Аппаратное и программное обеспечение ЭВМ и сетей

Раздел 7 Сетевые операционные системы

Тема № 51. Проектирование доменов и развертывание Active Directory

- На сервере Windows 2003 может храниться более чем миллионе объектов. Служба каталога Active Directory позволяет структурировать, организовать управление и доступ к объектам и ресурсам сервера и сети. В предыдущей лекции отмечалось, что организация объектов каталога представляет собой древовидную структуру, которую также принято называть иерархией объектов каталога. Формирование этой иерархии входит в обязанности администратора, осуществляющего развертывание в сети Active Directory. Именно от администратора, осуществляющего проектирование структуры каталога, зависит то. насколько эффективно будет функционировать корпоративная сеть. Правильное проектирование позволяет избежать появления проблем в будущем.
- Архитектура службы каталога позволяет администратору осуществлять формирование структуры каталога на трех уровнях:
  - доменная структура каталога (создание структуры доменов);
  - логическая структура каталога (создание подразделений);
  - физическая структура каталога (создание подсетей и сайтов).

- Прежде чем приступить к созданию и реализации этих уровней, необходимо собрать информацию об организационной структуре и состоянии сетевых коммуникаций предприятия. Необходимо оценить общее количество пользователей сети, количество филиалов и количество пользователей в каждом из них. Дополнительно оцените возможность увеличения числа пользователей. В процессе проектирования структуры каталога рекомендуется исходить из расчета, что произойдет увеличение количества пользователей в полтора раза. Соберите информацию о существующих коммуникационных линиях. Важными являются сведения о пропускной способности, степени ее использования, количестве компьютеров в каждой из подсетей. В данной лекции мы рассмотрим некоторые важные вопросы планирования структуры Active Directory, которые нужно решить до начала процесса развертывания доменов на базе Active Directory. Затем мы подробно рассмотрим операции по установке контроллеров и созданию дерева доменов.

Сценарии формирования пространства имен DNS

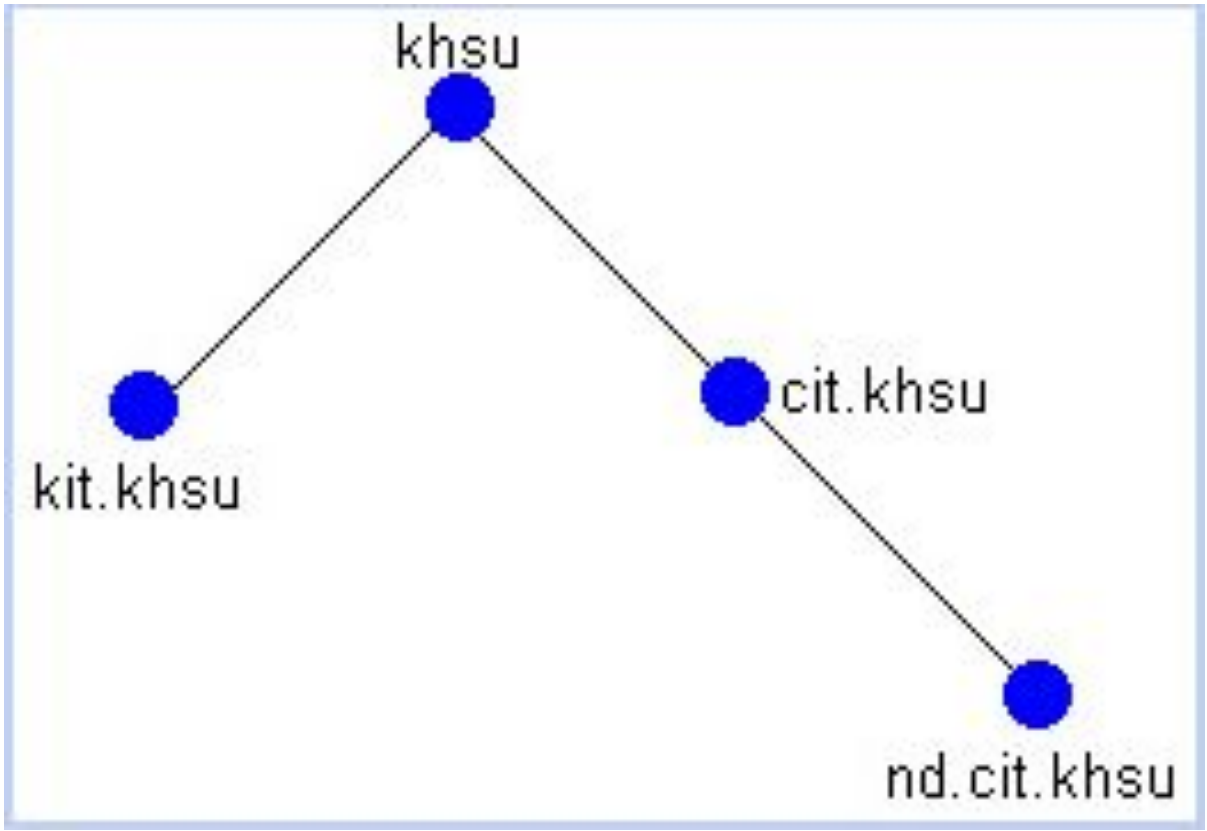
- . Фактически существует три сценария:
  - изолированное пространство имен DNS;
  - пространство имен DNS, интегрированное с внешним пространством имен:
  - пространство имен DNS, являющееся фрагментом другого более глобального пространства имен.

Изолированное корпоративное пространство имен.

- Данный сценарий является наиболее простым. Корпоративное пространство имен DNS полностью изолировано от других пространств имен, являющихся внешними по отношению к компании. Для решения задач, стоящих перед работниками компании, не требуется доступ к внешним ресурсам. Пример подобного пространства имен приведен на рис. 51.1.
- Для реализации подобного пространства имен необходимо, чтобы DNS-сервер. стоящий на вершине корпоративного пространства имен DNS. являлся корневым сервером. Для этого необходимо, чтобы все корпоративные DNS-серверы указывали на этот сервер как на корневой сервер пространства имен. Кроме того, корневой сервер не должен быть сконфигурирован для переадресации запросов на другой DNS-сервер. Другими словами, вкладка ***Пересылка*** (Forwarders) окна свойств этого сервера должна быть пустой.

Сценарии формирования пространства имен DNS

- Для адресации хостов в корпоративной сети администратор может использовать в принципе любые IP- адреса, но лучше все-таки частные адреса для локальных сетей.



- Рис. 7-51.1. Изолированное пространство имен DNS

Сценарии формирования пространства имен DNS

- На следующем этапе администратор должен выбрать способ именования доменов. Формируя пространство имен DNS. не являющегося частью пространства DNS-имен Интернета, администратор может не придерживаться схемы именования доменов, принятой в этой глобальной сети. Нет нужды использовать для имен доменов первого уровня стандартные имена Интернета — by, ru, com. edu и т. п. Определяющим здесь является понятность и простота.

Корпоративное пространство имен, интегрированное с внешним пространством имен.

- Данный сценарий предполагает существование внутреннего корпоративного пространства имен, с возможностью выхода в другую сеть в том числе и Интернет. Фактически оба пространства (корпоративное и внешнее) представляют собой отдельные непересекающиеся пространства имен. Корпоративное пространство имен по своей сути идентично изолированному пространству имен, рассмотренных в предыдущем сценарии.

Сценарии формирования пространства имен DNS

- Администратор может выбрать любую схему именования доменов, а также может выбрать любую схему адресации хостов. *Все запросы пользователей на разрешение доменных имен можно условно разделить на две категории:*
  - запросы на разрешение доменных имен, принадлежащих к корпоративному пространству имен. Эти запросы разрешаются корпоративными DNS-серверами;
  - запросы на разрешение доменных имен, принадлежащих ко внешнему пространству имен. Эти запросы разрешаются внешними DNS-серверами, обслуживающими внешнее пространство имен.
- Данный сценарий реализуется следующим образом. Корпоративное пространство формируется также, как и в предыдущем случае. Однако корневой DNS-сервер конфигурируется таким образом, чтобы все запросы, адресованные к внешним доменам, переадресовывались на один из внешних DNS-серверов. Для этого используется режим выборочного перенаправления, который конфигурируется на вкладке ***Перенаправление*** (***Forwarders)*** окна свойств корневого сервера.

Сценарии формирования пространства имен DNS

- Для внутренних доменов корпоративного пространства имен режим перенаправления на корневом сервере должен быть отключен. Для остальных доменов запросы должны переадресовываться на внешний DNS-сервер.

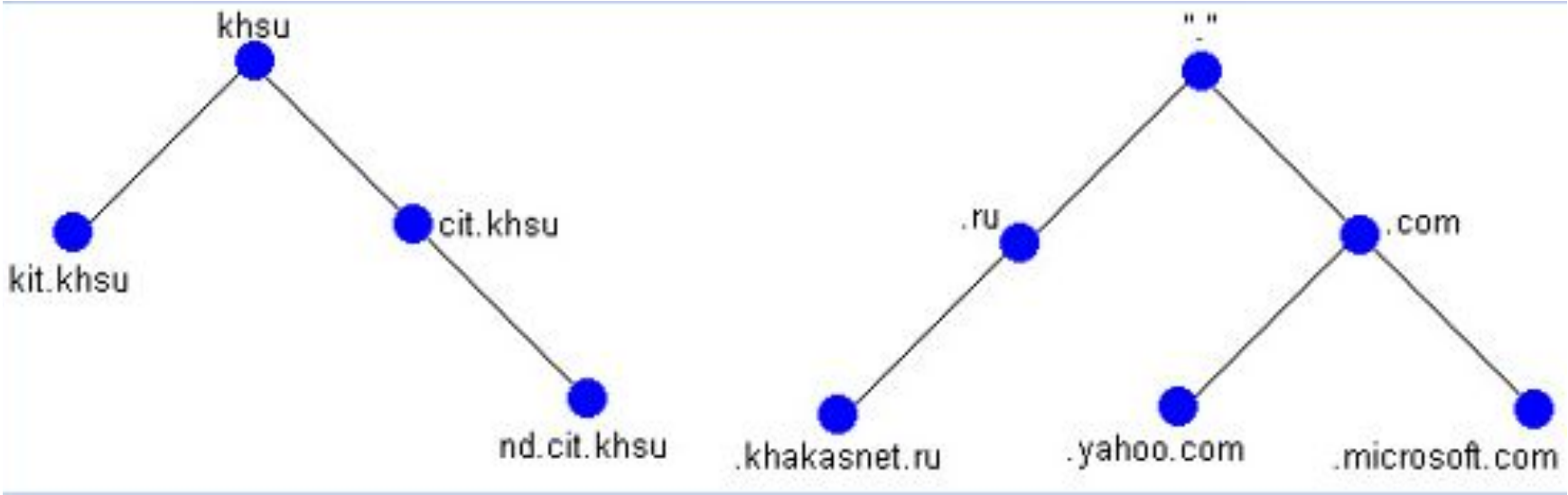


Рис. 7-51.2. Корпоративное пространство имен и пространство имен Интернета

- *Примечание*
- *Для решения этой задачи администратору необходимо соответствующим образом сконфигурировать маршрутизаторы и межсетевые экраны.*

Сценарии формирования пространства имен DNS

Корпоративное пространство имен, являющееся частью внешнего пространства имен.

