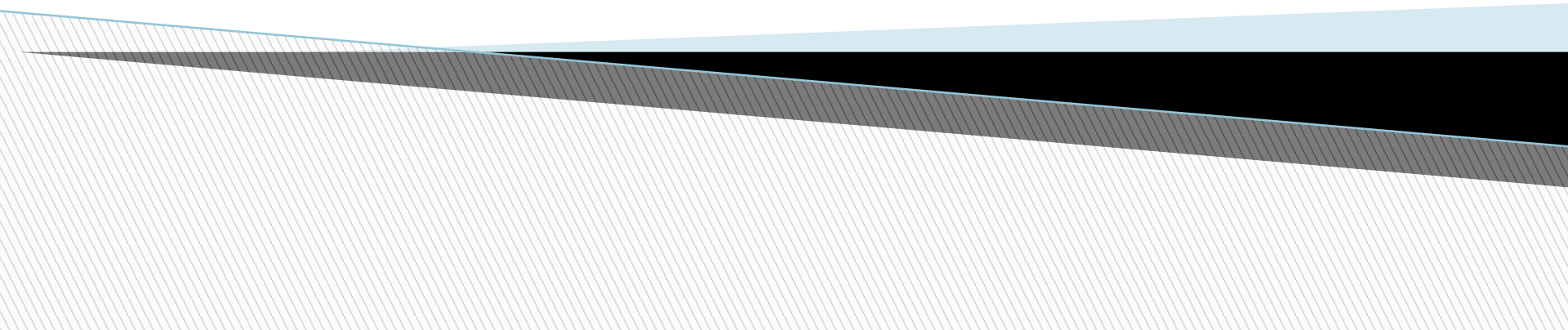


Аппаратное и программное обеспечение ЭВМ и сетей

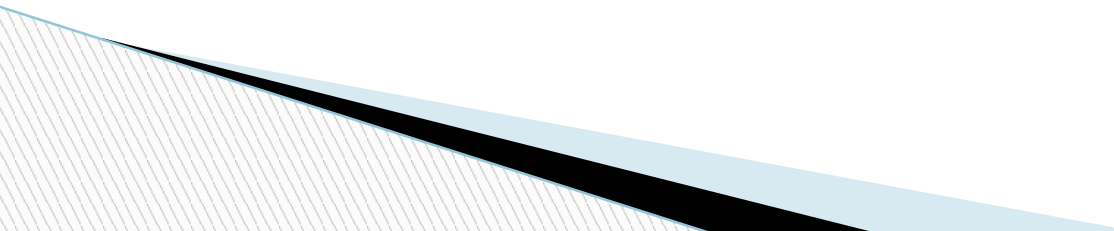
Раздел 7 Сетевые операционные системы

Тема № 43. Проектирование доменов и развертывание **Active Directory**



- Служба каталога Active Directory позволяет структурировать, организовать управление и доступ к объектам и ресурсам сервера и сети на трех уровнях:

