Лекция №8. ПРОЕКТИРОВАНИЕ СТРУКТУРЫ ACTIVE DIRECTORY

Учебные вопросы:

1. Структура доменов ADDS
2. Модели доменов
3. Понятие организационных единиц и групп

Вопрос №1. Структура доменов ADDS

Доверительные отношения между доменами

Доверительные отношения между доменами различных лесов **раньше требовали явного определения** для каждого домена. Это приводило к экспоненциальному накоплению доверительных отношений и сложности управления ими.

В Windows Server 2003 и более поздних версиях возможности доверительных отношений были расширены транзитивными доверительными отношениями **с автоматическим созданием путей "вверх и вниз по дереву".**

Такие доверительные отношения, гораздо более понятные и удобные для устранения неполадок, значительно улучшили управляемость сетей Windows.

Транзитивные отношения доверия

Двунаправленные транзитивные отношения доверия устанавливаются автоматически при создании **поддоменов** или добавлении в лес AD DS **нового дерева** доменов.

Транзитивные отношения обычно являются **двунаправленными**, когда каждый домен доверяет другим доменам. То есть пользователи каждого домена имеют доступ к ресурсам, например, принтерам или серверам, в другом домене, если им **явно предоставлены** права в этом домене.

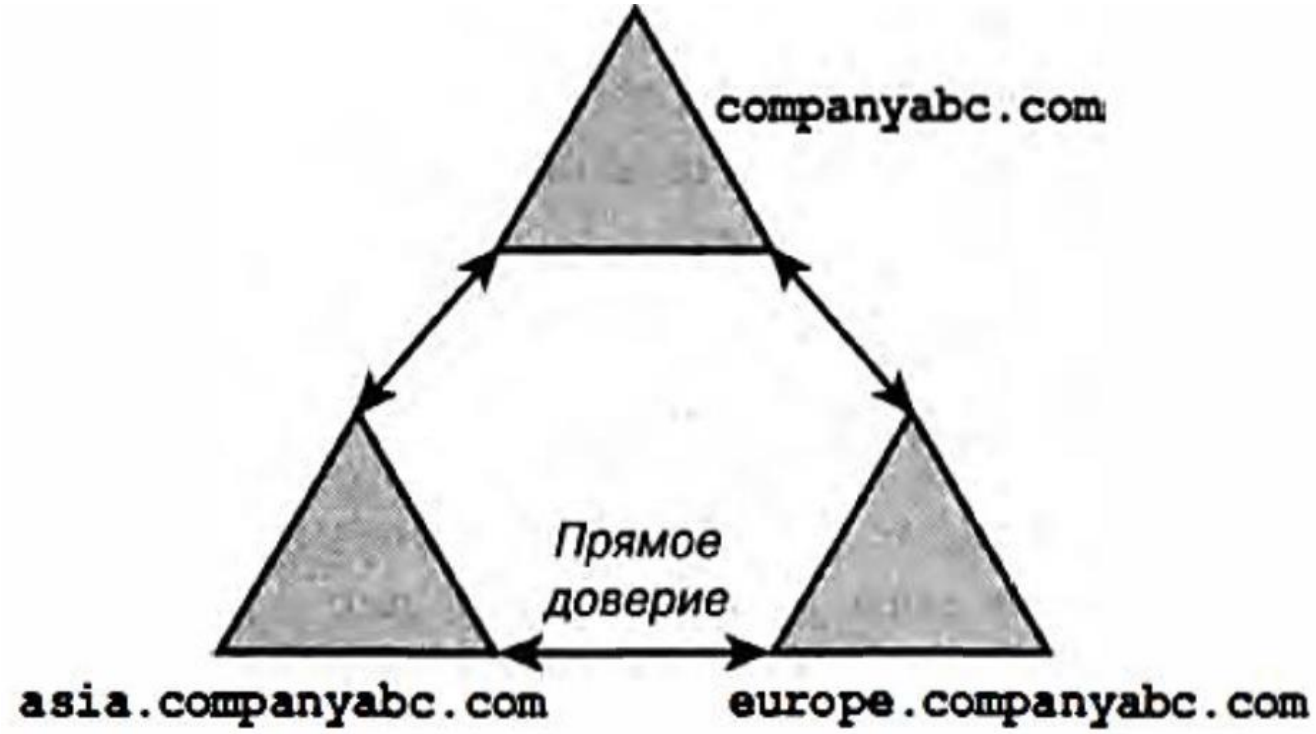
Явные отношения доверия

Явные отношениями доверия называются такие отношения, которые устанавливаются **вручную** - подобно тому, как это делалось в Windows NT. Такие отношения могут устанавливаться, например, для объединения **двух несвязанных** деревьев доменов в один лес.