- В последнем рассматриваемом сценарии корпоративное пространство имен является фрагментом другого более крупного пространства имен. Например, корпоративная вычислительная сеть интегрируется с глобальной сетью Интернет. В этом случае все корпоративные доменные имена, а также адреса хостов являются реальными адресами и именами Интернета. Такая интеграция имеет массу преимуществ. Одно из них — ресурсы корпоративной сети могут быть доступны из любой точки мира. При этом доступность не предполагает незащищенность. Администратор может отделить внутреннюю сеть от внешней сети межсетевым экраном и использовать системы сертификации и аутентификации.
- В случае Интернета для регистрации имен и получения пула адресов корпорация должна обратиться в соответствующие инстанции.
- Для интеграции необходимо сконфигурировать корпоративный корневой DNS-сервер для перенаправления всех запросов на внешний DNS-сервер.

Сценарии формирования пространства имен DNS

Функциональные уровни

- В службе каталога Windows 2000 существует понятие режима функционирования домена (domain mode). Домен может находиться в одном из двух режимов — основном (native) или смешанном (mixed). Режим функционирования домена определяет возможность использования контроллеров домена Windows NT. В Windows Server 2003 появилось понятие функционального уровня (functional level). Функциональный уровень определяет доступные функциональные возможности.
- В табл. 51.1 перечислены существующие функциональные уровни домена и допустимые типы контроллеров домена.
- **Таблица 51. 1Функциональные уровни домена.**

Функциональный уровень	Допустимые контроллеры домена
Windows 2000 mixed	Windows NT, Windows 2000, Windows Server 2003
Windows 2000 native	Windows 2000, Windows Server 2003
Windows Server 2003	Только Windows Server 2003

Сценарии формирования пространства имен DNS

- Необходимость введения понятия функционального уровня обусловлена ограничением на использование некоторых функциональных возможностей в ситуации, когда в домене (или лесе доменов) присутствуют контроллеры домена Windows NT/2000. Администратор может реализовать постепенный, поэтапный перевод корпоративной сети на новую версию операционной системы.
- Функциональный уровень определяется как для отдельных доменов, так и для всего леса доменов в целом.
- Охарактеризуем каждый из функциональных уровней.
  - Windows 2000 mixed. Этот функциональный уровень допускает сосуществование в домене контроллеров домена, находящихся под управлением различных операционных систем (Windows NT/2000 и Windows Server 2003). Контроллеры домена Windows NT могут быть только в качестве резервных контроллеров домена (Backup Domain Controller, BDC). Один из контроллеров домена (Windows Server 2003/2000) выступает в качестве основного контроллера домена Windows NT (Primary Domain Controller, PDC). На данном уровне недоступен ряд возможностей Windows 2000 доменов — универсальные (universal) группы безопасности, вложенность групп и т. д. Все создаваемые домены по умолчанию находятся на этом функциональном уровне.

Сценарии формирования пространства имен DNS

- Windows 2000 native. Данный функциональный уровень ограничивает перечень используемых контроллеров доменов только Windows 2000 и Windows Server 2003. Тем не менее, клиенты могут работать под управлением любых операционных систем. На этом функциональном уровне становятся доступны все возможности Windows 2000 доменов. Однако ряд функциональных возможностей Windows Server 2003 недоступен — возможность переименования контроллеров домена, использование объектов класса InetOrgPerson, номера версий ключей Kerberos.
- Windows Server 2003. Если домен переведен на этот функциональный уровень, в нем допускается использование только контроллеров домена Windows Server 2003. На этом уровне становятся доступны все функциональные возможности службы каталога Windows Server 2003.

Сценарии формирования пространства имен DNS

Функциональный уровень леса доменов

- Функциональный уровень леса доменов определяет набор функциональных возможностей Active Directory, доступных в масштабах всего леса доменов. Существует два функциональных уровня.
- ***Windows 2000***. Данный функциональный уровень предполагает наличие в сети контроллеров домена различных версий — Windows NT/2000 и Windows Server 2003. В этом случае некоторая часть новых возможностей Active Directory недоступна. Используется функциональность леса, поддерживаемая системами Windows 2000.
- ***Windows Server*** 2003. Чтобы поднять лес доменов на этот функциональный уровень, нужно перевести все контроллеры домена леса под управление Windows Server 2003. На этом функциональном уровне становятся доступными новые возможности, перечисленные в табл. 51.2. Эти функции касаются всего леса доменов и доступны в любом домене.
- Таким образом, чтобы сделать доступными весь спектр возможностей Windows Server 2003, администратор должен поднять лес доменов на функциональный уровень Windows Server 2003.

Сценарии формирования пространства имен DNS

- **Таблица 51. 2 Новые возможности доменов и леса, доступные на функциональном уровне Windows Server 2003**

Функция	Описание
Переименование домена	Любой домен может быть переименован. Процесс переименования может привести к изменению положения домена в рамках иерархии домена (за исключением корневого домена леса)
Доверительные отношения между лесами доменов	Между двумя лесами доменов, находящимися на функциональном уровне Windows Server 2003, могут быть установлены транзитивные доверительные отношения (как односторонние, так и двусторонние)
Репликация связанных (linked) значений	Изменение состава группы пользователей приводит к передаче информации только о новых или удаленных членах группы
Деактивация объектов схемы	Определения классов объектов и атрибутов, содержащиеся в схеме, не могут быть удалены (поскольку это нарушило бы целостность каталога). Вместо этого администратор может выполнить деактивацию требуемого объекта (например, если он содержит ошибку). Впоследствии объект может быть снова активирован
Оптимизация процесса репликации содержимого глобального каталога	Если происходит изменение одного из атрибутов объекта, содержащегося в глобальном каталоге, реплицируется не весь объект, а только измененный атрибут
Динамические объекты и вспомогательные классы	Администратор может создавать в каталоге объекты, которые имеют , ограниченный срок жизни (существуют в каталоге в течение строго определенного периода времени)
Усовершенствованный алгоритм генерации топологии репликации	Оптимизирована работа сервиса Knowledge Consistency Checker (KCC) для лесов доменов, имеющих большое количество сайтов

Сценарии формирования пространства имен DNS

Изменение имен доменов

- В службе каталога Active Directory, реализованной в составе Windows 2000. лес доменов представлял собой статичную структуру. Администратор мог либо добавить новые домены или даже целые деревья, либо удалить их. Он не мог изменить пространство имен каталога, переименовав один или несколько доменов.
- В службе каталога Active Directory Windows Server 2003 ‘реализована возможность изменения имени домена.
- ***Изменение DNS- или NetBIOS-имени домена***. Этот процесс предполагает изменение имени, не приводящее к изменению структуры леса доменов. **Изменение имени корневого домена приводит к автоматическому изменению имен всех дочерних доменов**.
- ***Перемещение домена в рамках дерева доменов***, либо перемещение в другое дерево доменов. В этом сценарии процесс переименования сводится к изменению родительского домена. Частным случаем является ситуация, когда перемещаемый домен образует новое дерево доменов.
- Процесс переименования является далеко не тривиальным. Непосредственно переименование выполняется утилитой командной строки Rendom.exe. Эта утилита используется исключительно для изменения имени домена. Она не может использоваться для добавления нового домена или удаления существующего.

Установка контроллеров домена

- Развертывание службы каталога начинается непосредственно с установки контроллеров домена и процессу установки контроллеров домена необходимо уделять особое внимание.

Подготовка к установке контроллера домена

- Перед установкой контроллера домена, администратор должен проделать несколько подготовительных операций.

1. Администратор должен убедиться в том, что компьютер, выбранный на роль контроллера домена отвечает предъявляемым к нему требованиям: -минимальные аппаратные и программные требования, первое из условий успешного выполнения операции установки.
2. Кроме того, перед выполнением установки контроллера домена необходимо убедиться в работоспособности службы DNS, без которой Active Directory работать не будет. Тестирование службы DNS на подготовительном этапе позволит предотвратить возникновение проблем в процессе установки контроллера домена.

Установка контроллеров домена ***Требования и ограничения***

- Обычно выделенный сервер «повышают» до контроллера домена, что требует выполнения определенных условий..

3. Перед установкой должен быть установлен стек протоколов TCP/IP и ***для каждого из интерфейсов сервера выделен статический IP-адрес.*** Впоследствии можно изменить этот адрес и заново зарегистрировать в базе данных DNS доменное имя с новым адресом.
4. Для сервера должен быть установлен DNS-суффикс, соответствующий имени домена, для которого будет устанавливаться контроллер домена. Требование является необязательным, если установлен флажок «***Сменить основной DNS-суффикс при смене членства в домене»***. При включении сервера в состав домена, система автоматически определит DNS-суффикс.
5. ***Служба каталога должна быть установлена на раздел диска с файловой системой NTFS***. Соблюдаем необходимый уровень безопасности, с разграничением

Установка контроллеров домена ***Требования и ограничения***

6. Раздел, предназначенный для установки службы каталога, должен иметь как минимум 250 Мбайт свободного дискового пространства.
7. *С целью повышения производительности службы каталога файлы хранилища каталога и журнала транзакций лучше разместить на отдельные физические диски. Это позволит избежать конкуренции операции ввода/вывода*. (на NTFS раздел.).
8. Полномочия системного администратора:

- При установки первого контроллера домена на одиночном сервере, сисадмин должен обладать полномочиями локального администратора на этом сервере.
- Если происходит установка первого контроллера в домене в рамках уже существующего леса доменов, пользователь должен являться членом группы Enterprise Admins (*Администраторы корпорации*).
- В случае установки дополнительного контроллера в домене пользователь должен быть либо членом уже упомянутой группы, либо членом группы Domain Admins (*Администраторы домена*).

