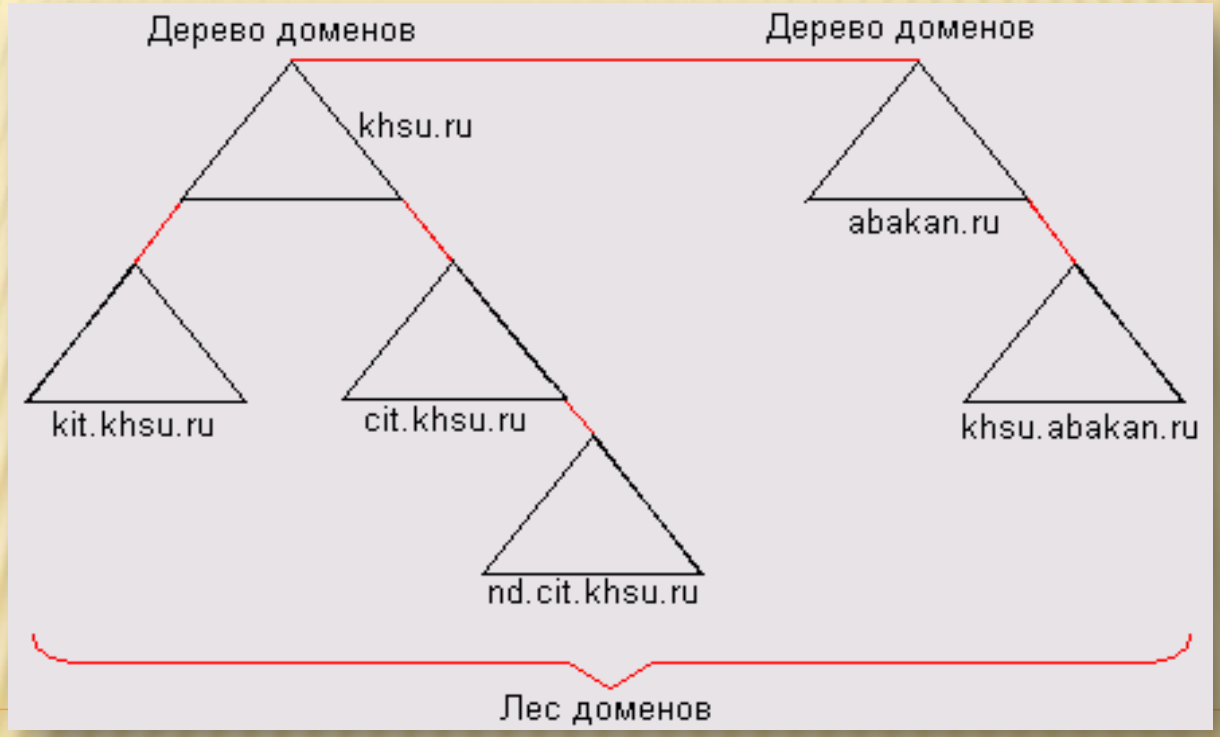
ДОМЕНЫ



Операционные системы Windows традиционно использовали **понятие "домена" для логического объединения компьютеров, совместно использующих единую политику безопасности**.

Домен выступает в качестве основного способа создания областей административной ответственности. Как правило, каждым доменом управляет отдельная группа администраторов.

ЗАДАЧИ, РЕШАЕМЫЕ ПРИ ФОРМИРОВАНИИ ДОМЕННОЙ СТРУКТУРЫ

- **Создание областей административной ответственности**. Используя доменную структуру, администратор может поделить корпоративную сеть на области (домены), управляемые отдельно друг от друга. Каждый домен управляется своей группой администраторов (администраторы домена).

- **Создание областей действия политики учетных записей**. Политика учетных записей определяет правила применения пользователями учетных записей и сопоставленных им паролей. В частности задается длина пароля, количество неудачных попыток ввода пароля до блокировки учетной записи, а также продолжительность подобной блокировки.

- **Разграничение доступа к объектам**. Каждый домен реализует собственные настройки безопасности (включая идентификаторы безопасности и списки контроля доступа). Разнесение пользователей в различные домены позволяет эффективно управлять доступом к важным ресурсам.

