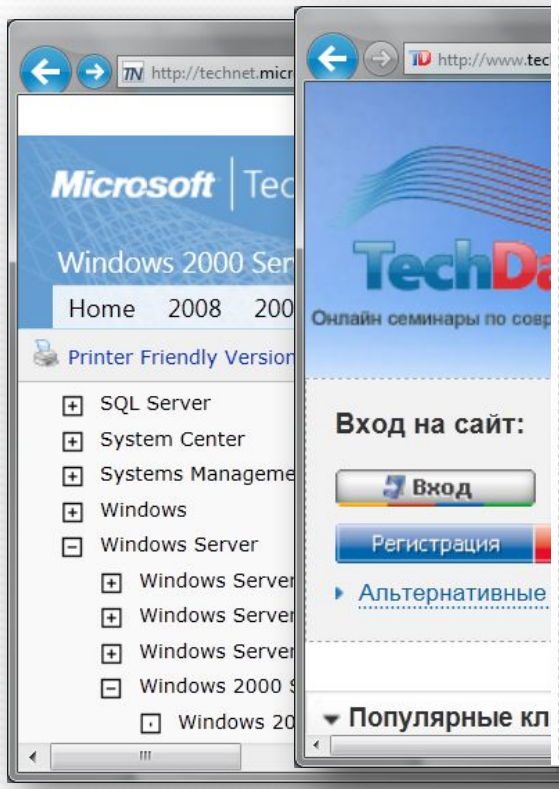
Введение в Active Directory

к.т.н., доц. каф. ITM
Алексеев Н.А.

…“Война и мир” в 3-х СМСках

Литература:

1. http://technet.microsoft.com
2. http://www.techdays.ru/videos/2089.html
3. Д. В. Чижиков Методология внедрения Microsoft Active Directory (Есть в эл. виде в Интернете)
4. Bing/Google/Yandex…



Д. В. Чижиков

Методология внедрения Microsoft Active Directory

Серия: Основы информационных технологий

Издательства: Интернет-университет информационных технологий, Бином. Лаборатория знаний, 2008 г.
Мягкая обложка, 168 стр.
ISBN 978-5-94774-969-4
Тираж: 2000 экз.
Формат: 60x90/16 (~145x217 мм)

Всего отзывов: 1. Оставить свой отзыв (Отзывов ожидает 1 чел.)
Подписаться на отзывы

Сообщить о неточности в описании

Поставить метку
Метки пользователей: admin (1)

Поделиться:

Введение в Active Directory

Аннотация

- Определение и назначение служб каталогов, их основные функции и задачи.
- Службы каталогов - предвестники Microsoft Active Directory.
- Ключевые преимущества службы Active Directory
- Основные понятия службы каталогов
- Архитектура Active Directory

Вне зависимости от

- топологии сети компании
- реальной инфраструктуры
- организационной структуры географически распределенных филиалов
- имеющейся в компании разнородной информационной среды

существует общая методология развертывания и применения службы Active Directory.

Определение каталога и службы каталогов

- ***Каталог (directory)*** — это информационный ресурс, используемый для хранения информации о каком-либо объекте.
  - Например, телефонный справочник (каталог телефонных номеров) содержит информацию об абонентах телефонной сети.
  - В файловой системе каталоги хранят информацию о файлах

В распределенной вычислительной системе или в компьютерной сети общего пользования (например, Интернет) имеется множество объектов - серверы, базы данных, приложения, принтеры и др.

Пользователи хотят иметь доступ к каждому из таких объектов и работать с ними,

а администраторы - управлять правилами использования этих объектов

Определение каталога и службы каталогов

- ***Служба каталогов (directory service)*** - сетевая служба, которая идентифицирует все ресурсы сети и делает их доступными пользователям.
  - Служба каталогов централизованно хранит всю информацию, требуемую для использования и управления этими объектами, упрощая процесс поиска и управления данными ресурсами.
  - Служба каталогов работает как главный коммутатор сетевой ОС. Она управляет идентификацией и отношениями между распределенными ресурсами и позволяет им работать вместе

Определение каталога и службы каталогов

- *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

Альтернативы Active Directory

- Active Directory - это не первая и не единственная служба каталогов.
- В современных сетях используется несколько служб каталогов и стандартов :
  - X.500 и Directory Access Protocol (DAP).
    - X.500 - спецификация Internet Standards Organization (ISO), определяющая, как должны быть структурированы глобальные каталоги. X.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. Спецификация LDAP быстро стала стандартным протоколом каталогов в Интернете;
  - Novell Directory Services (NDS).
    - Служба каталогов для сетей Novell NetWare, совместимая со стандартом X.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.

