1. Основные службы каталогов и стандарты, используемые в современных сетях.

Active Directory (AD) - служба каталогов, поставляемая с Microsoft Windows, начиная с Windows 2000 Server. Active Directory содержит каталог, в котором хранится информация о сетевых ресурсах и службы, предоставляющие доступ к этой информации.

Х.500 и Directory Access Protocol (DAP). X.500 - спецификация International Organization for Standardization (ISO), определяющая, как должны быть структурированы глобальные каталоги. Х.500 также описывает применение DAP для обеспечения взаимодействия между клиентами и серверами каталогов;

Lightweight Directory Access Protocol (LDAP). Протокол LDAP был разработан в ответ на критические замечания по спецификации DAP, которая оказалась слишком сложной для применения в большинстве случаев.

Novell Directory Services (NDS). Служба каталогов для сетей Novell NetWare, совместимая со стандартом Х.500;

Windows NT и SAM. Ядром Windows NT NOS (Network Operating System - сетевая операционная система) является база данных SAM (Security Accounts Management - управление безопасными учетными записями). Она представляет центральную базу данных учетных записей, включающую все учетные записи пользователей и групп в домене. Эти учетные записи используются для управления доступом к совместным ресурсам, принадлежащим любому серверу в домене Windows NT.

2. Основные функции службы каталогов.

Централизация. Смысл централизации - уменьшение количества каталогов в сети. Включение информации обо всех сетевых ресурсах в централизованный каталог создает единственную точку управления, что упрощает администрирование ресурсов и позволяет эффективнее делегировать административные задачи.

Масштабируемость. Служба каталогов должна допускать рост сети, не создавая при этом слишком больших издержек, - то есть она должна поддерживать какой-либо способ разбиения базы данных каталога на разделы, чтобы не утратить контроль над базой данных из-за ее чрезмерного разрастания и при этом сохранить преимущества централизации.

Стандартизация. Служба каталогов должна предоставлять доступ к своей информации по открытым стандартам.

Расширяемость. Служба каталогов должна тем или иным способом позволять администраторам и приложениям расширять в соответствии с потребностями организации набор информации, хранимой в каталоге.

Разделение физической сети. Благодаря службе каталогов топология физической сети должна быть прозрачной для пользователей и администраторов.

Безопасность. Служба каталогов должна поддерживать защищенные средства хранения, управления, выборки и публикации информации о сетевых ресурсах.

3. Область действия, пространство имен Active Directory.

Область действия (scope) Active Directory достаточно обширна. Она может включать отдельные сетевые объекты (принтеры, файлы, имена пользователей), серверы и домены в отдельной глобальной сети. Она может также охватывать несколько объединенных сетей. Active Directory может быть настроена на управление как отдельным компьютером, так и компьютерной сетью или группой сетей.

Пространство имен — это такая ограниченная область, в которой может быть распознано данное имя. Распознавание имени заключается в его сопоставлении с некоторым объектом или объемом информации, которому это имя соответствует. Active Directory образует пространство имен, в котором имя объекта в каталоге может быть поставлено в соответствие самому этому объекту.

4. Домен. Доверительные отношения. Типы доверительных отношений.

Домен — это единая область, в пределах которой обеспечивается безопасность данных в компьютерной сети под управлением ОС Windows

Поскольку домены разграничивают зоны безопасности, специальный механизм, называемый доверительными отношениями (trust relationships), позволяет объектам в одном домене [доверяемом (trusted domain)] обращаться к ресурсам в другом [доверяющем (trusting domain)].

Типы доверительных отношений:

Доверие к родительскому и дочернему доменам

Доверие к корневому домену дерева

Доверие к внешнему домену

Доверие к сокращению

Доверие к сфере

Доверие к лесу

5. Сайт, узел.

Сайт представляет область сети, где все контроллеры домена связаны быстрым, недорогим и надежным сетевым подключением.

Узлом (сайтом) называется такой элемент сети, который содержит серверы Active Directory. Узел обычно определяется как одна или несколько подсетей, поддерживающих протокол TCP/IP и характеризующихся хорошим качеством связи, которое подразумевает высокую надежность и скорость передачи данных.