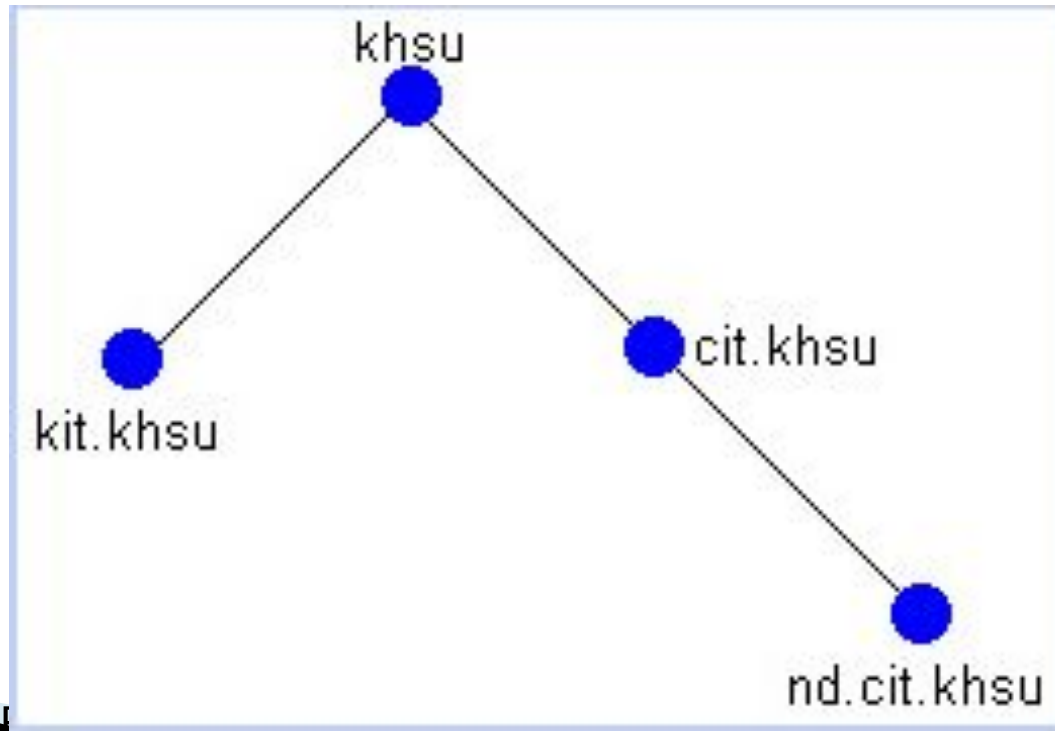
 - Уровни формирования структуры каталогов:
 - доменная структура каталога (создание структуры доменов);
 - логическая структура каталога (создание подразделений);
 - физическая структура каталога (создание подсетей и сайтов).

 - Сценарии формирования пространства имен DNS:
 - изолированное пространство имен DNS;
 - пространство имен DNS, интегрированное с внешним пространством имен:
 - пространство имен DNS, являющееся фрагментом другого более глобального пространства имен.
- 

Сценарии формирования пространства имен DNS

Изолированное корпоративное пространство имен.

- Корпоративное пространство имен DNS полностью изолировано от других пространств имен, являющихся внешними по отношению к компании.
- Для реализации необходимо, чтобы DNS-сервер, стоящий на вершине корпоративного пространства имен DNS, являлся корневым сервером и не был сконфигурирован для переадресации запросов на другой DNS-сервер (вкладка ***Пересылка*** (Forwarders) окна свойств этого сервера должна быть пустой).



Сценарии формирования пространства имен DNS

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.
- 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 (режим выборочного перенаправления конфигурируется на вкладке **Перенаправление (*Forwarders*)** окна свойств корневого сервера).

Сценарии формирования пространства имен DNS

- Для внутренних доменов режим перенаправления на корневом сервере должен быть отключен.