Явные отношения доверия являются **однонаправленными**, но из двух таких отношений можно составить двунаправленное.

Явные отношения доверия

Когда явное доверие устанавливается для **направления потока** доверительных отношений от одного поддомена к другому, оно называется **прямым доверием**. Прямые доверия просто **ускоряют аутентификацию**, устраняя необходимость в перемещениях по дереву вверх и вниз.



Явные отношения доверия

Еще одним возможным способом применения явных отношений доверия является **обеспечение связности** между лесом ADDS и внешним доменом. Подобные типы явно определенных отношений называются **внешними отношениями** доверия и позволяют различным лесам совместно использовать информацию без фактического объединения данных схемы или глобальных каталогов.

Вопрос №2. Модели доменов

При проектировании доменной структуры в ADDS достаточно следовать такому базовому принципу: **начать с** самого **простого** варианта и **расширять** его только **при необходимости** в удовлетворении какого-то конкретного требования.

При проектировании доменов он означает, что всегда нужно начинать с создания **одного домена** и затем добавлять другие, если того **потребуют** сложившиеся в организации условия.

В зависимости от индивидуальных потребностей организаций можно выбирать из множества доступных моделей проектирования. К числу **главных моделей** относятся:

- модель с единственным доменом;
- модель с несколькими доменами;
- модель с несколькими деревьями в одном лесе;
- модель с федеративными лесами;
- модель с выделенным корнем;
- модель с фиктивным доменом;
- модель специализированного домена.

Модель с единственным доменом

Структура домена такого типа обладает главным **преимуществом** по сравнению с другими моделями - **простотой**.

Еще одним преимуществом в случае создания структуры с единственным доменом является **возможность централизованного администрирования**.

Но не все структуры AD DS могут состоять из единственного домена, например, **единая граница безопасности**, образуемая одним доменом, может оказаться **не совсем такой,** какая необходима организации.

Модель с единственным доменом

Для делегирования прав на администрирование элементов безопасности могут использоваться **организационные единицы**, но члены группы Domain Admins (Администраторы домена) **все равно** смогут перекрывать права доступа в разных OU.

Если контуры безопасности внутри организации должны иметь **точные границы**, то единый домен может оказаться **неподходящим** вариантом.

Например, если *отдел кадров* требует, чтобы ни у кого из пользователей *IT-отдела* не было доступа к ресурсам его среды, то структуру домена придется расширить в соответствии с этим дополнительным требованием безопасности.

Модель с несколькими доменами

По различным причинам в организациях может возникать необходимость в добавлении в их среду более одного домена, но при сохранении **функциональных возможностей**, присущих **единственному лесу**. В таких случаях в лес можно добавить один или более доменов.

Модель с несколькими доменами

Причинами возникновения такой необходимости могут быть перечисленные ниже факторы.

- **Децентрализованное администрирование**. Если в различных филиалах в основном применяются собственные структуры информационных технологий, и руководство не планирует объединять их в одну централизованную модель, то идеальным вариантом будет добавление нескольких взаимосвязанных доменов.

Модель с несколькими доменами

Причинами возникновения такой необходимости могут быть перечисленные ниже факторы.

- **Географические ограничения.** Если различные филиалы компании соединяются очень медленными или ненадежными каналами связи или если они находятся на больших расстояниях друг от друга.