Проверка службы DNS

- Прежде чем запустить на сервере мастер установки Active Directory, администратор должен проверить настройки стека протоколов TCP/IP для данного компьютера, обратив, в первую очередь, внимание на параметры службы DNS-клиента. Одним из важнейших параметров в этой ситуации является адрес «***Предпочитаемого DNS-сервера»*** (preferred DNS server). Именно указанный в этом параметре сервер будет использоваться мастером установки для диагностики пространства имен DNS, предшествующего созданию нового домена Active Directory, и поиска существующих носителей копий каталога. Этот же DNS-сервер впоследствии будет использоваться для регистрации доменного имени сервера. Ошибки, допущенные на этом этапе, могут привести к тому, что по окончании процедуры установки контроллер домена окажется неработоспособным. Типичны следующие ошибки:

Проверка службы DNS

- Типичны следующие ошибки:
  - настройки сервера, выбранного на роль контроллера домена, не содержат сведений о предпочитаемом DNS-сервере;
  - В DNS сервера не установлен режим динамической регистрации доменных имен.
  - DNS-сервер, указанный в настройках будущего контроллера домена в качестве предпочтительного, не является носителем требуемой зоны. Кроме того, возможна и другая ситуация, когда указан сервер, являющийся дополнительным носителем зоны.

1. На первом этапе развертывания в сети службы каталога (первый контроллер домена в лесу), необходимо предоставить возможность мастеру установки Active Directory установить на сервере службу DNS и произвести ее последующее конфигурирование. При этом в настройках стека протоколов TCP/IP данного сервера параметр Preferred DNS Server (Предпочитаемый DNS-сервер) должен указывать непосредственно на сам сервер. После установки контроллера домена все ассоциированные с ним ресурсные записи будут зарегистрированы службой DNS. Все последующие контроллеры домена должны указывать уже на существующий DNS-сервер.

2. Если сервер имен DNS не Windows 2003/2000, необходимо убедиться в том, что он поддерживает ресурсные записи SRV-типа и допускает возможность динамической регистрации имен.
3. Проверить конфигурацию службы DNS с точки зрения возможности повышения некоторого сервера до роли контроллера домена в уже существующем домене khsu.ru можно с помощь утилиты DCdiag.exe, поставляемой в составе вспомогательного комплекта утилит Windows Server 2003 Support Tools, например:

- ***C:\dcdiag.exe /test:dcpromo /dnsdomain:khsu.ru /replicadc***

Установка контроллеров домена

- В случае ошибки проверяются настройки DNS-сервера или берется другой DNS.
- С помощью этой утилиты можно проверить способность будущего контроллера домена выполнить динамическую регистрацию доменного имени в базе данных DNS-сервера: (данная утилита запускается на будущем сервере- контроллере домена)
- ***c:\dcdiag.exe /test:RegisterlnDNS /dnsdomain:khsu.ru***
- Но обычно достаточно утилиты ***Dcpromo*** -Мастера установки Active Directory в Windows Server 2003, которая имеет новые встроенные средства диагностики конфигурации DNS.

Обновление существующего леса доменов Windows 2000

- Архитектура службы каталога Windows Server 2003 претерпела ряд принципиальных изменений.
- Как следствие, наличие различий в архитектуре потребовало выполнения специальной процедуры "подготовки" службы каталога Windows 2000 к установке контроллеров домена Windows Server 2003. Фактически эта процедура сводится к выполнению расширения схемы. Для выполнения процедуры используется специальная утилита командной строки Adprep.exe. Эта утилита поставляется в составе дистрибутивного диска Windows Server 2003 и располагается в каталоге \I386.
- *Перед выполнением "подготовки" леса доменов Windows 2000 на всех контроллерах домена должен быть установлен пакет обновления Windows 2000 Service Pack 2 (или выше). В противном случае работа утилиты Adprep может привести к нарушению работоспособности отдельных контроллеров домена.*

Установка контроллеров домена

*Установка контроллера домена **Windows Server 2003***

- Процедура установки контроллера домена (повышение роли сервера до контроллера домена) выполняется при помощи мастера Active Directory Installation Wizard (Мастер установки Active Directory). Этот мастер запускается утилитой командной строки Dcpromo.exe.
- В процессе установки контроллера домена происходит наполнение каталога. В случае установки первого контроллера домена в лесе все содержимое каталога создается непосредственно мастером установки. Если в лесе создается новый домен, то мастер установки создает только доменный раздел. Раздел схемы и каталога копируется с уже существующих контроллеров домена. В ситуации, когда администратор создает дополнительный контроллер в уже существующем домене, имеется два варианта наполнения каталога:
- все содержимое каталога копируется с уже существующего контроллера домена;

- содержимое каталога воссоздается из резервной копии каталога.
- Каждый вариант имеет свои плюсы и минусы.

Выполнение установки

- При использования мастера установки Active Directory возможны четыре сценария (рис. 7-51.3):

1) создание нового леса доменов;
2) создание нового дерева доменов в рамках существующего леса доменов;
3) создание нового домена в рамках существующего дерева доменов;
4) установка дополнительного контроллера домена в уже существующем домене.

Установка контроллеров домена

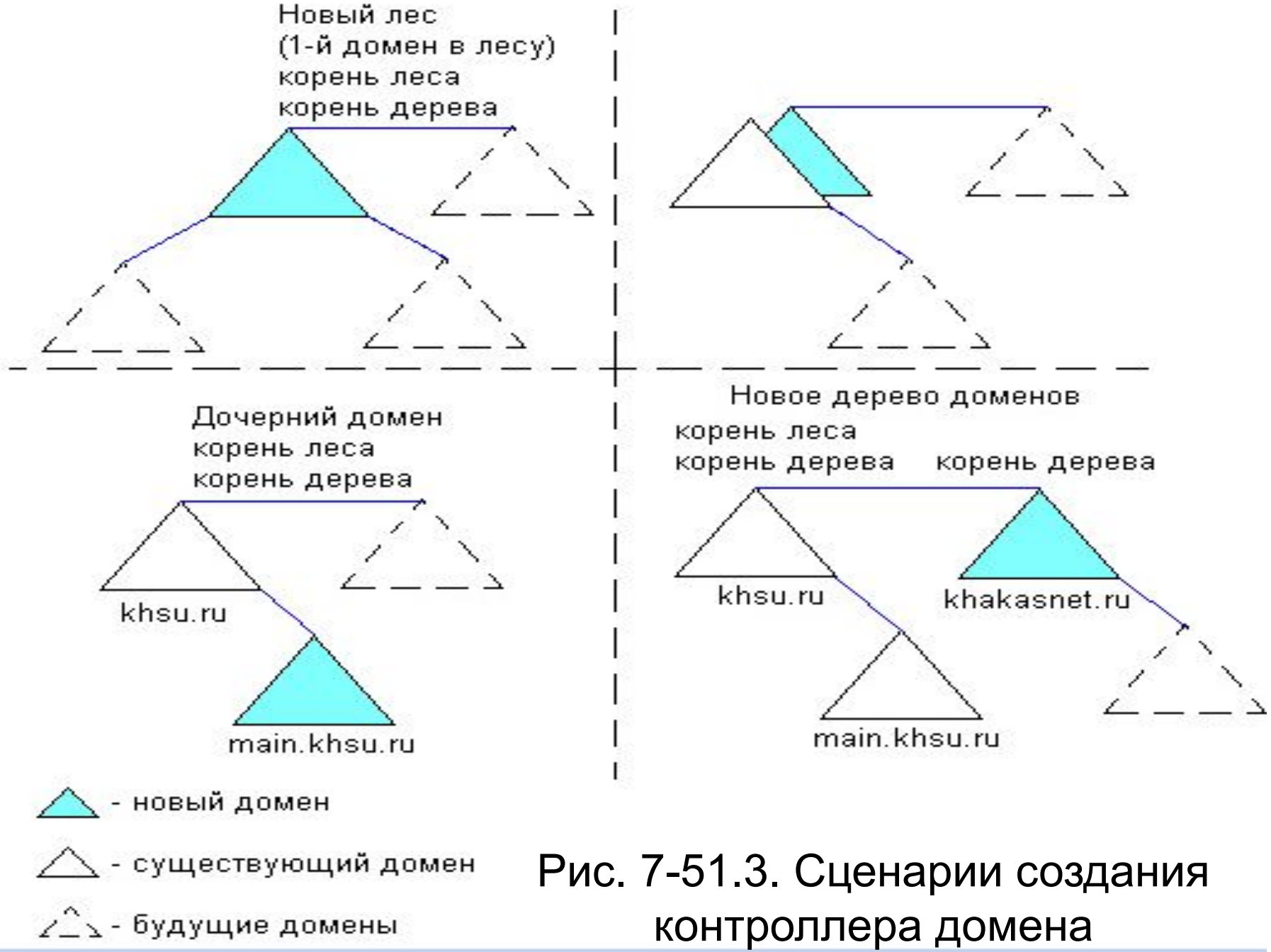


Рис. 7-51.3. Сценарии создания контроллера домена

Установка контроллеров домена

- Администратор осуществляет выбор одного из этих сценариев на первых страницах мастера. Если сценарий предполагает создание нового домена, мастер предложит ввести доменное и NetBIOS-имя будущего домена. В сценарии, предполагающем установку дополнительного контроллера, администратору будет необходимо ввести имя существующего домена.
- Независимо от избранного сценария мастер предложит выбрать место расположения файлов хранилища (БД), журналов и системного тома SYSVOL. Вы можете согласиться с предложенным по умолчанию (%SystemRoot%\NTDS и %SystemRoot%\NTDS) разместить их в одной папке (по умолчанию предлагается %SystemRoot%\ SYSVOL), либо разместить на разные папки или физические диски.
- На следующем этапе мастер, учитывая информацию о выбранном администратором доменном имени, обратится с запросом к службе DNS. В этом случае используется информация о предпочитаемом DNS-сервере. Версия мастера установки Active Directory Windows Server 2003, позволяет выполнить диагностику имеющейся конфигурации службы DNS в случае возникновения проблем. На рис. 7-51.4 изображено окно мастера в ситуации, когда предпочитаемый DNS-сервер не содержит зоны для создаваемого домена Active Directory. При этом администратору будет предложено несколько вариантов дальнейших действий.