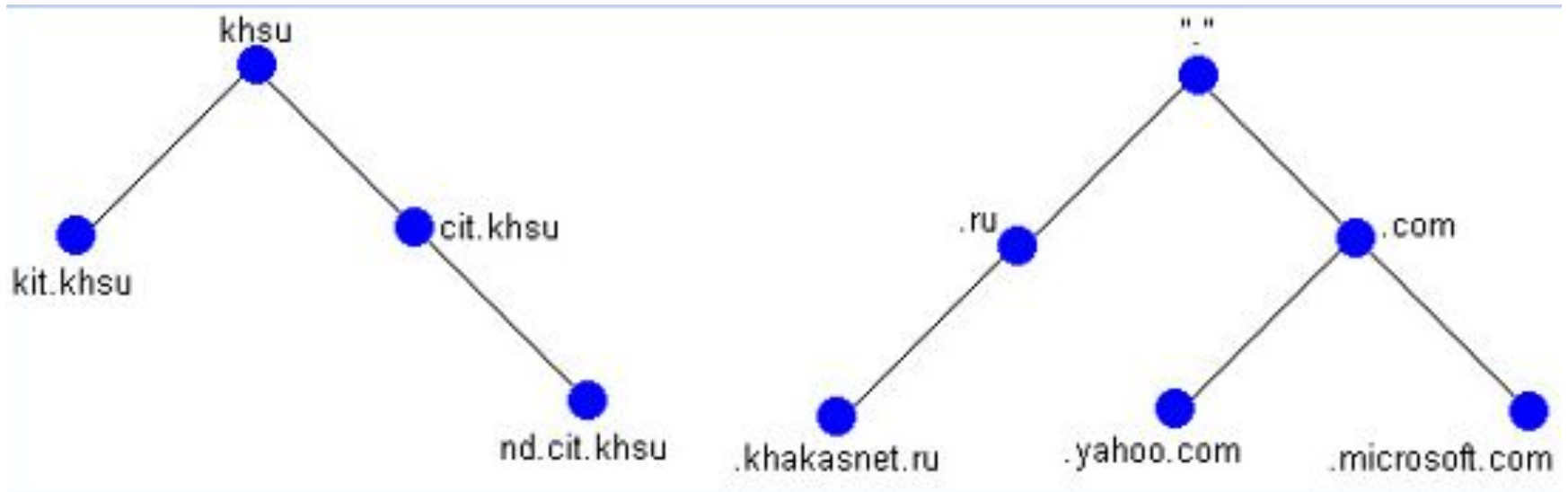


Рис. 7-43.2. Корпоративное пространство имен и пространство имен Интернета

Сценарии формирования пространства имен DNS

Корпоративное пространство имен, являющееся частью внешнего пространства имен.

- В этом случае все корпоративные доменные имена, а также адреса хостов являются реальными адресами и именами Интернета.
- Преимущество — ресурсы сети доступны из любой точки мира. При этом администратор может отделить внутреннюю сеть от внешней межсетевым экраном и использовать системы сертификации и аутентификации.
- Для интеграции необходимо сконфигурировать корпоративный корневой DNS-сервер для перенаправления всех запросов на внешний DNS-сервер.

Сценарии формирования пространства имен DNS

Функциональные уровни

- ▣ В Windows Server 2012 доступны следующие функциональные уровни домена:
 - ▣ · Windows Server 2003
 - ▣ · Windows Server 2008
 - ▣ · Windows Server 2008 R2
 - ▣ · Windows Server 2012

Если вы устанавливаете контроллер домена, то можете выбрать любой функциональный уровень домена вплоть до Windows Server 2012. Учтите, что если вы выберете функциональный уровень домена Windows Server 2012, то не сможете добавлять контроллеры домена, отличные от Windows Server 2012. Таким образом, если вы присоедините контроллер домена Windows Server 2012 к функциональному уровню домена Windows Server 2008 R2, то не сможете поднять функциональный уровень до Windows Server 2012 при наличии контроллера домена Windows Server 2008 R2.

Сценарии формирования пространства имен DNS

Функциональный уровень домена Windows Server 2003

- Можно переименовывать контроллеры доменов с помощью Netdorn.exe
- Добавлен атрибут lastLogonTimestamp.
- Имеется возможность переадресации контейнеров Users (Пользователи) и Computers (Компьютеры).
- Поддерживается избирательная аутентификация для указания, кто имеет доступ к тем или иным ресурсам в доверенном лесе.
- Имеется ограниченное делегирование с целью защиты учетных данных делегированного пользователя с применением Kerberos.

Функциональный уровень домена Windows Server 2008

- Предоставляется поддержка DFS-R для папки SYSVOL.
- Доступна поддержка алгоритмов шифрования AES 128 и AES 256 для Kerberos.
- Предоставляется детальная информация о последнем интерактивном входе в систему.
- Используются детализированные политики паролей.

Функциональный уровень домена Windows Server 2008 R2

- Обеспечение механизма аутентификации определяет метод входа в систему, применяемый пользователем. Это хранится в маркере Kerberos.
- Автоматическое управление SPN доступно для учетных записей управляемых служб (Managed Service Accounts).

Функциональный уровень домена Windows Server 2012

- Поддержка КОС доступна для утверждений, комплексной аутентификации и защиты Kerberos через две настройки: Always provide claims (Всегда предоставлять утверждения) и Fail unarmored authentication requests (Отклонять незащищенные запросы на аутентификацию).

Сценарии формирования пространства имен DNS

Функциональный уровень леса доменов

Windows Server 2003. Функциональный уровень леса Windows Server 2003 под держивает следующие средства.

- Возможность создания доверительных отношений в лесе.
- Возможность переименования домена.
- Возможность развертывания контроллера домена только для чтения (RODC).
- Усовершенствованное средство проверки целостности знаний (Knowledge Consistency Checker - KCC).
- Усовершенствованная репликация связанных значений (linked-value replication), при которой реплицируются только различия членства в группах.
- Перечисление на основе доступа в пространстве имен DFS.