Active Directory

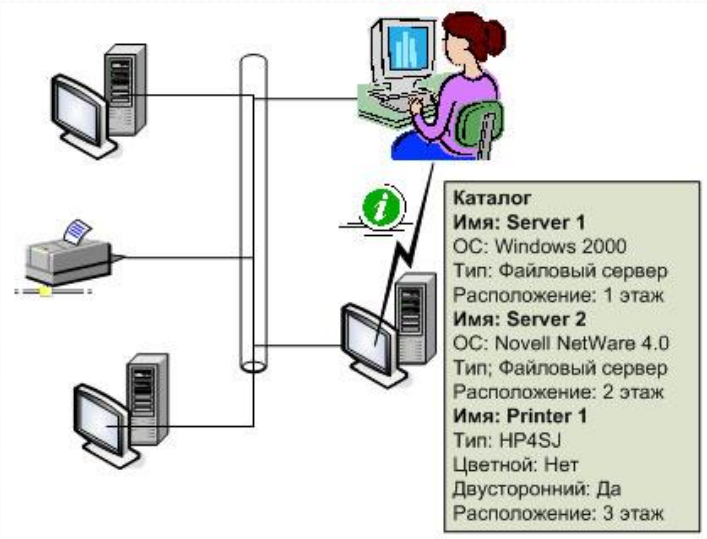
Служба Active Directory, в отличие от перечисленных служб каталогов, является защищенной, распределенной, сегментированной и реплицируемой, что позволяет обеспечить следующие возможности:

- упрощенное администрирование;
- масштабируемость;
- поддержку открытых стандартов;
- поддержку стандартных форматов имен.

Active Directory

- С помощью Active Directory осуществляется
  - централизованное управление
    - пользователями,
    - группами,
    - общими папками
    - сетевыми ресурсами,
  - администрирование среды пользователя и программного обеспечения средствами групповой политики.

Назначение службы каталогов



- Служба каталогов является как инструментом администрирования, так и инструментом пользователя
- Пользователи и администраторы зачастую не знают точных имен объектов, которые им в данный момент требуются. Они могут знать один или несколько их признаков или атрибутов (attributes) и могут послать запрос (query) к каталогу, получив в ответ список тех объектов, атрибуты которых совпадают с указанными в запросе

Назначение службы каталогов

Назначение службы каталогов

- Служба каталогов позволяет
  - обеспечивать защиту информации от вмешательства посторонних лиц в рамках, установленных администратором системы;
  - распространять каталог среди других компьютеров в сети;
  - проводить репликацию (тиражирование) каталога, делая его доступным для большего числа пользователей и более защищенным от потери данных;
  - разделять каталог на несколько частей, обеспечивая возможность хранения очень большого числа объектов.

Назначение службы каталогов

- По мере роста числа объектов в сети служба каталогов начинает играть все более важную роль.
- Можно сказать, что служба каталогов - это та основа, на которой строится вся работа крупной распределенной компьютерной системы.
- В сложной сети служба каталогов должна обеспечивать эффективный способ управления, поиска и доступа ко всем ресурсам в этой сети, например к компьютерам, принтерам, общим папкам и т. д

Функции службы каталогов

Служба каталогов была бы крайне полезной злоумышленнику, так как она хранит подробную информацию о данной организации.
Поэтому служба каталогов должна поддерживать защищенные средства хранения, управления, выборки и публикации информации о сетевых ресурсах.

