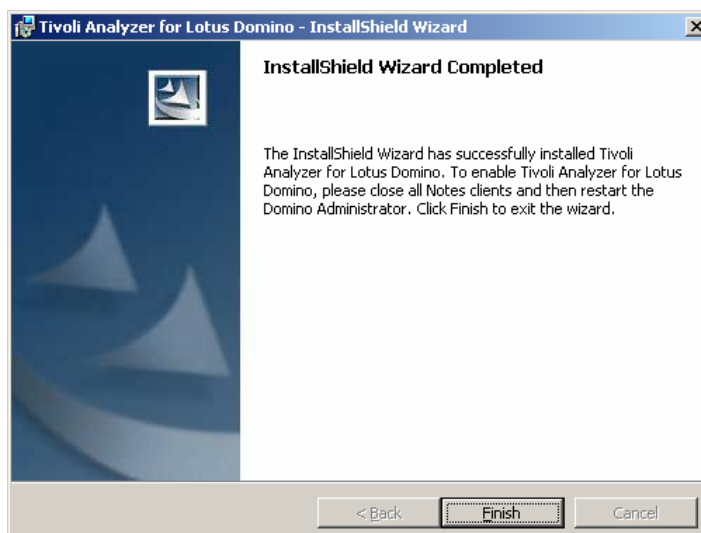


Рис. 535 Конец установки

После перезапуска клиентов заставка (Рис. 530) исчезнет. Находясь в одном из «псевдовидов» Activity trends и выбрав в меню Activity trends – options или Resource balancing – options, можно получить окно настроек с закладками.

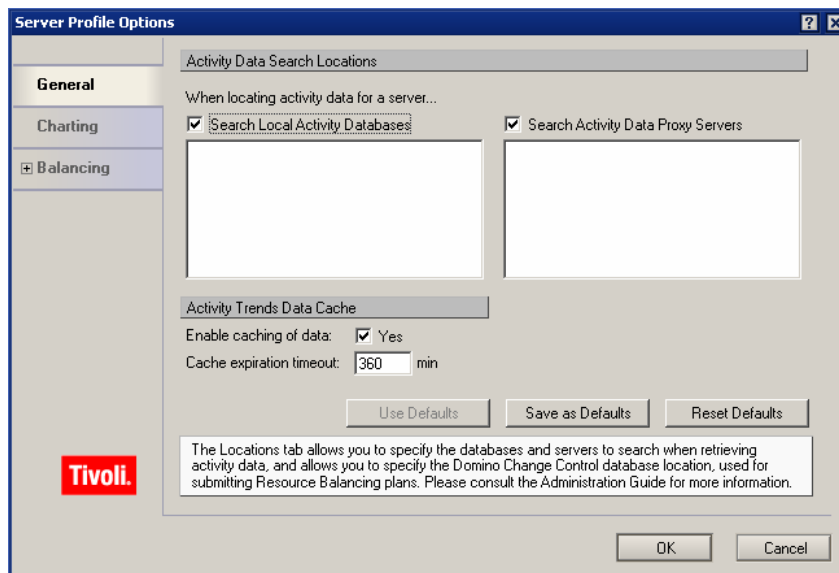


Рис. 536 Местонахождение баз Activity Data

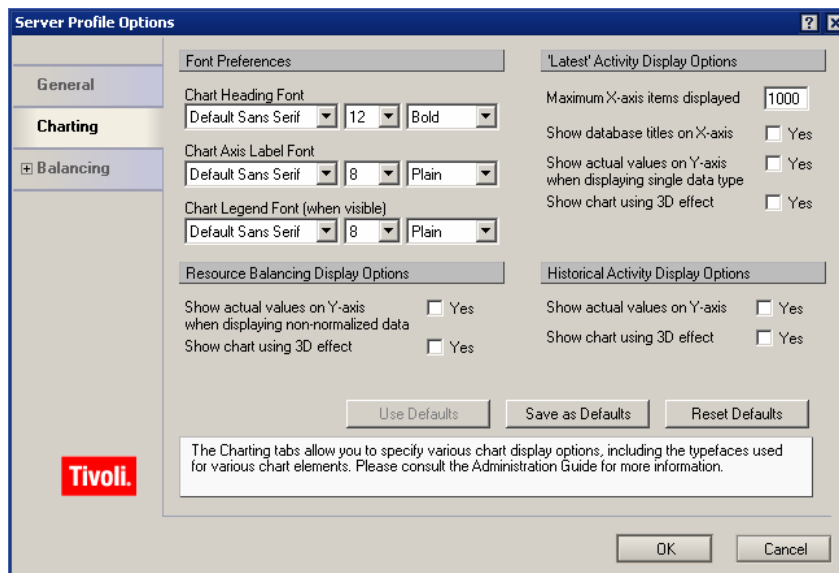


Рис. 537 Оформление

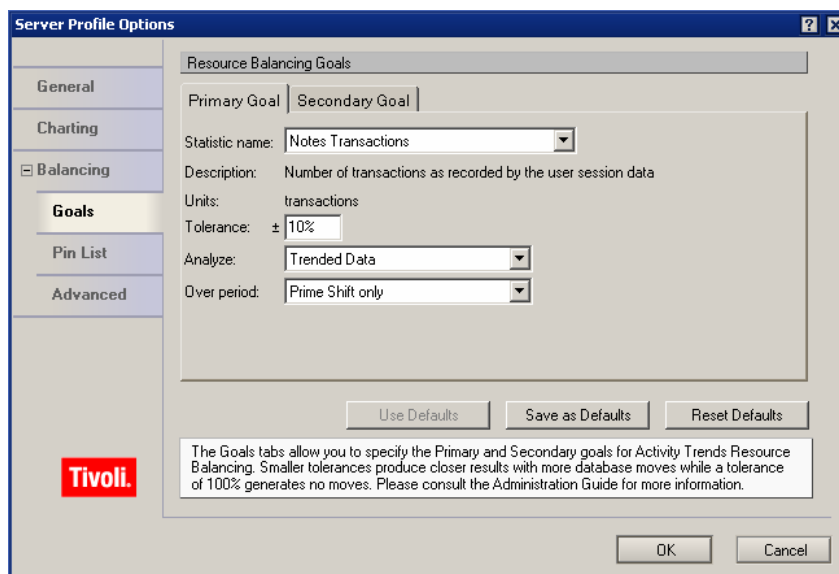


Рис. 538 Основная цель балансировки

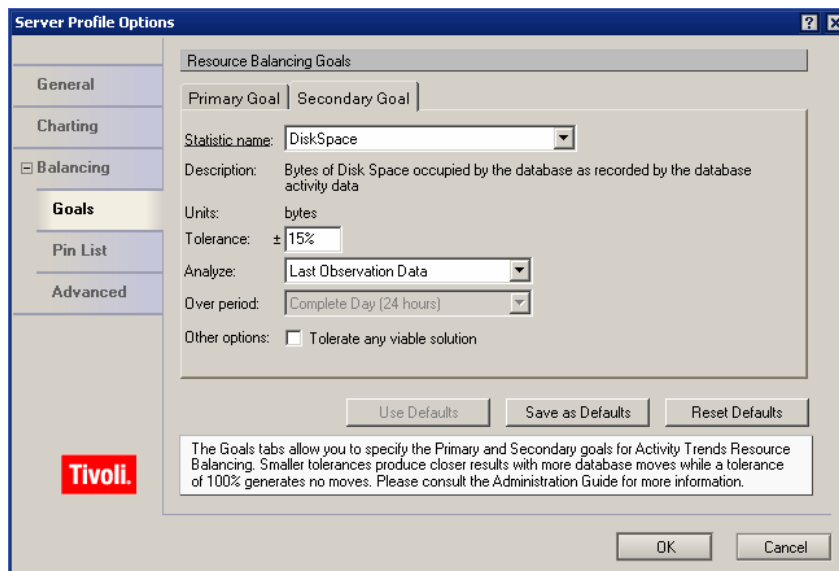


Рис. 539 Вторичная цель балансировки

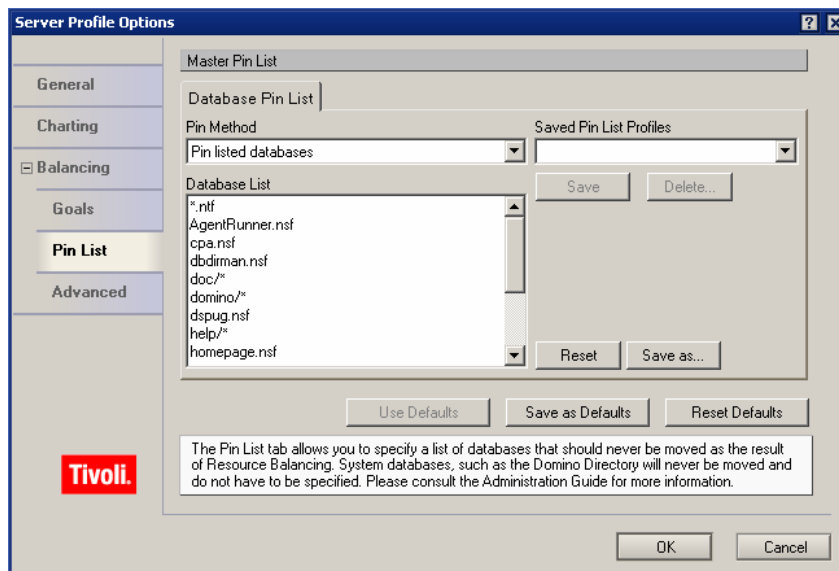


Рис. 540 Список «закрепленных» баз

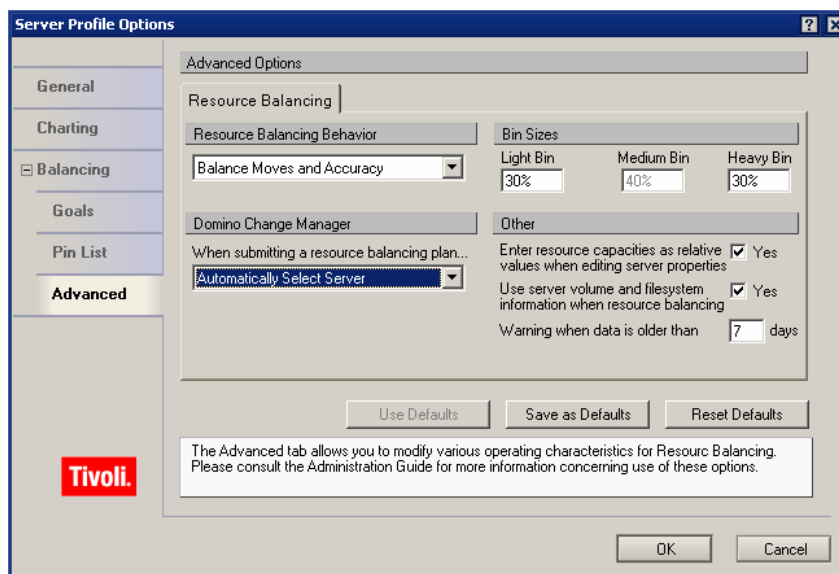


Рис. 541 Advanced

1.61.10.2. 1.1.10.2. Activity Trends Analysis - анализ тенденций

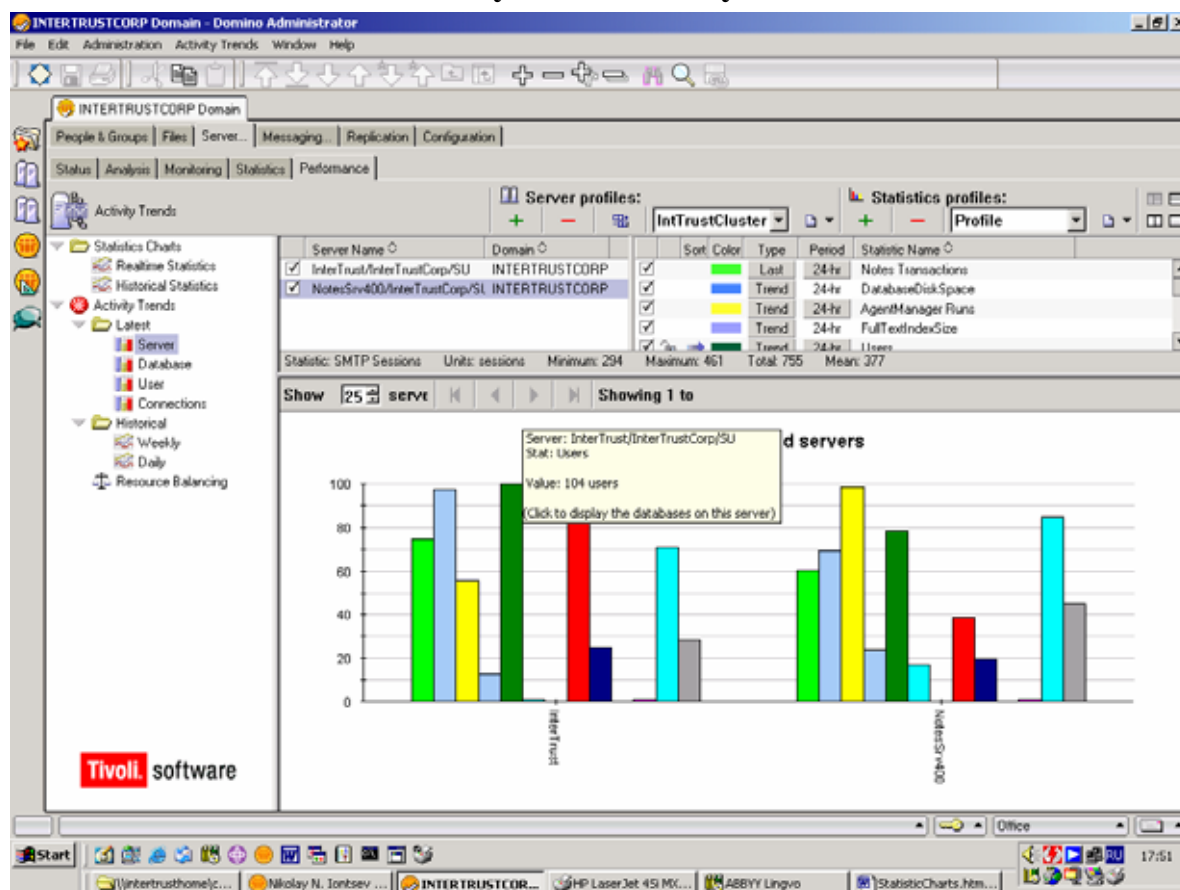


Рис. 542 Характеристики использования серверов

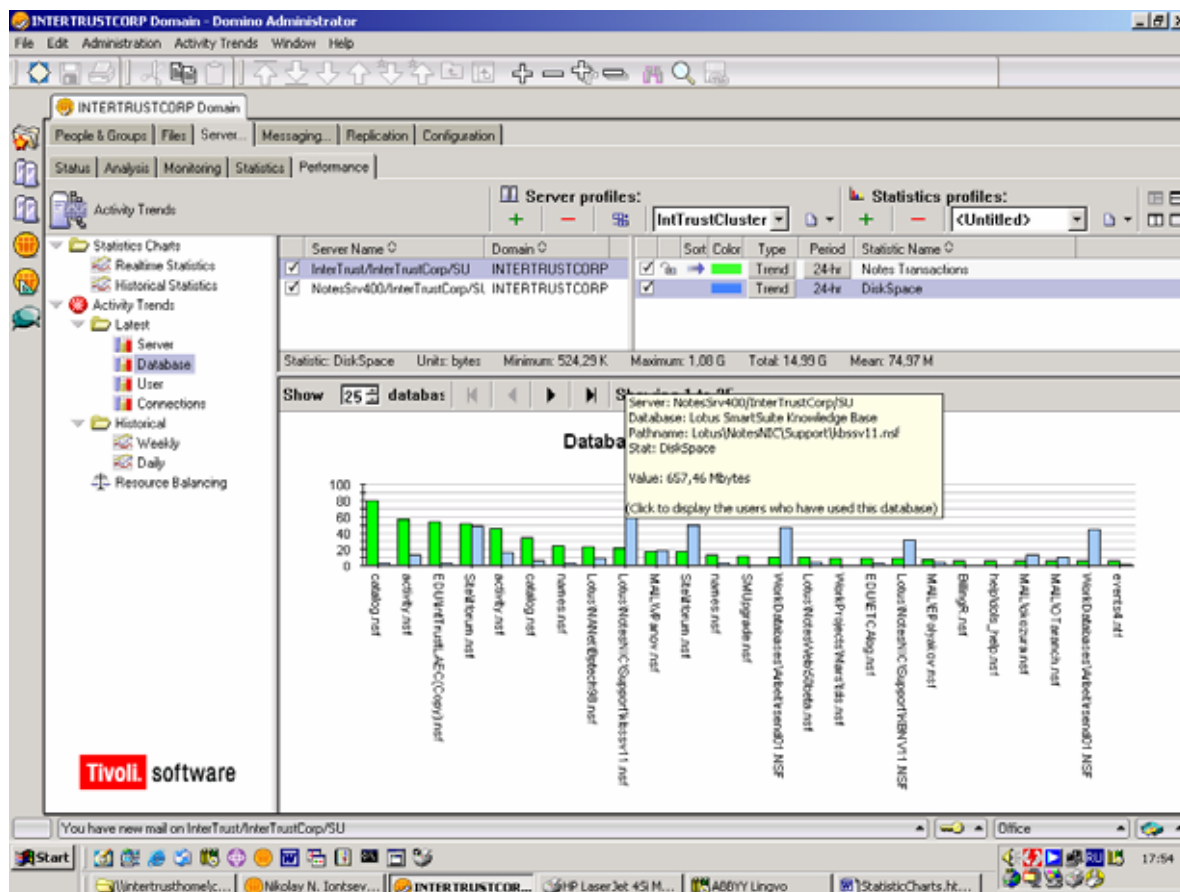


Рис. 543 Использование баз

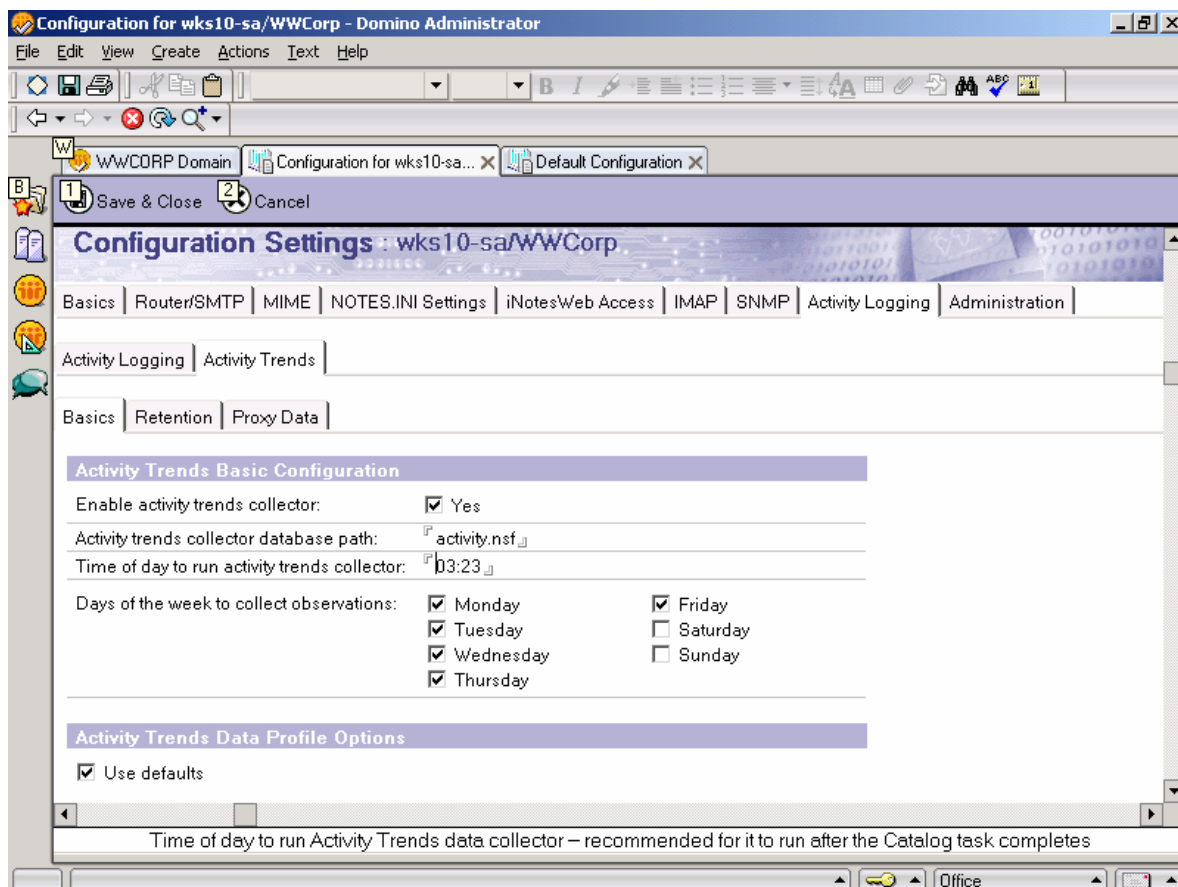


Рис. 544 Активность пользователей (и серверов при репликациях)

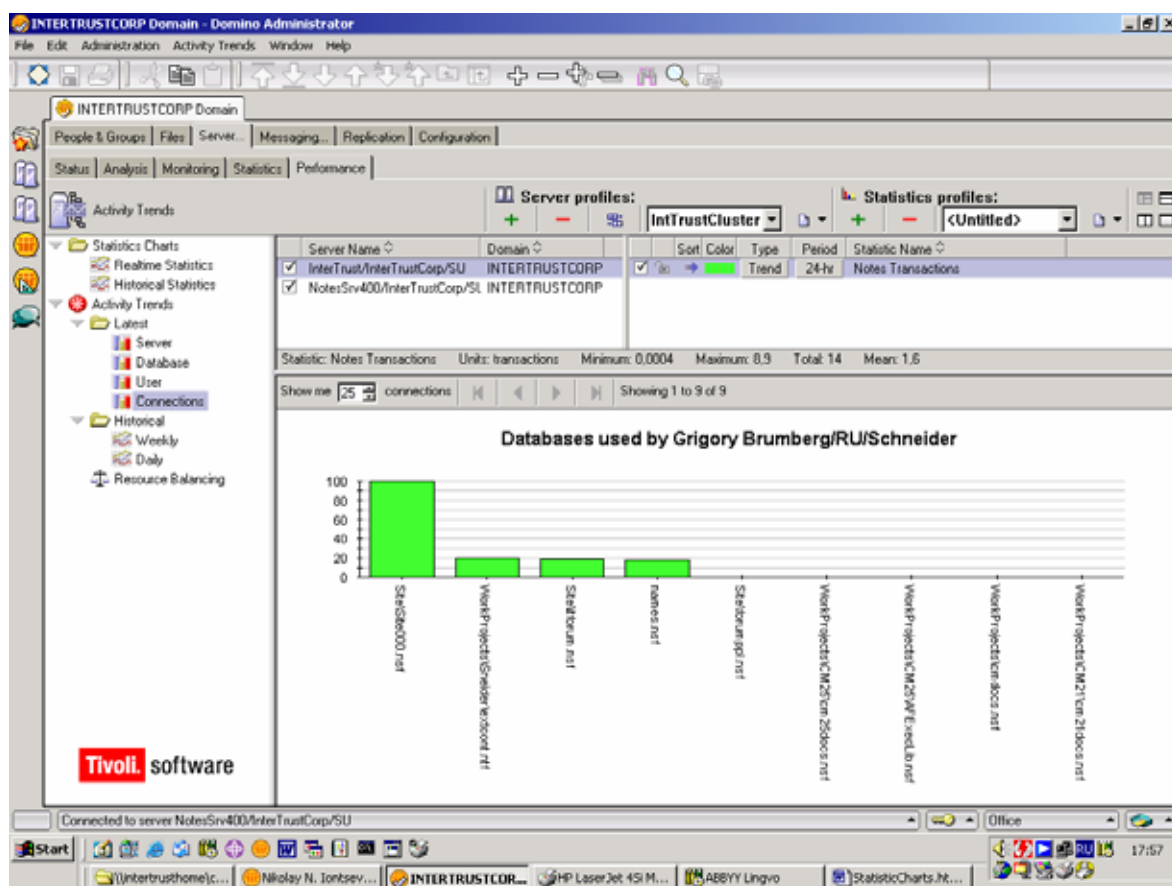


Рис. 545 Активность конкретного пользователя

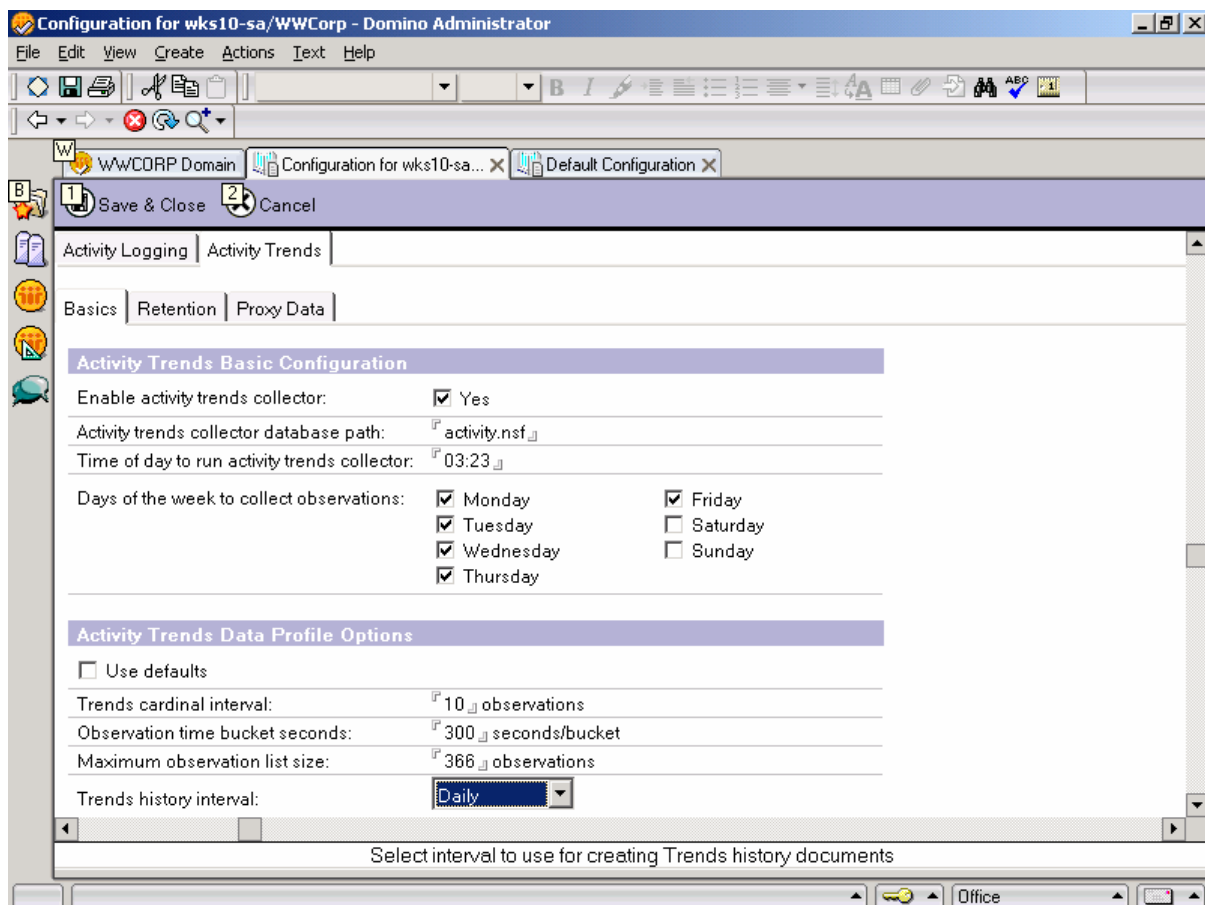


Рис. 546 Тенденции характеристик по неделям (количество транзакций)

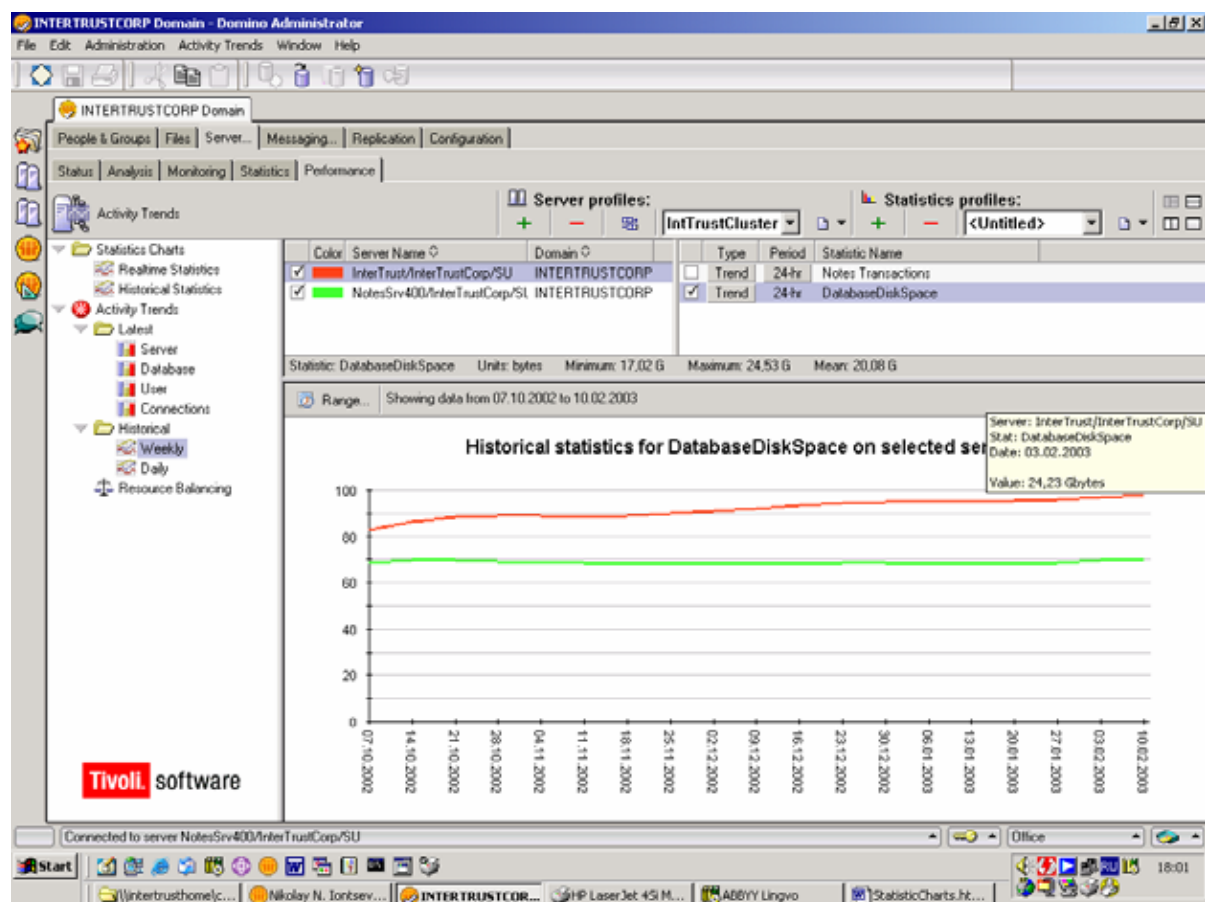
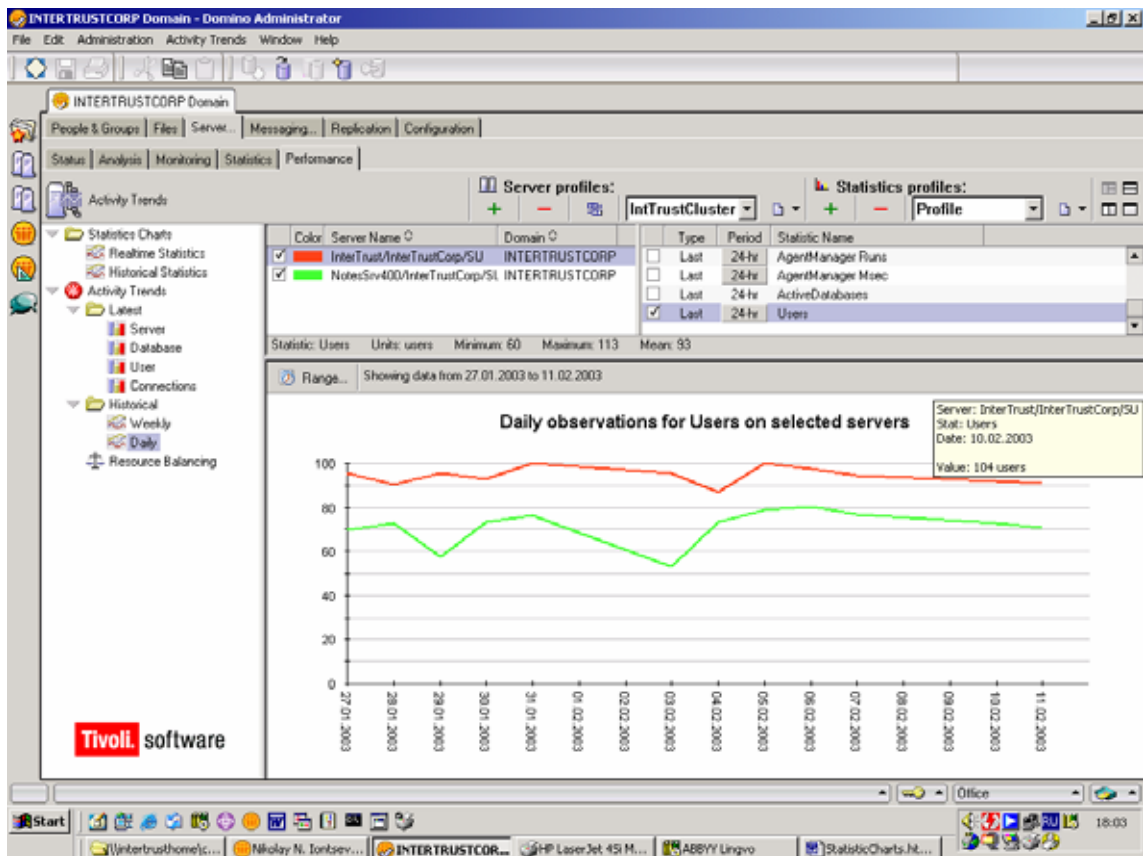
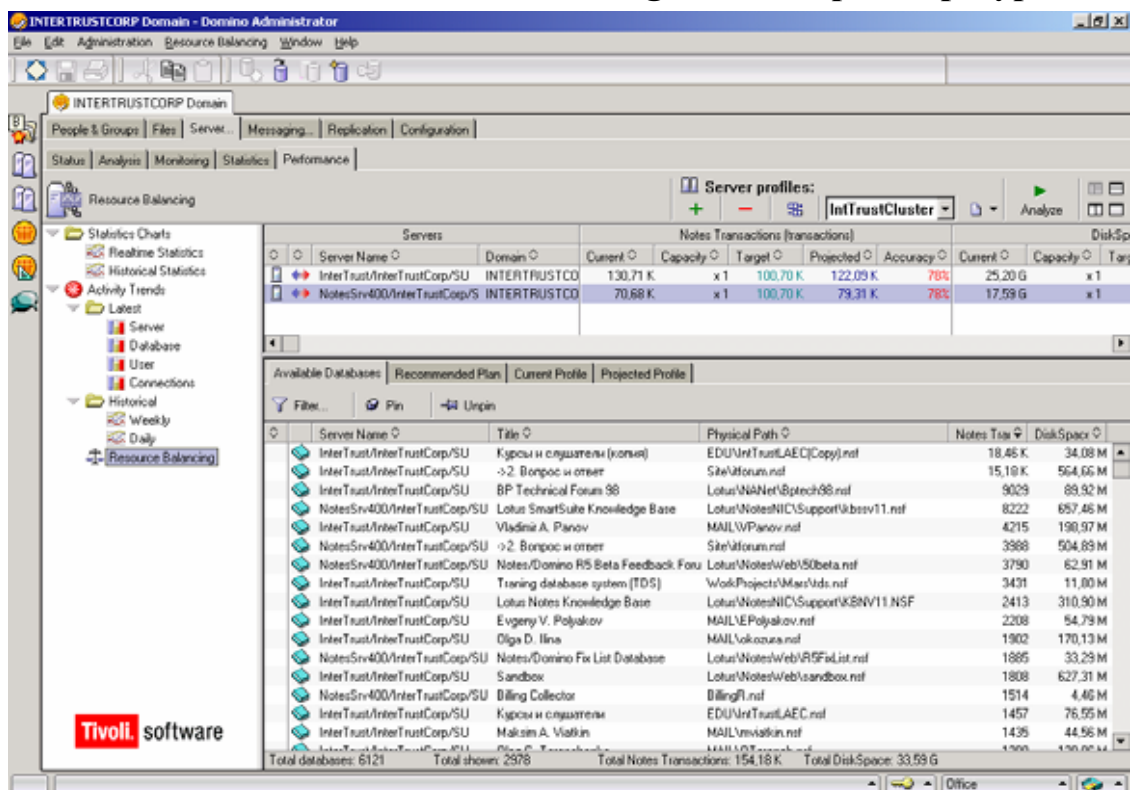


Рис. 547 Тенденции характеристик по неделям (место на дисках)



1.61.10.3. 1.1.10.3. Resource Balancing - балансировка ресурсов



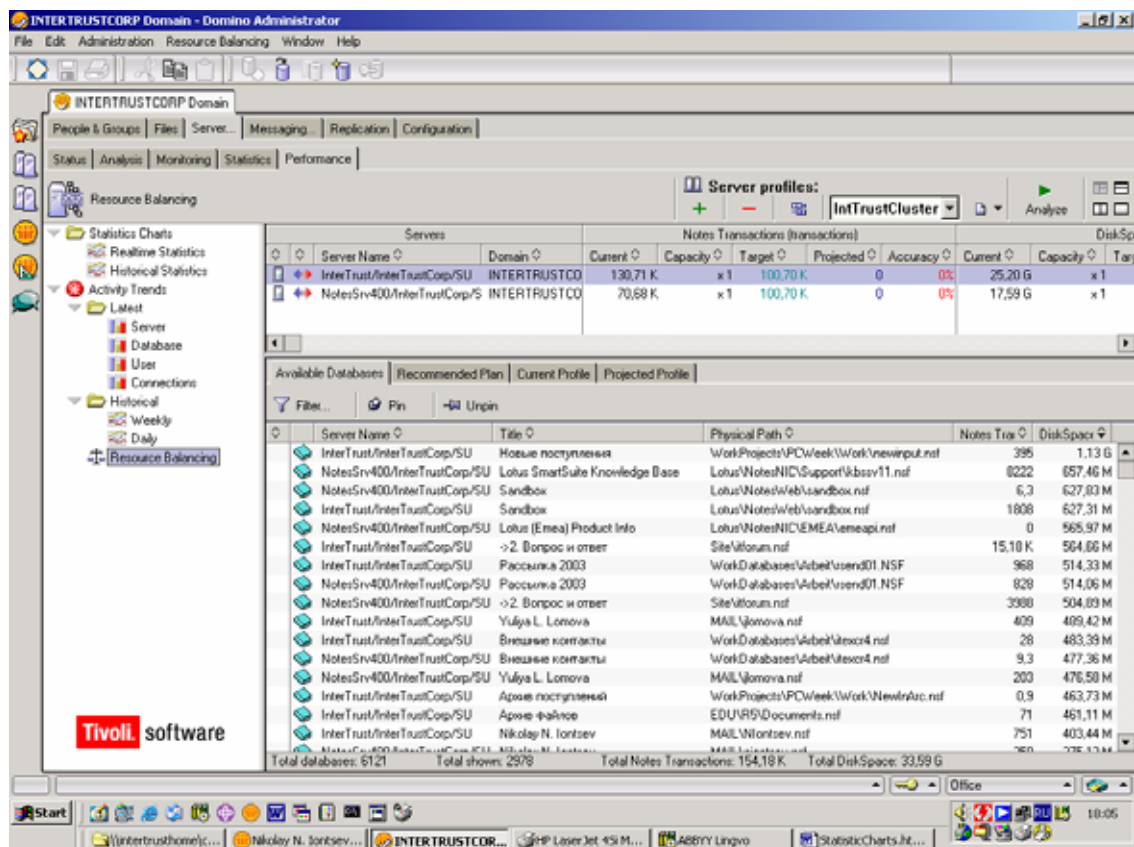


Рис. 550 ... и, во-вторых, дисковое пространство. Нажимается кнопка Analyze...

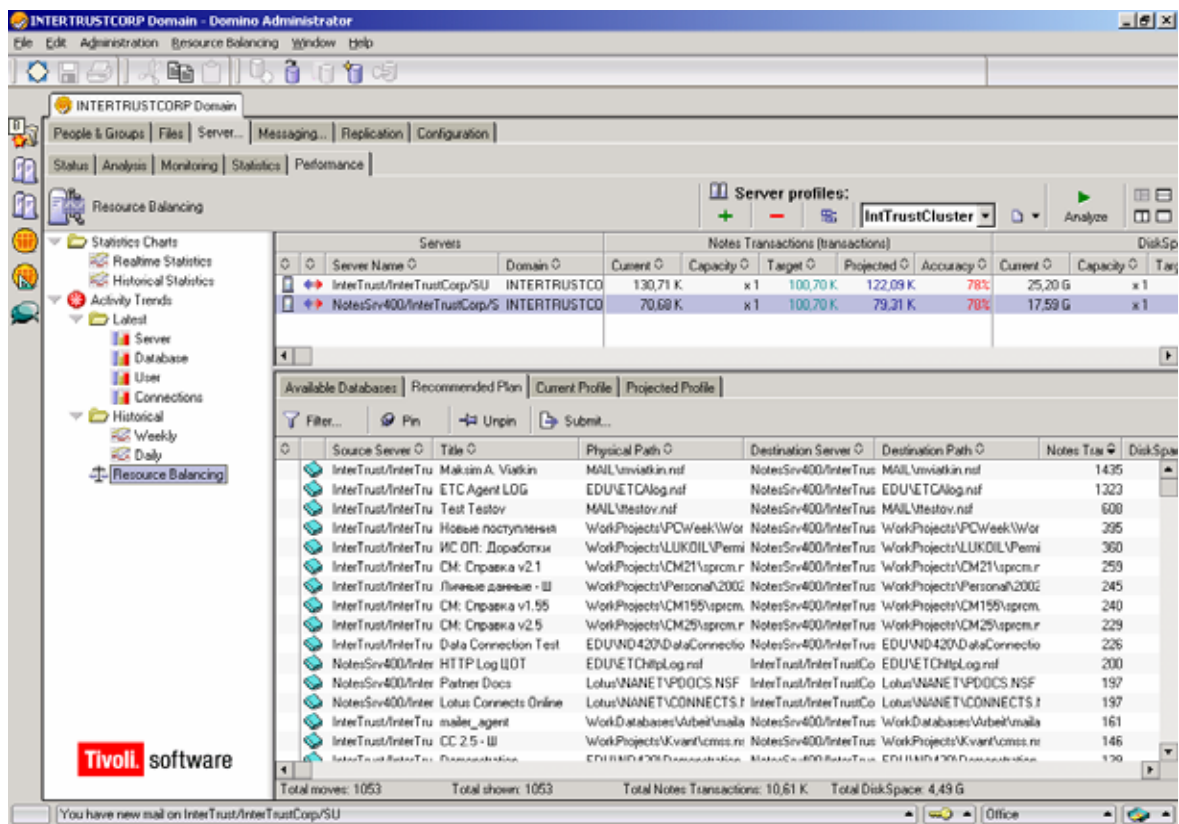


Рис. 551 Нам предлагается следующий план переноса баз...

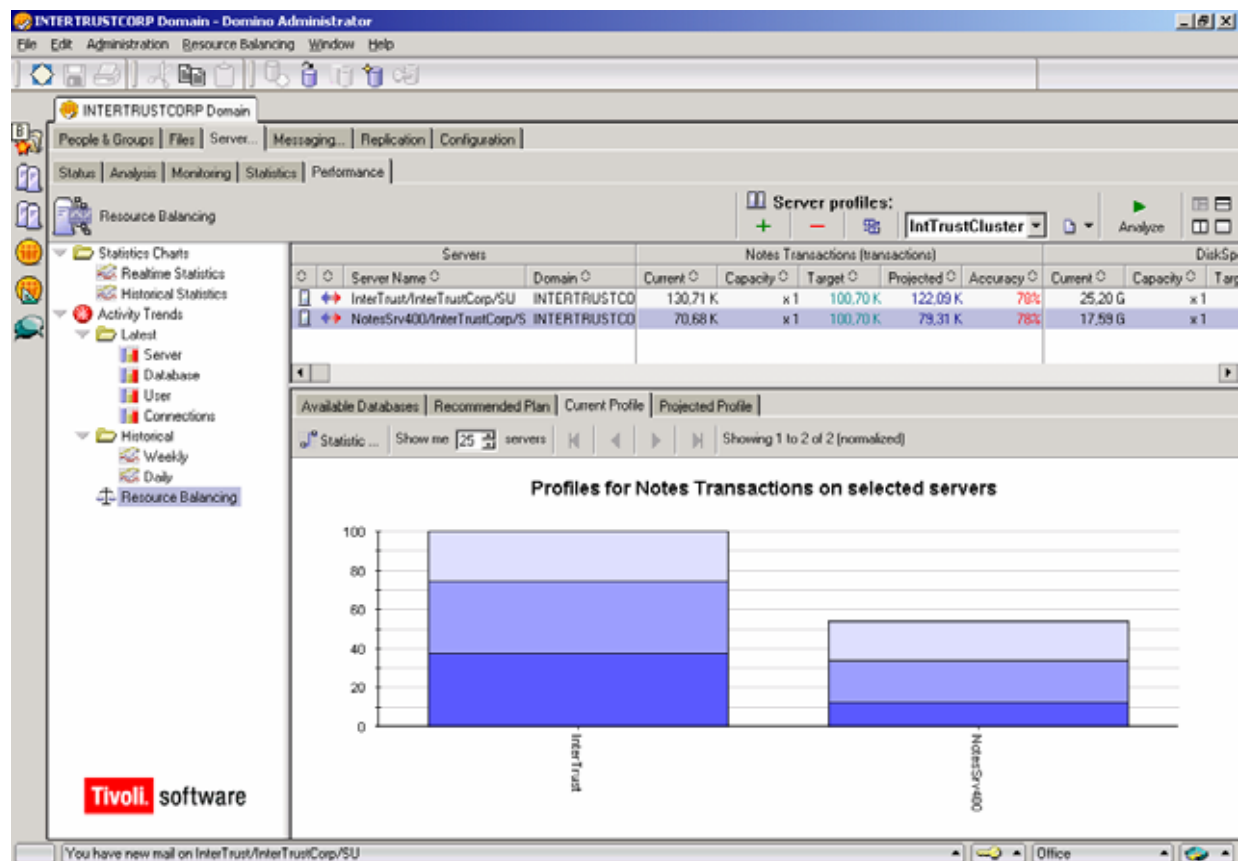


Рис. 552 Текущее состояние таково

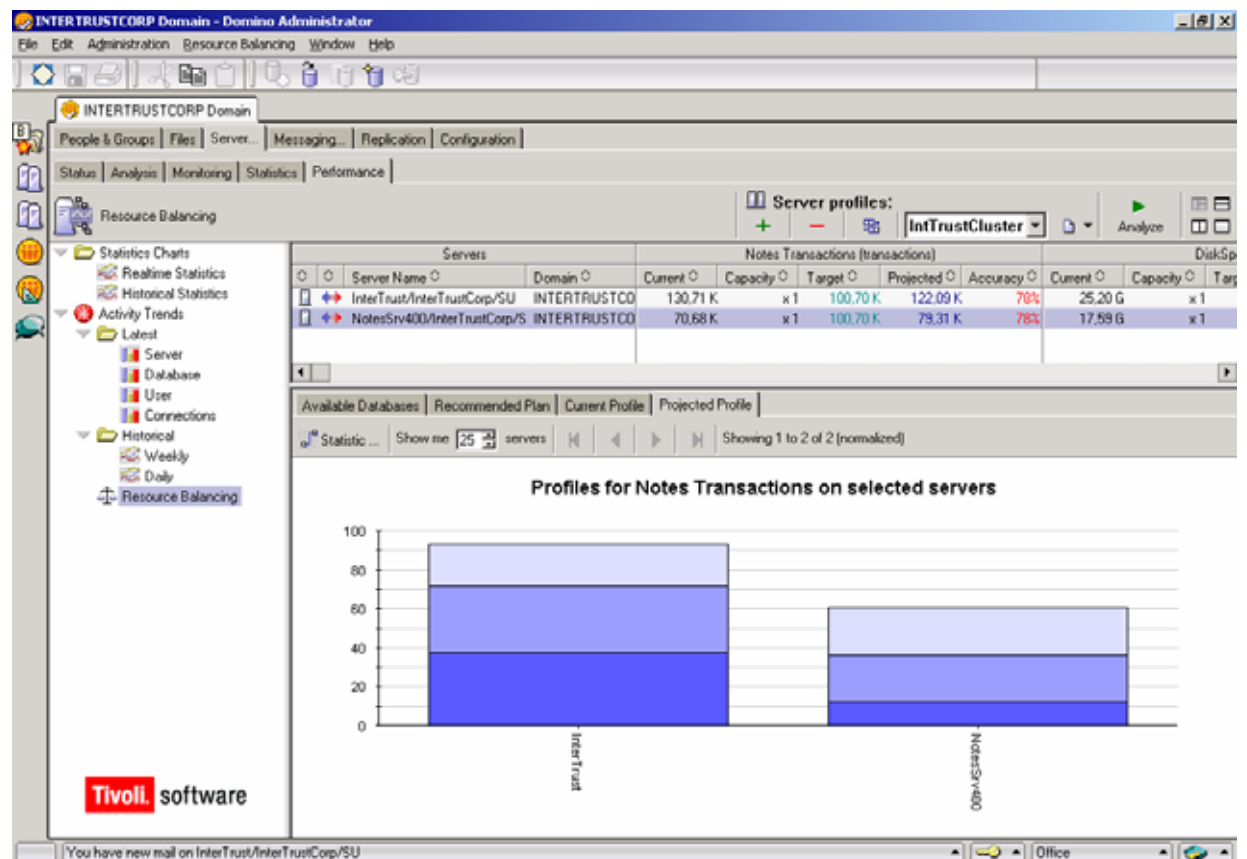


Рис. 553 В результате переноса баз ожидается следующий результат

Допустим, цель была сформулирована разумно и предложенный план приемлем. Как его реализовать? Замысел разработчиков продукта таков...

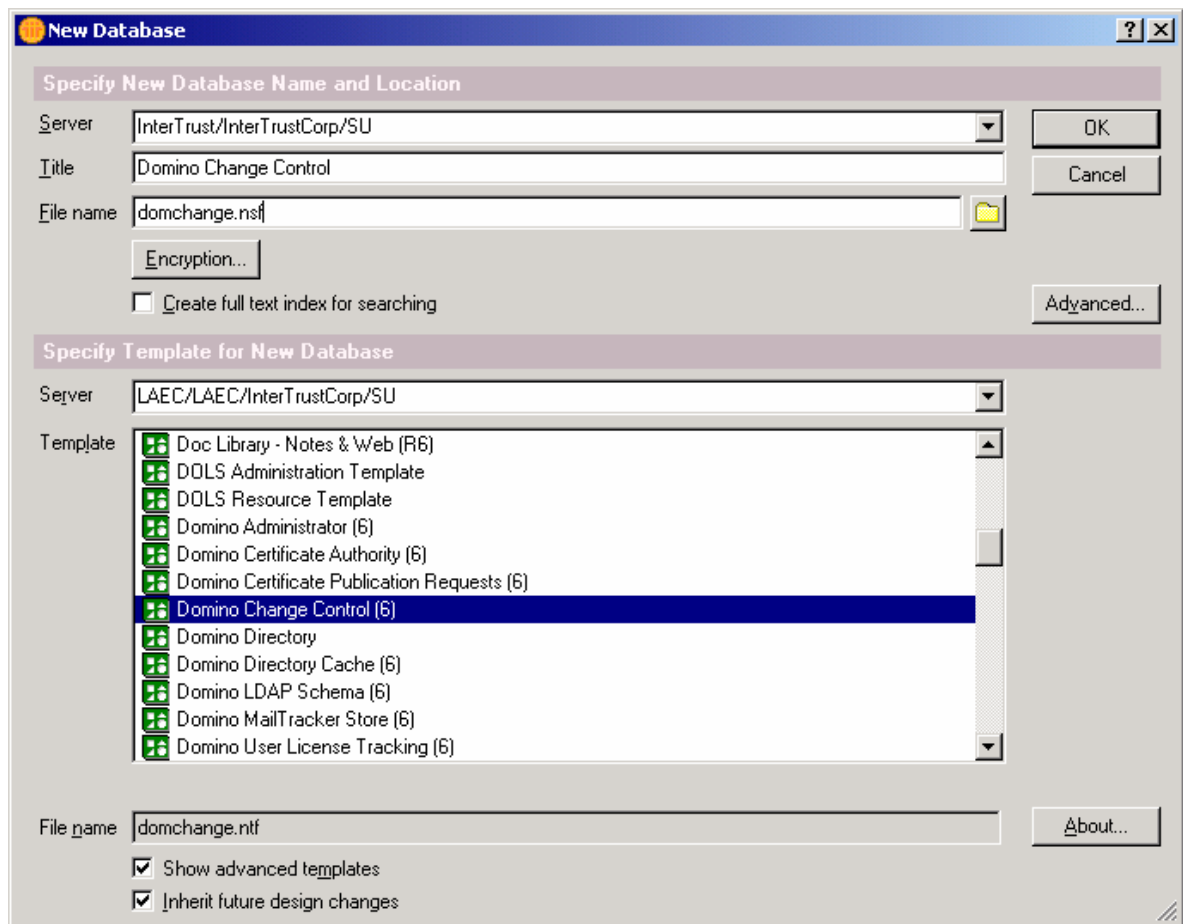


Рис. 554 Создать базу *domchange.nsf* на сервере. Указать это в настройках (Рис. 541)...