1. ***Проблема решена. Запустить диагностический тест DNS снова.*** (I have corrected the problem. Perform the DNS diagnostic test again). Выбор этого переключателя предписывает мастеру произвести повторную диагностику службы DNS. Предполагается, что администратор вмешался и устранил возникшую проблему. Применительно к рассматриваемой ситуации, администратор может выполнить создание необходимой зоны.
2. ***Установить и настроить DNS- сервер на этом компьютере и выбрать этот DNS- сервер в качестве предпочитаемого.*** (Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server). Выбор этого переключателя перекладывает все обязанности по конфигурированию DNS-сервера на мастера установки Active Directory. Мастер сам выполнит установку службы DNS и создаст все необходимые зоны (за исключением зон обратного разрешения).

Установка контроллеров домена

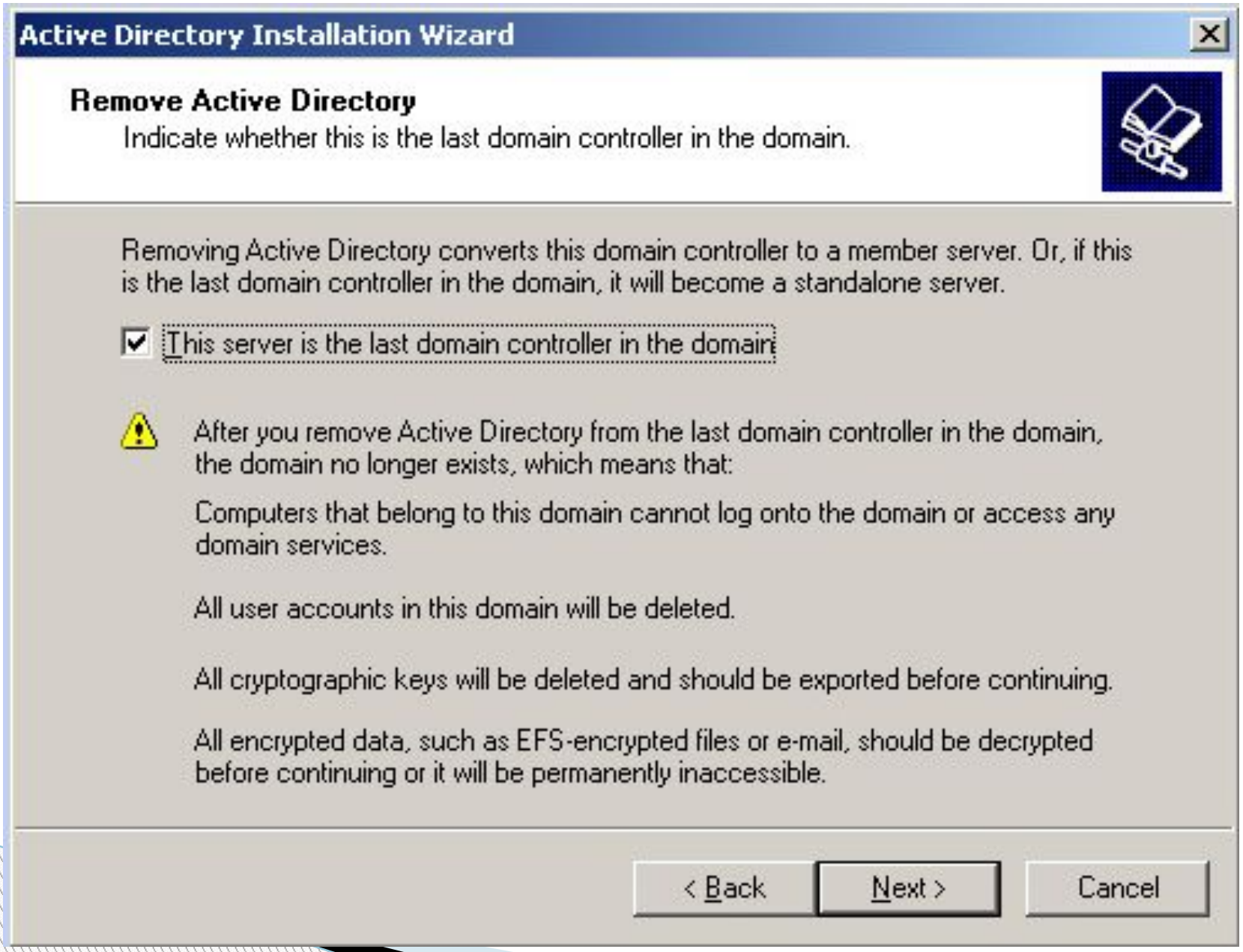


Рис. 7-51.4. Мастер установки обнаружил проблемы с разрешением имени будущего домена

3. ***Проблема будет решена позже ручной настройкой DNS (расширенная)*** (I will correct the problem later by configuring DNS manually (Advanced)). Эта опция означает, что мастер должен продолжить свою работу, несмотря на обнаруженные ошибки. Администратор в этом случае берет на себя все обязанности по конфигурированию службы DNS после окончания процедуры установки. Администратору нужно будет создать две зоны для создаваемого домена и зарегистрировать в них все необходимые ресурсные записи.

- *Примечание*
- *Мастер также выдаст сообщение об ошибке, если предпочтительный DNS-сервер не содержит информацию о домене, для которого предполагается установить дополнительный контроллер домена.*

4. Если процесс тестирования структуры DNS закончился успешно, мастер выдаст соответствующую информацию (рис. 7-51.5).

Установка контроллеров домена

5. На заключительном этапе работы мастера администратору необходимо будет определить уровень совместимости разрешений с подсистемой безопасности Windows NT. Если в среде Windows Server 2003 планируется существование серверов под управлением Windows NT (не обязательно контроллеров домена) с установленными на них серверными приложениями, необходимо выбрать уровень совместимости разрешений с платформой Windows NT (переключатель Permissions compatible with pre-Windows 2000 operating system).
6. По окончании установки контроллера домена потребуется перезагрузить систему. В процессе загрузки будет зарегистрировано доменное имя в базе данных предпочитаемого DNS-сервера.

- ***Если установленный контроллер домена является первым в лесу, то учетная запись локального администратора, в контексте которого производилась установка, преобразуется в учетную запись Administrator (Администратор созданного домена).***