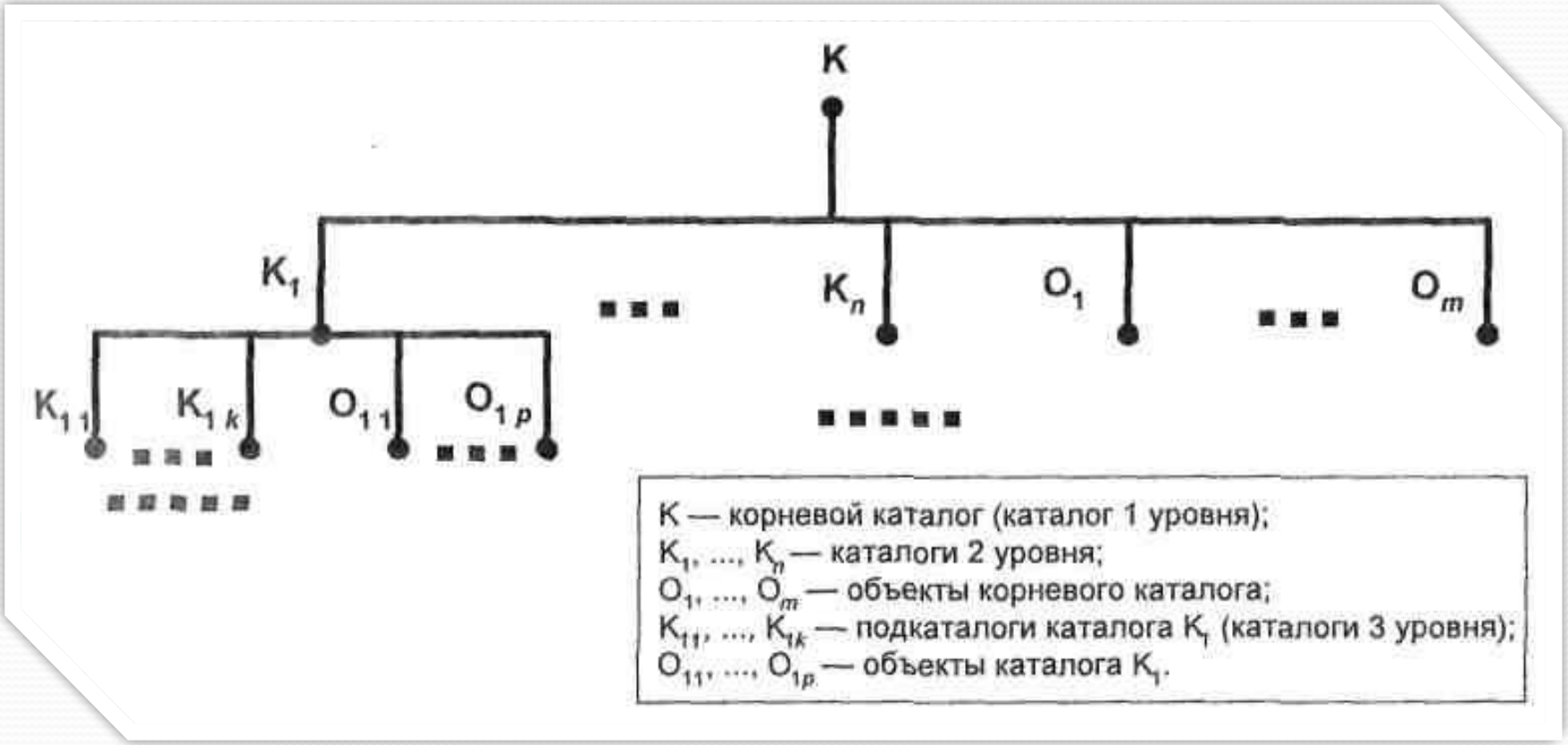
Служба к[illegible]жна тем или иным способом позволят[illegible]министраторам и приложениям расширять в соответствии с потребностями организации набор информации, хранимой в каталоге

Основные задачи службы Active Directory

- Хранить информацию об объектах сети и предоставлять эту информацию пользователям и системным администраторам.
- Позволять пользователям сети обращаться к общим ресурсам, единожды введя имя и пароль.
- Представлять сеть в интуитивно понятном иерархическом виде и позволять централизованно управлять всеми объектами сети.
- Повышать степень информационной безопасности за счет разграничения административных полномочий обслуживающего персонала и внедрения современных методов защиты информации.
- Позволять спроектировать единую структуру каталога так, как это необходимо в организации, чтобы обеспечить прозрачное использование информационных ресурсов в рамках компании.

Преимущества Active Directory

- Служба каталогов Active Directory является службой, интегрированной с MS Windows начиная с Windows 2000 Server.
- Active Directory обеспечивает иерархическую структуру



Преимущества интеграции управления учетными записями со службой каталогов Active Directory

- учетные записи пользователей, групп и машин могут быть организованы в виде контейнеров каталога, называемых организационными подразделениями или просто подразделениями.
  - В домене может быть произвольное число подразделений, организованных в виде древовидного пространства имен.
  - Это пространство имен может быть выстроено в соответствии с подразделениями и отделами в организации.
  - Так же как и организационные подразделения, учетные записи пользователей являются объектами каталога и могут быть легко переименованы внутри дерева доменов при перемещении пользователей из одного отдела в другой;

Преимущества интеграции управления учетными записями со службой каталогов Active Directory

- в каталоге Active Directory поддерживается большое число объектов: размер одного домена не ограничивается производительностью сервера, хранящего учетные записи. Дерево связанных между собой доменов может поддерживать большие и сложные организационные структуры;

Преимущества интеграции управления учетными записями со службой каталогов Active Directory

- администрирование учетной информации расширено за счет использования графических средств управления Active Directory, а также за счет поддержки OLE в языках сценариев.
  - Общие задачи могут быть реализованы в виде сценариев, позволяющих автоматизировать администрирование;

Преимущества интеграции управления учетными записями со службой каталогов Active Directory

- служба тиражирования каталогов позволяет иметь несколько копий учетной информации, причем обновления этой информации могут выполняться в любой копии, а не только на выделенных первичных контроллерах домена.
  - Протокол LDAP и синхронизация каталогов позволяют обеспечивать механизмы связи каталога Windows с другими каталогами на предприятии;

Преимущества интеграции управления учетными записями со службой каталогов Active Directory

- хранение учетной информации в Active Directory означает, что пользователи и группы представлены в виде объектов каталога.
  - Права на чтение и запись могут быть предоставлены как по отношению ко всему объекту целиком, так и по отношению к отдельным его свойствам.
  - Администраторы могут точно определять, кто именно и какую именно информацию о пользователях может модифицировать.
    - Например, оператору телефонной службы может быть разрешено изменять информацию о телефонных номерах пользователей, но при этом он не будет обладать привилегиями системного оператора или администратора.