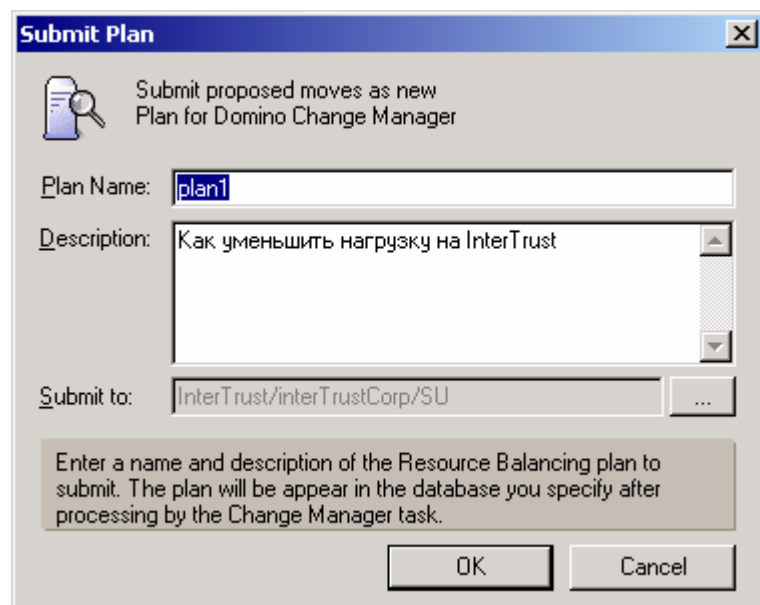


Рис. 555 Выбрав в меню *Resource Balancing – Submit Plan* или нажав кнопку *Submit*, передать план переноса баз в базу *domchange.nsf*

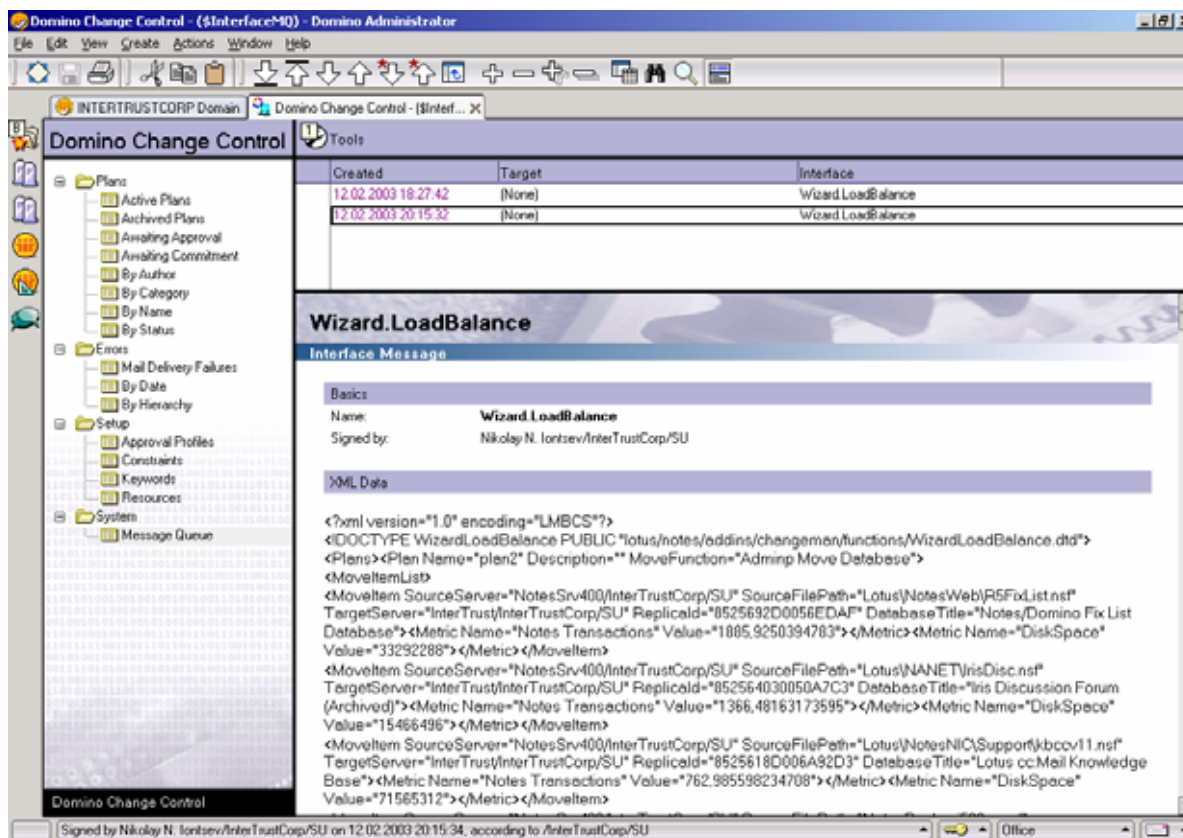


Рис. 556 База domchange.nsf, открыт только что переданный в нее план

Данная база позволяет согласовать выполнение переноса баз между людьми, во времени и с учетом прочих ограничений. Откройте документ Using Domino Change Control этой базы, чтобы убедиться в этом. После согласования процесс переноса может быть осуществлен программой Domino Change Manage с привлечением программы ADMINP.

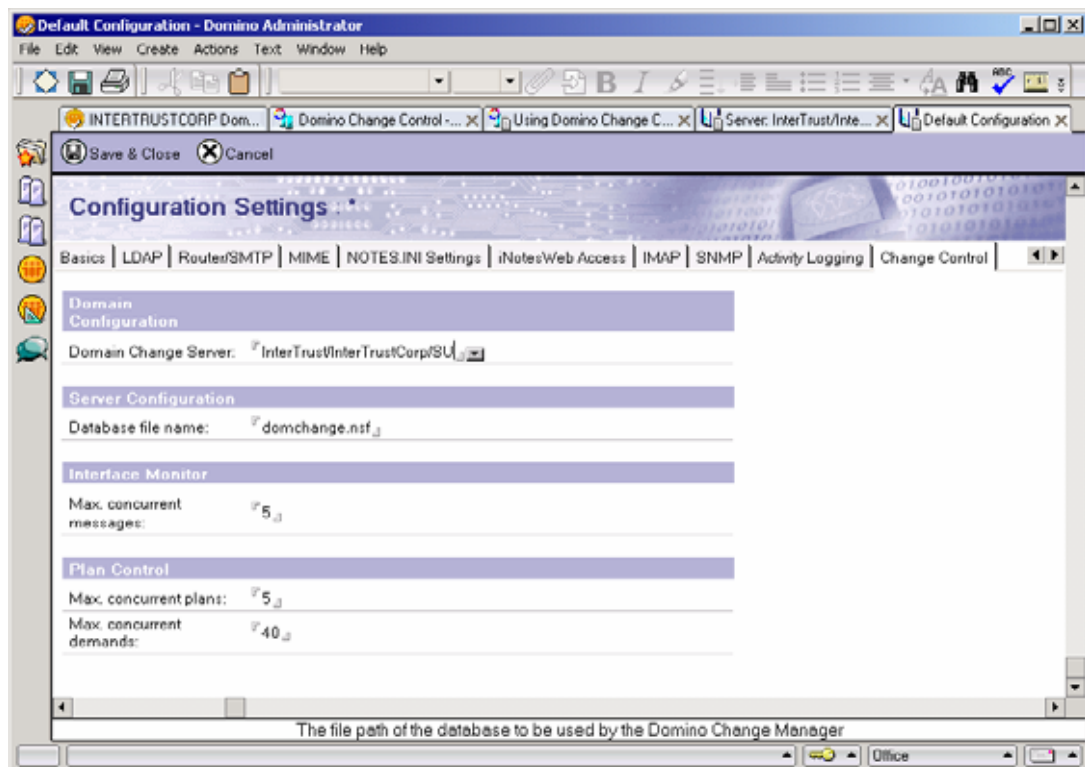


Рис. 557 Domino Change Manage настраивается в документе Server configuration для всех серверов и запускается как *runjava ChangeMan*

Таким образом, мы наблюдаем достаточно мощный инструмент для планирования размещения баз по серверам. Критерии и желаемые цели могут выбираться самые разные...

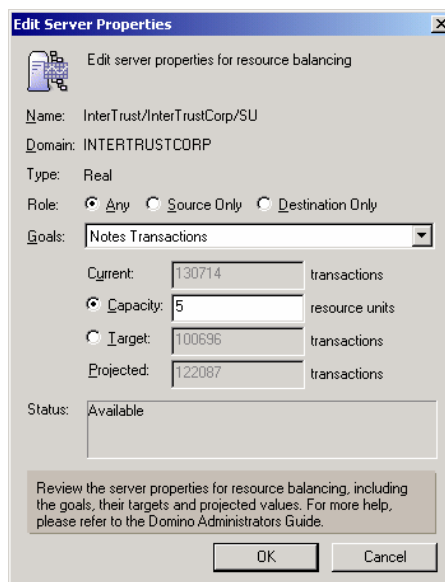


Рис. 558 Пример уточнения желаемой цели – поскольку компьютеры, несущие рассмотренные нами выше серверы Domino, в действительности существенно разной производительности, выполняем не балансировку 1:1, а наоборот увеличиваем нагрузку на более мощный и «недорабатывающий» сервер, разгружая при этом более слабый...

Можно так же добавлять Phantom server и выяснять, к чему хорошему может привести добавление еще одного сервера. Но все это естественно требует неспешного домашнего анализа.

1.62. 1.1. Репликации между серверами

- • Репликации баз Domino
- • Программа Replicator (REPLICA)
- • Документ Connection
 - • Способы установления соединений
 - • Устранение проблем установления соединений с серверами
 - • Поля, непосредственно относящиеся к репликациям
- • Алгоритм репликаций
- • Разрешение репликационных конфликтов
- • Использование истории репликаций
- • Выбор подмножества документов для репликаций
- • Обсуждение различных топологий для репликаций
- • Создание и использование групп при репликациях между серверами
- • Расписание репликаций
- • Мониторинг расписания репликаций
- • Поиск и устранение проблем при репликациях
 - • Устранение проблем, возникающих из-за невозможности серверов читать документы (поля типа Readers)
 - • Координация Purge Interval (время жизни документа и replication stub) и частоты репликаций
 - • Проверка доступа сервера по ACL базы (Effective Access tool)
- • Репликации между клиентом и сервером
- • Устранение проблем при установлении соединений с серверами и репликациях

1.62.1. 1.1.1. Создание реплики базы

Кто может создавать реплики баз на сервере? Не все, а только те, кто перечислен (явно или как член группы) в поле с меткой Create replica databases: документа Server из Каталога Domino.

Для создания реплики базы выберите из меню **File - Replication - New Replica...** В массовом порядке создавать реплики с сервера на сервер удобнее делать из клиента Администратора с закладки Files.

Копия базы данных, выполненная средствами операционной системы, будет иметь тот же идентификатор реплики, что и оригинал, поскольку само значение идентификатора реплики хранится в файле базы. На практике в ряде случаев администраторы предпочитают создавать реплики баз именно путем их копирования как файлов. Однако во избежание возможных проблем, связанных с одновременной работой с файлом базы из нескольких приложений, рекомендуется перед созданием «физической копии» останавливать сервер.

1.62.2. 1.1.2. Репликации и серверная задача Replicator

1.62.2.1. 1.1.2.1. Схема Pull-Pull

Хотя термин «репликация» (replication) подразумевает двунаправленный процесс обмена изменениями, серверная задача «репликатор» (Replicator), работая по схеме Pull-Pull (pull – «притягивать», а Pull-Pull - «принять-принять»), только принимает измененные

документы с другого сервера. Репликация становится двунаправленной, когда репликатор на втором сервере начинает прием изменений с первого, инициировавшего этот процесс сервера. На втором сервере репликатор первого сервера «обслуживается» задачей Database Server, как обычный пользователь. Существенно то, что один репликатор одновременно может принимать изменения только с одного сервера, тогда как задач Database Server на сервере запускается столько, сколько необходимо (в пределах «физических возможностей» компьютера, несущего сервер). В результате сервер может поддерживать ряд одновременных процессов приема изменений с него репликаторами других серверов, но сам может принимать изменения одним репликатором одновременно только с одного сервера. Чтобы репликация стала двунаправленной (Pull-Pull), инициировавший ее сервер посылает на вызванный сервер запрос на прием изменений «от себя». Этот запрос поступает в очередь репликатора вызванного сервера.

При репликации по локальной сети запрос на прием изменений репликатором другого сервера делается только по окончании приема изменений инициировавшим репликацию сервером, так что процессы «приема изменений» обоими серверами происходят не одновременно. Это, во-первых, минимизирует нагрузку на каждый сервер в ходе репликации (репликация интенсивно загружает компьютер сервера), и, во-вторых, способствует недопущению пиков сетевого трафика.

При репликации по модемному соединению или сети X.25 такой запрос выполняется практически сразу после установления связи, так что оба сервера принимают изменения друг от друга одновременно. Поскольку такой канал связи - типично «узкое» место, параллельная работа репликаторов способствует выполнению репликации за наименьшее время при наиболее полной загрузке канала связи между серверами.

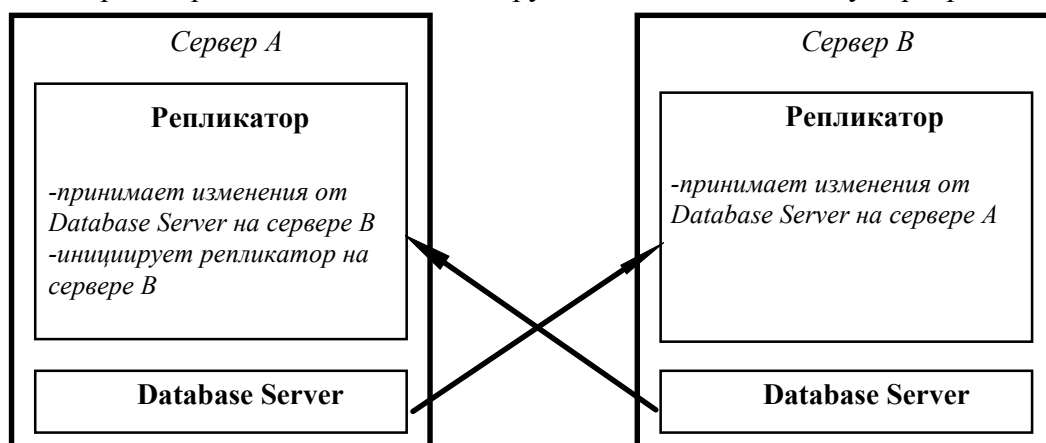


Рис. 559 Репликация по схеме «Pull-Pull»

Репликатор может иметь в очереди до 5 запросов на репликацию (это запросы от других серверов или из-за перекрытий в расписании репликаций). Все запросы сверх пяти игнорируются.

Схема Pull-Pull являлась стандартом в Notes версий 3.x. В настоящее время применяется редко.

1.62.2.2. 1.1.2.2. Схемы Pull-Push, Pull-only, Push-only

В некоторых случаях может быть целесообразно изменить принцип работы репликатора: вместо схемы Pull-Pull применить схему Pull-Push или «односторонние» схемы Pull-only или Push-only. Выбор схемы репликации выполняется в документе Connection (поле Replication Type:) или в зависимости от команды консоли, осуществляющей репликацию (PULL - схема Pull-only, PUSH - схема Push-only, REPLICATE - схема Pull-Push). В настоящее время схема Pull-Push - стандарт.

- • **Pull-Push** («принять-затолкнуть»). Двусторонний процесс, полностью реализуемый репликатором на вызывающем сервере. Сначала репликатор вызывающего сервера принимает

изменения с вызванного сервера, затем «заталкивает» свои изменения на вызванный сервер. На вызываемой стороне работу поддерживает задача DataBase Server.

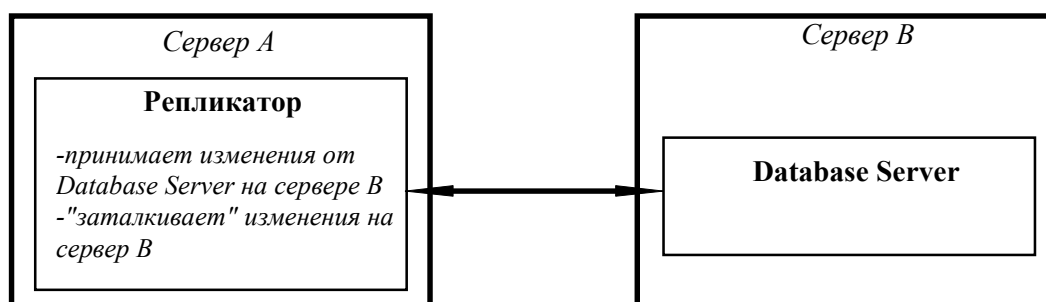


Рис. 560 Репликация по схеме Pull-Push

- • **Push-only** («только затолкнуть»). Односторонний процесс, в котором вызывающий сервер только «заталкивает» изменения на вызванный сервер.
- • **Pull-only** («только принять»). Односторонний процесс, в котором вызывающий сервер только принимает изменения с вызванного сервера.

1.62.2.3. 1.1.2.3. Сравнение схем Pull-Push и Pull-Pull

В широко распространенной конфигурации «hub-spoke» (по нашему «звезда») имеется один или несколько серверов, которые являются «поставщиками данных» (**hub-серверы**), и много серверов, которые занимаются в основном приемом «заказанных ими» данных с hub-серверов, хотя могут также передавать данные на hub-серверы (это **spoke-серверы**).

Преимущества схемы Pull-Push по сравнению с Pull-Pull

При использовании репликаций по схеме Pull-Push существенно упрощается администрирование hub-серверов:

- • администратор hub-сервера не планирует связь с каждым spoke-сервером;
- • репликатор hub-сервера не вовлечен в репликационные события, инициированные spoke-серверами, тогда как многие spoke-серверы могут одновременно реплицировать данные с hub-сервера.

Схема Pull-Push обычно позволяет более быстро завершить репликационный цикл, т.е. выполнить репликации между hub-сервером и каждым из его spoke-серверов. При репликациях по схеме Pull-Pull spoke-сервер принимает изменения с hub-сервера, а затем репликатор hub-сервера принимает изменения от spoke-сервера. Но в этом случае hub-сервер каждым своим репликатором одновременно может принимать изменения только от одного из spoke-серверов. При использовании схемы Pull-Push многие spoke-серверы могут одновременно принимать изменения с hub-сервера и «заталкивать» их на hub-сервер.

Недостатки схемы Pull-Push по сравнению с Pull-Pull

Документы Connection будут находиться на разных spoke-серверах. Если таких серверов много и они из разных доменов, может оказаться организационно трудно составить «равномерное» расписание, если только на hub-сервере не имеются реплики адресных книг всех участвующих в репликациях доменов.

Hub-сервер не будет иметь информации о репликационных событиях в своем протоколе работы (LOG.NSF) - с «его точки зрения» имеет место лишь доступ к находящимся на нем базам. Для анализа возможных проблем в конфигурации «hub-spoke» администратор hub-сервера будет вынужден просмотреть большее количество протоколов работы spoke-серверов, чем в случае репликаций по схеме Pull-Pull.

1.62.3. 1.1.3. Репликации между сервером и станцией Notes

На станции нет явного аналога серверной задачи Replicator. Программное обеспечение станции при репликации сначала принимает изменения с сервера, а затем отправляет измененные документы на сервер (аналог схемы Pull-Push). Репликация между станцией и сервером для конкретной базы может быть инициирована со станции вручную выбором File - Replication - Replicate в основном меню или Replicate во всплывающем меню базы. Однако значительно более удобно пользоваться мощными возможностями закладки Replicator.

Возможны и фоновые репликации по расписанию. Расписание фоновых репликаций определяется в документах Location из персональной адресной книги.

1.62.4. 1.1.4. Как отождествляются между собой документы в разных репликах и как происходит удаление документов при репликации

Подобно идентификатору реплики базы, каждый документ в любой базе Notes имеет свой универсальный идентификатор документа (**DocumentUniqueID** или **UNID**). Вы можете «увидеть» универсальный идентификатор документа в окне свойств этого документа.

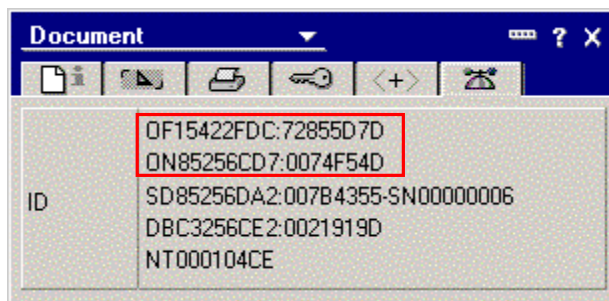


Рис. 561 Универсальный идентификатор документа обведен рамкой

Универсальный идентификатор документа используется при репликациях для нахождения «одинаковых» - имеющих один и тот же универсальный идентификатор - документов в обеих репликах базы.

Если имеющийся в двух репликах документ был **модифицирован** в одной из реплик, остается по дате модификации выяснить более новую версию и заменить ею документ в другой реплике.

Если в одной из реплик появился **новый** документ, то у него свой универсальный идентификатор, а в другой реплике нет документа с таким же универсальным идентификатором, так что приходится добавить этот документ в другую реплику.

Если же документ присутствовал в обеих репликах, но затем был **удален** в одной из них, при удалении Notes заменяет этот документ на «deletion stub». **Deletion stub** (*stub* - пень, корень зуба, окурок, ам. корешок чековой книжки) можно рассматривать как документ с тем же универсальным идентификатором, который имел удаленный документ, с датой модификации, соответствующей моменту удаления, и не содержащий никаких полей данных. В соответствии со сказанным выше о модификации документа в одной из реплик при репликации «оставшийся от документа окурок» должен заменить в другой реплике «нормальный», но имеющий более раннюю дату модификации, документ.

«Окурок», как бы мал он ни был, занимает место в базе данных. Постепенно в базе происходит «накопление окурков». Для решения этой проблемы в репликационных установках каждой базы присутствует параметр, называемый «интервалом удаления» - это количество дней **XXX** в поле с меткой **Remove documents not modified in the last: XXX days**. По умолчанию параметр принимается равным 90 дней, но может быть изменен. В базах данных, находящихся как на сервере, так и на станции, в некоторые моменты времени выполняется удаление «окурков». В базах, находящихся на сервере, процесс удаления «окурков» запускается с интервалом в 1/3 от интервала удаления (по умолчанию раз в каждые 30 дней). При этом удаляются только те «окурки», которые появились в базе

раньше, чем текущее время (когда выполняется процесс удаления «окурков») минус интервал удаления.

Будьте внимательны: речь шла только о поле с меткой **Remove documents not modified in the last: XXX days**, содержащем количество дней XXX, а вовсе не о выборе самой опции **Remove documents not modified in the last: XXX days**. Если вы выберете эту опцию, то в базе станут автоматически удаляться документы, которые не изменились за последние XXX (интервал удаления) дней. Процесс же удаления «окурков» функционирует независимо от того, выбрана эта опция или нет, и не имеет к ней никакого отношения.

Возможна ситуация, когда «окурки» будут удалены до того, как произойдет репликация. Например, если базы реплицируются один раз в неделю, а интервал удаления равен 3 дня, то процесс удаления «окурков» запускается ежедневно, устраняя при этом «окурки с возрастом» не менее трех дней. При этом репликатор может вновь восстанавливать удаленный в одной реплике документ из другой реплики. Так что в случае, если такое явление происходит, увеличьте интервал удаления и, тем самым, интервал запуска процесса удаления «окурков».

1.62.5. 1.1.5. Репликационные установки для базы данных

Репликационные установки для базы данных задаются в диалоговом окне, получаемом выбором в меню **File - Replication - Settings** (или множеством других способов). Чтобы изменять репликационные установки, вы должны иметь доступ менеджера к базе. Только для изменения формул селективной репликации вам достаточно доступа дизайнера.

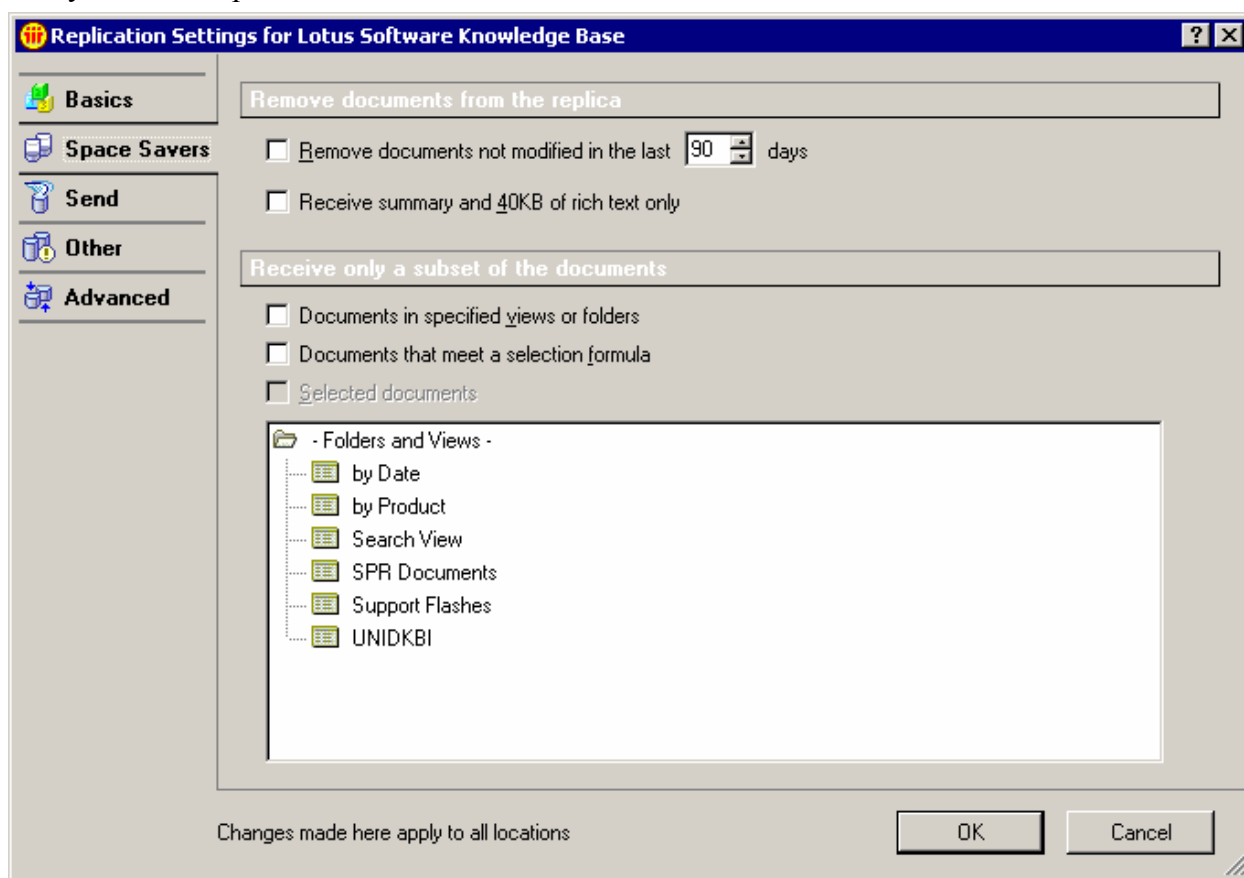


Рис. 562 Закладка окна репликационных установок, отвечающая за «сохранение дискового пространства»

- **Remove documents not modified in the last: XXX days.** Установка опции «заставляет» автоматически удалять из данной базы все документы с датой сохранения или модификации

более ранней, чем XXX дней назад от текущей даты. Документы, удаленные из данной реплики базы на основании этой установки, будут удалены в других репликах распределенной базы, если только вы не выбрали на закладке Send дополнительно опцию **Do not send deletions made in this replica to other replicas**. Если опция **Remove documents not modified...** не выбрана, «автоудаление» документов не выполняется, невзирая на значение XXX. Имеются нюансы, связанные с моментами выполнения «автоудаления». В частности, для баз на сервере условие «автоудаления» проверяется запускаемой ночью серверной задачей UPDALL, а на станции для локальных баз - в момент открытия базы.

Значение XXX из **Remove documents not modified in the last: XXX days** также определяет интервал запуска процесса удаления «окурков». Фактическое удаление «окурков» выполняется с периодом, равным 1/3 интервала удаления XXX. Так, если интервал удаления равен 30 дней, то тогда каждые 10 дней выполняется удаление всех «окурков», возраст которых более 30 дней.

- • **Receive only a subset of the documents.** Опция используется, если в данную реплику должны поступать не все документы, а только документы или из некоторых видов и папок, или удовлетворяющие заданной вами формуле отбора документов (если дополнительно выбрана опция **Select by formula**). Подробнее эти и другие опции, относящиеся к вопросу селективных репликаций, рассматривается в 7.13.11.

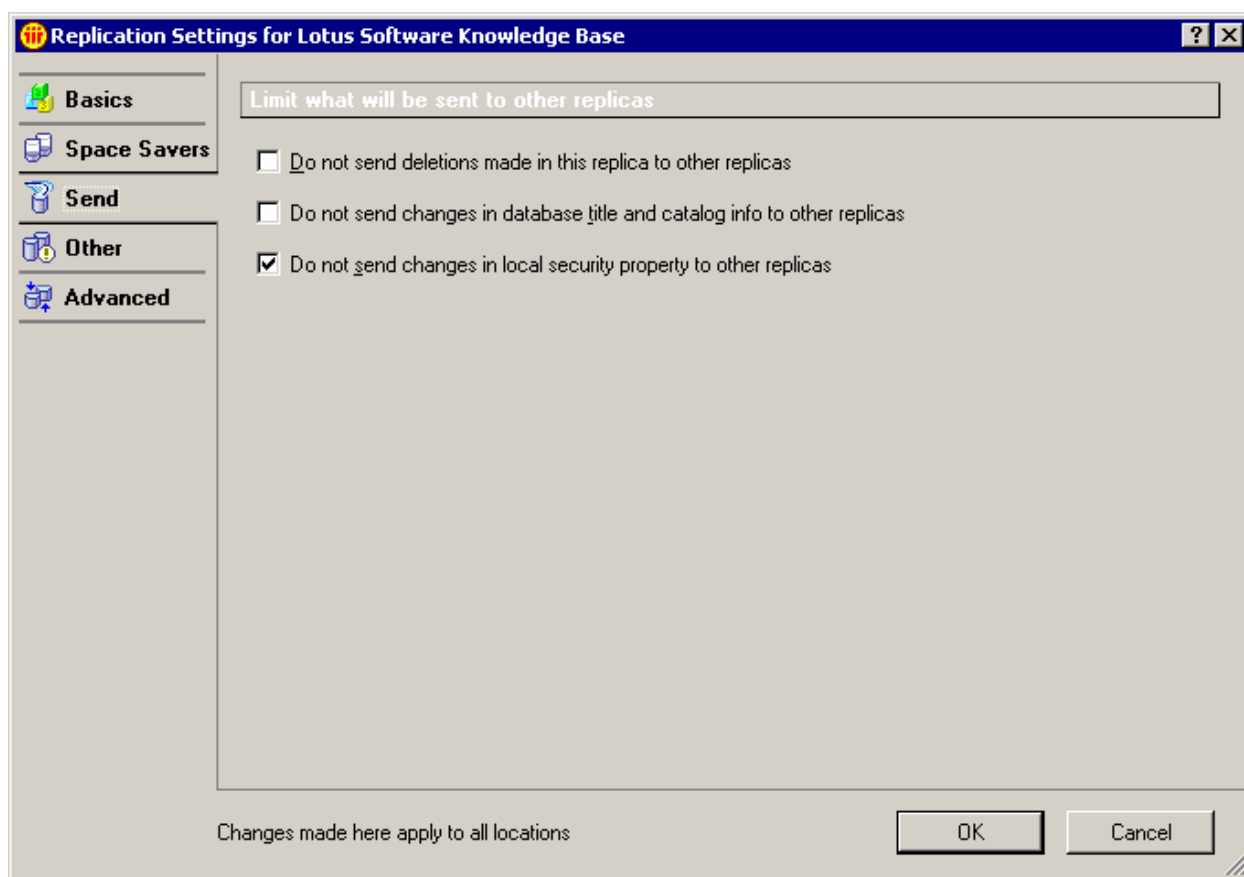


Рис. 563 Закладка окна репликационных установок, отвечающая за отправку документов из этой реплики в другие реплики

- • **Do not send deletions made in this replica to other replicas.** Выбор опции означает, что при репликации этой базы в ее другие реплики не должна передаваться информация об удаленных документах (т.е. «окурки»). В результате удаленные в этой реплике документы при репликации не вызовут удаления соответствующих документов в других репликах. Невозможно «описать множество» уже удаленных документов («множество окурков») с помощью формулы отбора. «Окурки» можно только не реплицировать в другие реплики, и это достигается выбором данной опции. Если же опция не выбрана, то появляющиеся после

удаления документов в этой базе «окурки» при репликациях попадают в другие реплики этой базы и вызывают в них удаления соответствующих документов.

- • **Do not send changes in database title & catalog info to other replicas.** Опция требует не изменять название базы и информацию о том, следует ли создавать документ об этой базе в базе CATALOG.NSF, в других репликах, если они изменились в данной. Если опция не выбрана, то самые последние изменения должны замещать более старые значения во всех репликах. Однако для этого дополнительно необходимо, чтобы сервер данной реплики имел в репликах на других серверах доступ дизайнера или выше.
- • **Do not send changes in local security proreprey to other replicas.** Подобно предыдущему, но в отношении репликации свойств, касающихся локальной безопасности этой реплики (поддержка локального функционирования списка управления доступом, локальное шифрование).

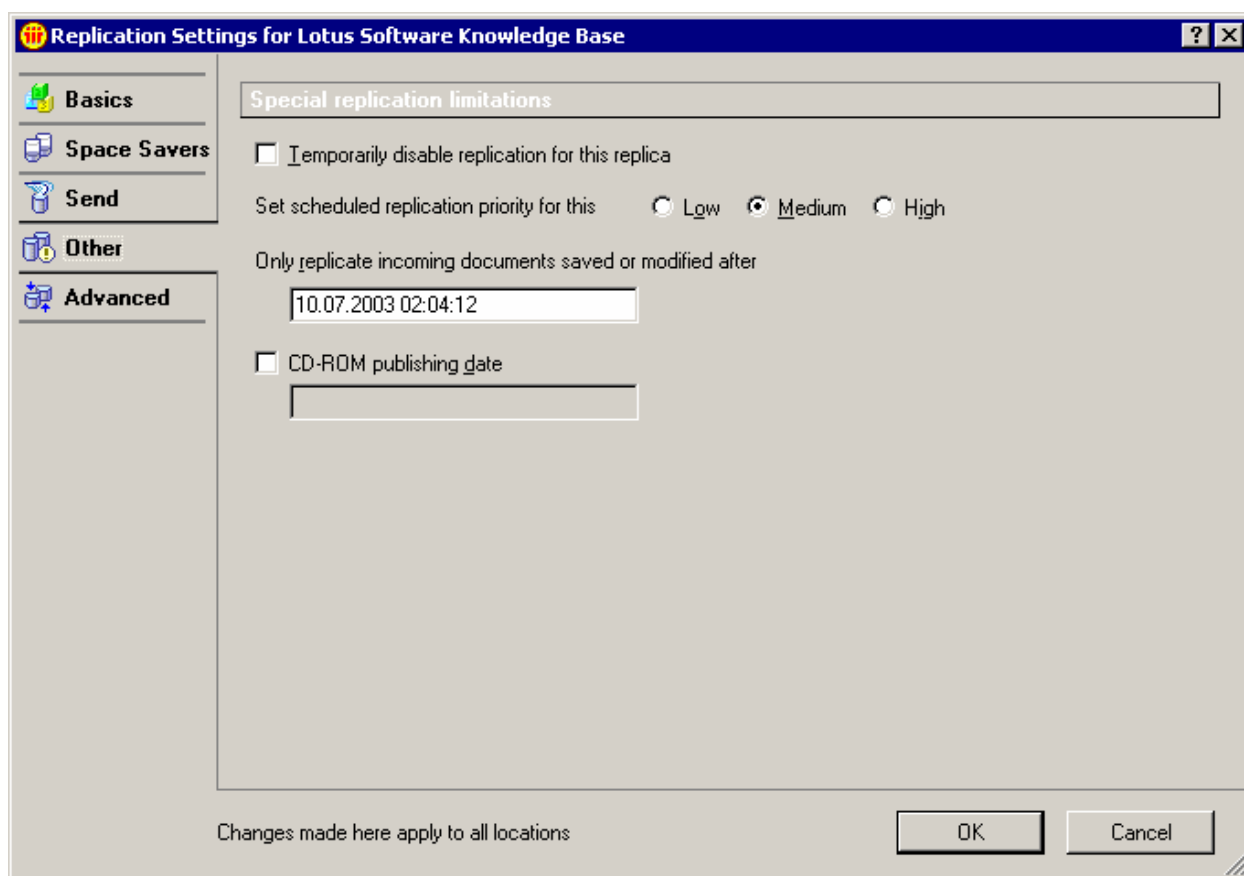


Рис. 564 Закладка дополнительных репликационных установок

- • **Temporary disable replication.** Выбор опции запрещает участие базы в любых репликационных процессах. Сервер выдает сообщение Replication is disabled for <имя>, а станция: Unable to Replicate with Server <имя>: None of the Selected Databases has a Replica on the Server. Опция может быть полезна администратору, если база по каким-то причинам оказалась поврежденной и требуется ее восстановление, прежде чем для нее будут возобновлены репликации.
- • **CD-ROM publishing date.** Если база данных поступила к вам на CD-ROM, после ее копирования на диск рекомендуется указать в этом поле «дату публикации» базы. Тогда при первой репликации базы с оригиналом на сервере поставщика на предмет участия в репликации будут просматриваться только документы, появившиеся после даты публикации, а не все множество документов (поскольку в историях репликаций в этот момент нет сведений о вашей копии). В результате первая репликация будет выполнена быстрее. Если же вам предстоит записать базу данных на CD-ROM, предварительно рекомендуется задать дату публикации базы, чтобы снять заботу об этом с потребителя.

Приоритеты баз (Scheduled replication priority), поле Only replicate incoming documents saved or modified after: (в версиях до 4.x и до сих пор по базе знаний известное как Cutoff Date), история репликаций и селективные репликации будут рассмотрены ниже.

1.62.6. 1.1.6. Планирование репликаций и приоритеты баз

Репликации между серверами не происходят автоматически, они должны быть запланированы. Расписание репликаций задается набором документов Connection в Каталоге Domino. Вы должны обычно составлять расписание репликаций так, чтобы только один из двух серверов выполнял вызов другого. Ситуация, когда оба сервера вызывают друг друга поочередно, в принципе допустима, но требует наличия двух согласованных документов Connection, тогда как обычно можно обойтись только одним.

Репликация может быть намечена на заданный отрезок времени с интервалом повторения или только на заданное время. Если вы намечаете репликацию только однократно на заданное время, вы должны задать интервал повторения равным «0». Если в документе Connection поле интервала повторения пустое, сервер принимает интервал повторения равным 60 минут.

1. Отрезок времени с интервалом повторения - 8:00-18:00 с инт. 180 мин.

$$\begin{matrix} R & & R & & R & & R \\ 8 & \_ & 9 & \_ & 10 & \_ & 11 & \_ & 12 & \_ & 13 & \_ & 14 & \_ & 15 & \_ & 16 & \_ & 17 & \_ & 18 \end{matrix}$$

Репликатор впервые вызывает другой сервер в 8:00. Если попытка неуспешна, он повторяет попытку соединения в течение интервала (180 мин.), пока она не будет успешной (см. ниже Randomized exponential backoff algorithm). Следующий вызов будет производиться **через 180 мин после успешного завершения репликации**. Такой вариант рекомендуется для баз, которые должны реплицироваться наиболее часто.

Server Connection : LAEC/ETC/InterTrust/RU to InterTrust/InterTrustCorp/SU

Basics | Replication/Routing | **Schedule** | Comments | Administration

Scheduled Connection

Schedule:	☒ ENABLED ☐
Connect at times:	☒ 00:00 - 23:59 ☐ each day
Repeat interval of:	☒ 60 ☐ minutes
Days of week:	☒ Sun, Mon, Tue, Wed, Thu, Fri, Sat ☐

Рис. 565 На отрезке времени с интервалом повторения 60 минут

2. Отрезок времени без интервала повторения - 8:00-18:00 с инт. 0 мин.

Репликатор впервые вызывает другой сервер в 8:00. Если попытка неуспешна, он повторяет попытку соединения в границах отрезка (до 18:00), пока она не будет успешной. После успешного соединения сервер не будет производить новых вызовов. Такой вариант рекомендуется для баз, которые должны реплицироваться со средней частотой.

3. Заданное время - 8:00 с инт. 0 мин.

Репликатор впервые вызывает другой сервер в 8:00. Если попытка неуспешна, он повторяет попытку соединения в течение часа, пока она не будет успешной (обычно не более 4 попыток). После успешного соединения сервер не будет производить новых вызовов. Такой вариант рекомендуется для баз, которые должны реплицироваться относительно редко.

4. Список заданных времен - 8:00 AM; 1:00 PM; 4:00 PM с инт. 0 мин.

Репликатор впервые вызывает другой сервер в 8:00 утра. Если попытка неуспешна, он повторяет попытку соединения в течение часа, пока она не будет успешной. После успешного соединения сервер не будет производить новых вызовов, пока не наступит

следующий указанный в списке момент времени (1:00 дня). Такой вариант рекомендуется для баз, которые должны реплицироваться со средней частотой.

Server Connection : LAEC/ETC/InterTrust/RU to InterTrust/InterTrustCorp/SU

Basics | Replication/Routing | **Schedule** | Comments | Administration

Scheduled Connection

Schedule: ☐ ENABLED ☐

Connect at times: ☐ 11:00, 14:00, 18:00 ☐ each day

Repeat interval of: ☐ 0 ☐ minutes

Days of week: ☐ Sun, Mon, Tue, Wed, Thu, Fri, Sat ☐

Рис. 566 Три раза в заданное время

В окне **Replication Settings** для каждой базы можно также задать приоритет участия базы в репликациях. Указывая приоритет, вы фактически относите эту базу в одну из трех групп баз: редко реплицируемые базы (Low); базы, реплицируемые со средней частотой (Medium); базы, реплицируемые часто (High). Соответствующим образом составляя расписание, вы можете реплицировать критические базы данных более часто, чем другие. Например, базы с приоритетом High - несколько раз в день, базы с приоритетом Medium - один раз в день ночью, а базы с приоритетом Low - один раз в неделю по субботам. Для этого потребуется создать несколько документов Connection: например, один для баз только высокого приоритета, один для баз высокого и среднего приоритета и один для баз всех трех приоритетов.

Учтите, что документы Connection для баз данных различного приоритета не должны содержать перекрывающиеся отрезки времени. Если отрезки времени накладываются даже всего на минуту, расписание репликаций считается составленным некорректно. В этом случае репликации могут происходить беспорядочно или могут быть пропущены части списков реплицируемых баз.

Результат	High Высокий	High & Medium Средний и высокий
Это правильно	03:00 A.M. - 04:59 A.M.	05:00 A.M - 10:00 P.M.
Возможны проблемы	03:00 A.M. - 06:00 A.M.	05:00 A.M - 10:00 P.M.

Еще в версиях 4.x появилась возможность явно задавать в документах Connection списки реплицируемых баз или каталогов, содержащих базы. Такой подход значительно более гибок. С версий 6.x появилась и возможность явно задавать в документах Connection списки баз или каталогов, содержащих базы, которые реплицироваться не должны.

Сервер создает в своей виртуальной памяти список запланированных вами репликаций (расписание) из скрытого вида (\$Connections) в Каталоге Domino. Этот вид нельзя изменять, ибо в противном случае репликаторы всего домена не будут работать должным образом.

В документах Connection следует задавать полные имена связываемых серверов. Часто начинающие администраторы задают неполные имена иницилирующих репликацию серверов (например, InterTrust вместо InterTrust/InterTrustCorp/SU) и удивляются, почему в заданное время не происходит вызов. А вызов не происходит потому, что сервер (в этом примере InterTrust/InterTrustCorp/SU) «считает», что этот документ Connection «просто не имеет к нему никакого отношения» - документ должен «исполнять» несуществующий сервер InterTrust. Другой распространенный «подвох» для начинающих – использование неполных имен вызываемых серверов (например, InterTrust вместо InterTrust/InterTrustCorp/SU) в командах консоли PULL, PUSH и Replicate. Только

поведение несколько иное – репликация обычно начинается, поскольку установить соединение с указанным в команде сервером удастся, но документы не реплицируются должным образом, поскольку неполное имя сервера не встречается в ACL или не входит в группы.

1.62.7. 1.1.7. Randomized exponential backoff algorithm

Вы составили прекрасное расписание. Однако не всегда удастся установить соединение точно в запланированные моменты времени...

Если сервер должен выполнять репликацию, но ему **не удастся установить соединение** с вызываемым сервером, то:

- Если в документе Connection был задан **диапазон** (отрезок времени с интервалом повторения), сервер будет повторять попытки установления связи на основе «exponential backoff algorithm»: сервер повторяет попытку установления связи через 10 минут после первой попытки, 20 минут после первой попытки, 40 минут после первой попытки, и т.д. Учтите, что здесь приведены **средние** значения. Слово randomized из названия алгоритма предупреждает вас, что в действительности сервер добавляет к средним значениям случайные поправки, чтобы избежать совпадения по времени встречных вызовов. Например, если начальная попытка была в 1:00pm, последующие попытки будут сделаны в 1:10+s pm, 1:20+s pm, 1:40+s pm, где s - случайное число. Если время очередной из попыток по «exponential backoff algorithm» превышает время начальной попытки плюс интервал повторения (из документа Connection), очередная попытка установления связи происходит в момент времени, равный времени начальной попытки плюс интервал повторения (в нашем примере, если интервал повторения равен 60 минут, сервер повторно вызывает в 2:00pm, и повторяет в 2:10+s pm, 2:20+s pm, 2:40+s pm, а затем снова в 3:00pm). Только в случае, если предыдущий вызов был успешен, интервал повторения определяет, через сколько минут после завершения последней репликации будет происходить следующий вызов. Если вы задали в документе интервал повторения «пустым», сервер принимает интервал повторения равным 60 минут
- Если в документе Connection задан не диапазон, а **конкретное время** типа 08:00am, или даже список конкретных времен, сервер повторяет вызовы в течение часа. В соответствии с Randomized exponential backoff algorithm за это время произойдет около 4 попыток соединения. Но независимо ни от чего попытка следующей репликации будет происходить в следующее намеченное время в списке. Это означает, что если вы наметили репликации на 8:00 и 9:00, даже если репликация, назначенная на 8:00, заканчивается в 8:37, очередная репликация будет начинаться в 9:00, а не будет отсрочена до 9:37.

Иногда запланированные репликационные события подавляются сервером. Это может случаться, если подобное репликационное событие произошло совсем недавно (в течение часа) или если подобный запрос на репликацию все еще находится в очереди. В выборе репликатора между новыми запланированными и уже имеющимися в его очереди запросами на репликацию новые запланированные запросы имеют более высокий «приоритет». Это напоминает стратегию «заваленного» работой исполнителя, который при завершении очередного задания переключается на вновь полученное задание в ущерб уже имеющимся в его очереди заданиям. Такой принцип гарантирует завершение всех запланированных запросов до обслуживания «ждущих» запросов из очереди. Если запрос внесен в очередь, но связь с нужным сервером прервалась, происходит или повторное соединение (при работе по локальной сети) или снятие запроса (при работе по соединению типа Dialup Modem или X.25).

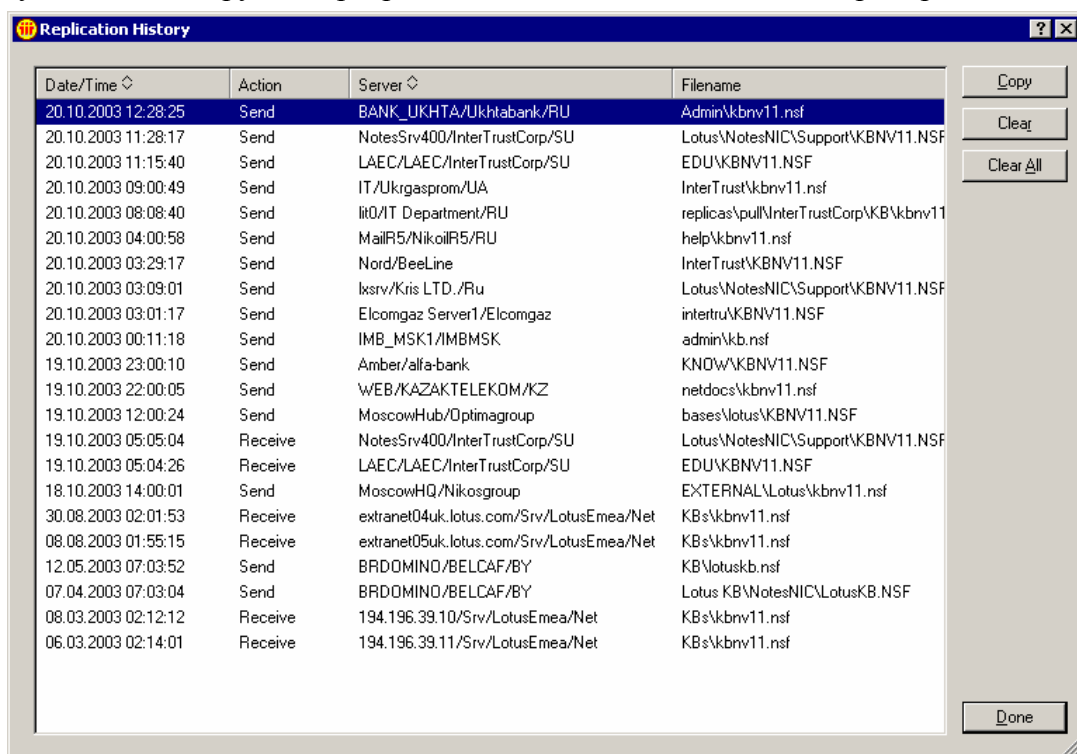
Обратите также внимание, что когда репликатор установил с сервером соединение типа Dialup Modem или X.25, этот факт становится известен Router-у (серверной задаче, отвечающей за передачу почты) вызванного сервера. Если Router вызванного сервера имеет ожидающую отправки на вызывавший сервер почту, эта почта будет передана в течение репликационной сессии. Обратное силы не имеет - выполнение репликаций осуществляется только по расписанию.

1.62.8. 1.1.8. Поле Cutoff Date и история репликаций базы

Проверки поля Cutoff Date и истории репликаций позволяют репликатору максимально сократить множество документов, просматриваемых на предмет возможного участия в репликации.

Поле **Cutoff Date** (метка поля **Only replicate incoming documents saved or modified after**) требует при репликациях принимать в данную реплику только те документы, которые имеют дату модификации позже указанной в поле.

Документы из других реплик этой базы с датой модификации до Cutoff Date никогда не включаются в списки реплицируемых документов и, следовательно, никогда не будут приняты в эту реплику. Репликатор всегда проверяет Cutoff Date и принимает в «свою» реплику только документы, созданные или измененные после этой даты. Аналогично и «окурки» документов, удаленных ранее Cutoff Date, не будут приниматься в реплику этой базы с других серверов. Даже если вы очищаете «историю репликаций».