Windows Server 2008. Функциональный уровень леса Windows Server 2008 не предлагает каких-то дополнительных возможностей.

Windows Server 2008 R2. Корзина Active Directory (Active Directory Recycle Bin) позволяет восстанавливать удаленные объекты без необходимости в перезапуске контроллера домена в режиме восстановления Active Directory. Вы должны включить поддержку Active Directory Recycle Bin с использованием командлетов PowerShell. Корзина Active Directory - это великолепное средство, которое было улучшено в Windows Server 2012. Теперь корзину намного проще настраивать и управлять ею, как будет показано далее в этой книге.

Windows Server 2012. Функциональный уровень леса Windows Server 2012 не предлагает каких-то дополнительных возможностей.

Установка контроллеров домена

Подготовка к установке контроллера домена

1. Администратор должен убедиться, что компьютер, выбранный на роль контроллера домена отвечает минимальным аппаратным и программным требованиям.
2. Необходимо убедиться в работоспособности службы DNS.
3. Должен быть установлен стек протоколов TCP/IP и для каждого из интерфейсов сервера выделен статический IP-адрес.
4. Для сервера должен быть установлен DNS-суффикс, соответствующий имени домена, для которого будет устанавливаться контроллер домена.
5. Служба каталога должна быть установлена на раздел диска с файловой системой NTFS.
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.

Установка контроллеров домена Требования и ограничения

Полномочия системного администратора:

- При установке 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

- Администратор должен проверить настройки стека протоколов TCP/IP. Одним из важнейших параметров является адрес «**Предпочитаемого DNS-сервера**» (preferred DNS server), который будет использоваться мастером установки для диагностики пространства имен DNS и для регистрации доменного имени сервера.
- 1. Необходимо предоставить возможность мастеру установки Active Directory установить на сервере службу DNS и произвести ее последующее конфигурирование. Параметр Preferred DNS Server (Предпочитаемый DNS-сервер) должен указывать на сам сервер. Все последующие контроллеры домена должны указывать уже на существующий DNS-сервер.
- 2. Необходимо убедиться, 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 с помощью утилиты DCdiag.exe:

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

Установка контроллеров домена

Обновление существующего леса доменов **Windows 2000**

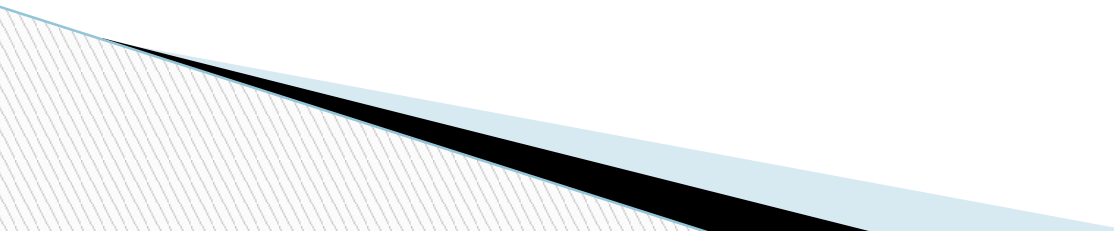
- Для процедуры "подготовки" службы каталога Windows 2012 к установке контроллеров домена используется утилита командной строки Adprep.exe.

Установка контроллера домена **Windows Server 2012**

- 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.

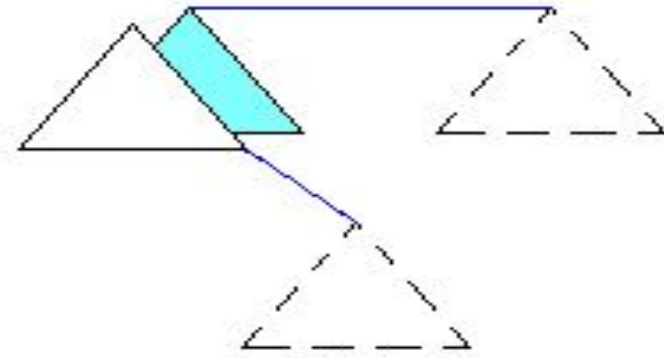
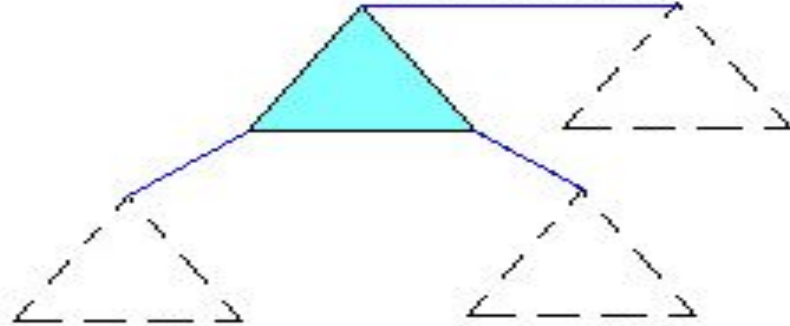
Выполнение установки