Преимущества интеграции управления учетными записями со службой каталогов Active Directory

- Если в компании-заказчике заинтересованы в выполнении наиболее сильно интегрированной службы каталога для Windows Server 2003/2008, то Active Directory является логичным выбором.
- Другая очень популярная причина, подталкивающая к реализации службы Active Directory, состоит в поддержке Microsoft Exchange Server (Exchange Server полагается на Active Directory для своей службы каталога, поэтому многие администраторы реализуют Active Directory, чтобы модернизироваться до Exchange Server)

Несколько ключевых преимуществ службы Active Directory Windows Server 2003

Централизованный каталог

- Active Directory является единственной централизованной службой каталога, которая может быть реализована в пределах предприятия. Это упрощает сетевое администрирование, поскольку администраторы не должны соединяться с несколькими каталогами, чтобы выполнять управление учетными записями. Другая выгода от применения централизованного каталога состоит в том, что он может также использоваться другими приложениями, такими как Exchange Server 2000. Это упрощает полное сетевое администрирование, так как используется единая служба каталога для всех приложений.

Единая регистрация.

- После успешной идентификации пользователям будет предоставлен доступ ко всем сетевым ресурсам, для которых им было дано разрешение, без необходимости регистрироваться снова на различных серверах или доменах.

Делегированное администрирование.

- Active Directory предоставляет администраторам возможность передавать административные права. Используя мастер Delegation Of Control Wizard (Делегирование управления) или устанавливая определенные разрешения на объекты Active Directory, администраторы могут предлагать тонко настроенные административные права. Например, можно назначить определенной учетной записи пользователя административное право сбрасывать пароли в домене, но не создавать, удалять или как-либо изменять пользовательский объект.

Интерфейс общего управления.

- Есть несколько способов, которыми можно получить выгоду от интеграции между Active Directory и операционной системой. Один из путей состоит в использовании интерфейса общего управления - консоли управления Microsoft (MMC - Microsoft Management Console). При взаимодействии с Active Directory через графический интерфейс пользователя MMC все инструментальные средства управления дают согласующееся друг с другом впечатление и ощущение от их использования. Для Active Directory эти средства включают Active Directory Users And Computers (Active Directory: пользователи и компьютеры), Active Directory Domains And Trusts (Active Directory: домены и доверительные отношения) и Active Directory Sites And Services (Active Directory: сайты и службы). Оснастки MMC функционируют так же, как все другие средства администрирования Windows Server 2003, например оснастки DHCP и DNS

Несколько ключевых преимуществ службы Active Directory Windows Server 2003

- **Интегрированная безопасность**
  - Служба Active Directory работает рука об руку с подсистемой безопасности Windows Server 2003 при аутентификации безопасных пользователей и обеспечении защиты общедоступных сетевых ресурсов. Сетевая защита в сети Windows Server 2003 начинается с аутентификации во время регистрации. Когда безопасный пользователь входит в домен Windows Server 2003, подсистема защиты вместе с Active Directory создает лексему доступа, которая содержит идентификатор защиты (SID - Security Identifier) учетной записи пользователя, а также идентификаторы SID всех групп, членом которых является данный пользователь. Идентификатор SID является атрибутом пользовательского объекта в Active Directory. Затем лексема доступа сравнивается с дескриптором защиты на ресурсе, и, если устанавливается соответствие, то пользователю предоставляется требуемый уровень доступа.
- **Масштабируемость.**
  - Поскольку организация либо постепенно растет в процессе бизнеса, либо это происходит быстро, через ряд слияний с другими компаниями и в результате приобретений, служба Active Directory спроектирована масштабируемой, для того чтобы справляться с этим ростом. Можно расширить размер доменной модели или просто добавить больше серверов, чтобы приспособиться к потребностям увеличения объема. Любые изменения в инфраструктуре Active Directory должны быть тщательно реализованы в соответствии с проектом Active Directory, который предусматривает такой рост. Отдельный домен, представляющий самый маленький раздел инфраструктуры Active Directory, который может реплицироваться на единственный контроллер домена, может поддерживать более одного миллиона объектов, так что модель отдельного домена подходит даже для больших организаций.

Основные понятия службы каталогов

- ***Область действия (scope) AD***
  - Может включать отдельные сетевые объекты (принтеры, файлы, имена пользователей), серверы и домены в отдельной глобальной сети.
  - Active Directory может быть настроена на управление как отдельным компьютером, так и компьютерной сетью или группой сетей.

Основные понятия службы каталогов

- Active Directory, как и любая другая служба каталогов, является прежде всего пространством имен.
- ***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.