Date/Time	Action	Server	Filename
20.10.2003 12:28:25	Send	BANK_UKHTA/Ukhtabank/RU	Admin\kbnv11.nsf
20.10.2003 11:28:17	Send	NotesSrv400/InterTrustCorp/SU	Lotus\NotesNIC\Support\KBNV11.NSF
20.10.2003 11:15:40	Send	LAEC/LAEC/InterTrustCorp/SU	EDU\KBNV11.NSF
20.10.2003 09:00:49	Send	IT/Ukrigasprom/UA	InterTrust\kbnv11.nsf
20.10.2003 08:08:40	Send	lit0/IT Department/RU	replicas\pull\InterTrustCorp\KB\kbnv11
20.10.2003 04:00:58	Send	MailR5/NikolR5/RU	help\kbnv11.nsf
20.10.2003 03:29:17	Send	Nord/BeeLine	InterTrust\KBNV11.NSF
20.10.2003 03:09:01	Send	lxsrvt/Kris LTD./Ru	Lotus\NotesNIC\Support\KBNV11.NSF
20.10.2003 03:01:17	Send	Elcomgaz Server1/Elcomgaz	intertru\KBNV11.NSF
20.10.2003 00:11:18	Send	IMB_MSK1/IMBMSK	admin\kb.nsf
19.10.2003 23:00:10	Send	Amber/alfa-bank	KNOW\KBNV11.NSF
19.10.2003 22:00:05	Send	WEB/KAZAKTELEKOM/KZ	netdocs\kbnv11.nsf
19.10.2003 12:00:24	Send	MoscowHub/Optimagroup	bases\lotus\KBNV11.NSF
19.10.2003 05:05:04	Receive	NotesSrv400/InterTrustCorp/SU	Lotus\NotesNIC\Support\KBNV11.NSF
19.10.2003 05:04:26	Receive	LAEC/LAEC/InterTrustCorp/SU	EDU\KBNV11.NSF
18.10.2003 14:00:01	Send	MoscowHQ/Nikosgroup	EXTERNAL\Lotus\kbnv11.nsf
30.08.2003 02:01:53	Receive	extranet04uk.lotus.com/Srv/LotusEmea/Net	KBs\kbnv11.nsf
08.08.2003 01:55:15	Receive	extranet05uk.lotus.com/Srv/LotusEmea/Net	KBs\kbnv11.nsf
12.05.2003 07:03:52	Send	BRDOMINO/BELCAF/BY	KB\lotuskb.nsf
07.04.2003 07:03:04	Send	BRDOMINO/BELCAF/BY	Lotus KB\NotesNIC\LotusKB.NSF
08.03.2003 02:12:12	Receive	194.196.39.10/Srv/LotusEmea/Net	KBs\kbnv11.nsf
06.03.2003 02:14:01	Receive	194.196.39.11/Srv/LotusEmea/Net	KBs\kbnv11.nsf

Рис. 567 История репликаций - база на сервере NotesSrv400 в последний раз «отправляла» изменения на сервер InterTrust в 11:28:17, а принимала с него изменения в 05:05:04

История репликаций содержит время и дату последней успешной репликации с перечисленными в записях истории серверами. Domino при очередной репликации будет при составлении списков реплицируемых документов учитывать только документы, добавленные, измененные или удаленные по времени позднее времени из записи в истории репликаций для этого сервера. После очередной успешной репликации с этим сервером относящиеся к нему записи в истории репликаций заменяются. Если списки истории на обеих сторонах не согласованы (например, если вы очищаете историю на одной стороне), в базе данных будут проверены на предмет участия в репликации все документы, более новые, чем Cutoff Date базы.

При некоторых ситуациях может быть даже полезно очистить историю, потому что этим вы обеспечите полную проверку всех документов в базе на предмет репликации. Вот одна из множества таких ситуаций. Предположим, в документах базы имелись поля типа Readers, в которых использовались имена групп. Ваш сервер не входил ни в одну из этих групп, и такие документы были серверу «не видны», а потому и не реплицировались. Вы добавили имя сервера в состав групп, и теперь хотите реплицировать «прежде невидимые» документы. Но не тут то было... Теперь эти документы стали «видны»

серверу, но не реплицируются, поскольку изменения в составе групп не привели к модификации самих документов, а согласно истории репликаций эти документы уже не учитываются.

Так что, если базы данных после репликации не синхронизированы или не имеют одинакового количества документов, причиной этого могли бы быть Cutoff Date или история репликаций. Но не только они.

1.62.9. 1.1.9. Идентификатор документа и свойство Seq Num поля (пункта)

Две реплики базы могут иметь разные версии одного документа, пока не произойдет репликация. После успешной репликации в обеих репликах содержатся одинаковые версии того же самого документа.

Идентификатор документа в базе данных Notes включает:

- • **DocumentUniqueID** - универсальный идентификатор документа, одинаковый во всех репликах. Это инвариант для всех версий документа
- • **DocumentVersionID** - описывает специфическую версию документа. Он изменяется при создании новых версий документа. Состоит из четырех компонент: дата-время последней модификации документа (SD), последовательный номер (SN), идентификатор реплики базы, в которой был создан документ (DB) и идентификатор местоположения документа в этой базе данных (NT).

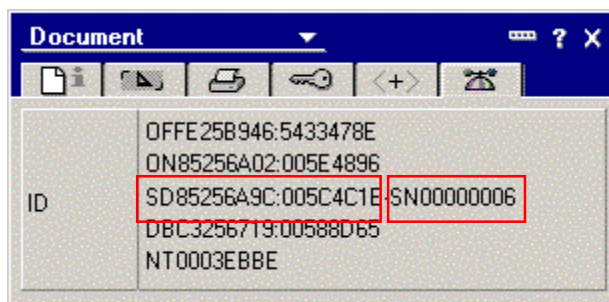


Рис. 568 Рамкой обведены дата-время последней модификации (SD) и последовательный номер (SN) документа

Две версии одного и того же документа (с одинаковым **DocumentUniqueID**) в разных репликах могут иметь разный последовательный номер (SN) и дату-время последней модификации (SD). При сохранении документа после внесения изменений увеличивается на единицу его последовательный номер (SN) и изменяется дата-время его модификации (SD).

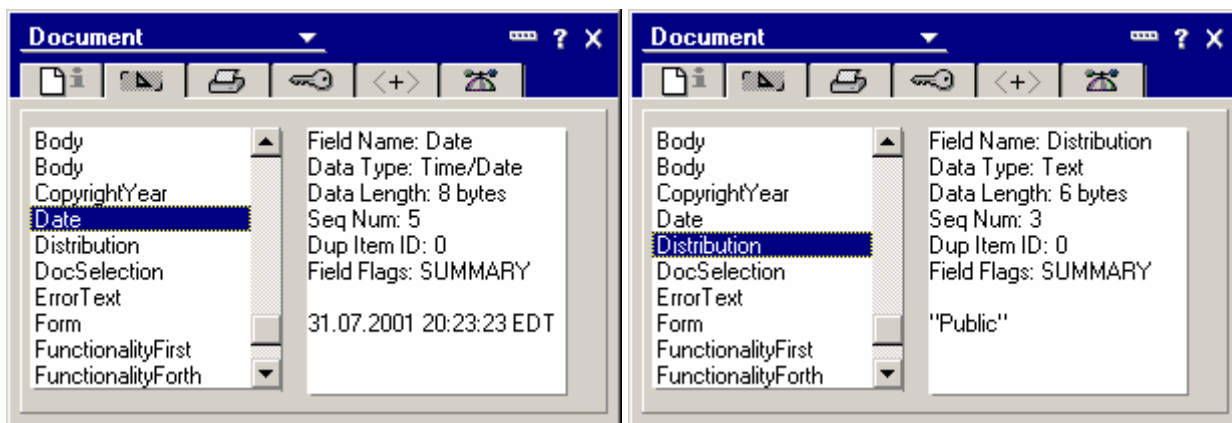


Рис. 569 Свойство Seq Num поля (пункта)

Кроме того, еще с версий 4.x в момент сохранения документа в базе отслеживается, какие поля (более строго, пункты полей, поскольку поля типа Rich Text хранятся в виде серии пунктов, каждый размером не более чем 64 Кб) действительно были изменены. Для тех полей, которые действительно изменились, свойство поля Seq Num устанавливается равным последовательному номеру документа (SN). Если же поле не изменилось, его Seq Num не меняется (сохраняет прежнее значение).

1.62.10. 1.1.10. Как влияют на репликацию списки управления доступом реплик базы

Для уяснения принципа влияния списка управления доступом (ACL) на репликацию лучше «временно забыть», что в действительности вначале репликатор на сервере А «тянет к себе» информацию с сервера В. Влияние ACL на репликацию таково, что если что-то (изменения в ACL, дизайн, документы...) поступает на сервер А, то это «как бы записывает» сервер В, а значит, его «возможности по записи» таковы, как то указано для сервера В в ACL на сервере А. И наоборот, когда выполняется вторая фаза репликации. Вне зависимости от того, «заталкивает» ли репликатор сервера А информацию на сервер В или сам репликатор сервера В «тянет ее к себе» с сервера А, эту информацию на сервер В «как бы записывает» сервер А, а значит его «возможности по записи» таковы, как то указано для сервера А в ACL на сервере В.

А ← В (информация поступает с сервера В на сервер А)

Если сервер В определен в ACL на сервере А как ...	При репликации сервер А принимает с сервера В ...
Менеджер	измененную ACL новые или измененные элементы дизайна новые или измененные документы (включая удаления)
Дизайнер	новые или измененные элементы дизайна новые или измененные документы (включая удаления)
Редактор	новые или измененные документы (включая удаления)
Автор	новые или измененные документы (включая удаления), в полях типа Authors которых явно или как член группы присутствует сервер В. Но поскольку обычно сервер не является автором документа (если только его имя, явно или как члена группы, специально не внесли в поле типа Authors), рекомендуется избегать назначения для серверов такого уровня доступа в ACL баз
Депозитор	только новые документы

Поскольку репликация обычно двусторонний процесс, необходимо анализировать и действие ACL «в обратную сторону» (когда информация поступает с сервера А на сервер В).

Рекомендации по настройке ACL

- ● База на сервере назначения принимает к себе только то, что ее ACL позволяет изменять серверу - источнику изменений. Хотите принимать в базу все - дайте серверу-источнику доступ менеджера, хотите только дизайн и документы - дизайнера, только документы - редактора. Если дополнительно необходимо, чтобы информация только принималась сервером назначения, но не поступала на сервер - источник изменений, в ACL его реплики дайте серверу назначения доступ читателя.
- ● Сервер - источник изменений должен иметь в ACL базы принимающего сервера тот же доступ, как и наивысший доступ пользователя на сервере-источнике.
- ● Если каждый сервер имеет доступ менеджера в ACL на обоих серверах и ACL был изменен на одной или на обеих сторонах, более новая версия ACL будет заменять более

старую версию. Вся информация из более старой версии ACL будет потеряна. Если «старая» ACL после репликации «вернулась обратно», проверьте правильность установки времени и информации о часовом поясе на обоих серверах.

- Если сервер указан в ACL только как член группы, всякая выясняющая его уровень доступа сторона (сервер или станция) обращается за списком группы в свою локальную адресную книгу. С этим связана часто встречающаяся проблема при репликациях между станцией и сервером: если указать имя сервера в ACL локальной реплики явно, сервер получает на станции заданный уровень доступа, если указать в ACL группу LocalDomainServers - сервер получает на станции только уровень доступа -Default-. Дело в том, что группа LocalDomainServers в персональной адресной книге станции обычно пуста. Аналогичный эффект может наблюдаться при использовании группы LocalDomainServers (или других групп) при репликациях между серверами из разных доменов.
- Так как имеются достаточно много связанных с доступом моментов, могущих сделать репликацию неудачной или неполной - ACL, поля Readers и Authors, роли и Directory Links/ACLs) - администраторам остается предложить только общую стратегию поиска причин неудачной репликации: «смотреть» на реплику базы данных на «другой» стороне «под ID своего сервера» и руководствоваться «старым, как сам Notes» правилом: **что вы «видите», то вы и можете реплицировать, а что вы «не видите», то вы не можете реплицировать**. Однако эта стратегия может «не сработать», если в ACL для имени вашего сервера был конкретизирован тип: «только как сервер».

1.62.11. 1.1.11. Селективные репликации

Начиная репликацию базы, ваш репликатор (или станция) прежде всего строит по документам в реплике на вызванном сервере вид, содержащий все документы, которые могли бы быть приняты вашей стороной. Для этого вида используется отбора **SELECT @All**.

При селективной репликации ваш репликатор (или станция) строит такой вид по документам в реплике на вызванном сервере, используя заданную вами формулу отбора и обычно «отфильтровывающую» меньшее количество документов, чем по формуле **SELECT @All**.

Для изменения формул селективной репликации необходимо иметь в вашей реплике базы доступ не ниже дизайнера. Чтобы определить формулу, выбирают в окне Replication Settings на закладке Space Savers опцию **Replicate only a subset of the documents**. Далее возможны два варианта. Если не выбирать опции **Documents that meet a selection formula**, можно выбрать один или несколько видов или папок, документы из которых должны приниматься в вашу реплику. По сути дела, этим вы «сообщаете», что формула отбора селективной репликации является объединением формул отбора выбранных видов плюс объединение коллекций документов из выбранных папок.

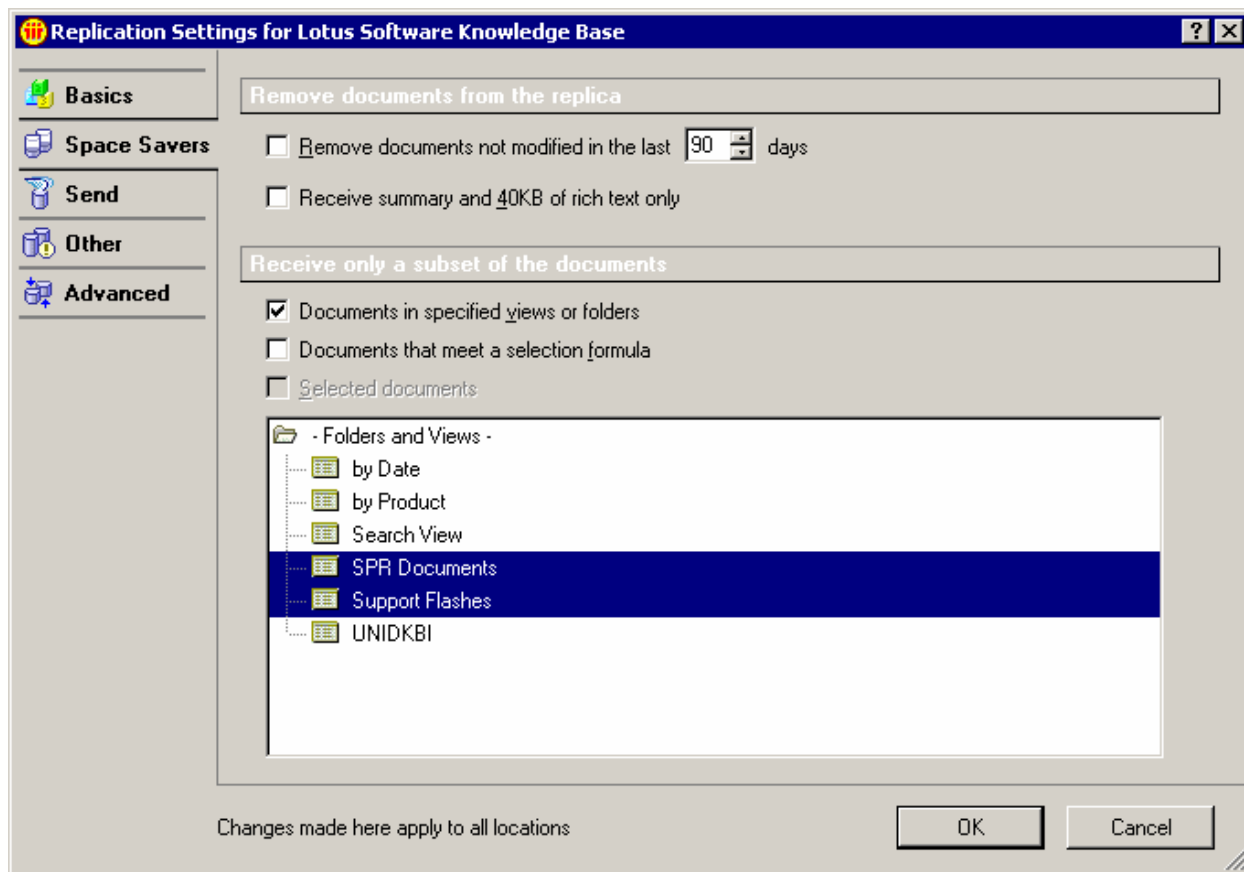


Рис. 570 В данную базу принимаются только документы из выбранных видов

Если выбрать опцию **Documents that meet a selection formula**, можно явно указать формулу отбора селективной репликации. В результате в вашу реплику будут приниматься только документы, удовлетворяющие этой формуле.

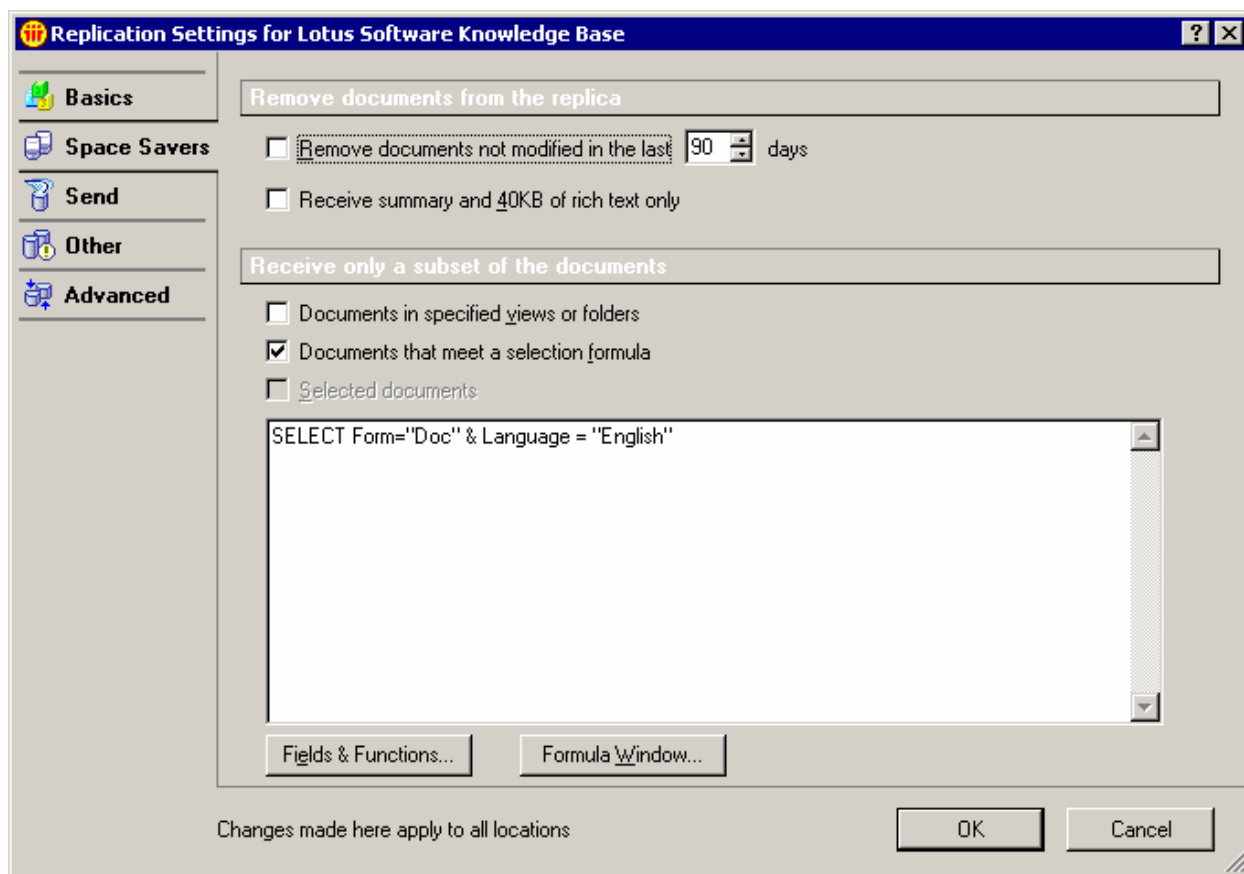


Рис. 571 В данную базу принимаются только документы, удовлетворяющие формуле отбора

Дополнительные возможности по определению формул отбора селективной репликации имеются в окне Replication Settings на закладке Advanced.

Прежде всего, там имеется возможность задать разные формулы отбора для разных пар принимающих изменения (**When Computer**) серверов или станций и серверов или станций, с которых принимаются изменения (**Receives from**). Если вы уже определили для вашей реплики формулу отбора на закладке Space Savers, то эта формула «окажется» на закладке Advanced как формула отбора в случае, когда в поле When Computer: выбран ваш сервер (или станция), а в поле Receives from: выбрано -Any Server-, т.е. когда в вашу реплику принимаются изменения с любого сервера.

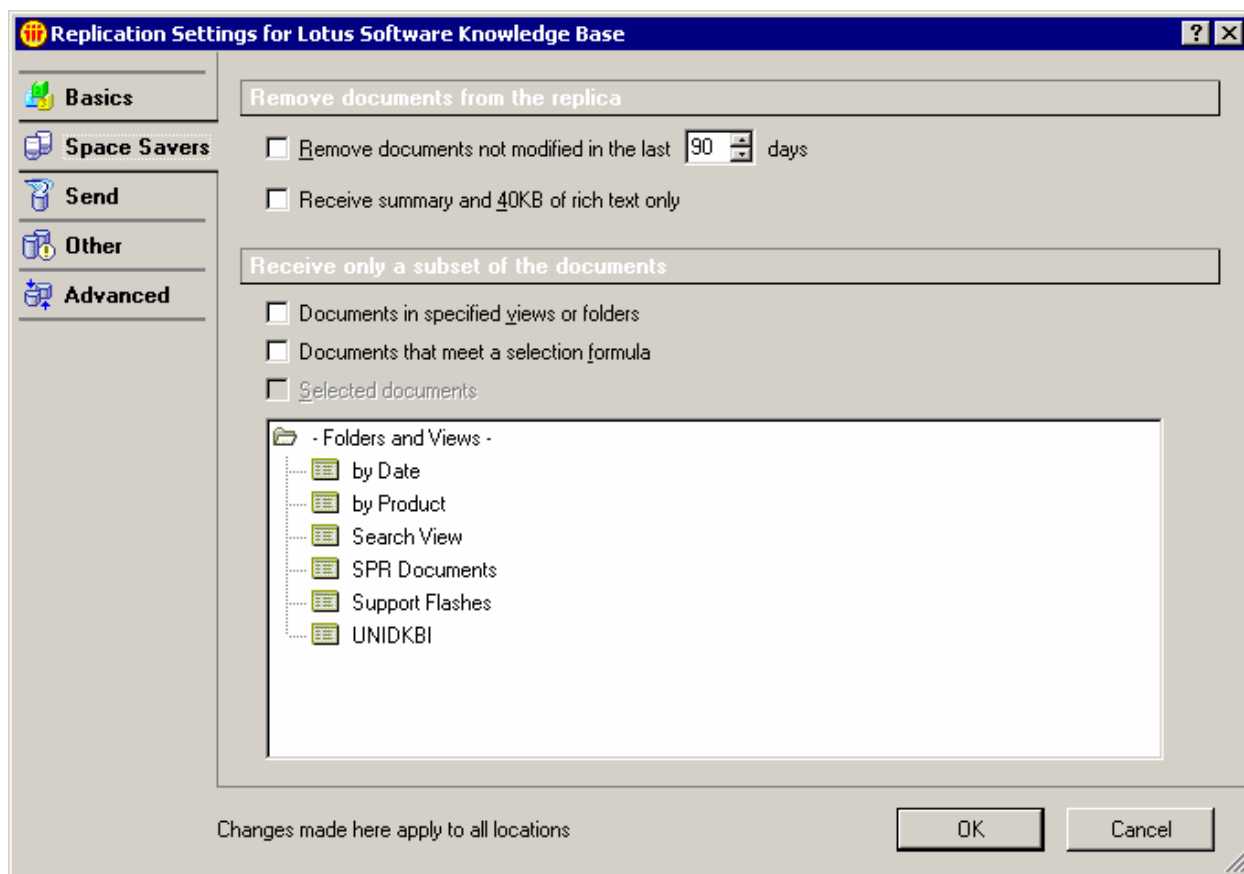


Рис. 572 Возможности закладки *Advanced*

Кроме того, для разных пар **When Computer** и **Receives from** можно указать, что должно происходить при репликации списка управления доступом, элементов дизайна, а также конкретизировать вопрос репликации документов. Это достигается выбором опций **Receive those elements from other replicas**:

- • **Access Control List** - принимаются изменения в списке управления доступом;
- • **Design elements** - принимаются все элементы дизайна, кроме агентов и репликационных формул;
- • **Agents** - принимаются агенты;
- • **Replication formula** - принимаются репликационные формулы;
- • **Deletions** - принимаются «окурки», вызывая тем самым удаление документов;
- • **Fields** - принимаются не все поля документов, а только выбранные из списка.

Только имейте в виду, что эти опции должны быть согласованы со списком управления доступом базы. Так, если выбрали на закладке *Advanced* «прием» в вашу базу элементов дизайна, но в списке управления доступом базы предоставили «поставляющим» эти изменения серверам только доступ редактора, то никаких изменений дизайна вы не получите. Наоборот, даже если «поставляющий» изменения сервер имеет в ACL вашей базы доступ менеджера, но вы не выбрали на закладке *Advanced* «прием» в вашу базу «окурков», они не будут приниматься в вашу базу.

Опция **Replication Formula** разрешает принимать в базу назначения (When Computer) формулы селективной репликации, имеющие более позднее время модификации. В принципе это позволяет менеджеру «центральной» реплики базы разрабатывать формулы селективной репликации для всех других серверов, перебирая всевозможные сочетания When Computer и Receives from.

Таким образом:

- • селективная репликация будет фактически уменьшать количество принимаемых в данную реплику документов, если вы создаете более ограничительную формулу, чем SELECT @All;
- • использование ... | @IsResponseDoc в формуле отбора будет реплицировать вообще все ответные документы (responses), независимо от того, соответствуют ли они отбираемому главному документу или нет;
- • использование ... | @AllDescendants в формуле отбора будет реплицировать все ответные документы (responses) на отбираемые главные документы и, рекурсивно, на их ответные документы;
- • использование ... | @AllChildren в формуле отбора будет реплицировать только ответные документы (responses) непосредственно на отбираемые главные документы;
- • информация о формуле отбора принимаемых в базу документов сохраняется в той базе, в которой она создана, но может реплицироваться в другие базы, если у них выбрана опция Replication Formula и предоставлен необходимый уровень доступа.

1.62.12. 1.1.12. Алгоритм репликации

Подробно алгоритм репликации включает следующие шаги.

- • **Установление соединения с сервером.** В соответствии с имеющимся в адресной книге расписанием, составленным администратором, или по введенной вне расписания команде консоли, используя Randomized exponential backoff algorithm, инициирующий репликацию сервер соединяется с вызываемым сервером. Выполняется процедура аутентификации серверов и дополнительные процедуры, выбранные в секциях Security и Restrictions документа Server на вызванном сервере.
- • **Построение списка реплицируемых баз.** Каждый сервер поддерживает в своей виртуальной памяти упорядоченную по идентификатору реплики базы таблицу с информацией обо всех имеющихся на нем базах - т.н. «кэш идентификаторов реплик». В нем содержатся сведения о базах и шаблонах, находящихся в каталоге данных Notes и рекурсивно его подкаталогах, а также во всех Directory Links и рекурсивно их подкаталогах. В общем случае репликатор, сравнивая кэш идентификаторов реплик «своего» сервера и кэш идентификаторов реплик на вызванном сервере, создает список имеющих одинаковый идентификатор реплики баз на обоих серверах. Однако из команды консоли или документа Connection может следовать, что в репликации должны участвовать только базы соответствующих приоритетов или только базы в указанных каталогах или явно перечисленные базы на вызываемом сервере. Если это так, то репликатор, сравнивая кэши идентификаторов реплик, учитывает не все, а только необходимые базы из кэша идентификаторов реплик «своего» сервера.
- • Далее для каждой базы из списка реплицируемых выполняется следующее.
 - • **Не запрещены ли репликации базы?** Если в установках одной из реплик выбрана опция Temporary disable replication, все заканчивается появлением на консоли сервера сообщения Replication is disabled for <сервер база>.
 - • **Может ли каждый из серверов открыть реплику на другом сервере?** Если один из серверов имеет в ACL реплики на другом сервере уровень доступа No Access, все заканчивается появлением сообщения Access control is set in <сервер база> to not allow replication from <сервер база>. Аналогично происходит, если реплика находится в Directory Link, а сервер не имеет доступа к этой Directory Link. Если же оба сервера имеют доступ к обеим репликам, репликатор открывает реплику на вызванном сервере.
 - • **Репликация ACL.** Это происходит, если вызванный сервер имеет в ACL вызвавшего сервера доступ менеджера и в установках реплики на вызвавшем сервере выбрана опция Replicate incoming: Access Control List. Репликатор проверяет, не изменилась ли ACL в реплике на вызванном сервере после последнего изменения ACL «своей» реплики. Если изменилась, репликатор получает ACL с вызванного сервера и заменяет ACL «своей» реплики, после чего снова проверяет, может ли каждый из серверов открыть реплику на другом сервере. Если репликация выполняется по схеме Pull-Push, зеркально-аналогичные проверки и действия выполняются этим репликатором по отношению ACL на вызванном

сервере. При репликации по схеме Pull-Pull их выполнит репликатор вызванного сервера на второй фазе репликации.

- **Репликация элементов дизайна.** Это происходит, если вызванный сервер имеет в ACL вызвавшего сервера доступ не ниже дизайнера, а в установках реплики на вызвавшем сервере выбраны опции Replicate incoming: Forms, Views, etc., Agents, Replication formula.
- Элемент дизайна хранится в базе данных подобно документу. И, подобно документу, каждый элемент дизайна имеет свой идентификатор. Универсальный идентификатор, являющийся частью идентификатора, одинаков во всех репликах базы. Но имеющаяся в составе идентификатора дата-время последней модификации элемента дизайна (SD) может быть разной в каждой реплике.

Репликатор создает список идентификаторов всех элементов дизайна в реплике на вызванном сервере, которые были изменены со времени последней репликации, а если история репликаций очищена, то с Cutoff Date. Затем для каждого идентификатора из этого списка предпринимается попытка определить идентификатор элемента дизайна из «своей» реплики, имеющего такой же универсальный идентификатор.

Если это удалось (т.е. в репликах есть элементы дизайна с одинаковым универсальным идентификатором), остается сравнить времена последней модификации этих элементов. Если в реплике на вызванном сервере «более свежий» элемент дизайна, репликатор получает его и заменяет им имеющийся в «своей» реплике. Но если только этого не запрещают делать опции Replicate incoming: Forms, Views, etc., Agents, Replication formula «своей» реплики. Удаление элементов дизайна тоже происходит подобно удалению документов - посредством передачи «окуров» с более поздним временем модификации. А репликационных конфликтов для элементов дизайна не бывает.

Если же в реплике на «своем» сервере нет элемента дизайна с таким же универсальным идентификатором, как в реплике на вызванном сервере, остается добавить в «свою» реплику новый элемент дизайна.

Если репликация выполняется по схеме Pull-Push, зеркально-аналогичные проверки и действия выполняются этим репликатором и по отношению элементов дизайна на вызванном сервере. При репликации по схеме Pull-Pull их выполнит репликатор вызванного сервера на второй фазе репликации.

- **Репликация документов.** Это происходит, если вызванный сервер имеет в ACL вызвавшего сервера возможность создавать или изменять документы.
- Вначале репликатор, используя формулу отбора селективной репликации «своей» реплики (или по умолчанию SELECT @All), создает по документам на вызванном сервере вид, содержащий «потенциально допустимые» для приема в «свою» реплику документы. Затем репликатор «просматривает» этот вид и создает список идентификаторов документов в реплике на вызванном сервере, которые были изменены со времени последней репликации, а если история репликаций очищена, то с Cutoff Date. Если документ в реплике на вызванном сервере был в последний раз модифицирован раньше, чем текущее время минус интервал удаления для реплики на «своем» сервере, его идентификатор исключается из списка.

Для каждого идентификатора из этого списка предпринимается попытка определить идентификатор документа из «своей» реплики, имеющего такой же универсальный идентификатор.

Если это удалось (т.е. в обеих репликах есть документы с одинаковым универсальным идентификатором), остается сравнить времена последней модификации (SD) и последовательные номера (SN) этих документов.

Если документ с предшествующей репликации изменился в реплике на вызванном сервере, но не изменился в реплике на «своем» сервере, репликатор копирует измененный документ и замещает им документ в «своей» реплике. То же произойдет, если документ в реплике на вызванном сервере был удален. Вместо удаленного документа остается «окур» с большим последовательным номером и датой модификации. «Окур» должен копироваться репликатором в «свою» реплику и заместить имевшийся в ней документ, вызывая тем самым его удаление. Но если только этого не запрещает делать опция Replicate incoming: Deletions «своей» реплики.

Если же документ изменился на обеих сторонах, происходит репликационный конфликт (рассматривается в **Ошибка! Источник ссылки не найден.**).

Если же в реплике на «своем» сервере нет документа с таким же универсальным идентификатором, как в реплике на вызванном сервере, его остается добавить в «свою» реплику как новый документ.

Если репликация выполняется по схеме Pull-Push, зеркально-аналогичные проверки и действия выполняются этим репликатором и по отношению документов на вызванном сервере. При репликации по схеме Pull-Pull их выполнит репликатор вызванного сервера на второй фазе репликации.

Если документ был модифицирован в одной реплике позже, чем было произведено его удаление в другой реплике, модифицированный документ должен «перекрыть окурок». То же произойдет, если в результате ряда модификаций последовательный номер документа в одной реплике оказался больше, чем последовательный номер «окурка».

Наконец, при копировании документа происходит не полное копирование всех полей - копируются только поля, у которых неодинаковые Seq Num. Поля же с одинаковым Seq Num нет смысла копировать - они одинаковы в обеих репликах. Это существенным образом сокращает объем информации, передаваемой при репликации. Именно это и называют «репликацией на уровне полей» - а более строго, пунктов.

Обновление записи в истории репликаций. Только когда репликация успешно завершилась, репликатор вызывавшего сервера обновляет записи в истории репликаций «своей» реплики: когда с вызванного сервера были приняты документы (Received) и когда с вызывавшего сервера были отправлены документы на вызванный (Send). При неуспешной репликации записи в истории репликаций не обновляются. Если репликация выполняется по схеме Pull-Push, репликатор обновляет и историю репликаций на вызванном сервере. При репликации по схеме Pull-Pull это выполнит репликатор вызванного сервера на второй фазе репликации.

- • **Завершение репликационной сессии.** Когда список реплицируемых баз «исчерпан», репликатор или разрывает соединение (схема Pull-Push), или передает запрос «на обратную репликацию» в очередь репликатора на вызванном сервере (схема Pull-Pull).

1.62.13. 1.1.13. Репликационные конфликты

Когда репликатор обнаруживает конфликт, он выбирает версию документа, имеющую более позднее время модификации, и сохраняет в «своей» реплике в качестве главного документа. Другая версия этого документа тоже сохраняется в «своей» реплике, но в качестве ответного документа (response) на главный. В ответный документ также добавляется поле с именем \$Conflict и пустым значением. Ответные документы, имеющие поле \$Conflict, «отмечаются» ромбиком на левом поле вида и сопровождаются пояснением [Replication or Save Conflict].

	Doc Type	Title
	16.06.97	
	What's New	What's New in Knowledge Base - May 1997
	General Product Info	White Paper: Integrated Messaging
	Technote	"Unable to Replicate...Not Authorized to Use Server on Remote Server
	Technote	How to Migrate a DB8 Post Office with LMT 4.1
◆	[Replication or Save Conflict]	
	Technical Paper	The Basics of Creating a Notes Rich Text Item Using the Notes C API
	Technote	How to Use the HTDatabase Functions in HiTest C

Рис. 573 Пример конфликтных документов в виде: «How to Migrate...» - конфликтный главный документ, ромбиком же отмечен конфликтный ответный документ

Для разрешения возникших конфликтов в общем случае потребуется вмешательство лиц, вносивших изменения в документы, поскольку необходимо осмысление имеющихся изменений.

Технически же дело обстоит так. Если нет необходимости оставлять в базе конфликтный ответный документ, его попросту удаляют. Если нет необходимости оставлять конфликтный главный документ, нужно сначала открыть в режиме редактирования конфликтный ответный документ и заново сохранить его, а только потом удалять главный документ. Дело в том, что при «пересохранении» конфликтного ответного документа из него автоматически удаляются поля \$Conflict и \$Ref. Если же сразу удалить конфликтный главный документ, то конфликтный ответный окажется «документом без родителя» (его поле \$Ref содержит универсальный идентификатор уже не существующего главного документа), и в результате перестанет отображаться в виде, поддерживающем иерархию ответных документов. Наконец, если должны остаться оба конфликтных документа, достаточно «пересохранить» конфликтный ответный документ.

Если в процессе эксплуатации базы наблюдается «усиленная» тенденция к образованию конфликтов, скорее всего, наступило время задуматься об изменении дизайна базы. Для «борьбы» с конфликтами имеется ряд приемов, среди наиболее простых из которых можно отметить имеющиеся в окне свойств формы опции Versioning - управление версиями документа и Merge replication conflicts - автоматическое слияние конфликтных документов, если разные пользователи изменяли в них разные поля.

1.62.14. 1.1.14. Как обеспечить работу на сервере нескольких репликаторов

Если в документах Connection запланированы одновременные или перекрывающиеся по времени репликации с несколькими серверами, следует иметь на сервере несколько одновременно работающих репликаторов. При этом станут возможны одновременные репликации с разными серверами - каждый репликатор с одним сервером одновременно. Например, если на одно и то же время запланированы репликации сервера А с серверами В и С, и на сервере А запущено два репликатора, один из них будет выполнять репликацию с сервером В, в то время как второй - с сервером С.

Для запуска нескольких репликаторов возможны следующие варианты.

- • Переменная **Replicators** или переменная **ServerTasks** из файла NOTES.INI сервера.
- • Команда **Load Replica** с консоли.
- • Команда **Load Replica имя_сервера** с консоли. Запущенный такой командой репликатор завершится после выполнения репликации с указанным сервером, что эквивалентно команде Replicate имя_сервера.
- • Запуск репликатора на уровне операционной системы.

Запуск репликатора на уровне операционной системы выполняется командой

xREPLICA [direction] servername [filename or directory] ,

где: **x** – буква, зависящая от платформы, «N» для Windows;

[direction] - необязательный параметр, определяющий тип репликации:

- • пусто - Pull-Push,
- • -p - Pull-Only,
- • -s - Push-Only;

Servername - имя вызываемого сервера;

[filename or directory] - необязательный параметр, задающий имя файла базы или каталог с базами, для которых должна выполняться репликация.

Для того чтобы избежать недоразумений при столь необычном запуске репликатора, проверьте, чтобы в переменных KeyFileName и ServerKeyFileName из файла NOTES.INI были указаны одни и те же ID-файлы. Репликатор, запущенный на уровне операционной системы, будет работать под ID из KeyFileName, в то время как сервер Domino и запущенный из него репликатор работают под ID из ServerKeyFileName.

Наконец, целесообразность применения такого способа запуска репликатора при работающем сервере очень неочевидна, однако как способ осуществить репликацию при остановленном сервере это очень даже хорошо работает.

После того, как на сервере уже запущено несколько репликаторов, их можно остановить, но только все сразу, командой **Tell Replica Quit**.

1.62.15. 1.1.15. Переменные NOTES.INI, которые влияют на репликации

- • **Allow_Access** Список пользователей, групп и серверов, имеющих доступ на этот сервер.
- • **Create_Replica_Access** Список пользователей и групп, которые могут создавать реплики на этом сервере.
- • **Deny_Access** Список пользователей, групп и серверов, не имеющих доступа на этот сервер.
- • **Log_Replication** Значение 1 требует протоколировать начало и конец репликационной сессии в протоколе и на консоли сервера, значение 0 - не протоколировать.
- • **Repl_Error_Tolerance** задает количество ошибок одного и того же типа, которое может произойти при репликации двух баз, прежде чем сервер закроет репликацию.
- • **ReplicationTimeLimit** Задаёт максимальное время (в минутах), которое может занимать репликация между данным сервером и другими серверами.
- • **Replicators** Указывает количество задач Replicator, которые должны одновременно выполняться на сервере.

1.62.16. 1.1.16. Резервное копирование с применением механизма репликаций

Не секрет, что любая автоматизированная система работает до первого сбоя. Сбой произойдет всегда, как бы все не казалось надежным. Вопрос стоит лишь в скорости устранения сбоя, в количестве потерянной при сбое информации и в мере ответственности эксплуатирующих ее лиц за последствия сбоя.

В документации упоминаются следующие способы резервного копирования баз данных:

- • выгрузка на стример,
- • выгрузка на файл-сервер,
- • использование репликаций для поддержки резервных реплик.

По первому и второму вариантам, прежде чем начинать резервное копирование, необходимо остановить сервер Notes. Если же остановка «рабочего» сервера недопустима, предлагается «завести» выделенный сервер, «несущий» реплики баз всех рабочих серверов, а собственно резервное копирование выполнять на нем.

По третьему варианту также необходим отдельный архивный сервер, «несущий» реплики баз со всех рабочих серверов. Рассмотрим настройки в списках управления доступом (ACL) реплик баз, рекомендуемые в этой ситуации:

- • ACL «рабочей» реплики:
 - • -Default- - редактор с правом удалять документы,
 - • архивный сервер - читатель,
 - • рабочий сервер - менеджер с правом удалять документы;
- • ACL архивной реплики:
 - • -Default- - читатель,
 - • архивный сервер - менеджер с правом удалять документы,
 - • рабочий сервер - дизайнер или редактор.

Кроме того, в репликационных установках находящихся на архивном сервере реплик баз следует выбрать опцию **Do not send deletions made in this replica to other replicas**.

Еще один способ решения проблемы резервного копирования состоит в использовании кластеров из серверов Domino.

1.62.17. 1.1.17. Использование групп при репликациях между серверами

Все просто – вместо вызываемого сервера в документе Connection задается имя группы со списком серверов. Группа должна иметь тип Servers Only. Работает с R5. Только вот либо имена серверов должны быть «правильные», либо надо подправить файл hosts, либо воспользоваться программой GETADRS...

Basics			
Connection type:	Local Area Network	Usage priority:	Normal
Source server:	InterTrust/InterTrustCorp/SU	Destination server:	ServerGroup_Net
Source domain:	InterTrustCorp	Destination domain:	Net
Use the port(s):	TCPIP1	Optional network address:	

Choose ports

Рис. 574 Connection

Basics	
Group name:	ServerGroup_Net
Group type:	Servers only
Category:	
Description:	Admin\Репликации с группой серверов - серверы домена Net
Mail Domain:	
Internet Address:	
Members:	194.196.39.10/Srv/LotusEmea/Net 194.196.39.11/Srv/LotusEmea/Net extranet04uk.lotus.com/Srv/LotusEmea/Net extranet05uk.lotus.com/Srv/LotusEmea/Net

Рис. 575 Группа

1.63. 1.1. Репликации между клиентом и сервером

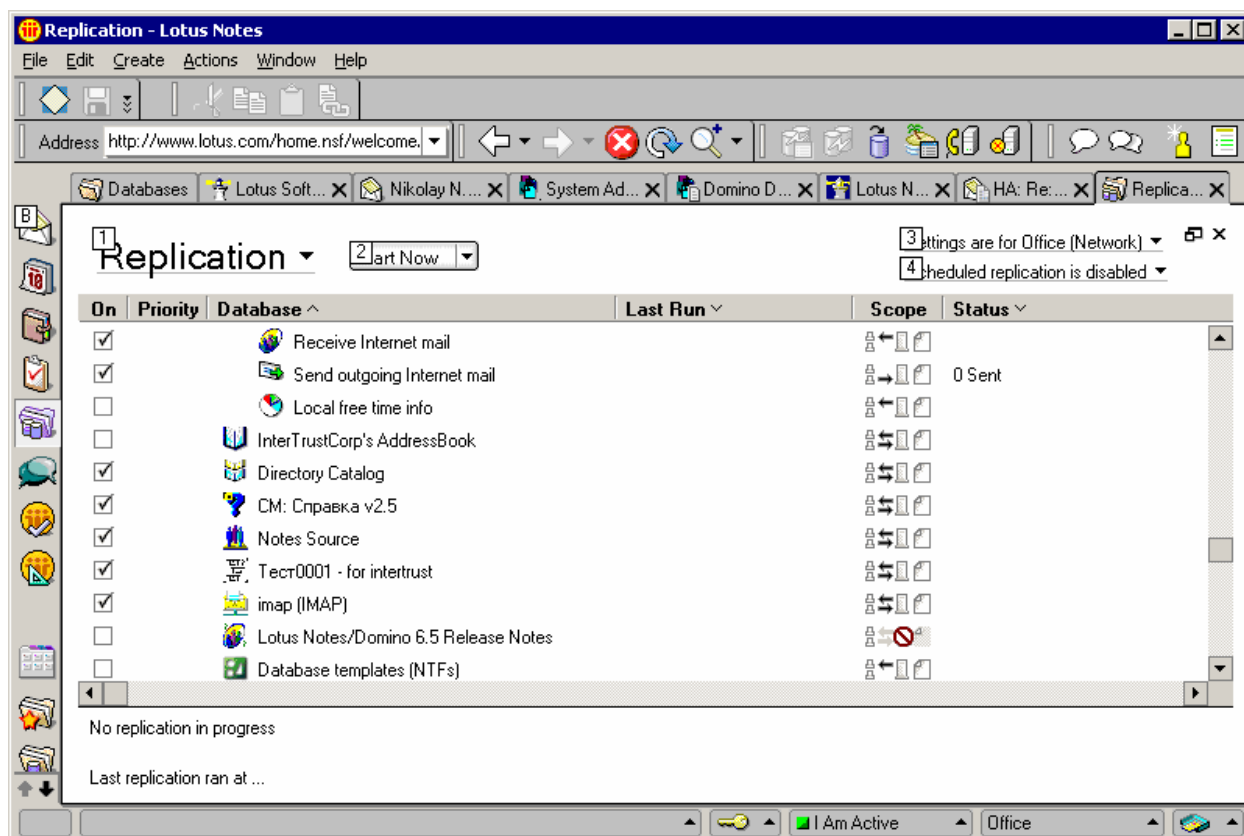


Рис. 576 Закладка Replication в клиенте задает, что и как реплицируется в данном Location

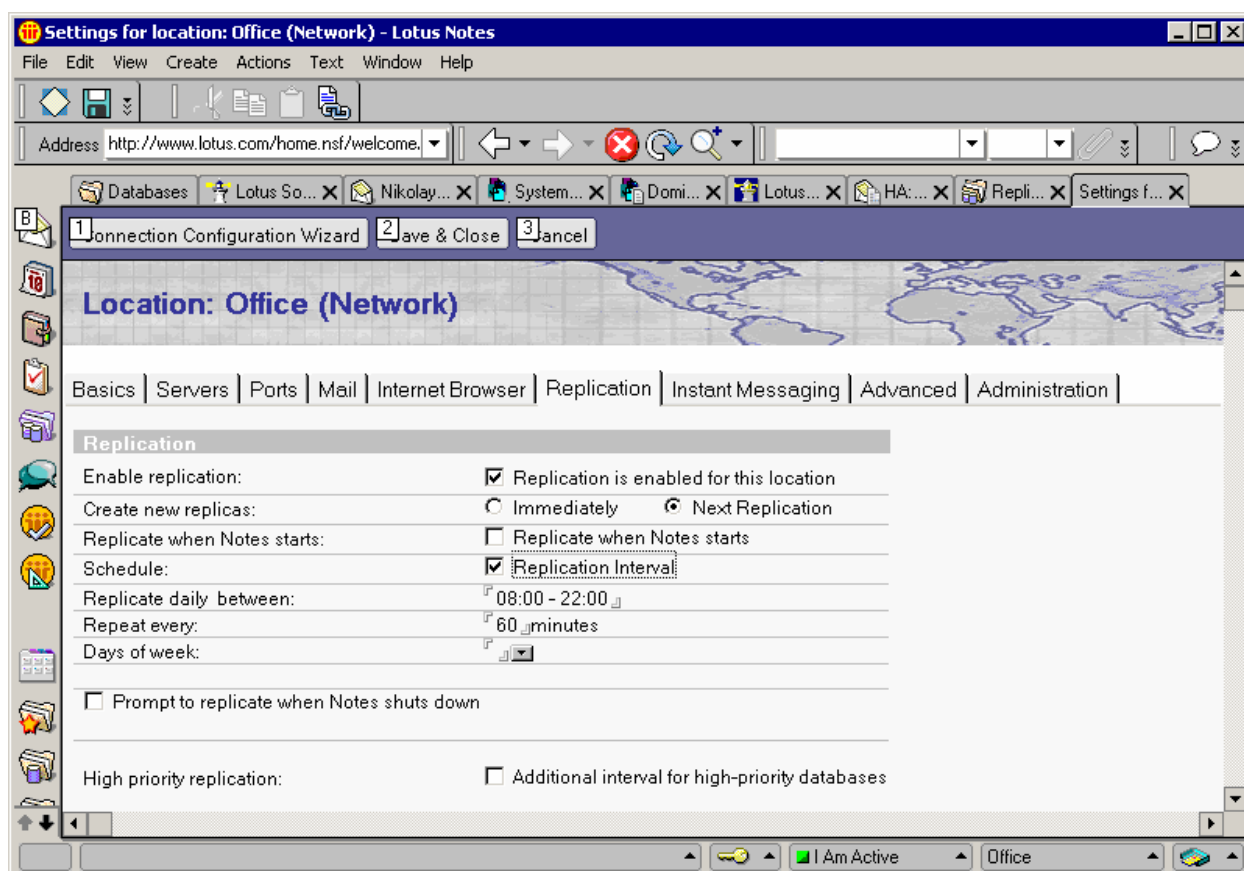


Рис. 577 В Location можно задать и расписание для выбранного на закладке Replication...

1.63.1. 1.1.1. Устранение проблем при установлении соединений с серверами и репликациях

Проблемы в основном те же, что и при репликациях между серверами.

- ● Распространенная ошибка — трактовка состава групп, в частности, группы LocalDomainServers по разным NAMES.NSF...

1.64. 1.1. Кластеры из серверов Domino: программы CLADMIN, CLDBDIR, CLREPL

Кластер из серверов Domino

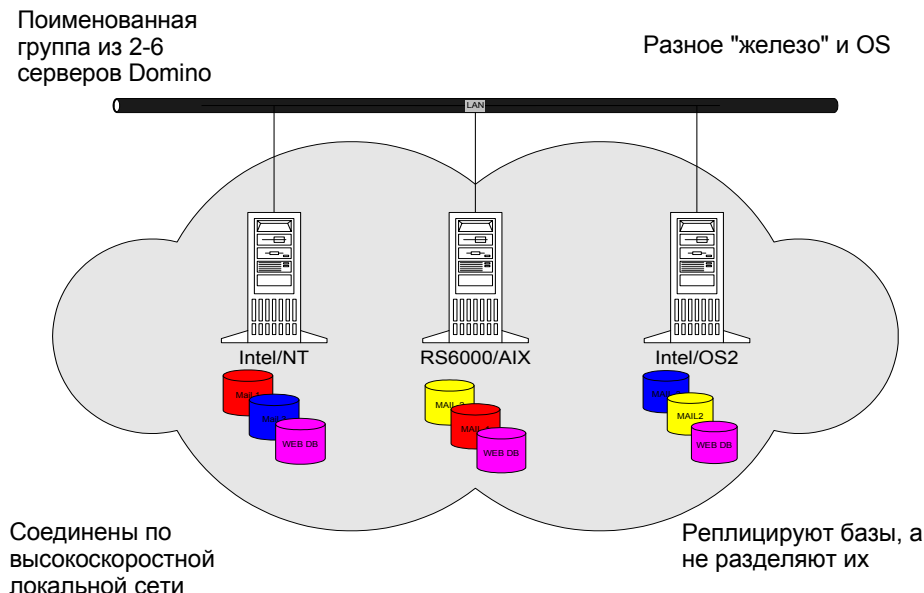


Рис. 578

Кластер из серверов Domino - группа до шести серверов Domino, взаимосвязанных и взаимодействующих между собой, чтобы обеспечить высокую степень доступности, масштабируемости и балансировку загрузки. Серверы кластера по возможности должны располагаться в одной высокоскоростной локальной сети. Обычно на серверах кластера для каждой «критической» для бизнес-процесса базы данных создаются реплики, которые внутри кластера синхронизируются не по расписанию, а по событию модификации документа, «почти в реальном времени».

1.64.1. 1.1.1. Серверные программы и компоненты, реализующие работу сервера в кластере

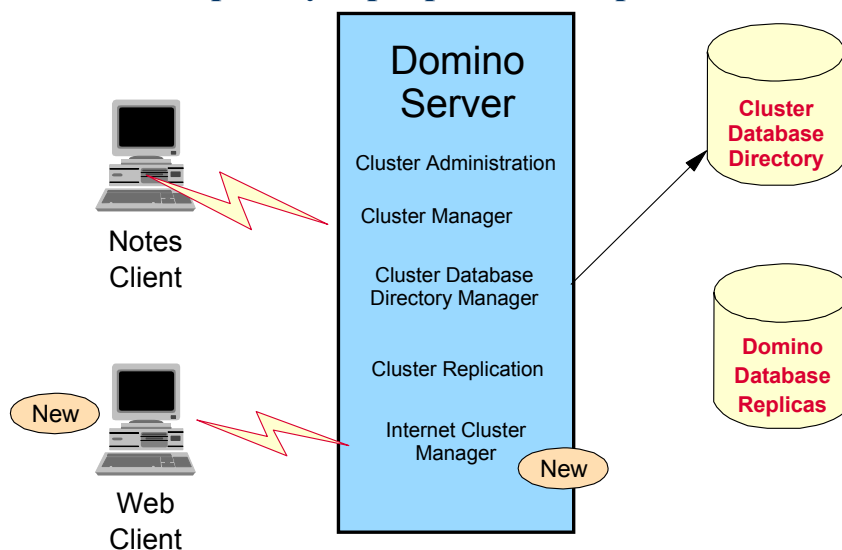


Рис. 579

1. Серверная программа **Cluster Administration Process (CLADMIN)** отвечает за корректную работу всех компонент кластера. На сервере-члене кластера эта программа автоматически запускается при старте сервера или в ситуации, когда было обнаружено изменение в составе кластера. В R6 как программа отсутствует – ее функции выполняет сам сервер Domino.