Такой подход позволит ограничить объем репликации между доменами, а также упростить сопровождение в рабочее время для офисов, находящихся в удаленных часовых поясах

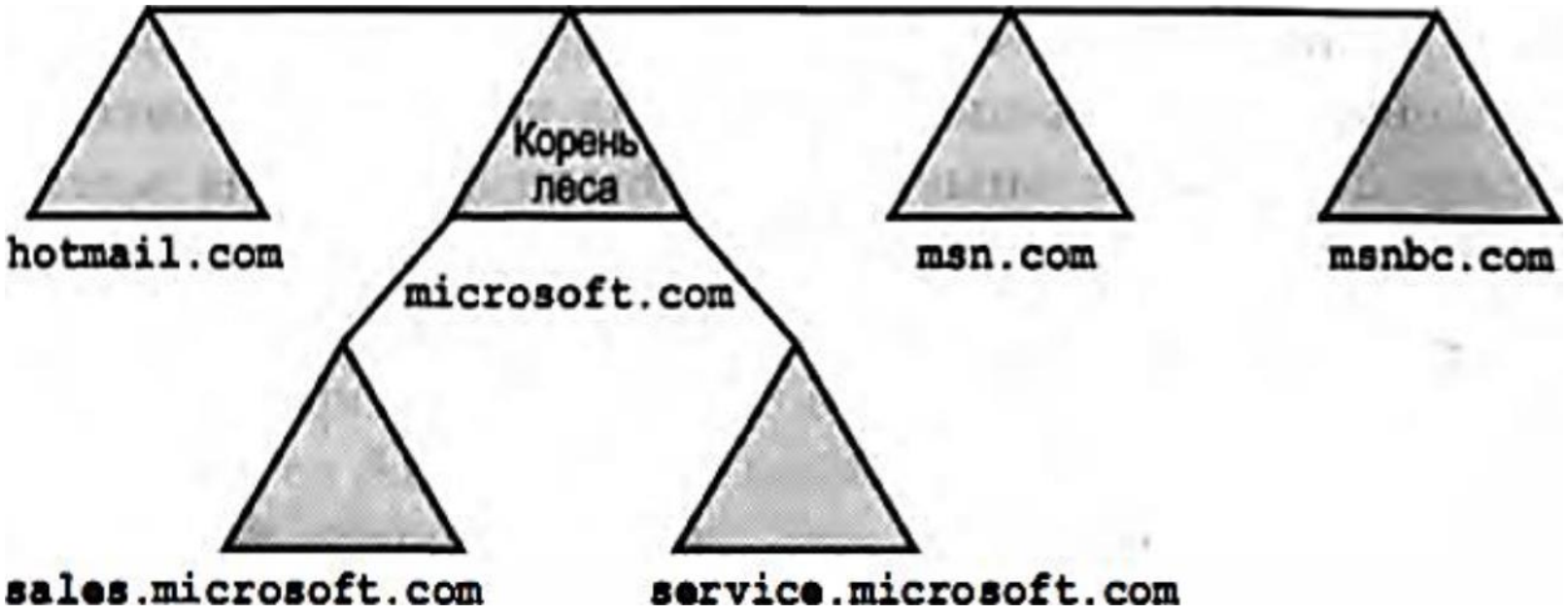
Модель с несколькими доменами

Причинами возникновения такой необходимости могут быть перечисленные ниже факторы.

- **Уникальное пространство имен DNS.** Если в каких-то подразделениях организации нужно использовать для AD DS **собственное зарегистрированное** в Интернете пространство имен, такое как hotmail.com или microsoft.com, но при этом использовать общий лес, их следует добавлять в виде отдельных доменов.
- **Необходимость в повышенной безопасности**.

Модель с несколькими деревьям и в одном лесе

В случае, если планируется реализовать структуру AD DS и использовать для нее **внешнее пространство имен**, однако в текущий момент в ее среде уже применяются несколько пространств DNS-имен, и их тоже необходимо включить в ту же структуру, то эти пространства имен можно интегрировать в единый лес AD с помощью **нескольких деревьев**, существующих **в одном лесе**.



Модель с несколькими деревьям и в одном лесе

Корневым в лесе является **только один** домен (в данном случае microsoft.com), и только он управляет доступом к схеме леса. Все остальные домены, в том числе поддомены Microsoft.com и **другие домены**, которые занимают другие структуры DNS, являются **членами** этого же **леса**. Все отношения доверия между доменами являются **транзитивными** и перетекают из одного домена в другой.

Модель с федеративными лесами

Модель федеративного леса удобна для двух случаев.

Первый - необходимость объединения двух различных структур AD DS, которая возникает в результате **приобретения** других компаний, **слияния** с другими корпорациями или других видов **организационной реструктуризации**, без применения сложных средств для миграции доменов.

Модель с федеративными лесами

В этом примере, благодаря установке между корнями лесов двусторонних доверительных отношений, пользователи двух организаций могут **получать доступ** к информации друг друга.