□ При использования мастера установки Active Directory возможны четыре сценария (рис. 7-43.3):

- 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

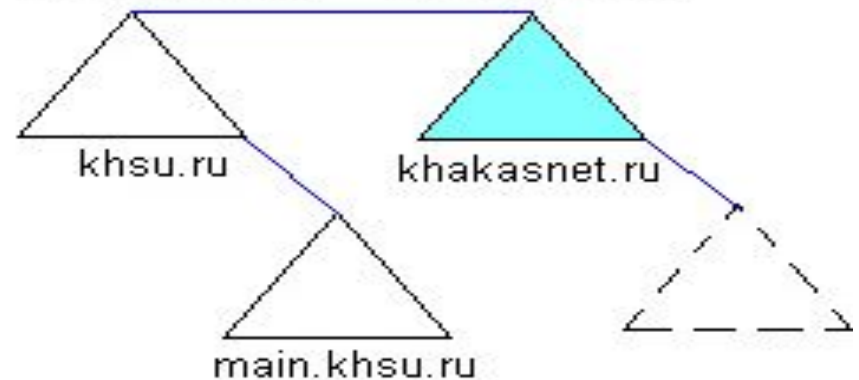
Новый лес
(1-й домен в лесу)
корень леса
корень дерева



Дочерний домен
корень леса
корень дерева



Новое дерево доменов
корень леса
корень дерева корень дерева






-  - новый домен
-  - существующий домен
-  - будущие домены

Рис. 7-43.3. Сценарии создания контроллера домена

Установка контроллеров домена

- Администратор осуществляет выбор сценария на первых страницах мастера.
- Независимо от избранного сценария мастер предложит выбрать место расположения файлов хранилища (БД), журналов и системного тома SYSVOL.
- На следующем этапе мастер обратится с запросом к службе DNS. Если предпочитаемый DNS-сервер не содержит зоны для создаваемого домена Active Directory, 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).
- 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).
- 3. Проблема будет решена позже ручной настройкой DNS (расширенная)** (I will correct the problem later by configuring DNS manually (Advanced))..

Установка контроллеров домена

- Если процесс тестирования структуры DNS закончился успешно, мастер выдаст соответствующую информацию.
- На заключительном этапе работы мастера администратору необходимо будет определить уровень совместимости разрешений с подсистемой безопасности Windows NT.
- По окончании установки контроллера домена потребуется перезагрузить систему.
- Если установленный контроллер домена является первым в лесу, то учетная запись локального администратора преобразуется в учетную запись Administrator (Администратор созданного домена).

Установка контроллеров домена

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

Установка контроллеров домена

Установка контроллера домена из резервной копии

- Данная возможность распространяется **только на установку дополнительных доменов**.
- Установка контроллера домена из резервной копии позволяет избежать копирования всего содержимого каталога через сеть.
- *Однако полностью исключить взаимодействие через сеть с уже существующими контроллерами домена нельзя.*
- 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.
- Для установки контроллера домена из резервной копии часто используют утилиту Backup.
- 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. Мастер предложит указать способ наполнения каталога на создаваемом контроллере:
 - **наполнение через сеть;**
 - **наполнение из резервной копии.**

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 2012 действительно являются контроллерами домена.

□ Способы проверки:

- 1. В Microsoft рекомендуют применять команду net share для проверки того, что папка SYSVOL совместно используется всеми контроллерами домена, и что эта открытая папка отображается на папку SYSVOL, реплицируемую службой FRS.
- 2. Вы должны удостовериться в наличии достаточного объема свободного пространства на диске, чтобы можно было создать копию структуры папки SYSVOL.
- 3. Используйте инструмент Ultrasound для мониторинга службы FRS и проверки ее функциональности.
- 4. На одном из контроллеров домена откройте окно командной строки и введите `repadmin /replsum`. Эта команда позволит удостовериться в корректной работе репликации Active Directory.