Основные понятия службы каталогов
Пространство имен

Телефонный справочник

имена телефонных абонентов	телефонные номера

Файловая система Windows

имя файла	конкретный файл

ACTIVE DIRECTORY

имя объекта в	сам

Основные понятия службы каталогов

- ***Объект*** - это непустой, именованный набор атрибутов, обозначающий нечто конкретное, например пользователя, принтер или приложение.
- Атрибуты содержат информацию, однозначно описывающую данный *объект*.
- Атрибуты пользователя могут включать имя пользователя, его фамилию и адрес электронной почты

Основные понятия службы каталогов

- ***Контейнер*** аналогичен объекту в том смысле, что он также имеет атрибуты и принадлежит пространству имен.
- Однако, в отличие от объекта, *контейнер* не обозначает ничего конкретного: он может содержать группу объектов или другие *контейнеры*

Основные понятия службы каталогов

- Термин "***дерево***" используется для описания иерархии объектов и контейнеров.
- Как правило, конечными элементами дерева являются объекты. В узлах (точках ветвления) дерева располагаются контейнеры.

Основные понятия службы каталогов

- ***Дерево*** отражает взаимосвязь между объектами или указывает путь от одного объекта к другому.
  - Простой каталог представляет собой контейнер.
  - Компьютерная сеть или *домен* тоже являются контейнерами.
- Непрерывным поддеревом называют любую непрерывную часть дерева, включающую все элементы каждого входящего в нее контейнера

Основные понятия службы каталогов

- Служба Active Directory допускает существование двух типов **имен**, используемых для идентификации объектов:
  - **Уникальное имя**. Каждый объект в Active Directory имеет уникальное имя (Distinguished Name, DN).
  - **Относительное имя**. Относительное уникальное *имя объекта* (Relative Distinguished Name, RDN)

Основные понятия службы каталогов

- **Уникальное имя**. Каждый объект в Active Directory имеет уникальное имя (Distinguished Name, DN).
  - Это имя содержит указание на *домен*, в котором находится объект, и полный путь в иерархической структуре контейнеров, который приводит к данному объекту.
  - Типичным уникальным именем (DN) является имя: /O=Internet/DC=COM/DC=Microsoft/CN=Users/CN=James Smith. Это имя обозначает объект типа "пользователь"с именем "James Smith", находящийся в домене Microsoft.com.

Основные понятия службы каталогов

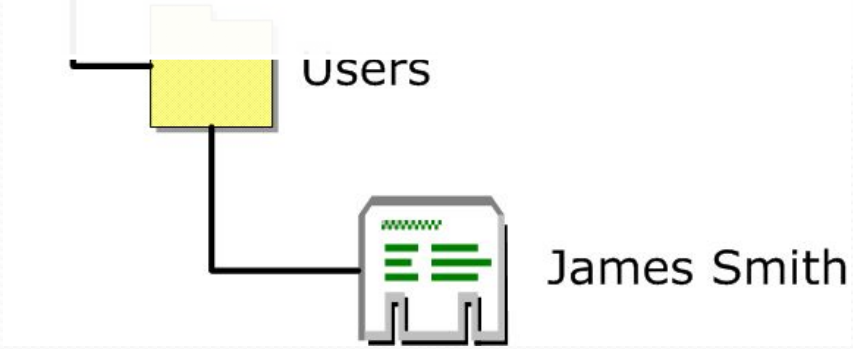
- **Относительное имя**.
  - Относительное уникальное *имя объекта* (Relative Distinguished Name, RDN) - это та часть имени, которая сама является частью атрибута объекта.
  - В приведенном выше примере RDN-именем объекта "James Smith"служит групповое имя (CN) CN=James Smith.
  - RDN-именем родительского объекта является имя CN=Users

Основные понятия службы каталогов

Distinguished Name, DN (Уникальное имя)

/O=Internet/DC=COM/DC=Microsoft/CN=Users/CN=James Smith

RDN для



Основные понятия службы каталогов

- Active Directory может состоять из одного или нескольких ***контекстов имен*** или ***сегментов (разделов)***.
- *Контекстом имен* может быть любое непрерывное поддерево каталога.
- *Контексты имен* являются единицами репликации.

- В Active Directory каждый сервер всегда содержит не менее трех контекстов имен:
  - логическую структуру;
  - конфигурацию (топологию репликации и соответствующие метаданные);
  - один или несколько пользовательских контекстов имен (поддеревья, содержащие объединенные в каталог объекты).

Основные понятия службы каталогов

- ***Домен*** - это единая область, в пределах которой обеспечивается безопасность данных в компьютерной сети под управлением ОС Windows
- (Более подробно – см. документацию по ОС Windows).

Основные понятия службы каталогов

- Active Directory состоит из одного или нескольких доменов.
- Применительно к отдельной рабочей станции доменом является сама станция. Границы одного домена могут охватывать более чем одно физическое устройство.

Основные понятия службы каталогов

- Каждый *домен* может иметь свои правила защиты информации и правила взаимодействия с другими доменами.

- Если несколько доменов связаны друг с другом доверительными отношениями и имеют единую логическую структуру, конфигурацию и глобальный каталог, то говорят о дереве доменов.