2. Серверная программа **Cluster Database Directory Manager (CLDBDIR)** занимается поддержкой в актуальном состоянии базы данных Cluster Database Directory (CLDBDIR.NSF). Как только программа «замечает» появление на «своем» сервере новой базы или шаблона, она создает в базе CLDBDIR.NSF соответствующий этой базе или шаблону документ. Документ включает название базы, имя сервера, путь к файлу базы, идентификатор реплики и прочие атрибуты. Этот документ «тут же» передается внутрикластерным репликатором в реплики базы CLDBDIR.NSF на других серверах-членах кластера. Когда же программа «замечает» удаление на «своем» сервере базы или шаблона, она удаляет в базе CLDBDIR.NSF соответствующий удаленной базе или шаблону документ. Кроме того, программа CLDBDIR выполняет операции с базами данных, для которых в базе CLDBDIR.NSF были установлены атрибуты «out of service» или «pending delete». В R6 в список ServerTasks не заносится – сервер запускает ее сам.

3. Компонента сервера Администратор кластера - **Cluster Manager** - постоянно «отслеживает» состояние всех серверов-членов кластера. Она поддерживает в своей виртуальной памяти (т.н. кэш кластера) в актуальном состоянии список всех функционирующих в данное время серверов-членов кластера, а также информацию о текущей загрузке каждого сервера-члена. Для получения этой информации программа периодически обменивается с другими серверами-членами кластера специальными сообщениями (probes). Эту информацию можно получить по команде консоли Show Cluster.

В ситуации, когда данный сервер «перегружен пользователями», программа Cluster Manager по информации из базы CLDBDIR.NSF всегда может определить, какие еще серверы кластера имеют реплику запрошенной очередным пользователем или сервером базы, и перенаправить этот запрос на соответствующий сервер-член кластера.

4. Серверная программа **Cluster Replicator (CLREPL)** функционирует на каждом сервере-члене кластера и обеспечивает выполнение внутрикластерных репликаций. Внутрикластерный репликатор работает по схеме Push-Only. Он «способен реплицировать» не только ACL, дизайн и документы, но и также частные папки, хранимые в базе. Информацию о других серверах-членах кластера, на которых имеется реплика «изменившейся» базы, программа CLREPL получает по информации из базы данных CLDBDIR.NSF. Однако для ускорения работы программа «кэширует» содержимое этой базы в своей виртуальной памяти, обновляя кэш только в тех случаях, когда содержимое базы данных CLDBDIR.NSF изменяется программой CLDBDIR. В R6 в список ServerTasks не заносится – сервер запускает ее сам.

5. Средство анализа кластера - **Cluster Analysis tool** - встроено в программное обеспечение станции Notes. Оно используется для анализа конфигурации кластера и определения, корректно ли он установлен. «Запускается» средство из окна Server Administration выбором пункта Cluster Analysis в меню кнопки Servers. Результаты работы этого средства помещаются в базу данных Cluster Analysis (CLUSTA4.NSF) в документы формы Cluster Analysis Results.

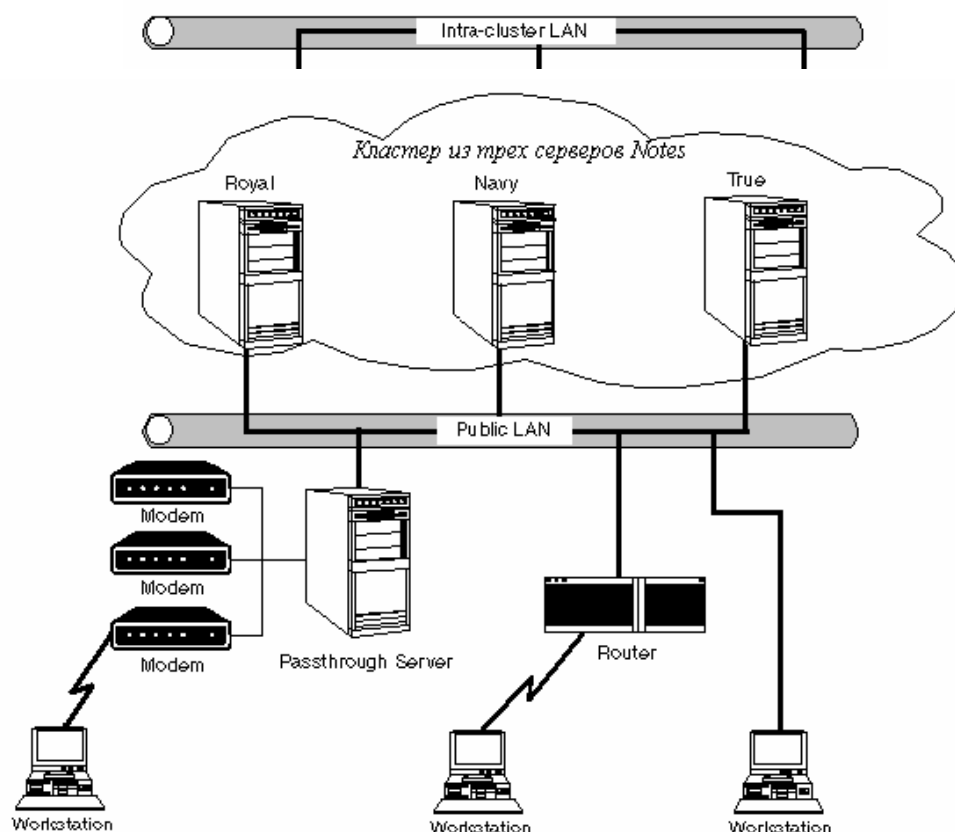


Рис. 580

1.64.2. 1.1.2. Состояния

Запрос от	Состояние сервера					
	Available	Busy	Restricted	MaxUsers	Unreachable	Invalid
Клиент	Access granted	Load balance	Failover	Failover	Failover	Access granted
Клиент (репликации)	Access granted	Access granted	Access granted	Access granted	Failover	Access granted
Domino Replicator	Access granted	Access granted	Access granted	Access granted	No access	Access granted
Cluster Replicator	Access granted	Access granted	Access granted	Access granted	No access	Access granted
Mail Router	Access granted	Access granted	Failover	Failover	Failover	Access granted

1.64.3. 1.1.3. Конфигурирование

- • Когда происходит «переключение» (failover) при доставке почты:
MailClusterFailOver=1 еще в R5 устарела. Управление осуществляется из документа Server Configuration с закладки Router\SMTP\Advanced, поле Cluster failover:
 - • Disabled - нет
 - • Enabled for last hop only - разрешено только последнему серверу в маршруте
 - • Enabled for all transfers within this domain - разрешено при любых передачах в пределах домена

Configuration Settings : ServerGroup_IntTrustCluster

Basics | Router/SMTP | MIME | NOTES.INI Settings | Domino Web Access | IMAP | SNMP | Activity Logging | Diagnostics | Administration

Basics | Restrictions and Controls | Message Tracking | Advanced |

Journaling | Commands and Extensions | Controls |

Miscellaneous Controls

Logging level:

Advanced Transfer Controls

Ignore message priority:

Dynamic cost reset interval: minutes

Additional Controls (Delivery and Transfer)

Restrict name lookups to primary directory only:

Cluster failover:

Select Keywords

Keywords

- Disabled
- Enabled for last hop only
- Enabled for all transfers in this domain

OK Cancel

Рис. 581 Cluster failover

- Чем достигается балансировка загрузки серверов кластера:
Server_Availability_Threshold = значение (Show cluster)
Server_MaxUsers = значение
Server_Restricted = значение (SET CONFIG SERVER_RESTRICTED=1)
- Количество репликаторов
Cluster_Replicators=value
- По какому порту осуществляется внутрикластерный обмен:
Server_Cluster_Default_Port = TCPIP1

1.64.4. 1.1.4. Добавление сервера в кластер и удаление из кластера

Добавление сервера в кластер - кнопкой **Add to Cluster** из вида Servers

Имя кластера содержится в документе Server в поле Cluster Name

Удаление сервера из кластера - кнопкой **Remove from Cluster** из вида Clusters

1.64.5. 1.1.5. Clustering Features

- С R6.5 внутрикластерный репликатор может реплицировать пометки о прочтении документов

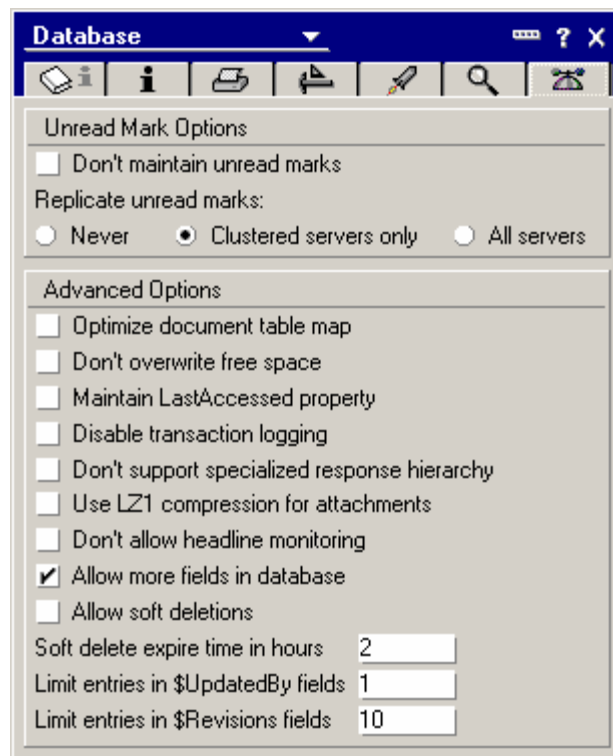


Рис. 582

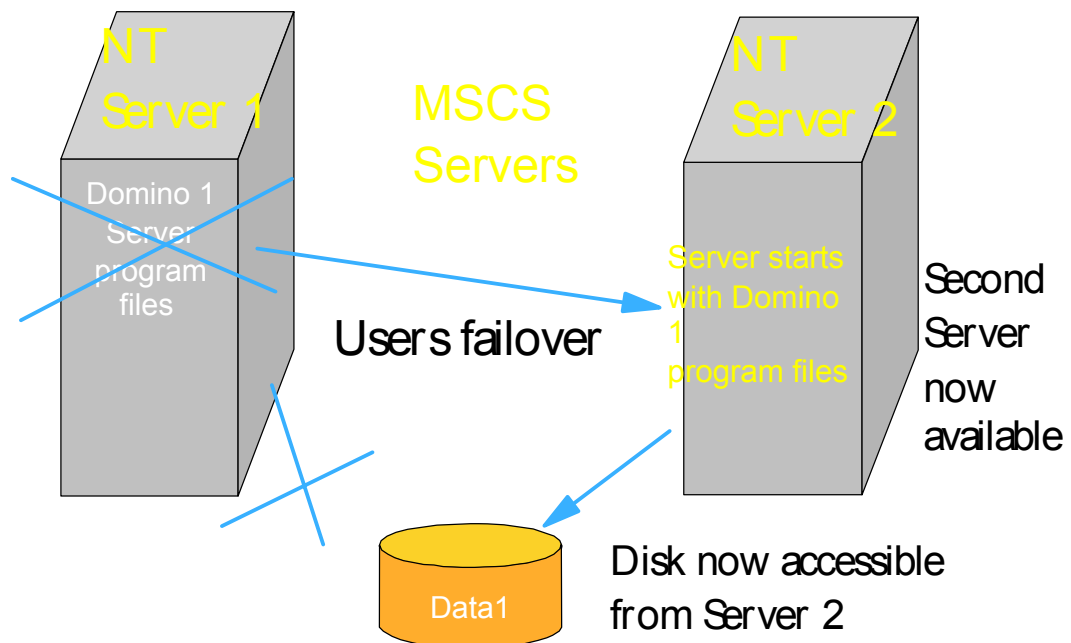
- • Селективные репликации не поддерживаются внутрикластерным репликатором.
 - • Индекс доступности вычисляется с учетом HTTP-нагрузки.
 - • Система Calendar & Scheduling выполняет Failover при поиске свободного времени
- Серверы вне кластеров используют базу BUSYTIME.NSF, а серверы кластера используют CLUBUSY.NSF. Когда почтовый сервер пользователя сильно загружен, при выполнении запроса на поиск свободного времени происходит failover на другой сервер этого кластера

В R6 failover **не происходит** в следующих случаях:

- • Сервер стал недоступен, когда пользователь работал в базе. Базу надо переоткрыть... Если пользователь редактировал документ, он может скопировать документ в другую реплику (*проверьте, как это сделать*).
- • Пользователь открывает базу по File - Database - Properties or File - Database – Open.
- • Пользователь создает новую базу на неработающем сервере или по шаблону с неработающего сервера.
- • Агенты, кроме mail predelivery agents.
- • Administration Process.

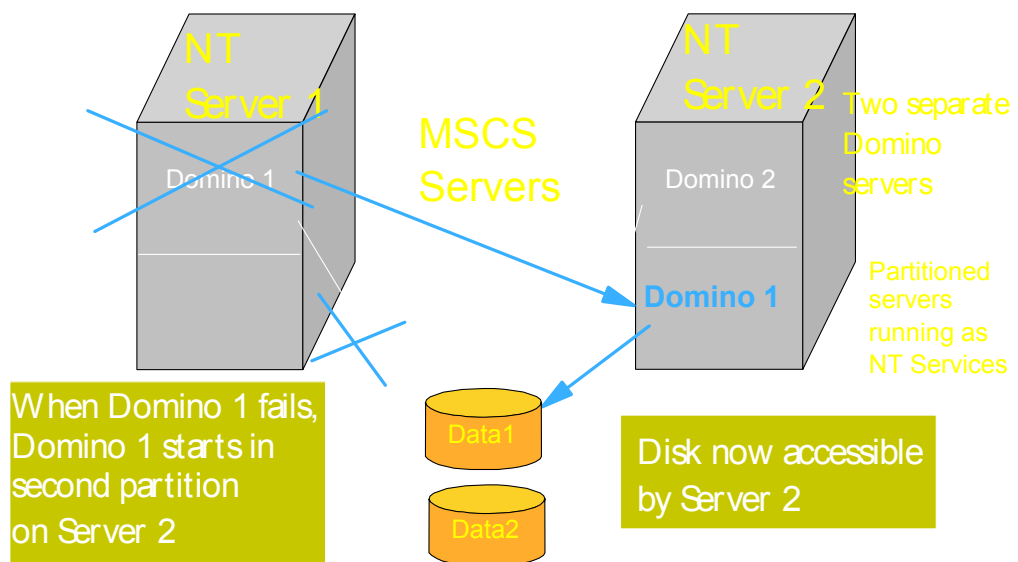
Сервер Domino может работать на Microsoft Cluster Server, но это не имеет никакого прямого отношения к кластерам Domino...

Domino & MSCS Active/Passive



Puc. 583

Domino & MSCS Active/Active



Puc. 584

1.65. 1.1. База Directory Assistance

➤  **стр. 232**

1.65.1. 1.1.1. Назначение, создание, конфигурирование

➤  **стр. 233-237**

1.65.2. 1.1.2. Документы типа Domino и LDAP

➤  **стр. 242-250**

1.66. 1.1. Программа HTTP Server (HTTP)

1.66.1. 1.1.1. Назначение и логика работы

HTTP Server ожидает установления соединения с ним по протоколу HTTP клиентом Web и затем запроса от клиента Web на нужный ресурс (например, GET URL). HTTP Server исследует URL входящего запроса и определяет, запрашивает ли клиент единицу информации из базы данных Notes или HTML-файл из файловой системы. Если был запрошен HTML-файл, HTTP Server, действуя точно так же, как и любой другой HTTP-сервер, передает запрошенный файл клиенту. Если же была запрошена единица информации из базы данных Notes, HTTP Server через Domino Engine обращается к соответствующей базе, извлекает из нее необходимую информацию, преобразует эту информацию в формат HTML и передает клиенту, или же, наоборот, помещает информацию от клиента в базу данных Notes.

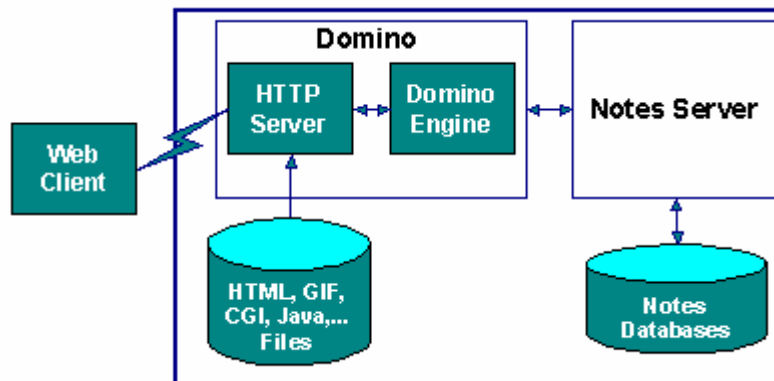


Рис. 585

1.66.2. 1.1.2. Процесс аутентификации клиентов

Неаутентифицированный – Anonymous. Если он «превышает» имеющийся уровень доступа, разрешенный для Anonymous, или если на сервере запрещен анонимный доступ, в браузере появляются окно или форма для ввода имени и пароля и передачи их на сервер.

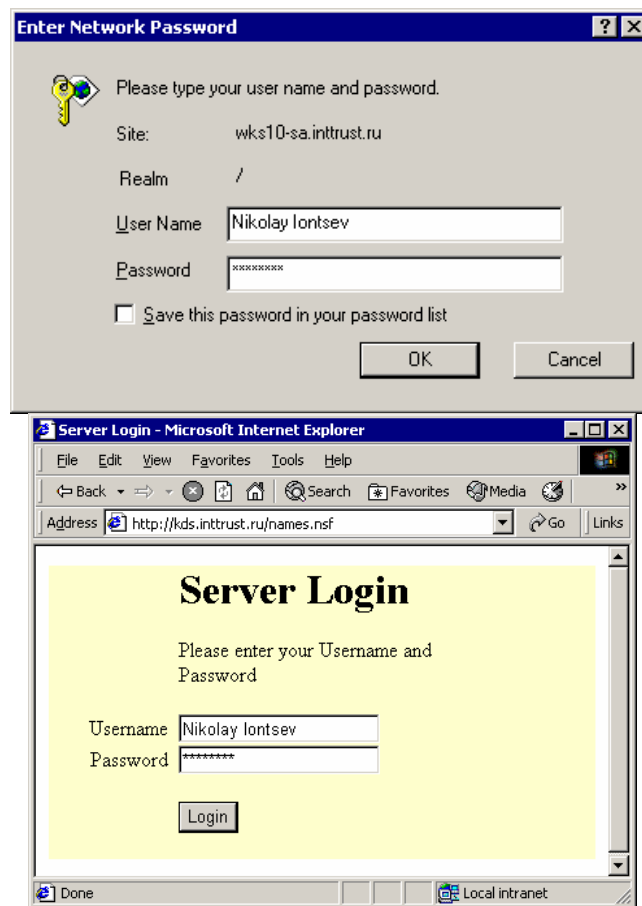


Рис. 586 в браузере окно или форма...

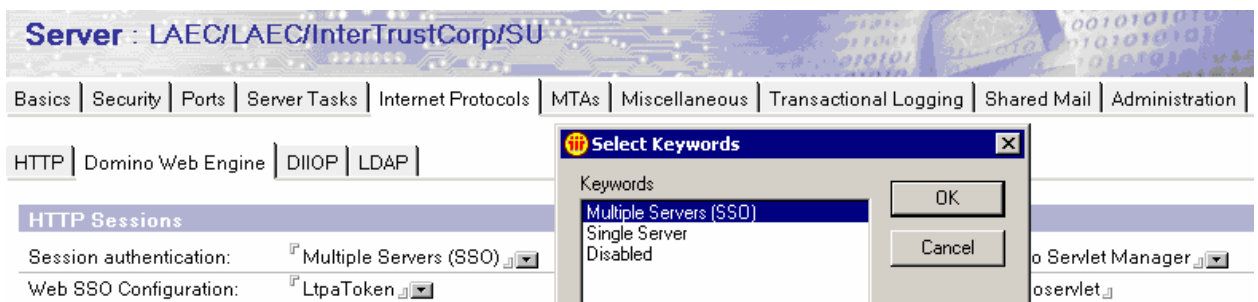


Рис. 587 Если Session authentication=Disabled, в браузере окно, иначе форма

Если нужна своя форма, создается база domcfg.nsf по шаблону Domino Web Server Configuration и в ней обычно изменяется форма \$\$LoginUserForm. Пользователь вводит имя и пароль и передает на сервер. Способ передачи: если Session authentication=Disabled, в заголовках «пакета» HTTP, иначе обычная передача формы. Если работа по порту с поддержкой SSL, это безопасно, иначе нет. Программа HTTP выбирает имя и по нему выполняет поиск «документа Person» в основном Каталоге Domino и выбранных в Directory Assistance дополнительных Каталогах Domino «с флагом Trusted» и LDAP-серверах, «разрешенных» для аутентификации Web-клиентов. В Каталоге Domino поиск выполняется по виду (\$Users) или виду (\$LDAPCN). Если документ найден, пароль, введенный пользователем, сравнивается с паролем в документе (поле InterNet Password). Если пароли совпали – пользователь аутентифицирован. Если на имя найдено более одного документа Person, R6 выбирает тот, в котором совпадает пароль, до R6 – отказ.

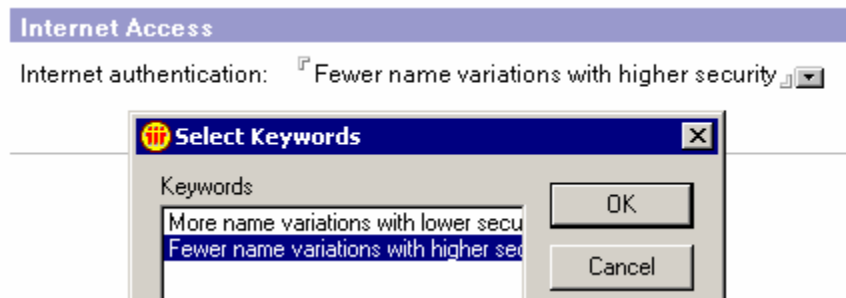


Рис. 588 Документ Server, закладка Security: More... - (\$Users), Fewer... - (\$LDAPCN)

Далее из документа Person выбирается первый элемент из поля-списка User Name. Это имя и будет использовано при проверке вхождения в группы и при вычислении доступа к базе по ACL. Последние моменты – ограничение в ACL Maximum Internet name and password и флаг Require SSL connection в свойствах базы.

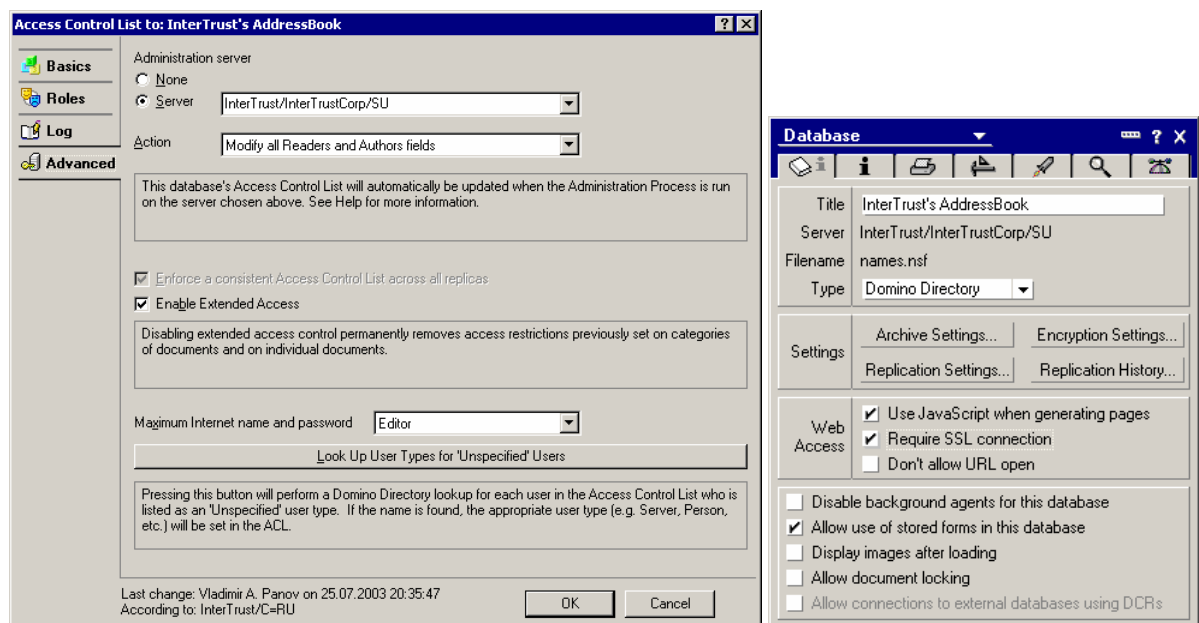


Рис. 589

1.66.3. 1.1.3. Организация поддержки SSL

- • Обзор возможности выпуска сертификатов X.509 с использованием Server-Based CA
- • Server-Based Certification Authority и серверная программа CA Process (CA) в контексте KeyRing-файла CA (сертификатора Internet)
- • Создание и миграция KeyRing-файла CA в Server-Based CA
- • Операция Certification-Migrate Certifier в контексте KeyRing-файла CA
- • Защита мигрированных KeyRing-файлов CA паролем или ID-файлом с паролем
- • Изучение базы ICL
- • Internet Certificate Authority R6
- • Получение пользователями сертификатов X.509 с использованием CA Process
- • Отзыв сертификатов X.509
- • Операция Certification-Modify Certifier в контексте KeyRing-файла CA

1.66.3.1. 1.1.3.1. Создание сертификатора Internet

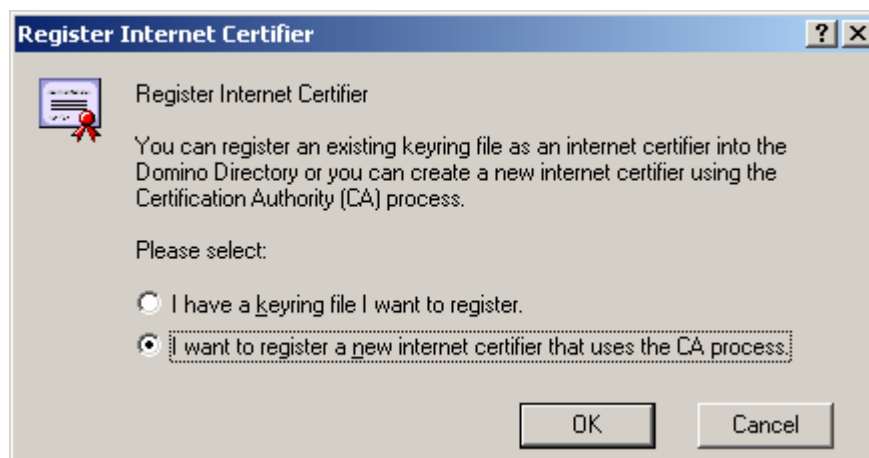


Рис. 590 Создается новый keyring-файл, но можно мигрировать старый

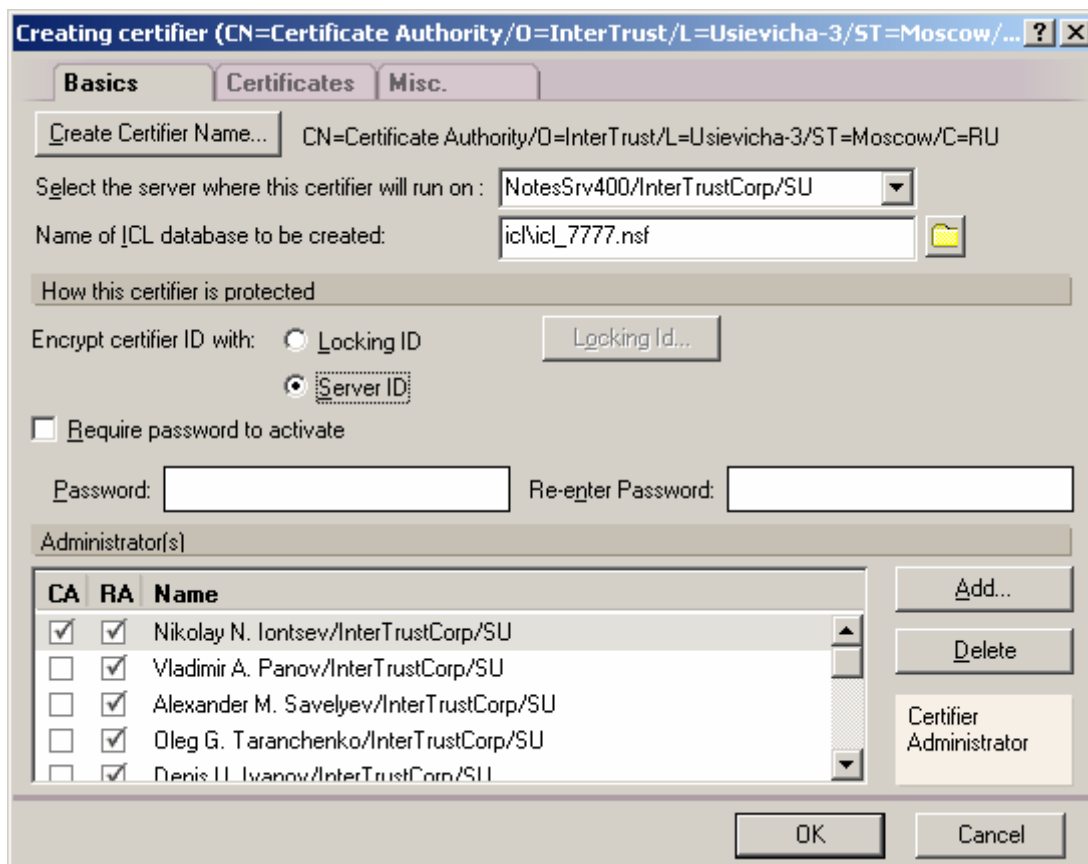


Рис. 591 Местонахождение базы ICL, способ защиты keyring-файла и администраторы CA и RA

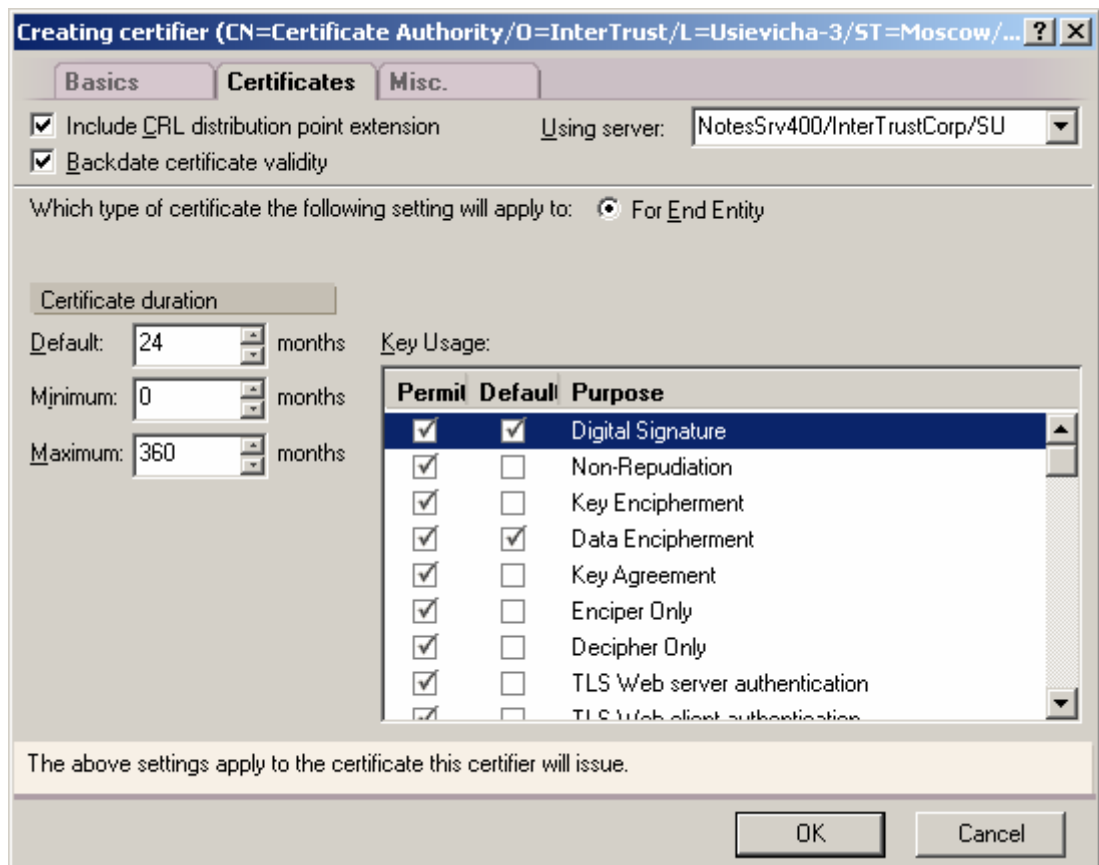


Рис. 592 Свойства и назначение сертификатов. Кроме того, выбраны поддержка CRL distribution point (списка отозванных сертификатов) на сервере и Backdate certificate validity – возможность того, чтобы сертификаты становились «валидными» (valid) не с момента выпуска, а с указанной даты

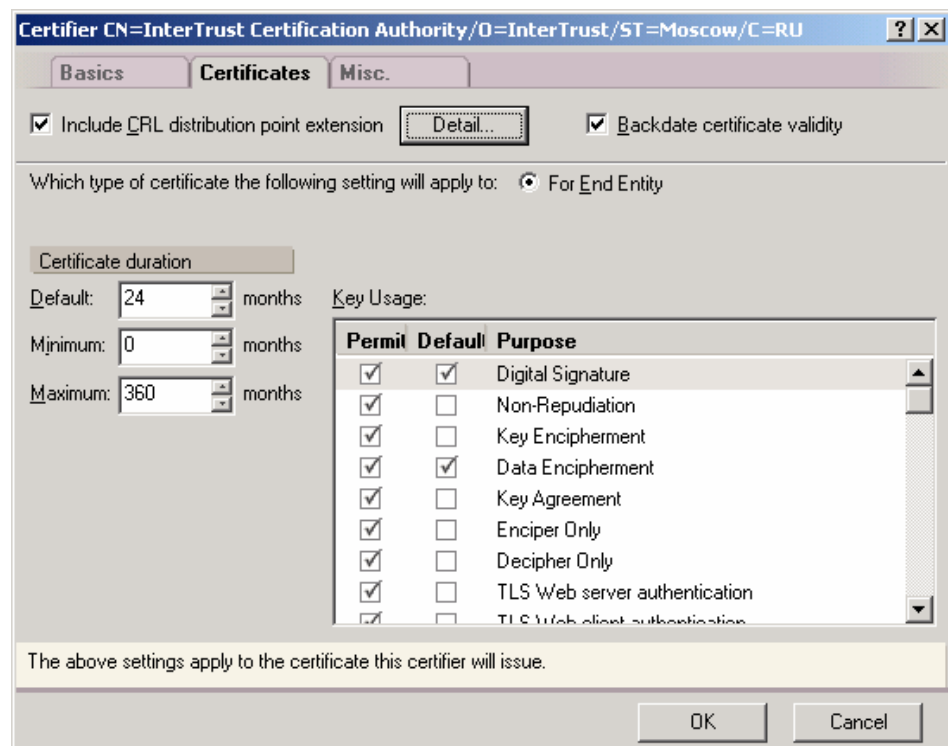


Рис. 593 В 6.01 закладка немного изменилось...

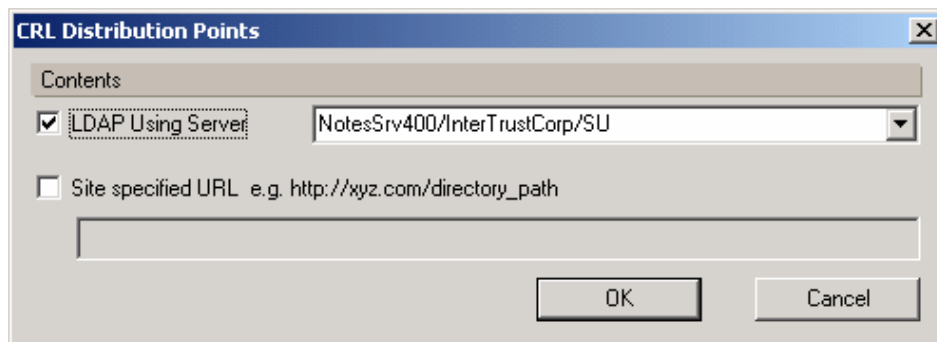


Рис. 594 По кнопке Detail возможен выбор LDAP-сервера, поддерживающего CRL - список отозванных сертификатов

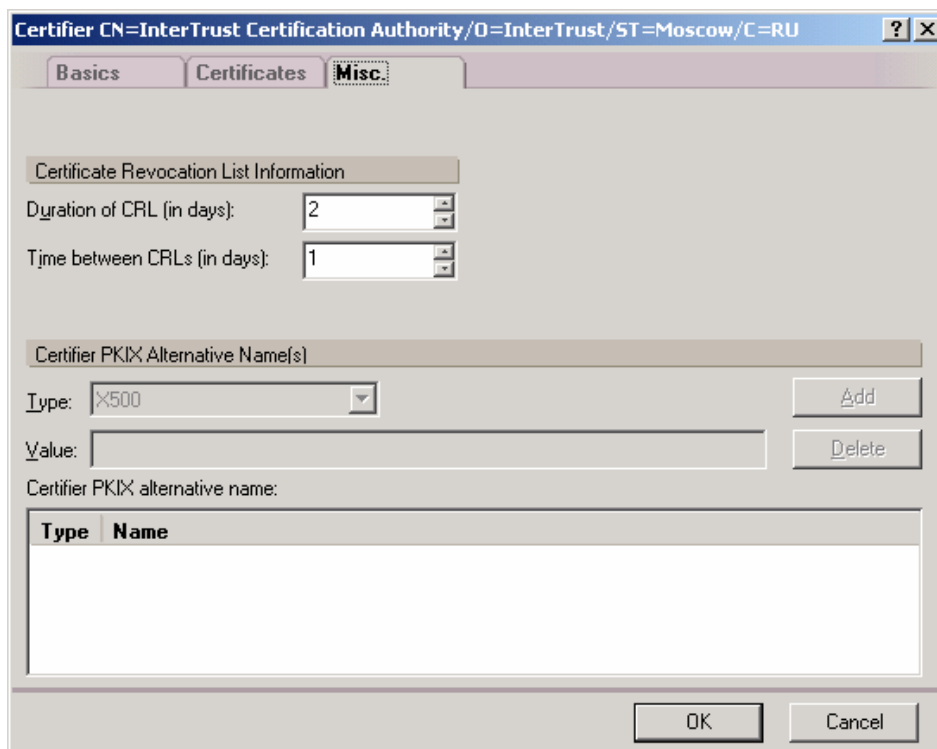


Рис. 595 Duration of CRL – число дней, в течение которого выпущенный CRL действителен. Time between CRLs – число дней между выпусками CRL

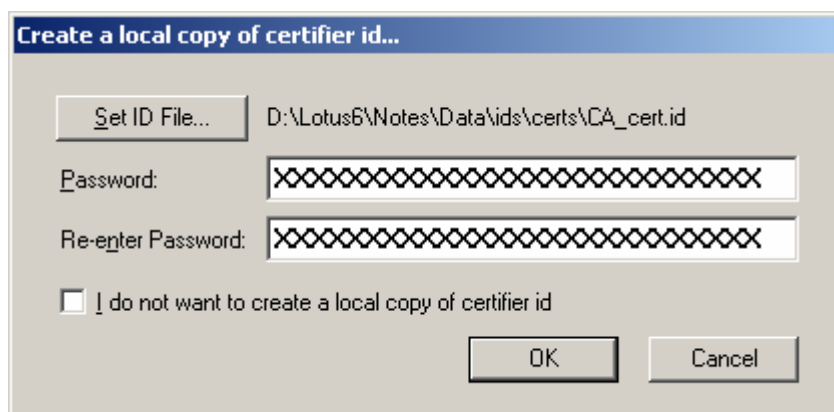


Рис. 596 Пароль для keyring-файла



Рис. 597

1.66.3.2. 1.1.3.2. Дальнейшие шаги

- • load ca – если не запущена
- • tell adminp process all – чтобы ADMINP поскорее «мигрировала» сертификатора Internet
- • tell ca refresh – чтобы задача CA загрузила сертификатора Internet (по умолчанию CA подгружает новых сертификаторов раз в 12 часов)
- • tell ca stat – для проверки
- • Создать и настроить базу CERTREQ.NSF

1.66.3.3. 1.1.3.3. База CERTREQ.NSF

Рис. 598 В браузере она «смотрится» по-старому...

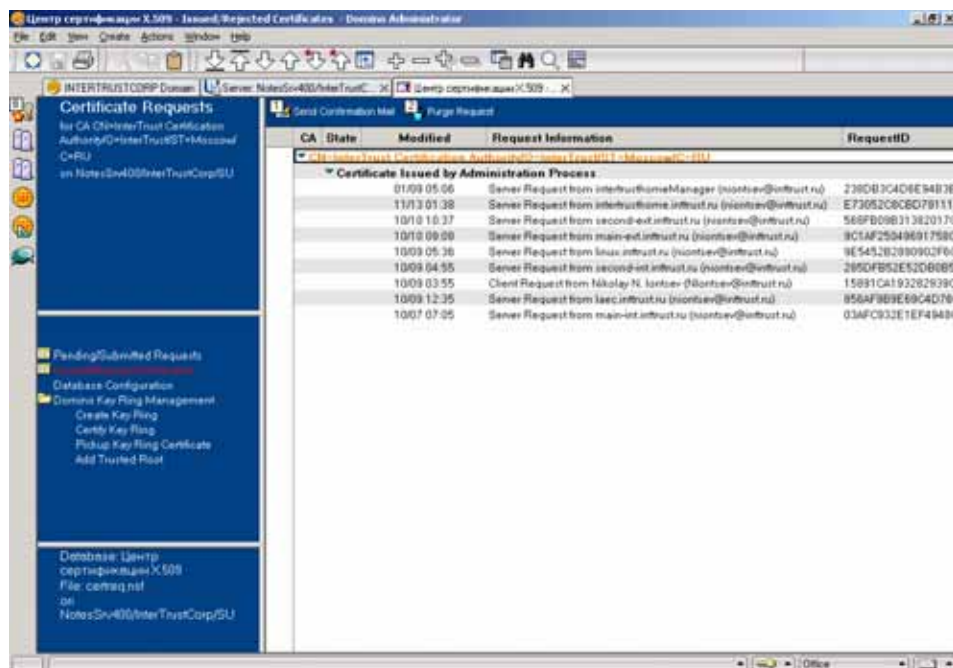


Рис. 599 Но в клиенте Notes все иначе... В ней теперь только создаются запросы на сертификаты и из нее они забираются клиентами

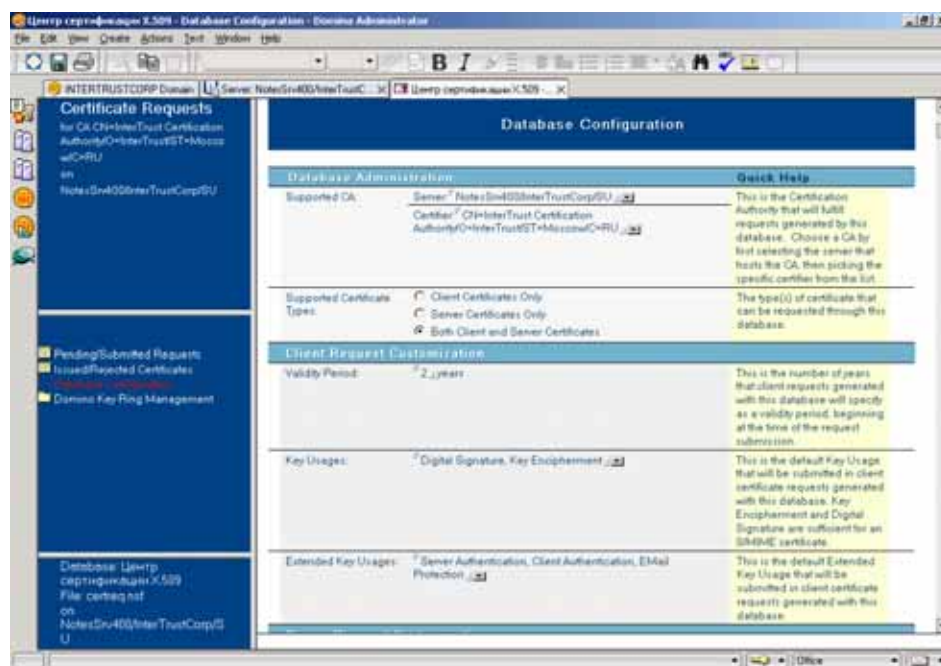


Рис. 600 Конфигурационный документ, начало

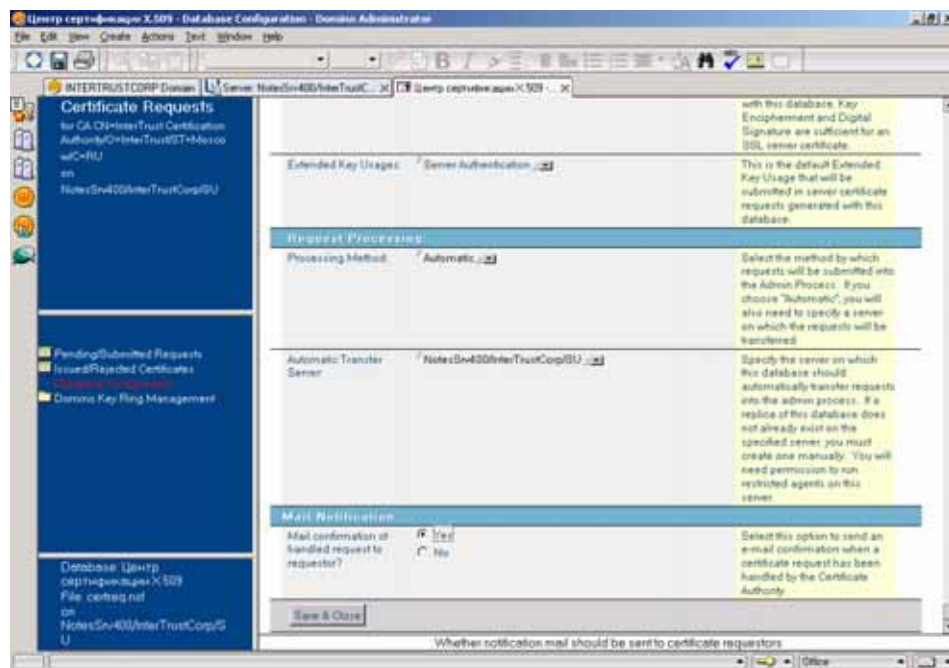


Рис. 601 Конфигурационный документ, окончание. Просматривается, что запрос на сертификат передается агентом в базу admin4.nsf, где администраторы RA «дают добро», и задача ADMINP при содействии задачи CA выпускает сертификат и помещает его назад в эту базу...

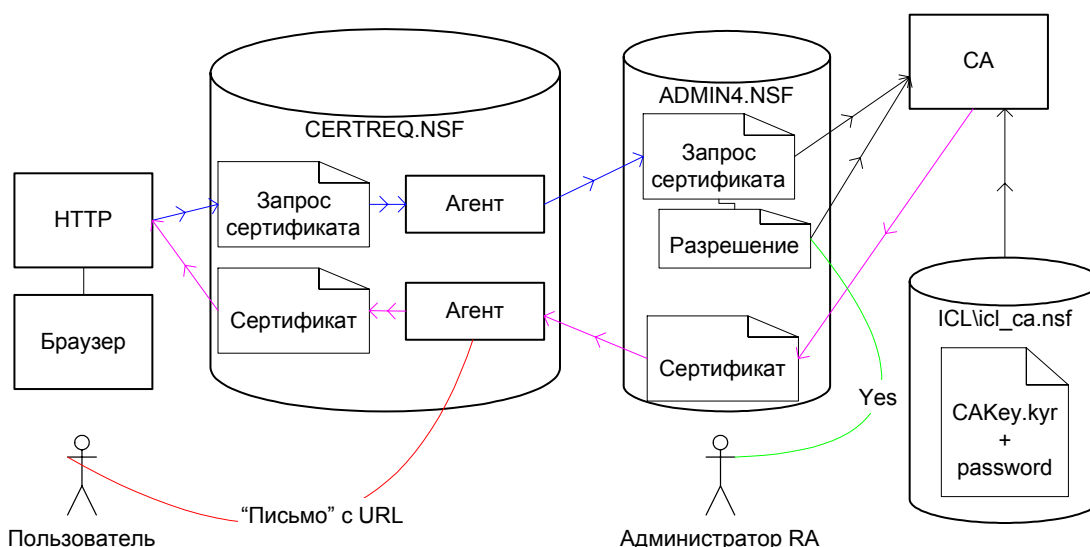


Рис. 602

1.66.3.4. 1.1.3.4. Заметки

To revoke a certificate

A CA administrator can easily revoke an Internet certificate if the subject of the certificate leaves the organization, or if the key has been compromised. After a certificate is revoked, it can never again be trusted.

If you revoke a certificate, especially if a key has been compromised, issue a non-regular CRL so that any entity checking CRLs has the most updated revocation information.

To revoke a certificate

1. From the Domino Administrator, click Files. Open the ICL directory.
2. From the list of ICL databases, open the ICL for the certifier that issued the certificate you need to revoke.
3. Open the Issued Certificates\By Subject Name view.

4. Open the Issued Certificate document for the certificate you want to revoke. The document name is the same as the subject name.
5. At the top of the document, click "Revoke Certificate."
6. In the Revocation Reason dialog box, select the reason for revoking the certificate, and click OK.
7. Issue a non-regular CRL.

The next time the CA process refreshes, the Issued Certificate document will be updated to indicate that the certificate has been revoked. When you open the Issued Certificate document again, the Revocation Information section will indicate that the certificate has been revoked, the revocation date and time, the reason for the certificate's revocation, and date and time the certificate became invalid.

Закладка Miscellaneous

Click Miscellaneous, and then click "Create a local copy of the certifier ID." Specify the certifier ID file name and password, and click OK. A copy of the certifier ID is saved to the default path ...\\notes\\data\\ids\\certs*cert.id*. You can select a different path. Use this local copy of the certifier ID as a backup to re-create the certifier if it become corrupted.

Complete these fields to specify Certificate Revocation List information for this certifier:

Field	Action
Duration of CRL (in days)	Enter the length of time, in days, for which a given CRL is valid. It is recommended that this time period extend beyond the time period between issued CRLs, as this ensures that the CRL is always valid.
Time between CRLs (in days)	Enter the time interval, in days, between issued CRLs.

Complete these fields to specify "Key and certifier certificate" information for this certifier:

Field	Action
Signing algorithm	Select the algorithm used to encrypt the certificate's signature.
Key length	Enter the key length to use for encryption. This setting determines the number of bits needed to be able to represent any of the possible values of a cryptographic key. The longer the key length, the more difficult it is to decrypt encrypted text.
Certificate will expire on	(Optional) Change the default certificate expiration date.

Complete these fields to specify the Certifier PKIX Alternative Name(s) information for this certifier:

Alternative name fields allow alternate names to be listed in certificates. Alternate subject names can appear in any certificate. If a CA has alternate names, those names should be included in the certificates it issues. For example, you can include the certifier's e-mail address in the certificates it issues, so that users know how to contact the certifier that issued them.

Note A PKIX Alternative Name is not the same as a Notes alternate name. The Notes alternate name is the foreign language version of a user name.

Field	Action
Type	Enter the type of alternative name you want to use.
Value	Enter the alternative name you want to use.

Click Add to add the alternative name to the certifier's certificate.

1.66.4. 1.1.4. Конфигурирование HTTP Server

Задача HTTP загружается командой **Load http**, а завершается командой **Tell http quit**. Чтобы задача автоматически запускалась при старте сервера, ее имя следует внести в список задач в переменной ServerTasks в файле NOTES.INI.

Основные настройки для задачи HTTP задаются на закладках Ports-InterNet Ports-Web, InterNet Protocols-HTTP и InterNet Protocols-Domino Web Engine документа Server.