Установка контроллеров домена

- 5. Откройте окно командной строки и введите DCDIAG. Эта утилита выполнит несколько проверок в системе. Вывод не должен содержать сообщения об ошибках. Если это не так, устраните проблемы, прежде чем продолжить.
- 6. В редакторе реестра на каждом контроллере домена перейдите в раздел HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters и удостоверьтесь в том, что значением параметра SYSVOL является диск : \windows folder\SYSVOL \SYSVOL, а значением параметра SYSVOLReady - число 1.
- 7. На каждом контроллере домена с помощью окна служб удостоверьтесь, что служба DFS Replication запущена, а тип ее запуска установлен в Automatic (Автоматически).

Изменение имени контроллера домена

- Изменение имени контроллера домена возможно только в домене, находящемся на функциональном уровне *Windows Server 2012*.
- 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:

netdom computername <текущее_имя> /add:<новое_имя>

- В результате новое имя контроллера домена будет зарегистрировано в базе данных службы DNS в качестве альтернативного. Необходимо подождать пока информация о новом имени не будет реплицирована на все носители зоны. После этого альтернативное имя надо сделать основным:

netdom computer-name <текущее_имя> /MakePrimary: <новое_имя>

- 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>

Удаление контроллера домена

- Под удалением контроллера домена фактически понимается понижение его до роли обычного сервера.
- *Перед выполнением операции понижения контроллера домена необходимо убедиться, что контроллер не является сервером глобального каталога или исполнителем специализированных ролей.*
- Понижение контроллера, являющегося последним в домене, приводит к удалению домена. Операция удаления домена не может быть осуществлена, если домен имеет дочерние домены. Перед понижением администратор должен вручную удалить разделы приложений с помощью утилиты Ntdsutil.exe.
- Операция понижения контроллера домена выполняется мастером установки Active Directory (утилита Dcpromo).

Управление доверительными отношениями

- Для управления доверительными отношениями используется оснастка Active Directory Domain and Trusts (Active Directory — домены и доверия).
- Также можно использовать утилиту командной строки *Netdom.exe*.

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.
- Для установки доверительных отношений необходимо щелкнуть по кнопке New Trust (Новые доверительные отношения), что приведет к запуску мастера New Trust Wizard.

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.

Управление доверительными отношениями

Удаление доверительных отношений

- Для удаления доверительных отношений необходимо выбрать в списке требуемую запись и нажать кнопку Remove (Удалить).
- *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 используется утилита командной строки NLtest.exe:
- **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

- ▣ Запустите мастер создания доверительных отношений для корневого домена леса. 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).
- ▣ На двух последующих страницах мастер попросит предоставить информацию о направлении доверительных отношений, сведения об учетной записи, в контексте которой создается отношение доверия. Далее администратор должен определить, какая часть ресурсов будет доступна аутентифицированным пользователям из другого леса доменов:
 - ▣ Allow authentication for all resources in the local forest (доступ к любым ресурсам в рамках другого леса доменов);
 - ▣ 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).
- ▣ На заключительном этапе администратор должен сконфигурировать механизм маршрутизации суффиксов (name suffix routing).

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.
- Для изменения функционального уровня могут использоваться две оснастки: **Active Directory Users and Computers** и **Active Directory Domain and Trusts**. В контекстном меню объекта выберите пункт **Raise (Поднять) Domain Functional Level**. Выберите из раскрывающегося списка необходимый функциональный уровень и нажмите кнопку **Raise (Поднять)**.
- *Изменение функционального уровня является необратимой операцией. Это означает, что возвращение домена на прежний функциональный уровень невозможно.*
- Изменение функционального уровня леса доменов выполняется аналогичным образом.


Изменение функционального уровня домена и леса доменов

Raise domain functional level ✕

Domain name:
my

Current domain functional level:
Windows Server 2008 R2

Select an available domain functional level:
Windows Server 2012 R2 ▾

 After you raise the domain functional level, it is possible that you may not be able to reverse it. For more information on domain functional levels, click Help.

▣ Изменение функционального уровня домена