Установка контроллеров домена

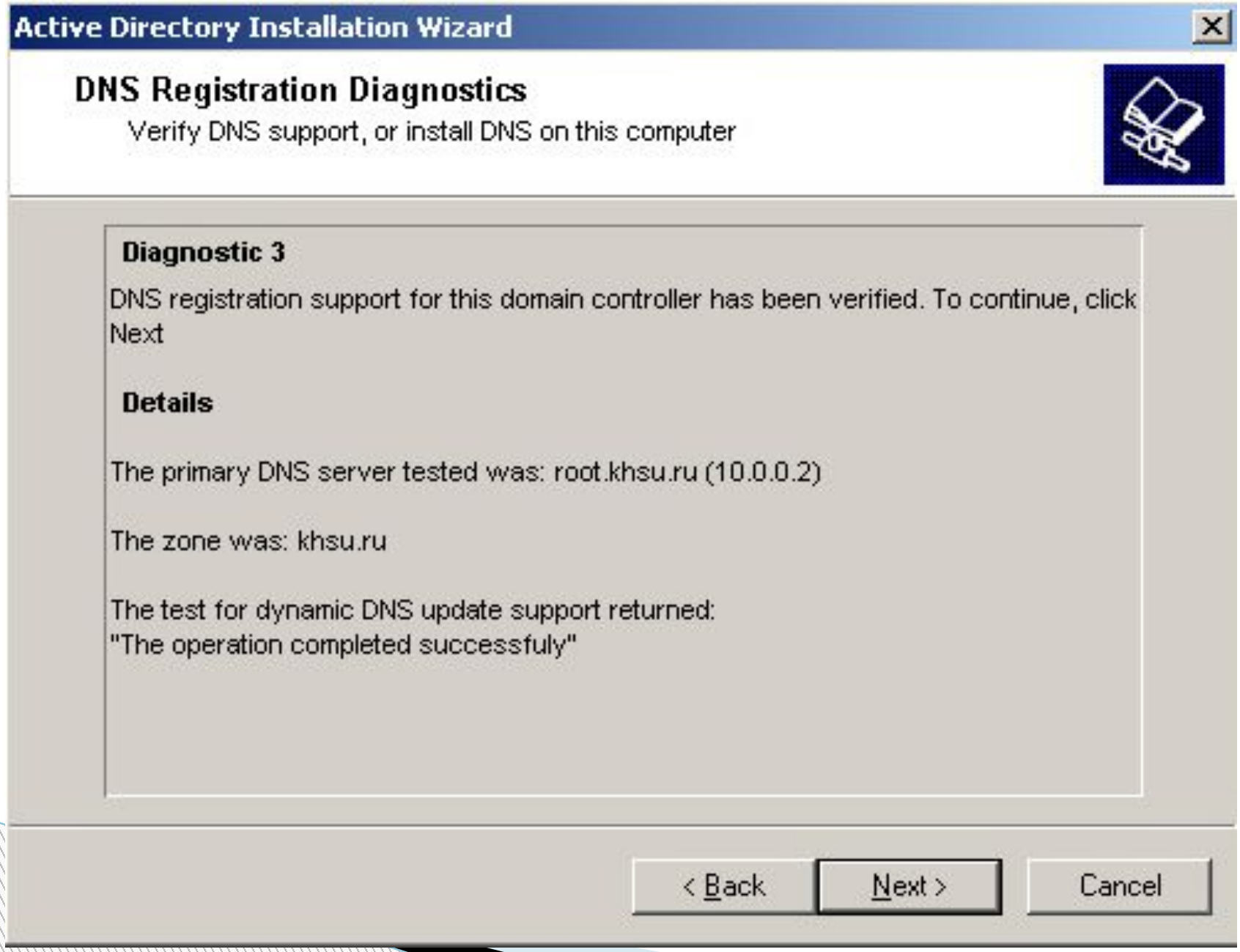


Рис. 7-51.5. Процедура тестирования службы DNS окончилась успешно

Установка контроллеров домена

- Эта учетная запись автоматически включается в состав следующих групп:
- ***Администраторы (Administrators).*** Встроенная локальная группа;
- ***Администраторы домена (Domain Admins)***. Группа с глобальной областью действия. Члены этой группы обладают необходимыми полномочиями для управления доменом. По умолчанию включается в состав группы ***Администраторы***;
- ***Пользователи домена*** (***Domain Users)***. Группа с глобальной областью действия. В состав этой группы включаются все создаваемые в контексте домена пользователи. По умолчанию группа включается в состав встроенной локальной группы ***Users***;
- ***Администраторы предприятия (Enterprise Admins).*** Группа с глобальной областью действия. Члены этой группы обладают полномочиями на управление инфраструктурой службы каталога. По умолчанию группа включается в состав группы ***Администраторы***;
- ***Владельцы-создатели групповой политики (Group Policy Creator Owners)***. Группа с глобальной областью действия. Члены этой группы могут редактировать параметры объектов групповой политики в рамках данного домена;
- ***Администраторы схемы*** (***Schema Admins)***. Группа с глобальной областью действия. Члены группы обладают полномочиями, необходимыми для изменения схемы каталога.

Установка контроллеров домена

Установка контроллера домена из резервной копии

- Архитектура Windows Server 2003 позволяет установить в домене дополнительный контроллер, используя резервную копию о состоянии системы (System state) **уже существующего контроллера домена**. Но данная возможность распространяется **только на установку дополнительных доменов**. Создание нового домена или дерева доменов может быть выполнено только стандартным способом.
- Установка контроллера домена из резервной копии позволяет избежать копирования всего содержимого каталога через сеть. Вместо этого, наполнение вновь устанавливаемого каталога будет производиться с резервной копии. Администратор может использовать эту возможность для установки контроллера домена в удаленных филиалах, соединенных с основной корпоративной сетью. Преимущества указанного метода особенно ощутимы в случае большого размера копии каталога. В этом сценарии на одном из контроллеров домена корпоративный администратор создает резервную копию и передает ее администратору удаленного филиала. Администратор филиала, используя полученную резервную копию, выполняет установку дополнительного контроллера домена. После процедуры синхронизации только что установленный контроллер готов обслуживать пользователей филиала.

Установка контроллера домена из резервной копии

- *Примечание*
- *Однако необходимо заметить, что даже в случае установки с резервной копии полностью исключить взаимодействие через сеть с уже существующими контроллерами домена нельзя. Поэтому в процессе выполнения установки создаваемый контроллер домена должен иметь сетевое соединение с другими контроллерами в домене.*
- Если резервная копия была создана на контроллере домена, выполняющем функцию сервера глобального каталога, устанавливаемый из этой копии контроллер домена может быть также сконфигурирован в качестве сервера глобального каталога непосредственно в процессе установки. С другой стороны, существующие разделы приложений не будут автоматически воссозданы на устанавливаемом контроллере домена, даже если оригинальный контроллер был их носителем. Для создания этих разделов администратор должен использовать утилиту Ntdsutil.exe.
- В процессе создания резервной копии, предназначенной для установки дополнительных контроллеров домена, необходимо снять флажок Automatically backup System Protected Files with the System State (***Автоматически резервировать защищенные системные файлы)***. В этом случае в создаваемую резервную копию не будут включаться защищенные системные файлы.

Установка контроллера домена из резервной копии

- Для установки контроллера домена из резервной копии часто используют утилиту Backup. В начале извлекают (воостанавливют) файлы из резервной копию в некоторую папку. Для этого из раскрывающегося списка Restore files to (Восстановить файлы в) выберают значение Alternate location (Альтернативное место расположения) и в одноименном поле указывают папку, в которую должна быть восстановлена резервная копия.
- После того как процесс восстановления из резервной копии закончится, необходимо запустить утилиту Dcpromo с ключом /adv. Это приведет к запуску мастера установки Active Directory в расширенном режиме. После того как будет выбран режим установки дополнительного контроллера домена, мастер предложит указать способ наполнения каталога на создаваемом контроллере (рис. 7-51.6):
- ***наполнение через сеть*** путем копирования с уже существующего контроллера домена. В данном случае процесс установки продолжится по стандартному сценарию;
- ***наполнение из резервной копии***. Этому способу соответствует пункт From these restored backup files. При этом администратору потребуется указать папку, в которой располагается восстановленная на предыдущем этапе резервная копия.

Установка контроллеров домена

- *Примечание*
- *Если будет выбран режим создания нового домена, процедура установки контроллера домена продолжится по стандартному сценарию.*

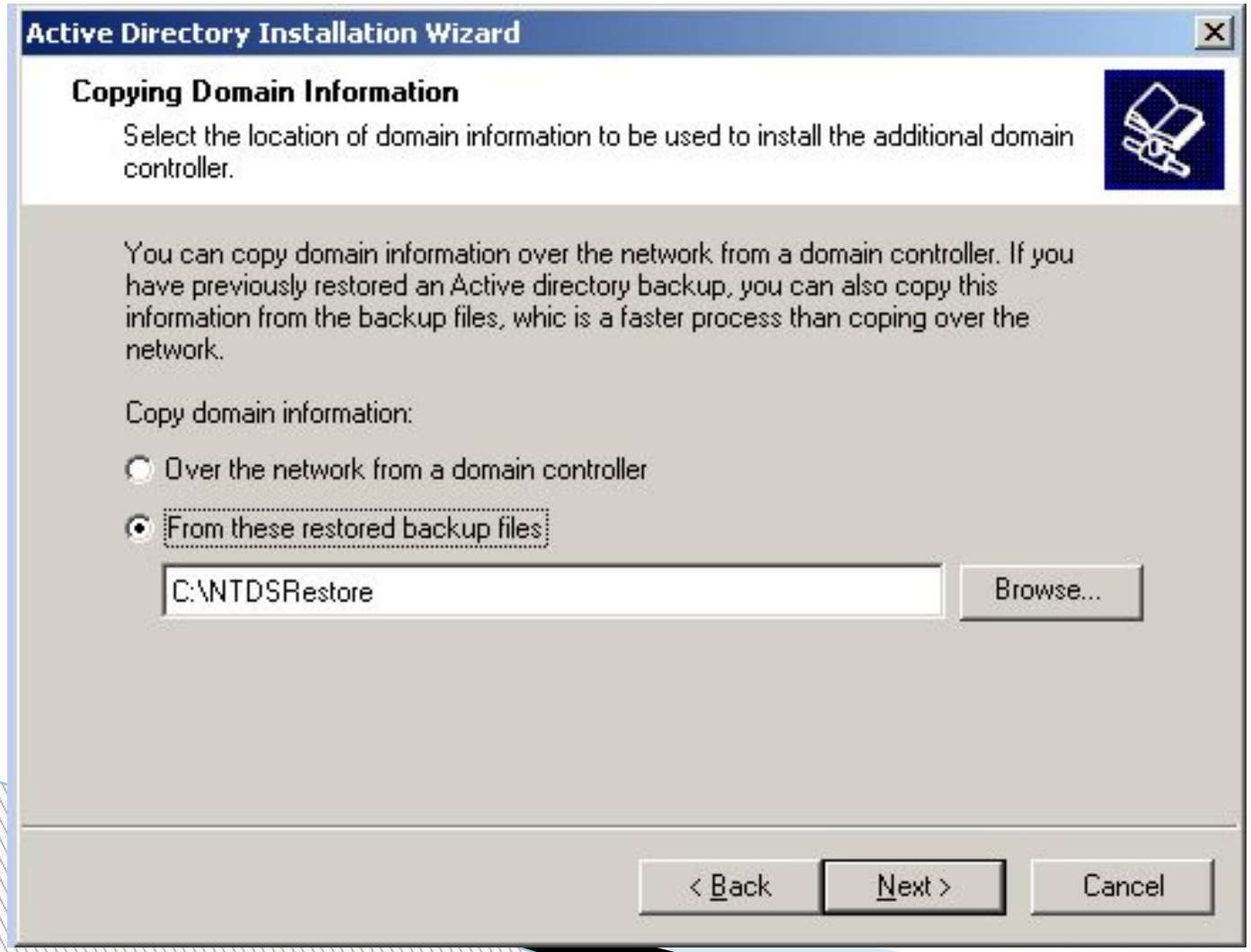


Рис. 7-51.6. Выберите способ наполнения каталога для устанавливаемого контроллера домена

Установка DC . Проверка состояния контроллера домена

- При возникновении неисправностей в Active Directory не работают: служба репликации, аутентификации, проблема с выполнением групповых политик и т. д. Необходимо убедиться в том, что серверы Windows Server 2003 действительно являются контроллерами домена.
- **Способы проверки операции повышения роли сервера (promotion) до контроллера домена:**
  - Раздел реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services должен содержать подраздел NTDS.
  - Введите в командной строке net accounts. Поле Computer role (Роль компьютера) должна содержать значение PRIMARY или BACKUP для контроллера домена. Для обычных серверов это поле имеет значение SERVERS.