1.66.4.1. 1.1.4.1. Закладка Ports-InterNet Ports-Web документа Server

Здесь задаются номера и статус портов TCP/IP, по которым задача HTTP должна ожидать обращений клиентов, а так же возможность «анонимного» доступа и (или) применяемые варианты аутентификации клиентов. Нововведение R6 – поле **Enforce server access settings**, выбором Yes в котором вы требуете, чтобы Web-клиент проходил те же проверки по списку управления доступом к серверу, что и пользователь Notes.

The screenshot shows the configuration window for the HTTP/HTTPS task in the Domino Server. The title bar reads "Server : LAEC/LAEC/InterTrustCorp/SU". The "Ports" tab is selected, and within it, the "Internet Ports" sub-tab is active. The "SSL settings" section includes fields for "SSL key file name" (laec.kyr), "SSL protocol version" (Negotiated), and radio buttons for "Accept SSL site certificates" (No) and "Accept expired SSL certificates" (Yes). Below this is the "Web (HTTP/HTTPS)" section with fields for "TCP/IP port number" (80), "TCP/IP port status" (Enabled), and "Enforce server access settings" (No). It also includes "Authentication options" for both HTTP and SSL, with "Name & password" and "Anonymous" access enabled. The "SSL Security" section lists supported ciphers (RC4, Triple DES, DES) and has an "Enable SSL V2" checkbox (unchecked).

Server : LAEC/LAEC/InterTrustCorp/SU

Basics | Security | Ports | Server Tasks | Internet Protocols | MTAs | Miscellaneous | Transactional Logging | Shared Mail | Administration

Notes Network Ports | Internet Ports | Proxies

SSL settings

SSL key file name: laec.kyr

SSL protocol version (for use with all protocols except HTTP): Negotiated

Accept SSL site certificates: ☐ Yes ☒ No

Accept expired SSL certificates: ☒ Yes ☐ No

Web | Directory | Mail | DIIOP | Remote Debug Manager

Web (HTTP/HTTPS)

TCP/IP port number: 80

TCP/IP port status: Enabled

Enforce server access settings: No

Authentication options:

Name & password: Yes

Anonymous: Yes

SSL port number: 443

SSL port status: Enabled

Authentication options:

Client certificate: Yes

Name & password: Yes

Anonymous: Yes

SSL Security

SSL ciphers: RC4 encryption with 128-bit key and MD5 MAC
RC4 encryption with 128-bit key and SHA-1 MAC
Triple DES encryption with 168-bit key and SHA-1 MAC
DES encryption with 56-bit key and SHA-1 MAC

Modify

Enable SSL V2: (SSL V3 is always enabled) ☐ Yes

Рис. 603

TCP/IP port number (по умолчанию 80). Задаёт номер порта, на котором сервер HTTP должен «ожидать» запросы по «обыкновенному» протоколу HTTP. Стандартно для

протокола HTTP используется порт 80. Не используйте значений, меньших чем 1024 (кроме стандартного 80), поскольку они зарезервированы для других прикладных программ TCP/IP. Если задается нестандартный номер порта, клиенты будут вынуждены явно указывать этот номер порта в URL. Например, URL `http://domino.lotus.com:8080/` «запрашивает» начальную страницу с хоста `domino.lotus.com`, который «ожидает» запросы по протоколу HTTP на порту 8080. После изменения номера порта, чтобы эти изменения «вступили в силу», выдается команда `Tell HTTP Restart`.

TCP/IP port status (по умолчанию Enabled). Выбор Enabled разрешает серверу HTTP обслуживать запросы по «обыкновенному» протоколу HTTP, выбор Disabled - запрещает обслуживать запросы по «обыкновенному» протоколу HTTP, а выбор Redirect to SSL требует «перенаправлять» запросы на порт с поддержкой SSL (по тому же URL, но с «префиксом протокола» `https://`). Должно быть разрешено обслуживание запросов хотя бы по одному из двух возможных портов: «обыкновенному» (TCP/IP port status) или с поддержкой SSL (SSL port status). Если обслуживание запрещено по обоим портам, сервер HTTP не сможет функционировать.

SSL port number (по умолчанию 443). Задает номер порта, на котором сервер HTTP должен «ожидать» запросы по протоколу HTTP с поддержкой SSL. После изменения номера порта, чтобы изменения «вступили в силу», выдается команда `Tell HTTP Restart`.

SSL port status (по умолчанию Disabled). Выбор Enabled разрешает серверу HTTP обслуживать запросы по протоколу HTTP с поддержкой SSL, а выбор Disabled - запрещает. Бессмысленно «разрешать» поддержку SSL, если для сервера не создан KeyRing-файл (его имя должно задаваться в поле **SSL key file**).

При работе по «обыкновенному» протоколу HTTP возможен как «анонимный» доступ (Yes в поле в строке Anonymous в верхней половине таблицы), так и аутентификация клиента по введенным им имени и паролю (Yes в поле в строке Name & password в верхней половине таблицы).

Если разрешен «анонимный» доступ, обратившийся к серверу HTTP-клиент «будет фигурировать на сервере» под именем Anonymous. Доступ такого клиента в каждой базе Notes определяется прежде всего списком управления доступом этой базы: как Anonymous или, если в ACL отсутствует имя Anonymous, как -Default-, но не выше максимального уровня доступа для HTTP-клиентов (поле Maximum Internet name & password access в ACL базы).

Если на сервере разрешена аутентификация клиента по введенным им имени и паролю (Yes в поле в строке Name & password в верхней половине таблицы), но «анонимный» доступ запрещен (No в поле в строке Anonymous в верхней половине таблицы), все HTTP-клиенты при обращении к серверу Domino «сразу» получают запрос на ввод имени и пароля. Если же на сервере разрешены как аутентификация клиента по введенным им имени и паролю (Yes в поле в строке Name & password в верхней половине таблицы), так и «анонимный» доступ (No в поле в строке Anonymous в верхней половине таблицы), все зависит от списка управления доступом базы, к которой обращается HTTP-клиент. Если к этой базе возможен «анонимный» доступ, то запроса на ввод имени и пароля не последует. Если же Anonymous и -Default- не имеют доступа к базе, клиенту придется ввести имя и пароль.

При работе по протоколу HTTP с поддержкой SSL возможны «анонимный» доступ (Yes в поле в строке Anonymous в нижней половине таблицы), аутентификация клиента по введенным им имени и паролю (Yes в поле в строке Name & password в нижней половине таблицы) и аутентификация клиента по информации из его сертификата стандарта X.509 (Yes в поле в строке Client certificate в нижней половине таблицы). Последний вариант аутентификации удобен тем, что клиенту не требуется вводить имя и пароль.

1.66.4.2. 1.1.4.2. Закладка InterNet Protocols-HTTP документа Server

Server : LAEC/LAEC/InterTrustCorp/SU	
Basics Security Ports Server Tasks Internet Protocols MTAs Miscellaneous Transactional Logging Shared Mail Administration	
HTTP Domino Web Engine DIIOP LDAP	
Basics	Mapping
Host name(s): laec.intrust.ru	Home URL: /EDU/intrustlaec.nsf
Bind to host name: Disabled	HTML directory: domino\html
DNS lookup: Disabled	Icon directory: domino\icons
DNS lookup cache: Enabled	Icon URL path: /icons
DNS lookup cache size: 256	CGI directory: domino\cgi-bin
DNS lookup cache found timeout: 120 seconds	CGI URL path: /cgi-bin
DNS lookup cache not found timeout: 240 seconds	
Number active threads: 20	

Рис. 604 Начало закладки

Группа полей Basics

Host name (по умолчанию пусто). Поле может содержать список имен хостов или IP-адресов компьютера, на котором установлен сервер Domino.

Bind to host name (по умолчанию Disabled). Выбирать в этом поле значение Enabled следует только в том случае, когда на вашем компьютере несколько IP-адресов и, возможно, установлены несколько серверов Domino (partitioned server), поддерживающих более одной задачи HTTP. В такой ситуации нужно «уточнить», по каким IP-адресам должно производиться обращение к задаче HTTP на конкретном сервере Domino. Это и достигается указанием в поле Host name IP-адресов или имен хостов (что определяет IP-адрес) и выбором Enabled в поле Bind to host name. Например, на одном компьютере, имеющем IP-адреса 194.220.133.11 (www1.acme.com) и 194.220.133.12 (www2.acme.com), установлены два сервера Domino (NotesServer1/Acme/US и NotesServer2/Acme/US). В документе Server для NotesServer1/Acme/US в поле Host name содержится www1.acme.com, а в документе Server для NotesServer2/Acme/US соответственно www2.acme.com. В обоих документах Server в поле Bind to host name выбрано Enabled. В результате обращения по URL http://www1.acme.com/... обрабатываются задачей HTTP сервера NotesServer1/Acme/US, а обращения по URL http://www2.acme.com/... обрабатываются задачей HTTP сервера NotesServer2/Acme/US.

DNS lookup (по умолчанию Disabled). Выберите Enabled, если требуется, чтобы сервер HTTP выполнял поиск имени хоста каждого своего клиента по его IP-адресу, обращаясь к серверам DNS. Выбор Enabled ухудшает эффективность работы сервера HTTP, однако в протоколах работы сервера HTTP будут содержаться имена хостов клиентов, а не IP-адреса, и в фильтрах протоколирования вы сможете использовать как маски на основе имен хостов клиентов, так и маски на основе IP-адресов клиентов. Если же выбрано Disabled, сервер HTTP не обращается к серверам DNS для определения имени хоста клиента. Выбор Disabled улучшает эффективность работы сервера HTTP, однако в протоколах работы HTTP будут содержаться только IP-адреса клиентов и в фильтрах протоколирования вы сможете использовать маски только на основе IP-адресов клиентов. Остальные поля **DNS lookup...** являются нововведением R6 и отвечают за настройки кэша имен хостов и IP-адресов для протоколирования.

Number active threads (по умолчанию 40). Задаёт количество потоков (thread's), порождаемых задачей HTTP. Когда все потоки заняты, запросы клиентов «ожидают в очереди» освобождения потоков. Чем более мощный компьютер используется в качестве сервера, тем и большее максимально возможное количество подпроцессов может задаваться в этом поле.

Группа полей Mapping

Группа полей Mapping задает реальное местоположение каталогов HTML-файлов, пиктограмм и CGI-программ и определяет URL для доступа к ним. Учтите, что на одном компьютере «под одним сервером Notes» может функционировать несколько виртуальных серверов. В этом случае для каждого виртуального сервера информация из группы полей Mapping «перекрывается» аналогичной информацией из документов Virtual Server.

Home URL (по умолчанию /homepage.nsf). Относительный URL элемента из базы данных Notes (например, документа About или навигатора), HTML-образ которого сервер HTTP должен возвращать, когда клиенты «входят на сервер», не указывая в URL требуемый им каталог или страницу (http://host-name/). Если вы используете начальную страницу (home page) непосредственно в формате HTML, в R6 укажите имя HTML-файла в этом же поле. В предыдущих же версиях «очистите» поле Home URL и укажите имя HTML-файла в поле Default home page.

HTML directory (по умолчанию domino\html). Каталог для HTML-файлов. Если указан не полный путь, он «отсчитывается» относительно каталога данных.

Icon directory (по умолчанию domino\icons). Каталог пиктограмм. Если указан не полный путь, он «отсчитывается» относительно каталога данных.

Icon URL Path (по умолчанию /icons). Относительный URL для каталога пиктограмм. Например, чтобы «открыть в броузере» файл abook.gif или форму search.htm, находящиеся в подкаталоге domino\icons каталога данных, необходимы URL http://host-name/icons/abook.gif или http://host-name/icons/search.htm. В большинстве случаев не следует изменять исходное значение этого поля.

CGI directory (по умолчанию domino\cgi-bin). Каталог для программ CGI. Если указан не полный путь, он «отсчитывается» относительно каталога данных.

CGI URL path (по умолчанию /cgi-bin). Относительный URL для каталога программ CGI на сервере Domino. Например, для запуска CGI-программы CGITest.exe, находящейся в подкаталоге domino\cgi-bin каталога данных, необходим URL http://host-name/cgi-bin/CGITest.

R5 Basics		Log File Settings	
Allow HTTP clients to browse databases:	☐ Yes ☒ No	Access log format:	Common
Maximum requests over a single connection:	1	Time format:	LocalTime
Minimum active threads: (Prior to 4.6 only)	20	Log file duration:	Daily
Default home page:	default.htm	Maximum log entry length:	10 kilobytes
Maximum cached commands:	128	Maximum size of access log:	0 megabytes
Optimize HTTP performance based on the following primary activity:	Advanced (Custom Settings)		
Enable Logging To:		DSAPI	
Log files:	Disabled	DSAPI filter file names:	ndolextn.dll
Domlog.nsf:	Enabled		
Log File Names		Exclude From Logging	
Directory for log files:		URLs:	
Access log:	access	Methods:	
Agent log:	agent	MIME types:	
Referer log:	referer	User agents:	
Error log: (R4 and R5 only)	error	Return codes:	
CGI error log:	cgi-error	Hosts and domains:	

Рис. 605 Продолжение закладки

Группа полей R5 Basics

Поля в этой группе не используются в R6. Однако упомянем некоторые...

Default home page (по умолчанию default.htm). Если в качестве начальной страницы (home page) должен использоваться обычный файл в формате HTML, укажите в этом поле имя файла и «очистите» поле Home URL в группе полей Mapping.

Allow HTTP clients to browse databases (по умолчанию No). Если в поле выбрано Yes, клиенты, указав URL `http://host-name/?OpenServer`, смогут получить список баз данных на, а из него, «переходя по ссылкам», предпринимать попытки открыть и сами базы. Когда же выбрано No, клиенты не смогут получить список имеющихся на сервере баз, но смогут открывать конкретные базы данных, если знают их имена файлов и имеют к ним доступ. В R6 URL `http://host-name/?OpenServer` вообще не поддерживается.

Группа полей DSAPI

Список dll, удовлетворяющих требованиям DSAPI, подгружаемых HTTP и используемых им в работе. Могут заменять процесс аутентификации или выполнять redirect части URL на другой HTTP-сервер, получать от него ответ, а ответ клиенту «формировать от себя». `ndolextn` (`libdolextn` в UNIX) – поддержка DOLS. `domino5_http` – (можно полный путь `c:\Program Files\WebSphere\AppServer\bin\domino5_http.dll`) – WebSphere HTTP plugin – редирект `.jsp, /servlet/` на WAS с возвратом HTML «от себя».

Группы полей Log File Setting, Enable Logging To, Log File Names и Exclude From Logging

Конфигурируют процесс протоколирования обращений к серверу Domino. По каждому HTTP-запросу, выполняемому браузером, сервер HTTP способен протоколировать следующую информацию: с какого IP-адреса (или имени хоста) поступил запрос, какой браузер использовал клиент, какой URL использовался для доступа, сколько байт было передано, какой был код возврата/ошибки, сколько миллисекунд заняла обработка запроса. Протоколируемая информация может быть

сохранена или в текстовом файле, или в базе данных с именем DOMLOG.NSF, или в обоих местах сразу. Протоколирование в текстовые файлы «включается» в поле **Log files**, а протоколирование в базу данных DOMLOG.NSF – в поле **Domlog.nsf**. База данных DOMLOG.NSF создается в каталоге данных Notes по шаблону Domino Web Server Log (DOMLOG.NTF). Протоколирование в базу данных при «малом ежедневном» количестве запросов обычно более удобно, но требует привлечения несколько больших ресурсов компьютера, чем протоколирование в текстовый файл. При «большом ежедневном» количестве запросов база DOMLOG.NSF «начинает измеряться гигабайтами» и создает огромную нагрузку на индексер, поэтому приходится протоколировать в текстовые файлы.

При протоколировании в текстовые файлы в поле **Access log format** можно выбрать менее подробный (Common) или более подробный (Extended Common) формат файла **Access log** (ACCESS-LOG). Поле **Time format** определяет формат, в котором записывается время обращения. Файлы ежедневных протоколов создаются в каталоге, указанном в поле **Directory for log files**, причем в день создается пять файлов: **Access log** (ACCESS-LOG), **Agent log** (AGENT-LOG), **Error log** (ERROR-LOG) – кроме R6, **CGI error log** (CGI-ERROR-LOG), **Referer log** (REFERER-LOG). В скобках указаны «имена по умолчанию» для этих файлов. Имена файлов могут быть изменены в «одноименных» полях. В качестве расширения для файлов выбирается дата их создания.

В группе полей **Exclude From Logging** определяются «исключения из протоколирования»:

- • **URLs** – список URL или «шаблонов» URL, например *.gif.
- • **Methods** – список запросов, например, POST и DELETE.
- • **MIME types** – список MIME-типов, например image/gif.
- • **User agents** – список браузеров, например Mozilla.
- • **Return codes** – список кодов возврата, например 300.
- • **Hosts or domains** – список IP-адресов, имен хостов или их «шаблонов», например 130.333.* или *.edu.

Timeouts		R5 Timeouts	
HTTP persistent connections:	☐ Enabled	Input timeout:	2 minutes
Maximum requests per persistent connection:	5	Output timeout:	300 minutes
Persistent connection timeout:	180 seconds	CGI timeout:	5 minutes
Request timeout:	60 seconds	Idle thread timeout:	0 minutes
Input timeout:	15 seconds		
Output timeout:	180 seconds		
CGI timeout:	180 seconds		
Network Settings		HTTP Protocol Limits	
Listen queue size:	512	Maximum URL length:	4 kilobytes
Maximum number of concurrent network sessions:	2000	Maximum number of URL path segments:	64
IP address allow/deny priority:	☐ Allow	Maximum number of request headers:	48
IP address allow list:		Maximum size of request headers:	16 kilobytes
IP address deny list:		Maximum size of request content:	10000 kilobytes (specify 0 to allow unlimited content)

Рис. 606 Окончание закладки

Группы полей Timeouts и R5 Timeouts

Задаются величины различного рода таймаутов.

Группа полей Network Settings (R6)

IP address allow/deny priority	Specify which IP address list -- Allow or Deny -- takes priority if an incoming IP address is listed in both the allow list and the deny list (this can happen when both lists contain wildcards). The default is that the Allow list takes priority.
IP address allow list	List the IP addresses that are allowed to access the ports.
IP address deny list	List the IP addresses that are denied access to the ports.

Группа полей HTTP Protocol Limits (R6)

Maximum URL length	Enter the maximum size, in KB, allowed for URLs received from HTTP clients. The length includes the query string. The default is 4KB. Increase the default only if you host an application that requires an extremely long URL.
Maximum number of URL path segments	Enter the number of segments allowed. The default is 64, which is usually more than enough. A segment is delimited by slashes; for example, the URL "/products.nsf/widgets" contains two segments.
Maximum number of request headers	Enter the total number of HTTP request headers allowed. The default is 48. Normally, there is no need to increase the setting; typical requests sent from browsers usually include less than a dozen headers.
Maximum size of request headers	Enter the total length, in KB, of all the headers in the request. The default is 16KB.
Maximum size of request content	Enter the total amount of data, in MB, that can be contained in a request. The default is 10MB. The two most common ways for users to send data to the server is by submitting forms or by uploading files. If none of the applications on the server allow users to upload large files, you can probably set this to a much lower value.

1.66.4.3. 1.1.4.3. Закладка InterNet Protocols-Domino Web Engine документа Server

Server : LAEC/LAEC/InterTrustCorp/SU

Basics | Security | Ports | Server Tasks | Internet Protocols | MTAs | Miscellaneous | Transactional Logging | Shared Mail | Administration

HTTP | Domino Web Engine | DIIOP | LDAP

HTTP Sessions Session authentication: Multiple Servers (SSO) Web SSO Configuration: LtpaToken Generating References to this Server Does this server use IIS? No Protocol: http Host name: Port number: 80	Java Servlets Java servlet support: Domino Servlet Manager Servlet URL path: /dominoservlet Class path: domino\servlet Servlet file extensions: Session state tracking: Enabled Idle session time-out: 30 minutes Maximum active sessions: 1000 Session persistence: Disabled POST Data Maximum POST data (in 0 kilobytes): File compression on upload: Disabled
Memory Caches Maximum cached designs: 128 Maximum cached users: 64 Cached user expiration interval: 120 seconds	

Рис. 607 Начало закладки

Группа полей HTTP Sessions

Выбор способа аутентификации. Для SSO необходим документ Web SSO Configuration.

Группа полей Generating References to this Server

Использовалось при установке Domino HTTP «под» IIS в R5 – IIS снабжался dll стандарта ISAPI разработки Lotus.

В R6 такой способ устарел. На внешний HTTP-сервер ставится WebSphere HTTP Plugin и конфигурируется в файле plugin.cfg («какие URL передавать Domino HTTP»). В Notes.ini надо добавить HTTPEnableConnectorHeaders=1.

Группа полей Java Servlets

Сервлеты поддерживаются, но API довольно старое. У меня url /servlet заменен на /dominoservlet. Поскольку в Domino HTTP эта подсистема развиваться более не будет (и поделом...), в качестве «движка» сервлетов и JSP используют WebSphere Application Server, а на Domino HTTP ставят WebSphere HTTP Plugin с файлом plugin.cfg, передающим URL /servlet/*, *.jsp и подобные на WAS.

Группа полей POST DATA

Maximum POST Data – ограничение на количество данных, которые клиент за одну операцию POST может передать на сервер. 0 – нет ограничения.

File compression on upload – при Enabled переданный с клиента присоединенный файл помещается в созданный документ в «сжатом виде» (флаг Compressed). Хотя место экономится, при скачивании этого файла по HTTP не будет поддерживаться "докачка". Поэтому ради поддержки "докачки" в этом поле оставляют Disabled. Но важно другое – все файлы и из клиента Notes помещать в документы со снятым флагом Compressed.

Группа полей Memory Caches

Для повышения производительности HTTP-сервера используются два кэша в виртуальной памяти.

- • **Кэш с информацией для быстрого доступа к элементам дизайна баз данных.** Когда клиент броузера «впервые открывает» базу данных, задача HTTP просматривает все элементы дизайна базы (формы, виды, агенты...) и создает таблицу, сопоставляющую имени каждого элемента дизайна его идентификатор. Эта таблица позволяет по идентификаторам более быстро извлекать из базы те элементы дизайна, которые нужны для генерации HTML-страницы, запрошенной клиентом (например, форму «для показа» документа). Кэширование таких таблиц в виртуальной памяти способствует уменьшению времени отклика для клиентов. В поле **Maximum cached designs** задается максимальный размер этого кэша.
- • **Кэш с информацией об именах и паролях аутентифицированных пользователей и их принадлежности к группам.** Когда клиент броузера впервые обращается в базу, «требующей» аутентификации клиента, ему приходится ввести свое имя и пароль. По завершении процесса аутентификации имя, пароль и информация о принадлежности этого имени к группам из адресной книги помещается в кэш и содержится в нем в течение указанного в поле **Cached users expiration interval** количества секунд. Если клиент вновь обращается к базе данных, «требующей» аутентификации, но информацию об этом клиенте удастся найти в кэше, клиенту не требуется в очередной раз вводить имя и пароль, а серверу – выяснять принадлежность клиента к группам. В поле **Maximum cached users** задается максимальный размер этого кэша.
- • В R4/5 поддерживался **кэш HTML-страниц** (поле **Maximum cached HTTP commands**). В R6 этот кэш не конфигурируется, но по всем признакам несомненно поддерживается...

Web User Preferences		Language	
Store user preferences in cookies:	☐ Multi-server	Default string resource language:	☐ English
Default regional locale:	☐ Browser's accept-language	Additional string resource languages:	☐
Conversion/Display		Character Set	
Image conversion format:	☐ GIF	Use UTF-8 for output:	☐ Yes
Interlaced rendering:	☐ Enabled	Use UTF-8 for HTML forms:	☐ Yes
Default lines per view page:		Default character set group:	
☐ 30		☐ Cyrillic	
Maximum lines per view page:	☐ 1000		
Default search result limit:	☐ 250		
Maximum search result limit:	☐ 1000		
Make this site accessible to web search site crawlers:	☐ Disabled		
Redirect to resolve external links:	☐ Disabled		
NOTE: The following settings are no longer used in Domino. You should use them only for servers running versions prior to 5.0			
Cache directory:			
☐ dominolcache			
Maximum cache size:	☐ 50 (MB)		
Delete cache on shutdown:	☐ Disabled		
Garbage collection:	☐ Enabled		
Garbage collection interval:	☐ 60 minutes		
Run web agents concurrently?		Character set in header:	
☐ Enabled		☐ Enabled	
		Meta character set:	
		☐ Enabled	

Рис. 608 Окончание закладки

Группа полей Conversion/Display

Default lines per view page (по умолчанию 30). Количество строк из вида в базе данных Notes, возвращаемое сервером HTTP в браузер за один запрос. Это лишь «значение по умолчанию», но оно касается всех баз на сервере. Клиент браузера в каждом конкретном случае может изменить получаемое им количество строк из вида, указав в URL параметр &Count наподобие <http://host-name/db-name.nsf/view-name?OpenView&Start=1&Count=9999&ExpandView>. Желание клиента «урезается» значением из поля Maximum lines per view page.

Default search result limit и **Maximum search result limit** – аналогичные ограничения на количество ссылок на документы, возвращаемых при полнотекстовом поиске.

Make this site accesible to web search site crawlers – замена «?» на «!» в URL. По моим наблюдениям лучше не использовать, а явно добавлять в код страниц тег <META name="Robots" CONTENT="INDEX,FOLLOW">.

Группа полей Character Set

Default character set group (по умолчанию Western). Набор символов, в котором HTML-текст будет предоставляться клиенту. Чтобы обеспечить 100%-правильную поддержку «русских букв» во всех местах, выбирают Cyrillic.

Use UTF-8 for output. Если выбрано No, в поле Cyrillic можно выбрать таблицы кодов символов ISO-8859-5, CP1251 или KOI8-R. Если выбрано Yes, вывод идет в UTF-8.

Use UTF-8 for HTML forms. Если выбрано No, передача формы на сервер выполняется в UTF-8.

Группа полей в конце закладки

Run web agents concurrently? – конечно, ибо в этом случае агенты выполняются параллельно в потоках, а не один за другим в одном специальном потоке. Но разработчики должны писать агентов, используя, где надо, семафоры при изменении «общего ресурса».

Character set in header – сервер должен добавлять в заголовки передаваемых клиенту «пакетов» HTTP информацию о наборе символов. Лучше выбрать.

Meta character set – сервер должен добавлять в код страниц тег <META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=windows-1251"> с указанием набора символов. Обычно тоже не мешает...

1.66.5.

1.1.5. Использование Internet Sites



Рис. 609 Этот рисунок - ссылка на статью LDD по теме

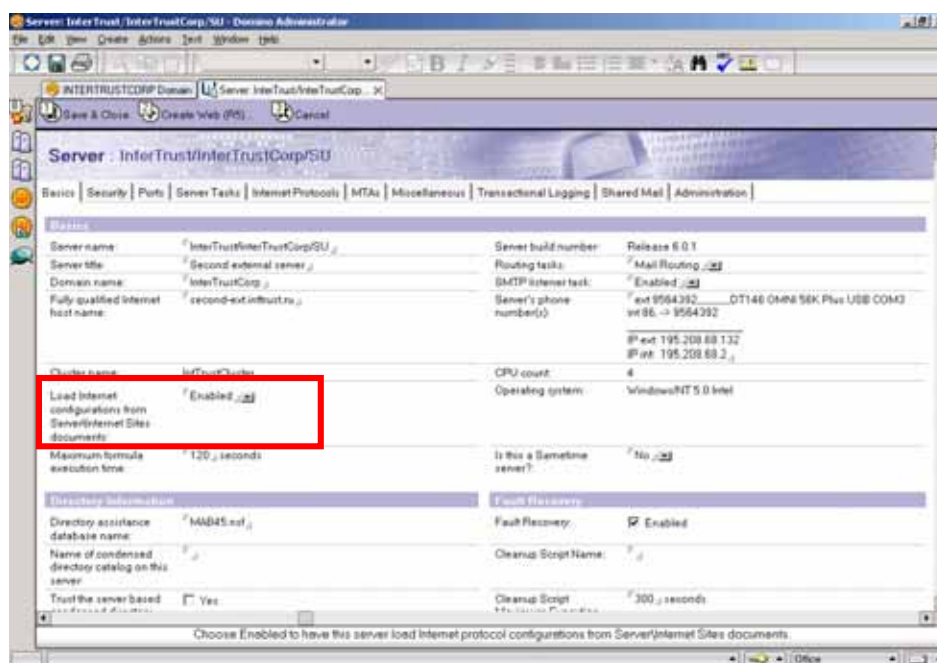


Рис. 610 Разрешение использовать документы из вида Internet Sites вместо «старых» Web Server Configuration

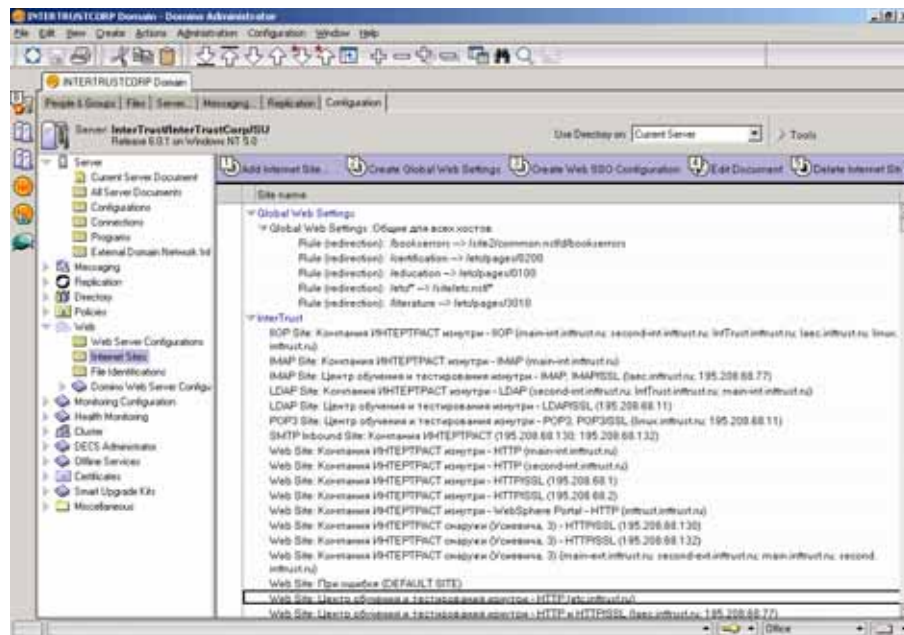


Рис. 611 Вид Internet Sites

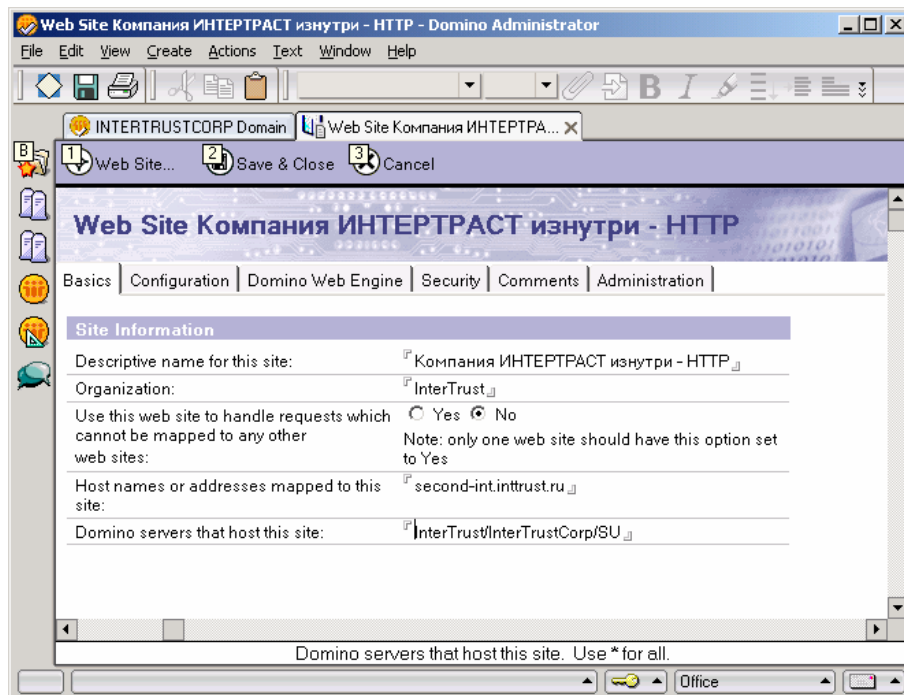


Рис. 612 Документ Web Site из вида Internet Sites, закладка Basics

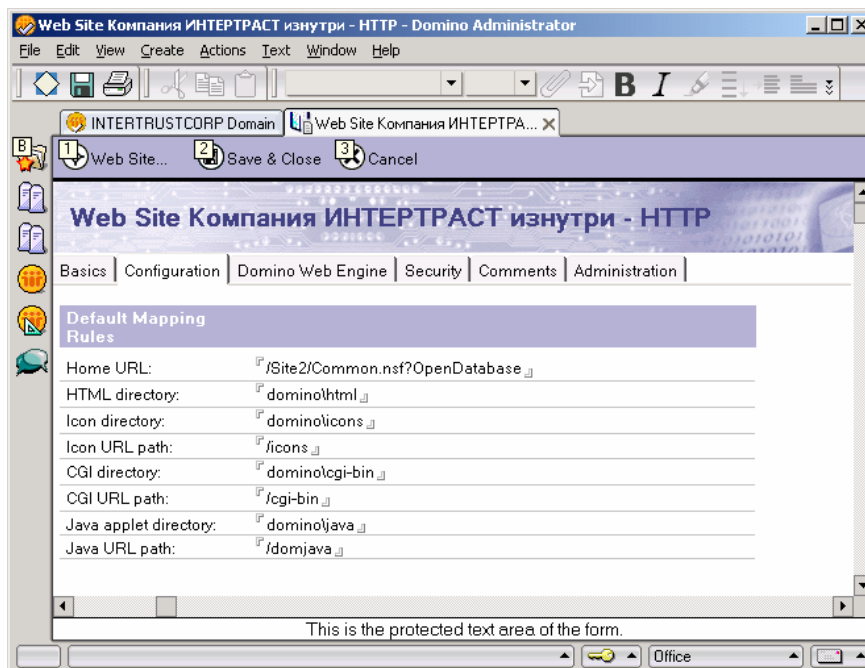


Рис. 613 Зкладка Configuration – начало

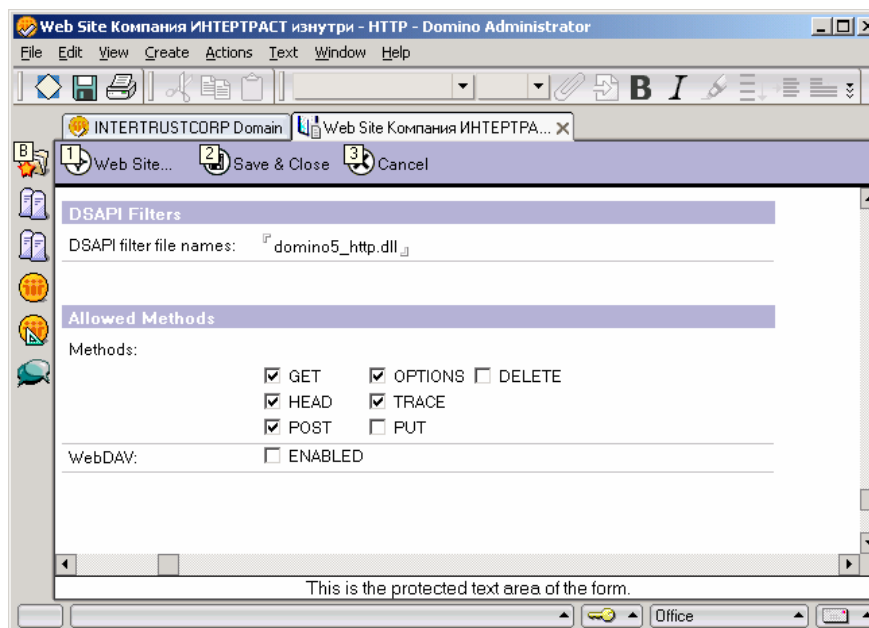


Рис. 614 Зкладка Configuration – окончание

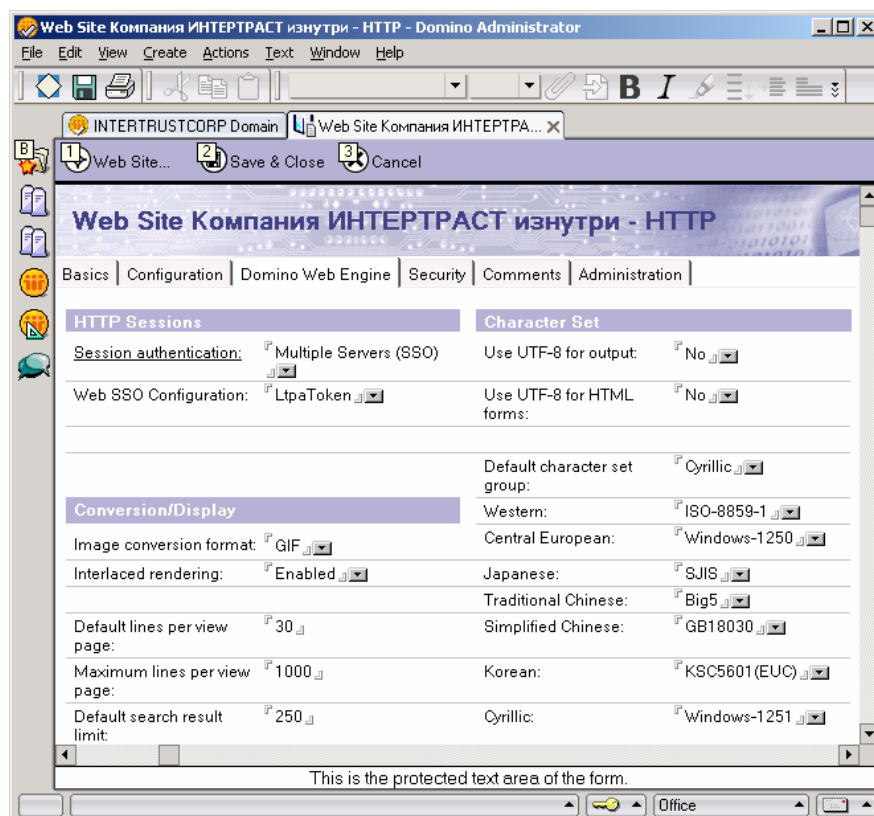


Рис. 615 Закладка Domino Web Engine - начало

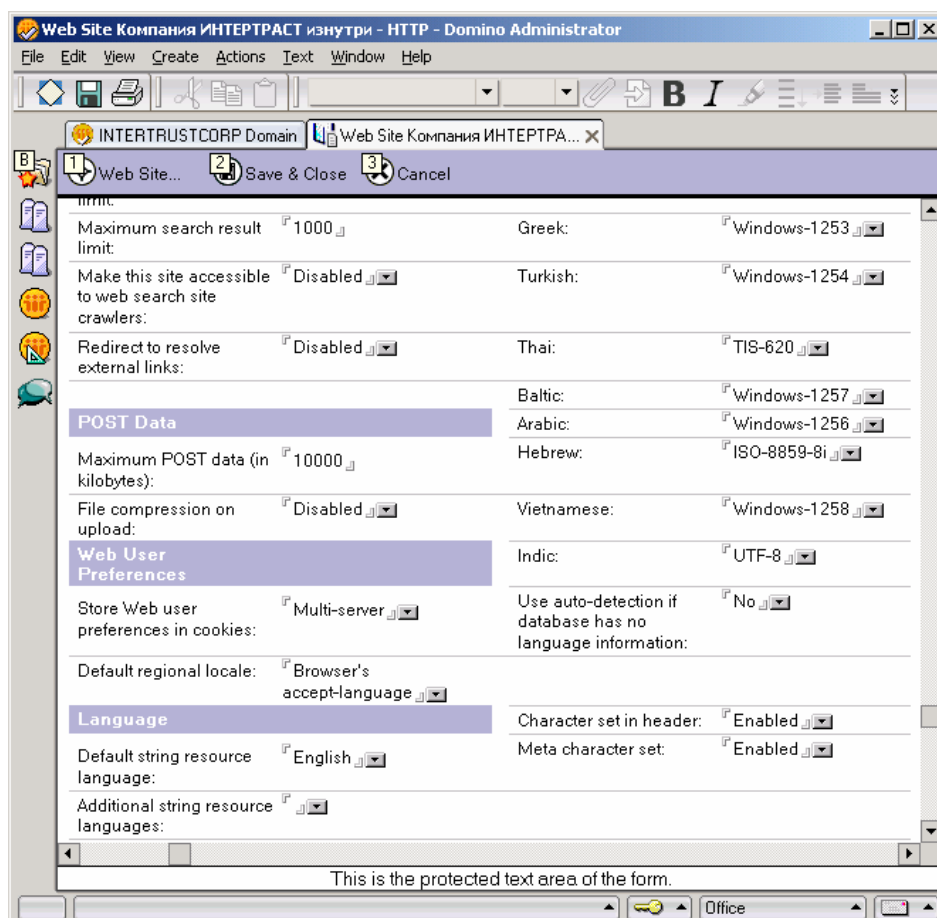


Рис. 616 Закладка Domino Web Engine – окончание

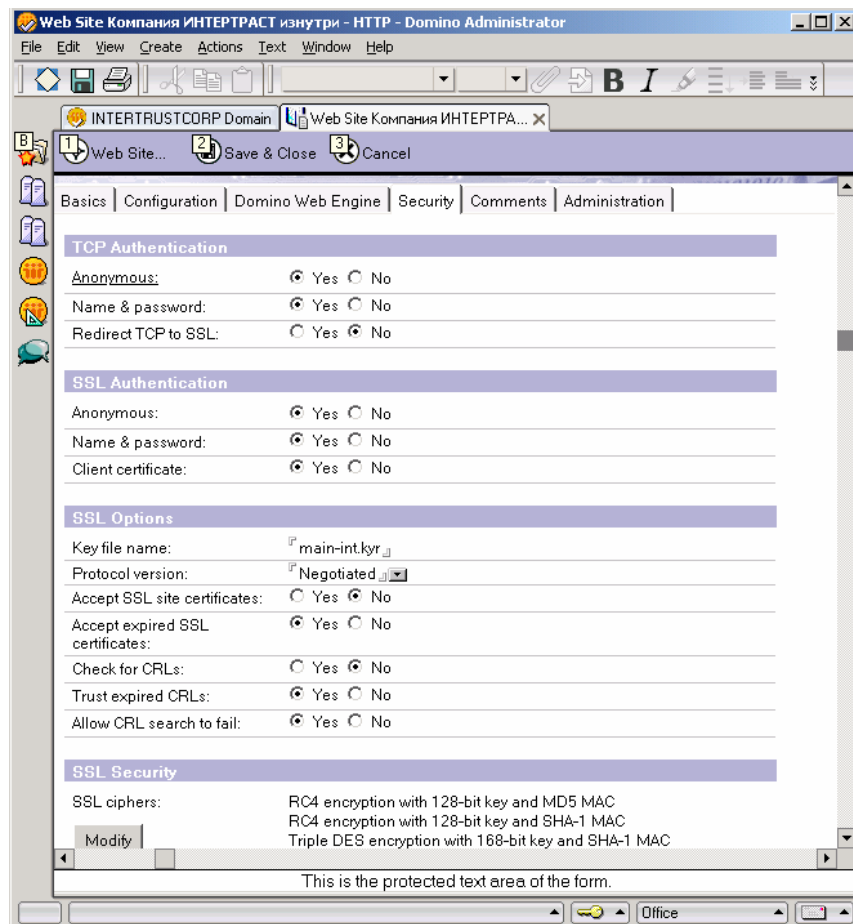


Рис. 617 Закладка Security

Для WebSite или Global Web Settings можно создавать документы Site Rules:

- • URL -> URL (Substitution),
- • URL -> Redirection URL (Redirection),
- • URL -> Directory (Directory).

Документы этих типов имелись и ранее, но теперь полная гибкость: привязать их к сайту или ко всем сайтам.

ВНИМАНИЕ! Включив в документе Server использование вида Internet Sites, Вы далее вынуждены создавать аналогичные POP3, IMAP, LDAP, SMTP Inbound, POP Sites – без них соответствующие задачи не отвечают на запросы клиентов.

1.66.6. 1.1.6. Организация поддержки WebDAV на сайте

1.66.6.1. 1.1.6.1. Документ WebSite в виде Internet Sites

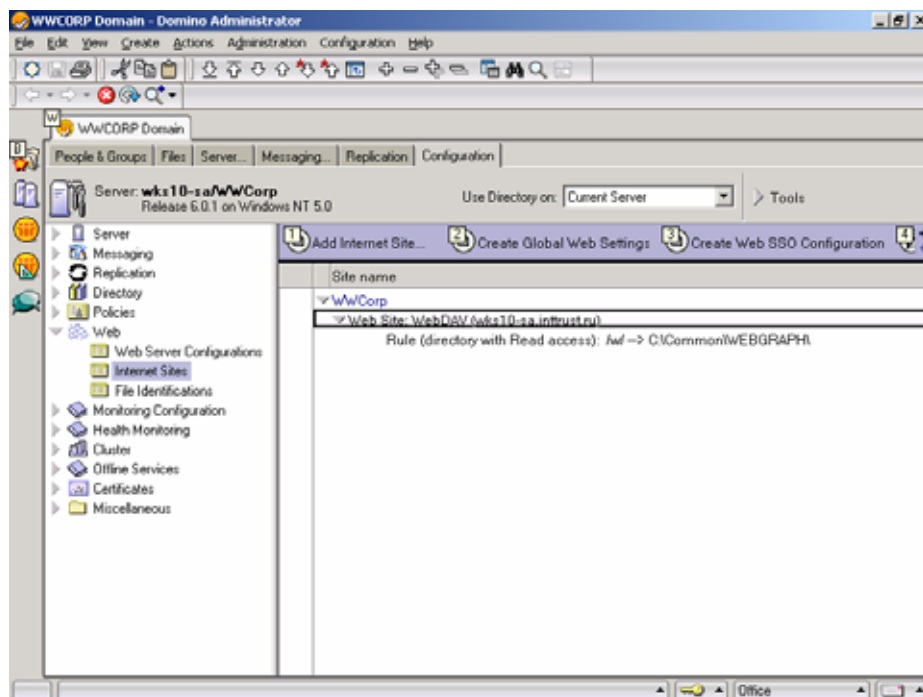


Рис. 618 В виде Internet Sites создается или модифицируется документ Web Site

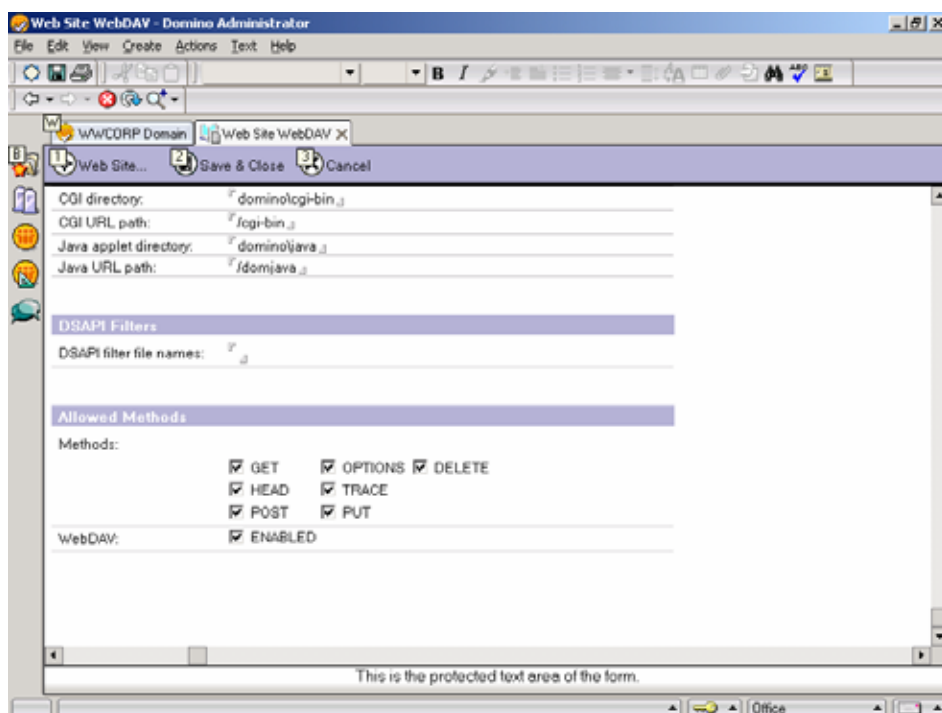


Рис. 619 В документе надо включить флаг WebDAV – при этом остальные нужные флаги включатся сами

1.66.6.2. 1.1.6.2. Подготовка базы

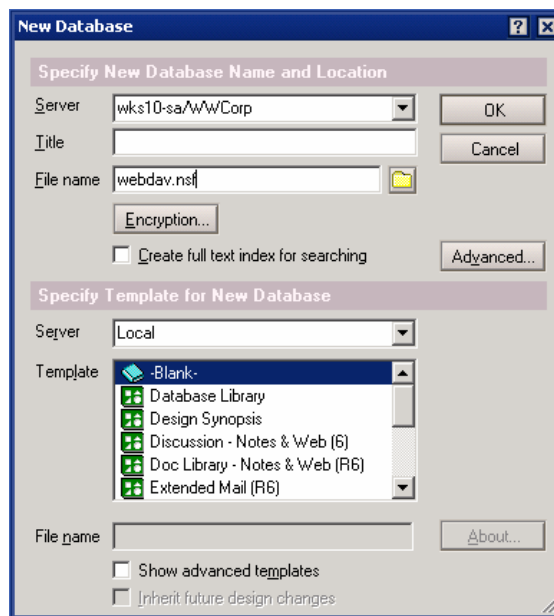


Рис. 620 База на сервере по шаблону -Blank-

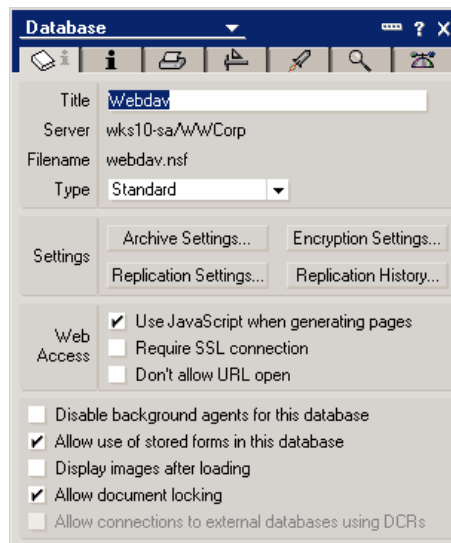


Рис. 621 В свойствах базы флаг Allow document locking

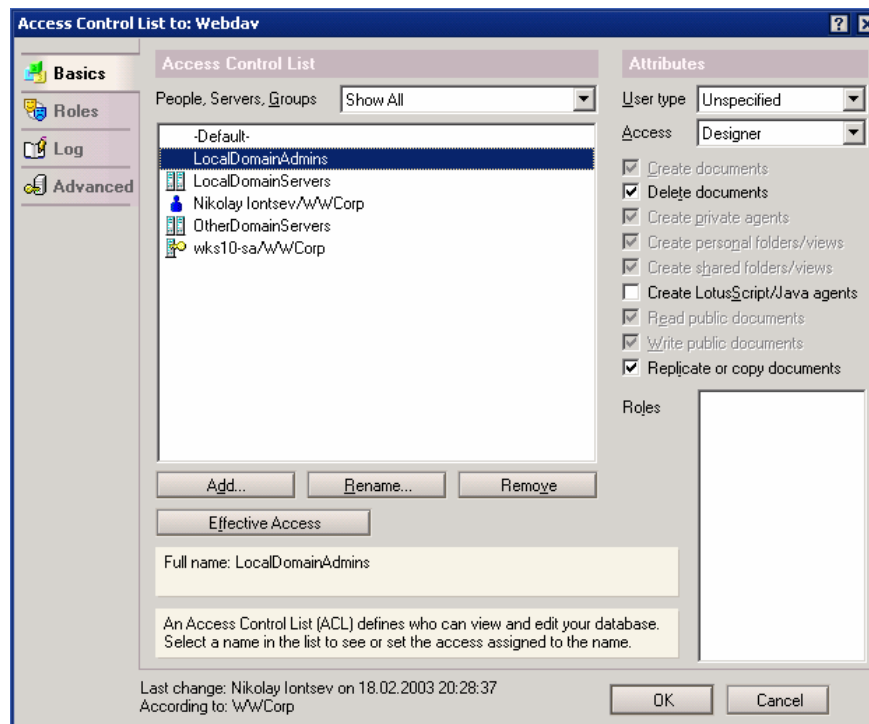


Рис. 622 В ACL субъекты, использующие webDAV для доступа к базе, должны иметь права Manager или Designer