Основные понятия службы каталогов

- 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)]
- Windows Server 2003 поддерживает шесть типов 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

Основные понятия службы каталогов
Доверительные отношения

- Доверие к родительскому и дочернему доменам

  Active Directory автоматически выстраивает транзитивные двусторонние *доверительные отношения* между родительскими и дочерними доменами в дереве доменов.

  При создании дочернего домена *доверительные отношения* автоматически формируются между дочерним доменом и его родителем.

  Эти отношения двусторонние.

  Доверие также является транзитивным, т. е. контроллеры доверяемого домена пересылают запросы на аутентификацию контроллерам доверяющих доменов.

Основные понятия службы каталогов
Доверительные отношения

- Доверие к корневому домену дерева

  Двусторонние транзитивные *доверительные отношения* автоматически создаются и между корневыми доменами деревьев в одном лесу.

  Это резко упрощает управление доменами по сравнению с тем, что было в версиях Windows, предшествовавших Windows 2000. Больше не нужно конфигурировать отдельные односторонние доверительные отношения между доменами.

Основные понятия службы каталогов
Доверительные отношения

- Доверие к внешнему домену
  - Внешнее доверие используется, когда нужно создать *доверительные отношения* между доменом Windows Server 2003 и доменом *Windows NT 4.0*.
  - Поскольку ограниченные домены (down-level domains) (домены, не поддерживающие Active Directory) не могут участвовать в двусторонних транзитивных доверительных отношениях, следует использовать внешнее доверие, которое является односторонним

Основные понятия службы каталогов
Доверительные отношения

- Доверие к сокращению

  Доверие к сокращению - это способ создания прямых доверительных отношений между двумя доменами, которые могут быть уже связаны цепочкой транзитивных доверий, но нуждаются в более оперативном реагировании на запросы друг от друга

Основные понятия службы каталогов
Доверительные отношения

- Доверие к сфере
  - Доверие к сфере служит для подключения домена Windows Server 2003 к сфере Kerberos (управление идентификацией), которая не поддерживает Windows и использует протокол защиты Kerberos V5.
  - Доверие к сфере может быть транзитивным или нетранзитивным, одно- или двусторонним

Основные понятия службы каталогов
Доверительные отношения

- Доверие к лесу

  Доверие к лесу упрощает управление несколькими лесами и обеспечивает более эффективное защищенное взаимодействие между ними.

  Этот тип доверия позволяет обращаться к ресурсам в другом лесу по той же идентификации пользователя (user IDentification, ID), что и в его собственном лесу

Основные понятия службы каталогов

- **Дерево доменов** состоит из нескольких доменов, которые имеют общую логическую структуру и конфигурацию и образуют непрерывное *пространство имен*.
- Домены в дереве связаны между собой доверительными отношениями.
- Active Directory является множеством, которому принадлежат одно или несколько деревьев доменов

Основные понятия службы каталогов

- Дерево доменов графически можно представить двумя способами:
  - **Представление доменного дерева через** *доверительные отношения* **между доменами**.
    - *Доверительные отношения* между доменами в ОС Windows 2000 устанавливаются на основе протокола безопасности Kerberos. Отношения, созданные с помощью этого протокола, обладают свойствами транзитивности и иерархичности: если домен A доверяет домену B и домен B доверяет домену C, то домен A доверяет и домену C.
  - **Представление доменного дерева через** *пространство имен* **доменного дерева**.
    - *Доменное дерево* можно также представить с помощью пространства имен. Уникальное *имя объекта* можно определить, двигаясь вверх по доменному дереву начиная с объекта. Такой метод оказывается удобным при объединении объектов в логическую иерархическую структуру. Главное достоинство непрерывного пространства имен состоит в том, что глубокий поиск, проводимый от корня дерева, позволяет просмотреть все иерархические уровни пространства имен.
- Несколько доменных деревьев могут быть объединены в лес

Основные понятия службы каталогов

- ***Лесом*** называется одно или несколько деревьев, которые не образуют непрерывного пространства имен.
- Все деревья одного *леса* имеют общие логическую структуру, конфигурацию и глобальный каталог.
- Все деревья данного *леса* поддерживают друг с другом транзитивные иерархические *доверительные отношения*, устанавливаемые на основе протокола Kerberos.

Основные понятия службы каталогов

- В отличие от дерева, *лес* может не иметь какого-то определенного имени.
- *Лес* существует в виде совокупности объектов с перекрестными ссылками и доверительных отношений на основе протокола Kerberos, установленных для входящих в *лес* деревьев.
- Поддержка протокола Kerberos требует, чтобы деревья одного *леса* составляли иерархическую структуру: имя дерева, располагающегося в корне этой структуры, может использоваться для обозначения всего данного *леса* деревьев.