6. Типовой план проектирования структуры Active Directory.

Проектирование структуры Active Directory начинается с компонентов высшего уровня, а затем проектируются компоненты низших уровней. Это означает, что первый шаг состоит в создании проекта леса, затем следует проект доменов, проект DNS и, наконец, проект организационной единицы (OU)

Планирование структуры лесов

Планирование доменов для каждого леса

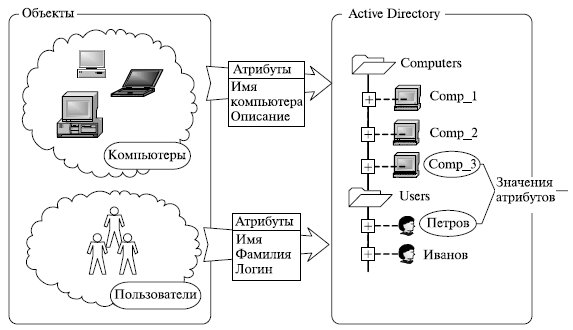
Планирование использования сайтов для каждого леса

Планирование структуры организационных единиц для каждого домена

Планирование реорганизации существующих доменов и их перевод на новую платформу Active Directory

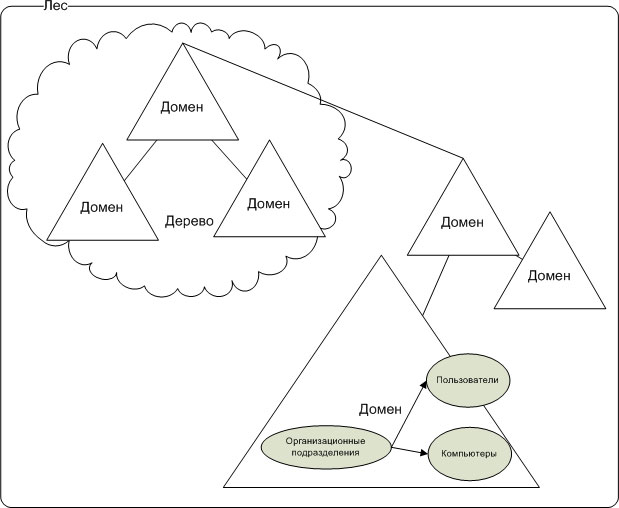
Тестирование внедряемых решений и установка стенда

7. Схема объектов Active Directory и их атрибуты



8. Логическая структура и физическая структура Active Directory.

Логическая структура Active Directory является моделью службы каталога, которая определяет каждого участника безопасности на предприятии, а также организацию этих участников.



Физическое проявление службы Active Directory состоит в наличии отдельного файла данных, расположенного на каждом контроллере домена. Физическая реализация службы Active Directory описывается местоположением контроллеров домена, на которых расположена служба. При реализации службы Active Directory можно добавлять столько контроллеров доменов, сколько необходимо для поддержания служб каталога в данной организации.

9. Контроллеры доменов, функции контроллера домена.

Контроллер домена — это компьютер-сервер, управляющий доменом и хранящий реплику каталога домена (локальную БД домена). Поскольку в домене может быть несколько контроллеров домена, все они хранят полную копию той части каталога, которая относится к их домену.

функции контроллеров доменов:

Каждый контроллер домена хранит полную копию всей информации Active Directory, относящейся к его домену, а также управляет изменениями этой информации и реплицирует их на остальные контроллеры того же домена.

Все контроллеры в домене автоматически реплицируют между собой все объекты в домене.

Важные обновления, например отключение учетной записи пользователя, контроллеры домена реплицируют немедленно.

Active Directory использует репликацию с несколькими хозяевами (multimaster replication), в котором ни один из контроллеров домена не является главным.

Наличие в домене нескольких контроллеров обеспечивает отказоустойчивость.

Контроллеры домена управляют взаимодействием пользователей и домена, например находят объекты Active Directory и распознают попытки входа в сеть.