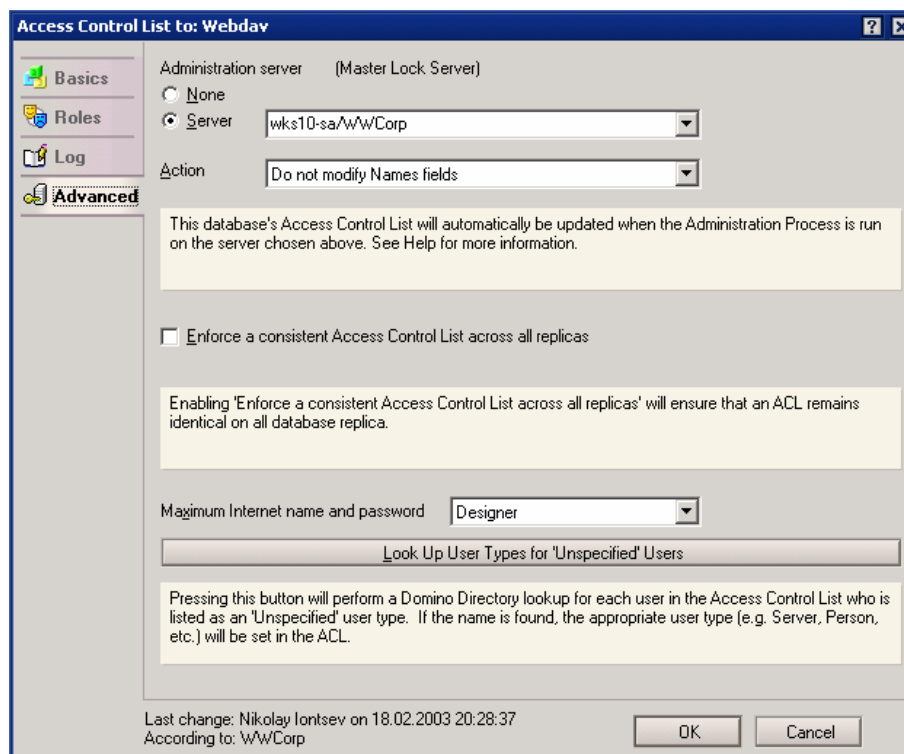


Рис. 623 Назначен сервер администрирования - чтобы работала блокировка документов, элементов дизайна, общих ресурсов. Минимальный уровень доступа по протоколам Internet с аутентификацией вводом имени и пароля – Designer

1.66.6.3. 1.1.6.3. Использование с Windows Explorer

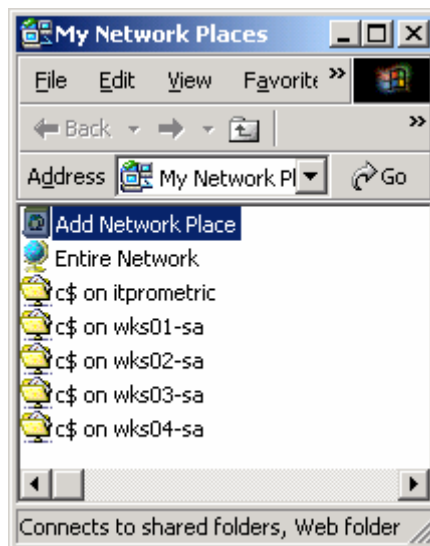


Рис. 624 Добавляется Network Place

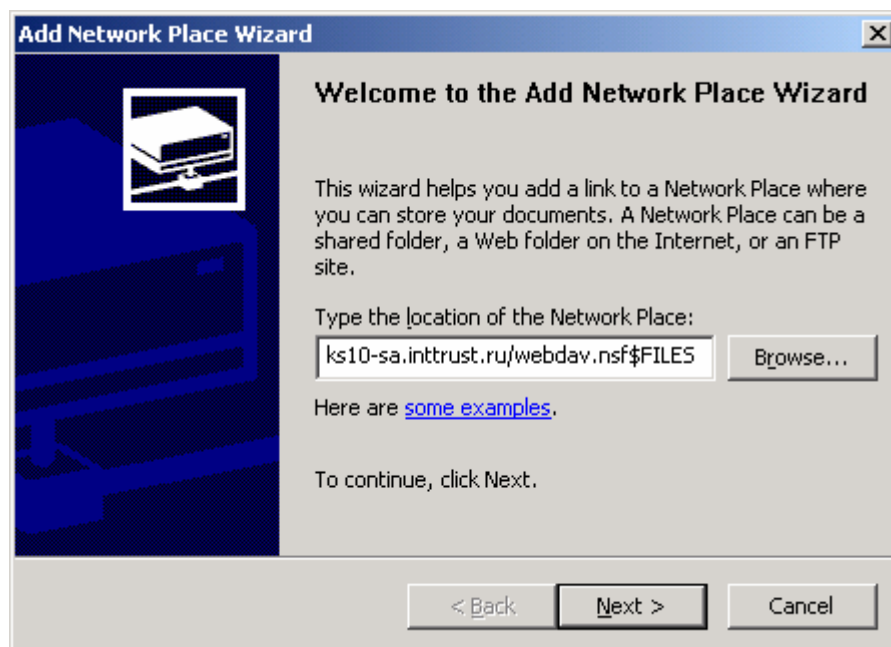


Рис. 625 http://wks10-sa.intrtrust.ru/webdav.nsf\$FILES

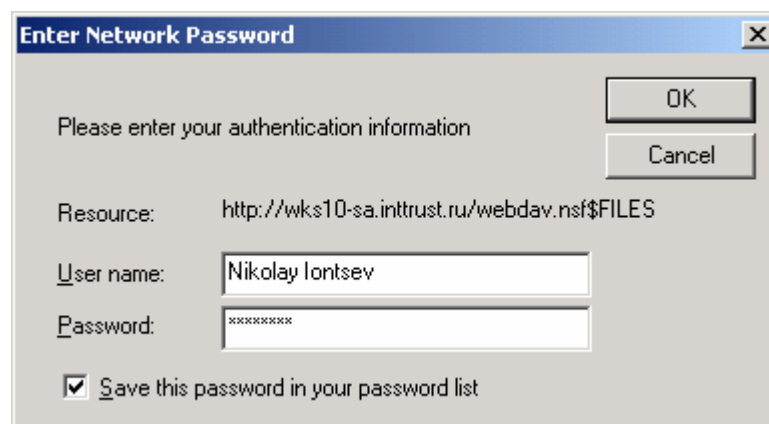


Рис. 626 Login и пароль

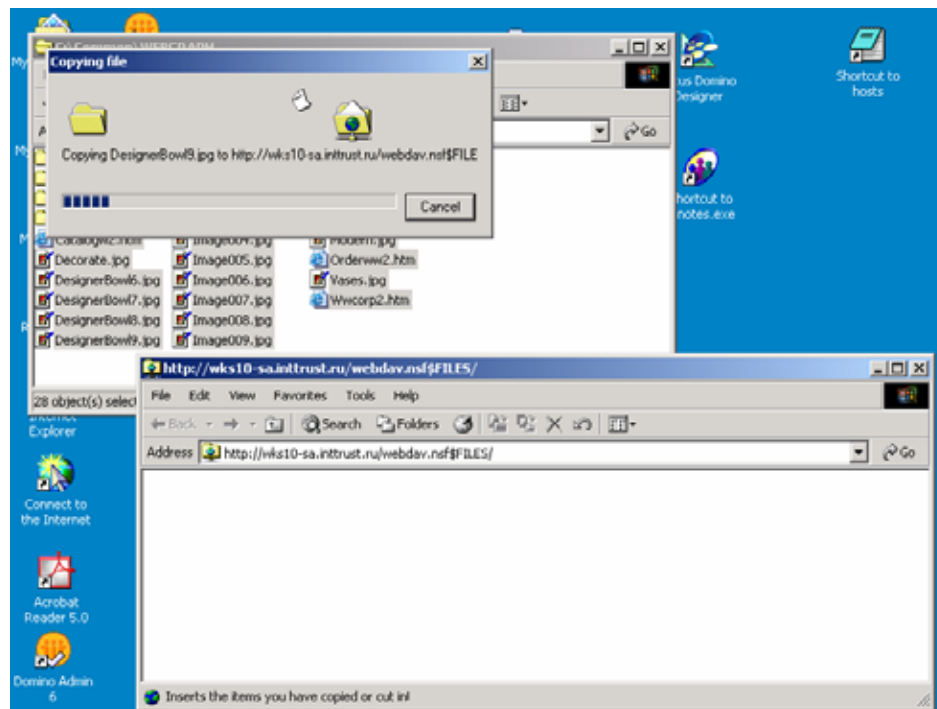


Рис. 627 Просто копируем файлы

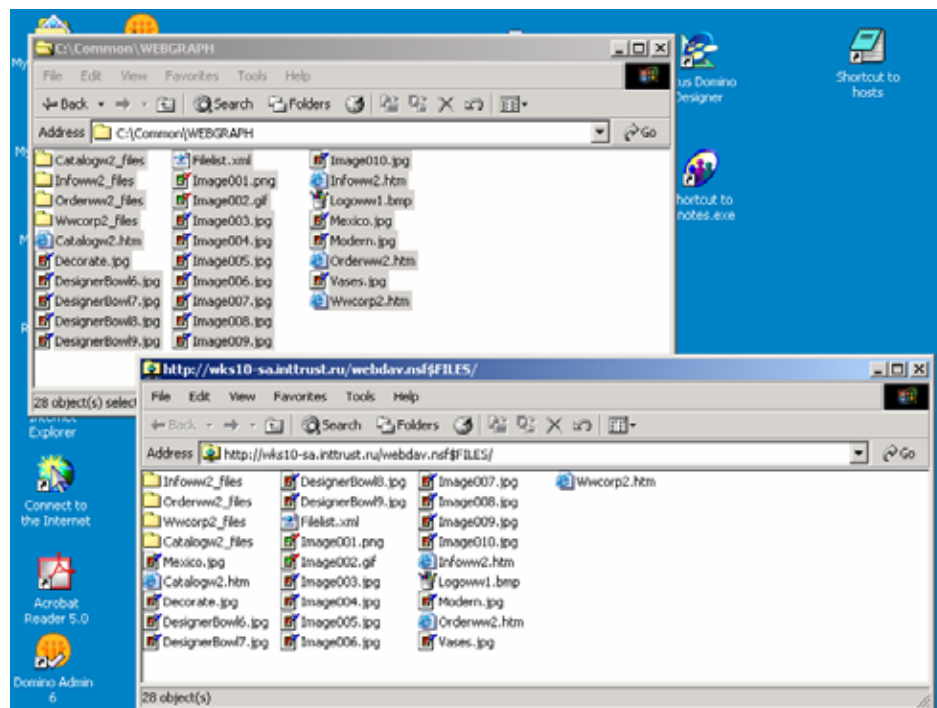


Рис. 628 Файлы скопировались...

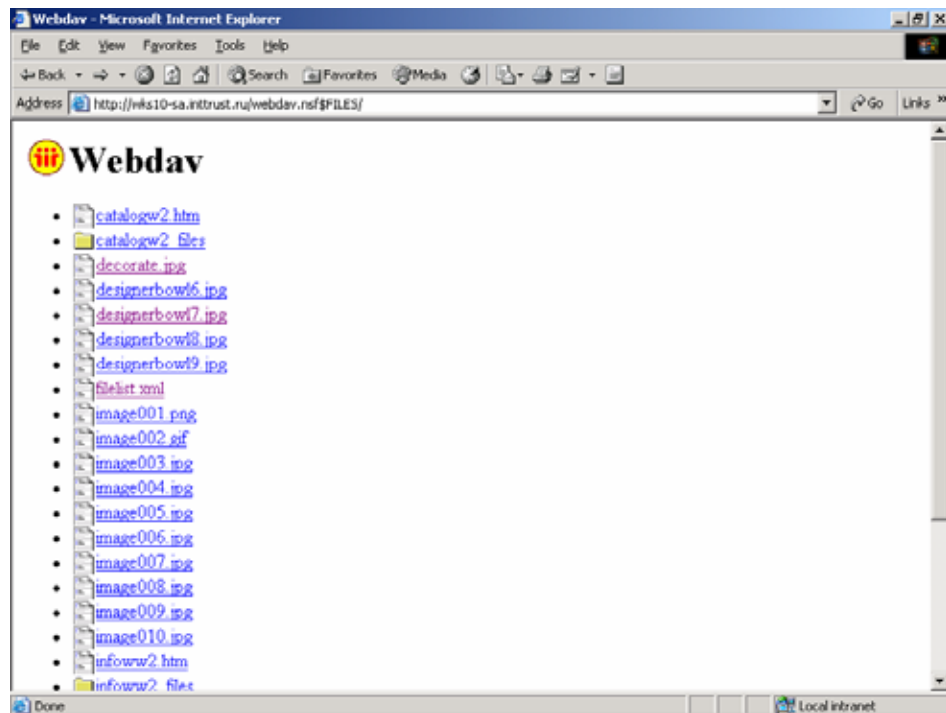


Рис. 629 В браузере результат выглядит так

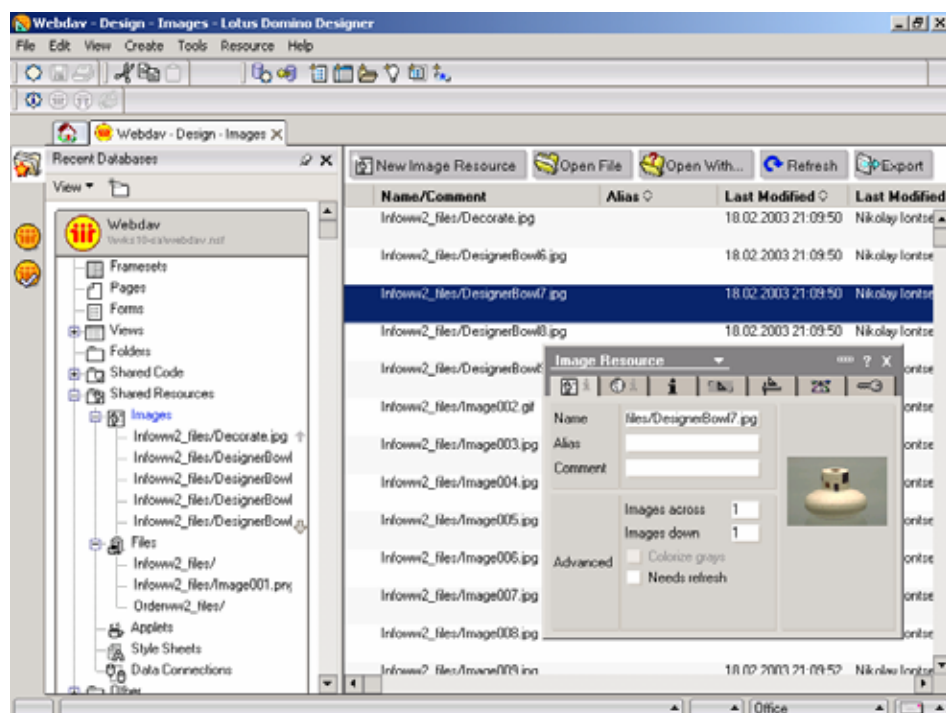


Рис. 630 А в Domino Designer это Shared Resources

1.66.7. 1.1.7. «Правила» Web-сайта (Web Site Rules)

Для WebSite или Global Web Settings можно создавать документы Site Rules:

- • URL -> URL (Substitution),
- • URL -> Redirection URL (Redirection),
- • URL -> Directory (Directory).

Документы этих типов имелись и ранее, но теперь полная гибкость: привязать их к сайту или ко всем сайтам.

1.66.8. 1.1.8. Организация поддержки Single Sign-On (SSO) на

сервера сайта

Вещь не новая. Из нового в R6 только возможность иметь много документов SSO и привязывать их к Internet Sites, а так же неприятность несовместимости SSO R5 и R6 при использовании документов Internet Site.

На серверах разрешается аутентификация на уровне сессий Multiple Servers (SSO). Это делается или в документе Server на закладке Internet Protocols – Domino Web Engine, или в соответствующем документе Internet Site.

Далее создается документ Web SSO Configuration или кнопкой Web – Create Web SSO Configuration, или кнопкой Create Web SSO Configuration из вида Internet Sites.

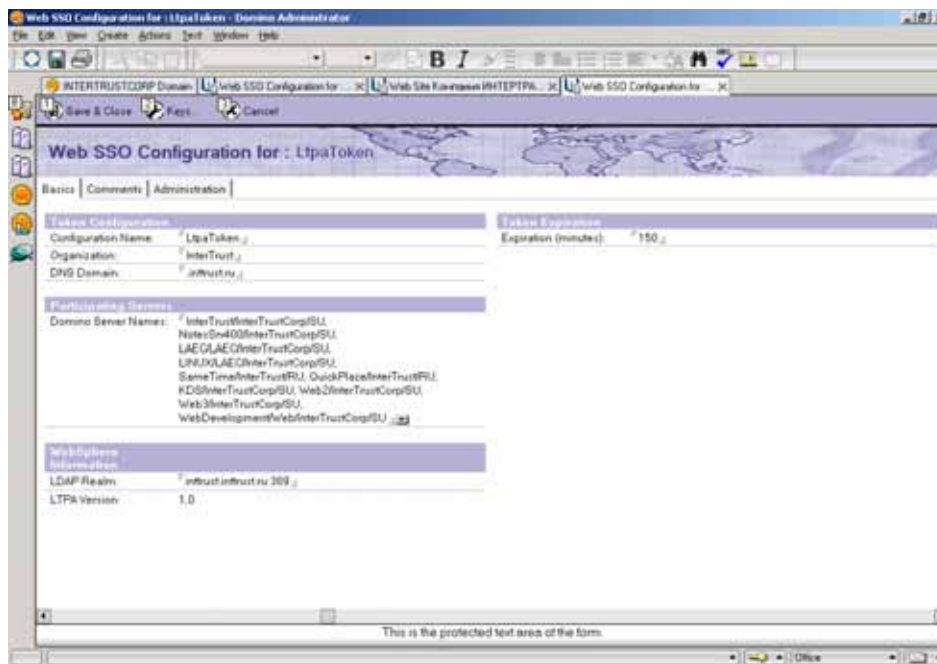


Рис. 631 Документ Web SSO Configuration

В документе кнопкой Keys – Create Domino SSO Key создается ключ шифрования. В поле Domino Server Names перечисляются сервера, которым должен быть известен этот ключ. Для скрытия от посторонних ключ шифрования сам шифруется по RSA на открытых ключах перечисленных Вами серверов и открытым ключом создавшего документ администратора.

Остается заполнить поле DNS Domain – имя домена internet, например, intrust.ru (cookies создается для домена, а не хоста, поэтому ее читают все сервера домена, но дешифрируют только знающие ключ шифрования). Точка перед intrust.ru добавляется автоматом. Поле Configuration Name – LtpaToken для сервера или любое, но лучше тоже LtpaToken, для Internet Site. Для Internet Site так же необходимо заполнить поле Organization. Поля LDAP... оставляют пустыми.

Изучать документы удобно в скрытом виде (\$WebSSOConfigs) – по CTRL + SHIFT keys and select View, Go To.

1.66.8.1. 1.1.8.1. SSO между WebSphere Application Server и Domino

Возможен SSO между WebSphere Application Server и Domino. При этом ключ создают в WAS и экспортируют в файл, а в документ Web SSO Configuration импортируют. При этом автоматически заполняются поля LDAP...

1.66.9. 1.1.9.iNotes Web Access

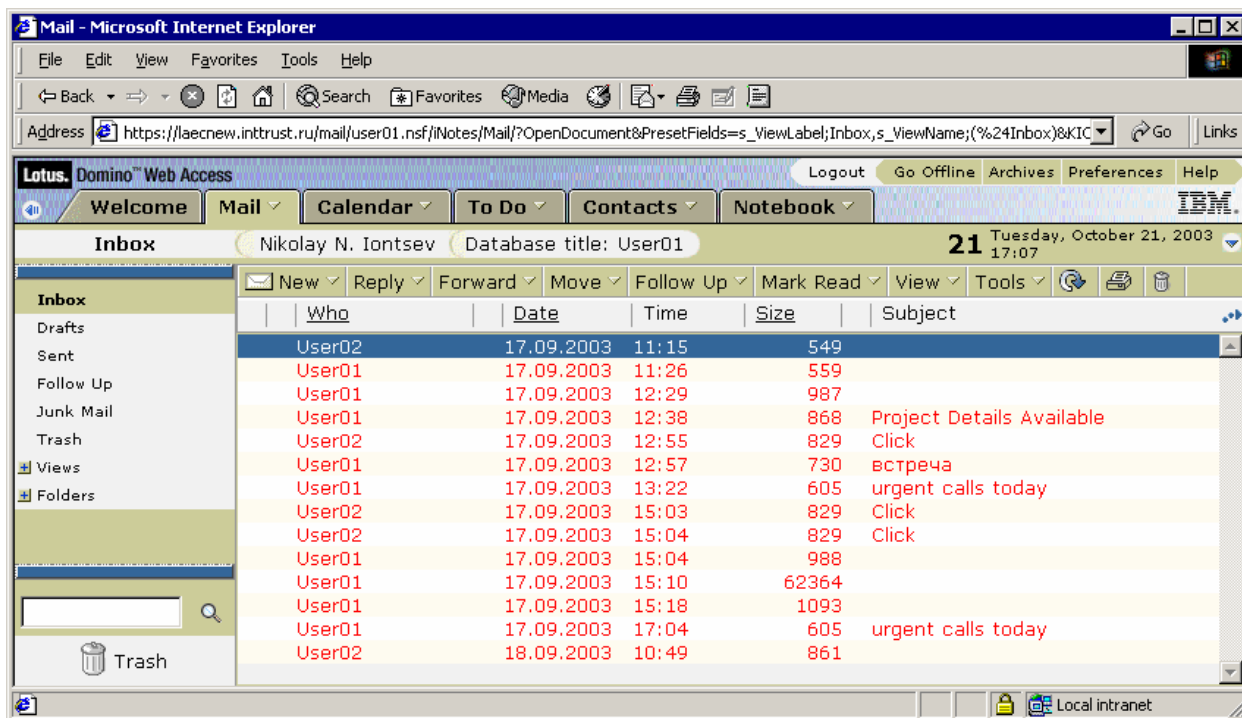


Рис. 632 С одной стороны это просто ориентированный на браузер шаблон для почтовой базы



Domino Web Access Settings

Welcome Page Setup		Offline	
Default Welcome Page:	View/Modify...	Encrypt offline mail databases:	☐ Enable
Allow user to edit the Welcome Page	☒ Enable	Allow user to go offline:	☒ Enable
		Only sync documents modified in the last 90 days:	☐ Enable
		Limit document attachments during sync	☐ Enable
Alarms		International	
Alarms	☒ Enable	Alternate name support:	☒ Enable
Minimum alarm polling time	5 minutes	Preferred alternate name languages:	English, Russian
		Allow user to choose alternate name display:	☒ Enable
Mail			
Minimum mail polling time	5 minutes		
When sending mail, set format to:	Let user decide		
	☒ Enable		
Name resolution and validation:	☒ Enable		

Рис. 633 Но ввиду широкого распространения он даже централизованно конфигурируется...

Mail		International	
Minimum mail polling time	5 minutes	Alternate name support:	☒ Enable
When sending mail, set format to:	Let user decide	Preferred alternate name languages:	English, Russian
Name resolution and validation:	☒ Enable	Allow user to choose alternate name display:	☒ Enable
Mail Encryption		Start Up View	
Encrypted mail support:	☒ Enable	Allow user to select default active view:	☒ Enable
Allow user to delete their Notes ID from their mail database:	☒ Enable	When opening Domino Web Access, open to:	Mail
Allow user to export their Notes ID:	☒ Enable		
Require SSL when accessing secure mail features:	Client		
Use JavaScript for SSL-redirection requests:	☒ Enable		
		Other Settings	
		Archiving on server:	☒ Enable
		Full-text indexing:	☒ Enable
		Modification of Internet password:	☒ Enable
		Calendar printing:	☒ Enable
		Domino Web Access ActiveX file attachment utility:	☒ Enable
		Compress HTTP response data	☒ Enable
Disclaimer Text			
Add disclaimer notice to mail memo	At the bottom		
Disclaimer text or HTML:			

Рис. 634 ... в документе Server Configuration

1.66.9.1. 1.1.9.1. Возможность чтения зашифрованной почты Notes

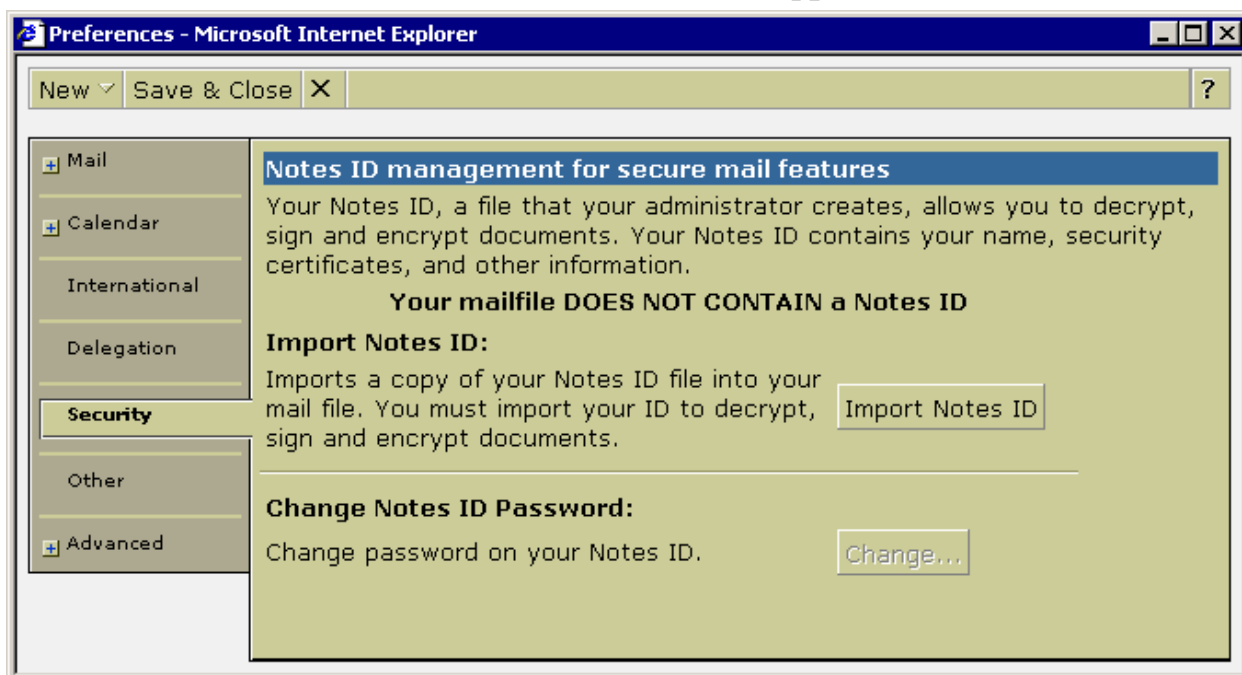


Рис. 635 Остюда ID-файл и пароль по https помещаются в почтовый файл



Рис. 636 Когда это сделано, имеем такие возможности...

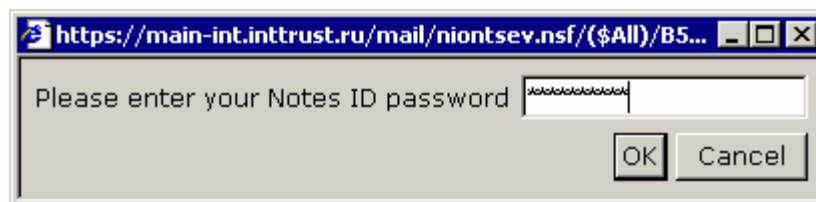


Рис. 637 При открытии зашифрованного письма вводится пароль для ID...

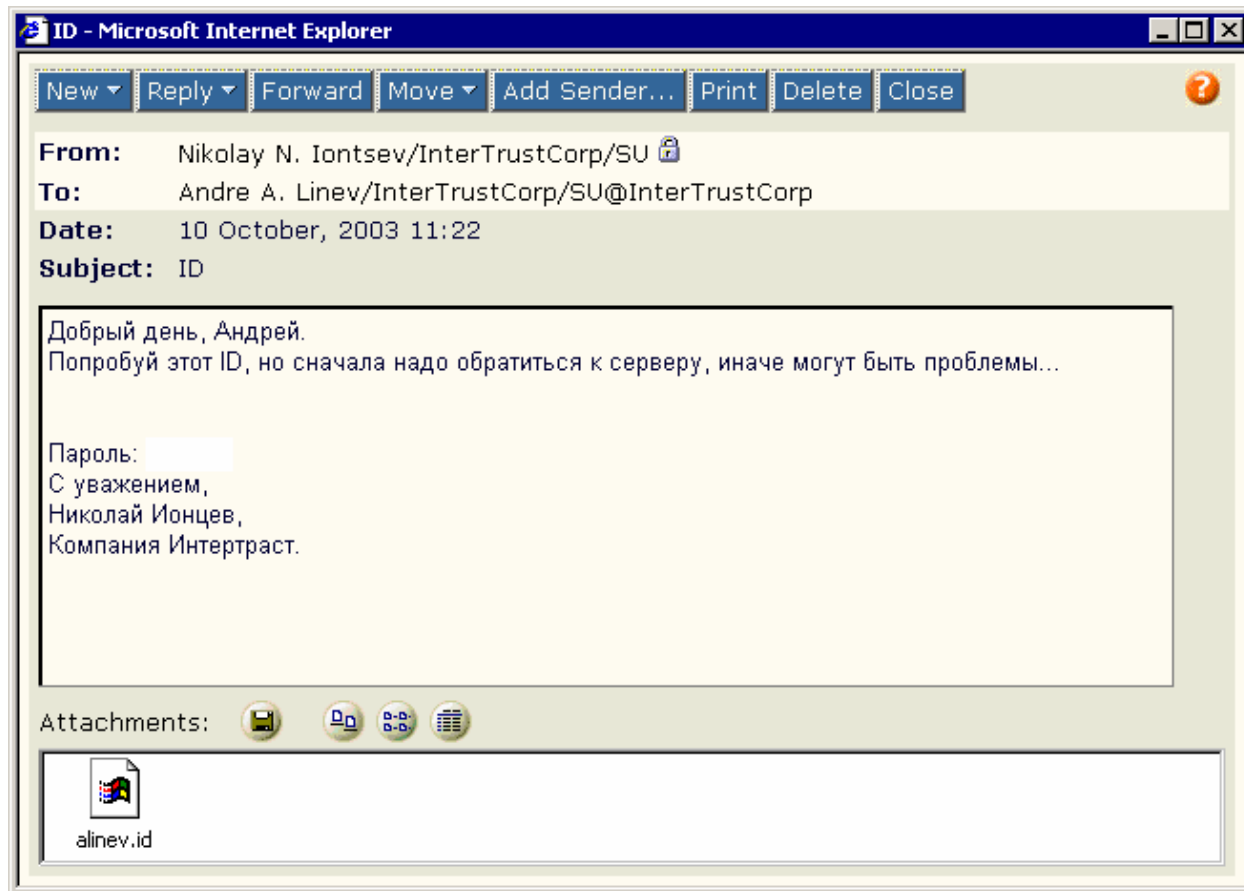


Рис. 638 Выглядит зашифрованное письмо обычно, только «замок», HTTPS и небольшая задержка «подтверждают», что это действительно так...

1.66.9.2. 1.1.9.2. Доступ к каталогам LDAP

1.66.10. 1.1.10. Обзор DOLS (Domino Off Line Services)

1.67. 1.1. Программа Internet Cluster Manager (ICM)

1.67.1. 1.1.1. Назначение, логика работы, конфигурирование, недостатки

1.67.1.1. 1.1.1.1. Как ICM работает по отношению к браузеру?

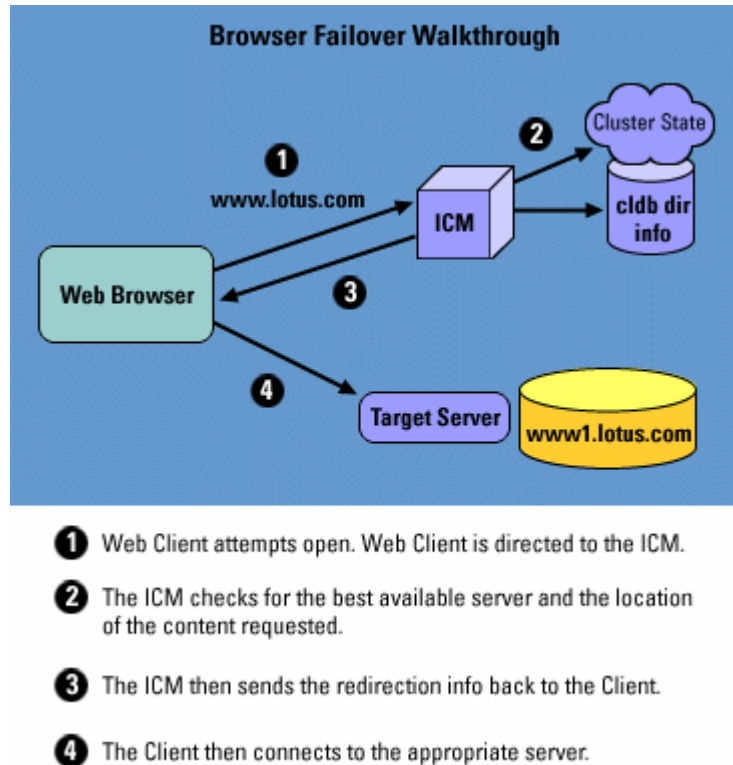


Рис. 639 ICM вовсе не кэширующий прокси или firewall...

1.67.1.2. 1.1.1.2. «Обратные ссылки»

Однако сервер, на который ICM перенаправляет запрос, должен «хотя бы изредка» генерировать обратные ссылки на ICM - иначе клиент никогда «автоматически» более не вернется на ICM. На рисунке ниже курсор стоит на ссылке на базу - в строке статуса виден генерируемый этим сервером URL.

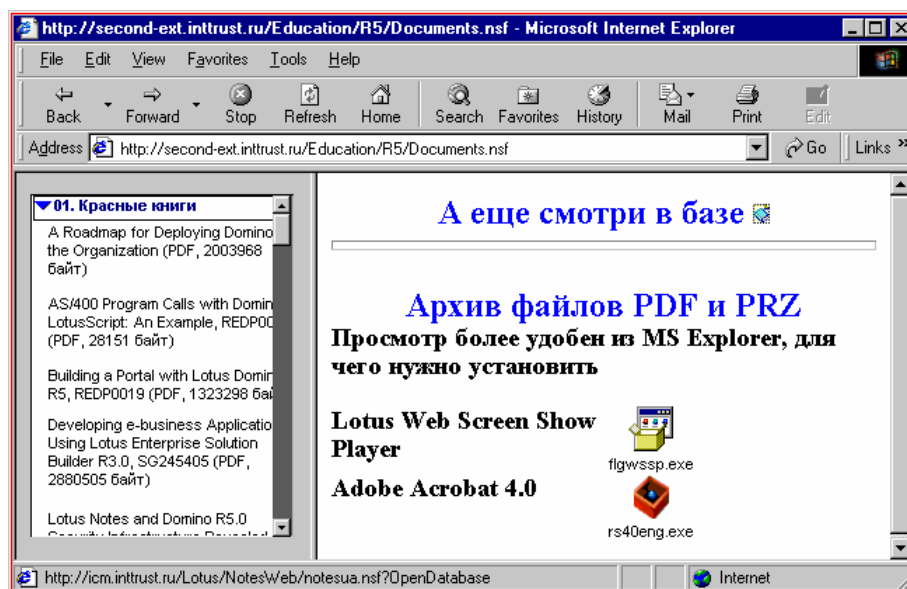


Рис. 640

Уточнение, когда имя хоста ICM используется задачей HTTP для генерации URL:

If the page that a Web server displays to a client includes links to other databases, the Web server includes the host name of the ICM in the URLs to those databases in the following instances:

- • When generating URLs to databases on the same server as the original database
- • When generating URLs to databases on different servers if there are replicas of those databases on the server that contains the original database

This ensures that users accessing those links go through the ICM.

Note In cases not mentioned above, you can use the Redirect URL command to create links to other servers.

1.67.1.3. 1.1.1.3. Некоторые варианты использования ICM

Single ICM outside the cluster

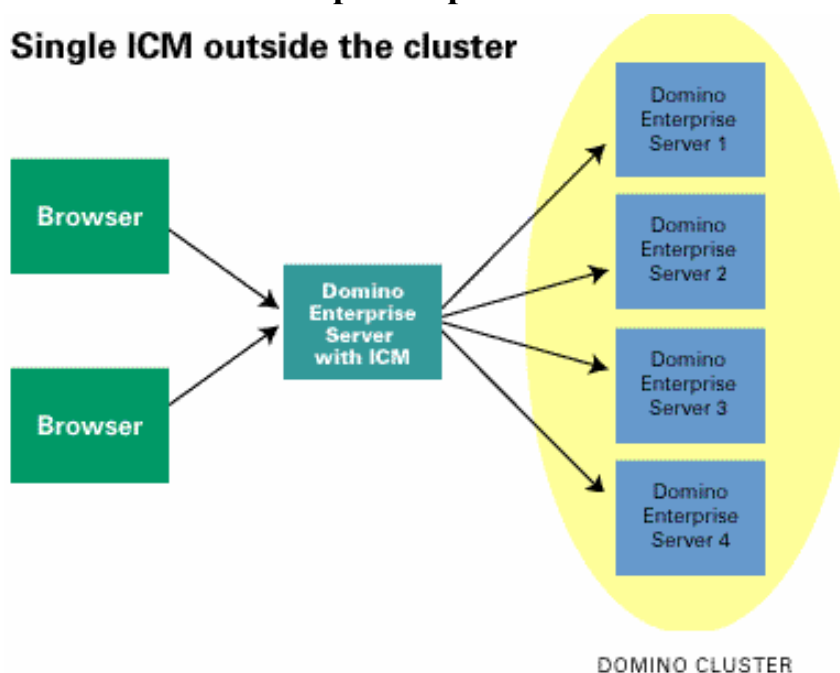


Рис. 641 Одна отдельная машина с ICM

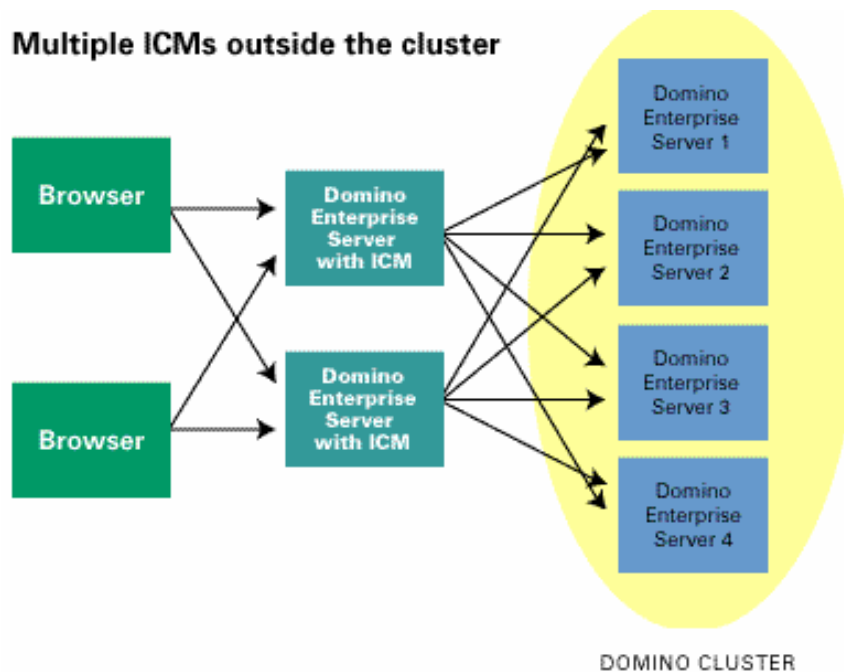


Рис. 642 Две машины с ICM, но тогда одно имя хоста на два IP-адреса, и в результате проблемы кэширования IP-адресов

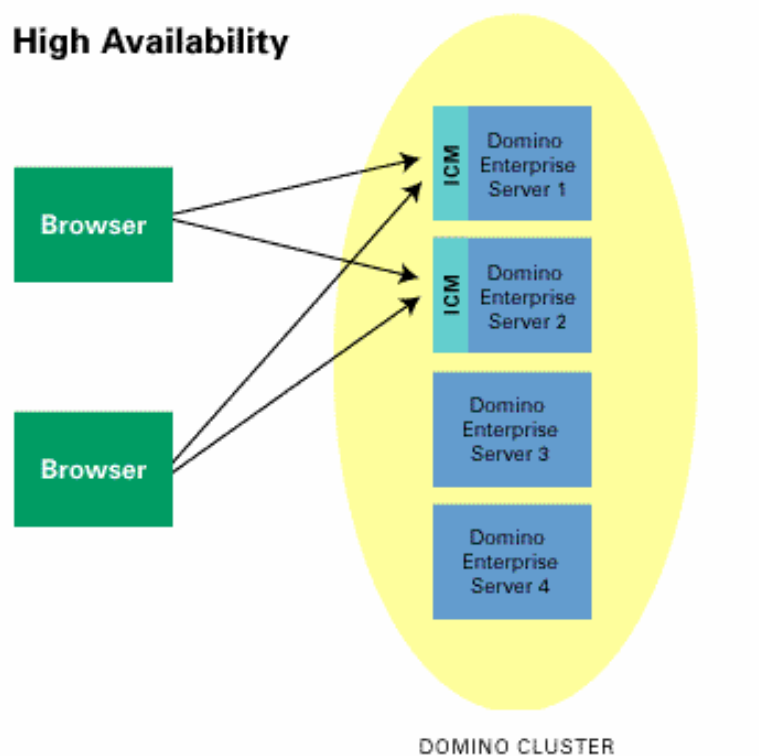


Рис. 643 Два ICM стоят на двух машинах из кластера (у этих машин обычно два IP-адреса), но проблемы кэширования IP-адресов остались...

1.67.1.4. 1.1.1.4. Как ICM конфигурируется

Конфигурируется в документе Server на закладке Server Tasks\ICM

Важен следующий момент:

Каждый сервер первично берет информацию о ICM «с закладки Server Tasks\ICM своего» документа Server. Поэтому закладка должна быть заполнена как для сервера или серверов, на которых запускается ICM, так и для других серверов из состава кластера,

обслуживаемого этим ICM, на которых ICM не запускается (чтобы они «знали», как надо генерировать URL, ссылающиеся на сервера, на которых запущен ICM).

Например, сервер, на котором запускается ICM:

The screenshot shows the configuration window for a server named 'Web1/InterTrustCorp/SU'. The 'Basics' tab is selected, showing the following settings:

- Cluster name: IntTrustCluster
- ICM Notes port: ICMPORT
- ICM SSL keyfile: keyfile.kyr
- Allow users to browse databases in the cluster over HTTP: Yes

The 'Configuration' tab is also visible, showing:

- Get configuration from: this server document
- ICM hostname: icm.inttrust.ru

The 'ICM HTTP Port Settings' section shows:

- TCP/IP port number: 80
- TCP/IP port status: Enabled
- SSL port number: 443
- SSL port status: Disabled

Рис. 644

И другие серверы из состава кластера, на которых ICM не запускается:

The screenshot shows the configuration window for a server named 'InterTrust/InterTrustCorp/SU'. The 'Basics' tab is selected, showing the following settings:

- Cluster name: IntTrustCluster
- ICM Notes port: TCP1P1
- ICM SSL keyfile: keyfile.kyr
- Allow users to browse databases in the cluster over HTTP: No

The 'Configuration' tab is also visible, showing:

- Get configuration from: another server document
- Obtain ICM configuration from: Web1/InterTrustCorp/SU

Рис. 645

Остальное просто:

- Если у сервера один IP-адрес, номера портов HTTP и ICM должны быть разными.
- Если IP-адресов несколько, надо делать «разнесение по портам»

Для автозапуска при старте сервера надо добавить ,ICM в переменную **ServerTasks** в NOTES.INI.

1.67.1.5. 1.1.1.5. Упражнение - сконфигурируйте ICM на вашем кластере

Сервер с ICM (wks01/Acme/RU, wks01.inttrust.ru):

- имя кластера - какое используется

- • порт Domino - TCPIP
- • из этого документа Server
- • имя хоста ICM - wks01.intrtrust.ru
- • порт для ICM - 8080 (поскольку порт 80 занят HTTP)

Сервер без ICM (wks02/Acme/RU, wks02.intrtrust.ru):

- • имя кластера
- • порт Domino - TCPIP
- • из документа Server для wks01/Acme/RU

Проверьте работоспособность

- • Выдайте команды **tell http restart** на обоих серверах и **load icm** на сервере wks01/Acme/RU.
- • Выдайте команду **tell icm show config** - должны получить список из двух серверов с номерами портов.
- • Из броузера несколько раз обратитесь по http://wks01.intrtrust.ru:8080/help/help5_admin.nsf - при этом может открываться база как с wks01/Acme/RU, так и с wks02/Acme/RU
- • Остановите http на сервере с icm - **tell http q**. Убедитесь из броузера, что по http://wks01.intrtrust.ru:8080/help/help5_admin.nsf открывается база с wks02/Acme/RU.
- • А еще дополнительно хорошо бы создать в какой-нибудь базе страничку со ссылками на другие базы (как Database Link) и, открыв ее, убедиться, что HTTP генерирует URL на них через ICM - порт 8080.

1.67.2. 1.1.2. Обсуждение других подходов к реализации задачи, решаемой программой ICM

- • WLM из Microsoft Windows 2000 Advanced Server
- • IBM Network Dispatcher
- • «Железные» решения

1.68. 1.1. Программа POP3 Server (POP3)

1.68.1. 1.1.1. Конфигурирование программы

➤  **стр. 188**

1.68.2. 1.1.2. Документ Internet Sites типа POP3

➤  **стр. 189, 161**

1.68.3. 1.1.3. Регистрация пользователя, использующего клиента POP3

➤  **стр. 189**

1.68.4. 1.1.4. Конфигурирование клиентов POP3

➤  **стр. 190**

1.68.5. 1.1.5. Тестирование доступа пользователя

➤  **стр. 186**

1.69. 1.1. Программа IMAP Server (IMAP)

1.69.1. 1.1.1. Архитектура IMAP Server R6

➤  стр. 147

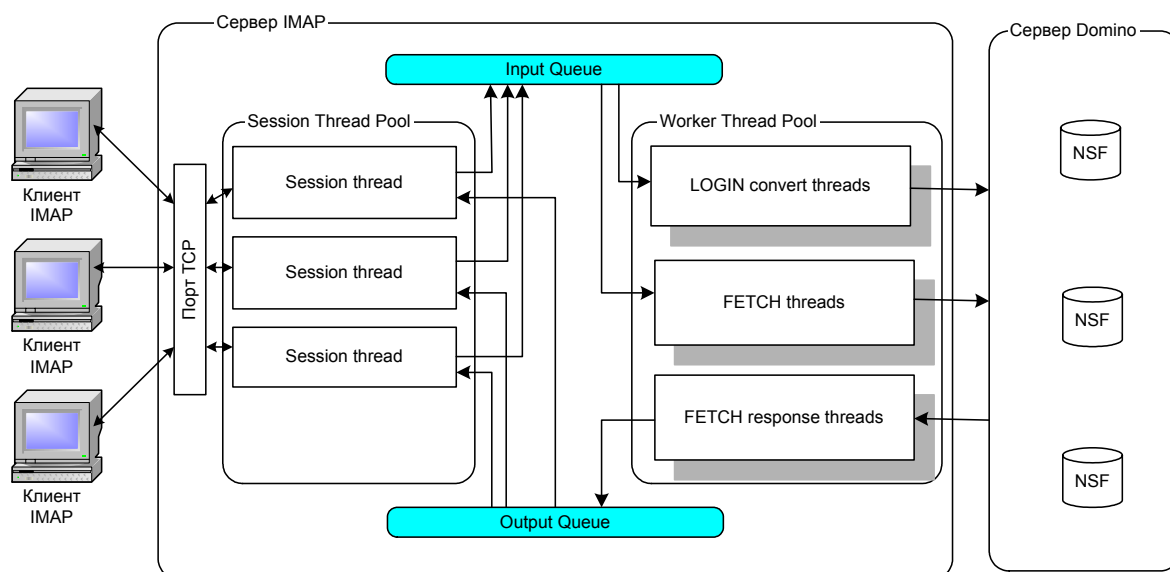


Рис. 646. Архитектура Domino IMAP Mail server

1.69.2. 1.1.2. Конфигурирование программы

➤  стр. 153

1.69.3. 1.1.3. Документ Internet Sites типа IMAP

➤  стр. 161

1.69.4. 1.1.4. Регистрация пользователя, использующего клиента IMAP

➤  стр. 165

1.69.5. 1.1.5. Программа Mail Conversion Utility (CONVERT)

1.69.5.1. 1.1.5.1. Общее назначение программы

➤  стр. 261

1.69.5.2. 1.1.5.2. Обеспечение «IMAP-совместимости» почтового файла

➤  стр. 170

1.69.6. 1.1.6. Конфигурирование клиентов IMAP

➤  стр. 174

1.69.7. 1.1.7. Тестирование доступа пользователя

➤  стр. 174, 142

1.70. 1.1. Программа LDAP Server (LDAP)

- • Новые возможности задачи LDAP:
- • Новая архитектура, расширены возможности и поднята производительность
- • Поддерживаются «все последние» RFC
- • Поддержка Extended ACL задачей LDAP, если эта возможность выбрана для Domino Directory
- • Упрощен процесс расширения схемы LDAP

1.70.1. 1.1.1. Архитектура LDAP Server R6

➤  стр. 202

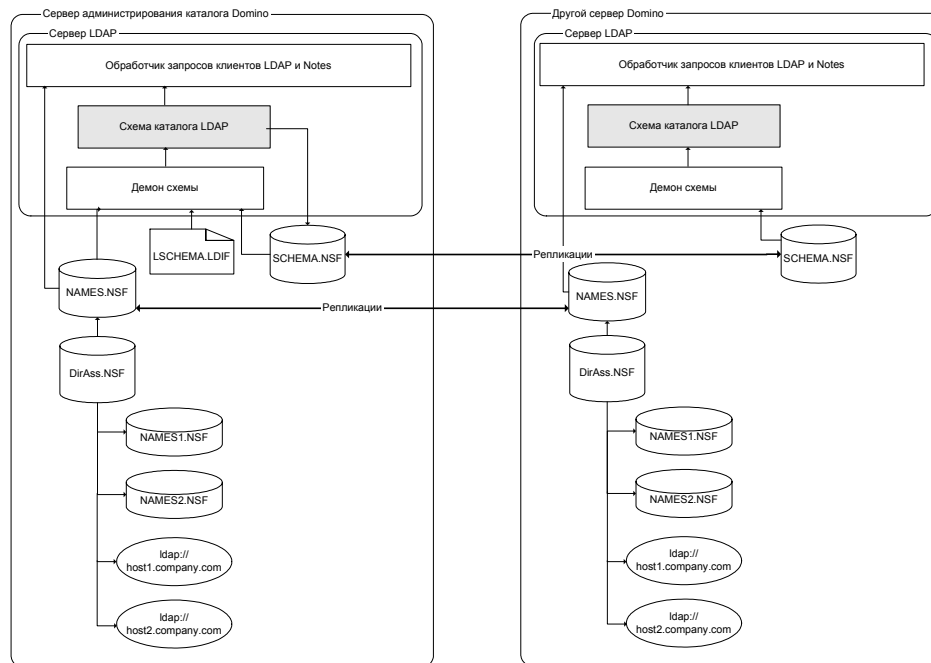


Рис. 647. Архитектура Domino LDAP server

1.70.2. 1.1.2. Конфигурирование программы

➤  стр. 205

1.70.3. 1.1.3. Настройка LDAP-клиентов и тестирование доступа

➤  стр. 224

1.70.4. 1.1.4. Обсуждение возможности расширения схемы каталога LDAP

➤  стр. 217

1.70.5. 1.1.5. Обзор роли программы при использовании сервера Domino совместно с WebSphere Application Server и WebSphere Portal

Domino LDAP может использоваться как LDAP-сервер для аутентификации и авторизации в WAS и портале.

1.70.6. 1.1.6. Дополнительные замечания

- • Поддержка имен LDAP в ACL
- • Аутентификация клиентов POP3, IMAP, LDAP возможна не только по основной Domino Directory, но и по указанным в Directory Assistance дополнительным Domino Directory и внешним LDAP-серверам
- • «Раскрытие состава групп» (group expansion) возможно по дополнительным Domino Directory и внешним LDAP-серверам
- • Directory Assistance Failover - при отказе LDAP-сервера может использоваться «его дублер»

1.70.6.1. 1.1.6.1. Поддержка имен LDAP в ACL баз

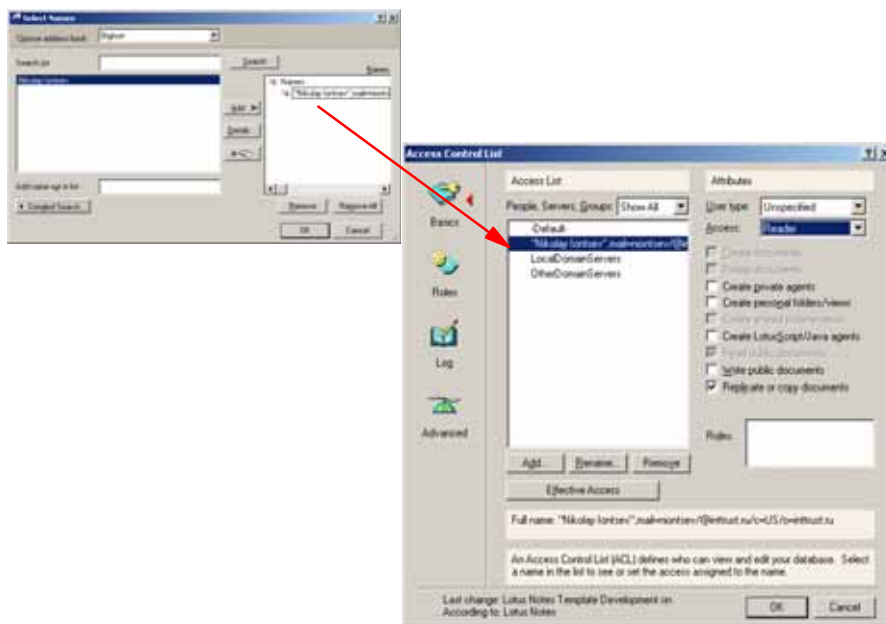


Рис. 648

You can use a secondary LDAP directory to authenticate Internet users. You can then add the names of these Internet users to database ACLs to control user access to databases.