Установка DC . Проверка состояния контроллера домена

- Введите в командной строке net start. В списке запущенных сервисов должна присутствовать служба Kerberos Key Distribution Center (Центр распределения ключей Kerberos). Если эта служба не запущена на контроллере домена, механизм аутентификации может не работать.
- Введите в командной строке nbtstat -n. Имя домена, имеющее тип <IC>, должно быть зарегистрировано (в поле **Состояние** (Status) указано значение REGISTERED).
- Введите в командной строке net share. На сервере должны присутствовать общие папки SYSVOL (%SystemRoot%\SYSVOL\sysvol) и NETLOGON (%SystemRoot%\SYSVOL\sysvol\<DomainDNSName>\SCRIPTS).

Установка контроллеров домена

- С помощью утилиты Ldp.exe проверьте значение атрибута isSynchronized объекта RootDSE. По окончании процесса повышения роли сервера система должна полностью синхронизировать все разделы каталога. Когда синхронизация закончена, атрибут isSynchronized принимает значение TRUE.
- Используйте утилиту командной строки NLtest.exe. Эта утилита поставляется в составе пакета вспомогательных утилит Windows Server 2003 Support Tools.
- С помощью утилиты Ntdsutil.exe можно подключиться к только что установленному контроллеру домена и проверить его способность отвечать на запросы LDAP. Утилита позволяет также проверить, знает ли контроллер о расположении ролей FSMO в своем домене.

Изменение имени контроллера домена

- Архитектура Windows Server 2003 допускает возможность изменения имени контроллеров домена (в Windows 2000 такая возможность отсутствует). Сам процесс изменения имени не сопряжен с какими-либо сложностями, однако от администратора требуется четкое выполнение определенной последовательности действий. Целью этих действий является последующее изменение всех записей об имени контроллера домена в базе данных службы DNS и в копиях каталога других контроллеров домена (фактически являющихся партнерами по репликации).
- *Внимание*
- *Изменение имени контроллера домена возможно только в домене, находящемся на функциональном уровне Windows Server 2003.*
- Процесс переименования контроллера домена не предполагает его перемещение между различными доменами. Чтобы выполнить перемещение контроллера между доменами, необходимо выполнить его понижение (demotion) до обычного сервера, а затем заново установить его в уже новом домене.
- Перед изменением имени контроллера домена необходимо проинформировать других носителей каталога о его новом имени. Для этого в режиме командной строки необходимо выполнить операцию:
- ***netdom computername <текущее_имя> /add:<новое_имя>***

Изменение имени контроллера домена

- В результате новое имя контроллера домена будет зарегистрировано в базе данных службы DNS в качестве альтернативного имени. Необходимо подождать пока информация о новом имени не будет реплицирована на все носители зоны. После этого альтернативное имя надо сделать основным. Для этого используется команда:
- ***netdom computer-name <текущее_имя> /MakePrimary: <новое_имя>***
- Данная команда обновляет сведения об имени контроллера домена в каталоге Active Directory. На этом этапе необходимо перезагрузить контроллер домена. После того как изменения будут реплицированы на все носители каталога, следует выполнить команду, удаляющую старое имя из базы данных DNS и каталога Active Directory:
- ***netdom computername <новое_имя> /Remove:<текущее_имя>***
- После этого можно изменять собственно имя компьютера. Для этого откройте окно свойств объекта My Computer (Мой компьютер) и перейдите на вкладку Computer Name (Имя компьютера). Щелкните по кнопке Change (Изменить) и в открывшемся окне замените существующее имя компьютера новым.

Удаление контроллера домена

- Под удалением контроллера домена фактически понимается понижение его до роли обычного сервера. Порой бывает необходимо удалить один или несколько контроллеров из домена или переместить их в другой домен. Нельзя просто вывести контроллер из состава домена, поскольку информация о нем останется в каталоге. Соответственно, этот контроллер домена будет приниматься во внимание при формировании топологии репликации, выполнении аутентификации пользователей и т. п.
- *Внимание*
- *Перед выполнением операции понижения контроллера домена необходимо убедиться в том, что контроллер не является сервером глобального каталога или исполнителем специализированных ролей. В последнем случае перед понижением контроллера домена администратор должен передать эти роли другим контроллерам. Необходимо, чтобы после понижения контроллера в домене оставался хотя бы один сервер глобального каталога.*

Удаление контроллера домена

- Понижение контроллера, являющегося последним в домене, приводит к удалению домена. Операция удаления домена не может быть осуществлена (соответственно, будет прервана операция понижения последнего контроллера домена), если домен имеет дочерние домены. Запрещается также понижать контроллеры домена, являющиеся последними носителями реплик разделов приложений. Перед выполнением операции понижения администратор должен вручную удалить разделы приложений с помощью утилиты Ntdsutil.exe.
- Для выполнения операции понижения необходимо, чтобы контроллер домена был работоспособным. Также должны быть доступны другие контроллеры домена. Это позволит выполнить изменения в каталоге, информирующие об удалении контроллера домена. Операция понижения контроллера домена выполняется мастером установки Active Directory (утилита Dcpromo).
- В процессе понижения роли компьютера мастер установки проверит копию каталога понижаемого контроллера домена на предмет наличия реплик разделов приложений. Если будут обнаружены реплики, являющиеся последними, мастер выдаст соответствующее предупреждение (рис. 7-51.7). В этом случае мастер в следующем окне потребует подтвердить готовность администратора удалить эту реплику.

Удаление контроллера домена

- *Внимание*
- *Удаление последней реплики раздела приложения приводит к потере всех хранящихся в ней данных. Как следствие это может привести к отказу или неверной работе приложений.*

На заключительном этапе администратор должен будет предоставить информацию о пароле, который будет сопоставлен учетной записи локального администратора.

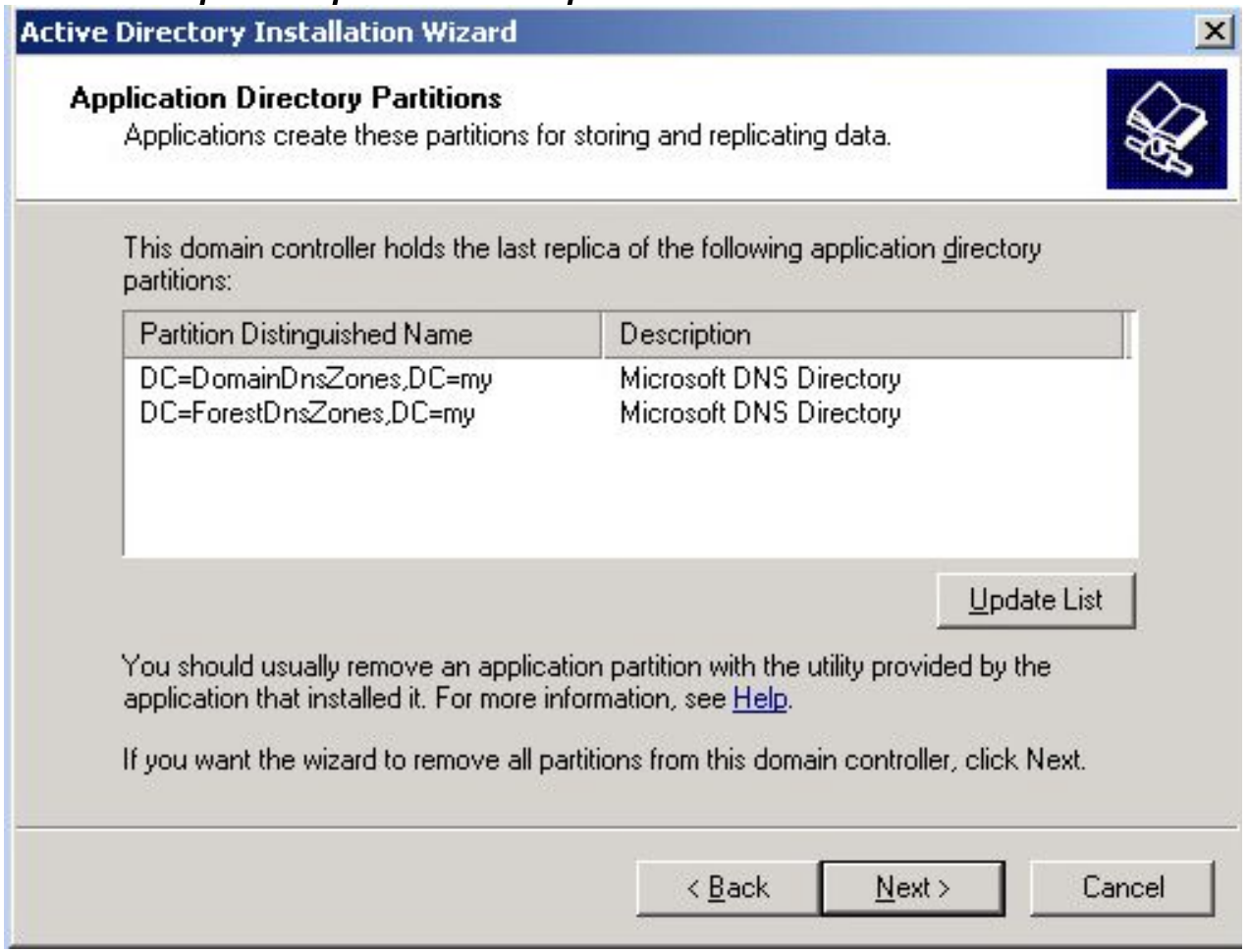


Рис. 7-51.7. На понижаемом контроллере домена обнаружены последние реплики разделов приложений

Управление доверительными отношениями

- На прошлой лекции говорилось о доверительных отношениях между доменами, как о связующем звене, посредством которого домены организуются в иерархию. Для управления доверительными отношениями используется оснастка Active Directory Domain and Trusts (Active Directory — домены и доверия).
- *Также можно использовать утилиту командной строки Netdom.exe для управления доверительными отношениями.*

Создание доверительных отношений

- Для создания доверительных отношений запустите оснастку Active Directory Domain and Trusts и откройте окно свойств объекта, ассоциированного с нужным доменом. Перейдите на вкладку Trusts (рис. 7-51.8). В поле Domains trusted by this domain отображаются домены, которым доверяет конфигурируемый домен (исходящие доверительные отношения), а в поле Domains that trust this domain — домены, доверяющие конфигурируемому домену (входящие доверительные отношения). Для каждого значения отображается информация о типе доверительных отношений и транзитивности.