Модель с федеративными лесами

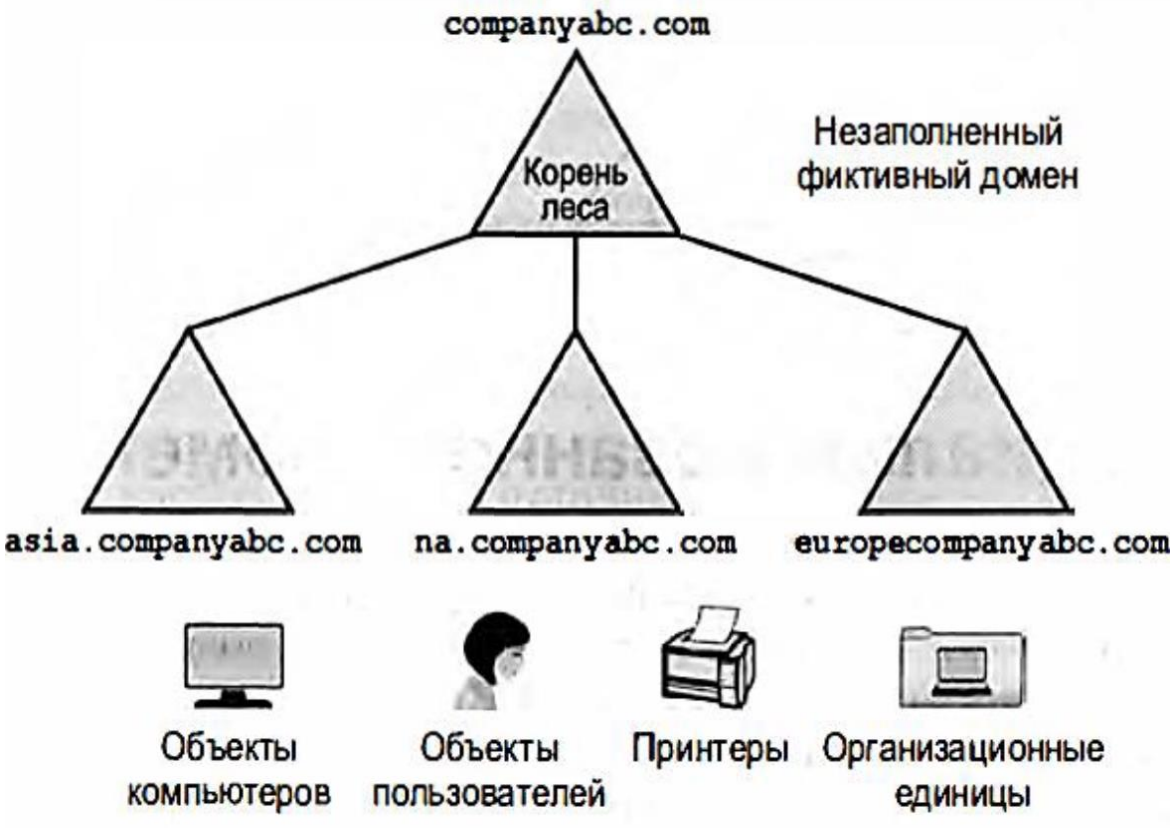
Вторым сценарием, при котором может выбираться проектирование такой структуры лесов, является ситуация, когда различным подразделениям и филиалам внутри организации требуется **полная защита** и права на владение информационной структурой, но все же с **возможностью** обмена информацией.

Модель домена с пустым корнем

Схема является самым **критически важным** компонентом AD DS и потому ее следует тщательно защищать и оберегать. Несанкционированный доступ к контроллеру домена эталона схемы может привести к серьезным проблемам. Поэтому выделение ключей к схеме из пользовательской базы представляет собой вполне разумный и заслуживающий рассмотрения вариант. Отсюда и появилась модель домена с пустым корнем

Модель с фиктивным доменом

Модель с фиктивным доменом, также называемая моделью со **стерильным родительским доменом**, представляет собой сочетание **модели нескольких доменов** с единым пространством имен и **модели с выделенным корнем**.



Модель с фиктивным доменом

Модель с фиктивным доменом содержит незаполненный домен в качестве корня леса и несколько поддоменов, заполненных пользовательскими учетными записями и другими объектами. У такой модели проектирования есть два очевидных **преимущества**.