You can also create groups in the secondary LDAP directory that include the Internet user names and then add the groups as entries in Notes database ACLs. For example, an Internet user may try to access a database on a Domino Web server. If the Web server authenticates the user, and if the ACL contains a group named "Web," the server can look up the Internet user's name in the group "Web" located in the foreign LDAP directory, in addition to searching for the entry in the primary Domino Directory. Note that for this scenario to work, the Directory Assistance database on the Web server must include an LDAP Directory Assistance document for the LDAP directory with the Group Expansion option enabled. You can also use this feature to look up the names of Notes users stored in foreign LDAP directory groups for database ACL checking.

When you add the name of an LDAP directory user or group to a database ACL, use the LDAP format for the name, but use a forward slash (/), rather than a comma (,), as a delimiter. For example, if the name of a user in the LDAP directory is:

uid=Sandra Smith,o=Acme,c=US

enter the following in the database ACL:

uid=Sandra Smith/o=Acme/c=US

To enter the name of a nonhierarchical LDAP directory group in an ACL, enter only the attribute value, not the attribute name. For example, if the nonhierarchical name of the LDAP group is:

cn=managers

in the ACL enter only:

managers

To enter the name of a hierarchical group name, include LDAP attribute names in ACL entries. For example, if the hierarchical name of the group is:

cn=managers,o=acme

in the ACL enter:

cn=managers/o=acme

Note that if the attribute names you specify exactly correspond to those used in Notes -- cn, ou, o, c -- the ACL won't display the attributes.

For example, if you enter this name in an ACL:

cn=Sandra Smith/ou=West/o=Acme/c=US

because the attributes exactly correspond to those used by Notes, the name appears in the ACL as:

Sandra Smith/West/Acme/US

1.70.6.2. 1.1.6.2. Аутентификация и «раскрытие состава групп» на серверах LDAP

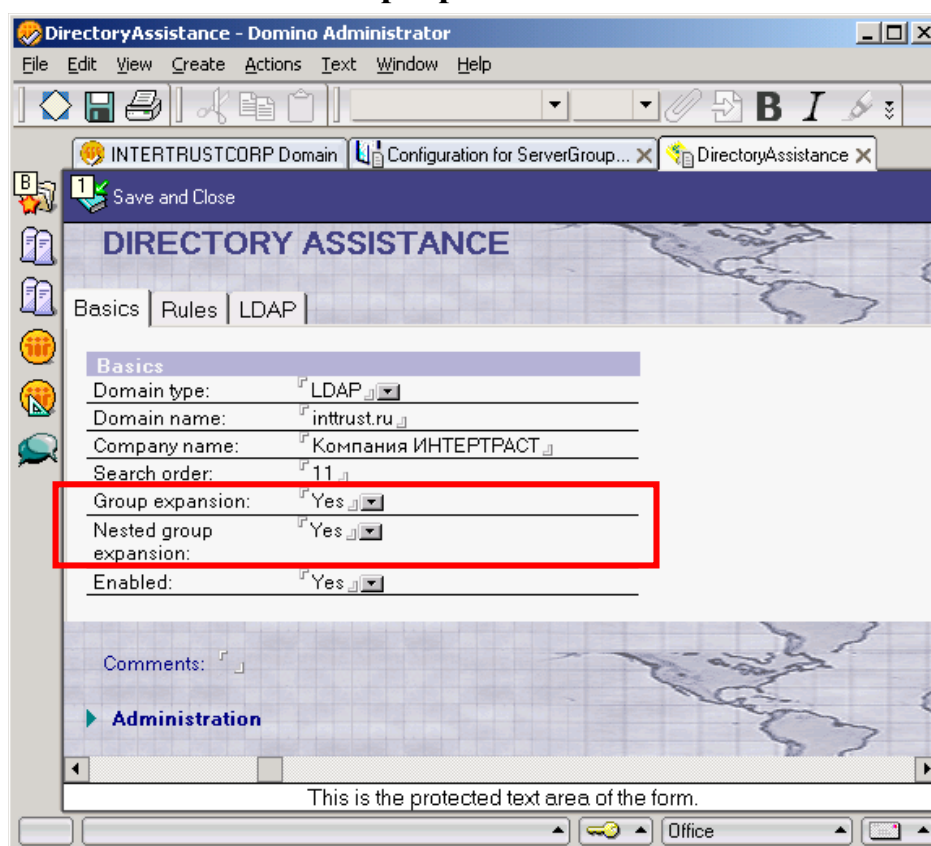


Рис. 649 «Раскрытие состава групп» по LDAP-серверам

1.70.6.3. 1.1.6.3. Directory Assistance Failover

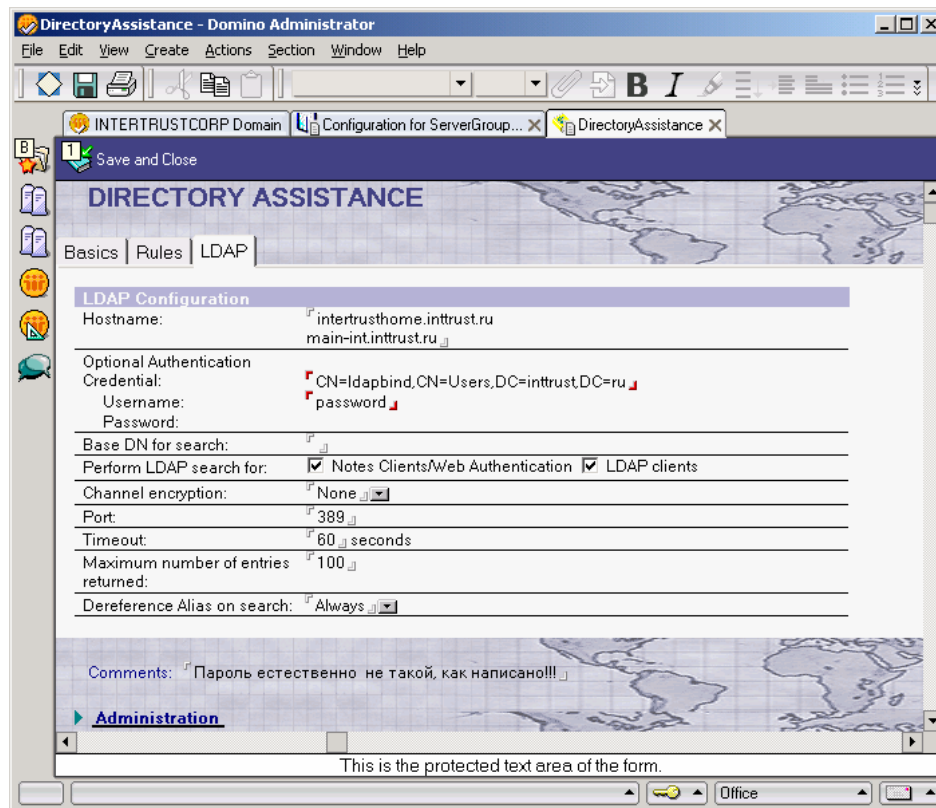


Рис. 650 Список LDAP-серверов в поле Hostname

To provide failover in the event that a remote LDAP directory configured in directory assistance is unavailable, on the LDAP tab of the Directory Assistance document for the remote LDAP directory, enter more than one host name in the Hostname field. Separate hostnames with commas. If the first LDAP directory server specified is unavailable, a Domino server attempts to use the next one listed, and so on.

1.71. 1.1. Программа ДПОР

1.71.1. 1.1.1. Назначение и конфигурирование программы

1.71.1.1. 1.1.1.1. Пакет lotus.domino

В любом Java-приложении, использующем классы Domino (программе, апплете, агенте или сервлете), должен быть «импортирован» пакет lotus.domino. Пакет lotus.domino допускает как «локальные», так и «удаленные» (ПОР) вызовы к объектам Domino.

Локальные вызовы (local calls) используют исполняемый код с локального компьютера, поэтому на локальном компьютере должен быть установлен Domino. Подробнее это означает следующее. Когда вы «вызываете» в своем Java-приложении какой-либо метод встроенного класса, например, Database db = DbDir.openDatabase("myDbFile.nsf"), то для объекта DbDir происходит вызов метода openDatabase класса DbDirectory. Байт-код метода openDatabase находится в пакете lotus.domino. Однако в самом байт-коде метода для выполнения необходимой операции производится т.н. native-вызов С-функции из библиотеки динамической компоновки, входящей в состав установленного на локальном компьютере Domino. Эта С-функция или «полностью самостоятельно» реализует «запрошенную» вами операцию, или, если это необходимо, обращается к серверу Domino, используя при этом Notes RPC (Remote Procedure Call).

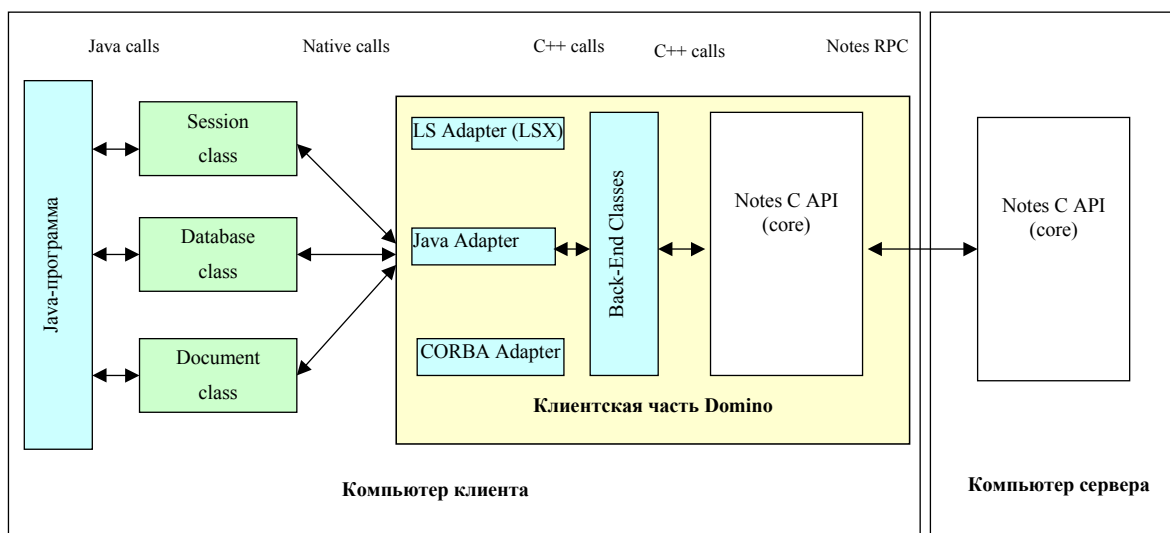


Рис. 651 Общая схема «локальных» вызовов

Удаленные (ПОР) вызовы (remote calls) используют исполняемый код с сервера Domino, так что в этом случае на локальной машине нет необходимости устанавливать Domino.

1.71.1.2. 1.1.1.2. Domino и CORBA

CORBA (Common Object Request Broker Architecture) - архитектура брокера запросов объектов - спецификация, принадлежащая некоммерческой группе Object Management Group (OMG). OMG - консорциум промышленных корпораций, членами которой являются Lotus, IBM, Netscape и более 700 других компаний, имеет Web-сайт <http://www.omg.org>.

CORBA специфицирует базовые механизмы для вызова с компьютера клиента методов объектов, которые находятся на компьютере сервера. ORB (Object Request Broker) - брокер запросов к объектам. Это распределенное приложение, функцией которого является предоставление механизма выполнения запроса, сделанного клиентом,

на вызов метода объекта, находящегося на сервере. Для связи между брокером запросов клиента и брокером запросов сервера (а более широко, между разными брокерами запросов), разработан протокол GIOP (General Inter-ORB Protocol), стандартизирующий множество форматов сообщений и низкоуровневое представление передаваемых данных. Реализация GIOP «поверх» протокола TCP/IP - IIOP (Internet Inter-ORB Protocol) - протокол связи между двумя компьютерами, обеспечивающий передачу параметров для вызываемого метода, его вызов и возврат значения метода клиенту.

Программное обеспечение брокеров запросов клиента и сервера могут быть написаны на разных языках программирования и разными производителями, но, являясь CORBA-совместимыми, «общаются» между собой по протоколу IIOP. Чтобы было возможным формально описывать методы объектов независимо от языка программирования, на котором эти объекты действительно реализованы, в CORBA предусмотрен IDL (Interface Definition Language) - язык определения интерфейсов. Описание объекта (класса) на IDL содержит лишь имена методов и их сигнатуры (имена и типы параметров, типы возвращаемых значений), но никак не затрагивает вопросов реализации методов. Имеются трансляторы с языка IDL на разные языки программирования для различных платформ. Результат работы таких трансляторов дает две компоненты: «скелетную» реализацию классов для «стороны» сервера (skeletons, «скелетоны») и «полную» реализацию этих классов для «стороны» клиента (stubs, «стабы»).

Разработчик объектов (в нашем случае сам Lotus) должен обеспечить «реальный» код для сервера, «дополняя» код «скелетонов», сгенерированный IDL-транслятором. Для «клиентской стороны» ничего разрабатывать не нужно, за исключением, разумеется, самого приложения или апплета, осуществляющего вызовы необходимых клиенту методов. Байт-код «стабов» и клиентского брокера запросов обычно загружаются в браузер клиента «как JAR-файл». «Стабы» сами формируют пакеты из входных параметров для каждого вызываемого клиентом метода в IIOP-совместимом буфере и посылают эти пакеты через клиентский брокер запросов брокеру запросов сервера. Затем «стабы» ожидают заполнения буфера ответов сервером и, если метод определен с возвращаемым значением, распаковывают это значение из буфера и возвращают его.

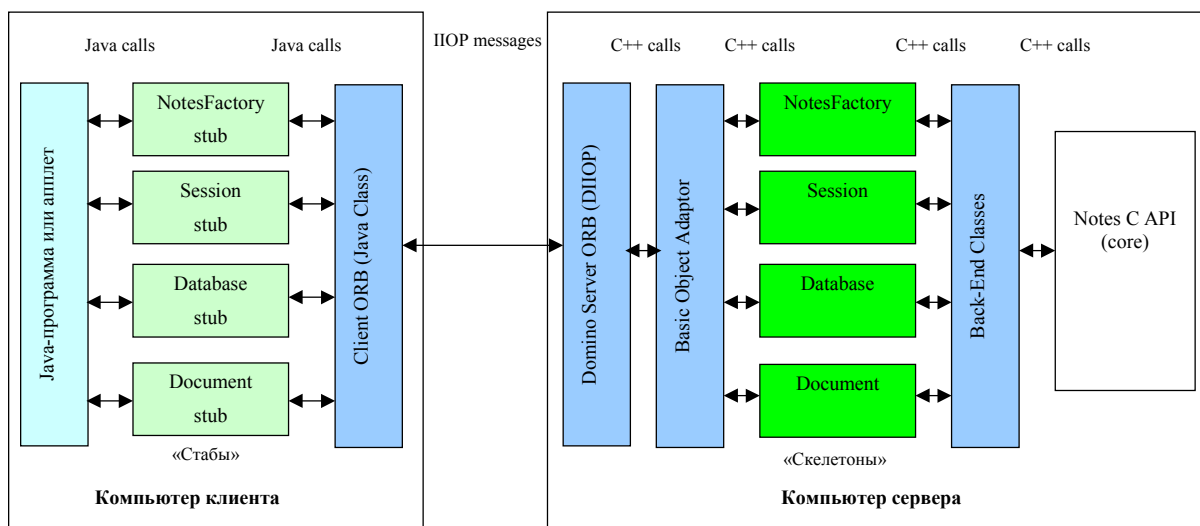


Рис. 652 Общая схема «удаленных» вызовов объектов Domino

1.71.1.3. 1.1.1.3. Конфигурирование программы

На сервере Domino должны быть запущены задачи HTTP (Domino Web Server) и DIIOP (Domino Internet Inter-Object request broker Protocol).

В документе Server применительно к задаче DIIOP обратите внимание на заполнение следующих полей.

- • **Internet Protocols – DIIOP – External HTML Directory.** Обычно должно быть пустое поле. Если поле пустое, DIIOP создает файл diiop_ior.txt в каталоге Lotus\Domino\data\domino\html (стандартный каталог Domino HTTP). Если в поле задан «путь на каталог», DIIOP создает diiop_ior.txt в этом каталоге. Если задан относительный путь, он «отсчитывается» относительно каталога данных сервера. Задавать в поле путь нужно тогда, когда каталог html поддерживается другим HTTP-сервером (не Domino HTTP server), например, Domino под IBM HTTP Server.
- • **Internet Protocols – DIIOP – Idle session timeout.** Таймаут для «неактивной» сессии в минутах. По умолчанию 60 мин. Значение 0 – «неактивная» сессия не должна закрываться по таймауту.
- • **Internet Protocols – DIIOP – Host name/Address.** Имя хоста или IP-адрес, заносимые в файл diiop_ior.txt и используемые при работе с задачей DIIOP этого сервера. По умолчанию пусто – IP-адрес этой машины. У меня в примере заполнено – чтобы в файл diiop_ior.txt заносилось имя хоста, разрешаемое по DNS на IP-адрес сетевой карты из внутренней сети. Внимание – это вовсе не «привязка» задачи к портам – задача «упорно слушает» по IP первой сетевой карты. Если видите, что слушает на IP не той карты (netstat -na), измените порядок следования карт (в Win2K: My Network places – Properties – в меню Advanced – Advanced Settings – в окне закладка Adapters and Bindings, у меня там выбрана карта внутренней сети).
- • **Internet Protocols – DIIOP – Number of threads.** В R4/5 задает количество подпроцессов задачи DIIOP для обработки удаленных вызовов. В R6 не используется.

Server : InterTrust/InterTrustCorp/SU

Basics | Security | Ports | Server Tasks | **Internet Protocols** | MTAs | Miscellaneous | Transactional Logging | Shared Mail | Administration

HTTP | Domino Web Engine | **DIIOP** | LDAP

Basics

External HTML directory:

Idle session timeout: minutes

Host name/Address:

Note: The following setting is obsolete in Notes 6.
It is used for compatibility with prior versions.

Number of threads:

Рис. 653 Закладка Internet Protocols – DIIOP

- • **Ports - Internet Ports - ИОР** - номера портов (TCP/IP port number), статус портов (TCP/IP port status), анонимный доступ и разрешенные способы аутентификации (Authentication options) для доступа к DIIOP по «обычному» порту TCP/IP и порту TCP/IP с поддержкой SSL.

Server : LAEC/LAEC/InterTrustCorp/SU

Basics | Security | Ports | Server Tasks | Internet Protocols | MTAs | Miscellaneous | Transactional Logging | Shared Mail | Administration

Notes Network Ports | Internet Ports | Proxies

SSL settings	
SSL key file name:	laec.kyr
SSL protocol version (for use with all protocols except HTTP):	Negotiated
Accept SSL site certificates:	☐ Yes ☒ No
Accept expired SSL certificates:	☒ Yes ☐ No

Web | Directory | Mail | DIIOP | Remote Debug Manager

Remote Java/Domino IIOP	
TCP/IP port number:	63148
TCP/IP port status:	Enabled
Enforce server access settings:	No
Authentication options:	
Name & password:	Yes
Anonymous:	Yes
SSL port number:	63149
SSL port status:	Disabled
Authentication options:	
Client certificate:	N/A
Name & password:	No
Anonymous:	Yes

Рис. 654 Используемые порты и способы аутентификации для задачи DIIOP – без использования Internet Sites

Server : InterTrust/InterTrustCorp/SU

Basics | Security | Ports | Server Tasks | Internet Protocols | MTAs | Miscellaneous | Transactional Logging | Shared Mail | Administration

Notes Network Ports | Internet Ports | Proxies

Web | Directory | Mail | **DIIOP** | Remote Debug Manager

Remote Java/Domino IIOP	
TCP/IP port number:	63148
TCP/IP port status:	Enabled
Enforce server access settings:	No
SSL port number:	63149
SSL port status:	Disabled

NOTE: This server uses Internet Site documents to configure SSL settings and Authentication options for each protocol. Internet Site documents are located in the Servers\Internet Sites view.

Рис. 655 С использованием Internet Sites

Domino IIOP Site Компания ИНТЕРТРАСТ изнутри - IIOP

Basics | Configuration | Security | Comments | Administration

Site Information

Descriptive name for this site:	Компания ИНТЕРТРАСТ изнутри - IIOP
Organization:	InterTrust
Host names or addresses mapped to this site:	main-int.intrust.ru second-int.intrust.ru IntTrust.intrust.ru laec.intrust.ru linux.intrust.ru
Domino servers that host this site:	*

Рис. 656 Не забудьте создать – без него задача «слушает порт», но не принимает ни один запрос...

- **Security - Server Access** - поля Access server, Not access server, Create new databases и Create replica databases содержат списки имен, шаблонов имен и групп, кому разрешается или не разрешается обращаться к серверу Domino, создавать на нем новые базы или реплики баз. Если кто-то не имеет доступа к серверу, или имеет, но, например, не может создавать на нем новые базы, то он не сможет этого сделать ни из клиента Domino, ни «через задачу» DIIOP.
- **Security - Programmability Restrictions** - в этой группе два поля, содержащие списки имен, шаблонов имен или групп тех, кому разрешается выполнять «удаленные» приложения на Java, Javascript, COM с «ограниченными» (Run restricted LotusScript/Java agents в R6 или Run restricted Java/Javascript/COM в R4/5) или «неограниченными» (Run unrestricted methods and operations в R6 или Run unrestricted Java/Javascript/COM в R4/5) функциональными возможностями. В ходе процесса аутентификации, происходящего при получении удаленным приложением объекта Session, задача DIIOP проверяет вхождение имени клиента в списки из этих полей.

Server : InterTrust/InterTrustCorp/SU

Basics | Security | Ports | Server Tasks | Internet Protocols | MTAs | Miscellaneous | Transactional Logging | Shared Mail | Administration

Administrators	Programmability Restrictions	Who can -
Full Access administrators: Administrators	Run unrestricted methods and operations:	InterTrust - Run unrestricted agents, InterTrust/InterTrustCorp/SU, Sametime Development/Lotus Notes Companion Products, Administrators, Lotus Notes Template Development/Lotus Notes
Administrators: Administrators, InterTrust/InterTrustCorp/SU	Sign agents to run on behalf of someone else:	
Database Administrators:	Sign agents to run on behalf of the invoker of the agent:	
Full Remote Console Administrators: Administrators	Run restricted LotusScript/Java agents:	InterTrust - Run restricted agents
View-only Administrators:	Run Simple and Formula agents:	InterTrust - Run personal agents
System Administrator: Administrators	Sign script libraries to run on behalf of someone else:	
Restricted System Administrator:	Note: The following settings are obsolete in Notes 6. They are used for compatibility with prior versions.	
Restricted System Commands:	Run restricted Java/Javascript/COM:	
Administer the server from a browser (pre-Notes 6 servers): Administrators	Run unrestricted Java/Javascript/COM:	

Рис. 657 Поля, определяющие возможность доступа к задаче DIIOP

1.71.2.

1.1.2. Команды консоли

Command	Result
Tell DIIOP Dump Config	Provide a list of the configuration data that DIIOP is using from the Domino Directory. Using dump the configuration is written to the file diiopcfg.txt in the server's data directory.
Tell DIIOP Show Config	Provide a list of the configuration data that DIIOP is using from the Domino Directory. Using show the configuration is displayed on the server console.
Tell DIIOP Log=n	This command determines the amount of information the DIIOP will log about it's operation. Valid values for n are as follows: 0 Show Errors & Warnings only 1 Also show informational messages 2 Also show session init/term messages 3 Also show session statistics 4 Also show transaction messages The setting of this command is saved in the NOTES.INI variable DIIOPLogLevel. Any change that is made to the DIIOP log level will be used the next time the server is restarted.
Tell DIIOP Refresh	Use this command to reload the configuration data that DIIOP is using from the Domino Directory and from notes.ini. By default DIIOP incorporates changes from the Domino Directory every 3 minutes or as often as specified in the NOTES.INI parameter DIIOPConfigUpdateInterval. The Refresh command will force DIIOP to look for changes in the configuration and apply them immediately.
Tell DIIOP Show Users или Tell DIIOP Show Users D	Show all the current active users known to the DIIOP task. This list is similar to the server console command "show tasks" but it includes more information. Appending "D" to this tell command the list of current users will also include the databases the user has open and along with a count of objects that are in use. Example: <pre>tell diiop show users d UserName ClientHost IdleTime ConnectTime SessionId Anonymous 9.95.74.178 0:00 0:00 SN00048DE22 perf/user1.nsf Objects in use: Databases: 1 Views: 0 Documents:0 Items: 0 Others: 0 Users: 1, Network Connections: 1</pre>

1.71.3. 1.1.3. Обзор роли программы при использовании сервера Domino совместно с WebSphere Application Server и WebSphere Portal

Основной способ обмена информацией объектов, выполняющихся на сервере приложений (JSP, сервлеты, JavaBeans, EJB) или порталном сервере (портлеты) с базами Domino состоит в использовании DIIOP.

Способы обмена информацией между базами Domino и сервлетами, JSPs, JavaBeans и EJBs в WebSphere Application Server

- • Domino Objects for Java: Local access
- • Domino Objects for Java: Remote access (CORBA/IIOP)
- • Domino Tag Libraries (JSP)
- • Domino Collaboration Objects (DCO)

- • Web Services
- • Java Database Connectivity (JDBC)

Domino Objects for Java: Local access

- • Local access вовсе не означает, что оба сервера находятся на одном компьютере. Если на разных, то на компьютере WAS стоит клиент Notes и имеется ID-файл. Обращение к серверу Domino происходит по цепочке Java Native Interface => Notes Client API => Notes RPC (например, TCPIP/1352).
- • Это работает относительно быстро, можно сказать, со скоростью клиента Notes.
- • Это безопасно в плане обмена информацией между серверами, но безопасность на стыке «вызов из Web-браузера» - «обращение к Domino под ID клиента Notes» зависит от реализации.
- • Однако по сути требуется разработка собственных JavaBeans или EJB с управлением сессиями, что реализуемо, но трудоемко. Разработчик должен особо заботиться об инициализации и завершении тредов, реализующих сессии Domino, что обременительно.

Domino Objects for Java: Remote access (CORBA/IIOP)

- • На сервере Domino должна быть запущена задача DIIOP. На сервере WAS ничего, кроме NCSO.jar, не требуется. Обмены между серверами происходят поверх TCPIP/63148 по протоколу прикладного уровня IIOP (Internet Inter-Orb Protocol, архитектура CORBA)
- • Способ обычно менее быстр, чем предыдущий
- • В плане безопасности в принципе получается то же самое.
- • Более прост для разработчика, поскольку не требуется управление сессиями. В остальном же обеспечивает полную гибкость.

Domino tag libraries (JSP)

- • Domino R6 имеет библиотеку тегов для разработки JSP, извлекающих информацию из баз Domino или изменяющих информацию в базах. Библиотека описана в HELP разработчика Domino R6. Реализация тегов использует или IIOP(CORBA), или локальные вызовы.
- • Библиотека весьма универсальна и созданные на ее основе «разумные» страницы достаточно быстро работают.
- • Библиотека просто добавляется в проект в WebSphere Studio Application Developer.
- • Lotus разработал Lotus Domino Toolkit for WebSphere Studio. Продукт устанавливается на WebSphere Studio как дополнительный модуль (технология Eclipse) и обеспечивает «импорт» дизайна (форм, видов) из баз Domino в создаваемые в WebSphere Studio страницы JSP.

Техника работы Domino TAG Library и Lotus Domino Toolkit for WebSphere Studio с базами Domino

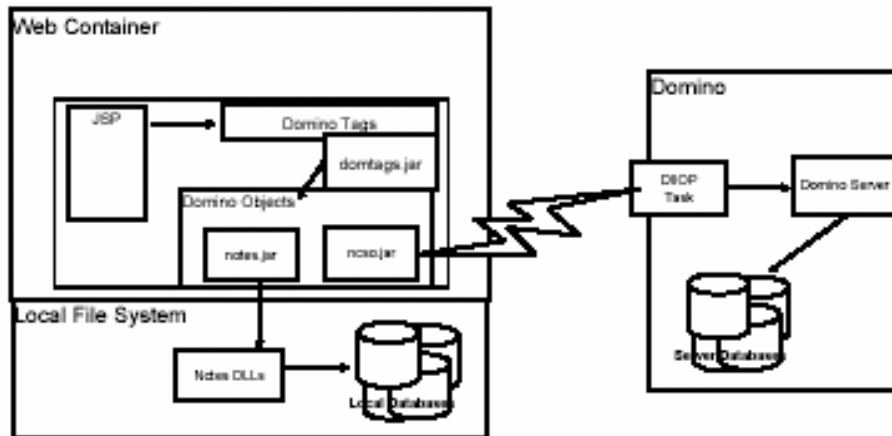


Рис. 658 Приложение WAS, использующее Domino TAG Library

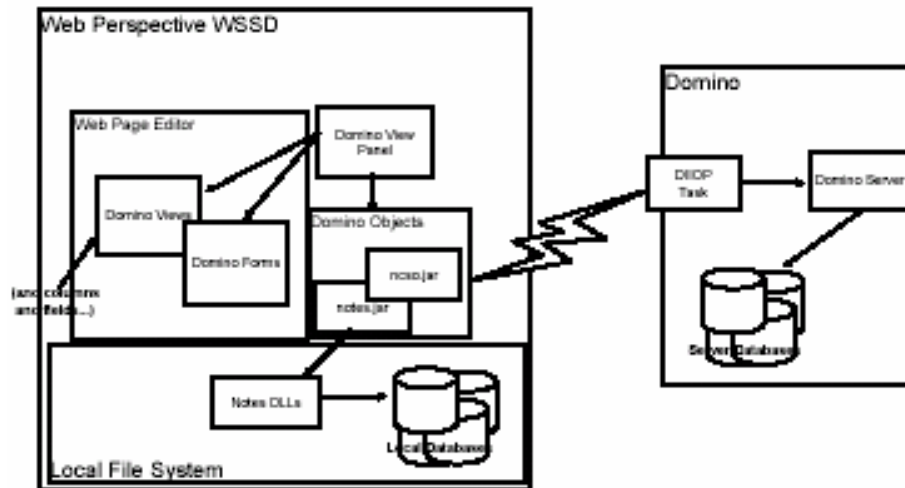


Рис. 659 WSSD с Lotus Domino Toolkit for WebSphere Studio

1.72. 1.1. Почтовая система DOMINO

1.72.1. 1.1.1. Структура и основные функции программы Router (ROUTER)

➤  стр. 3

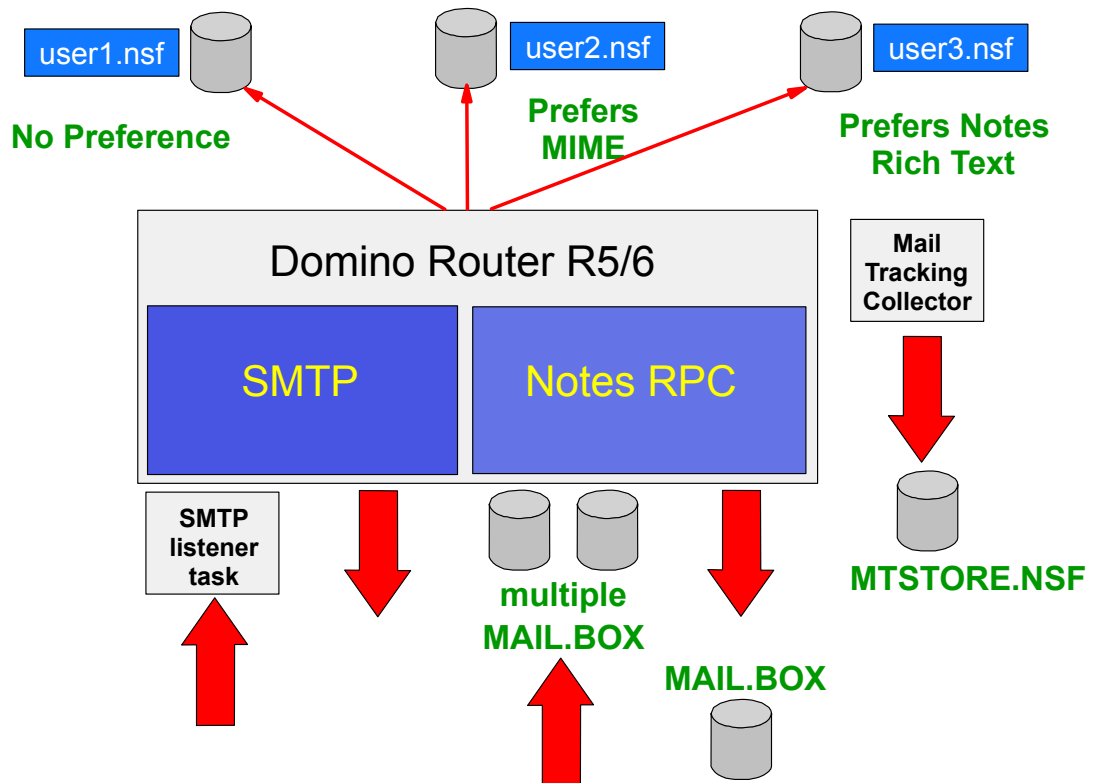


Рис. 660 Общая схема Domino Router R5/6

Новое:

- • Quota Enhancements - расширение трактовки квот
- • Mail Journalling – «журналирование» сообщений
- • System Mail Rules - системные почтовые правила
- • Support for Realtime Blackhole Lists (RBLs) для борьбы со спамом
- • Новые консольные команды **tell router update configuration** и **set rules**
- • New Mail Statistics - новые показатели работы почтовой системы

1.72.2. 1.1.2. Передача почты по протоколам Notes RPC

1.72.2.1. 1.1.2.1. Логика работы системы передачи почты по Notes RPC

➤  стр. 8

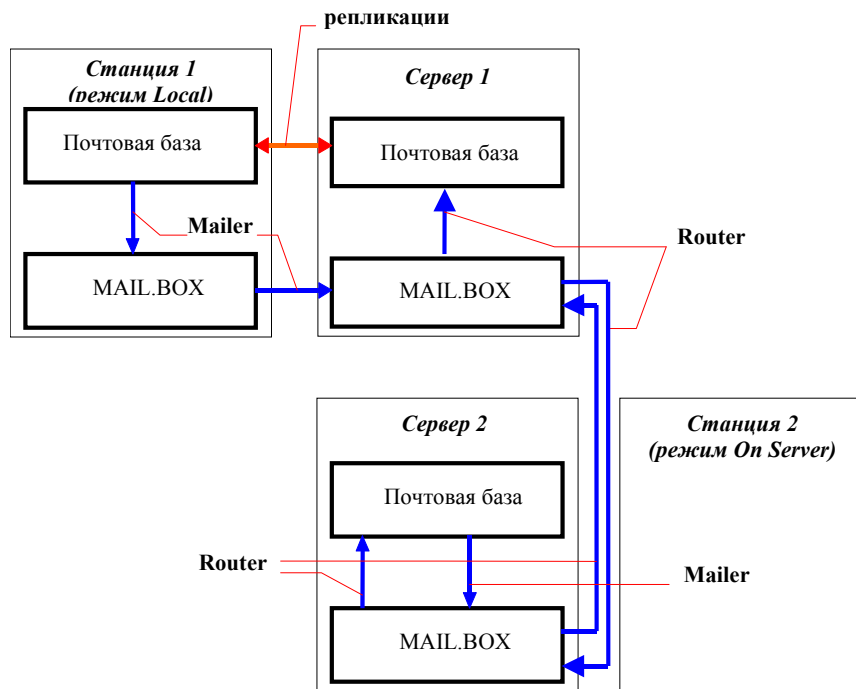


Рис. 661. Иллюстрация режимов *Local* и *On Server*, выбираемых в документе *Location* адресной книги пользователя

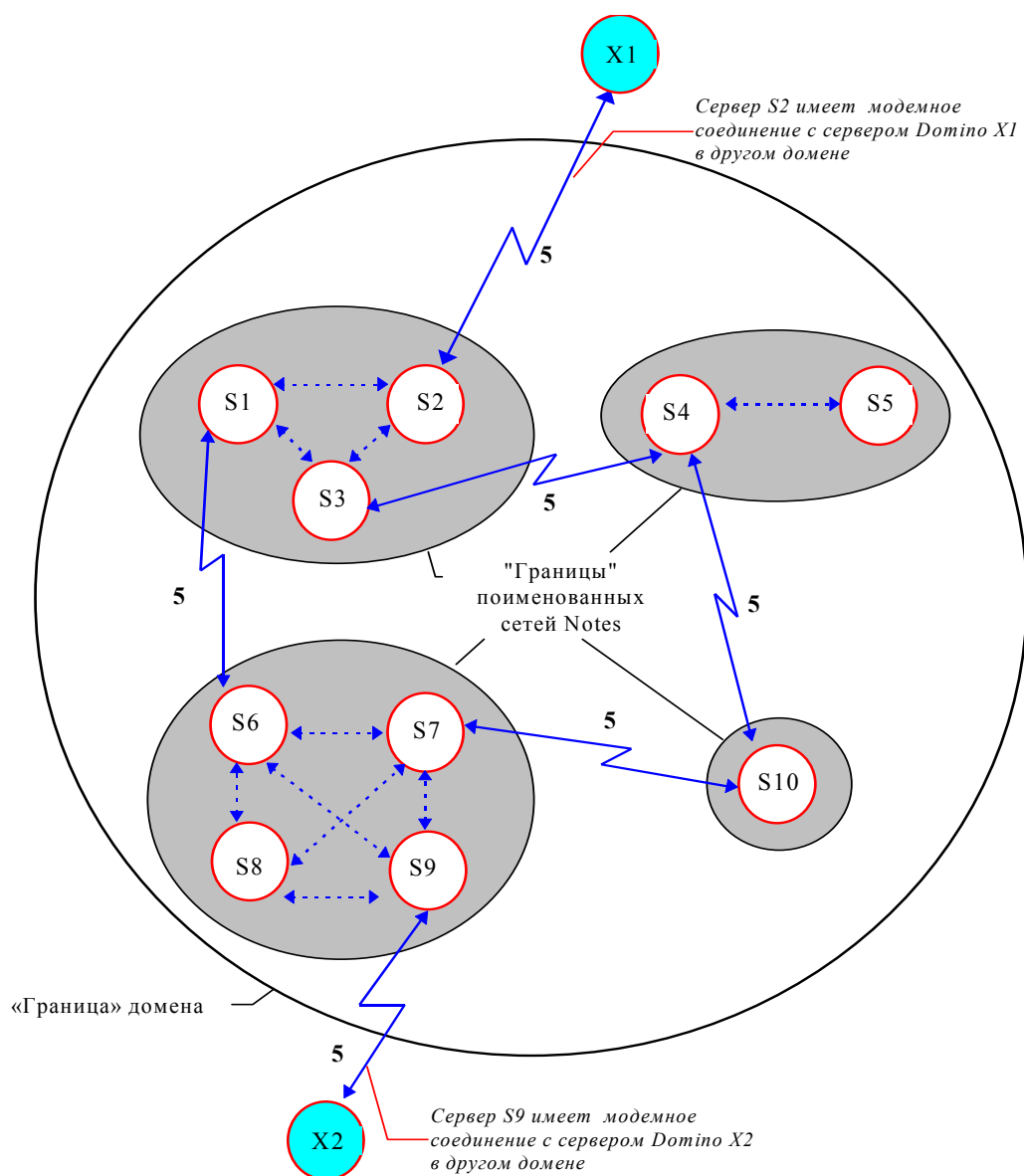


Рис. 662. «Почтовая» топология домена как ориентированный граф

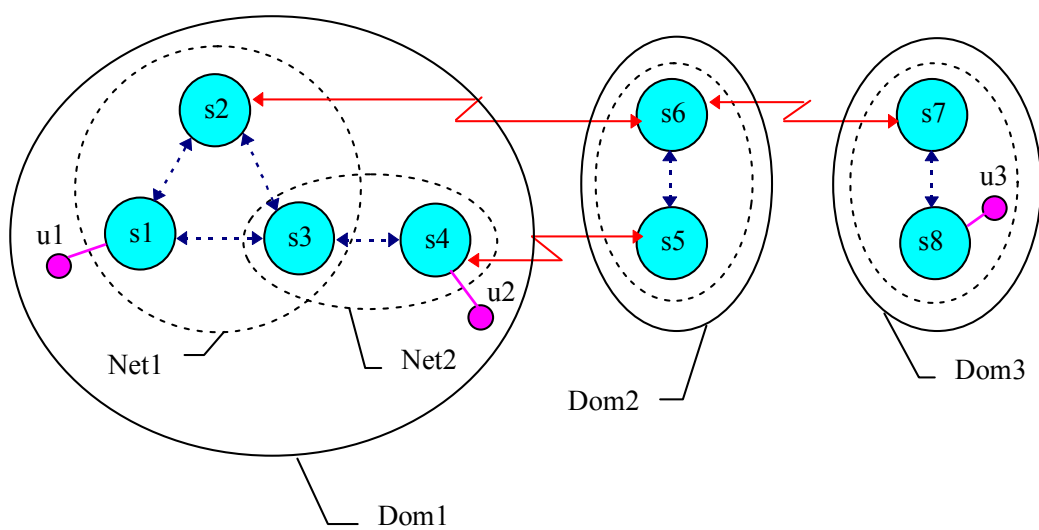


Рис. 663. Топология сети Notes из трех доменов

1.72.2.2. 1.1.2.2. Формат хранения сообщений

➤  стр. 6-7

1.72.2.3. 1.1.2.3. Конфигурирование передачи почты по Notes RPC

- • Поименованные сети Domino (DNN)
 -  стр. 13-14
- • Использование документов Connection для передачи почты между поименованными сетями Domino
 -  стр. 29-32
- • Расписание передачи почты
 -  стр. 29-32
- • Документы Domain различных типов
 -  стр. 20-29

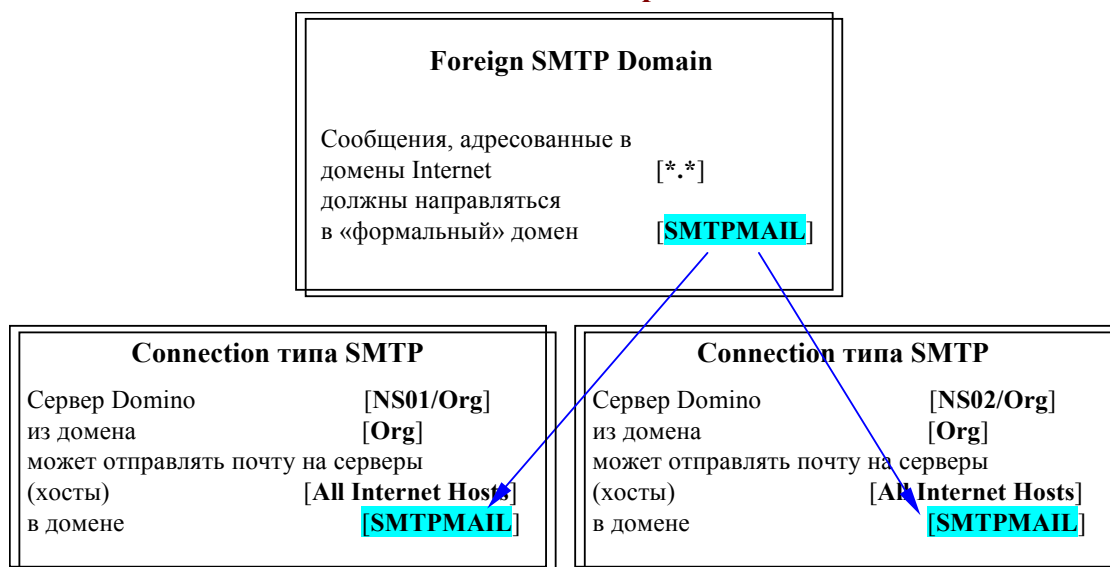


Рис. 664. Взаимосвязь документа Foreign SMTP Domain и документов Connection типа SMTP

1.72.3. 1.1.3. Передача почты по протоколу SMTP

1.72.3.1. 1.1.3.1. Логика работы системы передачи почты по SMTP

➤  стр. 4-5

1.72.3.2. 1.1.3.2. SMTP Listener, его конфигурирование и запуск

➤  стр. 41-44

1.72.3.3. 1.1.3.3. Выбор конфигурации и настройка основных параметров передачи почты по SMTP

- • Закладка Configuration Settings - Router/SMTP – Basics
 -  стр. 46-52

1.72.3.4. 1.1.3.4. Примеры топологий передачи почты по протоколу SMTP

➤  стр. 52-59

1.72.3.5. 1.1.3.5. Конфигурирование Internet-адресации

- • Документ Person и операции Set и Validate Internet Address в клиенте Администратора
 -  стр. 49-51 (Address lookup), стр. 127 (RFC822 phrase)

1.72.3.6. 1.1.3.6. Наложение различных ограничений на почтовые потоки

- • Закладки Configuration Settings - Router/SMTP - Restrictions and Controls - Restrictions / SMTP Inbound Controls / SMTP Outbound Controls
 -  **стр. 62-75**

1.72.3.7. 1.1.3.7. Управление производительностью подсистемы передачи сообщений

- • Использование нескольких Mail.Box –ов
 -  **стр. 46-48**
- • Закладки Configuration Settings - Router/SMTP - Restrictions and Controls - Delivery Controls / Transfer Controls
 -  **стр. 75-85**

1.72.3.8. 1.1.3.8. Конфигурирование параметров расширений протокола SMTP

- • Закладка Configuration Settings - Router/SMTP - Advanced - Command and Extensions
 -  **стр. 95-101**

1.72.3.9. 1.1.3.9. Закладка Configuration Settings – MIME

-  **стр. 103-128**

1.72.3.10. 1.1.3.10. Проверка функционирования передачи почты по протоколу SMTP

Отправка тестовых писем и telnet.

1.72.4. 1.1.4. Квоты на размер баз, в частности, почтовых в R6

1.72.4.1. 1.1.4.1. Конфигурирование квот

-  **стр. 77-79**

1.72.4.2. 1.1.4.2. Установка реакций на превышение квот

-  **стр. 79-80**

1.72.5. 1.1.5. Политики архивирования почтовых баз

1.72.5.1. 1.1.5.1. Создание политики архивирования

Archiving Settings : InterTrust

[Basics](#) | [Selection Criteria](#) | [Logging](#) | [Schedule](#) | [Advanced](#) | [Comments](#) | [Administration](#)

Basics

Name:

Description:

Archiving Options:	Inherit from parent policy:	Enforce in child policies:
☐ Prohibit archiving	☐ Inherit	☐ Enforce
☐ Prohibit private archiving criteria	☐ Inherit	☐ Enforce

Archiving will be performed on:

☒ User's local workstation
☐ Server

Archiving source database is on:	Inherit from parent policy:	Enforce in child policies:
Source Server:		
☐ Local	☐ Inherit	☐ Enforce
☐ Specific server		
☒ Mail server		

Destination database is on:

Destination Server:

☒ Local
☐ Specific server
☐ Mail server

Destination database is on:	Inherit from parent policy:	Enforce in child policies:
☒ Local	☐ Inherit	☐ Enforce
☐ Specific server		
☐ Mail server		

Рис. 665 Архивирование выполняет клиент с почтового сервера на локал

Archiving Settings : InterTrust

[Basics](#) | [Selection Criteria](#) | [Logging](#) | [Schedule](#) | [Advanced](#) | [Comments](#) | [Administration](#)

☐ Inherit Selection Criteria ☐ Enforce Selection Criteria

Currently Selected Criteria

Рис. 666 Кнопкой New Criteria создаем новый критерий (это отдельный документ с именем)

Archive Criteria Settings : ArchCrit1

Basics | Destination | Comments | Administration |

Basics

Name: 『 ArchCrit1 』

Description: 『 』

☒ Enable archive criteria

How should documents be archived?

- ☒ Copy old documents into archive database; then clean up database
☐ Clean up database without archiving

How should documents be cleaned up?

- ☒ Delete older documents from the database
☐ Reduce the size of documents in the database

Which documents should be cleaned up?

marked expired after 365 days

Archive By View/Folder:

Server: InterTrust/InterTrustCorp/SU

Template: Mail (R6)

Change template server:

Choose template:

☐ In views or folders:

Рис. 667 Документ Archive Criteria Settings - Basics

Archive Criteria Settings : ArchCrit1

Basics | Destination | Comments | Administration |

Path Information

Archive Directory: 『 archive 』

Archive Prefix: 『 a_ 』

Archive Suffix: 『 』

Number of Characters
from
original filename: 『 6 』

[Preview an example:](#)

archive\a_Nlonts.nsf

Рис. 668 Документ Archive Criteria Settings - Destination

Archiving Settings : InterTrust

Basics
Selection Criteria
Logging
Schedule
Advanced
Comments
Administration

☐ Inherit Selection Criteria ☐ Enforce Selection Criteria

New Criteria
Add Criteria
Remove Criteria

Currently Selected Criteria

ArchCrit1

Рис. 669 После сохранения предыдущего документа кнопкой Add Criteria выбираем созданный документ по имени

Archiving Settings : InterTrust

Basics
Selection Criteria
Logging
Schedule
Advanced
Comments
Administration

Archive Logging	Inherit from parent policy:	Enforce in child policies:
☒ Log all archiving activity into a log database	☐ Inherit	☐ Enforce

Path Information	Inherit from parent policy:	Enforce in child policies:
Log Directory: archive	☐ Inherit	☐ Enforce
Log Prefix: _	☐ Inherit	☐ Enforce
Log Suffix: _	☐ Inherit	☐ Enforce
Number of Characters from original filename: 6	☐ Inherit	☐ Enforce
☒ Include document links to archived documents	☐ Inherit	☐ Enforce

[Preview an Example:](#)

archive\l_Nlonts.nsf

Рис. 670 Продолжаем заполнять субполитику

Archiving Settings : InterTrust

Basics
Selection Criteria
Logging
Schedule
Advanced
Comments
Administration

Schedule	Inherit from parent policy:	Enforce in child policies:
☒ Enable client based scheduled archiving	☐ Inherit	☐ Enforce
☒ Allow End User To ModifyTime	☐ Inherit	☐ Enforce
Frequency: Daily Weekly	☐ Inherit	☐ Enforce
Run at: 12:00	☐ Inherit	☐ Enforce
Days of week: Mon, Tue, Wed, Thu, Fri	☐ Inherit	☐ Enforce

Location	Inherit from parent policy:	Enforce in child policies:
☒ Any Location	☐ Inherit	☐ Enforce
☐ Specific Location:		

Рис. 671 Продолжаем заполнять субполитику

Archiving Settings : InterTrust						
Basics	Selection Criteria	Logging	Schedule	Advanced	Comments	Administration
Advanced Settings			Inherit from parent policy:		Enforce in child policies:	
☒ Don't delete documents that have responses			☐ Inherit		☐ Enforce	

Рис. 672 Продолжаем заполнять субполитику

1.72.5.2. 1.1.5.2. Проверка функционирования политики архивирования

Для ускорения желательно перезапустить клиента.

Рис. 673 «Ну вот и допрыгался пользователь» - изменить не может

Рис. 674 Только добавления вносить осталось...

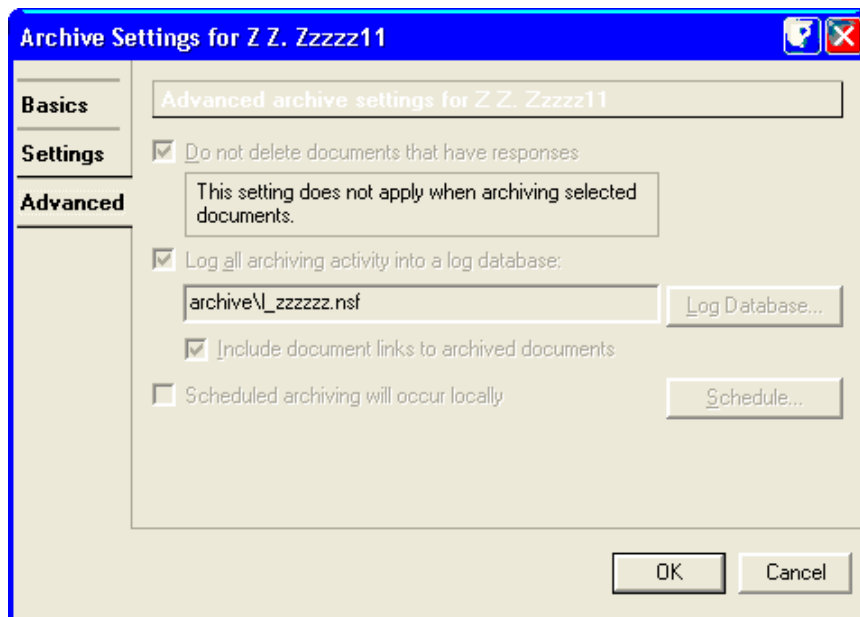


Рис. 675 Но непонятно, почему расписание нельзя менять...