Основные понятия службы каталогов

- *Организационные единицы* (Organizational Units, OU) или *организационные подразделения* (ОП) позволяют разделять домен на зоны административного управления, т. е. создавать единицы административного управления внутри домена.
  - По расположению
  - По функциям
  - По орг.структуре
- В основном это дает возможность делегировать административные задачи в домене.
- До появления Active Directory домен был наименьшим контейнером, которому могли быть назначены административные разрешения.

Основные понятия службы каталогов

- ***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.
  - Определение узла как совокупности подсетей позволяет администратору быстро и без больших затрат настроить топологию доступа и репликации в Active Directory и полнее использовать достоинства физического расположения устройств в сети.

Основные понятия службы каталогов

- Сайты являются способом физической (а не логической) группировки на основе подсетей IP.
- Сайты подразделяются на имеющие подключения по низкоскоростным каналам (например по каналам глобальных сетей, с помощью виртуальных частных сетей) и по высокоскоростным каналам (например через локальную сеть).
- Сайт может содержать один или несколько доменов, а домен может содержать один или несколько сайтов.
- При проектировании Active Directory важно учитывать сетевой трафик, создающийся при синхронизации данных AD между сайтами

Основные понятия службы каталогов

- Когда пользователь входит в систему, клиент Active Directory ищет серверы Active Directory, расположенные в узле пользователя. Поскольку компьютеры, принадлежащие к одному узлу, в масштабах сети можно считать расположенными близко друг к другу, связь между ними должна быть быстрой, надежной и эффективной.
- Распознавание локального узла в момент входа в систему не составляет труда, так как рабочая станция пользователя уже знает, в какой из подсетей TCP/IP она находится, а подсети напрямую соответствуют узлам Active Directory.

Архитектура Active Directory
Модель данных

- Active Directory хранит информацию о сетевых ресурсах:
  - данные пользователей
  - описания принтеров
  - описания серверов
  - описания баз данных
  - группы
  - компьютеры
  - политики безопасности

называются *объектами*.

Архитектура Active Directory
Модель данных

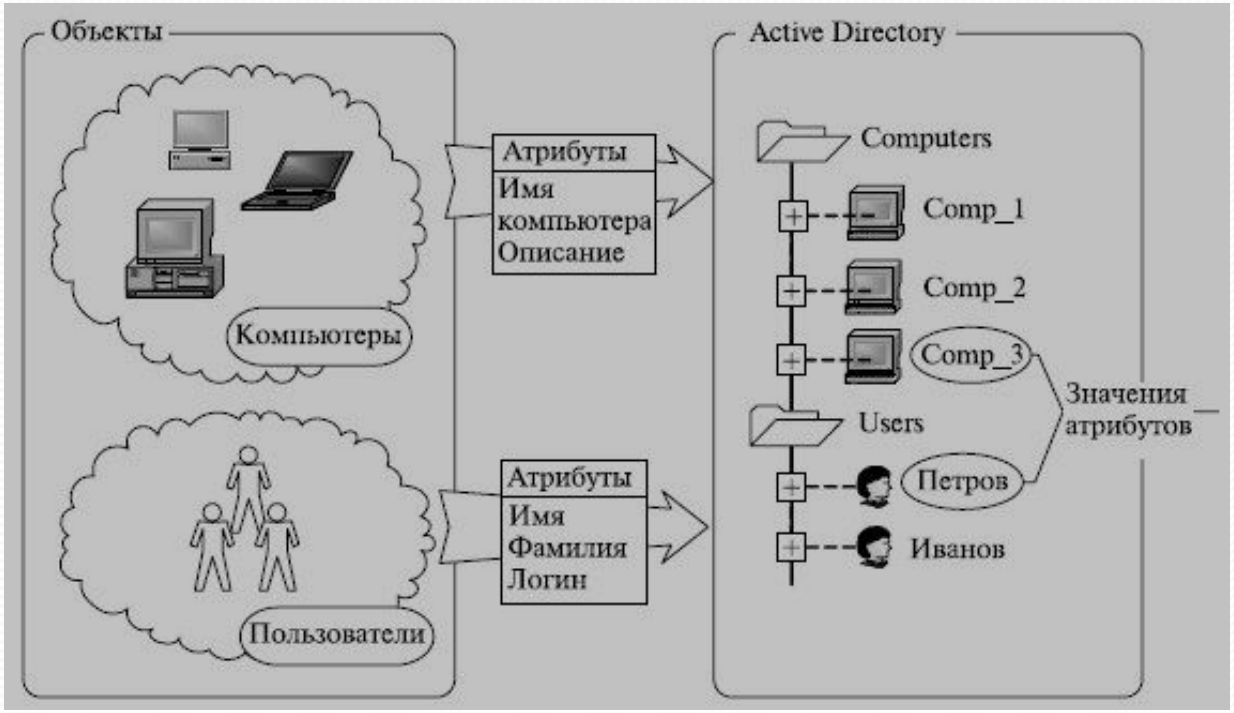


Схема объектов Active Directory и их атрибуты

- Объект - это отдельный именованный набор атрибутов, которыми представлен сетевой ресурс.