Во-первых, как и в модели с выделенным корнем, схема отделена от пользовательских доменов, что снижает уязвимость пользователей и помогает защитить схему.

Во-вторых, пространство имен для пользовательских учетных записей отражает структуру организации, что устраняет какие-либо политические проблемы.

Модель специализированного домена

Специализированный домен или лес - это домен или лес, созданный для удовлетворения какой-то конкретной потребности.

Например, в организации такой домен может быть создан для вынесения **временных** и **работающих по контракту** пользователей в **отдельную категорию** и ограничения их участия в главном лесе AD DS, а также для установки между ним и остальными доменами доверительных отношений для обеспечения им доступа к ресурсам.

Вопрос №3. Понятие организационных единиц и групп

Организационной единицей (Organizational Unit - OU) называется контейнер административного уровня, который используется для логической организации объектов в AD DS.

Объекты в Active Directory могут логически **помещаться** в организационные единицы в соответствии с указаниями администратора.

По умолчанию объекты всех пользователей помещаются в **контейнер Users** (Пользователи), а объекты всех компьютеров - в **контейнер Computers** (Компьютеры), хотя их можно переместить оттуда в любой момент.

С технической точки зрения стандартные папки **Users** (Пользователи) и **Computers** (Компьютеры) в AD DS являются не организационными единицами, а **объектами класса Container**.

Структура OU может быть **вложенной**, т.е. содержать организационные подъединицы с множеством уровней в глубину. Не рекомендуется создавать структуру OU с более чем 10 уровнями вложенности.

Концепция **групп** предназначена для **логической** организации пользователей в легко идентифицируемые структуры. Тем не менее, между функционированием групп и OU имеются серьезные **отличия**, которые перечислены ниже.

- **Пользователи могут просматривать данные о членстве в группах.**
- **Членство в нескольких группах.**
- **Группы как параметры доступа.** Каждая группа доступа в AD DS обладает уникальным идентификатором безопасности (Security ID - SID), поэтому могут применяться для обеспечения безопасности на уровне объектов
- **Почтовые группы.** Посредством групп рассылки и почтовых групп пользователи могут отправить одно почтовое сообщение группе и тем самым распространять его среди всех членов этой группы.

Группа доступа (security group) - наиболее знакомый администраторам тип групп. Они применяются для **массового назначения прав** доступа к ресурсам и тем самым упрощения администрирования больших групп пользователей.

Группы доступа могут создаваться для каждого отдела в организации. Например, администратор может создать для пользователей из отдела маркетинга группу доступа под названием Marketing (Маркетинг), а затем предоставить этой группе права доступа к каким-то конкретным каталогам в среде.

Под **группой рассылки** подразумевается такая группа, члены которой могут получать отправляемые группе почтовые сообщения по протоколу **SMTP** (Simple Mail Transfer Protocol - простой протокол электронной почты).

В AD DS для групп существуют четыре основных области действия (scope):

- локальные группы компьютера;
- локальные группы домена;
- глобальные группы;
- универсальные группы.

Локальными группами компьютера (machine local group) называются группы, которые встроены в операционную систему и могут применяться **только** к объектам, локальным для компьютера, на котором они существуют.

Термином "**локальная группа домена**" (domain local group) обозначаются группы доменного уровня, которые могут применяться для задания прав доступа к ресурсам домена, в котором они находятся.

Глобальные группы в основном применяются для разбиения пользователей на легко идентифицируемые категории и для назначения прав доступа к ресурсам.

Универсальные группы могут содержать объекты из любого доверяемого домена и могут использоваться для применения прав доступа к любому ресурсу домена.

- Используйте **глобальные группы** для объединения пользователей по функциональному или географическому признаку (Менеджеры, Операторы, Бухгалтеры или Работники Рижского отделения компании, Сотрудники Третьего Этажа и т.п.)

- Используйте **локальные группы домена** для назначения доступа к ресурсам (Пользователи Базы 1С, Принтер HPLJ2600, Общие Документы Бухгалтерии)

- Добавляйте **глобальные группы в локальные группы домена**, выражая нужды простым человеческим языком: "Хочу, чтобы Менеджеры имели доступ к Базе 1С".

- Используйте **универсальные группы**, когда нужно дать доступ Множеству пользователей из Множества доменов к Множеству ресурсов, расположенных в Многих доменах.