Управление доверительными отношениями

- ***Применительно к типу доверительных отношений возможны следующие значения:***

- **Forest** — доверительные отношения, установленные между лесами доменов;
- **Tree Root** — доверительные отношения, установленные между деревьями доменов в рамках одного леса доменов;
- **Child** — доверительные отношения, установленные в рамках дерева доменов между дочерним и родительским доменами;
- **External** — доверительные отношения, установленные с внешним доменом любого типа;
- **Shortcut** — перекрестные доверительные отношения, установленные между отдельными доменами леса;
- **Realm** — доверительные отношения, установленные между областями Kerberos.

- Доверительные отношения между лесами доменов могут быть установлены только в том случае, если оба леса находятся на

Управление доверительными отношениями

- Процесс создания доверительных отношений зависит от того, какой именно тип отношений администратор хочет создать. Например, если администратор хочет создать отношения полного доверия с внешним доменом, он должен создать пару встречных односторонних доверительных отношений.
- Для установки доверительных отношений необходимо щелкнуть по кнопке New Trust (Новые доверительные отношения), что приведет к запуску мастера New Trust Wizard. В ходе работы мастера администратор должен будет предоставить мастеру информацию об имени домена, с которым устанавливаются доверительные отношения. Если домен с указанным именем не обнаружен, мастер предполагает, что подразумевается имя области Kerberos.
- *Внимание*
- *В пределах леса отношения доверия между родительским и дочерним доменами, а также между деревьями леса доменов не могут быть созданы администраторами вручную. Эти отношения создаются мастером установки Active Directory в ходе создания нового домена.*

Управление доверительными отношениями

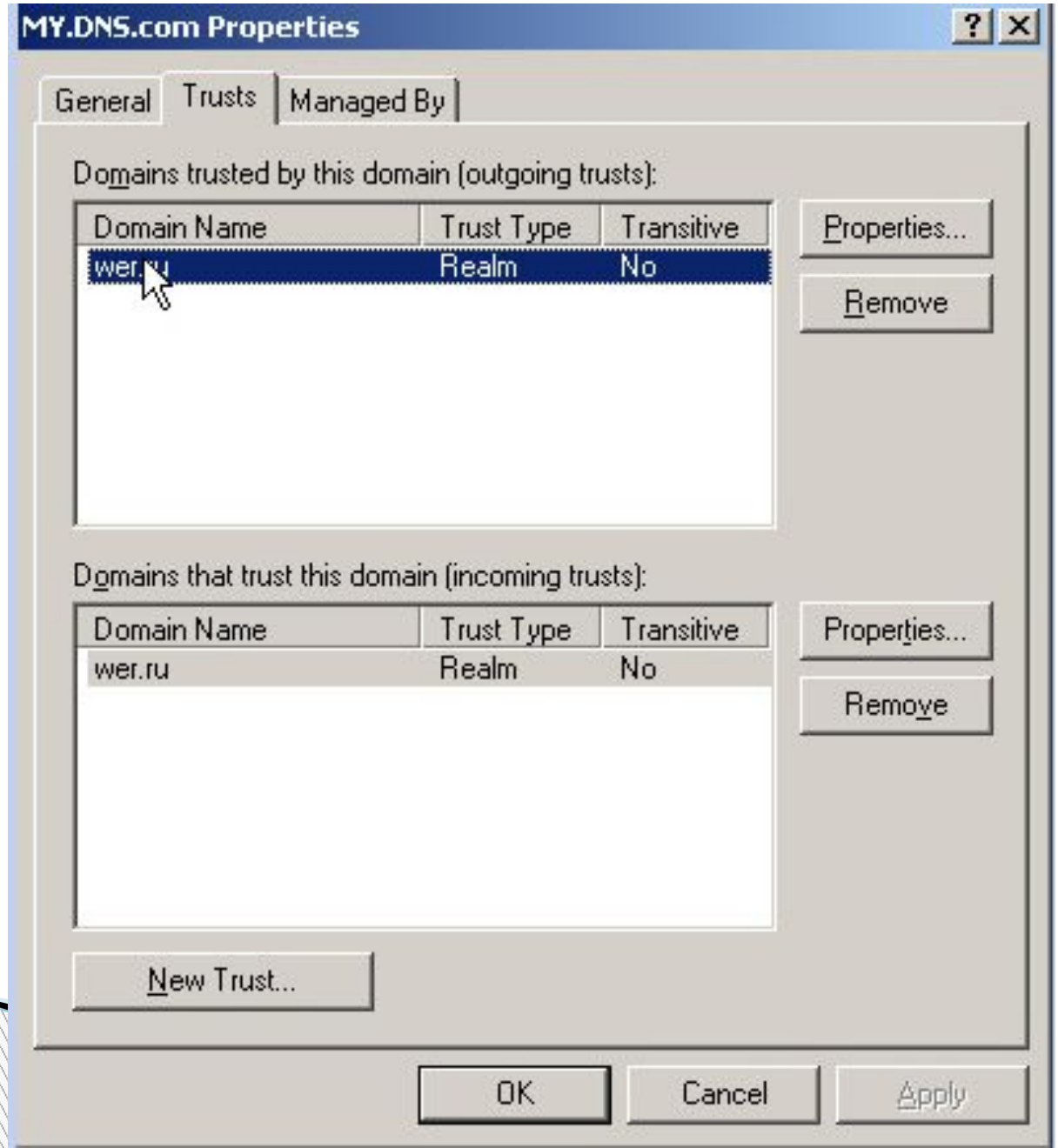


Рис. 19.8. Вкладка Trusts окна свойств домена

Управление доверительными отношениями

Удаление доверительных отношений

- Для удаления доверительных отношений необходимо выбрать в списке требуемую запись и нажать кнопку Remove (Удалить). Если отношения двусторонние, администратор может при желании удалить отношения доверия направленные как в одну сторону, так и в другую. Может быть удалено только одно из направлений двусторонних отношений доверия.
- *Внимание*
- *Необходимо помнить, что не могут быть удалены отношения доверия между корневыми деревьями домена, а также отношения между родительским и дочерним доменами.*
- Для получения информации о состоянии доверительных отношений администратор может использовать утилиту командной строки NLtest.exe. Ниже приводится результат проверки состояния доверительных отношений между текущим доменом и доменом khsu.khakasnet.ru:
- C:\>nltest /sc_query:khsu.khakasnet.ru
- Flags: 30 HAS_IP HAS_TIMESERV
- Trusted DC Name\\main.khsu.khakasnet.ru Trusted DC Connection Status Status = 0 0x0 NERR_Success
- The command completed successfully

Управление доверительными отношениями

Управление доверительными отношениями между лесами доменов

- Если два леса доменов находятся на функциональном уровне Windows Server 2003, они могут быть соединены друг с другом посредством транзитивных доверительных отношений. Если хотя бы один из лесов доменов находится на функциональном уровне Windows 2000, леса доменов могут быть соединены только посредством внешних доверительных отношений (external trusts), которые не обладают свойством транзитивности.
- *Внимание*
- *Перед выполнением процедуры создания доверительных отношений между лесами доменов необходимо убедиться, что DNS-сервер способен разрешить доменные имена корневых доменов обоих лесов*.
- Запустите мастер создания доверительных отношений для корневого домена леса. В ответ на просьбу указать имя домена на противоположном конце доверительных отношений, укажите имя корневого домена другого леса. Мастер предложит выбрать способ соединения двух лесов: либо посредством транзитивных доверительных отношений между лесами (forest trust), либо посредством нетранзитивных внешних доверительных отношений (external trust).