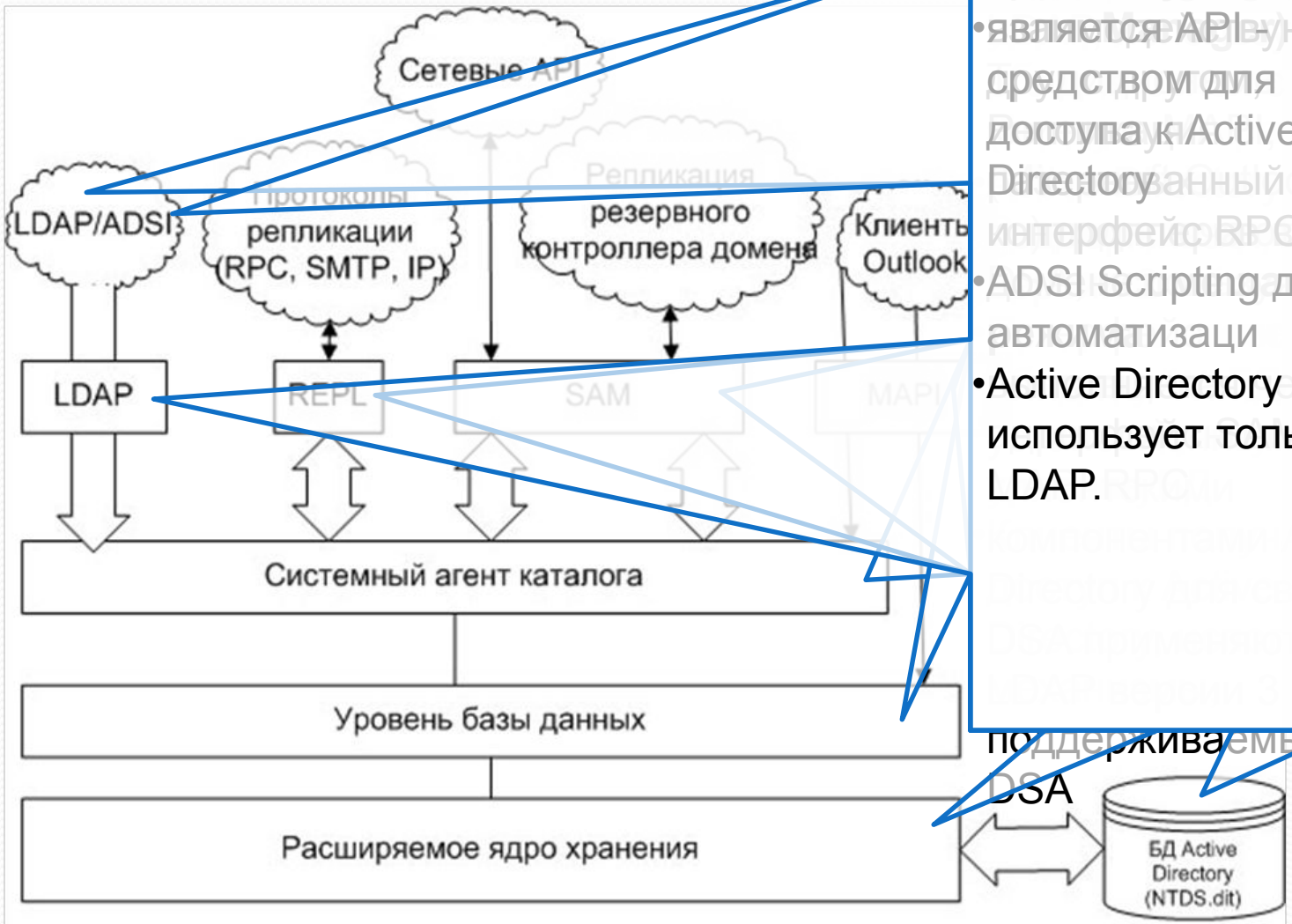
Архитектура Active Directory
Модель данных

- Для каждого класса объектов *логическая структура* определяет
  - какие атрибуты обязательно должен иметь представитель данного класса
  - какие дополнительные атрибуты он может иметь
  - какой класс объектов может являться родительским по отношению к данному классу.

Архитектура Active Directory
Модель данных

- **Схема Active Directory**
  - содержит формальное описание содержания и структуры Active Directory
    - все атрибуты,
    - классы,
    - свойства классов.

Архитектура Active Directory
Функциональная структура



LDAP/ADSI (Active Directory Service Interface)

- является API – средством для доступа к Active Directory
- ADSI Scripting для автоматизаци
- Active Directory использует только LDAP.

Многоуровневая архитектура Active Directory

Архитектура Active Directory
База данных Active Directory

Содержит структурные объекты:

- Разделы (сегменты)
- Домены
- Деревья доменов
- Леса
- Сайты
- Организационные единицы