1.72.6. 1.1.6. Реализация Shared Mail в R6

➤ стр. 253

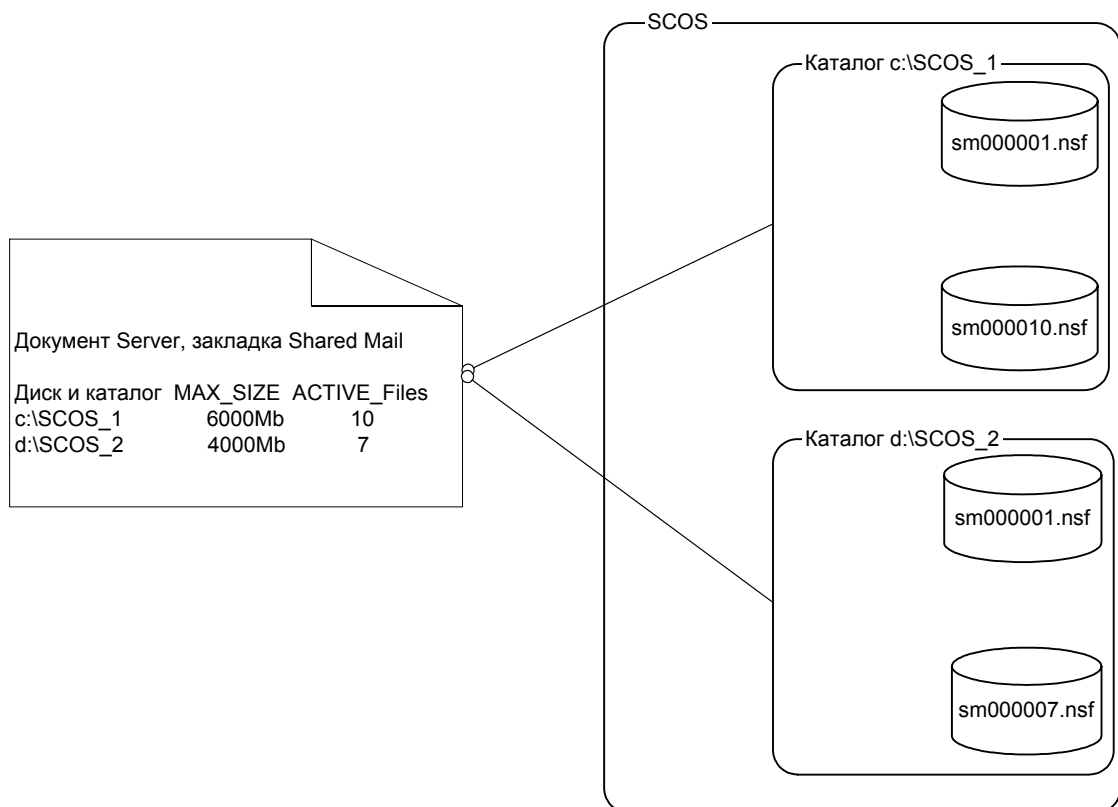


Рис. 676. Архитектура SCOS R6

1.72.7. 1.1.7. Использование Single Copy Template (SCT)

➤ стр. 262

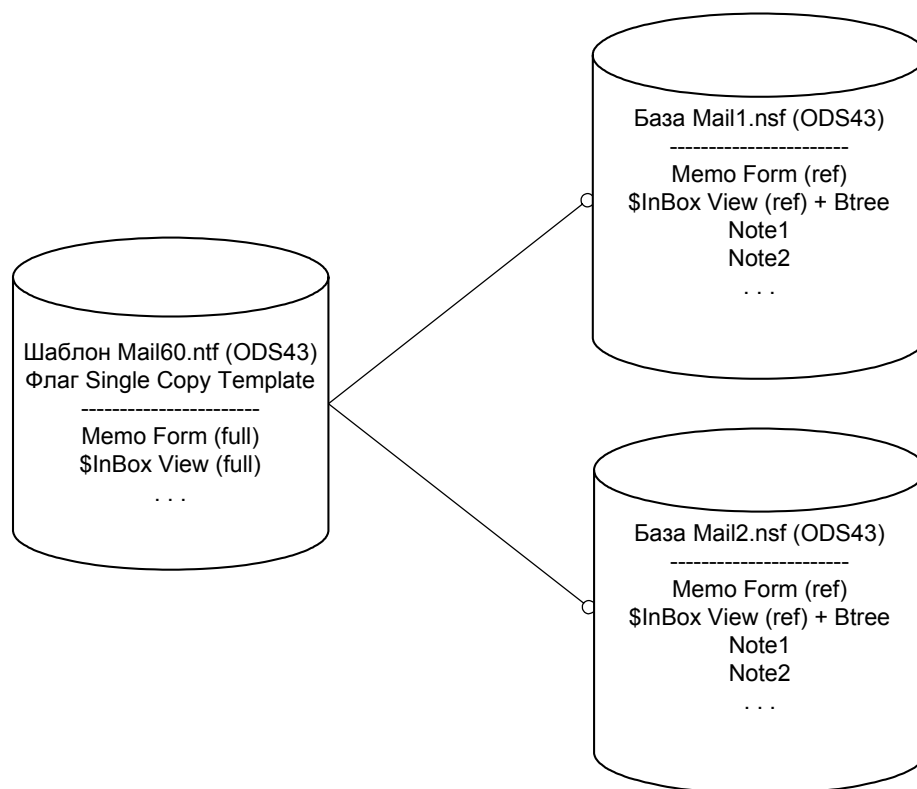


Рис. 677. Принцип функционирования SCT

1.72.8. 1.1.8. «Журналирование» сообщений (Mail Journaling)

➤ стр. 91-95

1.72.8.1. 1.1.8.1. Организация «журналирования» сообщений

➤ стр. 91-95

1.72.9. 1.1.9. Почтовые правила (Mail Rules)

➤ стр. 85-90

1.72.9.1. 1.1.9.1. Создание почтовых правил

➤ стр. 87-89

1.72.9.2. 1.1.9.2. Активизация почтовых правил

➤ стр. 90

1.72.10. 1.1.10. Мониторинг работы почтовой системы

1.72.10.1. 1.1.10.1. Тестирование работы почтовой системы

В SG ND760 предлагается следующий путь:

- • The network connections.
- • The servers and router are up and running.
- • The DNNs are set up properly.
- • The appropriate Connection documents exist and contain the following:
 - • The server name is correct.
 - • The Schedule is enabled.
 - • The router type is correct.

- • The connection requirements for sending mail, such as calling times or message thresholds, have been met.
- • Replication between servers is successful, ensuring Connection document information is up-to-date on all relevant servers.
- • Router restrictions do not prohibit message delivery.
- • SMTP settings are correct.
- • Inbound and outbound controls are properly set.
- • Quotas are not exceeded.
- • Mail rules do not prohibit message delivery.
- • The mail address is correct.
- • The person information is correct.

1.72.10.2. 1.1.10.2. Мониторинг доставки почты

Во-первых, из Domino Administrator с закладки Messaging – Mail выбрать апплет Mail Routing Status и вид Mail Routing Events.

Во-вторых, показатели...

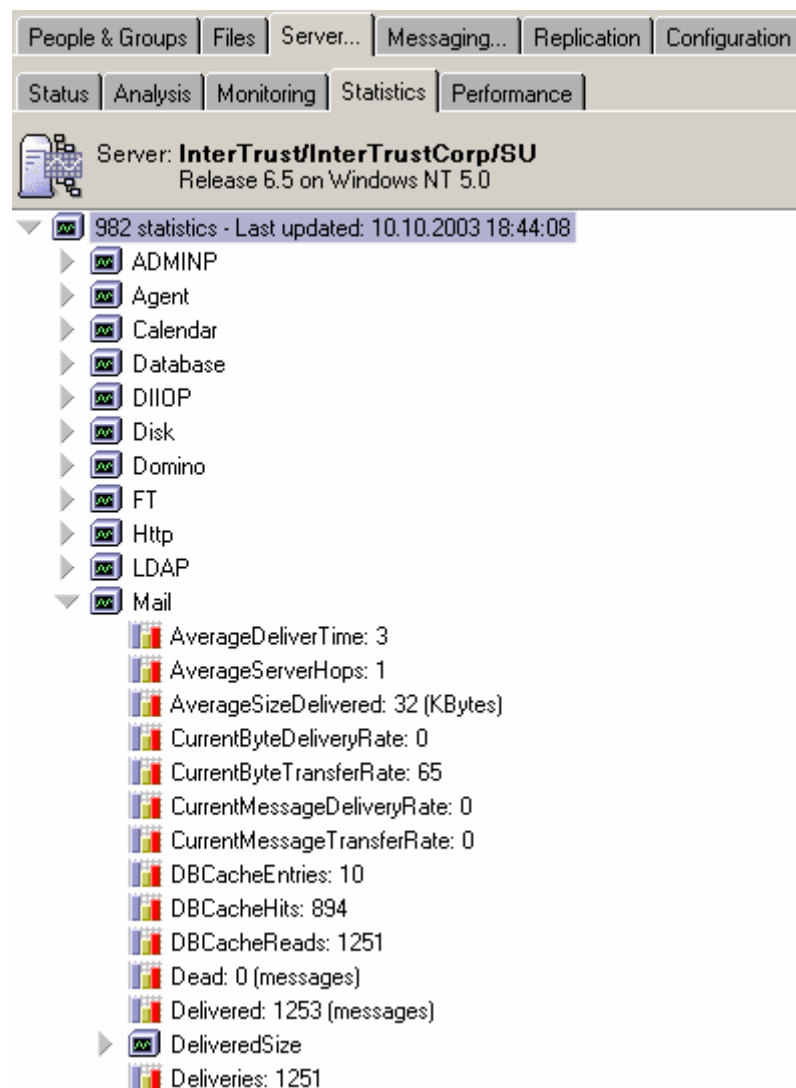


Рис. 678

1.72.10.3. 1.1.10.3. Мониторинг показателей функционирования почтовой системы

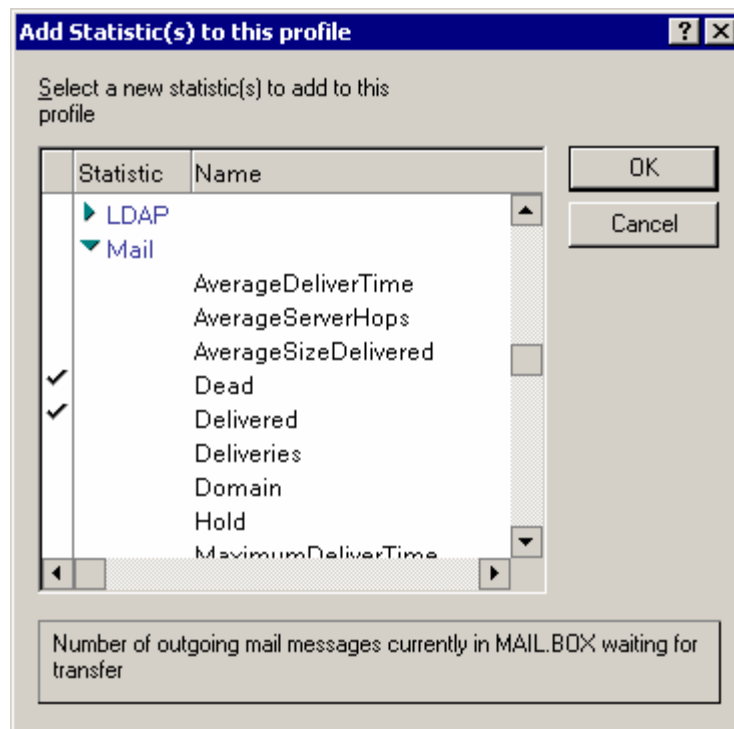


Рис. 679

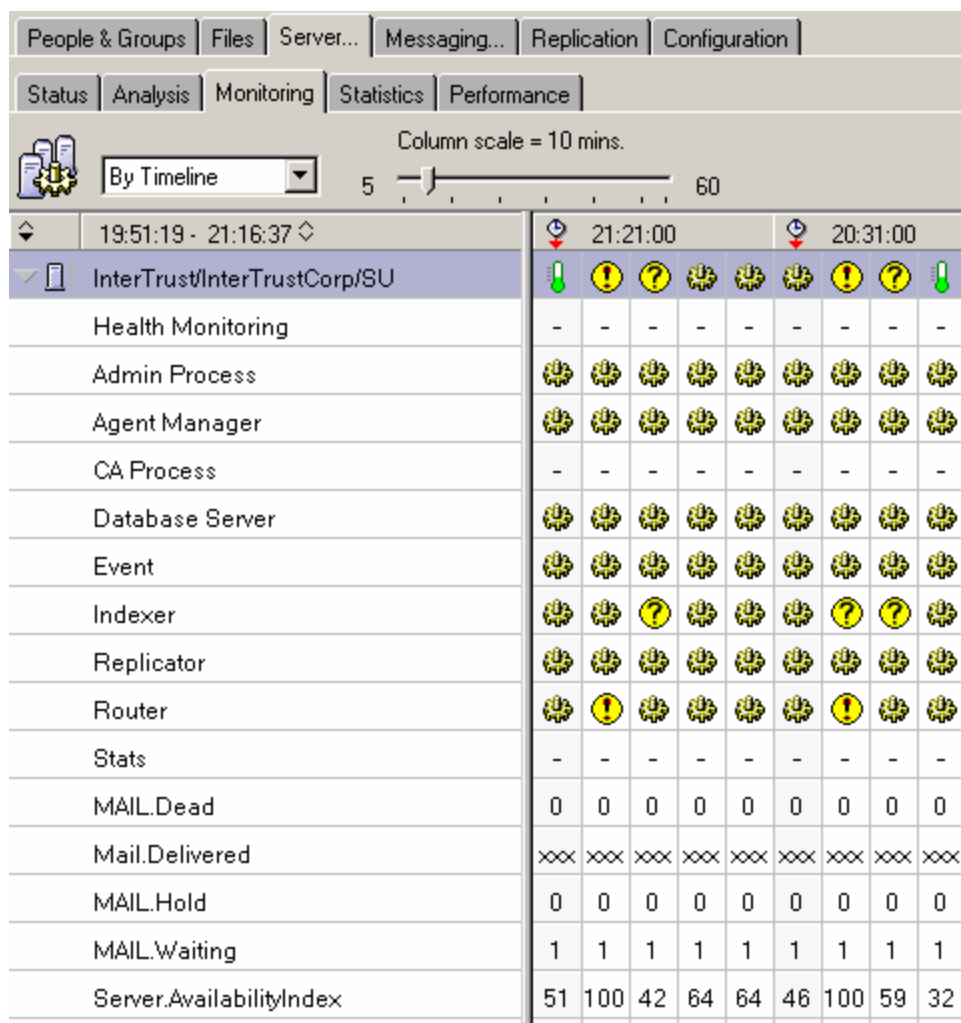


Рис. 680

1.72.10.4. 1.1.10.4. Программа Message Tracking Collector (MTC)

- • Конфигурирование программы
 - 📖 стр. 133-141
- • База Reports.nsf и создание отчетов о работе почтовой системы
 - 📖 стр. 133-135
 - 📖 стр. 136-138
- • Отслеживание сообщений и состояния их доставки
 - 📖 стр. 139-141

1.72.10.5. 1.1.10.5. Подсистема протоколирования почтовой активности

➤ 📖 стр. 270

1.72.11. 1.1.11. Устранение типовых почтовых проблем

- • **Тестирование соединений, используемых для передачи почты:** из Domino Administrator с закладки Messaging – Mail в меню Tools операция Send Mail Trace.
- • **Перезапуск серверной программы Router:** из Domino Administrator с закладки Messaging – Mail в меню Tools операции Stop Router и затем Start Router.
- • **Форсирование передачи почты:** из Domino Administrator с закладки Messaging – Mail в меню Tools операция Route Mail, что эквивалентно консольной команде route имя_сервера_Domino.
- • **Обработка «мертвой» (Dead) и недоставленной (Undelivered) почты:** из Domino Administrator с закладки Messaging – Mail выбрать вид YourServername Mailbox, изучить сообщения, по возможности применить к ним операции на кнопке Release.
- • **Поиск и устранение типовых неисправностей передачи почты по Notes RPC**
 - • The server's Mail.box has become corrupt. Остановить сервер и «отлечить» программой Fixup. Если не лечится – удалить.
 - • Unable to find path to server. Ping, а лучше Nconnect. Команда trace «имя_сервера_Domino или IP/host». Команда trace tcpip!!!«имя_сервера_Domino» - только заданным портом.
 - • The server is not responding. «Упал» или «завис» - поднять. Выдали команду stop port tcpip и забыли про start port tcpip – после перезапуска нет порта. Закрыли порт 1352 на файрволе.
 - • The remote server is not a known TCP/IP host. Работает ли DNS. Очистить клиентский кэш DNS. Убедиться в правильности имен хостов и IP-адресов в документах Connection, поименованных сетях (Network Address в документе Server), командах. Сменили IP-адрес, но забыли изменить его в NOTES.INI на сервере с привязкой портов к сетевым картам. Бывает, нужно «почистить» скрытые поля \$SavedAddresses, \$SavedPorts и \$SavedServers в документе Server.
- • **Поиск и устранение типовых неисправностей передачи почты по SMTP**

1.72.12. 1.1.12. Почтовые возможности клиента Notes

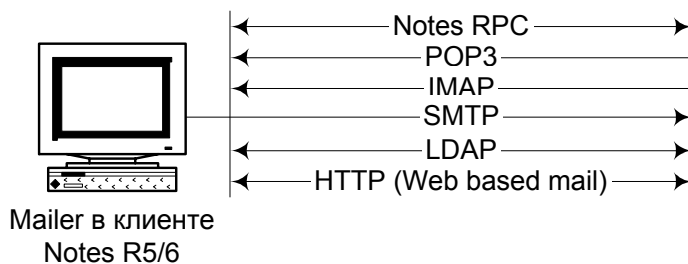


Рис. 681. Почтовые протоколы клиента Notes R5/6

- • Конфигурируется документами Account и Location в локальной NAMES.NSF.
- • Для чтения групп новостей (NNTP с клиента) и работы с почтовым ящиком по IMAP (режим Online, в режиме offline работа идет через стандартный почтовый ящик) создаются специальные клиентские базы. «Клик по документу» в такой базе влечет обращение к соответствующему серверу и получение документа. Работает «перетаскивание документов» между базами.

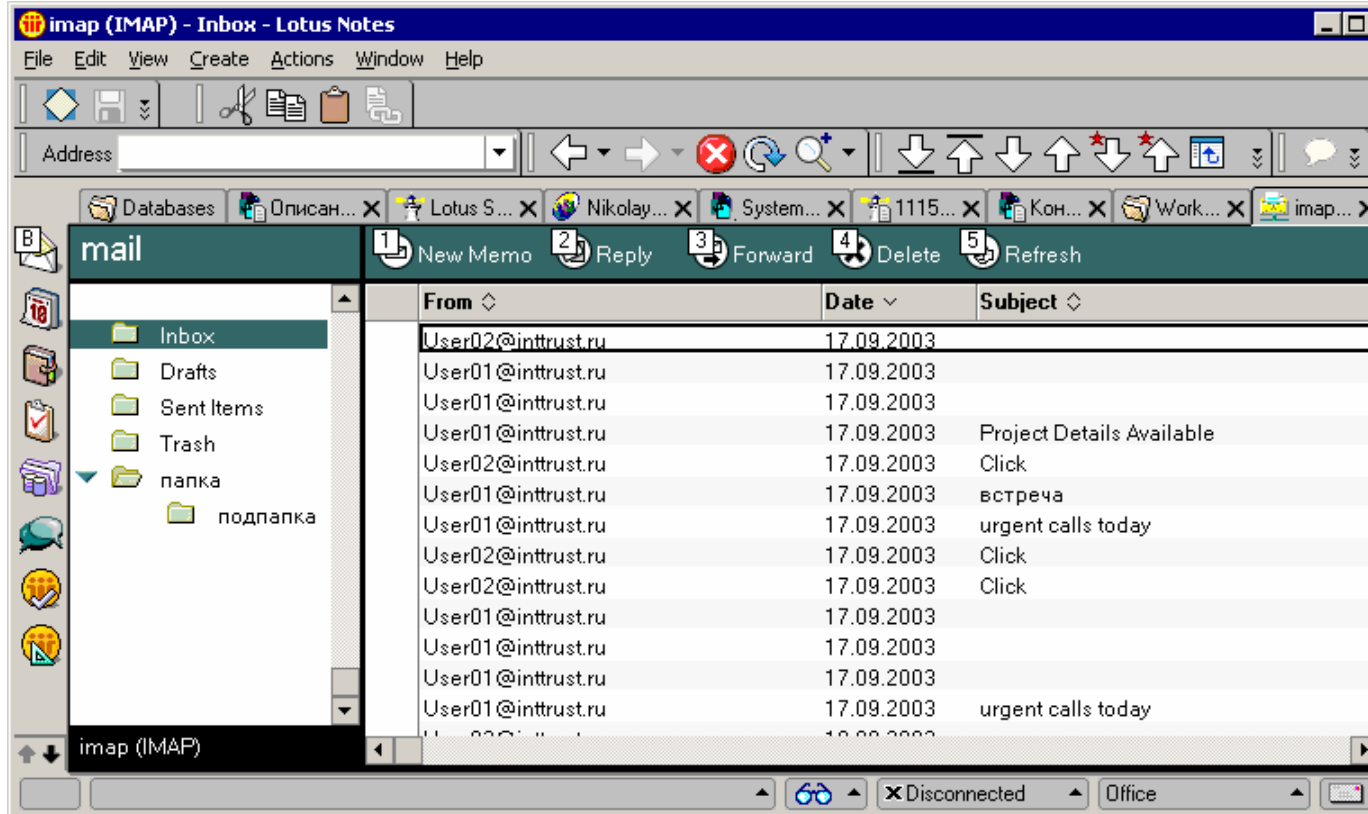


Рис. 682 База IMAP (режим Online). Тип базы IMAP Server Proxy

Можно создать ее реплику – будут содержать все документы, извлеченные по IMAP с сервера. Тип базы для реплики будет Standard.

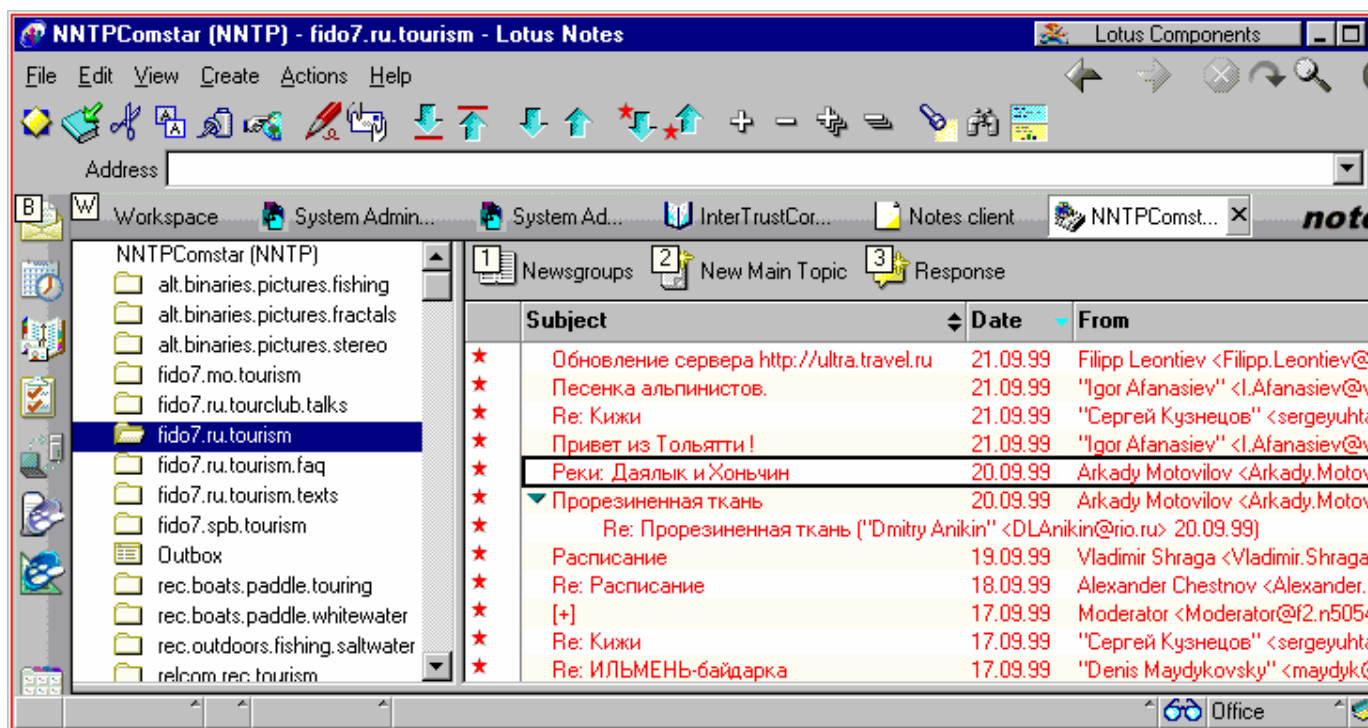


Рис. 683 Вид клиентской базы для чтения групп новостей (NNTP с клиента)

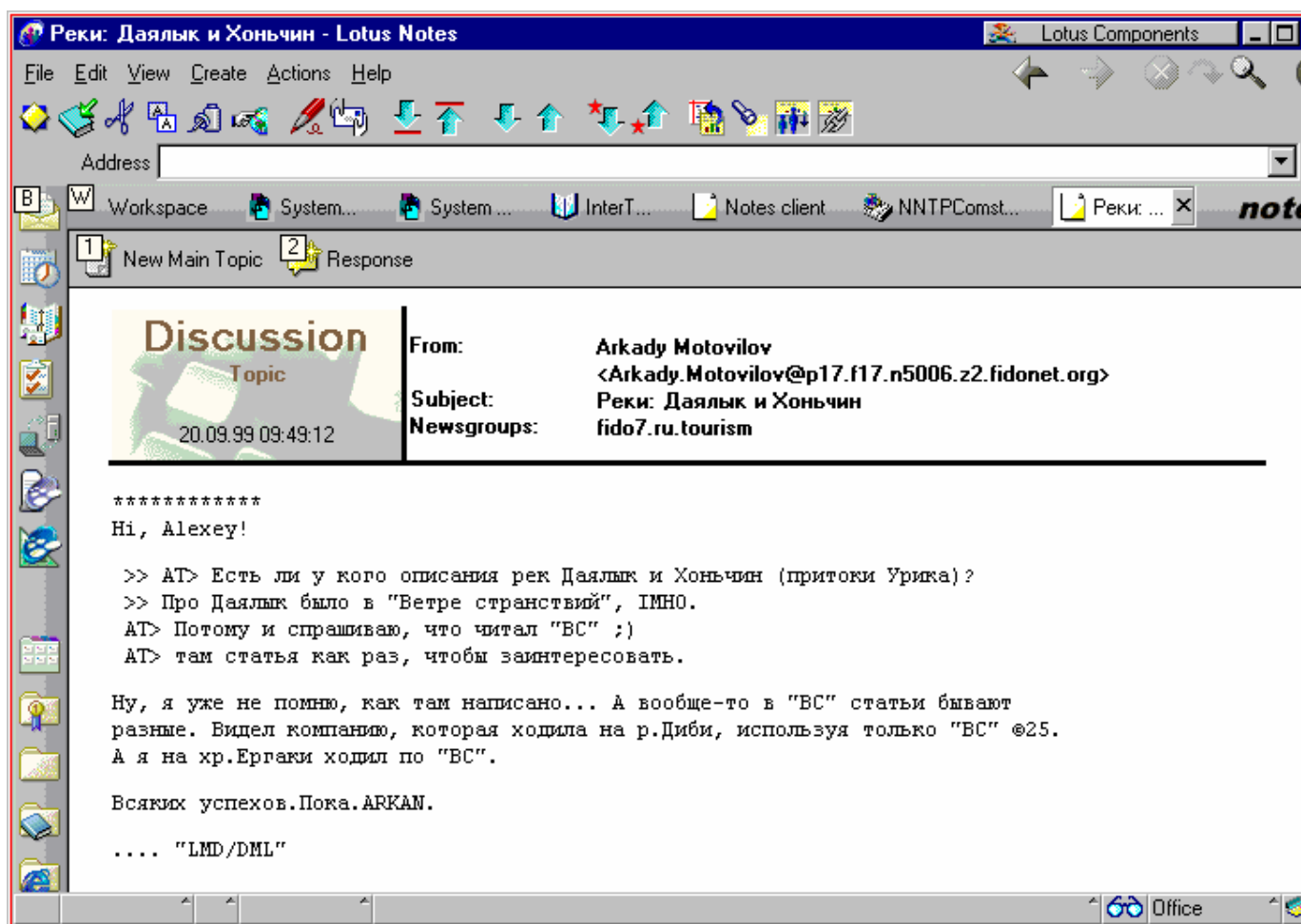


Рис. 684 Сообщение из группы новостей в клиенте Notes

1.72.12.1. 1.1.12.1. Устранение проблем с передачей почты с клиента Notes

- • Для устранения проблем с кодировками необходимо модифицировать документ International MIME Settings в локальной адресной книге клиента – на закладке Advanced в поле For non-MIME messages or MIME messages with an unknown character set, 8-bit character set is assumed to be выбирать кодировку.
- • Пользователь разрешил в почтовом файле mail rules, переносящие входящую почту в другую папку (не Inbox).

1.72.13.

1.1.13.

Краткий обзор S/MIME



стр. 281-298

1.73. 1.1. Программа Directory Cataloger (DIRCAT)

1.73.1. 1.1.1. Назначение, создание и конфигурирование Condensed Directory Catalog

➤  стр. 237

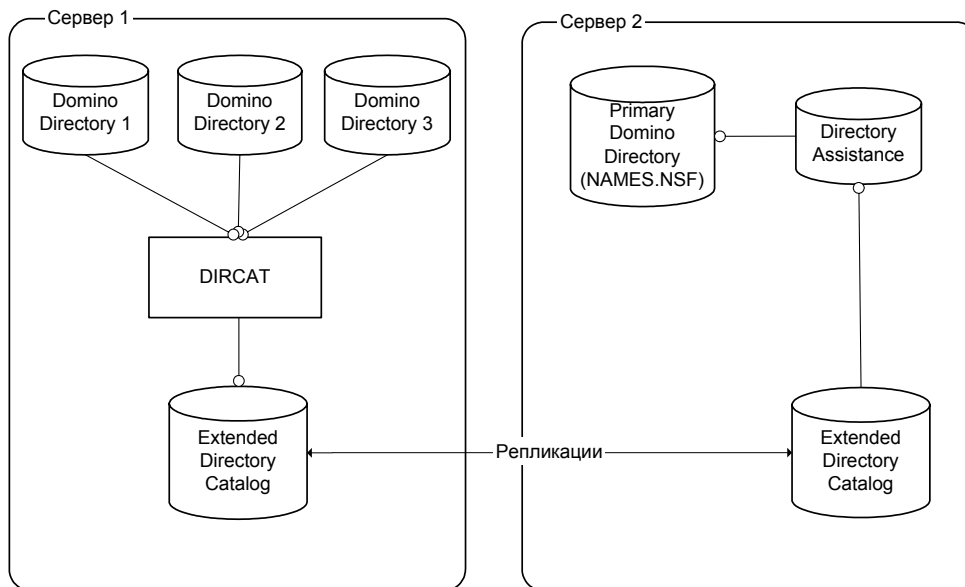


Рис. 685. Схема формирования и использования расширенного каталога

1.73.2. 1.1.2. Назначение, создание и конфигурирование Extended Directory Catalog

➤  стр. 265

«Полноразмерные» каталоги (Domino Directory)			Condensed Directory Catalog	
Название каталога	Кол-во элементов	Размер	Кол-во элементов	Размер
IBM US	103000	1 GB	127400	12 MB
Lotus	23000	518 MB		
Iris	1400	30 MB		
Итого	127400	1.55 GB	127400	12 MB

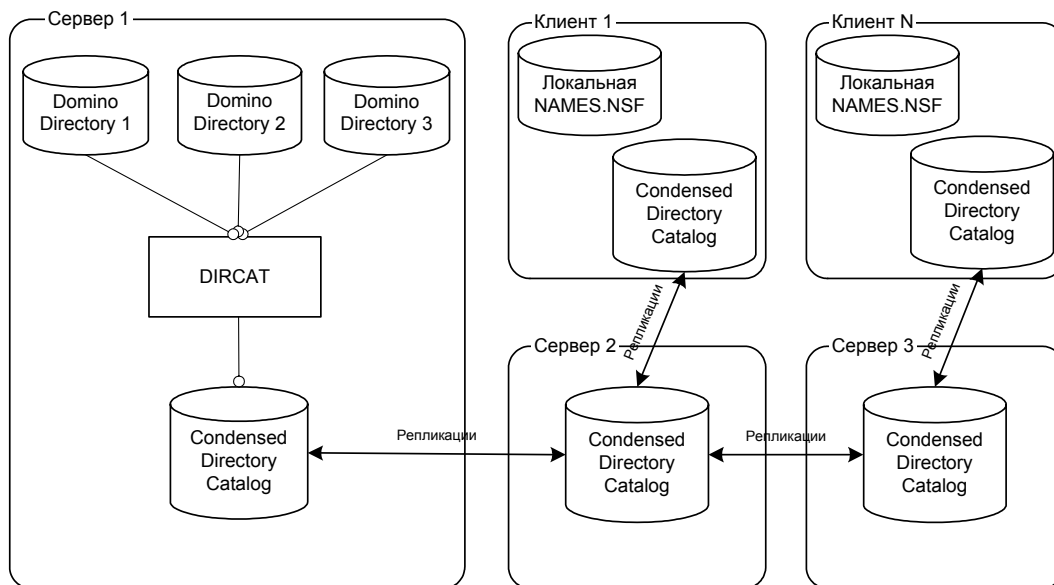


Рис. 686 Схема формирования и использования мобильного каталога

1.73.2.1. 1.1.2.1. Just-In-Time Encryption

When Notes users send encrypted mail to users registered in secondary Domino Directories, servers can use an Extended Directory Catalog to look up the public keys of the recipients to encrypt the mail. Even off-line Notes users with condensed Directory Catalogs can flag mail for encryption; then when they reconnect to the network to send the mail, the clients look up the public keys in the Extended Directory Catalog.

Storing public keys in a condensed Directory Catalog isn't recommended because it greatly increases its size. Instead, set up directory assistance for the aggregated Domino Directories so servers can look up the public keys in them.

Servers do not have to trust a directory catalog or a Domino Directory for credentials to use the directory to look up public keys for mail encryption.

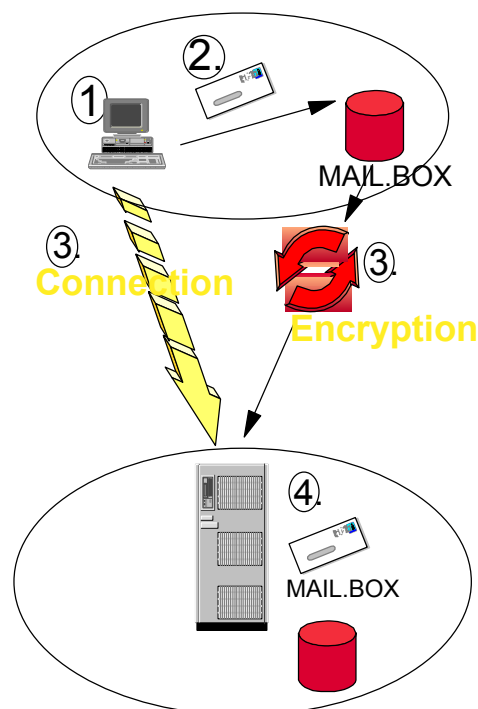
1. Пользователь создает почтовое сообщение и требует его шифровать.

2. Сообщение сохраняется локально в незашифрованном виде (открытый ключ получателя на клиенте неизвестен).

3. В момент соединения клиента с сервером клиент получает с сервера открытый ключ получателя.

4. Сообщение доставляется на сервер в зашифрованном виде.

Note: This feature is implemented for the NRPC protocol only.



1.74. 1.1. Программа GETADR и документ External Domain Network Information

Этот документ в Каталоге Domino функционирует совместно с серверной программой GETADRS и сервисом имен (name service). Все эти элементы позволяют пользователям соединяться с серверами вне своего домена (при этом предполагается, что возможно необходимые перекрестные сертификаты имеются) без создания в пользовательских адресных книгах документов Connection для каждого сервера, как это требовалось в версиях, предыдущих R5.

Хотя в предыдущих версиях такой документ Connection мог существовать в адресной книге сервера, используемого пользователями как сервер-посредник по умолчанию. Но в этом случае такой документ должен был существовать для каждого сервера из другого домена, до которого имелаась необходимость «добираться» пользователям. Обычно многие из таких документов не использовались для репликаций и передачи почты, а служили только для поддержки возможности установить соединение.

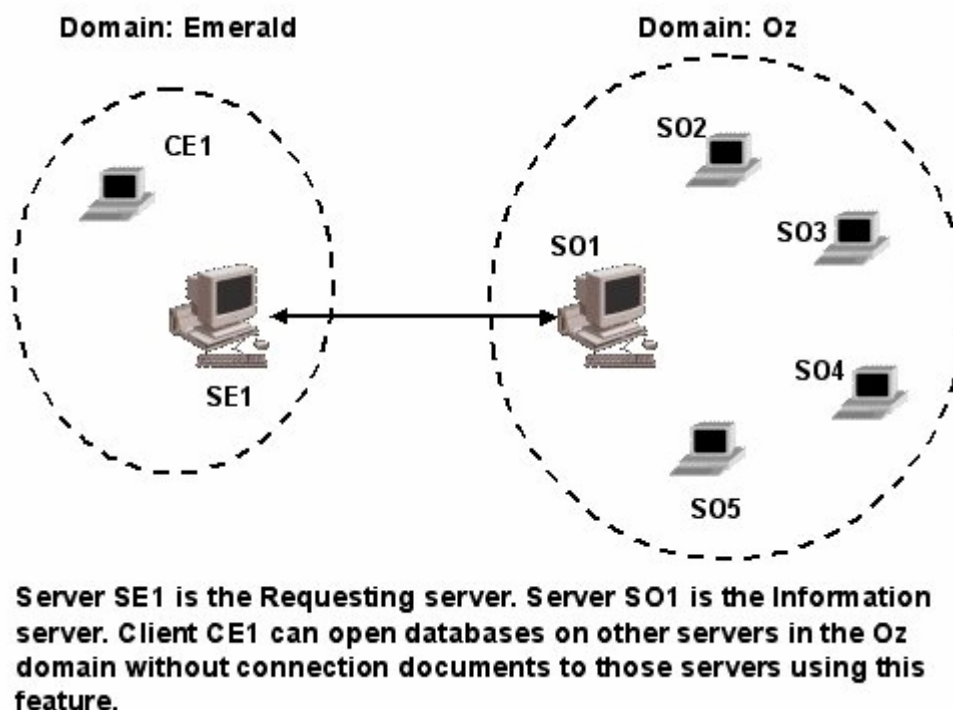


Рис. 687

На этом рисунке даны два домена, Oz и Emerald. Имеются взаимные сертификаты и документы Connection между серверами SE1 и SO1. В документе External Domain Network Information в Emerald сервер SE1 выбран как Requesting server. Когда на сервере SE1 запускается задача GETADRS (хотя бы командой консоли LOAD GETADRS), она список серверов и их адресов домена Oz у сервера SO1. В итоге клиенты домена Emerald могут после этого пытаться открывать базы данных на любых серверах домена Oz без создания документов Connection.

1.74.1. 1.1.1. Конфигурирование

Конфигурирование выполняется следующим образом.

1. В клиенте Администратора на закладке Configuration выберите вид Server\External Domain Network Information, и кнопкой Add External Domain Network Information создайте новый документ.

- • Requesting server (запрашивающий сервер) - сервер в вашем домене, задача GETADRS которого обращается к серверу из другого (внешнего) домена для получения информации о его серверах.
- • Information server (информационный сервер) - сервер во внешнем домене, с которым ваш запрашивающий сервер осуществляет соединение и получает от него необходимую информацию.
- • Domain (домен) - название внешнего домена.

2. Выберите необходимые протоколы, для которых выполняется запрос. Обычно это протокол TCPIP. Но если ситуация такова, что в обоих доменах используются протоколы TCPIP и NetBIOS, добавьте оба из этих протоколов. Сохраните и закройте документ. Пример документа показан ниже.

EXTERNAL DOMAIN NETWORK INFORMATION	
Basics	Administration
Basics	
Requesting server:	NotesSrv400/InterTrustCorp/SU
Information server:	194.196.39.10/Srv/LotusEmea/Net
Domain to query:	Net
Protocols to query:	TCPIP

Рис. 688

3. Выполните программу GETADRS на запрашивающем сервере. Задача выполняет опрос серверов из доменов, для которых есть документы External Domain Network Information, и создает или модифицирует в Каталоге Domino вашего сервера соответствующие документы, после чего завершается. Поэтому целесообразно создать в Каталоге Domino вашего сервера документ Program для запуска этой задачи по расписанию. Например, если выполнить задачу один раз в день, то любые изменения в другом домене по крайней мере через день станут известны Вашему домену.

> 1 getadrs

```

24.03.2000 20:55:13   GetAdrs: External server addresses retriever started
24.03.2000 20:55:17   Lookup on server 194.196.39.10/Srv/LotusEmea/Net
24.03.2000 20:55:17   Network: Connecting to 194.196.39.10/Srv/LotusEmea/Net
over TCPIP1
24.03.2000 20:55:17   Network: Using address '194.196.39.10' for
194.196.39.10/Srv/LotusEmea/Net on TCPIP1
24.03.2000 20:55:29   Network: Connected to server
194.196.39.10/Srv/LotusEmea/Net
24.03.2000 20:55:40   GetAdrs: There were no TCP address changes in domain
Net
24.03.2000 20:55:42   Lookup on server Notes1/Notesweb
24.03.2000 20:55:42   Network: Connecting to Notes1/NotesWeb over TCPIP1
24.03.2000 20:55:42   Network: Using address 'notes1.notes.net' for
Notes1/NotesWeb on TCPIP1
24.03.2000 20:55:44   Network: Connected to server Notes1/NotesWeb
24.03.2000 20:55:46   GetAdrs: Obtained 5 TCP addresses from domain notesWeb
24.03.2000 20:55:46   GetAdrs: Done. Processed 2 request(s)

```

Каждый создаваемый задачей документ представляет собой ответный документ на соответствующий документы External Domain Network Information. Этот документ содержит имена серверов и адреса, используемые для обращения к этим серверам по соответствующему протоколу. После того, как эти ответные документы появились в адресной книге вашего сервера, служба имен начинает функционировать.

Add External Domain Network Information
 Delete External Domain Network Information

Domain	Configuration
▼ Net	▼ Configuration for NotesSrv400/InterTrustCorp/SU to query 194.196.39.10/Srv/LotusEmea/Net for network information for c TCP addresses
▼ notesWeb	▼ Configuration for NotesSrv400/InterTrustCorp/SU to query Notes1/Notesweb for network information for domain notesWeb TCP addresses

EXTERNAL DOMAIN NETWORK ADDRESSES

Basics
 Administration

Basics

Domain to query:	notesWeb
Protocol:	TCPIP
Server names:	Iris2/Notesweb Iris3/NotesWeb Notes1/Notesweb Notes2/Notesweb Sandinbox2/NotesWeb
Server addresses:	10.0.0.4 10.0.0.3 205.159.212.140 205.159.212.143 205.159.212.184

Рис. 689

Учтите только такой момент, что на самом деле программа GETADRS не создает ответные документы сама, а лишь помещает в базу ADMIN4.nsf запрос на создание этих документов программой ADMINP сервера администрирования базы NAMES.NSF. Поэтому с момента завершения задачи GETADRS до момента появления ответных документов в NAMES.NSF проходит вполне определенное время.

▼ Net		
22.03 14:57		▼ Update External Domain Information
22.03 15:05		NotesSrv400/InterTrustCorp/SU performed action on: 22.03 15:05
24.03 20:58		► Update External Domain Information
▼ notesWeb		
24.03 20:55		▼ Update External Domain Information
24.03 20:58		NotesSrv400/InterTrustCorp/SU performed action on: 24.03 20:58
24.03 20:58		► Update External Domain Information

Рис. 690

1.75. 1.1. Ответы на вопросы слушателей

1.75.1. 1.1.1. Использование в Domino/Notes R6 (NotesRPC) алгоритмов шифрования с одним ключем с длиной ключа 128 бит

Между двумя сторонами R6 при шифровании трафика по порту используется RC4 с длиной ключа 128 бит (про другие контексты - шифрование почты и документов в базах – четких сведений пока не обнаружено). Причем даже в случае, когда ID-файл одной стороны R6 с международными лицензиями (создан еще в R3), а с другой стороны R6 – с северо-американскими лицензиями.

Lotus Software Knowledge Base, документ 1097816:

<http://second->

int.intrust.ru/Lotus/NotesNIC/Support/LotusKB.nsf/B48A95F9B4A7A68185256C8D0072E04C/3B8D17F6902CD55C85256CD70068BCF7?OpenDocument

<http://main->

int.intrust.ru/Lotus/NotesNIC/Support/LotusKB.nsf/B48A95F9B4A7A68185256C8D0072E04C/3B8D17F6902CD55C85256CD70068BCF7?OpenDocument

Для проверки поднять шифрование на порту, добавить в NOTES.INI параметры log_authentication=1 и Debug_Console=1, перезапустить сервер и рассмотреть сообщения на консоли.

Authenticate: CN=Nikolay N. Iontsev/O=InterTrustCorp/C=SU

T:128 E:1: S:128:22 A:4:1 L:N:I:N

1.75.2. 1.1.2. Partition-серверы разных версий в R6.5 и R6.0.3

Да, такое появилось, но только для серверов на платформе AS400.

Возможность упоминается в

<http://second->

int.intrust.ru/Lotus/NotesWeb/Today.nsf/8A6D147CF55A7FD385256658007AACF1/38CE21A6F60CC20885256DA40049EEF9?OpenDocument

<http://main->

int.intrust.ru/Lotus/NotesWeb/Today.nsf/8A6D147CF55A7FD385256658007AACF1/38CE21A6F60CC20885256DA40049EEF9?OpenDocument

Подробности в главе 12 в руководстве по R6.5 для AS400 [http://www-12.lotus.com/ldd/doc/uafiles.nsf/docs/series65/\\$File/i400help.pdf](http://www-12.lotus.com/ldd/doc/uafiles.nsf/docs/series65/$File/i400help.pdf)

1.75.3. 1.1.3. Compress network data в настройках порта

Появилось в R6, причем в ранних версиях R6 в Lotus Software Knowledge Base отмечались проблемы

1.75.4. 1.1.4. Проблема ранних версий R6 с обновлением состава групп в полях документа Server Configuration, разрешающих/запрещающих отправлять почту в Internet

Зафиксирована Lotus Software Knowledge Base, документ 1091128, должна быть уже исправлена в текущих версиях

<http://second->

int.intrust.ru/Lotus/NotesNIC/Support/LotusKB.nsf/B48A95F9B4A7A68185256C8D0072E04C/36E838DDB4C75CC885256CD7006870E4?OpenDocument

<http://main->

int.intrust.ru/Lotus/NotesNIC/Support/LotusKB.nsf/B48A95F9B4A7A68185256C8D0072E04C/36E838DDB4C75CC885256CD7006870E4?OpenDocument

1.75.5. 1.1.5. Агент Before Mail Arrived

Проведем тест. Уровень протоколирования Router надо выставить на максимум - тогда сообщения из таких агентов будут попадать на консоль сервера (Юлия Кадашевич).

Sub Initialize

Dim agentLog As New NotesLog("Agent log")

Call agentLog.OpenAgentLog

Dim session As New NotesSession

Dim doc As NotesDocument

Set doc = session.DocumentContext

Print "Сообщение: " + doc.Subject(0)

Call agentLog.LogAction("Сообщение: " + doc.Subject(0))

doc.Subject = doc.Subject(0) & " - обработано Pre Delivery агентом"

' Call doc.Remove(True) – тогда не будет доставлено

Call agentLog.Close

End Sub

Протокол на консоли сервера

```
11.03.2004 20:58:03 Router: Delivery to local recipient Vasily V.
Pupkin/ETC/InterTrust/RU is ready with 1 messages
11.03.2004 20:58:03 Router: Delivery thread 00000006 searching for work
11.03.2004 20:58:03 Agent printing: Сообщение: Письмо Bace
11.03.2004 20:58:03 Router: Message 0058E594 delivered to Vasily V.
Pupkin/ETC/InterTrust/RU from Nikolay N.
Iontsev/InterTrustCorp/SU@INTERTRUSTCORP OF0248DA38:A38F1E6C
ONC3256E54:0058E594 Size: 1K Time: 00:00:00 Hop Count: 2
```

Записано в AgentLog

```
Started running agent 'BeforeMailAgent' on 11.03.2004 20:58:03
Running on new mail messages: 1 total
11.03.2004 20:58:03: Сообщение: Письмо Bace
Ran LotusScript code
Done running agent 'BeforeMailAgent' on 11.03.2004 20:58:03
```

В Subject полученного сообщения

Письмо Bace - обработано Pre Delivery агентом

1.75.6. 1.1.6. Привязка задач сервера Domino к IP-адресам

```
;;; <NotesTcpPortName>_TcpIpAddress=0,IPaddress:1352
TCPIP_TcpIpAddress=0,169.254.6.61:1352
;;; Сам сервер Domino портом 1352 слушает только с этого IP
;;; <InternetServer>NotesPort=<NotesTcpPortName>
IMAPNotesPort=TCPIP
;;; IMAP слушает портом, указанным документе Server, с IP, назначенного порту
с именем TCPIP
POP3NotesPort=TCPIP
LDAPNotesPort=TCPIP
SMTPNotesPort=TCPIP
```

HTTP привязывается к IP-адресам в документе Server на закладке Internet Protocols - HTTP

Host name(s): 169.254.6.61
Bind to host name: Enabled

Проблемы только с привязкой ДПОР

1.76. 1.1. Обзор Upgrade R5 → R6

Абгрейт R5 → R6 обычно проходит относительно безболезненно (если не принимать во внимание последний этап – приложения, используемые клиентами Notes и Web – встречаются несовместимости...).

Рекомендуемый IBM/Lotus порядок абгрейта представлен на следующем рисунке.

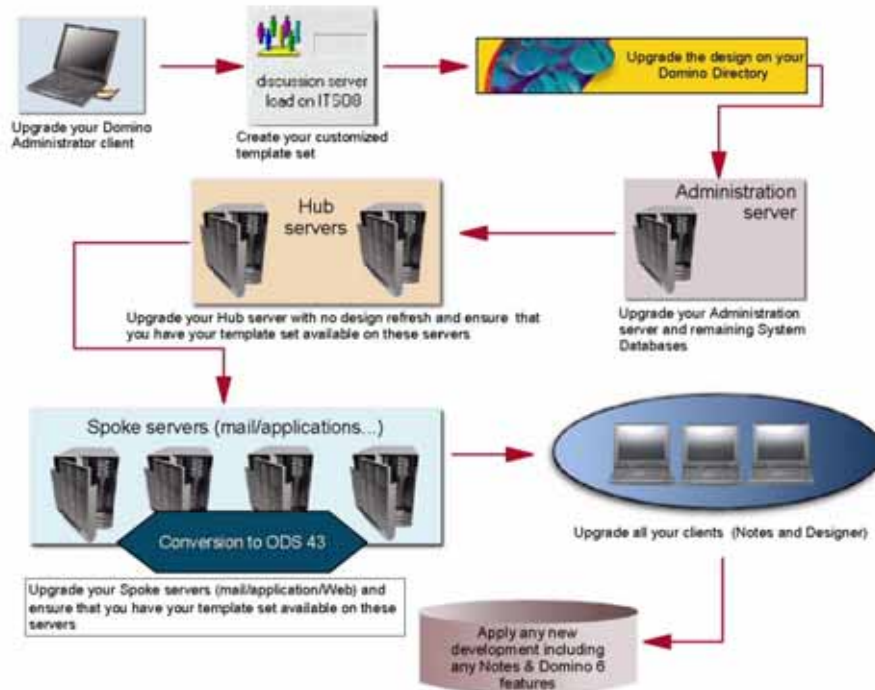


Рис. 691

Подробности абгрейта и использования новых возможностей в редбуке sg246889.pdf.

Инструктор посоветовал бы дополнительно следующий ставший ему привычным примитив:

- перед абгрейтом проверить в свойствах names.nsf флаг More Fields...
- остановить R5 и ncompact -C names.nsf
- выполнить установку, но не запускать сервер
- nfixup [-j]
- ncompact -C
- запустить сервер.