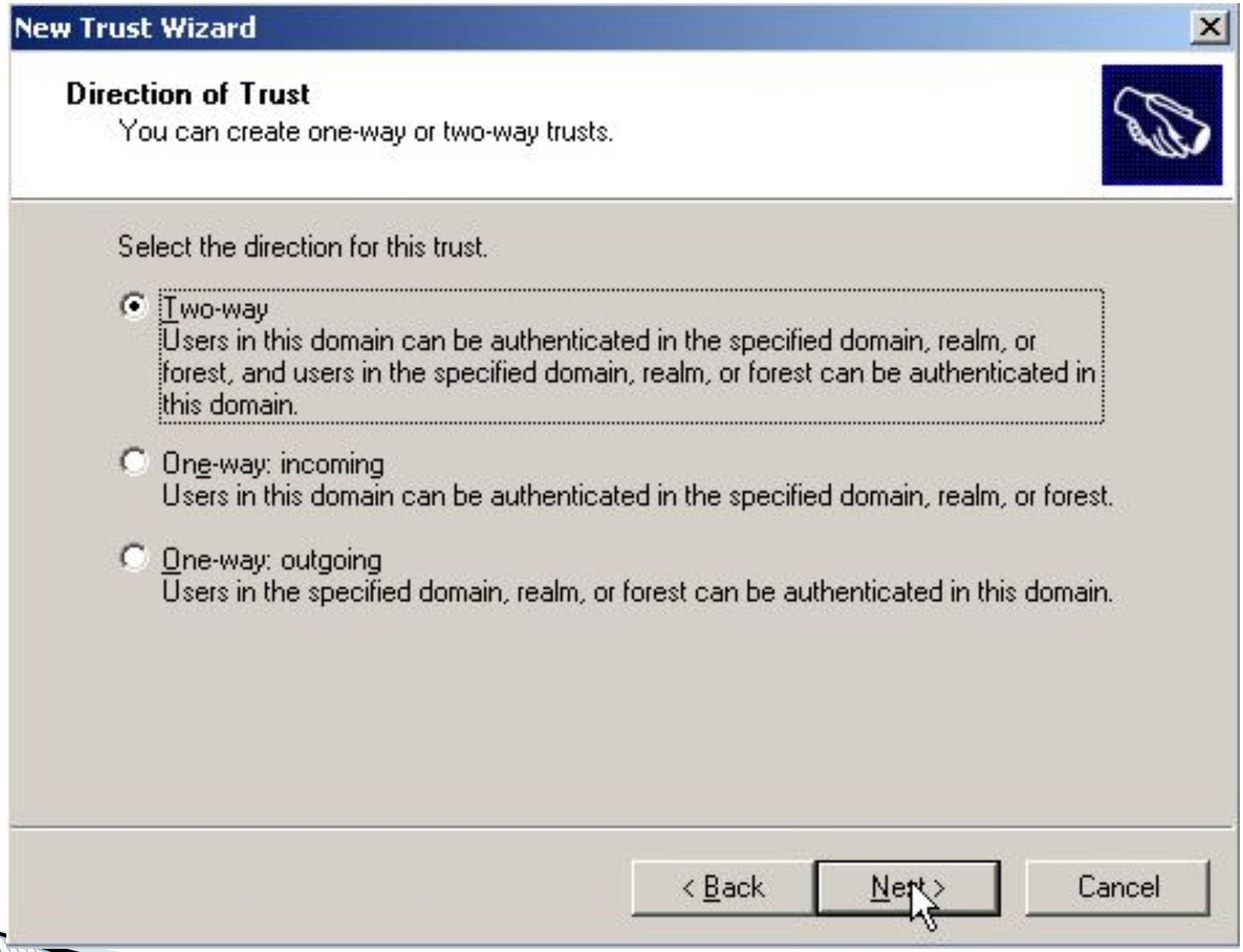
Управление доверительными отношениями

- На двух последующих страницах мастер попросит предоставить информацию о направлении доверительных отношений (односторонние или двусторонние), а также сведения об учетной записи, в контексте которой создается отношение доверия. Далее администратор должен определить, какая часть ресурсов леса доменов будет доступна аутентифицированным пользователям из другого леса доменов. Имеются два варианта (переключателя на странице мастера):
- Allow authentication for all resources in the local forest. В этом случае пользователи одного леса могут получить доступ к любым ресурсам в рамках другого леса доменов. Данный режим можно использовать в ситуации, когда оба леса доменов принадлежат одной организации;
- Allow authentication only for selected resources in the local forest. Администратор вручную указывает ресурсы в рамках леса доменов, которые будут доступны пользователям из другого леса. Этот способ разграничения доступа подходит для сценариев, когда леса доменов принадлежат различным организациям, не желающим предоставлять доступ ко всем ресурсам.

Управление доверительными отношениями

- Область доступности ресурсов может быть изменена администратором уже после того, как доверительные отношения созданы. Для этого необходимо открыть окно свойств доверительных отношений и перейти на вкладку Authentication.
- На заключительном этапе администратор должен сконфигурировать механизм маршрутизации суффиксов (name suffix routing). По умолчанию, если не обнаружены конфликты в доменных именах, мастер предлагает активизировать механизм маршрутизации суффиксов для всех доменов, входящих в оба леса (рис. 7-51.9). Администратор может снять флажки напротив имени определенного леса, чтобы предотвратить возможность доступа пользователей в указанный домен.
- Впоследствии администратор может произвести дополнительное конфигурирование механизма маршрутизации суффиксов. В окне свойств объекта, ассоциированного с доверительными отношениями между лесами доменов, имеется вкладка Name Suffix Routing, на которой перечислены все параметры. Администратор может отключить (disable) или, наоборот, включить маршрутизацию некоторого суффикса, а также исключить (exclude) некоторый домен из маршрутизации.

Управление доверительными отношениями



- Рис. 7-51 9. Конфигурирование механизма маршрутизации суффиксов

Изменение функционального уровня домена и леса доменов

- Функциональный уровень, на котором находится домен или лес доменов, определяет перечень возможностей, доступных в рамках домена или леса доменов. Чем выше функциональный уровень, тем шире диапазон возможностей. Механизм функциональных уровней был введен компанией Microsoft с целью сохранения совместимости с предыдущими версиями серверных операционных систем (Windows NT/ 2000. Организация перехода на Windows Server 2003 требует от компаний значительных финансовых и временных затрат, поэтому для многих из них предпочтительным вариантом является постепенный переход на новую платформу. Этот подход характеризуется одновременным сосуществованием в сети нескольких поколений операционных систем.
  Перевод домена на новый функциональный уровень возможен только в ситуации, когда отказываются от использования одного из поколений операционных систем в качестве контр. домена. Отказ от контроллеров домена под управлением Windows NT позволяет перевести домен на функциональный уровень Windows 2000 native. Соответственно, отказ от использования контроллеров домена Windows 2000 позволяет перевести домен на функциональный уровень Windows Server 2003.

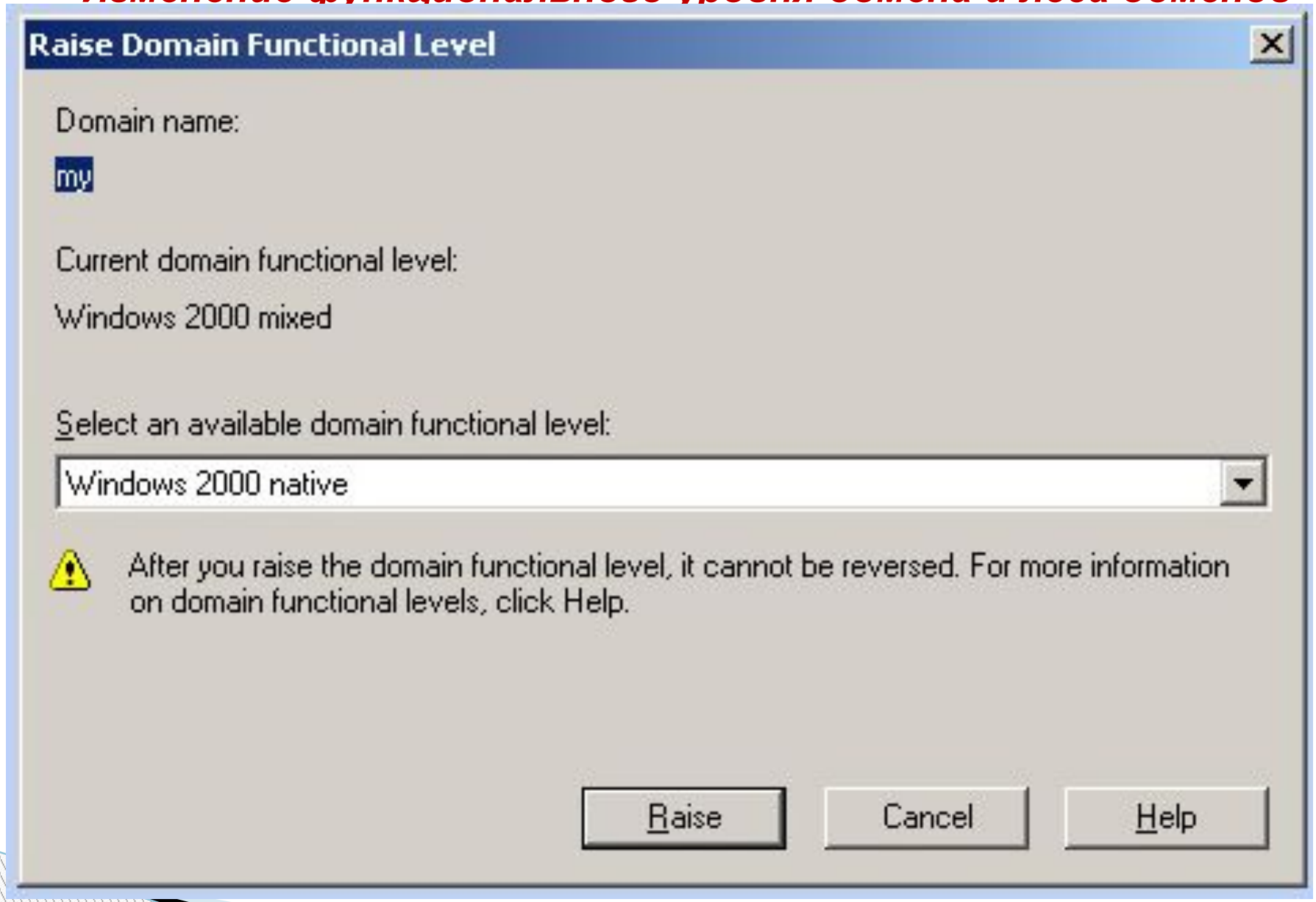
Изменение функционального уровня домена и леса доменов

- Только после того как все домены переведены на функциональный уровень Windows Server 2003, администратор может перевести лес доменов на функциональный уровень Windows Server 2003. На этом этапе становится доступен весь спектр возможностей Windows Server 2003. Для изменения функционального уровня могут использоваться две оснастки: **Active Directory Users and Computers** и **Active Directory Domain and Trusts**. Для изменения функционального уровня домена в контекстном меню объекта, ассоциированного с нужным доменом, выберите пункт **Raise (Поднять) Domain Functional Level**. В открывшемся окне (рис. 19.10) под строкой **Current domain functional level** отображается текущий функциональный уровень домена. Для его изменения выберите из раскрывающегося списка необходимый функциональный уровень и нажмите кнопку **Raise (Поднять)**. После изменения функционального уровня домена необходимо некоторое время, чтобы сведения об изменении реплицировались на все контроллеры в домене. *Изменение функционального уровня является необратимой операцией. Это означает, что возвращение домена на прежний функциональный уровень невозможно.*

Изменение функционального уровня домена и леса доменов

- Изменение функционального уровня леса доменов выполняется аналогичным образом. Вызвав контекстное меню объекта, находящегося в корне пространства имен оснастки **Active Directory Domain and Trusts**, необходимо выбрать в нем пункт **Raise Forest Functional Level**. Если возможность переведения леса доменов на новый функциональный уровень отсутствует, в открывшемся окне будет выведено соответствующее предупреждение, говорящее о том, что один из доменов, входящих в лес, еще не был переведен на функциональный уровень Windows Server 2003.
  Если все требования для изменения функционального уровня леса доменов соблюдены, необходимо нажать кнопку Raise. После того как сведения о произведенном изменении будут реплицированы на все контроллеры домена леса, администратор может использовать новые функциональные возможности

Изменение функционального уровня домена и леса доменов



- Изменение функционального уровня домена