- **Создание отдельного контекста имен для национальных филиалов.** В случае, если компания имеет филиалы, расположенные в других странах, может потребоваться создать отдельный контекст имен для каждого такого филиала. Можно отразить в имени домена географическое либо национальное местоположение филиала.

- **Изоляция трафика репликации**. Для размещения информации об объектах корпоративной сети используются доменные разделы каталога. Каждому домену соответствует свой раздел каталога, называемый доменным. Все объекты, относящиеся к некоторому домену, помещаются в соответствующий раздел каталога.

- **Ограничение размера копии каталога**. Каждый домен Active Directory может содержать до миллиона различных объектов. Тем не менее, реально использовать домены такого размера непрактично. Следствием большого размера домена является большой размер копии каталога. Соответственно, огромной оказывается нагрузка на серверы, являющиеся носителями подобной копии. Администратор может использовать домены как средство регулирования размера копии каталога.

ИЕРАРХИЯ ДОМЕНОВ

- Для именования доменов используется соглашение о доменных именах. Имя домена записывается в форме полного доменного имени (**Fully Qualified Domain Name, FQDN**), которое определяет положение домена относительно корня пространства имен. Полное доменное имя образуется из имени домена, к которому добавляется имя родительского домена.
- Например, для домена kit, являющегося дочерним по отношению к домену khsu.ru, полное доменное имя будет записано в форме kit. khsu.ru.

- Выбор подобной схемы именования позволил формировать доменное пространство имен, аналогичное пространству имен службы DNS. Отображение доменов Active Directory на домены DNS позволило упростить процессы поиска серверов служб и разрешения имен, осуществляемые серверами DNS в ответ на запросы клиентов службы каталога.

- Совокупность доменов, использующих единую схему каталога, называется **лесом доменов (forest).** Строго говоря, входящие в лес домены могут не образовывать "непрерывного" пространства смежных имен.
- Совокупность доменов, образующих непрерывное пространство смежных имен, называют **деревом доменов (domain tree).** Лес может состоять из произвольного количества деревьев домена.

- Первое созданное в лесу доменов дерево является **корневым деревом**.
- Корневое дерево используется для ссылки на лес доменов. Первый созданный в дереве домен называется **корневым доменом дерева (tree root domain),** который используется для ссылки на данное дерево. Совершенно очевидно, что корневой домен является определяющим для всего дерева.

- Корневой домен леса играет очень **важную роль,** связывая деревья, образующие лес доменов, воедино и поэтому **не может быть удален**. В частности, он хранит информацию о конфигурации леса и деревьях доменов, его образующих.

КОНТРОЛЛЕРЫ ДОМЕНА

- Серверы Windows Server, на которых функционирует экземпляр службы каталога Active Directory, называются **контроллерами домена (domain controller, DC).** Контроллеры домена являются носителями полнофункциональных копий каталога.

КОНТРОЛЛЕРЫ ДОМЕНА ВЫПОЛНЯЮТ ЗАДАЧИ:

- **Организация доступа к информации**, содержащейся в каталоге, включая управление этой информацией и ее модификацию. Контроллер домена может рассматриваться как LDAP-сервер, осуществляющий доступ пользователя к LDAP-каталогу.

- **Синхронизация копий каталога**. Каждый контроллер домена является субъектом подсистемы репликации каталога. Любые изменения, осуществляемые в некоторой копии каталога, будут синхронизированы с другими копиями.

- **Централизованное тиражирование файлов**. Служба репликации файлов, функционирующая на каждом контроллере домена, позволяет организовать в корпоративной сети централизованное тиражирование необходимых системных и пользовательских файлов (включая шаблоны групповой политики).

- **Аутентификация пользователей**. Контроллер домена осуществляет проверку полномочий пользователей, регистрирующихся на клиентских системах. Каждый контроллер домена Windows Server может рассматриваться как Центр распределения ключей (KDC) Kerberos.

- **Особенно следует отметить тот факт**, что все контроллеры домена **обладают возможностью внесения изменений в собственную копию каталога.** Это позволяет рассматривать любой контроллер домена как точку административного воздействия на корпоративную сеть. Практически все административные утилиты работают в контексте какого-либо контроллера домена. Это означает, что администратор может осуществлять конфигурирование службы каталога и сети, подключившись к любому контроллеру домена Active Directory.